

BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG



BÁO CÁO CUỐI KÌ QUẢN TRỊ HỆ THỐNG MẠNG  
TRIỂN KHAI, QUẢN LÝ, CẤU HÌNH BẢO  
MẬT VÀ THEO DÕI SỰ VI PHẠM (GUI)

Người hướng dẫn: GV. LÊ VIỆT THANH  
Người thực hiện: LÊ ĐÌNH KHÁNH – 52200250  
LÊ ĐỨC HIỀN – 52200251  
Lớp: Nhóm 02  
Khóa: 26

HỒ CHÍ MINH – 2024

## LỜI CẢM ƠN

Trước tiên, chúng em xin gửi lời cảm ơn chân thành đến thầy Lê Việt Thanh đã luôn tận tình chỉ bảo, hướng dẫn và giúp đỡ chúng em trong suốt quá trình thực hiện đề tài báo cáo. Sự giúp đỡ và những chỉ dẫn quý báu của thầy đã giúp chúng em hoàn thành bài báo cáo này một cách tốt nhất.

Chúng em cũng xin cảm ơn Trường đại học Tôn Đức Thắng đã tạo điều kiện cho chúng em có cơ hội tiếp cận và tìm hiểu sâu hơn. Đây là cơ hội quý giá giúp chúng em phát triển kiến thức và kỹ năng trong quá trình học tập và nghiên cứu.

Chúng em hy vọng rằng những kiến thức và kinh nghiệm thu được từ quá trình thực hiện đề tài sẽ là nền tảng hữu ích cho những nghiên cứu và công việc sau này.

# ĐỒ ÁN ĐƯỢC HOÀN THÀNH TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của Thầy Lê Viết Thanh. 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 đồ 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 đồ 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 08 tháng 12 năm 2024

Tác giả

(ký tên và ghi rõ họ tên)

Lê Đức Hiền

Lê Đình Khánh

## TÓM TẮT

Báo cáo tập trung vào việc triển khai, quản lý và bảo mật hệ thống mạng thông qua Windows Server, chia thành ba chương chính:

### Chương 1: Cơ sở lý thuyết

Cung cấp nền tảng lý thuyết về các công cụ và kỹ thuật quản trị mạng, gồm:

### Chương 2: Thiết lập máy chủ và máy trạm

Hướng dẫn cấu hình máy chủ Windows Server (Server-DC-01) làm Domain Controller, quản lý tài nguyên và người dùng trong mạng. Đồng thời, cấu hình các máy trạm (Client1, Client2) để kết nối và tương tác với máy chủ.

### Chương 3: Cấu hình theo kịch bản

Triển khai các kịch bản thực tế nhằm tăng cường quản lý và bảo mật mạng:

- Quy tắc đặt mật khẩu, giám sát đăng nhập.
- Giám sát truy cập tệp, thư mục quan trọng và thay đổi tài khoản trong Active Directory.
- Cấu hình tường lửa bảo vệ hệ thống và phòng chống các cuộc tấn công DDoS.

Báo cáo mang tính ứng dụng cao, kết hợp lý thuyết và thực hành, giúp xây dựng hệ thống mạng bảo mật, ổn định và dễ quản lý.

# MỤC LỤC

<b>1 CHƯƠNG 1: CƠ SỞ LÝ THUYẾT</b>	<b>1</b>
1.1 Group Policy Object (GPO) . . . . .	1
1.1.1 Định Nghĩa và Khái Niệm GPO . . . . .	1
1.1.2 Cấu Trúc và Thành Phần của GPO . . . . .	1
1.1.3 Quy Trình Hoạt Động của GPO . . . . .	2
1.1.4 Vai Trò của GPO trong Quản Trị Mạng . . . . .	2
1.1.5 Ưu và Nhược Điểm của GPO . . . . .	3
1.2 Audit . . . . .	3
1.2.1 Định Nghĩa Audit . . . . .	3
1.2.2 Ý Nghĩa và Vai Trò Của Audit . . . . .	4
1.2.3 Các Thành Phần Chính Trong Audit . . . . .	4
1.2.4 Triển Khai Audit Trên Windows Server . . . . .	4
1.2.5 Ưu và Nhược Điểm của GPO . . . . .	5
1.3 Firewall . . . . .	5
1.3.1 Định Nghĩa và Khái Niệm Firewall . . . . .	5
1.3.2 Chức Năng Của Firewall . . . . .	5
1.3.3 Kiến Trúc Firewall . . . . .	6
1.3.4 Ưu và Nhược Điểm của Firewall . . . . .	6
1.4 Distributed Denial of Service (DDoS) . . . . .	7
1.4.1 Định Nghĩa và Khái Niệm DDoS . . . . .	7
1.4.2 Cơ chế hoạt động và hậu quả DDoS . . . . .	7
1.4.3 Các dạng tấn công DDoS . . . . .	8
1.4.4 Cách Phòng Chống DDoS . . . . .	8
1.4.5 Ưu và Nhược Điểm của Firewall . . . . .	9
<b>2 CHƯƠNG 2: THIẾT LẬP MÁY</b>	<b>10</b>
2.1 Máy Server-DC-01 . . . . .	10

2.2 Máy Client1 . . . . .	24
2.3 Máy Client2 . . . . .	31
<b>3 CHƯƠNG 3: CẤU HÌNH VỚI KỊCH BẢN</b>	<b>33</b>
3.1 Kịch bản 1: Cấu hình quy tắc đặt mật khẩu và giám sát đăng nhập . . . . .	33
3.2 Kịch bản 2: Giám sát truy cập các thư mục và tệp quan trọng	44
3.3 Kịch bản 3: Giám sát việc thay đổi tài khoản trong Active Directory . . . . .	56
3.4 Kịch bản 4: Giám sát các thay đổi trong GPO . . . . .	62
3.5 Kịch bản 5: Cấu hình Firewall . . . . .	68
3.6 Kịch bản 6: Cấu hình phòng chống DDoS và giám sát IP truy cập vào Web Server . . . . .	78

## DANH SÁCH HÌNH ẢNH

1	Vào Control Panel . . . . .	10
2	Vào Network and Internet . . . . .	11
3	Vào Network and Sharing Center . . . . .	11
4	Vào Change adapter settings . . . . .	12
5	Vào Ethernet0 . . . . .	12
6	Vào Properties . . . . .	12
7	Vào Internet Protocol Version 4 . . . . .	13
8	Vào Server Manager . . . . .	14
9	Tải ADDS . . . . .	14
10	Tải ADDS . . . . .	15
11	Tải ADDS . . . . .	15
12	Tải ADDS . . . . .	16
13	Tải ADDS . . . . .	16
15	Tải ADDS . . . . .	17
14	Tải ADDS . . . . .	17
16	Tải ADDS . . . . .	18
17	Tải ADDS . . . . .	18
18	Tải ADDS . . . . .	19
19	Tạo domain . . . . .	19
20	Tạo domain . . . . .	20
21	Tạo domain . . . . .	20
22	Tạo domain . . . . .	21
23	Tạo domain . . . . .	21
24	Tạo domain . . . . .	22
25	Tạo domain . . . . .	22
26	Tạo domain . . . . .	23

27	Restart máy . . . . .	23
28	Kiểm tra máy . . . . .	24
29	Kiểm tra máy . . . . .	24
30	Vào Control Panel . . . . .	25
31	Vào Network và Internet . . . . .	25
32	Vào Network and Sharing Center . . . . .	26
33	Vào Change adapter settings . . . . .	26
34	Thiết lập IP . . . . .	27
35	Thiết lập IP . . . . .	27
36	Thiết lập IP . . . . .	27
37	Thêm máy Client1 vào domain . . . . .	28
38	Thêm máy Client1 vào domain . . . . .	29
39	Thêm máy Client1 vào domain . . . . .	30
40	Thêm máy Client1 vào domain . . . . .	30
41	Thêm máy Client1 vào domain . . . . .	30
42	Thêm máy Client1 vào domain . . . . .	31
43	Máy Client2 . . . . .	31
44	Máy Client2 . . . . .	32
45	Server Manager > Dashboard và chọn Tools > Group Policy Management . . . . .	33
46	Tạo kịch bản 1 . . . . .	34
47	Tùy chỉnh GPO kịch bản 1 . . . . .	35
48	Password Policy . . . . .	36
49	Minimum password length . . . . .	36
50	Password complexity requirements . . . . .	37
51	Maximum password age . . . . .	37
52	Switching ip address . . . . .	38
53	gpupdate /force . . . . .	39
54	Audit Policies > Logon/Logoff . . . . .	40

55	Bật tính năng audit . . . . .	40
56	Liên kết GPO kích ban 1 vào Domain Control . . . . .	41
57	Event Viewer . . . . .	42
58	Đăng nhập thất bại . . . . .	42
59	Kiểm tra log . . . . .	43
60	Tạo folder . . . . .	44
61	Chọn Advanced Sharing . . . . .	45
62	Cấu hình Permission . . . . .	46
63	Security > Advanced . . . . .	47
64	Auditing > Add . . . . .	48
65	Add > Select a Principal . . . . .	48
66	Điền Everyone rồi nhấn Check Names > OK . . . . .	49
67	Cài đặt Auditing Entry . . . . .	49
68	Tạo GPO kịch bản 2 . . . . .	50
69	Chọn Audit File System cho cả sự kiện Success and Failure	50
70	Liên kết kịch bản 2 vào Domain Control . . . . .	51
71	gpupdate /force . . . . .	51
72	Windows 8.1 > Network . . . . .	52
73	SERVER-DC-01 > Kích ban 2 . . . . .	52
74	Tạo và xóa file . . . . .	53
75	Kiểm tra Event Viewer . . . . .	53
76	Tìm log ID 4660 . . . . .	54
77	Điền log ID . . . . .	54
78	Hoàn thành task . . . . .	55
79	Sau khi có một file bị xóa thông báo sẽ hiển thị . . . . .	55
80	Nhấn chuột phải vào <b>Group Policy Objects</b> rồi chọn <b>New</b> để tạo GPO “Kích ban 3” . . . . .	56

81 Chọn <b>Audit Application Group Management</b> và <b>Audit User Account Management</b> cho cả sự kiện <b>Success and Failure</b> . . . . .	57
82 . . . . .	57
83 gpupdate /force . . . . .	58
84 Vào tạo 1 user mới . . . . .	58
85 Trong Event Viewer, điều hướng đến: Windows Logs > Security. . . . .	59
86 Tạo popup . . . . .	59
87 hoàn thành task . . . . .	60
88 Tạo đoạn thông báo tin . . . . .	60
89 Sau khi có một tài khoản bị xóa thông báo sẽ hiển thị . . . . .	61
90 Nhấn chuột phải vào <b>Group Policy Objects</b> rồi chọn <b>New</b> để tạo GPO “Kích ban 4” . . . . .	62
91 . . . . .	63
92 Chọn <b>Audit Audit Policy Change</b> và bật cho cả sự kiện <b>Success and Failure</b> . . . . .	64
93 Liên kết GPO kịch bản 4 vào domain control . . . . .	64
94 gpupdate /force . . . . .	65
95 Tạo GPO demo > Click chuột phải vào GPO demo Chọn Edit và test thử . . . . .	65
96 Liên kết GPO vào domain control . . . . .	66
97 gpupdate /force . . . . .	66
98 Tìm mã <b>4719</b> : Đặt lại Audit Policy. . . . .	67
99 Diền tên cho GPO mới tạo là “Kích ban 5” và nhấn <b>OK</b> . . . . .	68
100 Group Policy Management Editor . . . . .	69
101 <b>Tại Rule Type</b> chọn <b>Custom</b> . . . . .	70
102 Program > All Programs . . . . .	71
103 Protocol and Ports > Any . . . . .	72

104	Cài đặt IP . . . . .	73
105	Chặn kết nối . . . . .	74
106	Áp dụng rule . . . . .	75
107	Đặt tên . . . . .	76
108	gpupdate /force . . . . .	77
109	Facebook đã bị chặn . . . . .	77
110	Server Manager . . . . .	78
111	Cài đặt Web Server IIS . . . . .	78
112	Tiếp tục cài đặt Web Server IIS . . . . .	79
113	IP and Domain Restrictions . . . . .	79
114	Cài đặt . . . . .	80
115	Internet Information Services (IIS) Manager . . . . .	81
116	Vào Edit Dynamic Restriction Setting . . . . .	81
117	Cấu hình Dynamic Restriction . . . . .	82
118	Kiểm tra P của Web vừa tạo . . . . .	82
119	Request Failed . . . . .	83
120	Nhấn <b>Browse</b> để chọn nơi lưu trữ file thông tin. Rồi chọn <b>Apply</b> . . . . .	84
121	Lịch sử các IP đã truy cập vào web . . . . .	84

# DANH SÁCH CHỮ VIẾT TẮT

## Danh sách các chữ viết tắt

Viết tắt	Ý nghĩa đầy đủ	Mô tả
AD	Active Directory	Dịch vụ thư mục quản lý tài nguyên mạng.
DNS	Domain Name System	Hệ thống phân giải tên miền thành địa chỉ IP.
GPO	Group Policy Object	Tập hợp các chính sách quản lý tập trung.
IIS	Internet Information Services	Máy chủ web của Microsoft.
IP	Internet Protocol	Giao thức Internet để địa chỉ hóa thiết bị mạng.
DDoS	Distributed Denial of Service	Tấn công từ chối dịch vụ phân tán.
OU	Organizational Unit	Đơn vị tổ chức trong Active Directory.
SIEM	Security Information and Event Management	Hệ thống quản lý bảo mật và sự kiện.
TCP	Transmission Control Protocol	Giao thức truyền dữ liệu tin cậy.
UDP	User Datagram Protocol	Giao thức truyền dữ liệu không tin cậy.
ISO	International Organization for Standardization	Tổ chức tiêu chuẩn hóa quốc tế.
HIPAA	Health Insurance Portability and Accountability Act	Đạo luật về bảo mật thông tin y tế.
GDPR	General Data Protection Regulation	Quy định bảo vệ dữ liệu chung của EU.
IDS	Intrusion Detection System	Hệ thống phát hiện xâm nhập.
IPS	Intrusion Prevention System	Hệ thống ngăn chặn xâm nhập.

Bảng 1: Danh sách các chữ viết tắt và ý nghĩa

# 1 CHƯƠNG 1: CƠ SỞ LÝ THUYẾT

## 1.1 Group Policy Object (GPO)

### 1.1.1 Định Nghĩa và Khái Niệm GPO

- Group Policy Object (GPO): Là tập hợp các quy tắc (policies) được quản lý tập trung, áp dụng cho tài khoản người dùng và máy tính trong một môi trường domain (Active Directory).
- Mục tiêu: Đảm bảo quản lý hiệu quả, tăng cường bảo mật và thiết lập môi trường làm việc nhất quán.

### 1.1.2 Cấu Trúc và Thành Phần của GPO

#### • Cấu trúc GPO

- Computer Configuration: Các chính sách áp dụng khi máy tính khởi động. Dùng để quản lý cài đặt hệ điều hành, dịch vụ hệ thống, bảo mật mạng.
- User Configuration: Các chính sách áp dụng khi người dùng đăng nhập. Dùng để quản lý môi trường làm việc, phần mềm, và quyền truy cập.

#### • Thành phần của GPO

- Core Policies: Administrative Templates gồm các mẫu chính sách định sẵn. Security Settings gồm các cài đặt bảo mật như tường lửa, quyền truy cập, mã hóa.
- Preferences: Cho phép tùy chỉnh linh hoạt hơn, như ánh xạ ổ đĩa, cài đặt máy in.
- Scripts: Hỗ trợ chạy các tập lệnh (Startup, Shutdown, Logon, Logoff).
- Folder Redirection: Chuyển hướng các thư mục hệ thống của người dùng (Documents, Desktop).

### 1.1.3 Quy Trình Hoạt Động của GPO

- Bước 1: Tạo GPO: Quản trị viên tạo GPO trong Group Policy Management Console (GPMC).
- Bước 2: Liên kết GPO (Link): GPO được liên kết với các đối tượng trong Active Directory
  - Sites: Áp dụng cho các site mạng.
  - Domains: Áp dụng cho toàn bộ domain.
  - Organizational Units (OUs): Áp dụng cho các nhóm máy tính hoặc người dùng trong OU.
- Bước 3: Thứ tự Ưu tiên (Order of Precedence):
  - Chính sách sẽ được áp dụng theo thứ tự: Local Policies → Site → Domain → OU
  - Nếu có xung đột, chính sách ở mức OU có ưu tiên cao hơn.
- Bước 4: Cập nhật GPO: Các chính sách được thực thi khi:
  - Máy tính khởi động hoặc người dùng đăng nhập.
  - Dùng lệnh: gpupdate /force để áp dụng ngay lập tức.

### 1.1.4 Vai Trò của GPO trong Quản Trị Mạng

- Quản lý môi trường hệ thống: Cấu hình tự động các máy tính và tài khoản người dùng, giảm thiểu công việc thủ công.
- Cải thiện bảo mật:
  - Chính sách bảo mật người dùng: Bắt buộc sử dụng mật khẩu phức tạp. Đặt giới hạn số lần đăng nhập sai (Account Lockout Policy).
  - Chính sách bảo mật máy tính: Tắt cổng USB hoặc CD/DVD. Tăng cường bảo vệ mạng thông qua Windows Firewall Rules.

- Quản lý phần mềm: Triển khai và cập nhật phần mềm tự động. Gỡ bỏ hoặc hạn chế phần mềm không được phép sử dụng.
- Kiểm soát tài nguyên: Áp dụng chính sách hạn chế quyền truy cập file, folder. Chuyển hướng thư mục hệ thống để lưu trữ tập trung.

#### 1.1.5 *Ưu và Nhược Điểm của GPO*

- **Ưu điểm**
  - Tập trung hóa quản lý: Quản trị viên dễ dàng cấu hình cho toàn hệ thống từ một nơi.
  - Tính nhất quán: Tạo môi trường làm việc đồng nhất cho người dùng.
  - Tăng cường bảo mật: Dễ dàng áp dụng các chính sách bảo mật.
- **Nhược điểm**
  - Phức tạp: Khi hệ thống lớn, việc quản lý nhiều GPO có thể gây khó khăn.
  - Khả năng xung đột: Các GPO không được cấu hình đúng thứ tự có thể gây lỗi.
  - Phụ thuộc Windows Server: GPO chỉ hoạt động tốt trong môi trường Windows.

## 1.2 Audit

### 1.2.1 *Định Nghĩa Audit*

- Audit là quá trình theo dõi và ghi lại các sự kiện trong hệ thống mạng hoặc máy tính nhằm tăng cường bảo mật, hỗ trợ quản trị, và đáp ứng các yêu cầu tuân thủ pháp lý. Audit thường được triển khai trong môi trường doanh nghiệp để giám sát hành vi của người dùng và trạng thái hệ thống.

### 1.2.2 Ý Nghĩa và Vai Trò Của Audit

- Giám sát hoạt động: Theo dõi các hành vi đăng nhập, truy cập tài nguyên, và thay đổi trên hệ thống.
- Bảo vệ hệ thống: Phát hiện các hành vi đáng ngờ hoặc vi phạm, như truy cập trái phép hoặc tấn công mạng.
- Hỗ trợ điều tra: Cung cấp dữ liệu lịch sử để phân tích sự cố hoặc xử lý khi xảy ra vấn đề.
- Đáp ứng tuân thủ: Đáp ứng yêu cầu của các tiêu chuẩn bảo mật như ISO 27001, HIPAA, và GDPR.

### 1.2.3 Các Thành Phần Chính Trong Audit

- Audit Policy (Chính sách kiểm tra): Định nghĩa những gì cần theo dõi, ví dụ:
  - Đăng nhập/dăng xuất (Logon/Logoff).
  - Quản lý tài khoản (Account Management).
  - Truy cập tài nguyên (Object Access).
  - Thay đổi chính sách (Policy Change).
- Log Audit: Dữ liệu được ghi lại trong hệ thống log, phổ biến nhất là Event Viewer trên Windows.
- Advanced Audit Policy Configuration: Cấu hình chi tiết hơn so với Audit Policy cơ bản, tập trung vào từng hành động cụ thể.

### 1.2.4 Triển Khai Audit Trên Windows Server

- Bật Audit Policy
  - Truy cập Group Policy Management Console (GPMC) hoặc Local Security Policy.

- Bật các chính sách trong: Computer Configuration → Windows Settings → Security Settings → Audit Policy.
- Xem Log Audit
  - Mở Event Viewer: Event Viewer → Security Logs.
  - Phân tích các sự kiện dựa trên Event ID, thời gian, và tài khoản liên quan.
- Tự động hóa theo dõi: Sử dụng các công cụ như SIEM (Splunk, QRadar) để tổng hợp và phân tích log một cách hiệu quả.

### **1.2.5 Ưu và Nhược Điểm của GPO**

- Ưu điểm
  - Theo dõi và phát hiện sự cố nhanh chóng.
  - Cung cấp thông tin chi tiết cho điều tra và phân tích.
  - Đáp ứng các yêu cầu pháp lý về bảo mật.
- Nhược điểm
  - Tốn tài nguyên lưu trữ log.
  - Khó quản lý khi có quá nhiều dữ liệu cần phân tích.
  - Phụ thuộc vào cấu hình chính xác để đạt hiệu quả cao.

## **1.3 Firewall**

### **1.3.1 Định Nghĩa và Khái Niệm Firewall**

- Firewall là công cụ bảo mật tích hợp trong hệ điều hành Windows Server, giúp quản lý và kiểm soát luồng dữ liệu vào/ra hệ thống mạng. Nó hoạt động như một tường lửa để bảo vệ máy chủ khỏi các truy cập trái phép và mối đe dọa từ bên ngoài.

### **1.3.2 Chức Năng Của Firewall**

- Lọc lưu lượng mạng: Kiểm soát kết nối dựa trên quy tắc cho phép hoặc từ chối các gói dữ liệu.

- Bảo vệ máy chủ: Ngăn chặn các cuộc tấn công từ bên ngoài, như DDoS, brute force.
- Quản lý linh hoạt: Cung cấp tùy chọn bật/tắt tường lửa hoặc cấu hình chi tiết từng dịch vụ.
- Tích hợp với Group Policy: Quản lý chính sách tường lửa tập trung trên các máy trạm trong hệ thống.

#### **1.3.3 Kiến Trúc Firewall**

- Firewall Rules (Quy tắc tường lửa)
  - Các quy tắc xác định cách xử lý gói dữ liệu vào hoặc ra.
  - Gồm ba loại: Inbound Rules dùng kiểm soát lưu lượng vào. Outbound Rules dùng kiểm soát lưu lượng ra. Connection Security Rules dùng xác định kết nối bảo mật giữa các máy chủ.
- Profile Types: Firewall hoạt động dựa trên các profile để áp dụng quy tắc phù hợp với môi trường mạng.
  - Domain Profile: Dành cho các kết nối thuộc domain.
  - Private Profile: Dành cho mạng nội bộ tin cậy.
  - Public Profile: Dành cho mạng không tin cậy (như Wi-Fi công cộng).

#### **1.3.4 Ưu và Nhược Điểm của Firewall**

- Ưu điểm
  - Tích hợp sẵn trong hệ điều hành, dễ sử dụng.
  - Quản lý chi tiết các quy tắc.
  - Hỗ trợ bảo mật toàn diện với các profile khác nhau.
  - Tương thích với Group Policy để quản lý tập trung.
- Nhược điểm

- Khả năng bảo mật hạn chế so với tường lửa phần cứng.
- Phụ thuộc vào cấu hình chính xác.
- Có thể gây gián đoạn nếu cấu hình sai

## 1.4 Distributed Denial of Service (DDoS)

### 1.4.1 Định Nghĩa và Khái Niệm DDoS

- DDoS (Distributed Denial of Service) là một dạng tấn công mạng phổ biến, trong đó kẻ tấn công sử dụng nhiều máy tính hoặc thiết bị bị kiểm soát để làm quá tải tài nguyên của một máy chủ, dịch vụ, hoặc mạng, dẫn đến tình trạng không thể phục vụ người dùng hợp pháp. Đây là một trong những mối đe dọa an ninh mạng lớn đối với hệ thống thông tin.

### 1.4.2 Cơ chế hoạt động và hậu quả DDoS

#### • Cơ Chế Hoạt Động

- Kẻ tấn công phát tán phần mềm độc hại để chiếm quyền điều khiển các thiết bị (botnet).
- Các thiết bị trong botnet gửi một lượng lớn yêu cầu đến mục tiêu (máy chủ hoặc dịch vụ).
- Mục tiêu bị quá tải tài nguyên (CPU, băng thông) và không thể xử lý yêu cầu hợp pháp.

#### • Hậu Quả

- Gián đoạn dịch vụ: Website, ứng dụng, hoặc máy chủ ngừng hoạt động.
- Thiệt hại tài chính: Do mất khách hàng, gián đoạn kinh doanh, và chi phí khôi phục.
- Ảnh hưởng uy tín: Làm giảm lòng tin của khách hàng và đối tác.

- Chiếm dụng tài nguyên: Hệ thống bị tấn công tiêu tốn tài nguyên vào việc xử lý lưu lượng không hợp pháp.

#### 1.4.3 Các dạng tấn công DDoS

- Tấn Công Băng Thông (Volumetric Attacks):
  - Mục tiêu: Tiêu tốn toàn bộ băng thông của mục tiêu.
  - Phương thức: Gửi một lượng lớn lưu lượng đến mạng mục tiêu.
  - Ví dụ: UDP Flood, ICMP Flood (Ping Flood).
- Tấn Công Giao Thức (Protocol Attacks):
  - Mục tiêu: Làm dụng giao thức mạng để làm cạn kiệt tài nguyên của máy chủ.
  - Phương thức: Tấn công vào tầng giao thức như TCP, UDP, hoặc ICMP.
- Tấn Công Ứng Dụng (Application Layer Attacks):
  - Mục tiêu: Làm cạn kiệt tài nguyên của ứng dụng hoặc dịch vụ cụ thể.
  - Phương thức: Gửi yêu cầu phức tạp đến ứng dụng như HTTP GET/POST.
  - Ví dụ: HTTP Flood, Slowloris.

#### 1.4.4 Cách Phòng Chống DDoS

- Tăng Cường Hạ Tầng
  - Tăng băng thông: Mở rộng băng thông mạng để giảm nguy cơ quá tải.
  - Load Balancer: Phân phối lưu lượng giữa các máy chủ để tránh tập trung tại một điểm.
- Sử Dụng Công Cụ Chuyên Dụng

- Firewall và IPS/IDS: Phát hiện và chặn các luồng dữ liệu bất thường.
- DDoS Mitigation Services: Dịch vụ như Cloudflare, Akamai, hoặc AWS Shield giúp lọc lưu lượng tấn công.
- Triển Khai Chính Sách Bảo Mật
  - Rate Limiting: Giới hạn số lượng yêu cầu từ một nguồn cụ thể.
  - Access Control: Chặn lưu lượng từ các IP đáng ngờ hoặc khu vực địa lý cụ thể.
  - Tăng cường DNS Security: Bảo vệ DNS để tránh bị tấn công DNS Amplification.
- Giám Sát Và Phát Hiện Sớm
  - Giám sát mạng: Sử dụng các công cụ như Nagios, SolarWinds, hoặc Zabbix để theo dõi lưu lượng.
  - Hệ thống cảnh báo: Đặt ngưỡng lưu lượng bất thường để cảnh báo.

#### **1.4.5 Ưu và Nhược Điểm của Firewall**

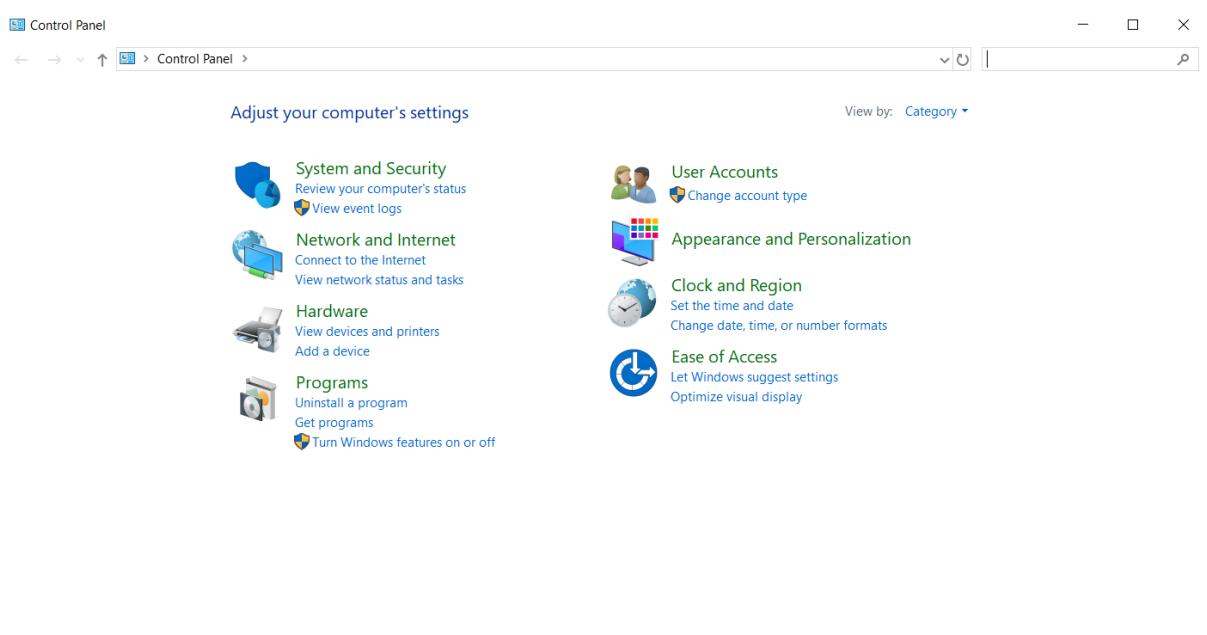
- Ưu điểm
  - Tăng cường bảo mật và khả năng chịu tải của hệ thống.
  - Ngăn chặn các cuộc tấn công nhỏ trước khi chúng gây hậu quả nghiêm trọng.
  - Bảo vệ tài nguyên và giảm chi phí khôi phục sau sự cố.
- Nhược điểm
  - Chi phí cao khi triển khai các biện pháp nâng cao.
  - Cần sự quản trị chuyên sâu và liên tục để phát hiện và ứng phó hiệu quả.

- Một số cuộc tấn công phức tạp vẫn có thể vượt qua các biện pháp bảo vệ.

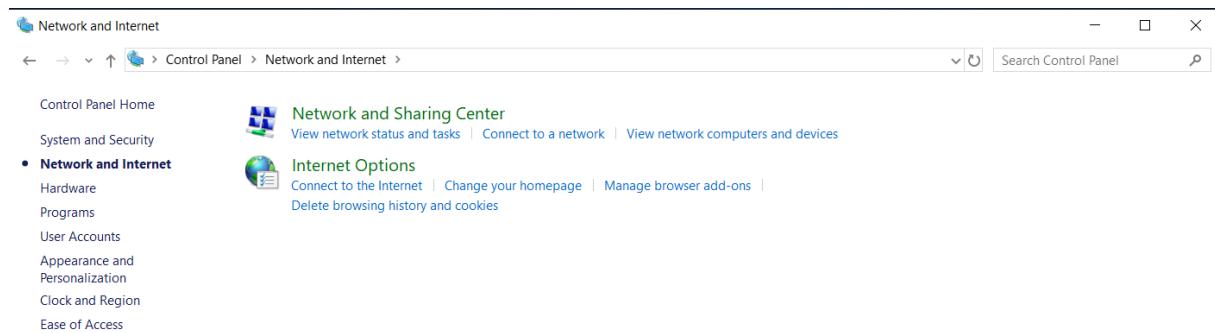
## 2 CHƯƠNG 2: THIẾT LẬP MÁY

### 2.1 Máy Server-DC-01

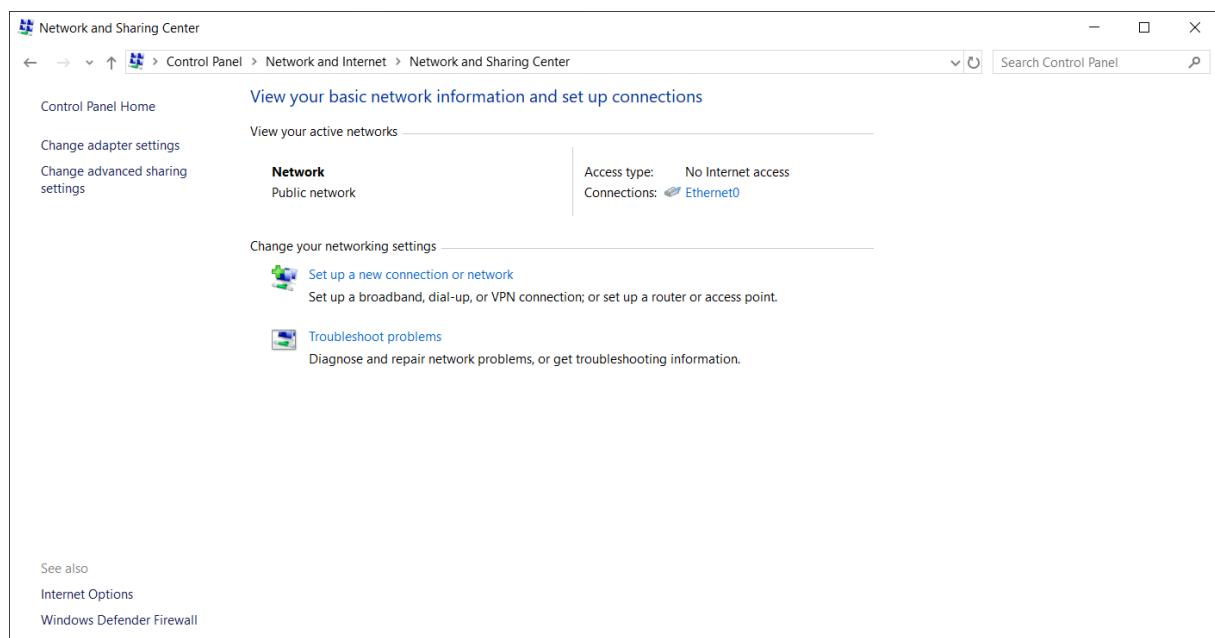
- Thiết lập địa chỉ IP
  - Vào Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings > Ethernet0 > Properties > Internet Protocol Version 4 (TCP/IPv4)



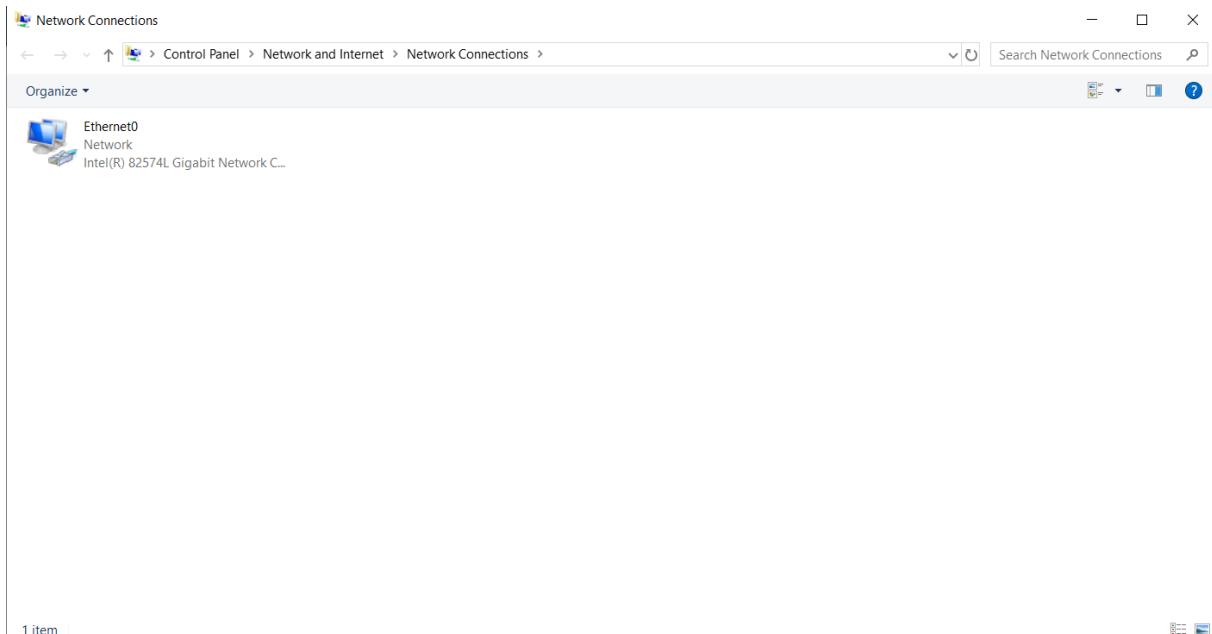
Hình 1: Vào Connntrol Panel



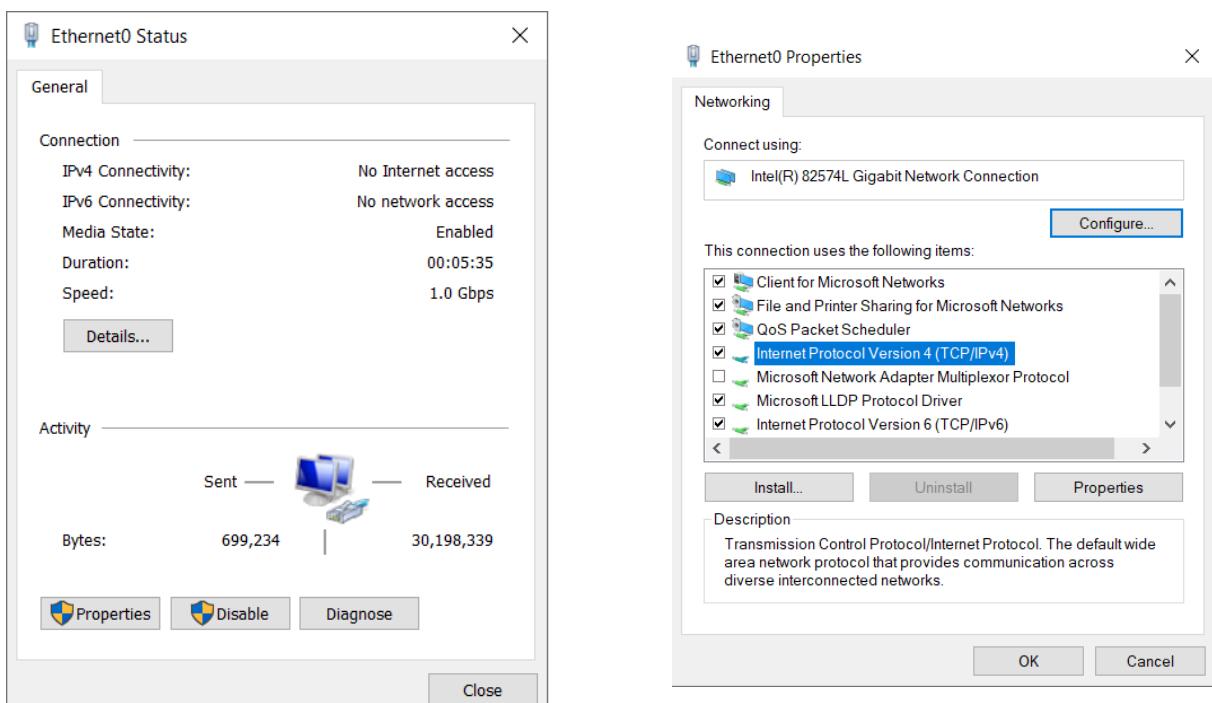
Hình 2: Vào Network and Internet



Hình 3: Vào Network and Sharing Center

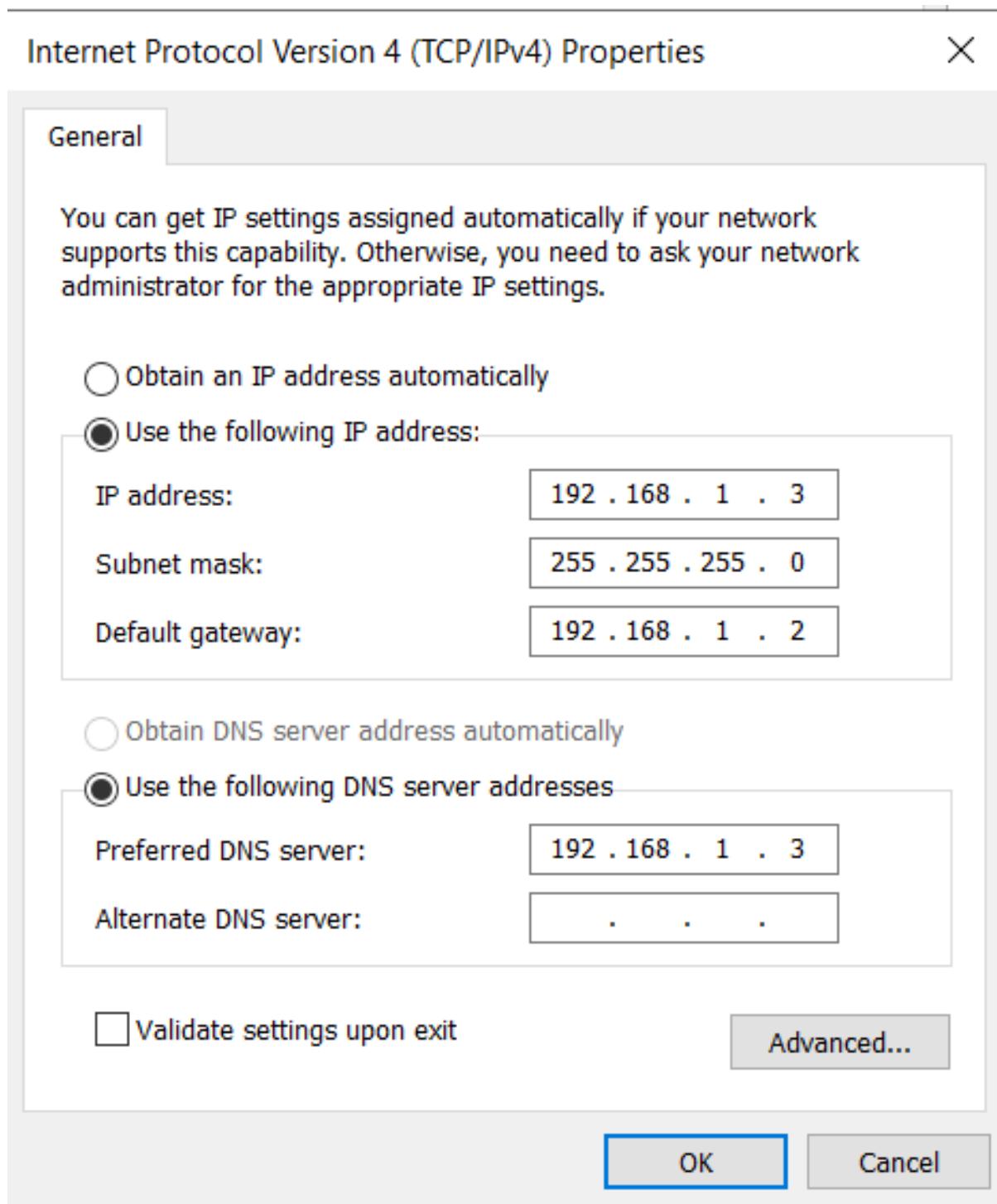


Hình 4: Vào Change adapter settings



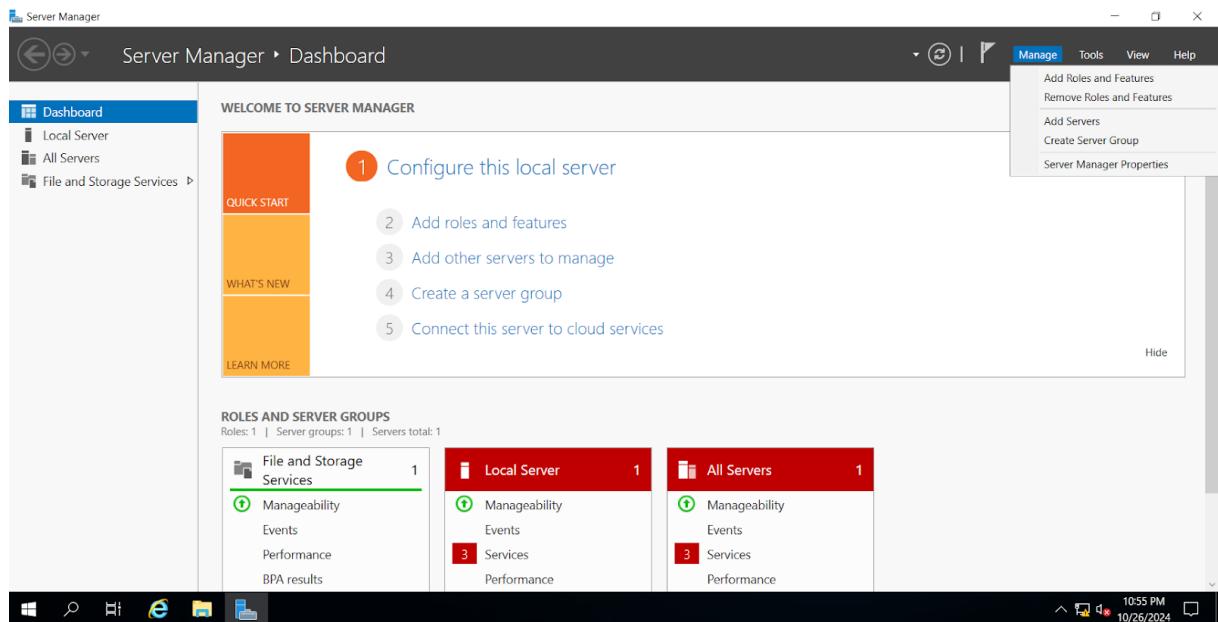
Hình 5: Vào Ethernet0

Hình 6: Vào Properties

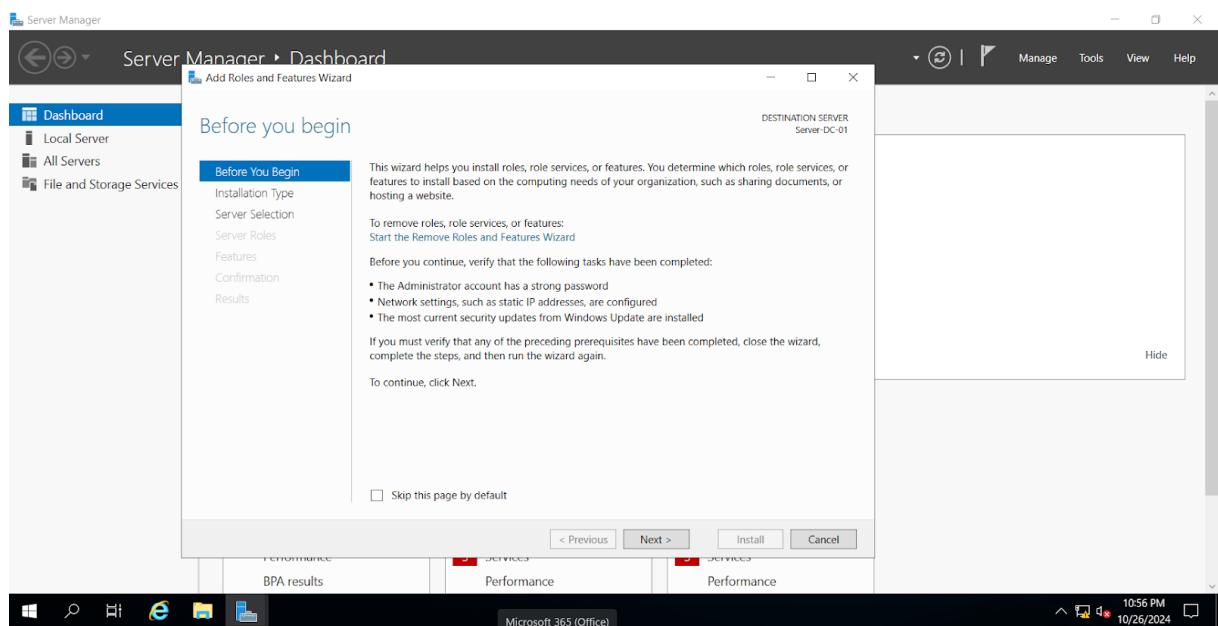


Hình 7: Vào Internet Protocol Version 4

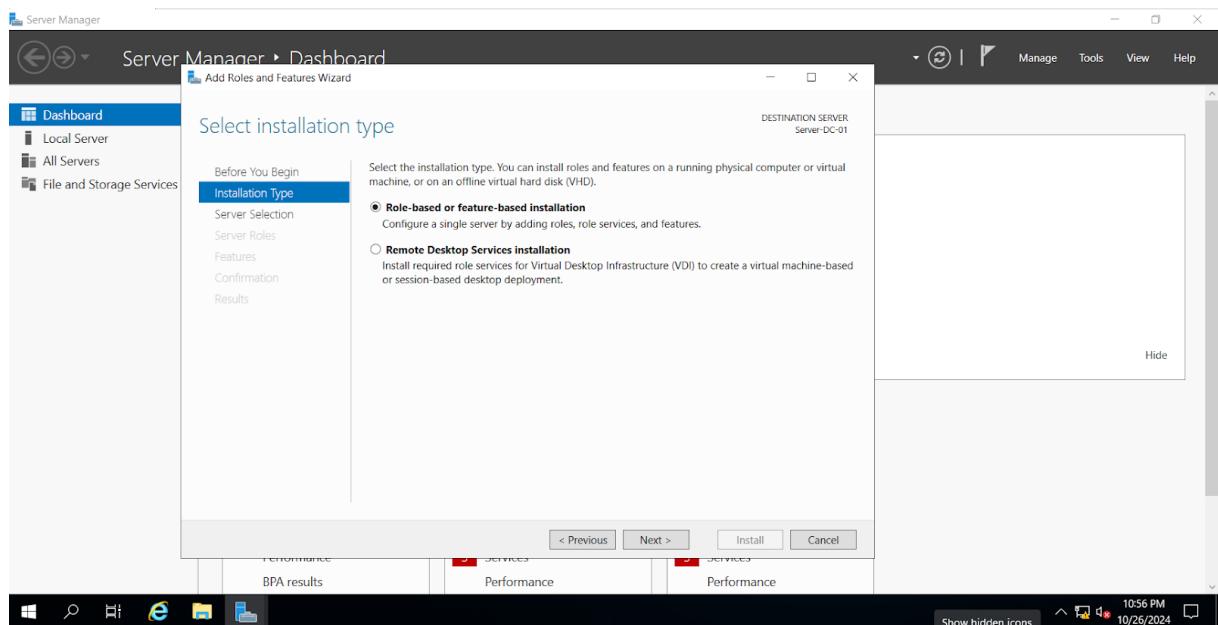
- Nâng cấp máy lên Domain Controller
  - Vào Server Manager > Manager > Add roles and features



Hình 8: Vào Server Manager

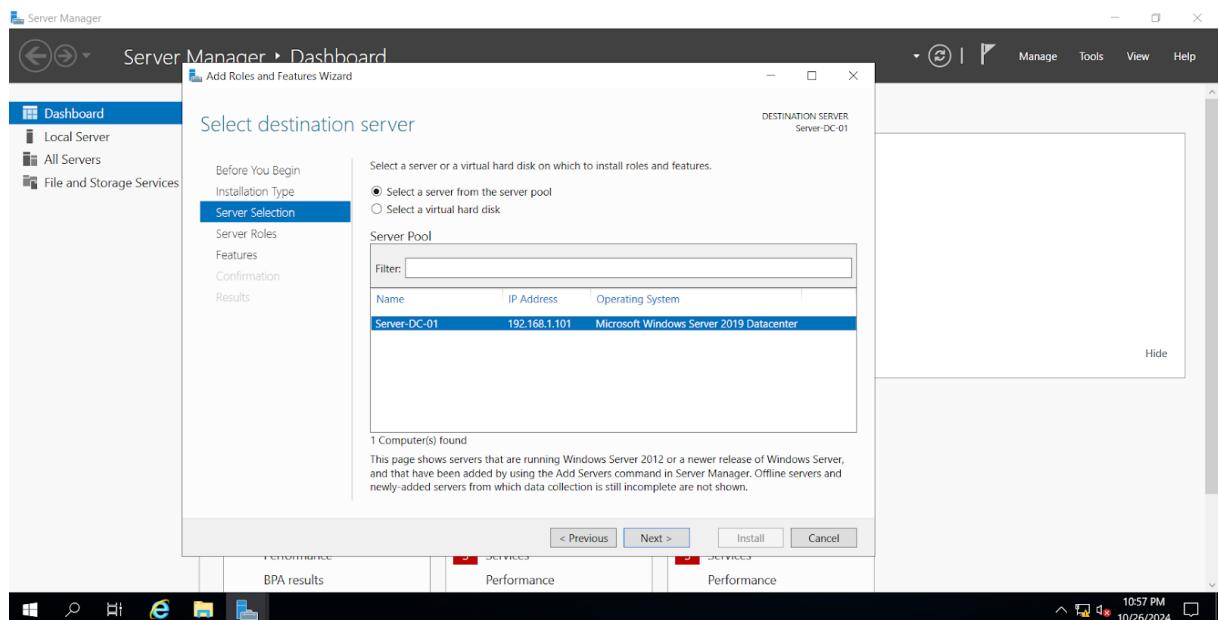


Hình 9: Tải ADDS



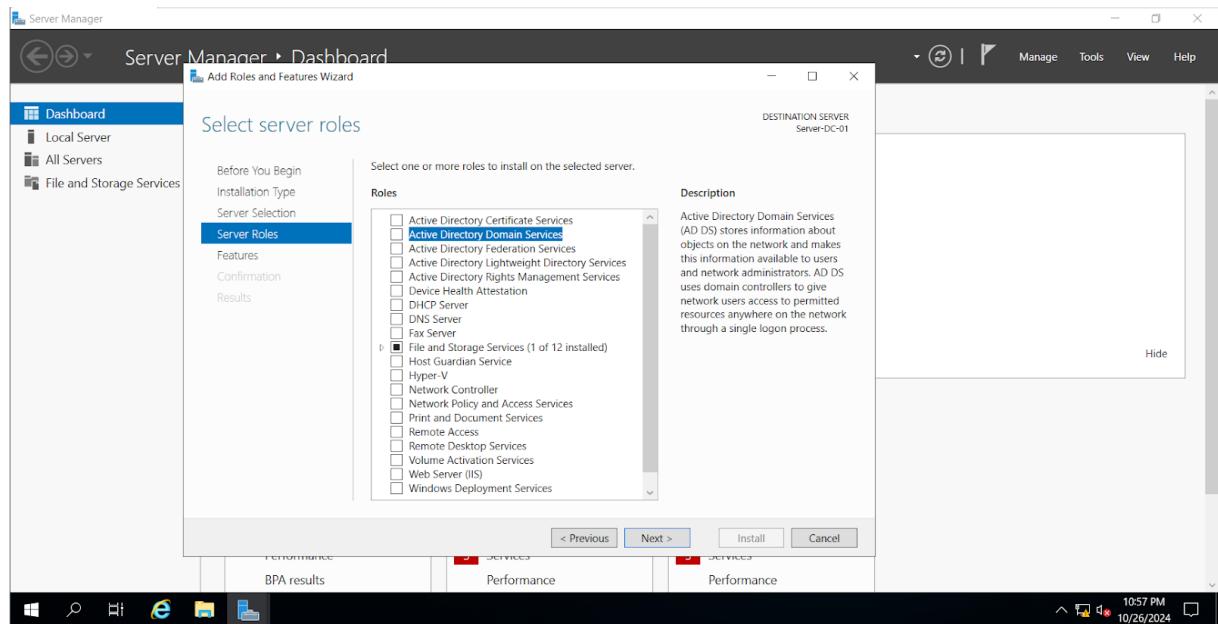
Hình 10: Tải ADDS

- Chọn Role-based or feature-based installation

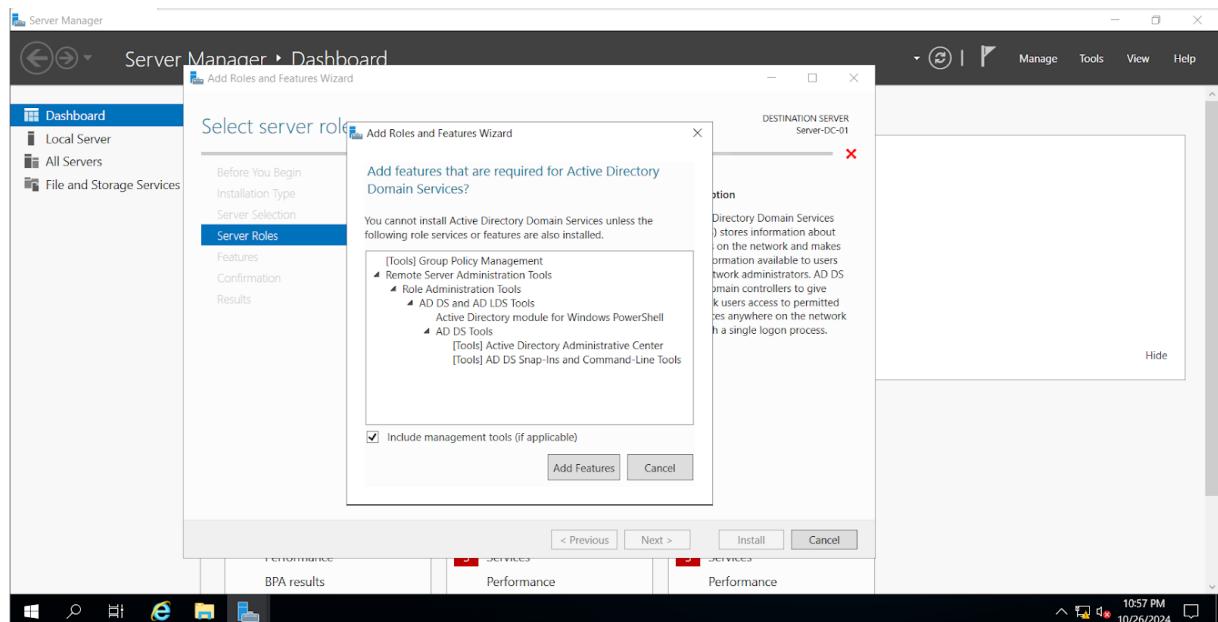


Hình 11: Tải ADDS

- Trong danh sách Roles, chọn Active Directory Domain Services.

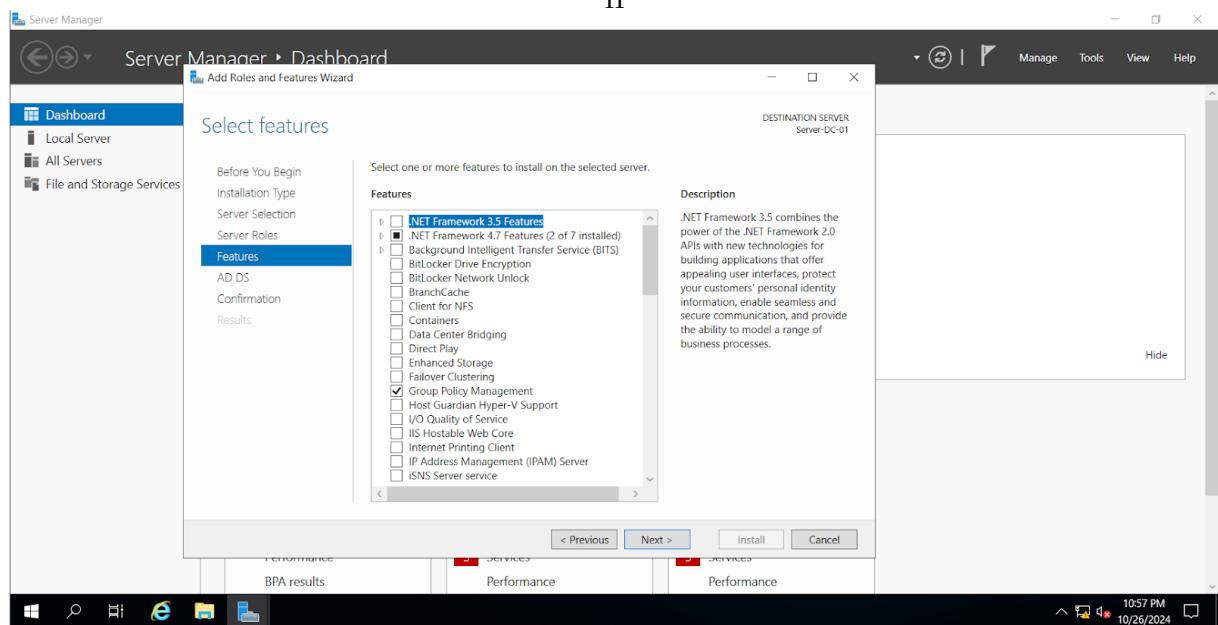


Hình 12: Tải ADDS

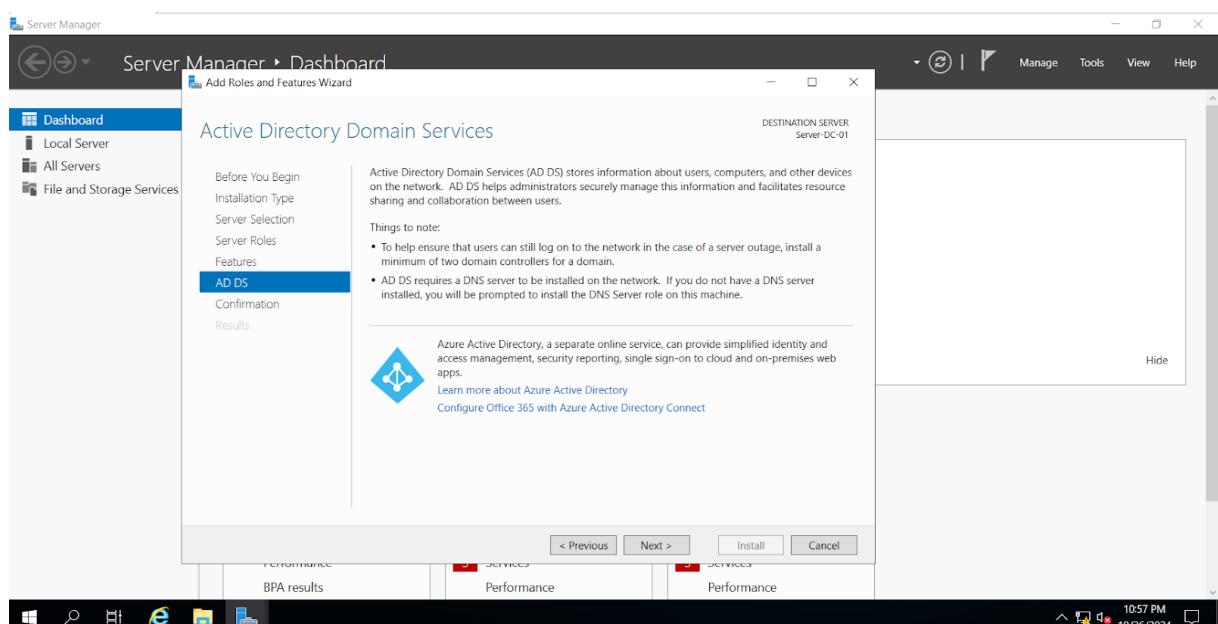


Hình 13: Tải ADDS

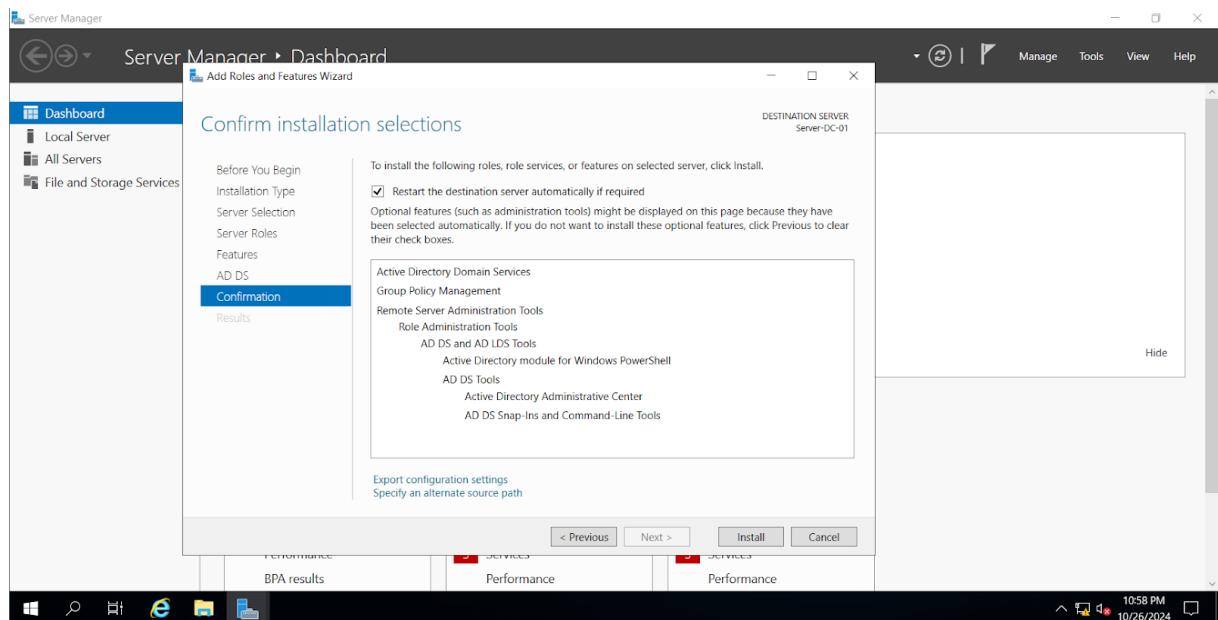
H



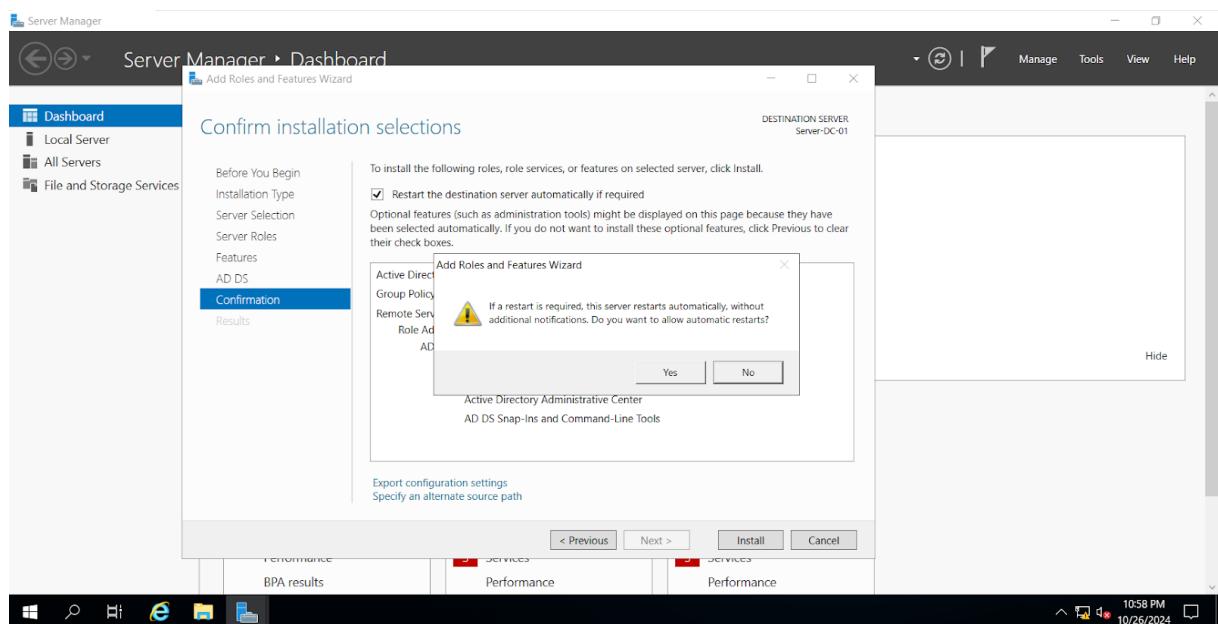
Hình 15: Tải ADDS



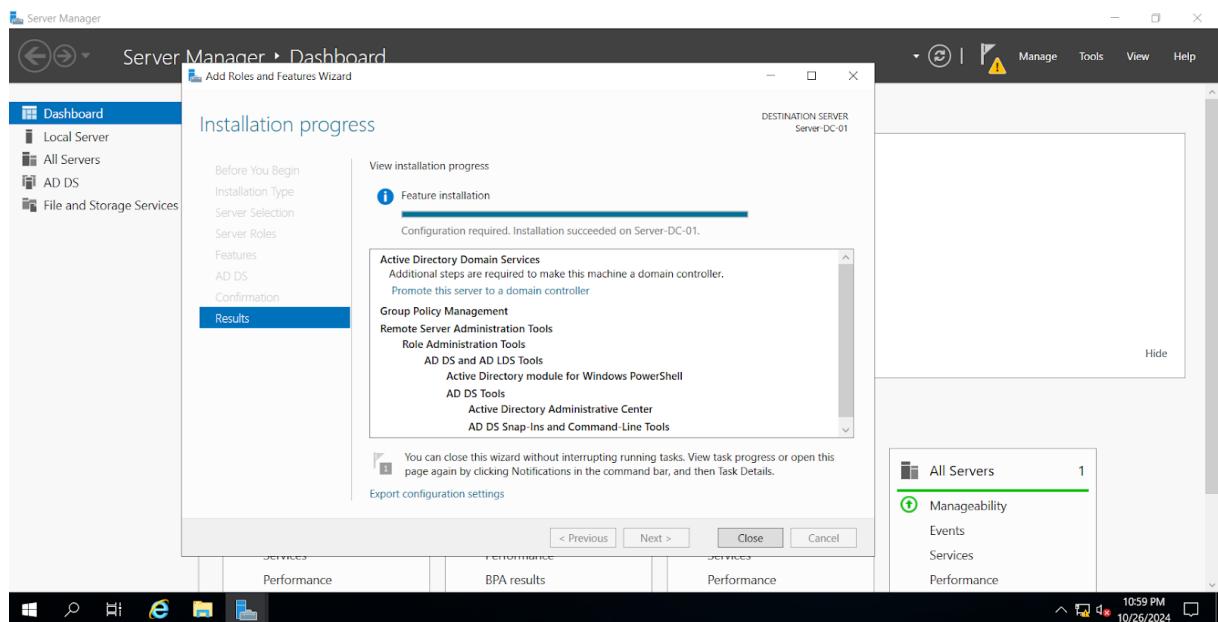
Hình 14: Tải ADDS



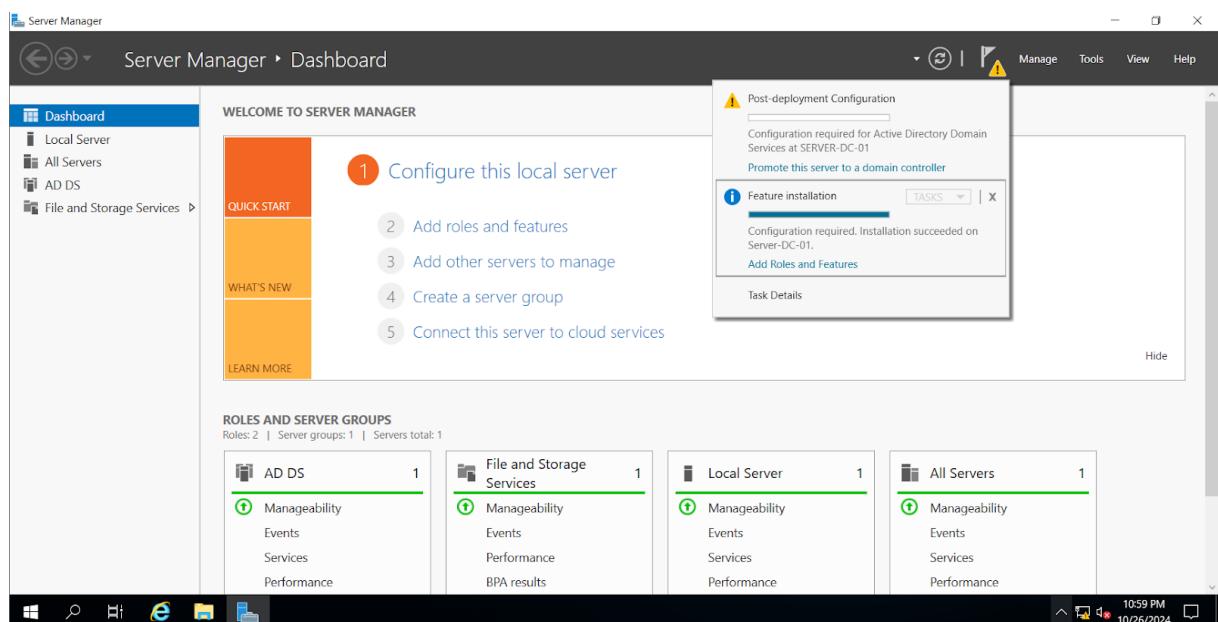
Hình 16: Tải ADDS



Hình 17: Tải ADDS

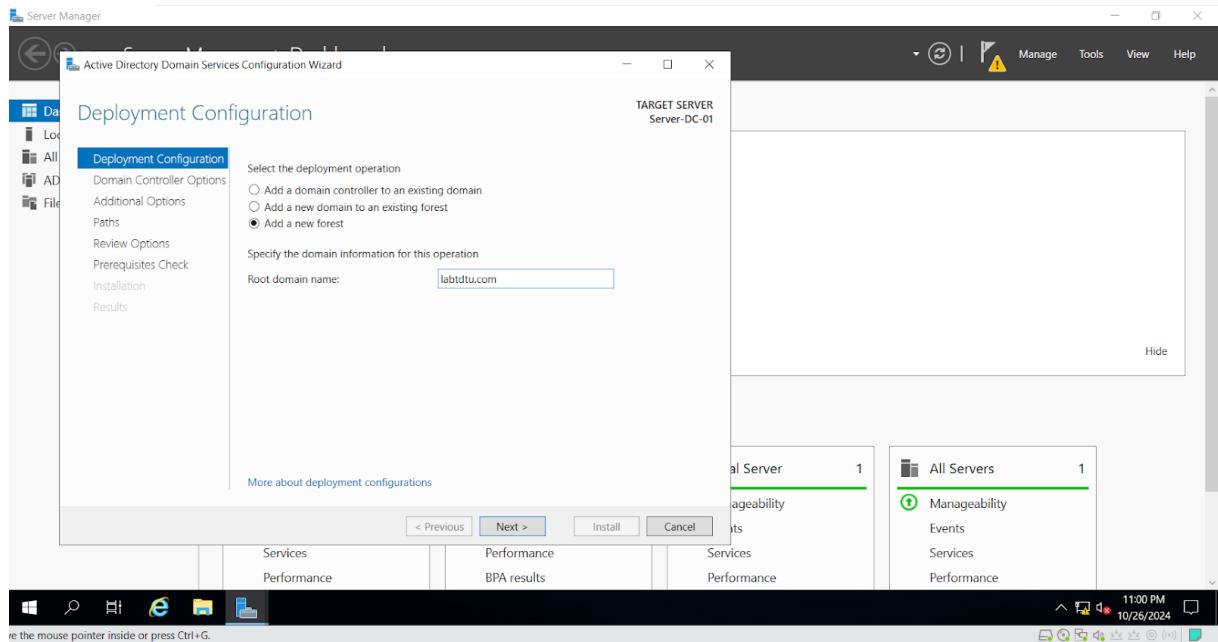


Hình 18: Tải ADDS



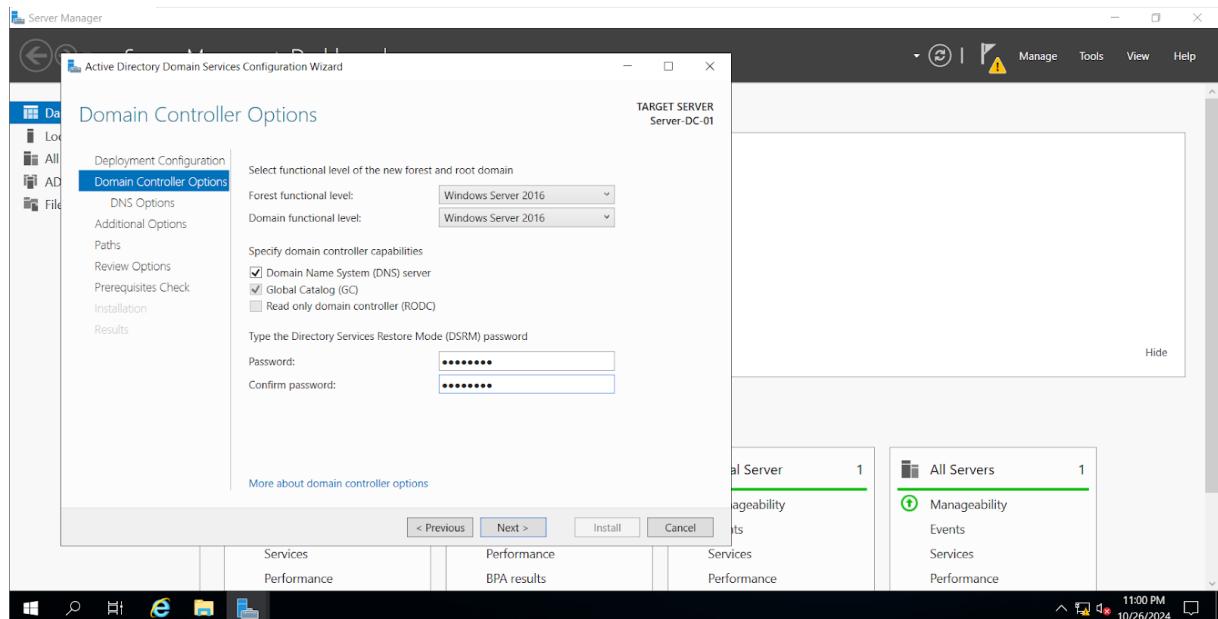
Hình 19: Tạo domain

- Chọn Add a new forest để tạo domain mới

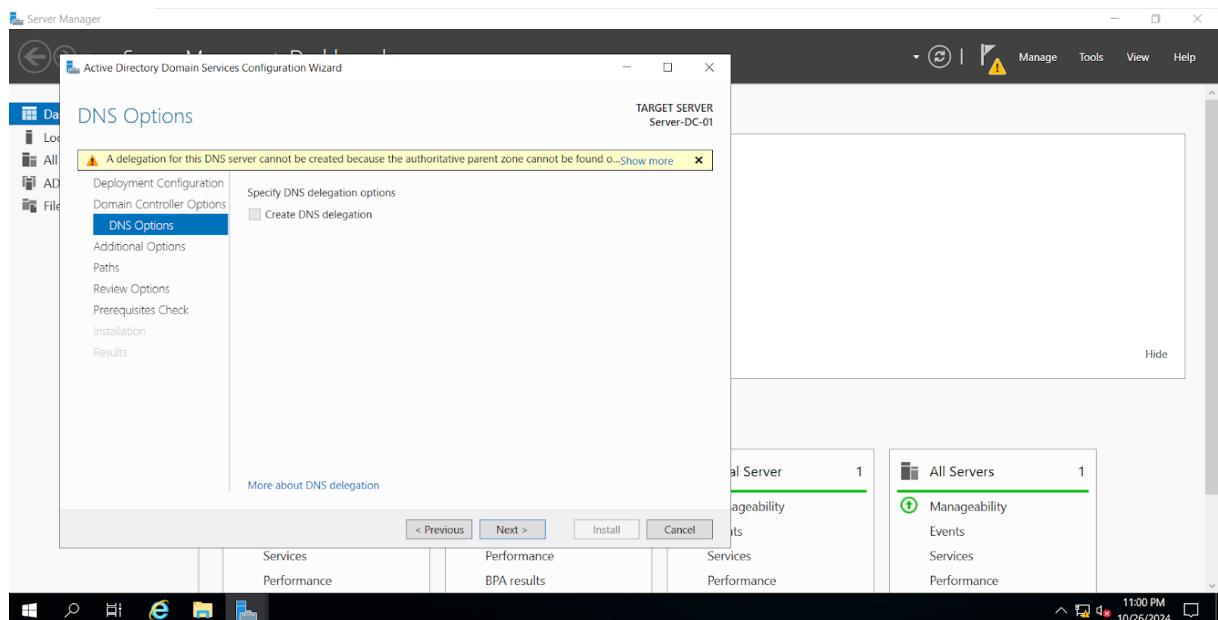


Hình 20: Tạo domain

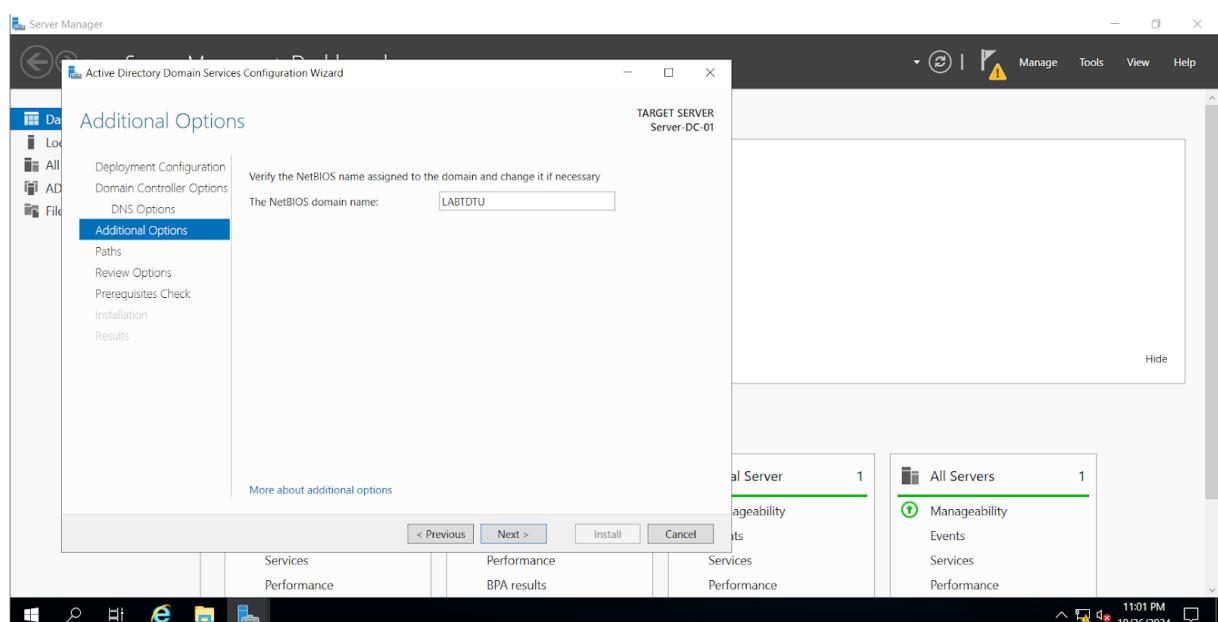
- Điền mật khẩu là P@ssw0rd



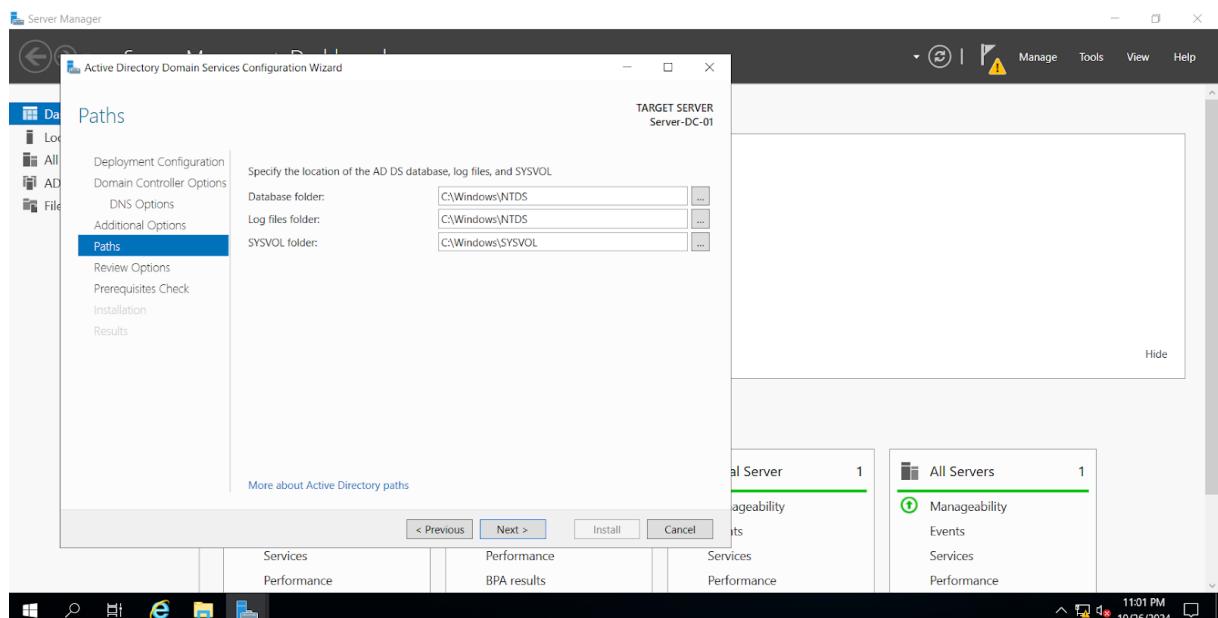
Hình 21: Tạo domain



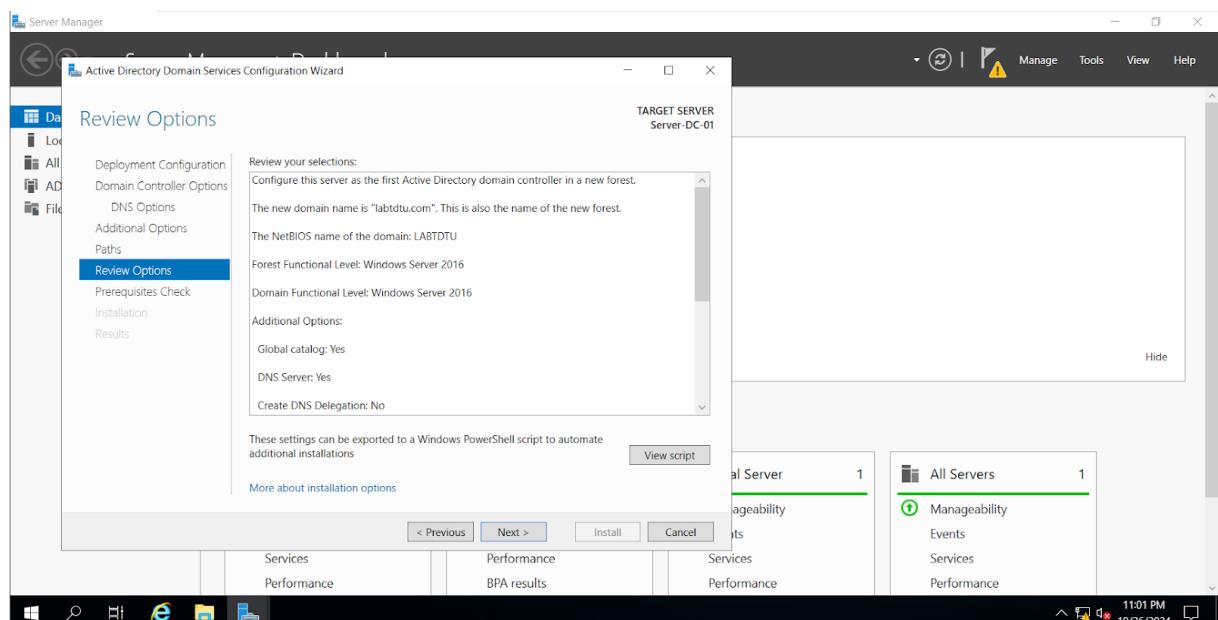
Hình 22: Tạo domain



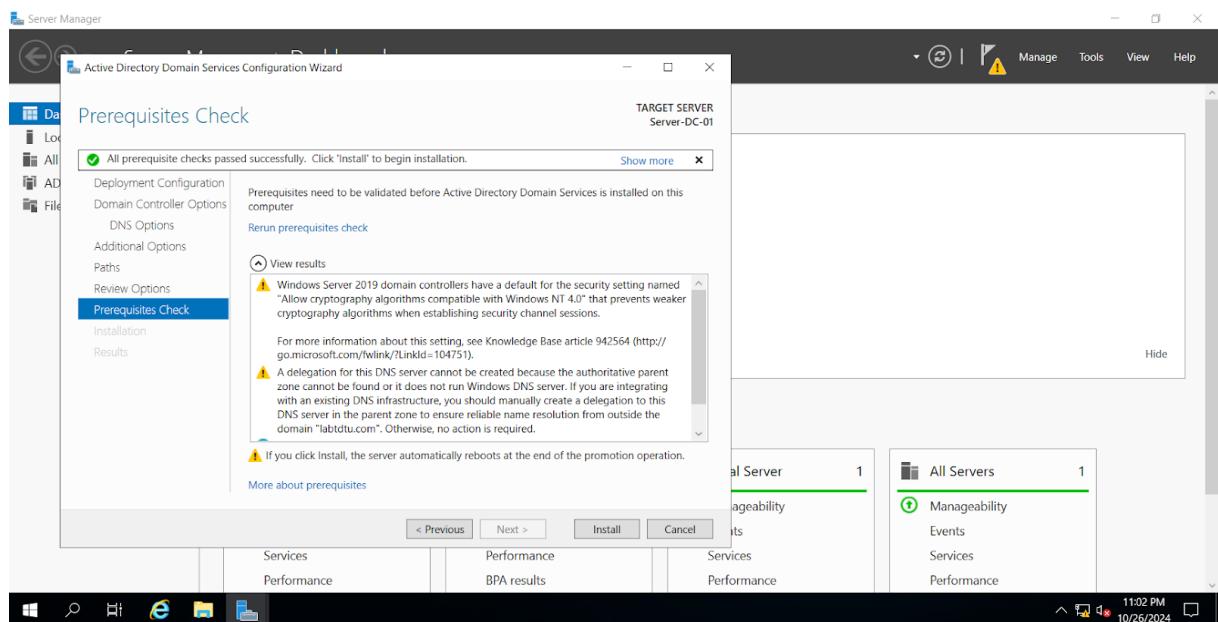
Hình 23: Tạo domain



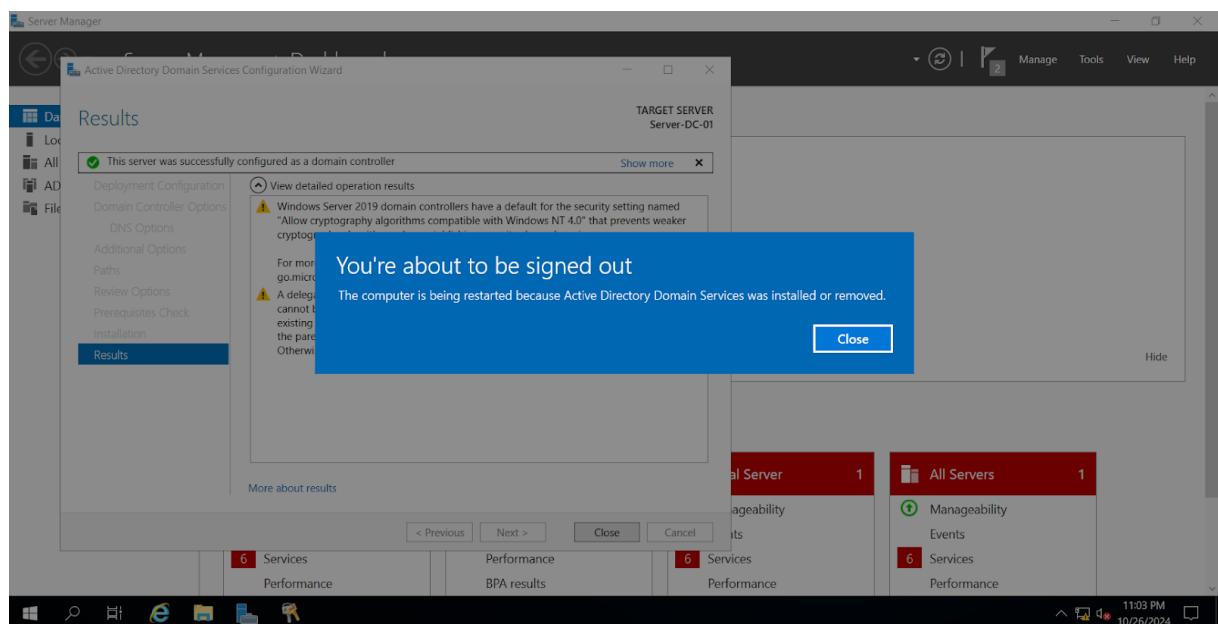
Hình 24: Tạo domain



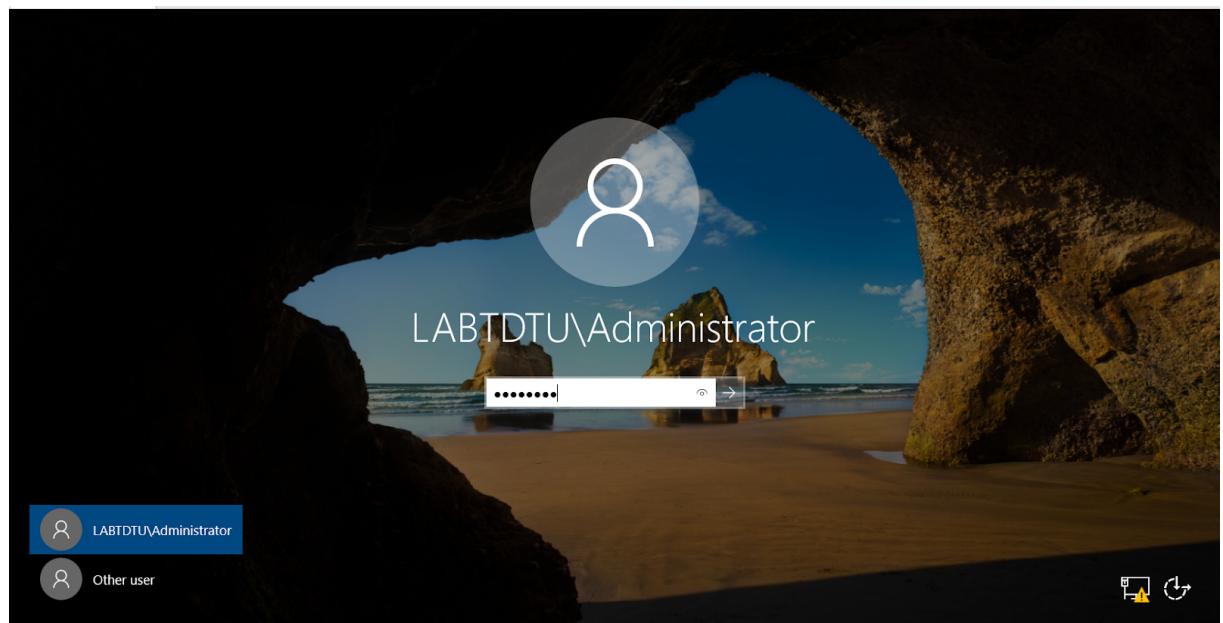
Hình 25: Tạo domain



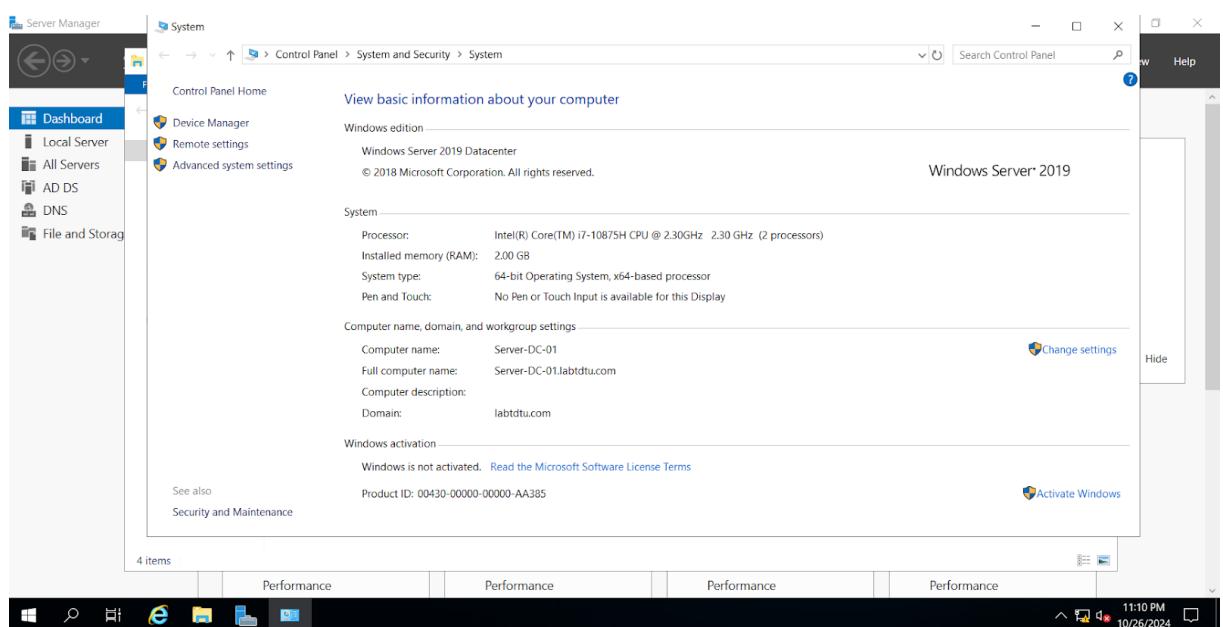
Hình 26: Tạo domain



Hình 27: Restart máy



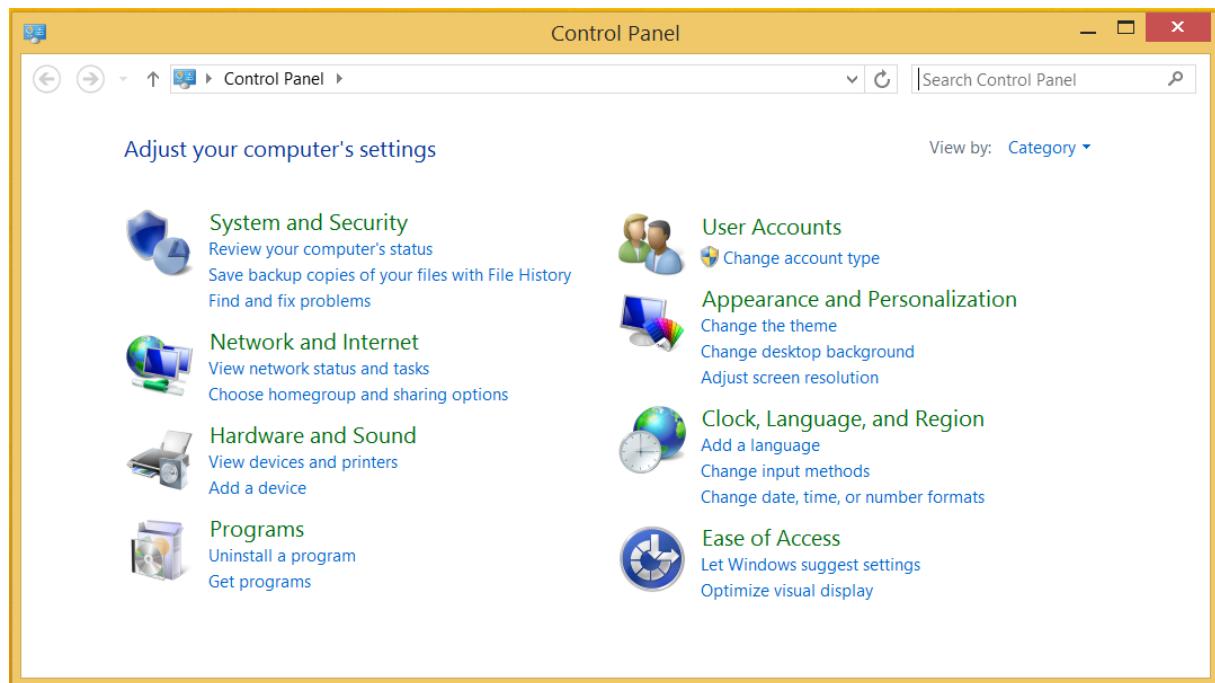
Hình 28: Kiểm tra máy



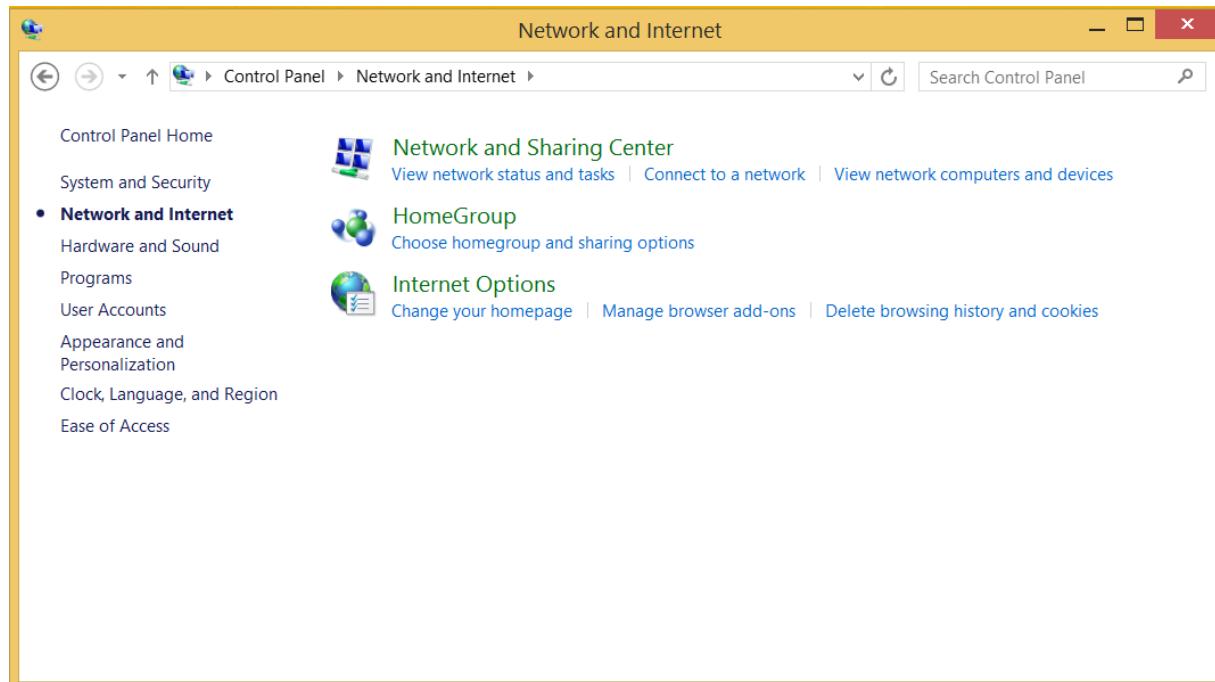
Hình 29: Kiểm tra máy

## 2.2 Máy Client1

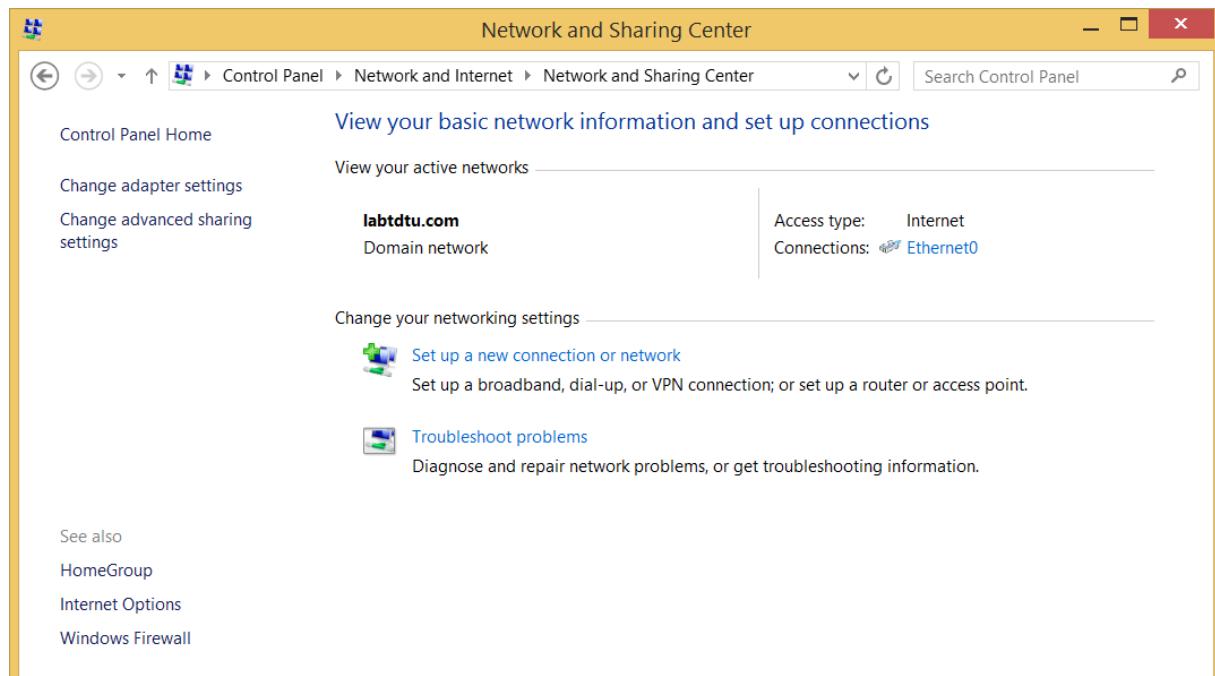
- Thiết lập địa chỉ IP
  - Vào Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings > Ethernet0 > Properties > Internet Protocol Version 4 (TCP/IPv4)



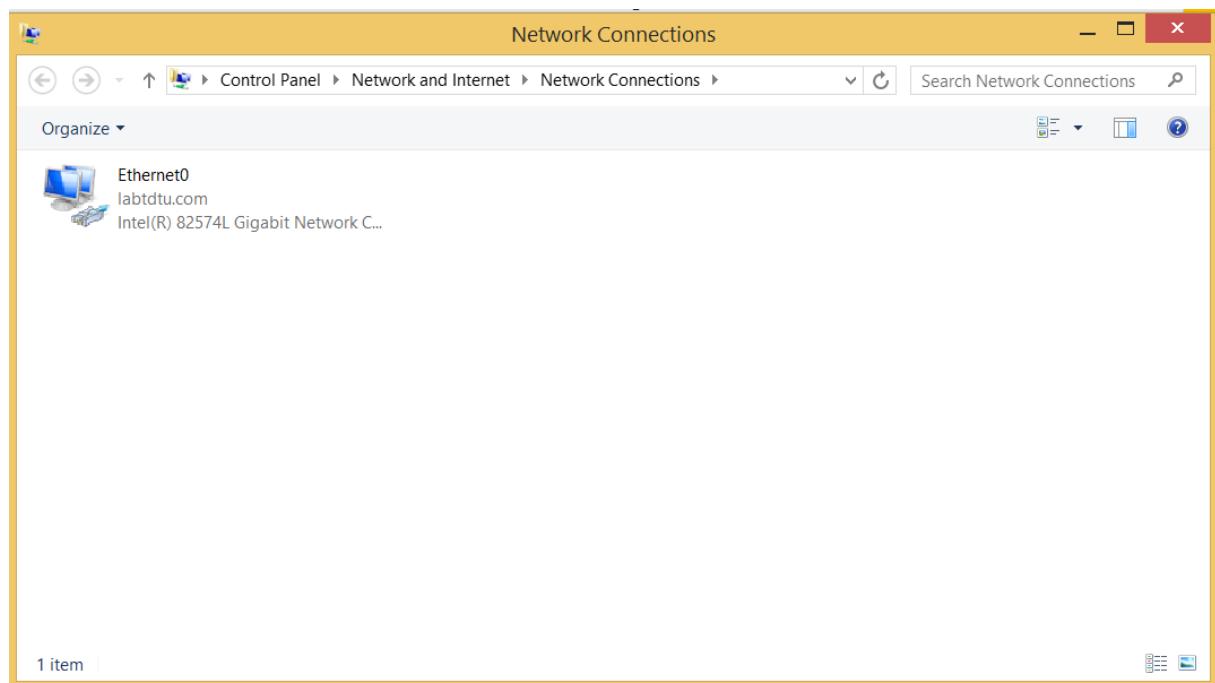
Hình 30: Vào Control Panel



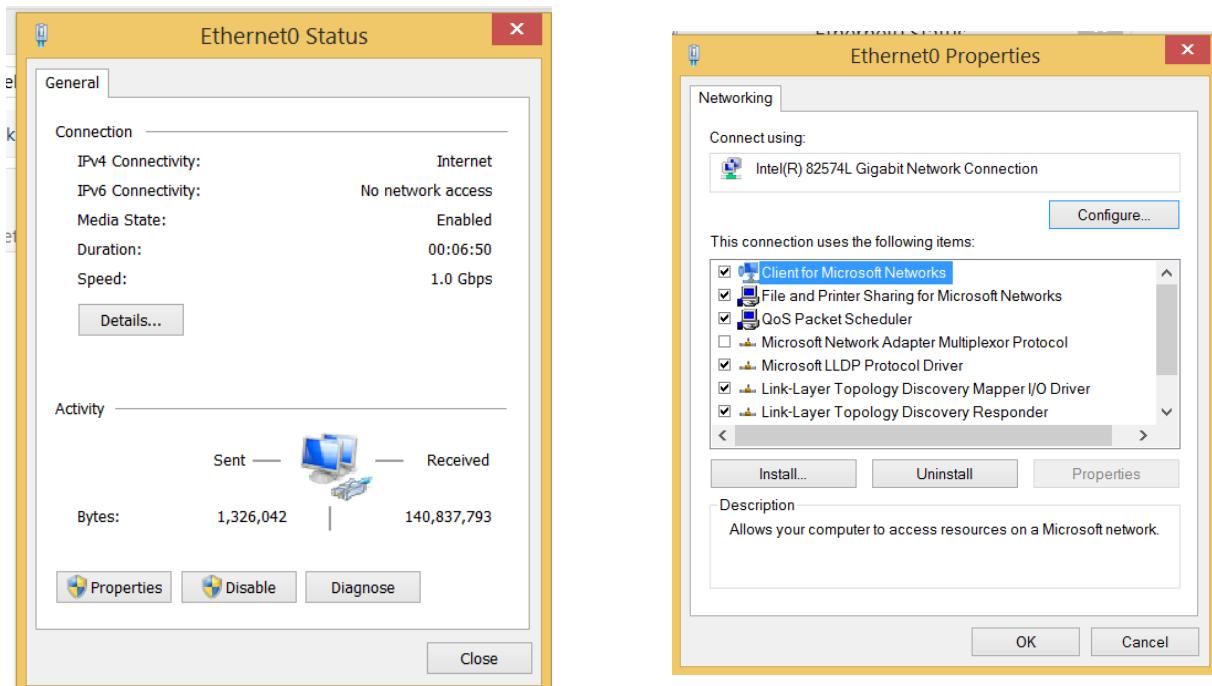
Hình 31: Vào Network và Internet



Hình 32: Vào Network and Sharing Center

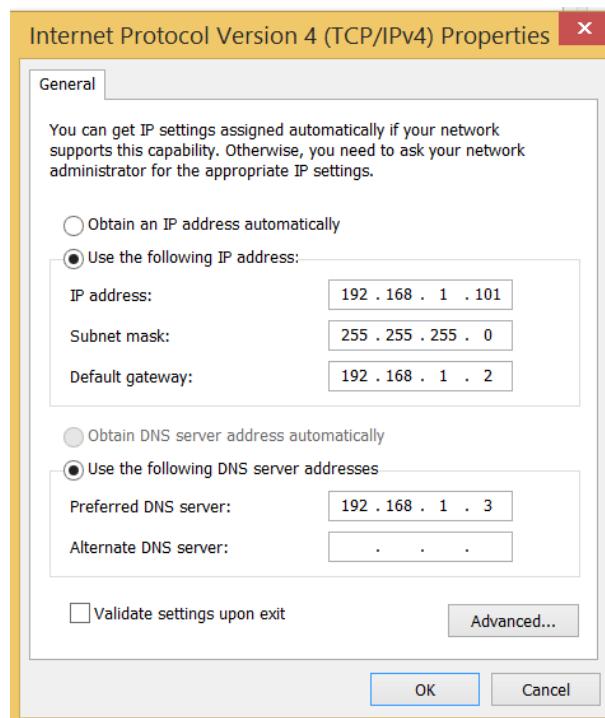


Hình 33: Vào Change adapter settings



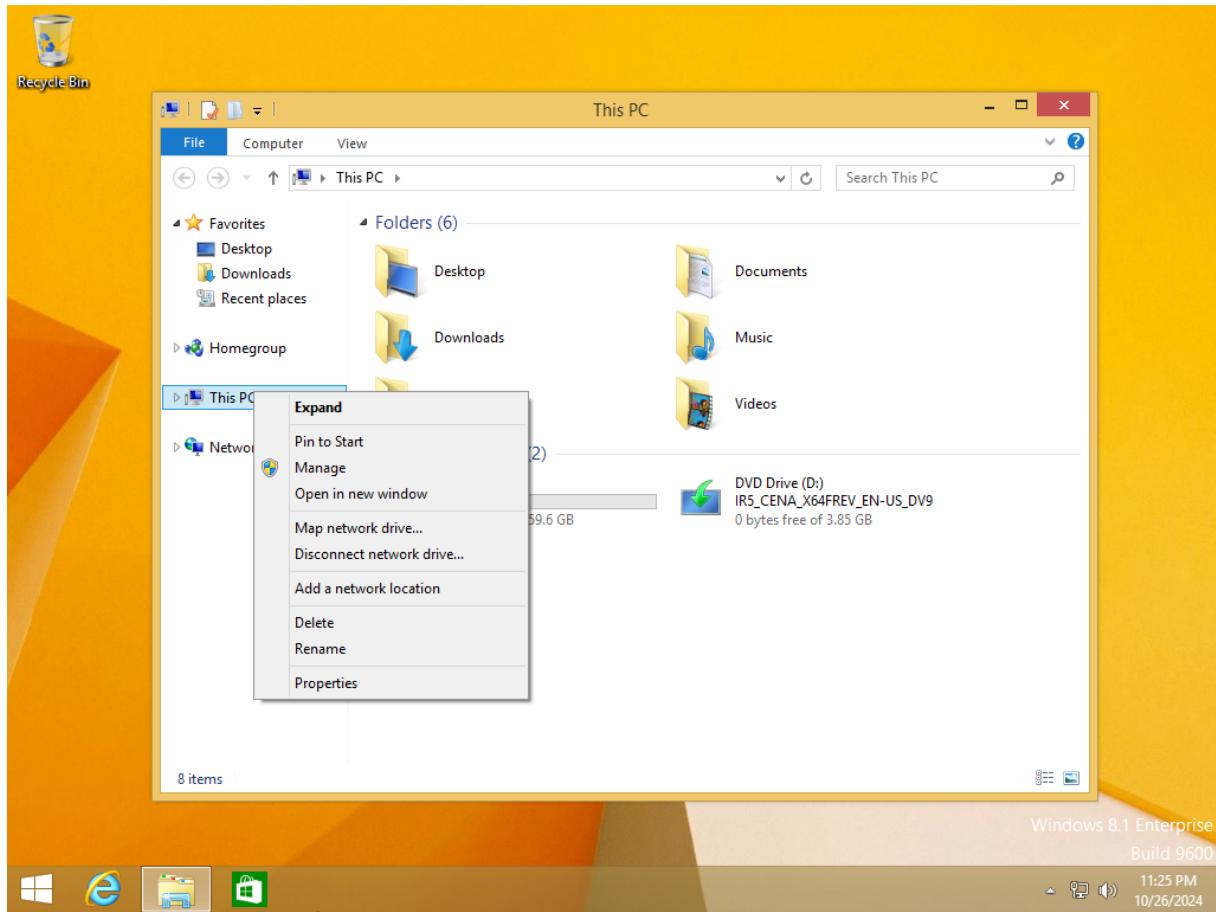
Hình 34: Thiết lập IP

Hình 35: Thiết lập IP



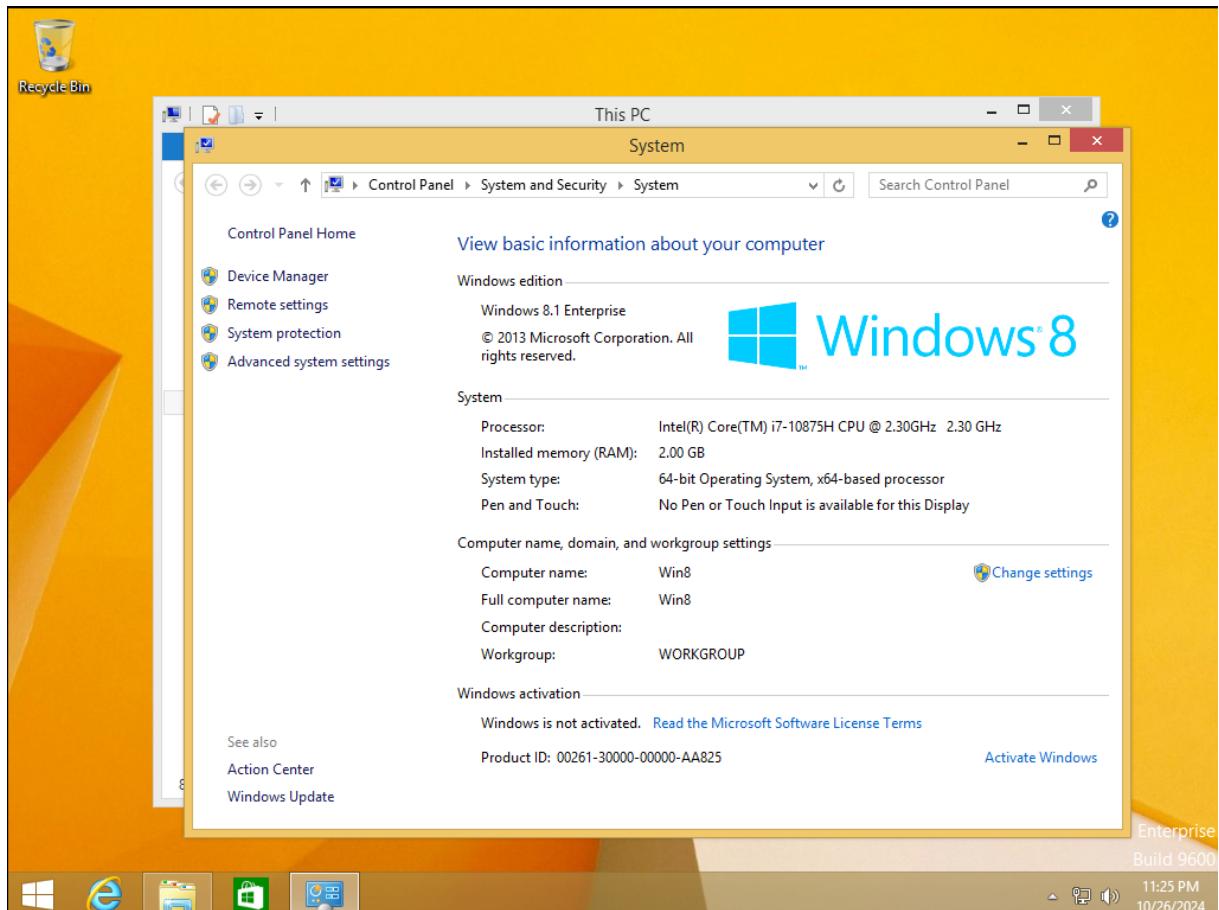
Hình 36: Thiết lập IP

- Thêm máy Client1 vào Domain
  - Vào This PC > Properties



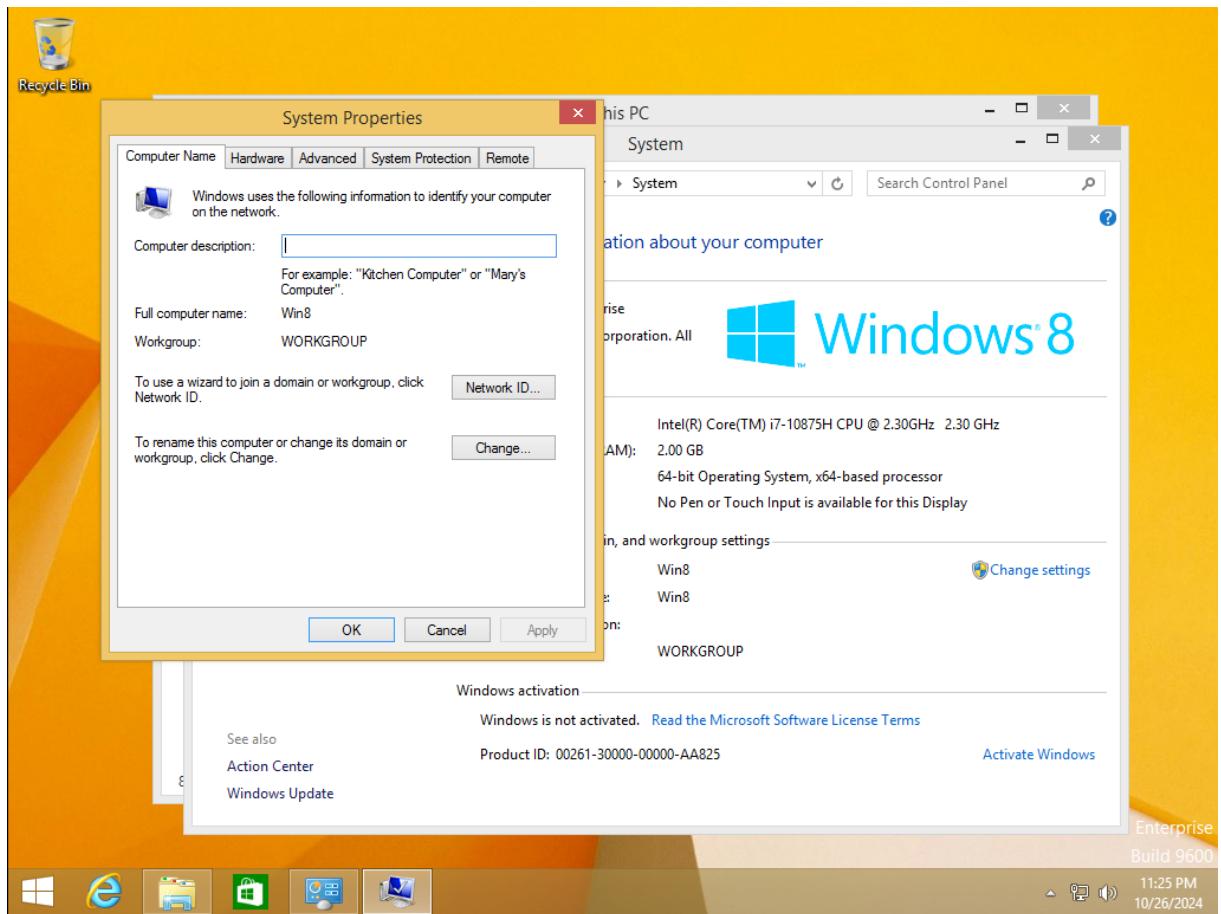
Hình 37: Thêm máy Client1 vào domain

- Chọn Change settings



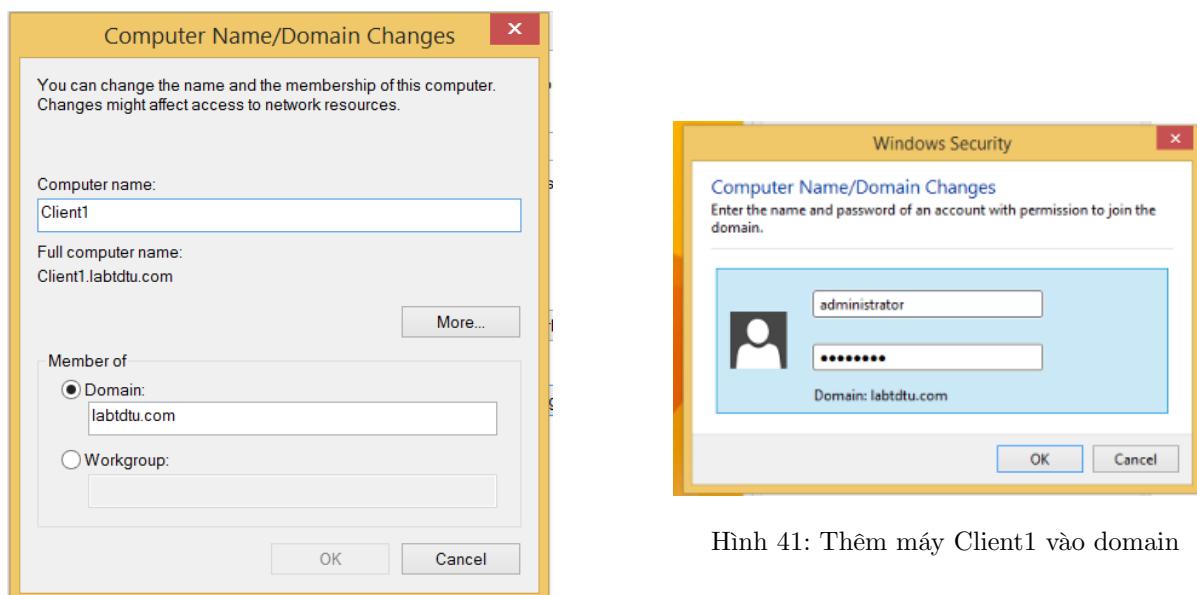
Hình 38: Thêm máy Client1 vào domain

- Chọn Change



Hình 39: Thêm máy Client1 vào domain

- Điền Computer name là Client1 và Domain là labtdtu.com sau đó nhập tài khoản admin vào.



Hình 41: Thêm máy Client1 vào domain

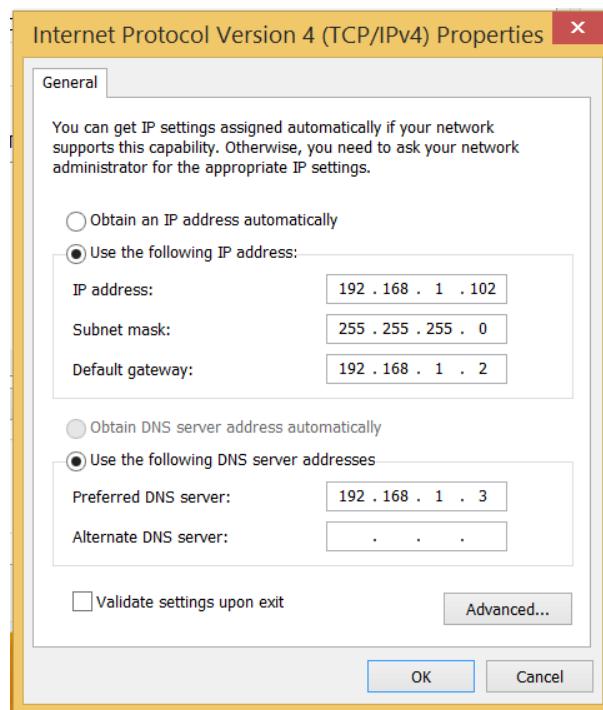
Hình 40: Thêm máy Client1 vào domain



Hình 42: Thêm máy Client1 vào domain

### 2.3 Máy Client2

- Thiết lập địa chỉ IP
  - Làm tương tự như máy Client1



Hình 43: Máy Client2

- Thêm máy Client2 vào Domain
  - Làm tương tự như máy Client1



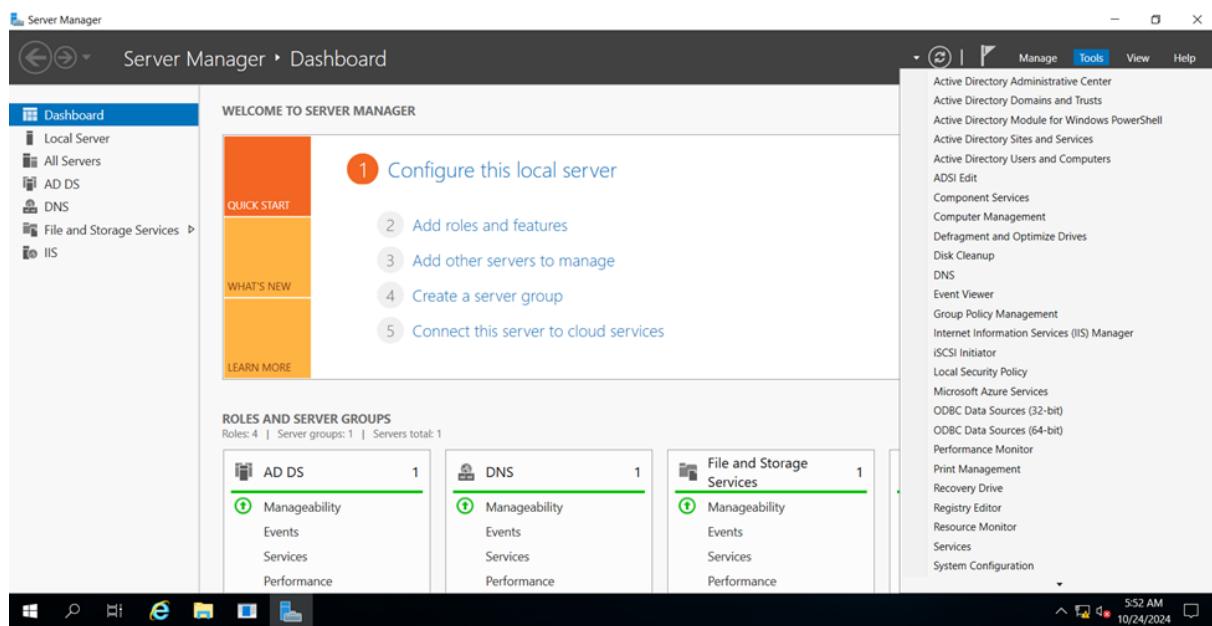
Hình 44: Máy Client2

### 3 CHƯƠNG 3: CẤU HÌNH VỚI KỊCH BẢN

#### 3.1 Kịch bản 1: Cấu hình quy tắc đặt mật khẩu và giám sát đăng nhập

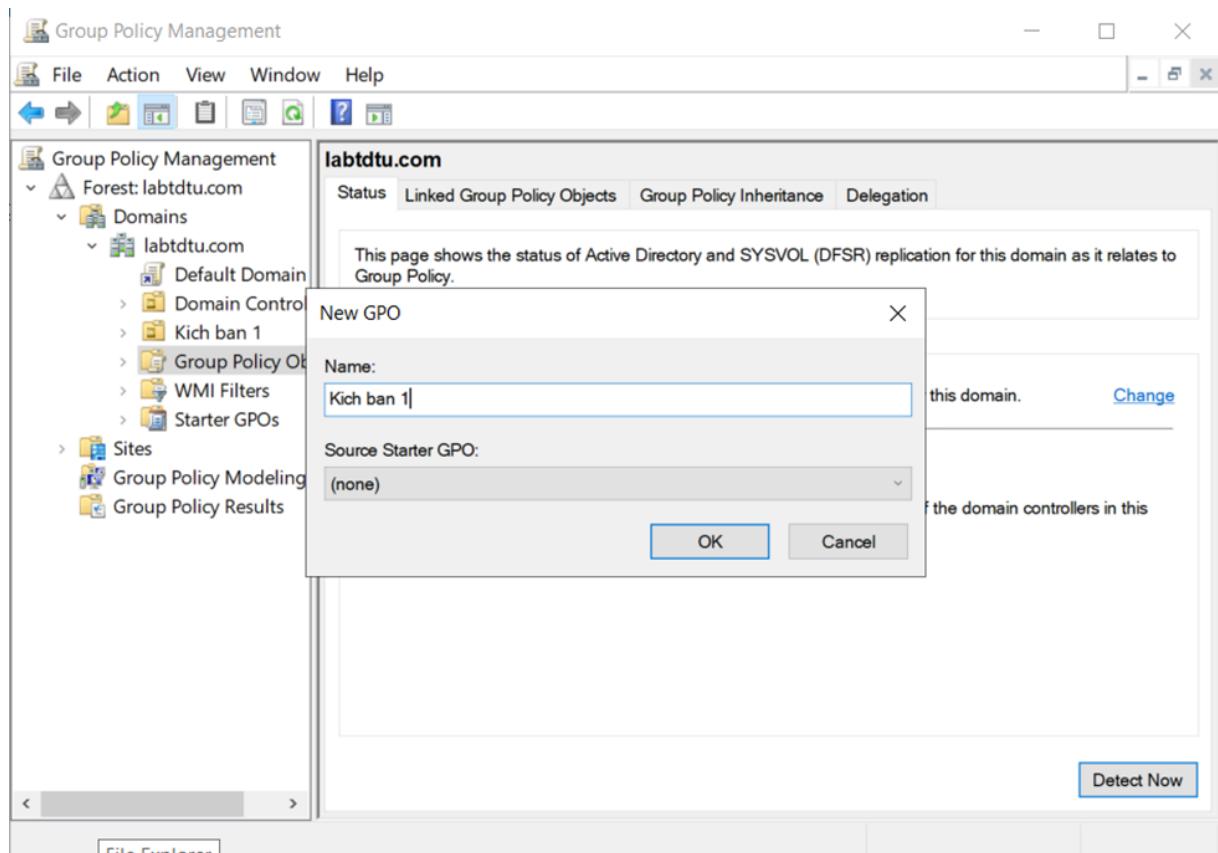
##### 1. Máy SERVER-DC-01

- Cấu hình Account Policies:
  - Mật khẩu ít nhất 8 ký tự, có số, ký tự đặc biệt, chữ hoa.
  - Thời gian khóa tài khoản sau khi nhập sai 3 lần.
  - Thời gian đổi mật khẩu định kỳ 1 tháng/lần.
  - Nhập sai mật khẩu 3 lần thì bị khóa tài khoản.
  - Mở Server Manager > Dashboard và chọn Tools > Group Policy Management .



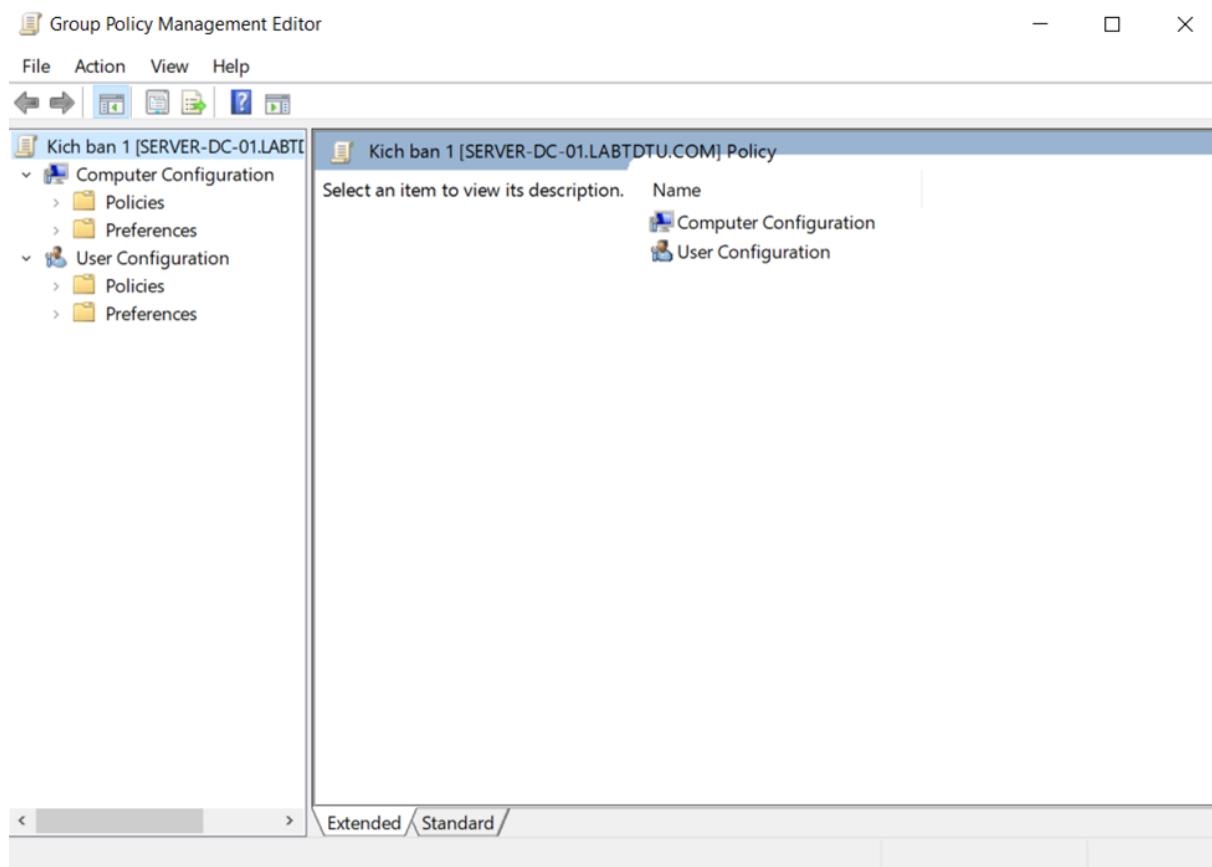
Hình 45: Server Manager > Dashboard và chọn Tools > Group Policy Management

- Trong Group Policy Management , mở rộng Forest > Domains. Nhấn chuột phải vào Group Policy Objects rồi chọn New
- Điền tên cho GPO mới tạo là “Kích ban 1” và nhấn OK



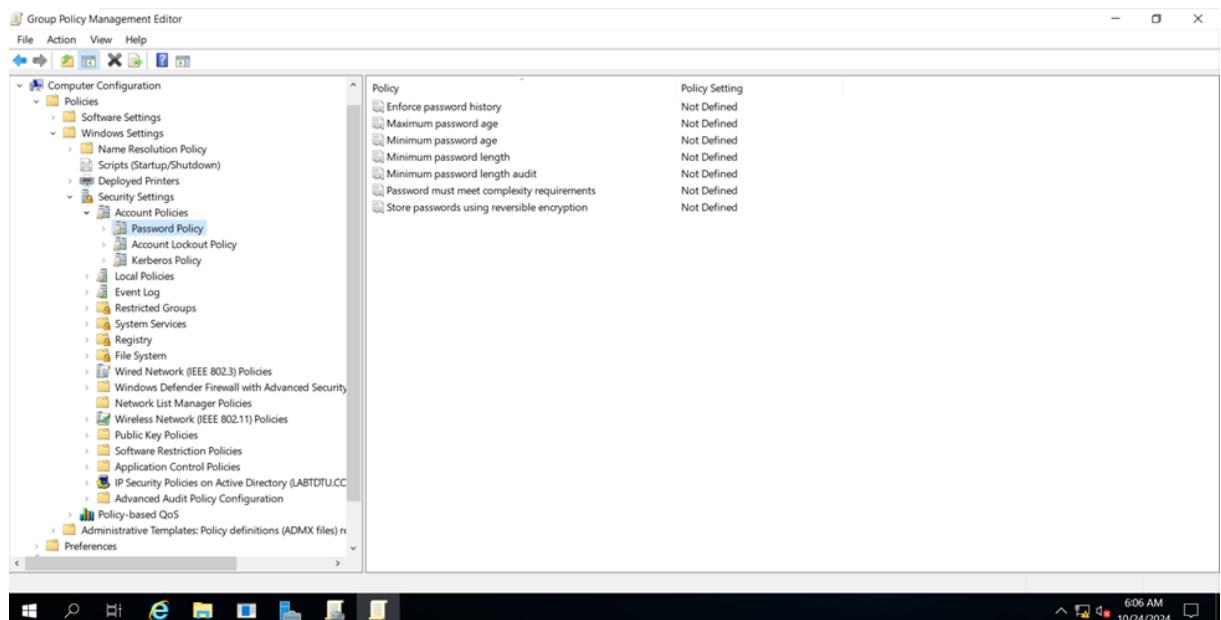
Hình 46: Tạo kịch bản 1

- Mở **Group Policy Objects** ta thấy các GPO được tạo
- Để tùy chỉnh GPO đã tạo ta nhấn chuột phải vào GPO “Kích ban 1” rồi chọn **Edit...** để mở **Group Policy Management**



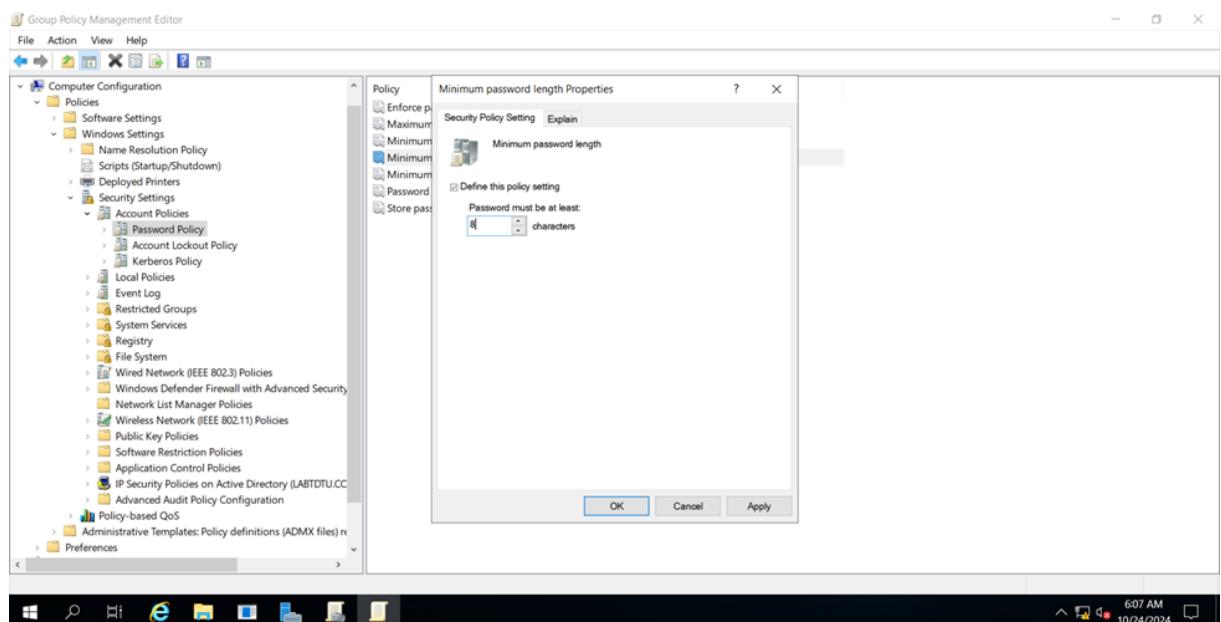
Hình 47: Tùy chỉnh GPO kịch bản 1

- Trong cửa sổ **Group Policy Management Editor**, điều hướng đến:
- Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy.



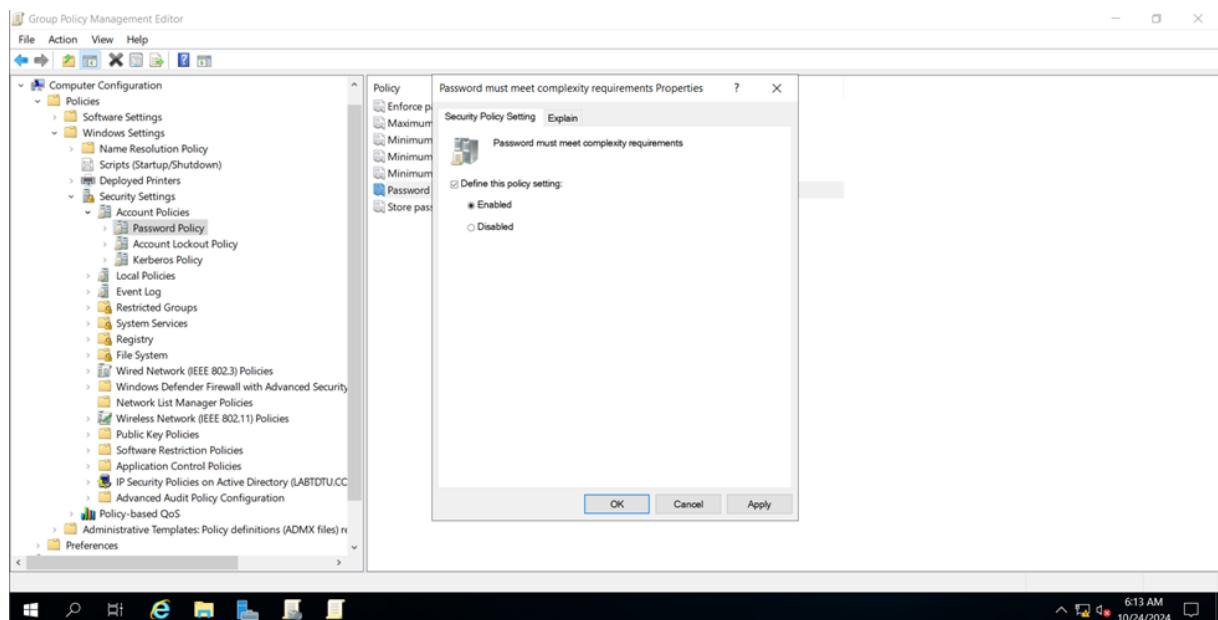
Hình 48: Password Policy

- Chọn Minimum password length rồi tích chọn Define this policy setting. Tại ô characters điền số 8 > Nhấn OK.



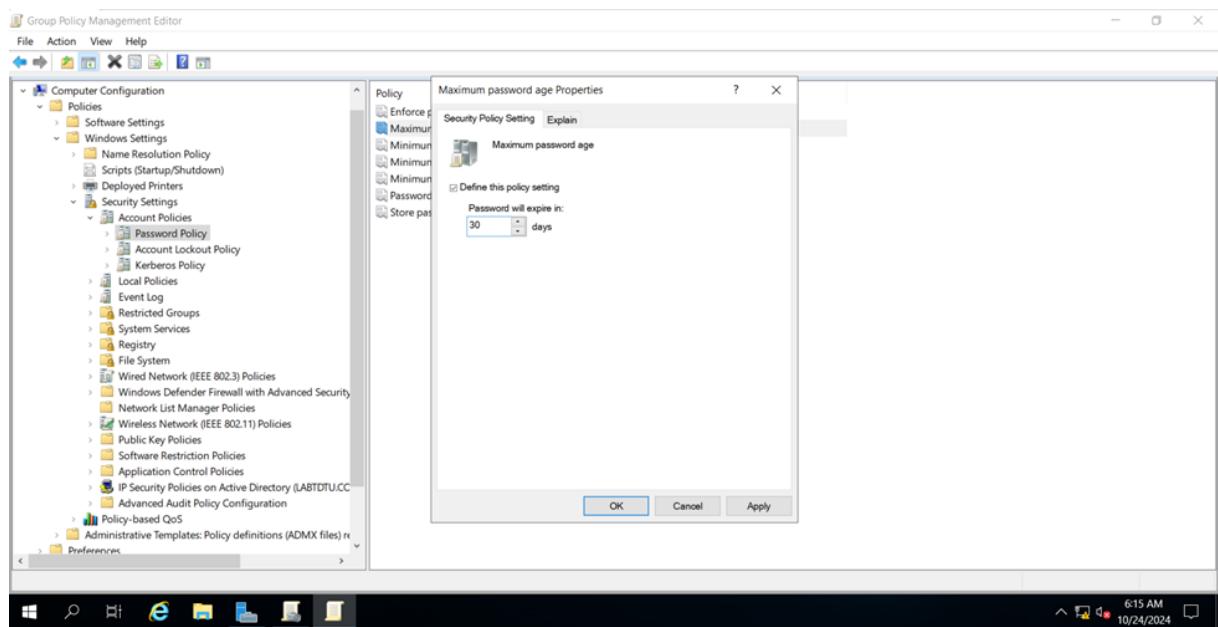
Hình 49: Minimum password length

- Để kích hoạt quy tắc cho mật khẩu chọn Password must meet complexity requirements rồi tích chọn Define this policy setting > Enabled



Hình 50: Password complexity requirements

- Để đặt thời gian đổi mật khẩu định kỳ hàng tháng thì chọn **Maximum password age** rồi tích chọn **Define this policy setting** rồi điền vào ô days là 30.

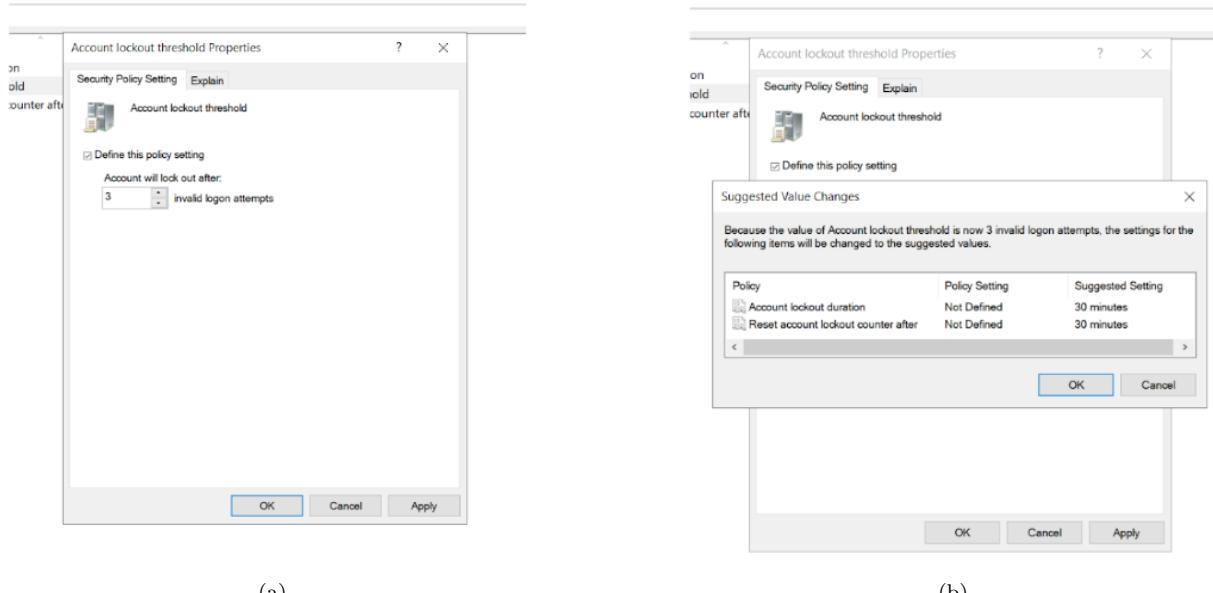


Hình 51: Maximum password age

- Trong cửa sổ Group Policy Management Editor, điều hướng đến: Computer Configuration >

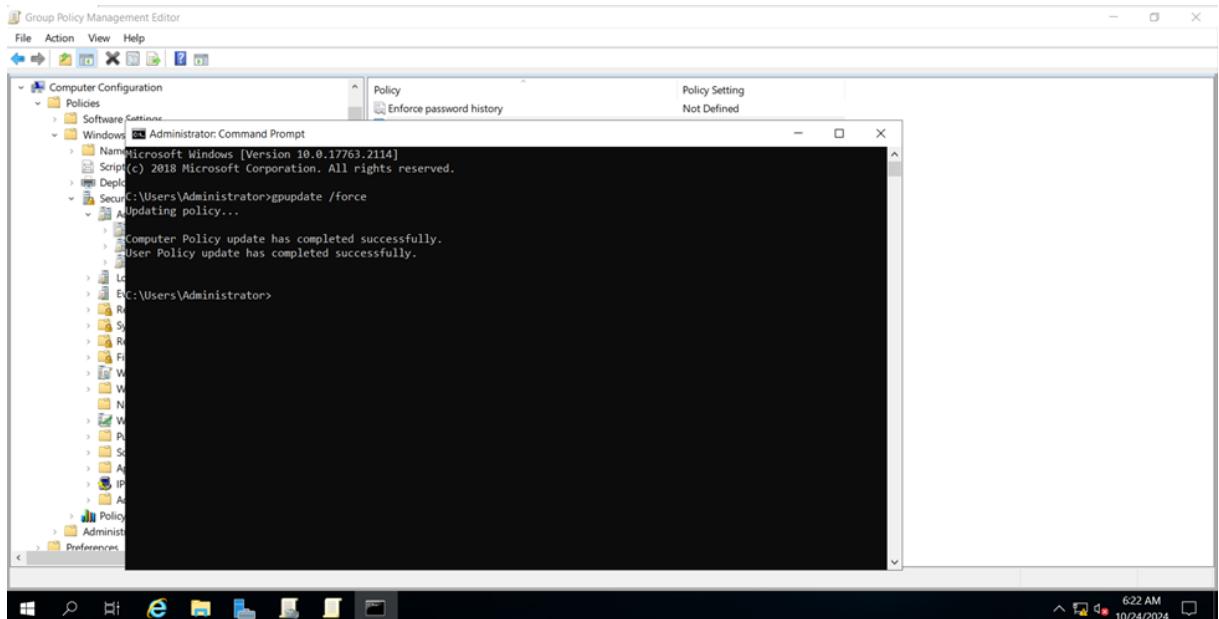
Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy.

- **Account lockout threshold:** Nhập đúp vào và đặt thành 3 (đây là số lần nhập sai mật khẩu tối đa trước khi tài khoản bị khóa).
- **Account lockout duration:** Đặt thời gian tài khoản bị khóa (ví dụ: 30 phút). Sau khoảng thời gian này, tài khoản sẽ tự động được mở khóa.
- **Reset account lockout counter after:** Đặt thời gian để bộ đếm số lần nhập sai sẽ được đặt lại (nên đặt tương tự với Account lockout duration, ví dụ: 30 phút).
- chọn **Account lockout threshold** rồi tích chọn **Define this policy setting** rồi điền vào ô invalid logon attempts là 30.



Hình 52: Switching ip address

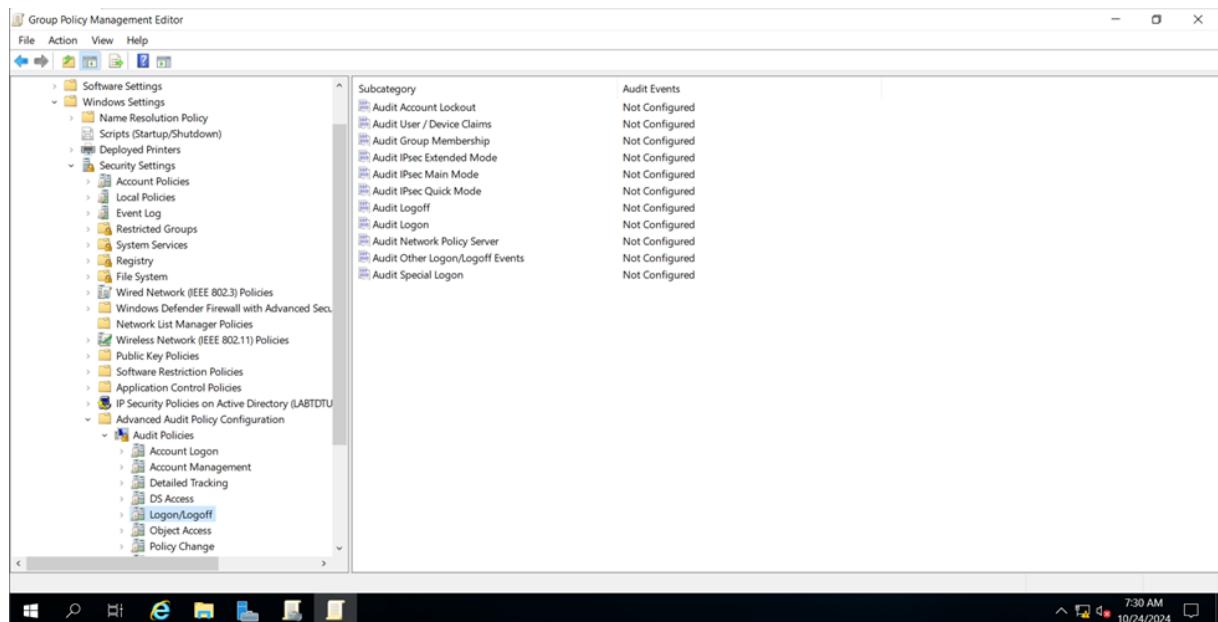
- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh `gpupdate /force` trong Command Prompt (với quyền Admin):



Hình 53: `gpupdate /force`

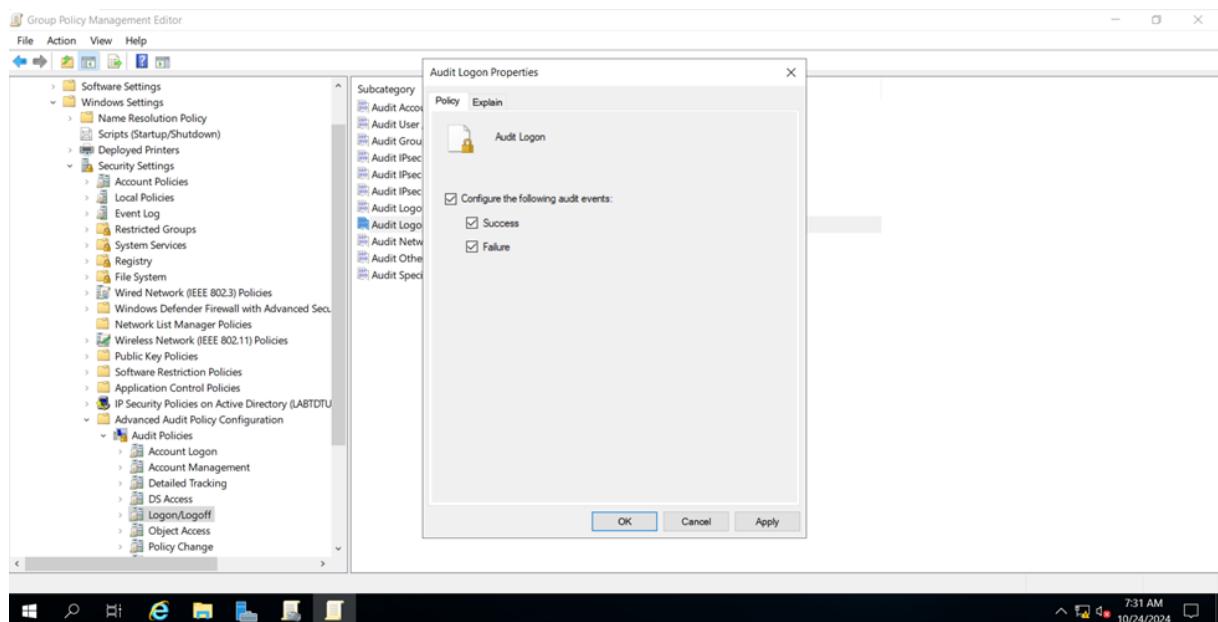
- Cấu hình giám sát:

- Bật tính năng Audit để theo dõi số lần nhập sai mật khẩu: Trong cửa sổ Group Policy Management Editor, điều hướng đến: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Logon/Logoff.



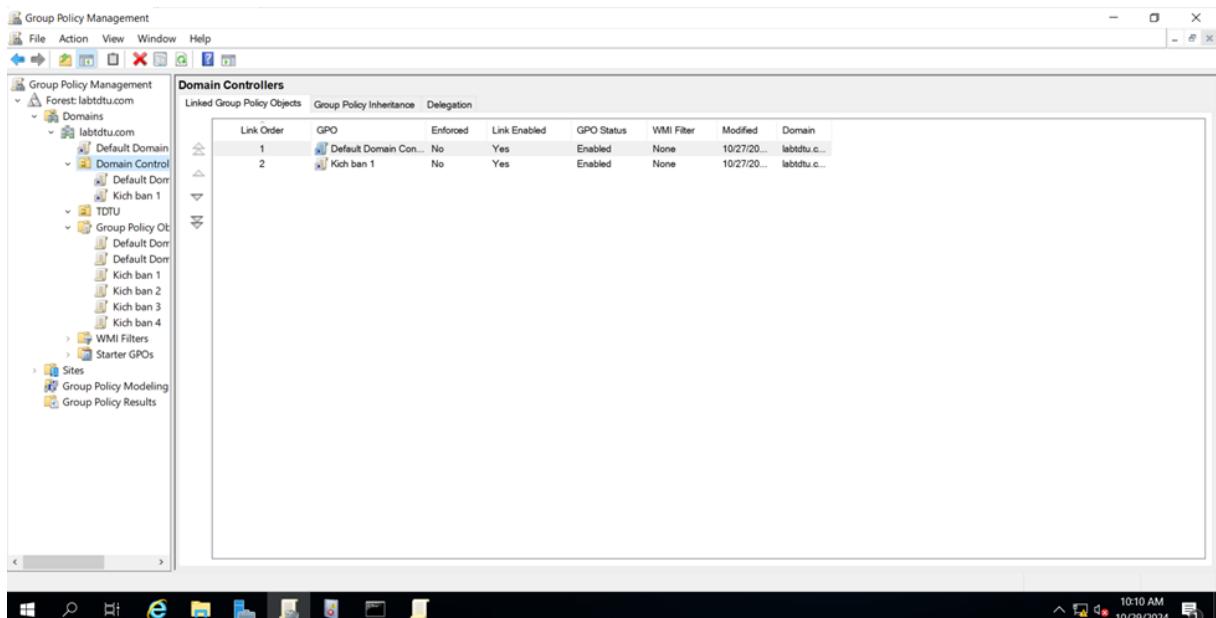
Hình 54: Audit Policies &gt; Logon/Logoff

- Nhập đúp vào Audit Logon và Audit Account Logon để bật.
- **Audit Logon:** Bật tính năng audit cho cả đăng nhập thành công và thất bại.
- **Audit Account Logon:** Bật tính năng audit cho sự kiện xác thực thông qua tài khoản domain.



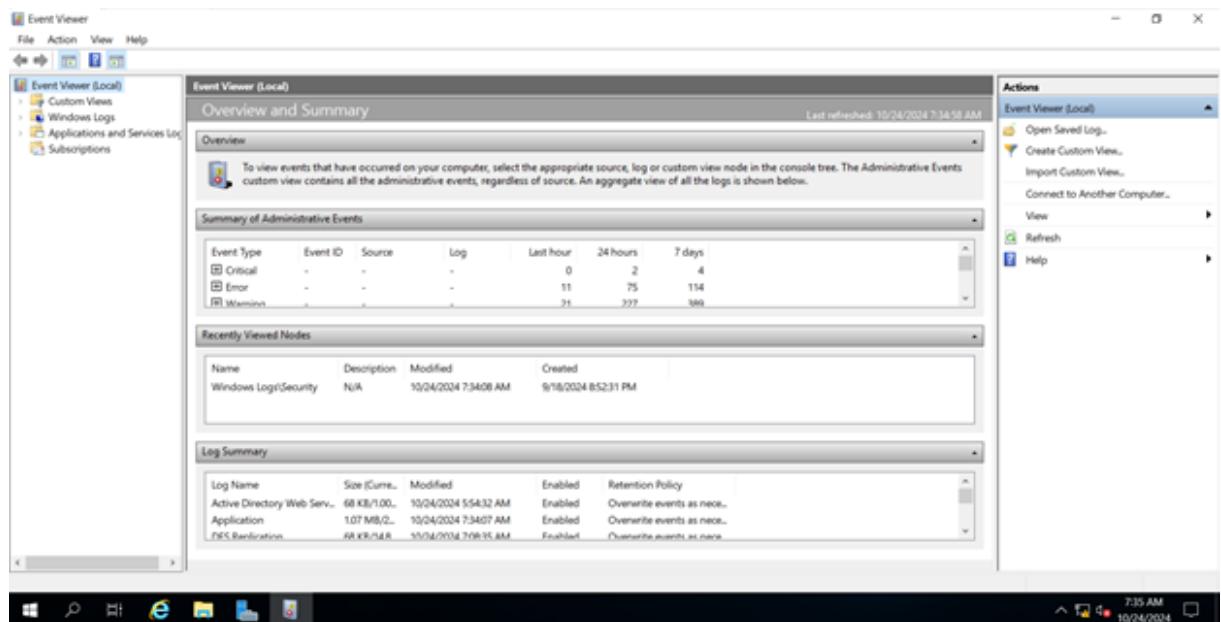
Hình 55: Bật tính năng audit

- Ra Group Policy Manager và kéo GPO kich ban 1 vào Domain Control



Hình 56: Liên kết GPO kich ban 1 vào Domain Control

- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh `gpupdate /force` trong Command Prompt (với quyền Admin):
- Xem sự kiện đăng nhập thất bại:
- Mở Server Manager > Tools > Event Viewer.



Hình 57: Event Viewer

## 2. Demo

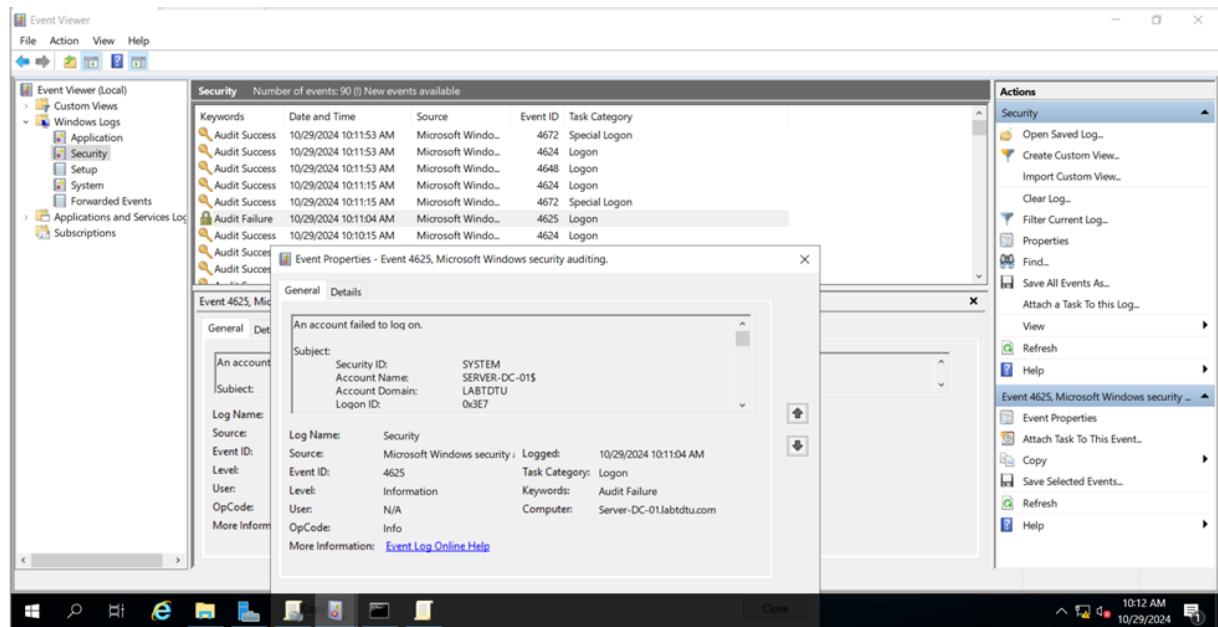
- Thủ đăng nhập với máy Server bằng mật khẩu không đúng



Hình 58: Đăng nhập thất bại

- Mở Server Manager > Tools > Event Viewer.
- Trong Event Viewer, điều hướng đến: Windows Logs > Security.

- Tìm các sự kiện có ID 4625: Sự kiện này ghi lại mỗi lần đăng nhập thất bại (bao gồm cả nhập sai mật khẩu).
- Bạn có thể xem thông tin chi tiết của sự kiện, bao gồm tài khoản người dùng nào đã nhập sai mật khẩu và thời gian cụ thể.

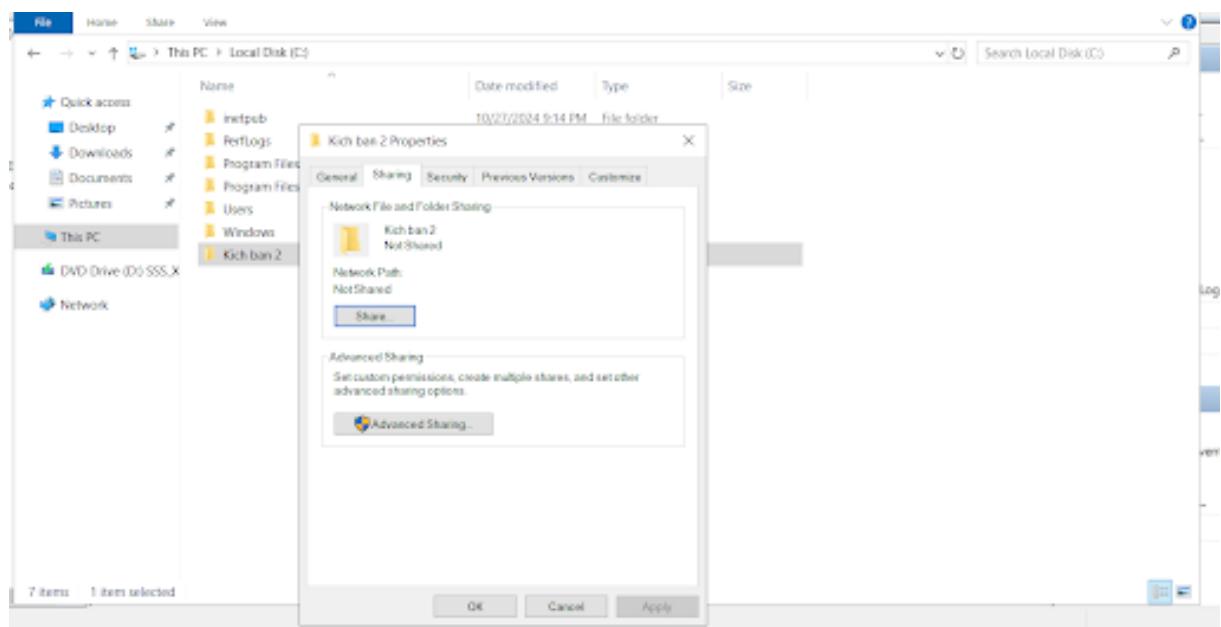


Hình 59: Kiểm tra log

### 3.2 Kịch bản 2: Giám sát truy cập các thư mục và tệp quan trọng

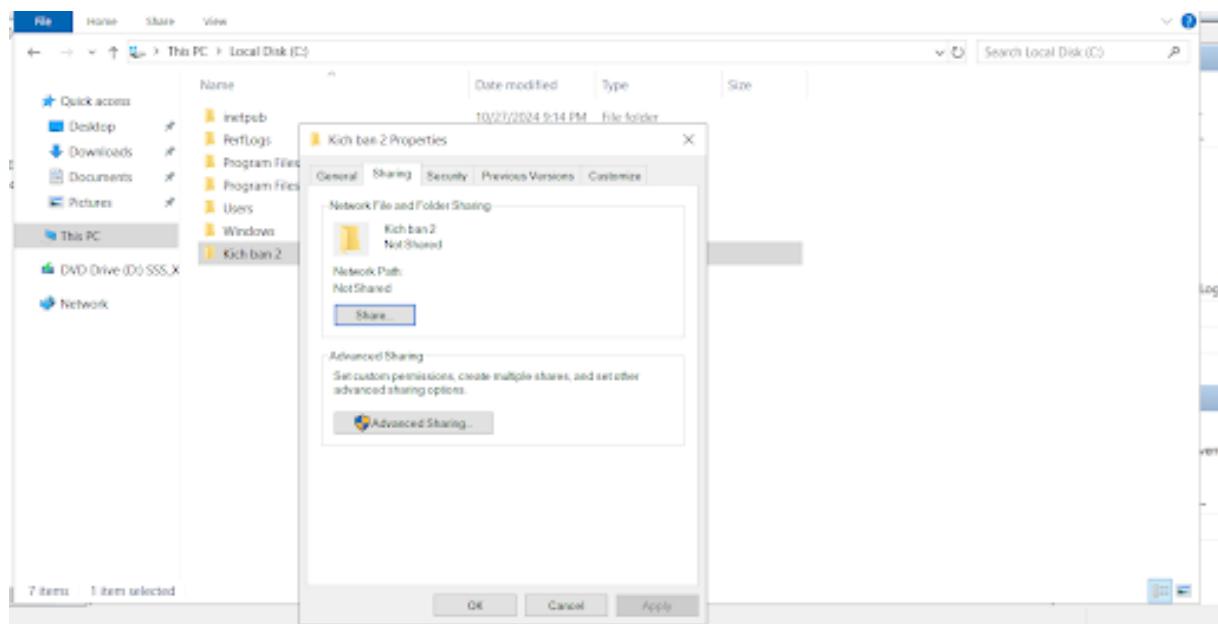
#### 1. Thiết lập Audit Policy

- Bật Audit Object Access trong Local Security Policy hoặc Group Policy.
  - Tạo Folder ‘‘Kích ban 2’’ sau nhấn chuột phải vào Folder mới tạo chọn Properties và chọn Sharing



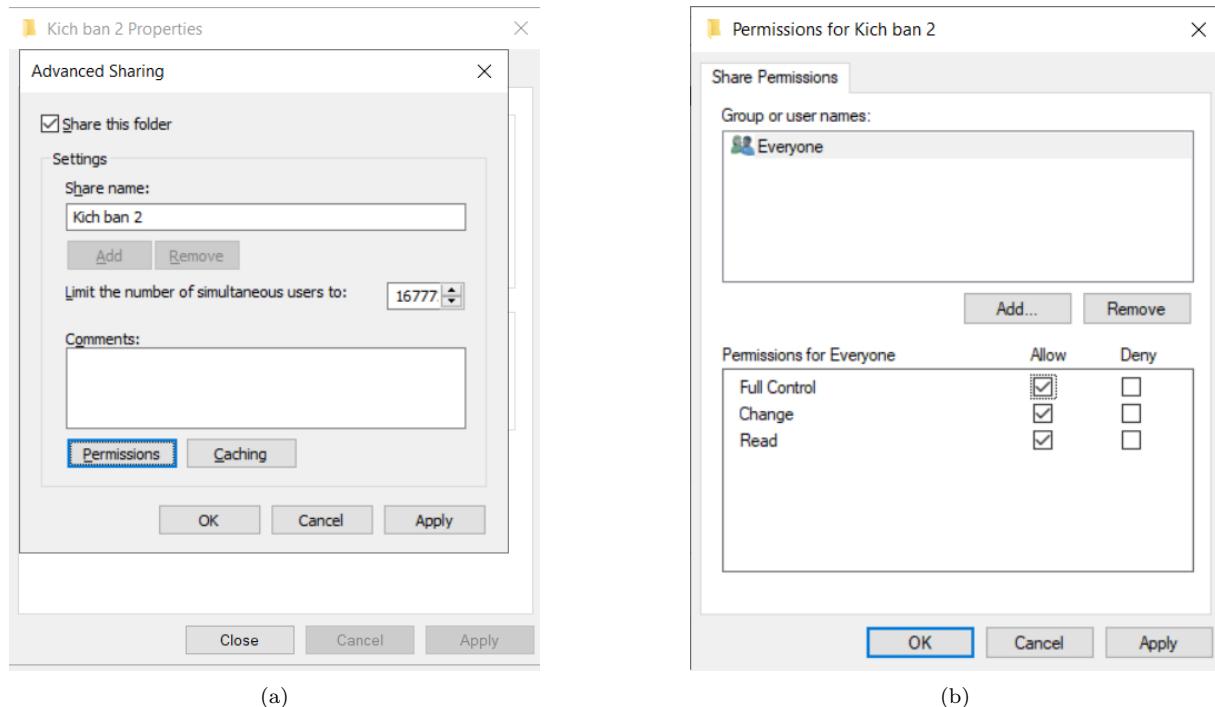
Hình 60: Tạo folder

- Nhấn Advanced Sharing rồi tích chọn Share this folder > Permissions rồi tích Full Control



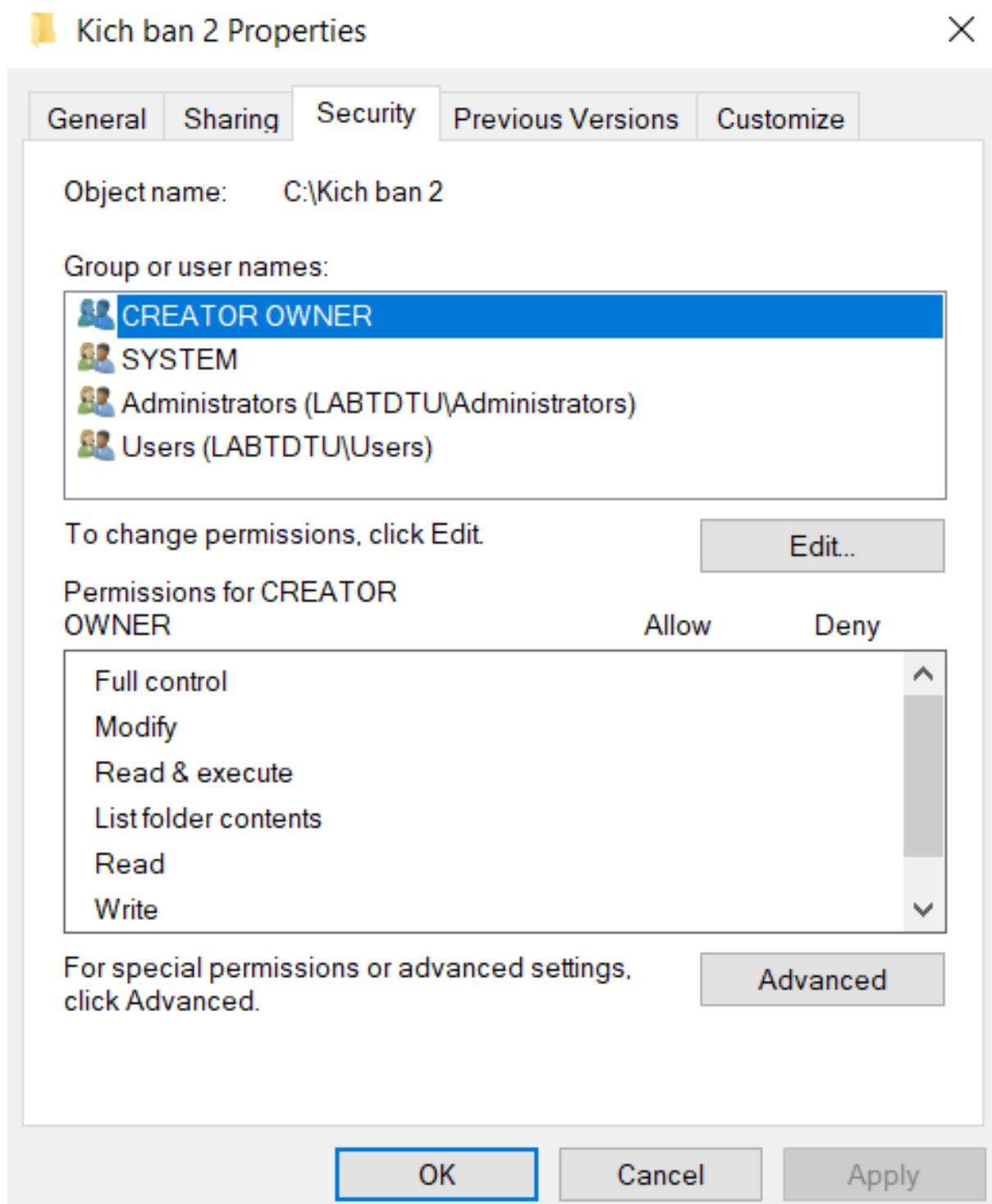
Hình 61: Chọn Advanced Sharing

- Nhấn chuột phải vào Folder ‘‘Kich ban 2’’ chọn Properties và chọn Security chọn Advanced > Auditing > Add > Select a Principal > Điền Everyone rồi nhấn Check Names > OK

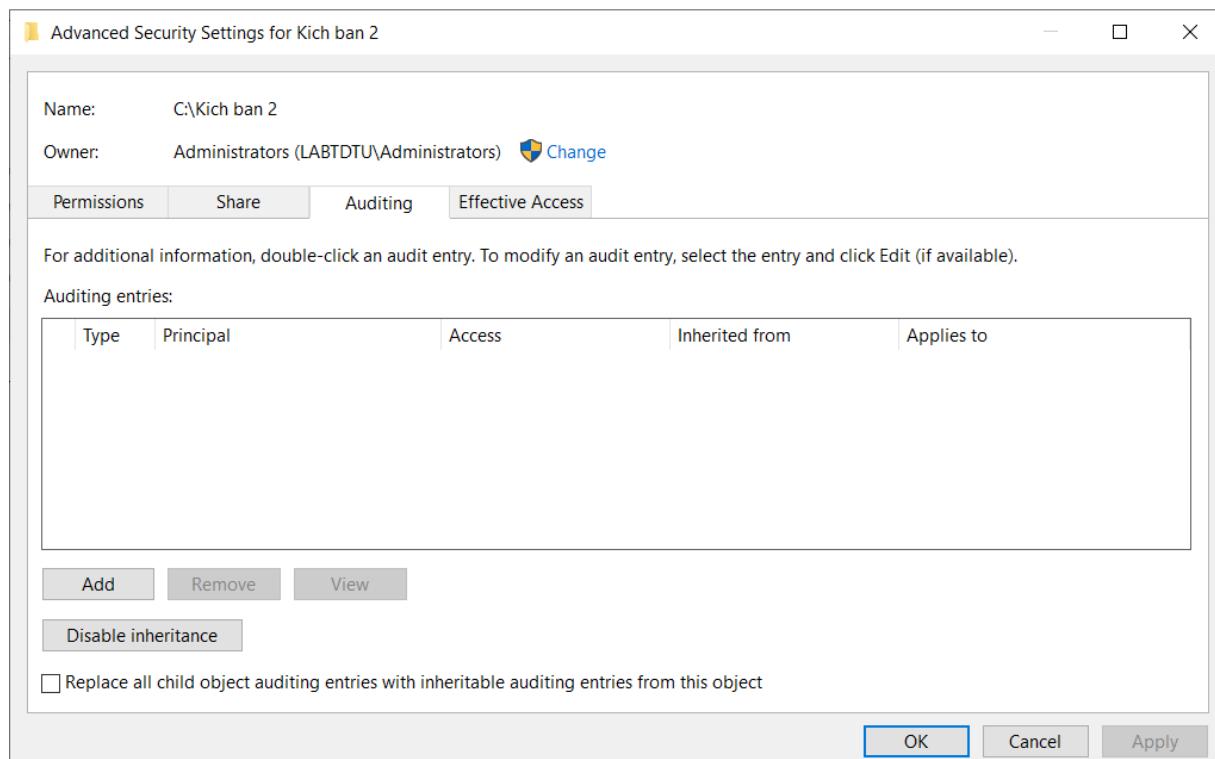


Hình 62: Cấu hình Permission

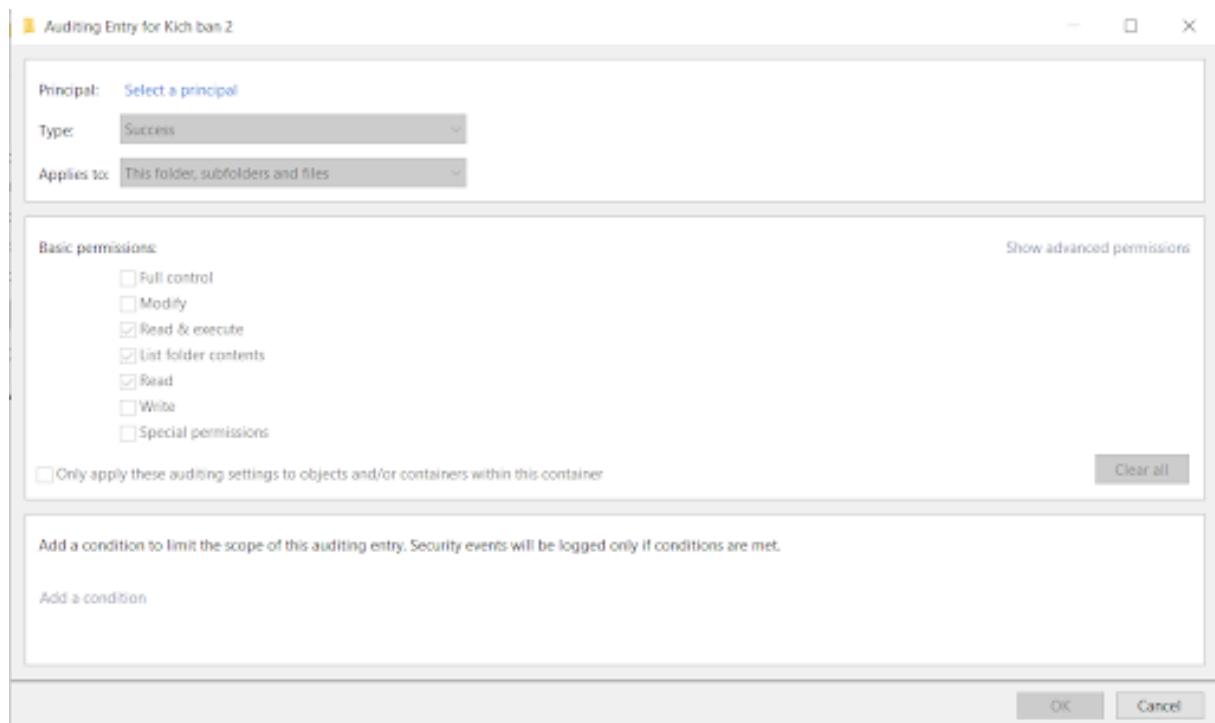
- Nhấn chuột phải vào Folder ‘‘Kich ban 2’’ chọn Properties và chọn Security chọn Advanced > Auditing > Add > Select a Principal > Điền Everyone rồi nhấn Check Names > OK



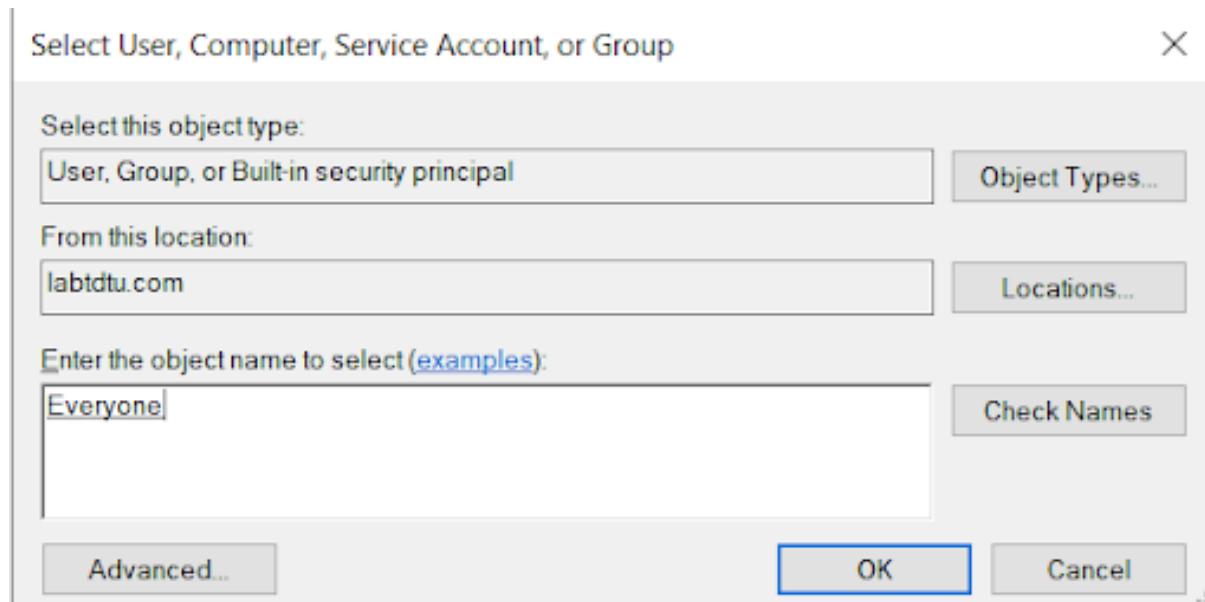
Hình 63: Security &gt; Advanced



Hình 64: Auditing &gt; Add

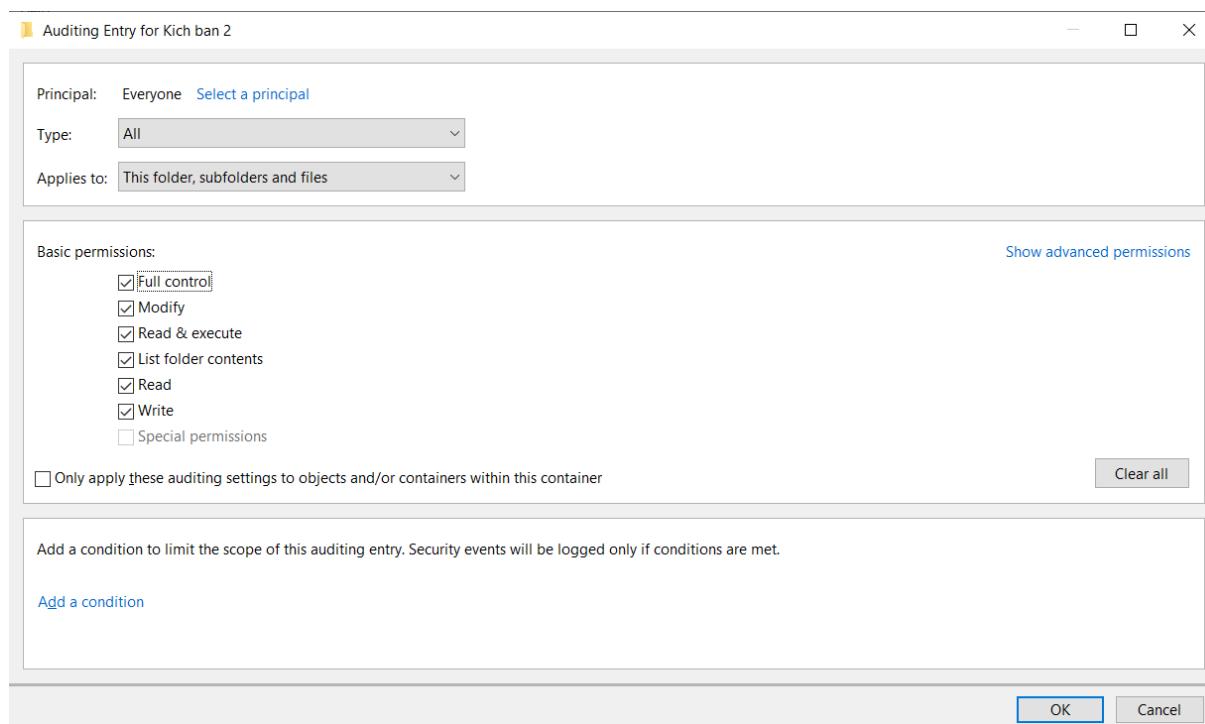


Hình 65: Add &gt; Select a Principal



Hình 66: Diền Everyone rồi nhấn Check Names &gt; OK

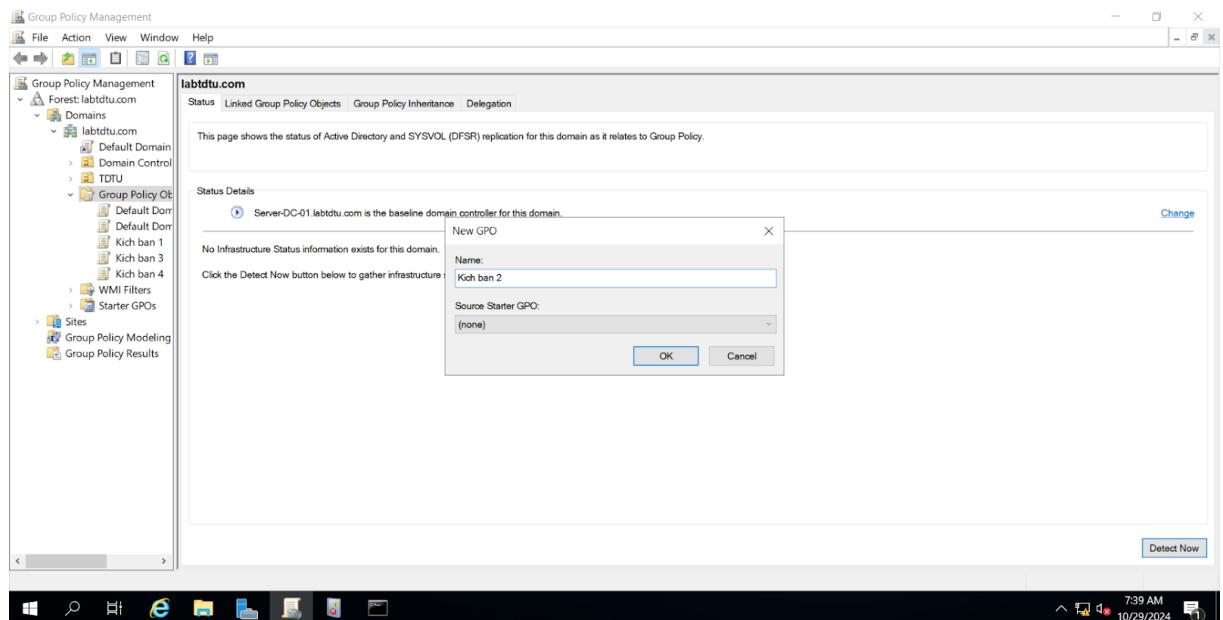
- Tại Auditing Entry for Kích ban 2, chỉnh Type: All và chọn Full control



Hình 67: Cài đặt Auditing Entry

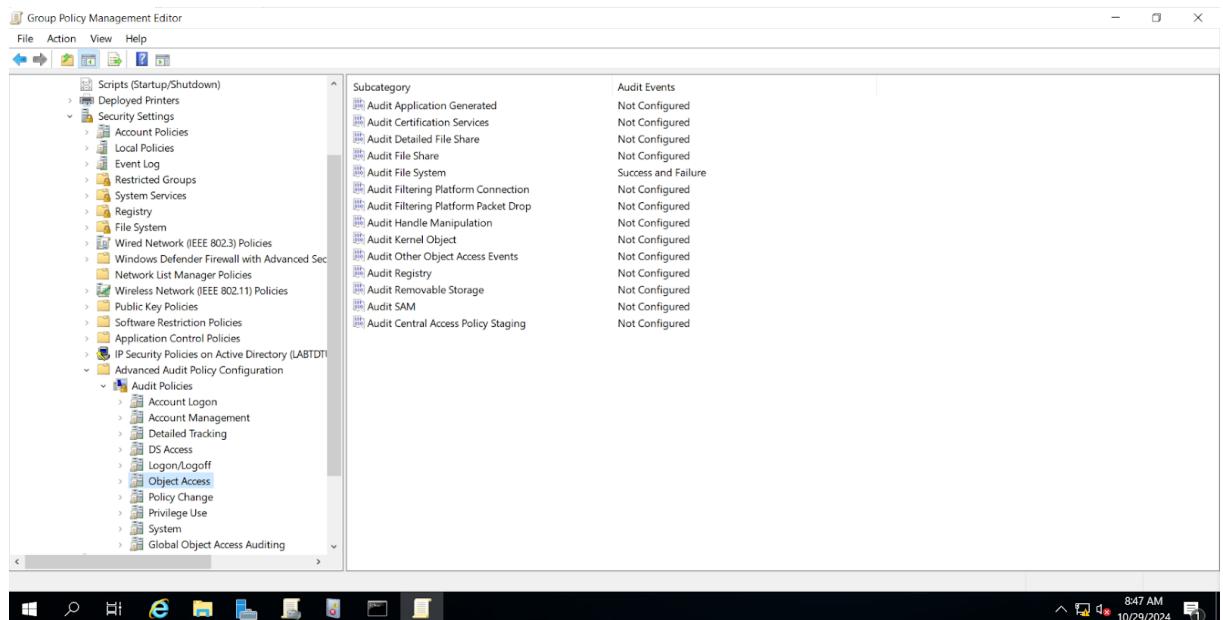
- Thiết lập Auditing trên các tệp và thư mục cần giám sát (Properties > Security > Advanced > Auditing).
- Nhấn chuột phải vào Group Policy Objects rồi

chọn New để tạo GPO ‘‘Kích bản 2’’



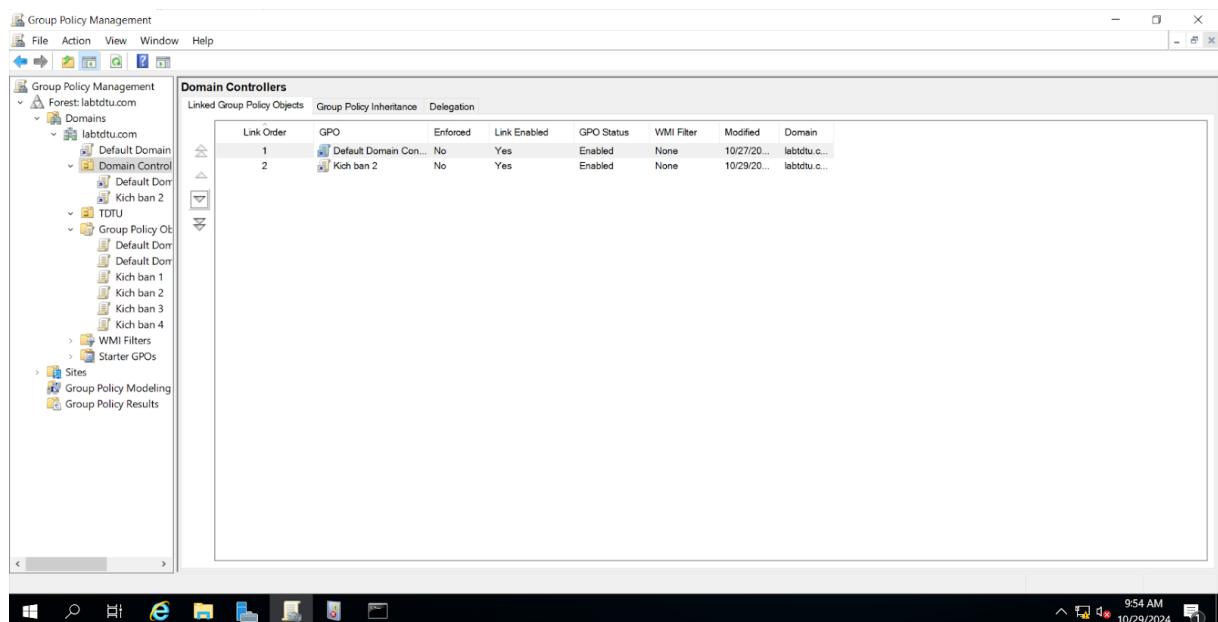
Hình 68: Tạo GPO kích bản 2

– Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access



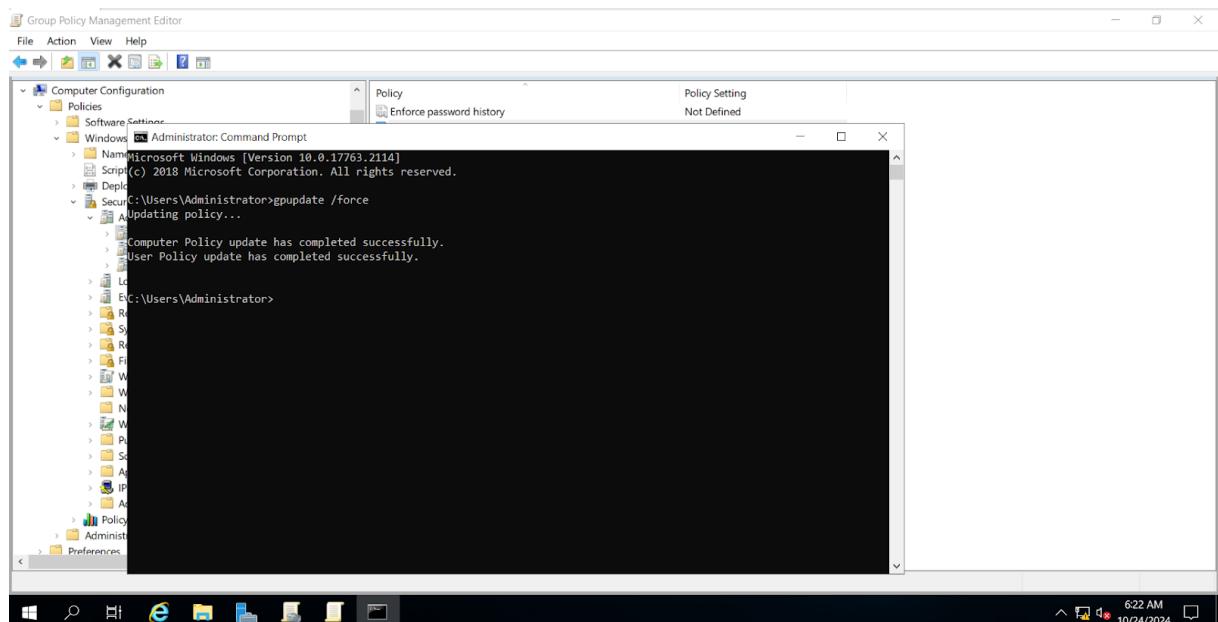
Hình 69: Chọn Audit File System cho cả sự kiện Success and Failure

- Ra Group Policy Manager và kéo GPO kích ban 2 vào Domain Control



Hình 70: Liên kết kịch bản 2 vào Domain Control

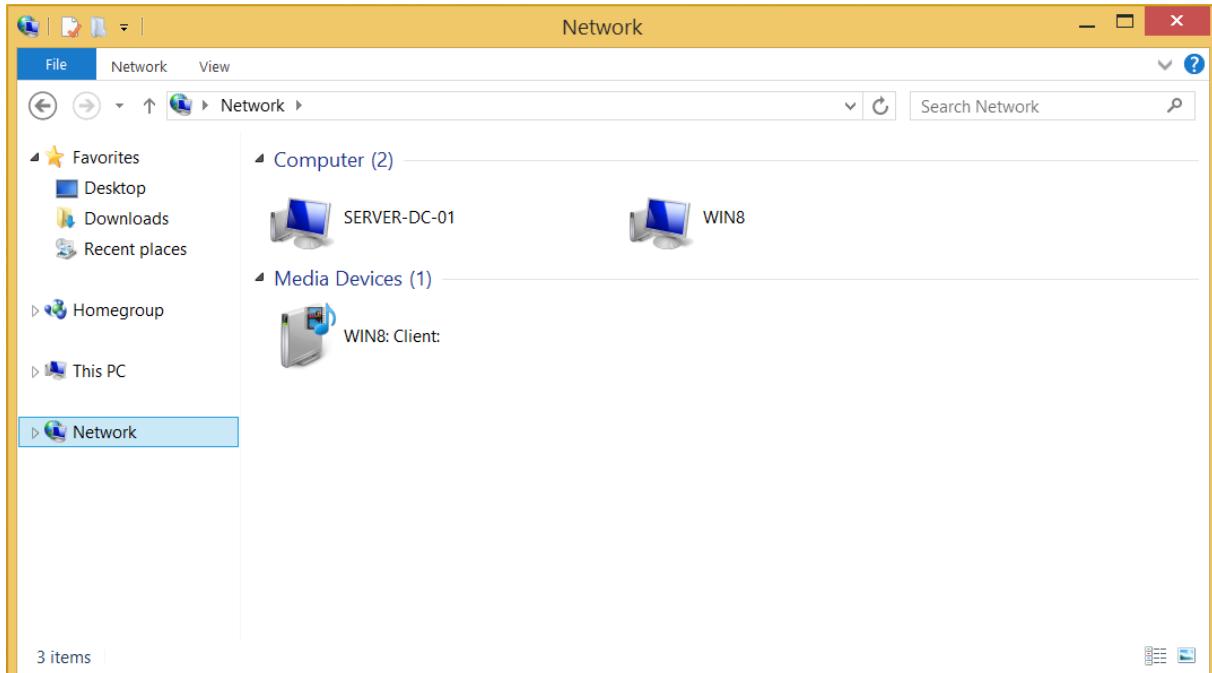
- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh gpupdate /force trong Command Prompt (với quyền Admin):



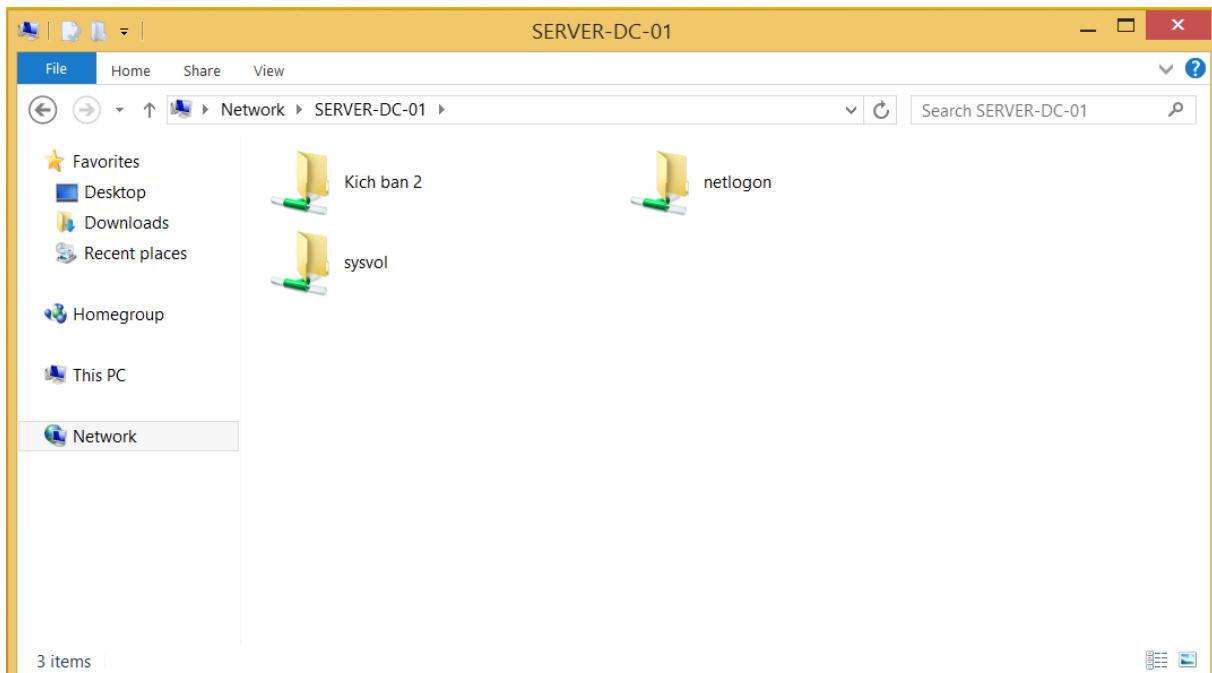
Hình 71: gpupdate /force

## 2. Demo: Kiểm tra trong Event Viewer

- Vào máy Windows 8.1 > Network > SERVER-DC-01 > Kích ban 2

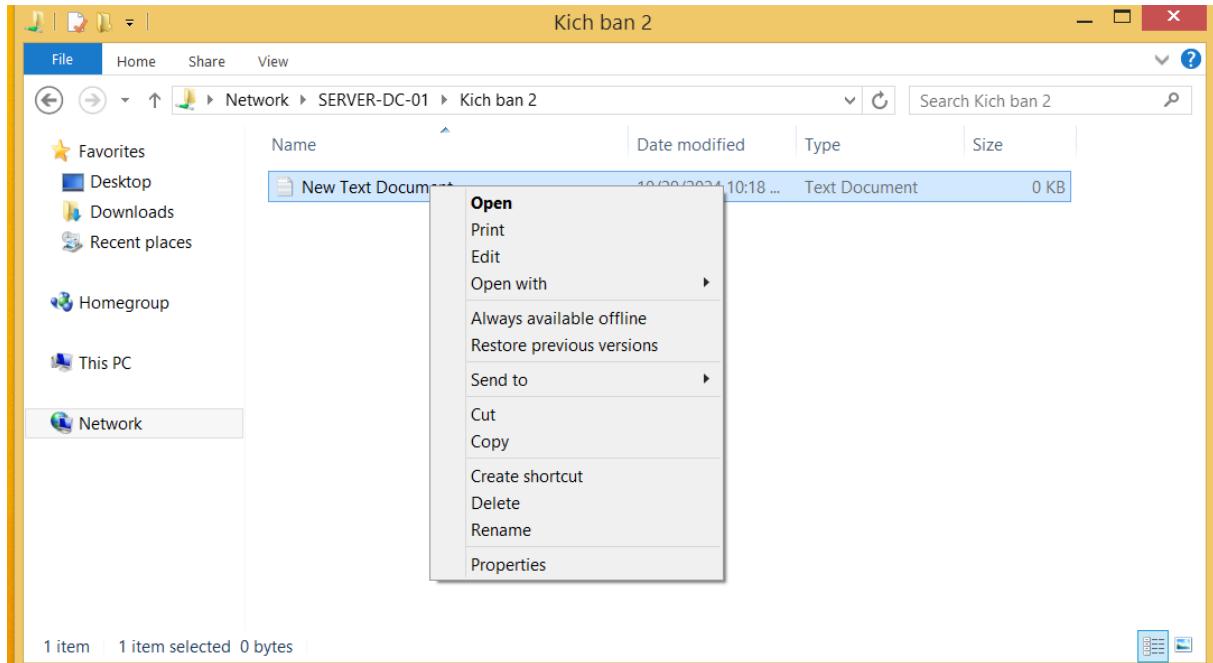


Hình 72: Windows 8.1 > Network



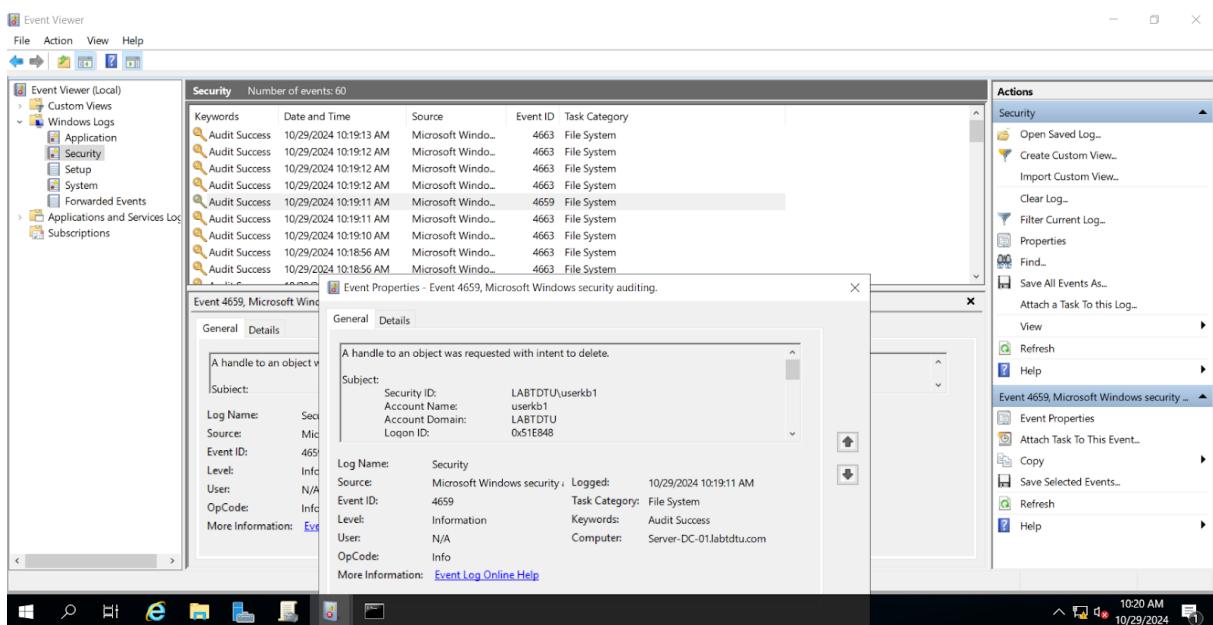
Hình 73: SERVER-DC-01 > Kích ban 2

- Tạo 1 file và xóa để kiểm tra thử



Hình 74: Tạo và xóa file

- Mở Server Manager > Tools > Event Viewer Trong Event Viewer, điều hướng đến: Windows Logs > Security.
- Tìm mã sự kiện 4663 (truy cập vào tệp hoặc thư mục) và 4660 và 4659 (xóa tệp)



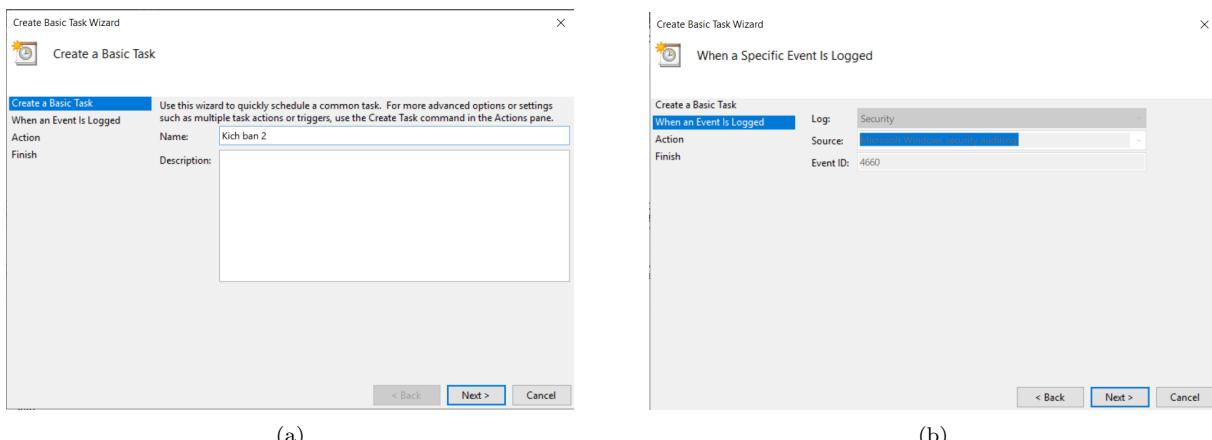
Hình 75: Kiểm tra Event Viewer

- Tạo POPUP hiện thông báo khi xóa object Tại Event Viewer, điều hướng đến: Windows Logs > Security.
- Chọn log có mã 4660, và nhấn chuột phải vào và chọn Attach Task To This Event

Security Number of events: 63 (0) New events available				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	11/21/2024 8:40:33 AM	Microsoft Windo...	4624	Logon
Audit Success	11/21/2024 8:40:33 AM	Microsoft Windo...	4660	File System
Audit Success	11/21/2024 8:40:33 AM	Microsoft Windo...	4663	File System
Audit Success	11/21/2024 8:40:33 AM	Microsoft Windo...	4663	File System
Audit Success	11/21/2024 8:40:26 AM	Microsoft Windo...	4663	File System
Audit Success	11/21/2024 8:40:19 AM	Microsoft Windo...	4624	Logon
Audit Success	11/21/2024 8:40:19 AM	Microsoft Windo...	4672	Special Logon
Audit Success	11/21/2024 8:40:19 AM	Microsoft Windo...	4624	Logon
Audit Success	11/21/2024 8:40:14 AM	Microsoft Windo...	4624	Logon
Audit Success	11/21/2024 8:40:12 AM	Microsoft Windo...	4624	Logon

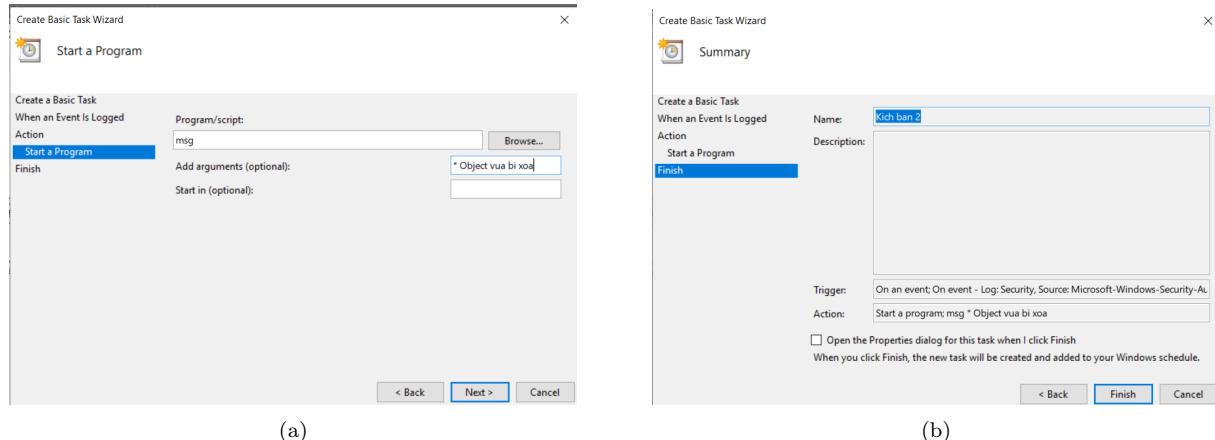
Hình 76: Tìm log ID 4660

- Tại mục Create a Basic Task > Điền name và Kích ban 2



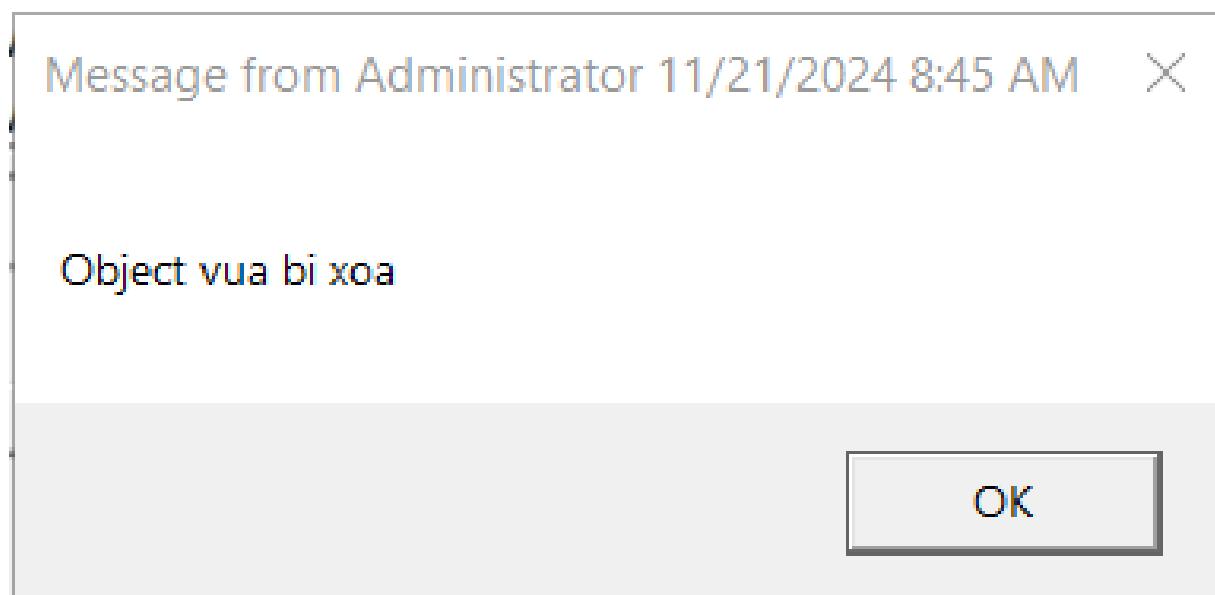
Hình 77: Diền log ID

- Tại Start a Program: Điền msg vào Program và điền “\* Object vua bi xoa” vào Add arguments



Hình 78: Hoàn thành task

- Kết quả

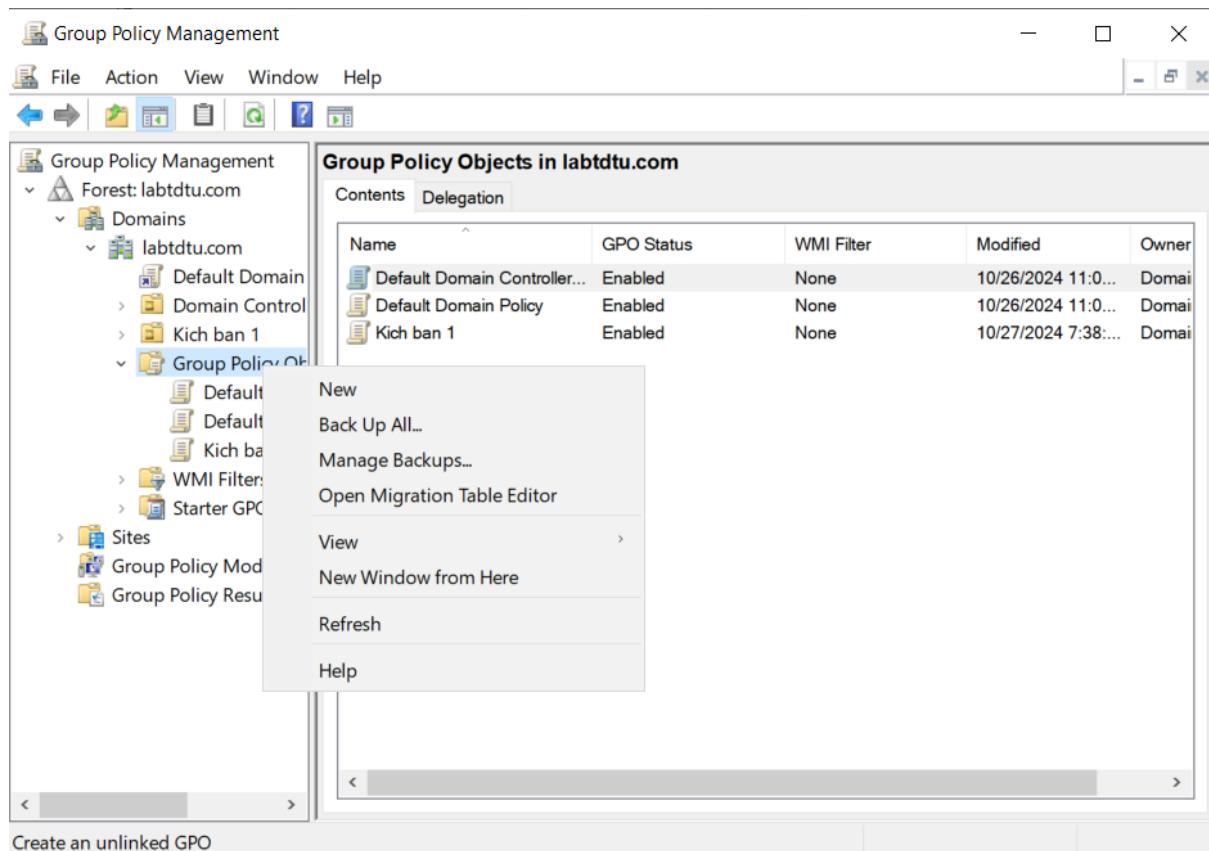


Hình 79: Sau khi có một file bị xóa thông báo sẽ hiển thị

### 3.3 Kích bản 3: Giám sát việc thay đổi tài khoản trong Active Directory

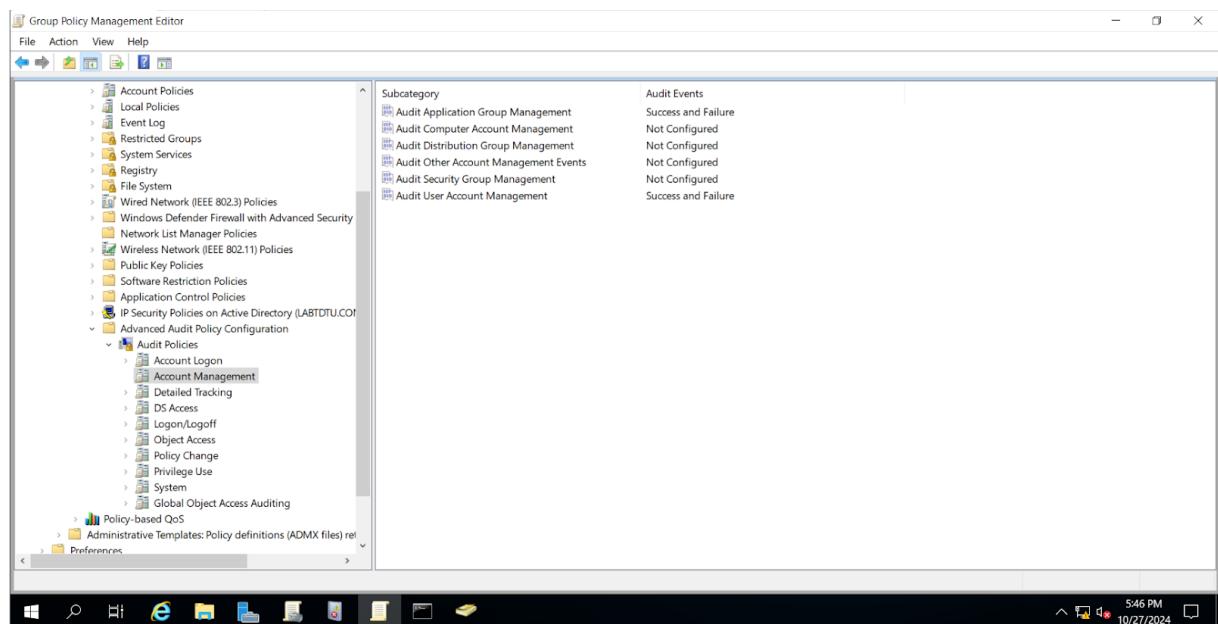
#### 1. Thiết lập Audit Policy:

- Bật Audit Account Management để ghi lại các thay đổi về tài khoản như tạo, xóa, hoặc chỉnh sửa tài khoản.
  - Vào **Group Policy Management** mở rộng **Forest > Domains > labtdtu.com**



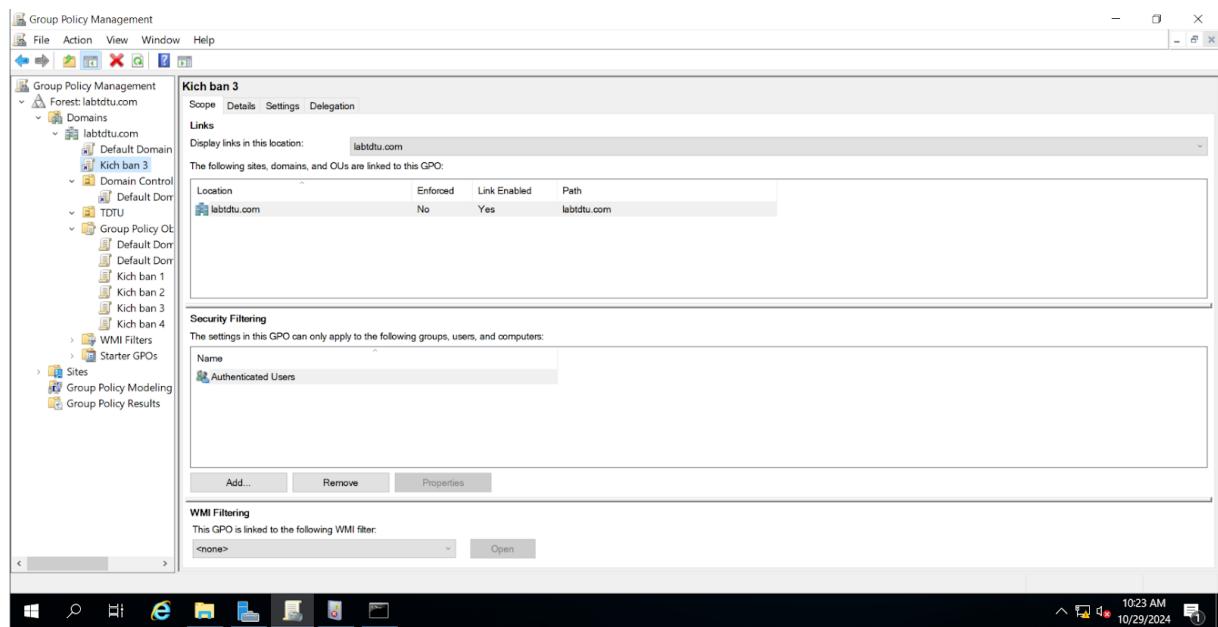
Hình 80: Nhấn chuột phải vào **Group Policy Objects** rồi chọn **New** để tạo GPO “Kích ban 3”

- Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Account Management.



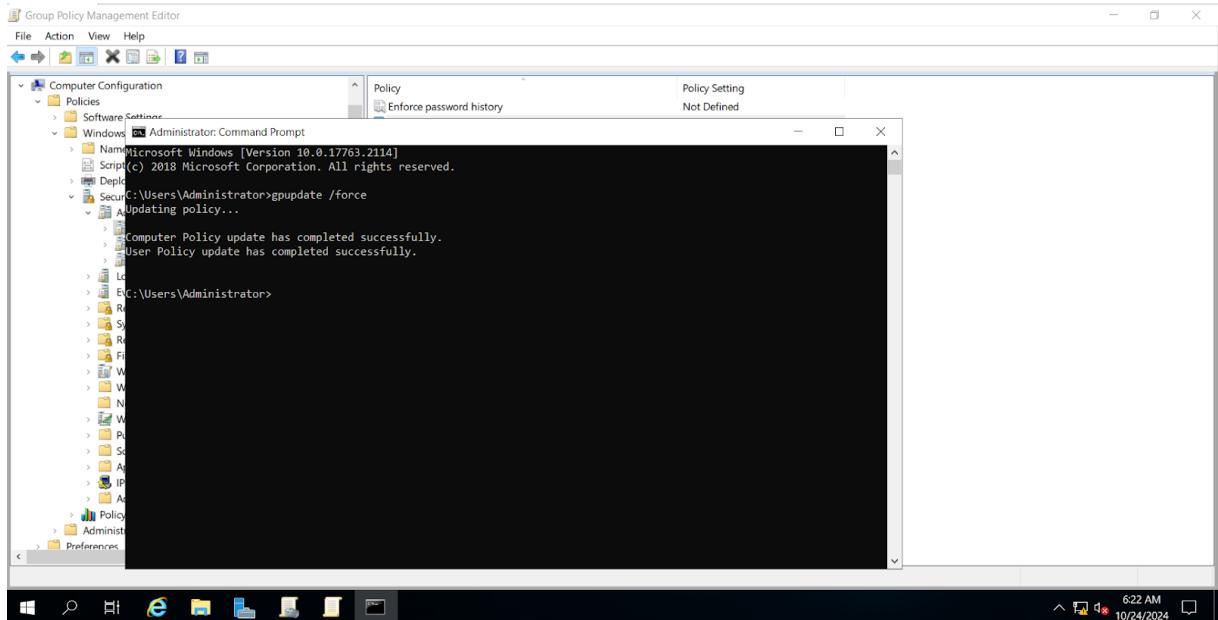
Hình 81: Chọn **Audit Application Group Management** và **Audit User Account Management** cho cả sự kiện **Success and Failure**

- Ra Group Policy Manager và kéo GPO kich ban 3 vào labtdu.com



Hình 82

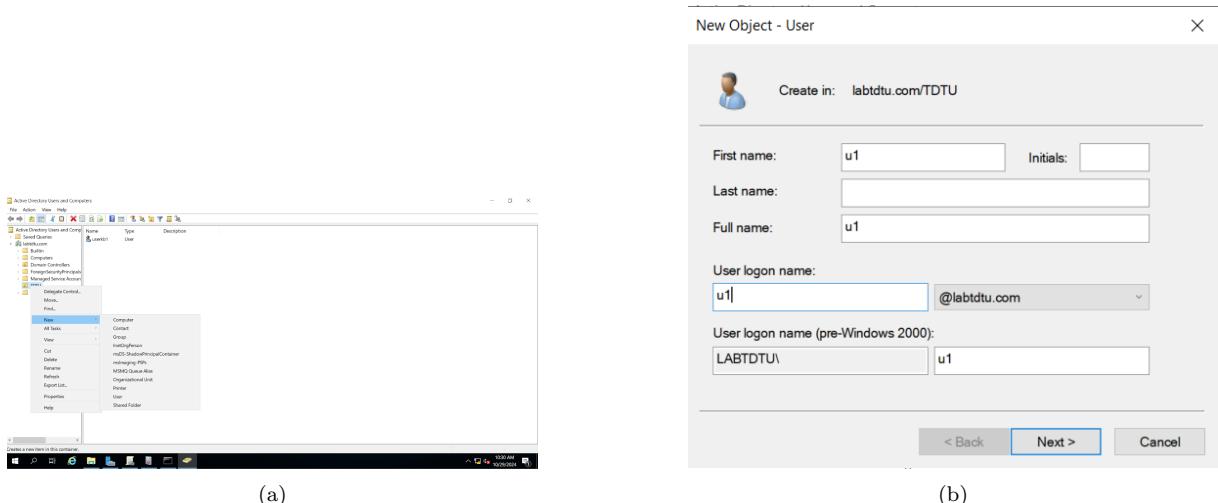
- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh **gpupdate /force** trong **Command Prompt** (với quyền Admin):



Hình 83: gpupdate /force

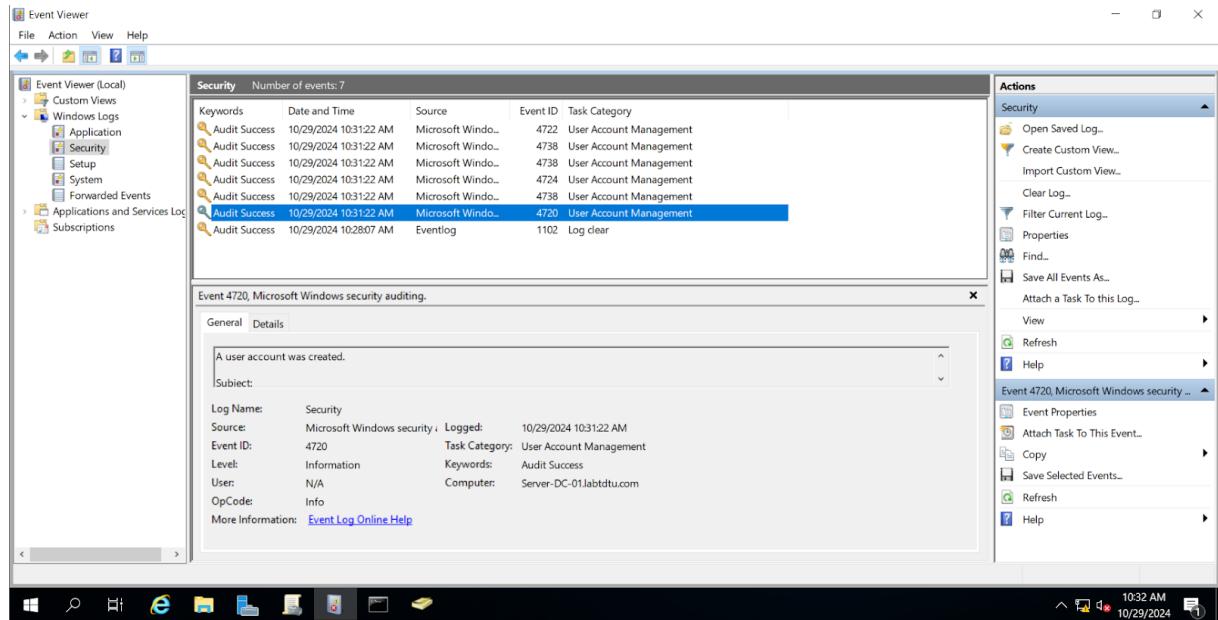
## 2. Demo: Theo dõi các mã sự kiện liên quan

- Vào Server Manager > Dashboard chọn Tools > Active Directory Users and Computers



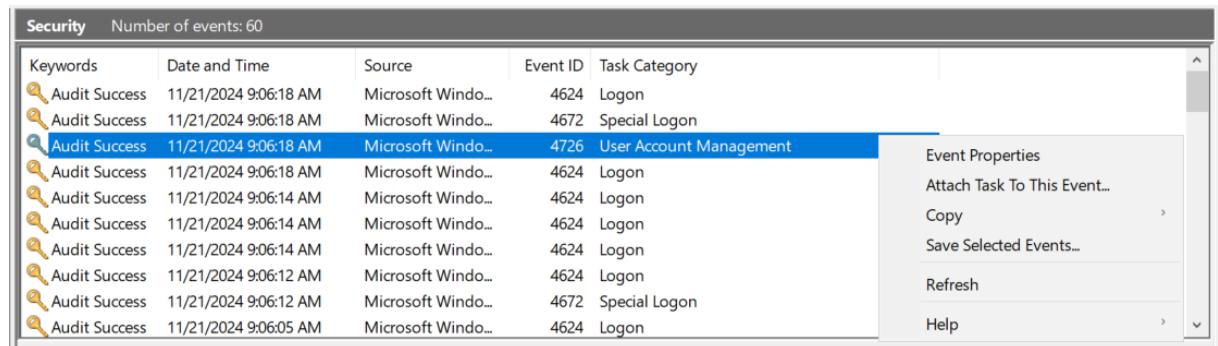
Hình 84: Vào tạo 1 user mới

– Mở Server Manager > Tools > Event Viewer



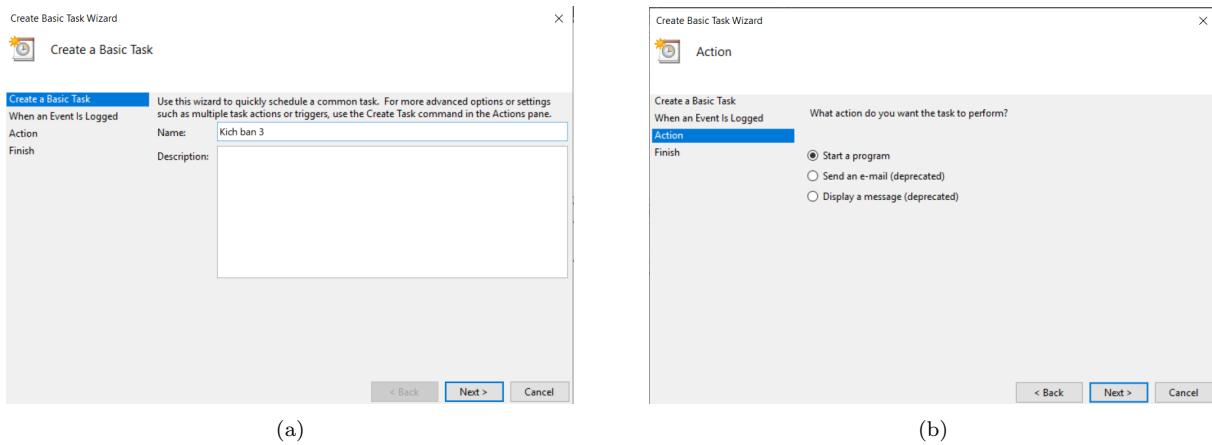
Hình 85: Trong Event Viewer, điều hướng đến: Windows Logs > Security.

– Tạo POPUP mỗi khi xóa user



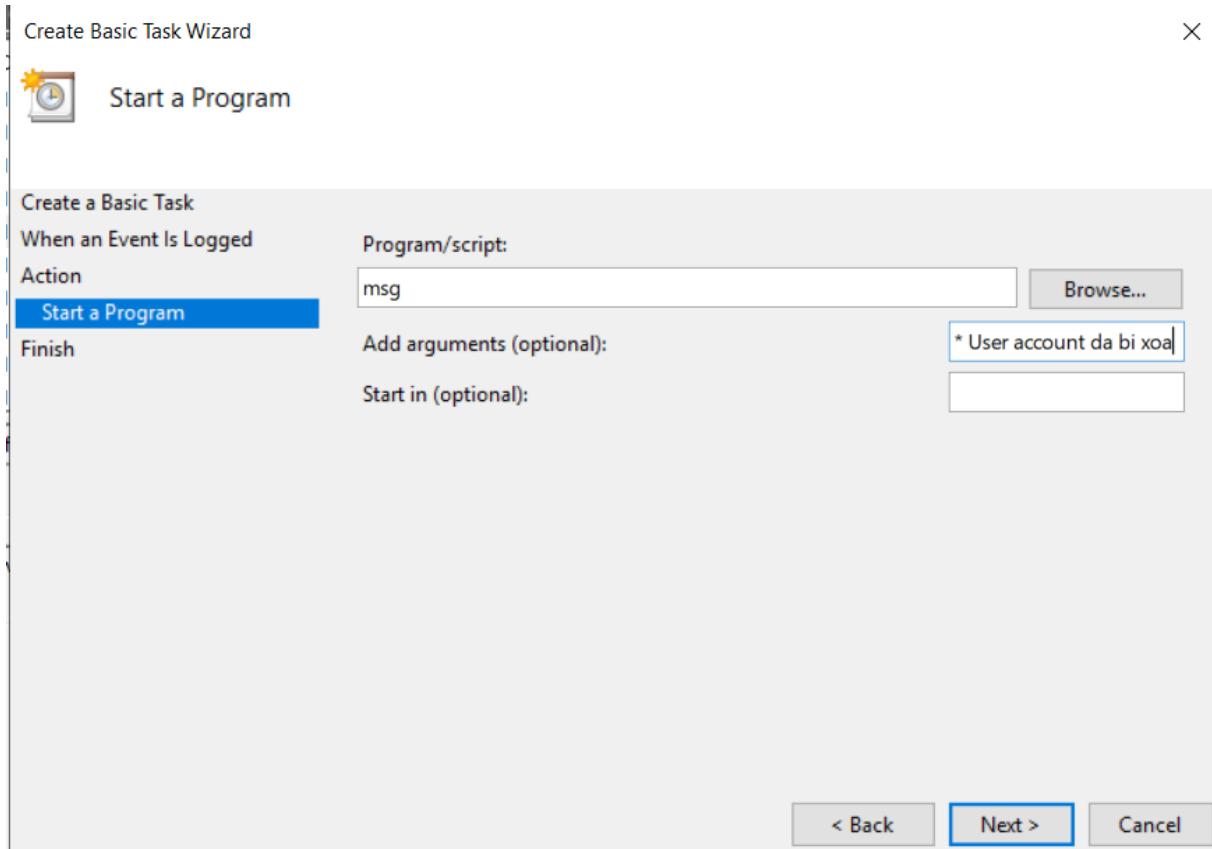
Hình 86: Tạo popup

- Tại mục Create a Basic Task > Điền name và Kích ban 3



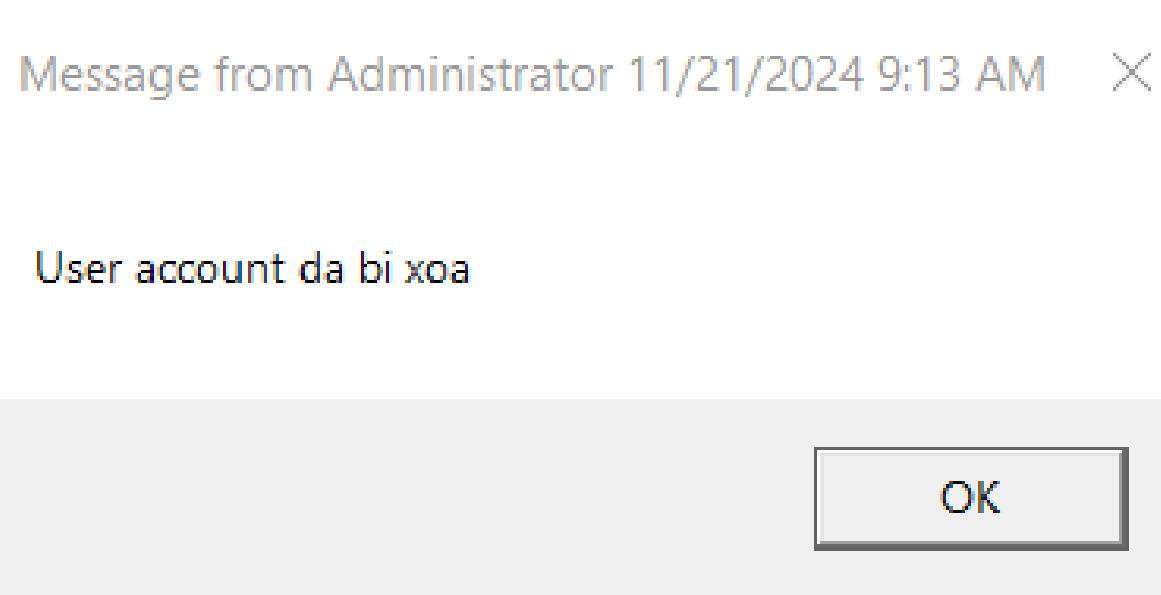
Hình 87: hoàn thành task

- Tại Start a Program: Điền msg vào Program và điền “ \* User account da bi xoa” vào Add arguments



Hình 88: Tạo đoạn thông báo tin

– Kết quả

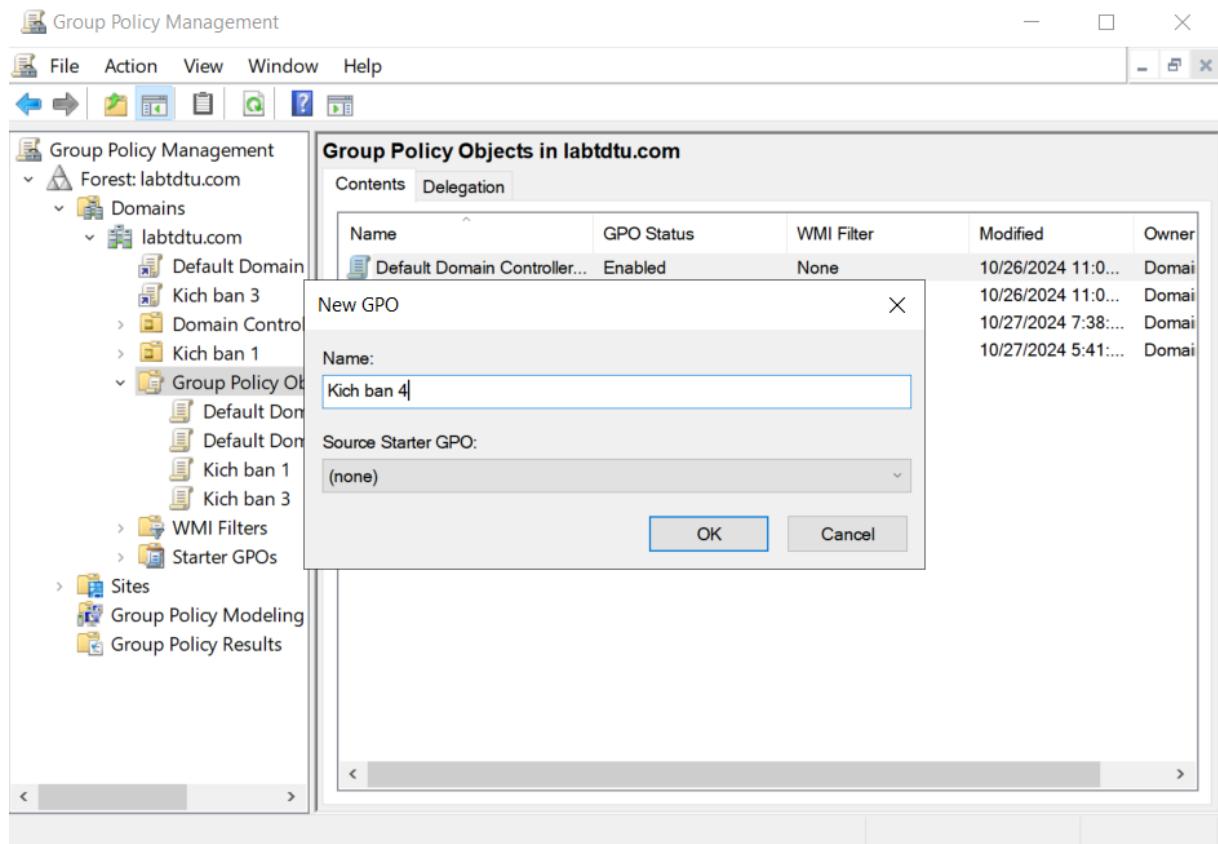


Hình 89: Sau khi có một tài khoản bị xóa thông báo sẽ hiển thị

### 3.4 Kịch bản 4: Giám sát các thay đổi trong GPO

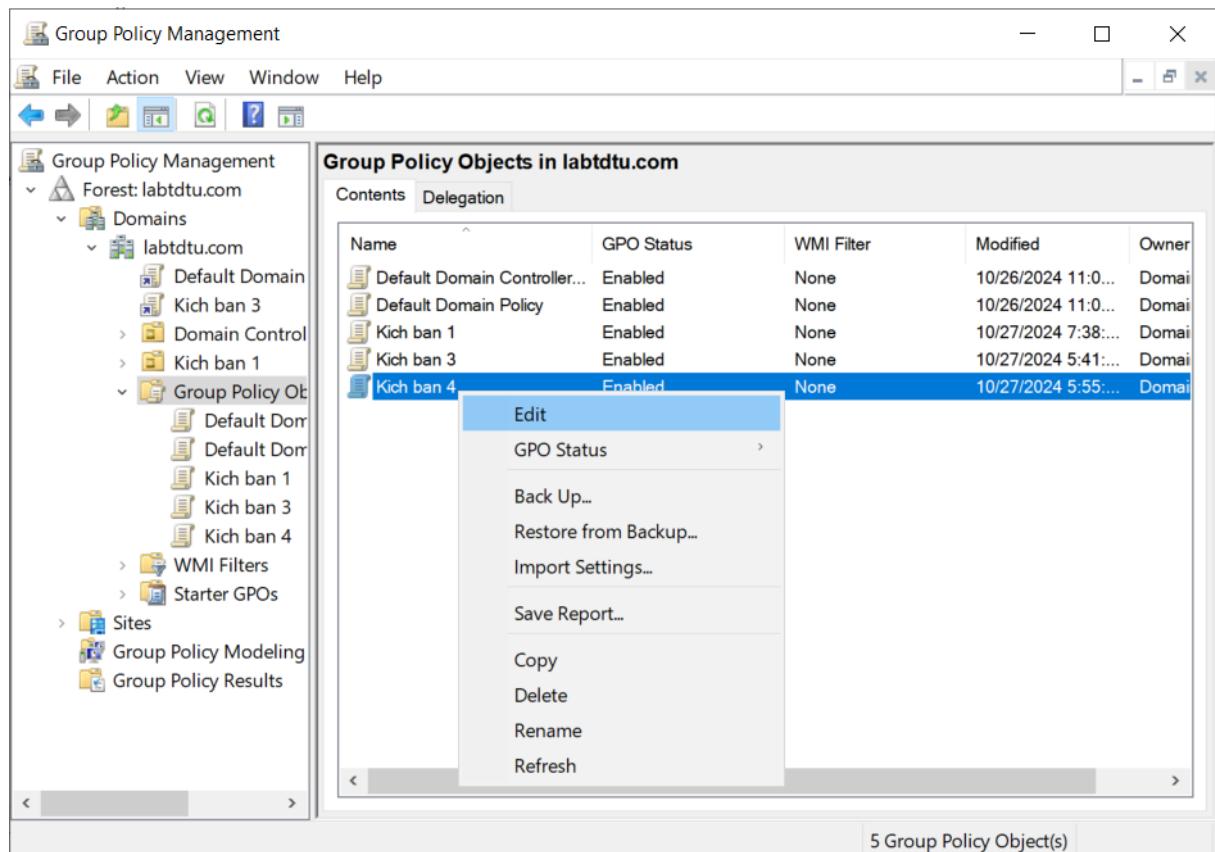
#### 1. Thiết lập Audit Policy:

- Bật Audit Policy Change để giám sát các thay đổi chính sách bảo mật.
- Vào **Group Policy Management** mở rộng **Forest > Domains > labtdtu.com**



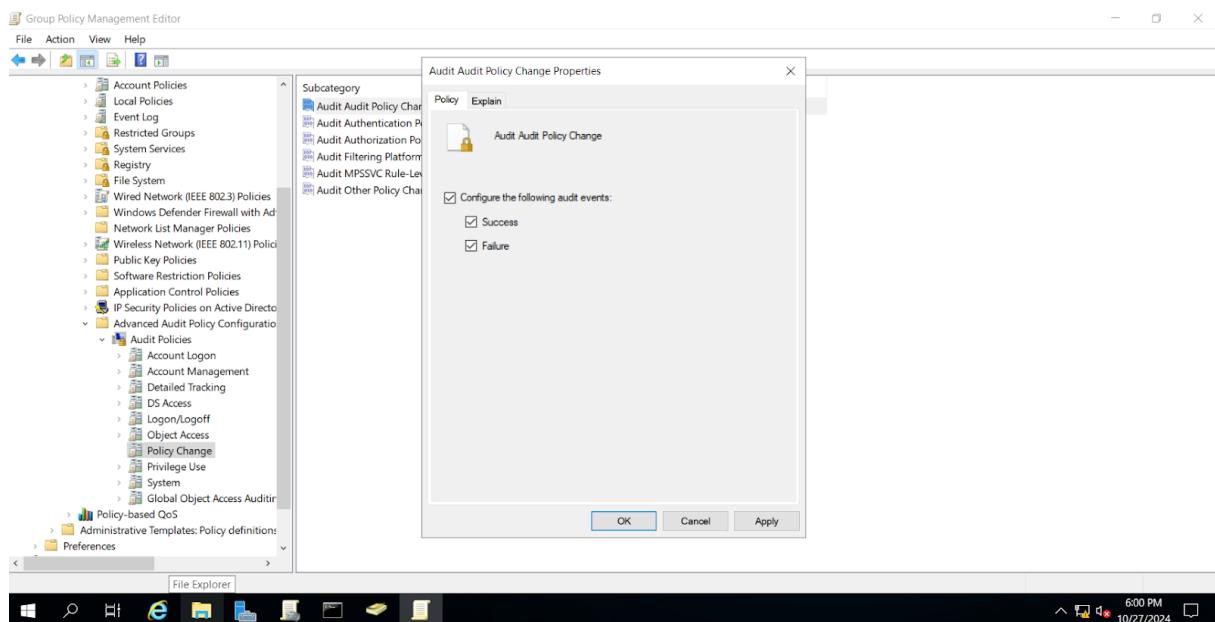
Hình 90: Nhấn chuột phải vào **Group Policy Objects** rồi chọn **New** để tạo GPO “Kich ban 4”

- Chuột phải vào GPO “Kích ban 4” vừa tạo và chọn **Edit** để vào tab **Group Policy Management Editor**



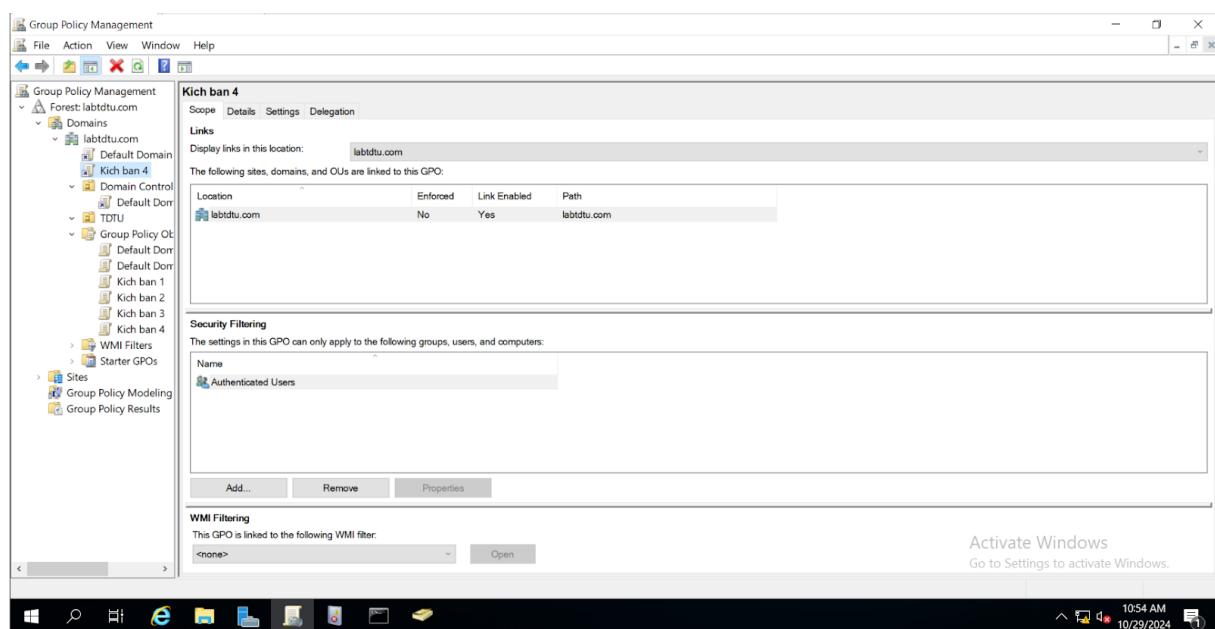
Hình 91

- Điều hướng đến **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Policy Change.**



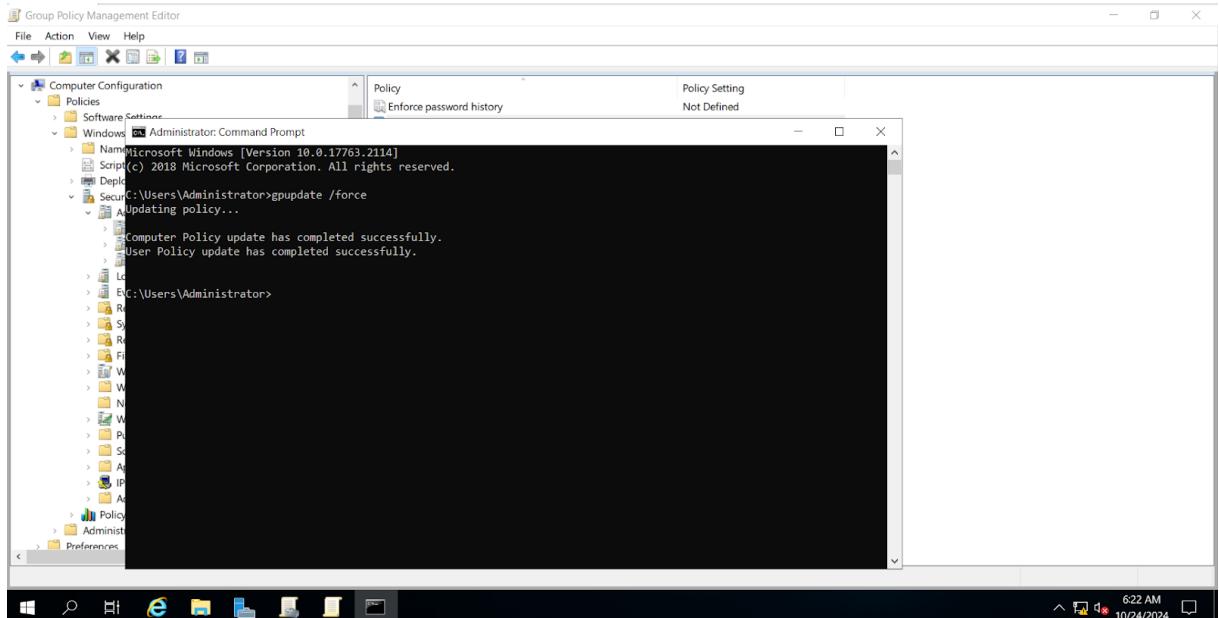
Hình 92: Chọn **Audit Audit Policy Change** và bật cho cả sự kiện Success and Failure

- Ra Group Policy Manager và kéo GPO kich ban 4 vào labtdu.com



Hình 93: Liên kết GPO kich ban 4 vào domain control

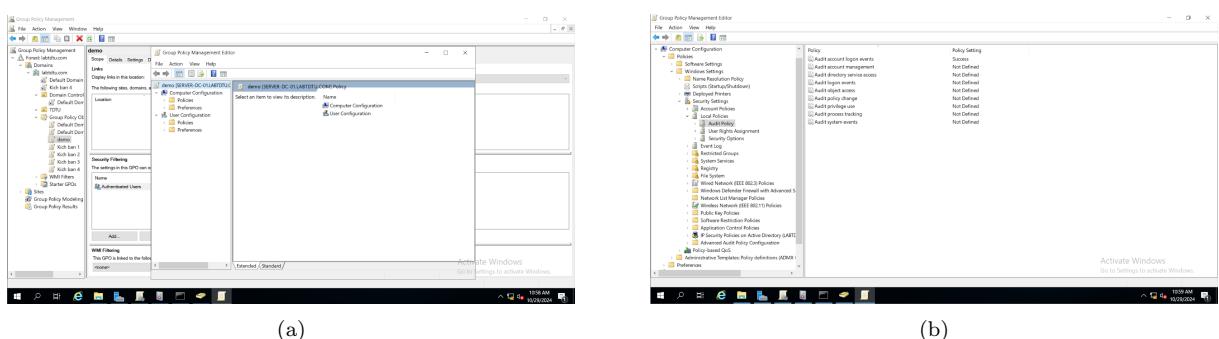
- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh **gpupdate /force** trong **Command Prompt** (với quyền Admin):



Hình 94: gpupdate /force

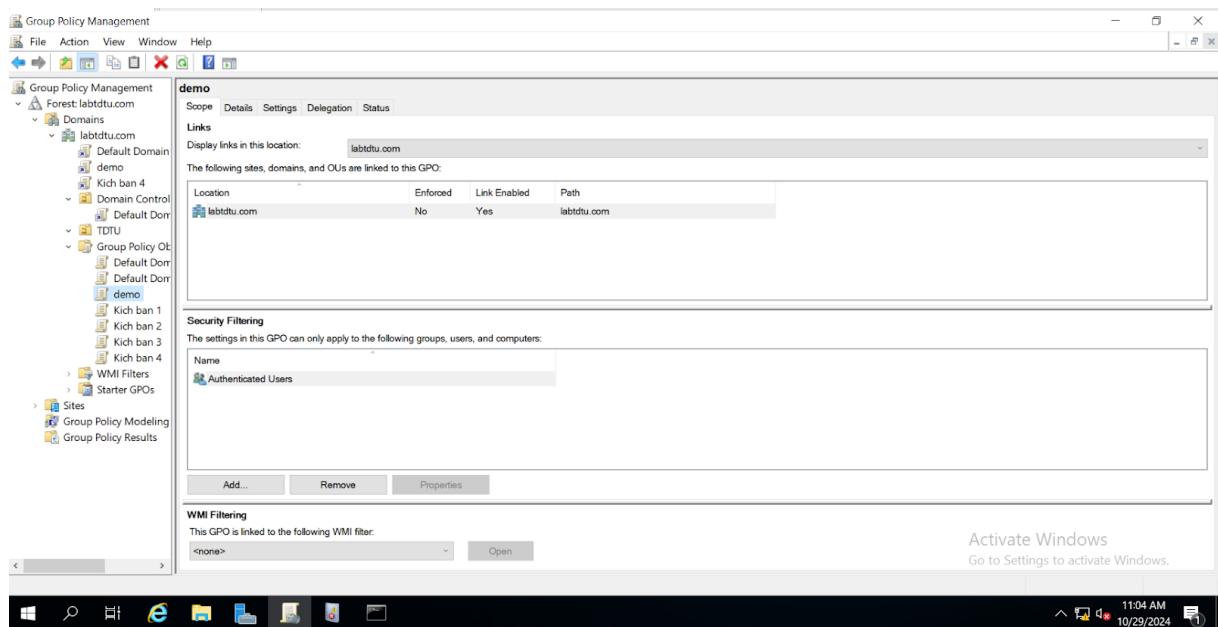
## 2. Demo: Kiểm tra các mã sự kiện liên quan

- Vào Server Manager > Dashboard chọn Tools > Group Policy Management



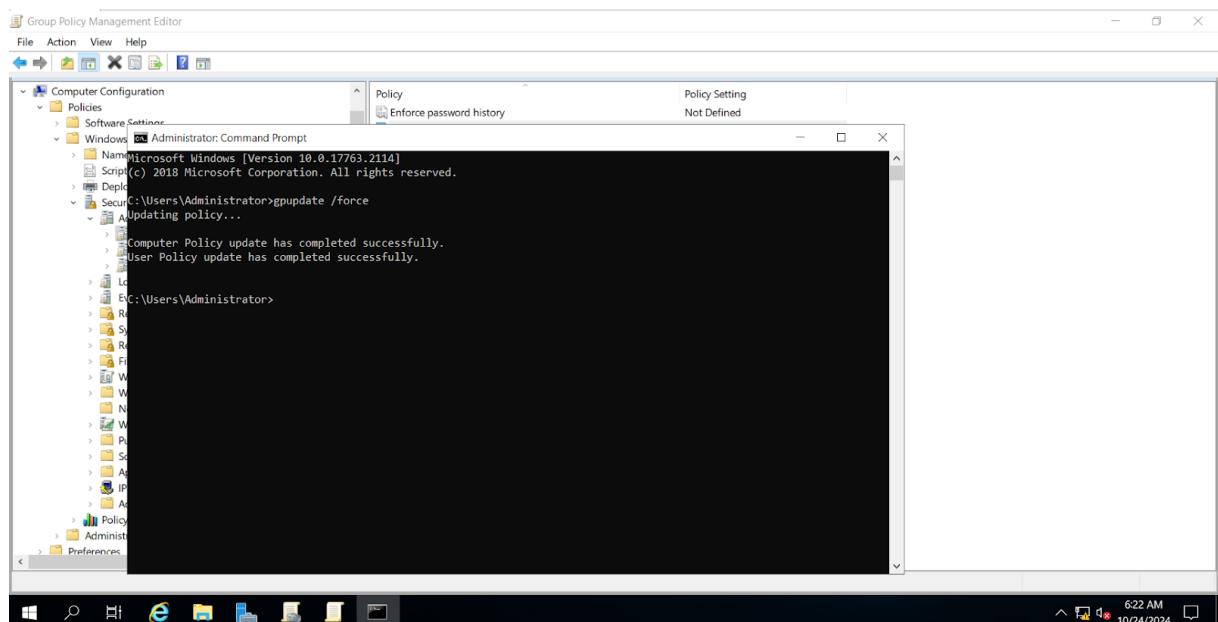
Hình 95: Tạo GPO demo > Click chuột phải vào GPO demo Chọn Edit và test thử

- Di chuyển GPO cho labtdtu.com



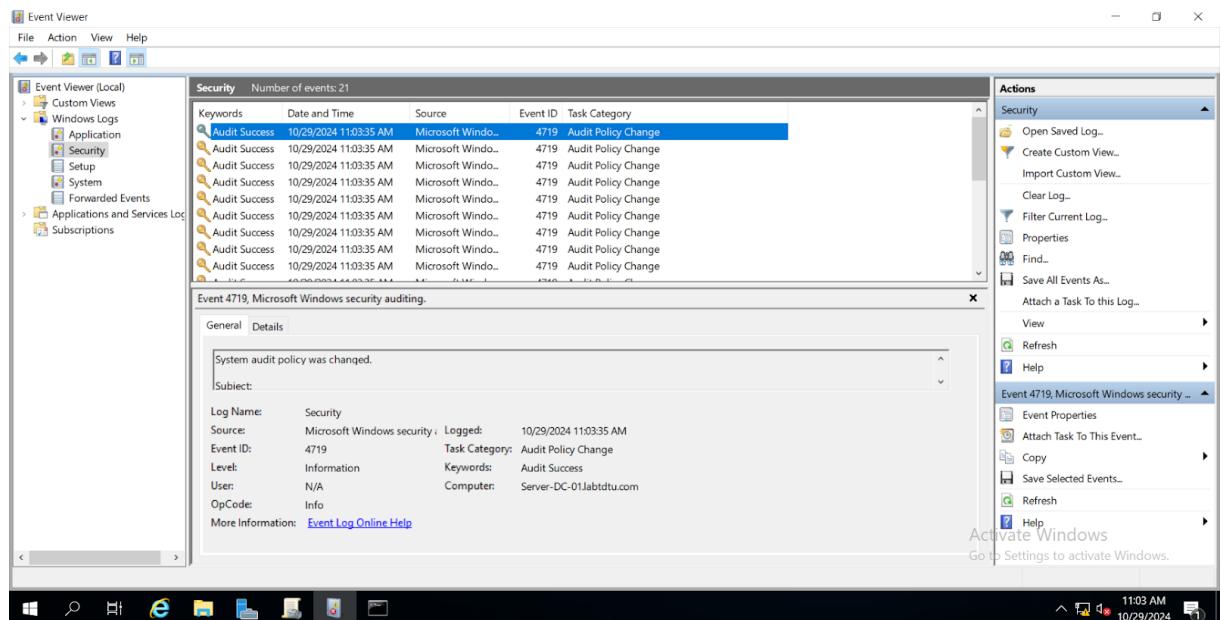
Hình 96: Liên kết GPO vào domain control

- Sau khi thực hiện các cấu hình, áp dụng Group Policy bằng cách chạy lệnh **gpupdate /force** trong **Command Prompt** (với quyền Admin):



Hình 97: gpupdate /force

- Mở **Server Manager** > **Tools** > **Event Viewer**
  - Trong Event Viewer, điều hướng đến: Windows Logs > Security.

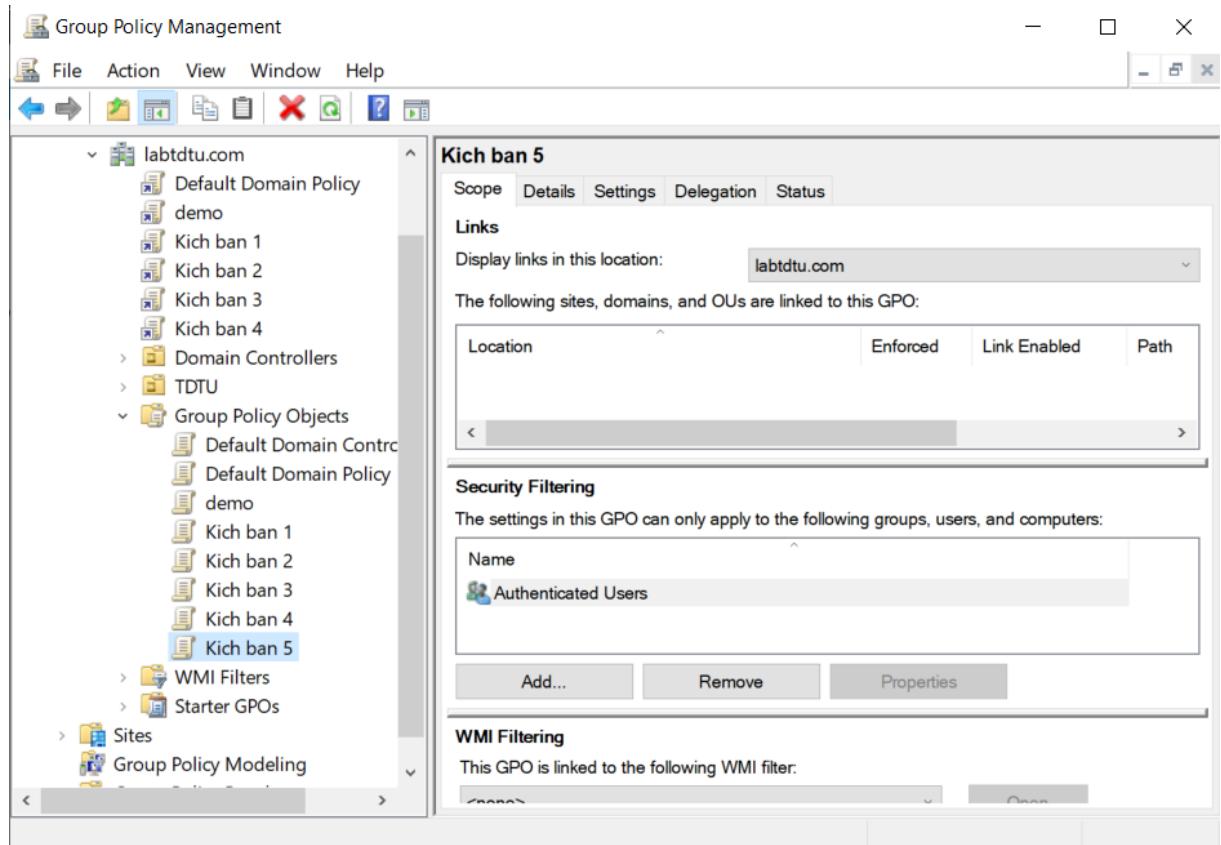


Hình 98: Tìm mã **4719**: Đặt lại Audit Policy.

### 3.5 Kịch bản 5: Cấu hình Firewall

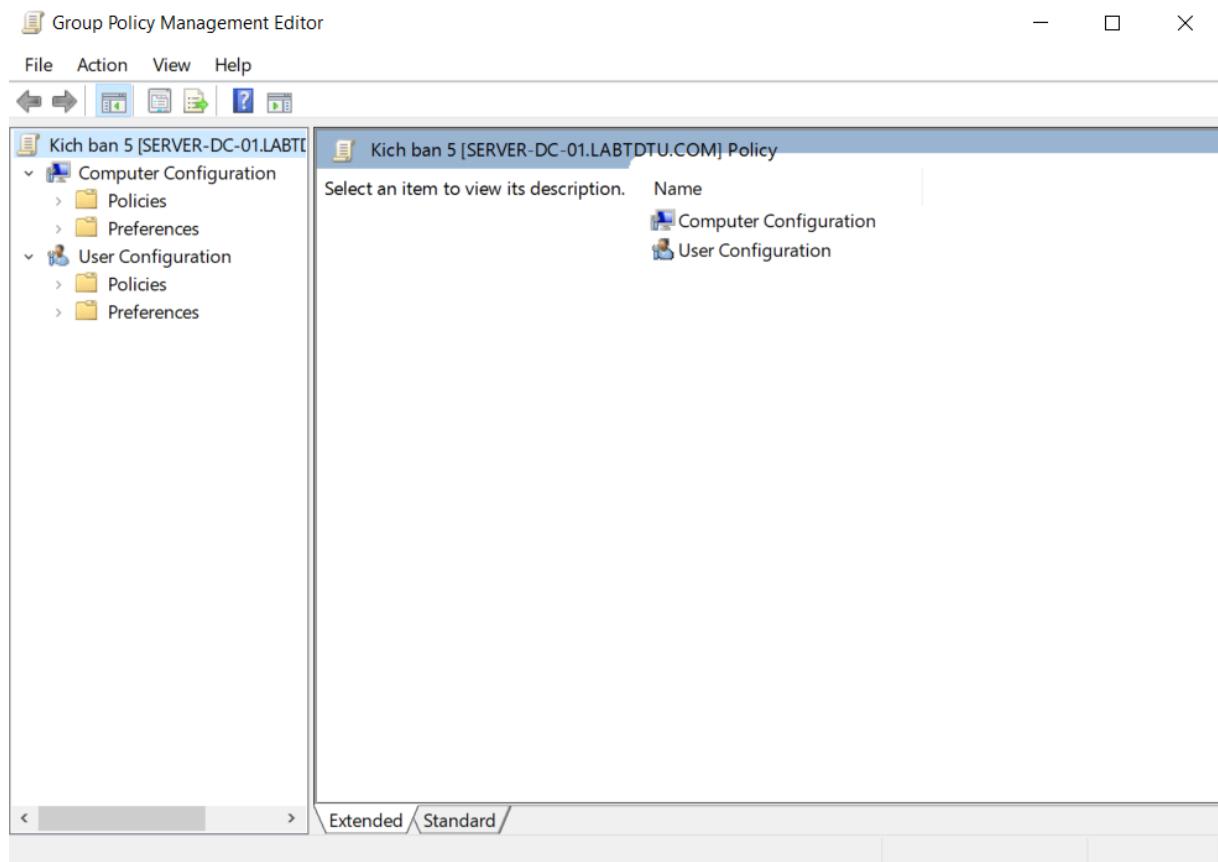
- Mở Server Manager > Dashboard và chọn Tools > Group Policy Management.

Trong **Group Policy Management**, mở rộng **Forest > Domains**. Nhấn chuột phải vào Group Policy Objects rồi chọn **New**



Hình 99: Diền tên cho GPO mới tạo là “Kich ban 5” và nhấn **OK**

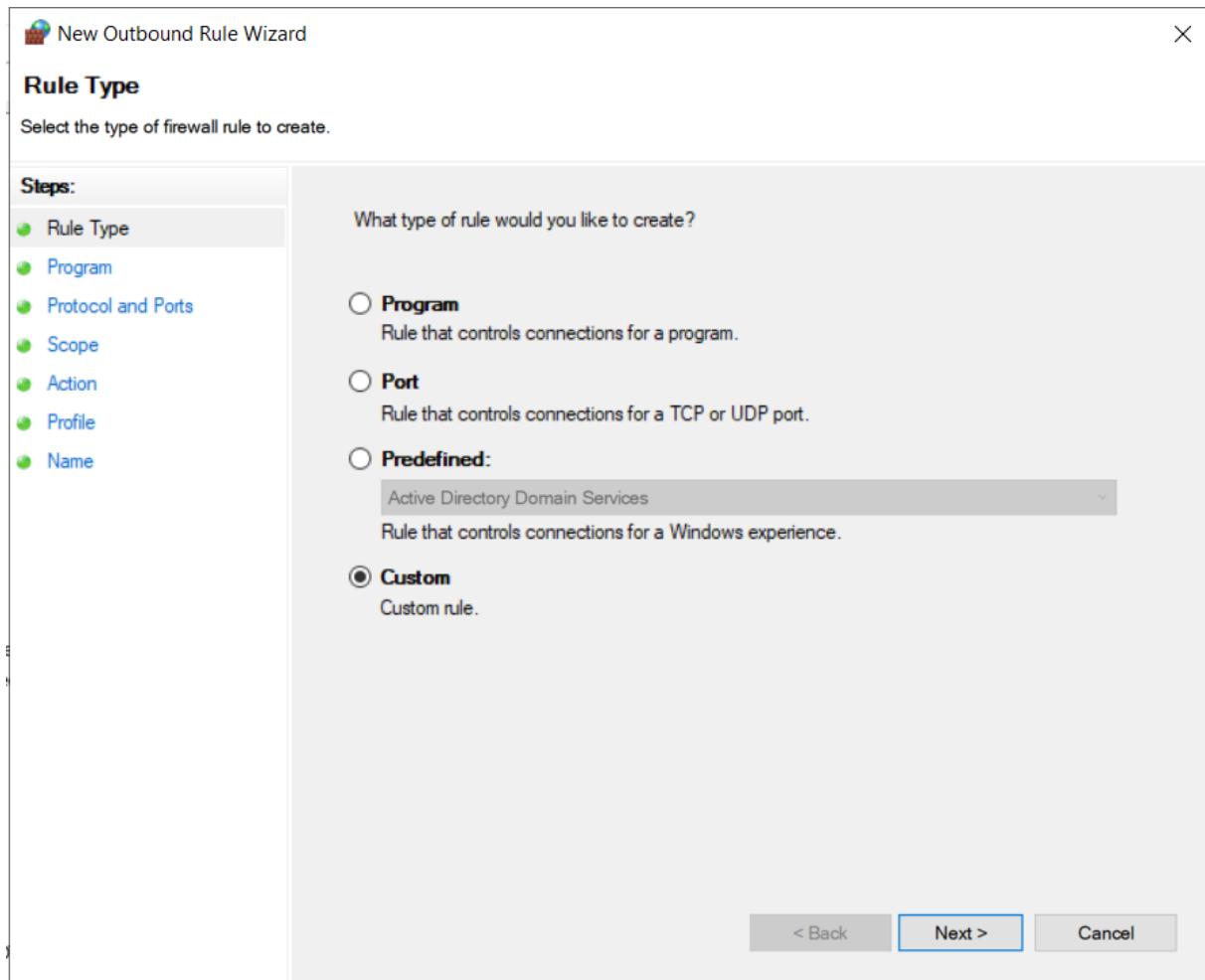
Để tùy chỉnh GPO đã tạo ta nhấn chuột vào GPO “Kích ban 5” rồi chọn **Edit...** để mở **Group Policy Management Editor**



Hình 100: Group Policy Management Editor

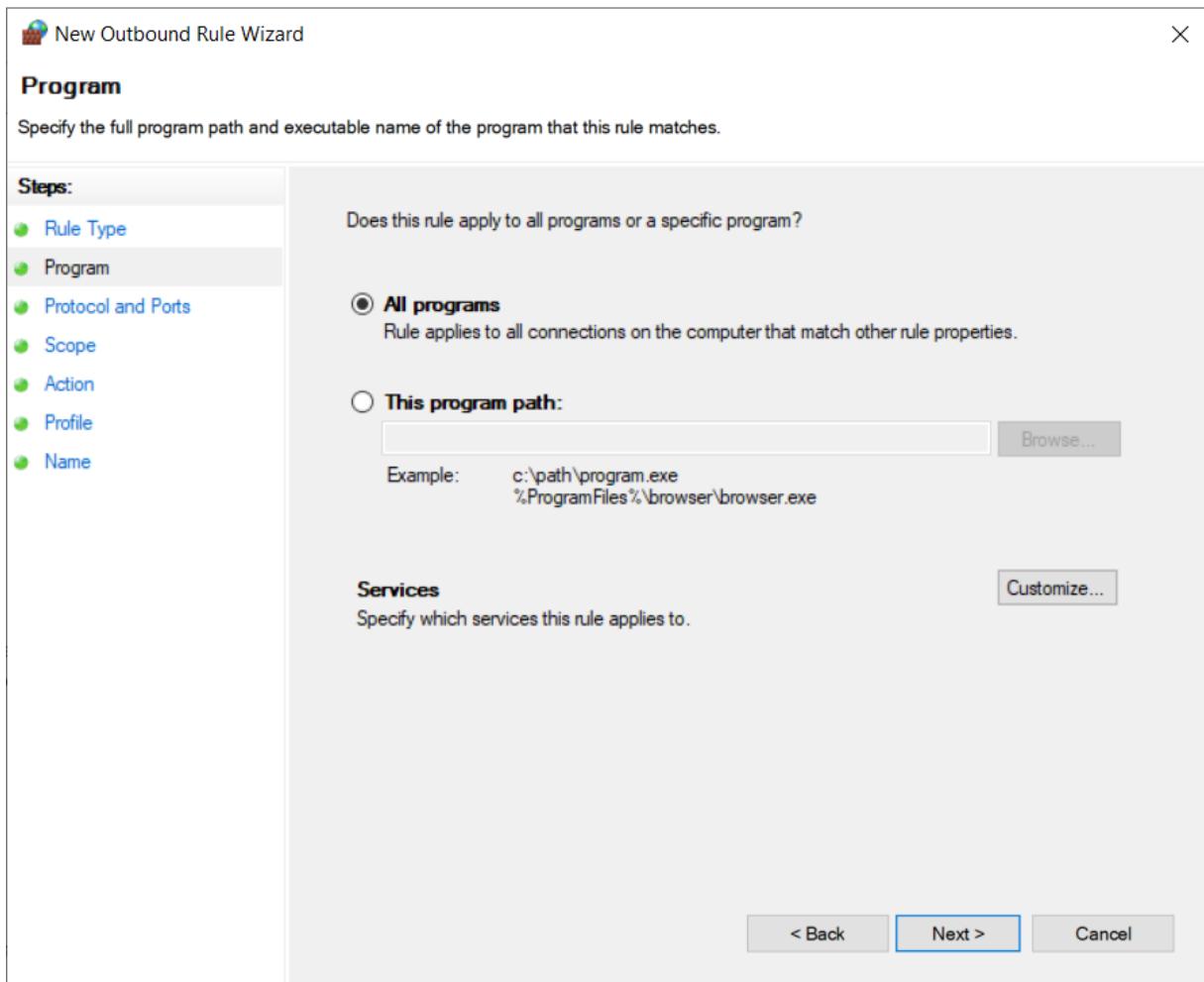
Trong cửa sổ **Group Policy Management Editor**, điều hướng đến:

**Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall with Advanced Security > Windows Defender Firewall with Advanced Security > Outbound Rules > New Rule**



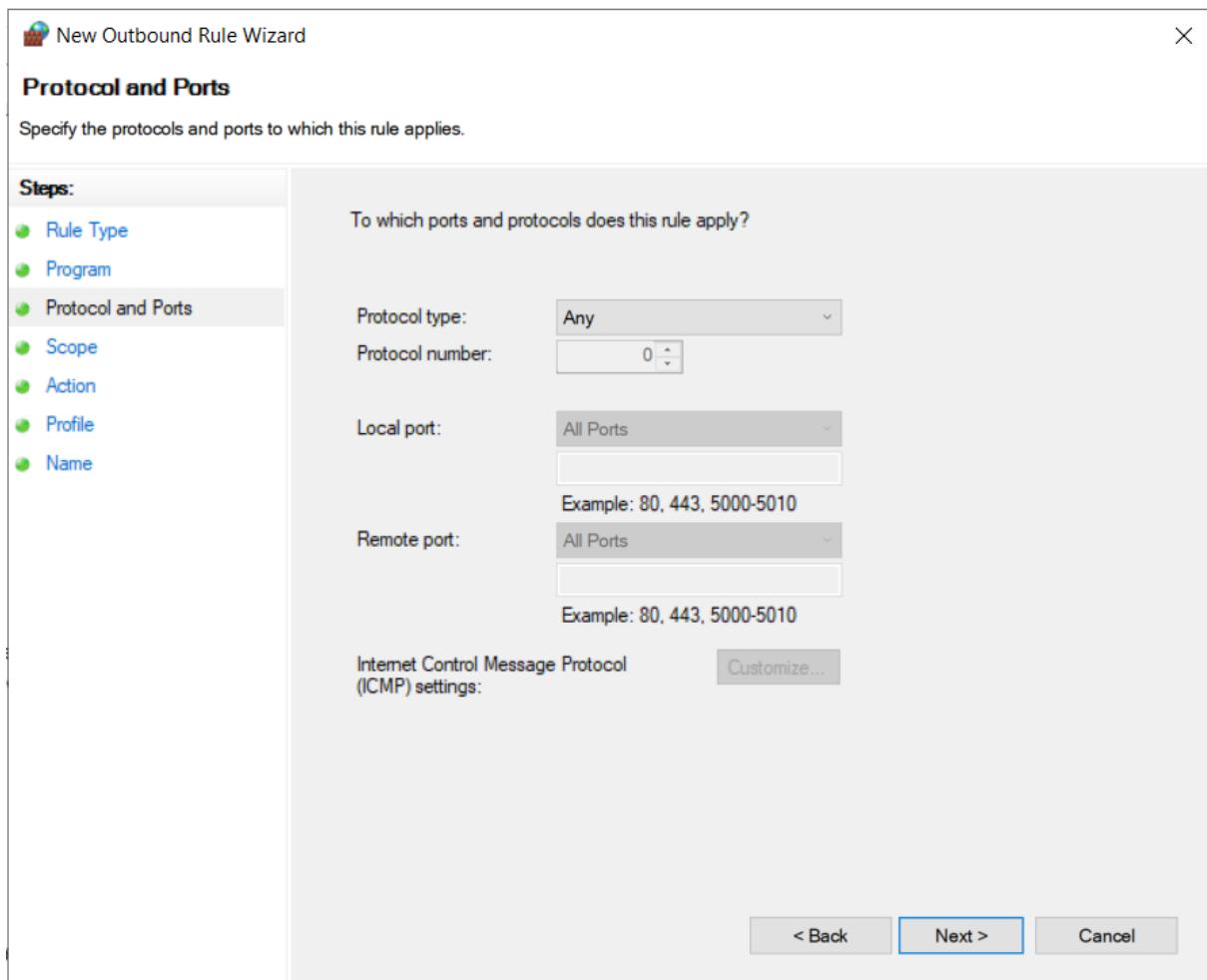
Hình 101: Tại Rule Type chọn Custom

## Tại Program > All Programs



Hình 102: Program > All Programs

## Tại Protocol and Ports > Any

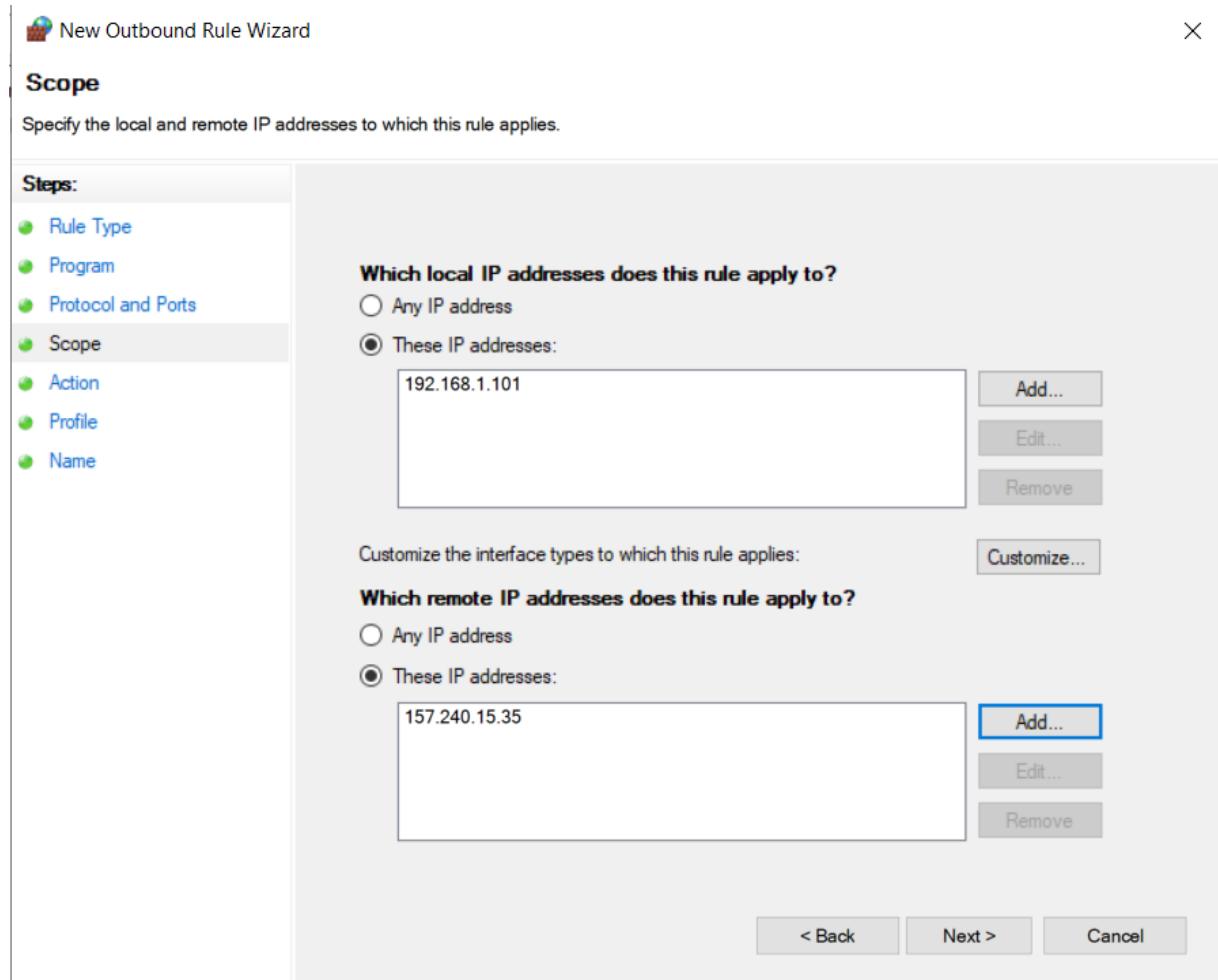


Hình 103: Protocol and Ports > Any

## Tại Scope

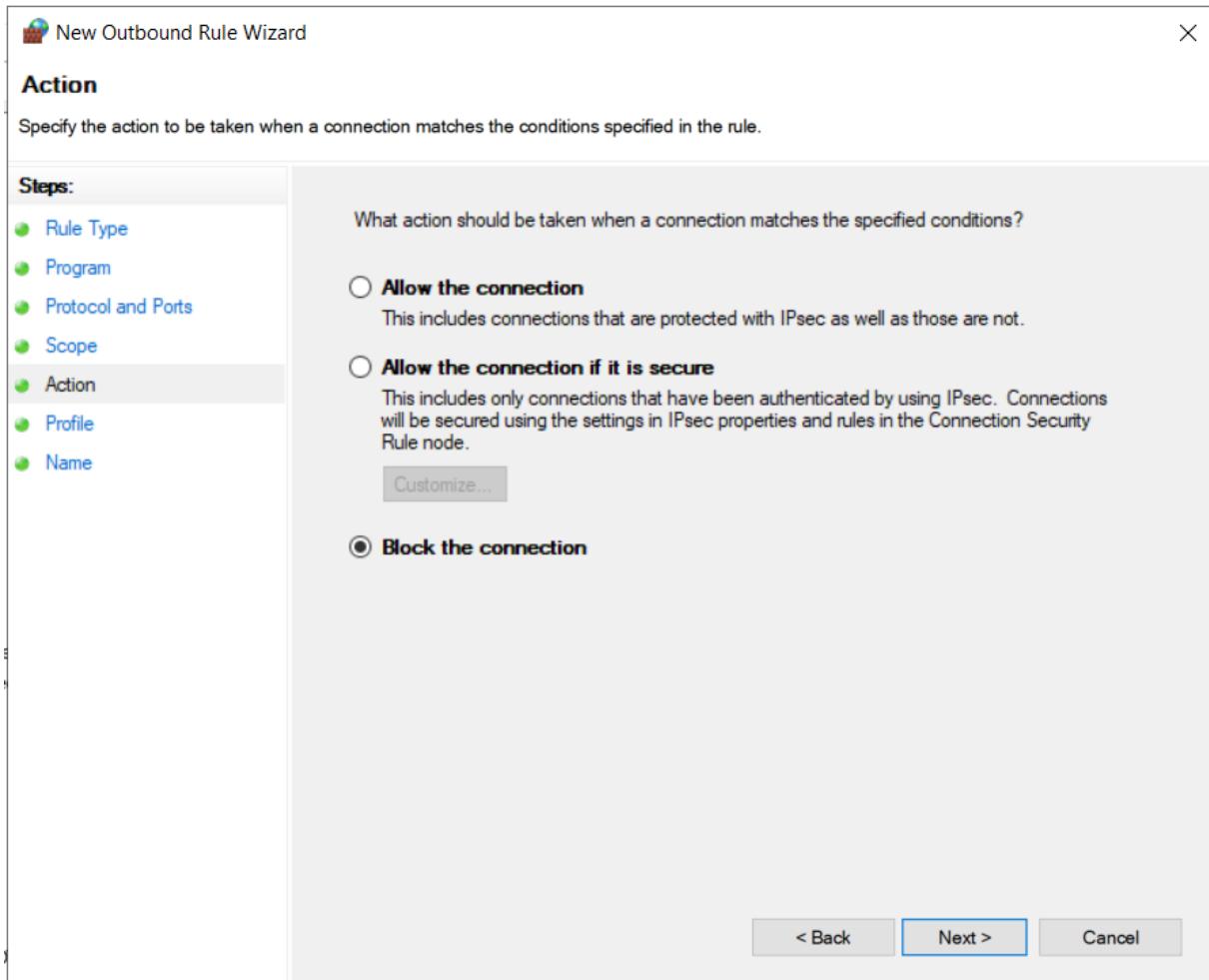
Which Local IP addresses does this rule apply to? Chọn These IP addresses và add ip của máy muốn chặn.

Which remote IP addresses does this rule apply to? Chọn These IP addresses và add ip của trang web muốn chặn.(ở đây là ip của facebook)



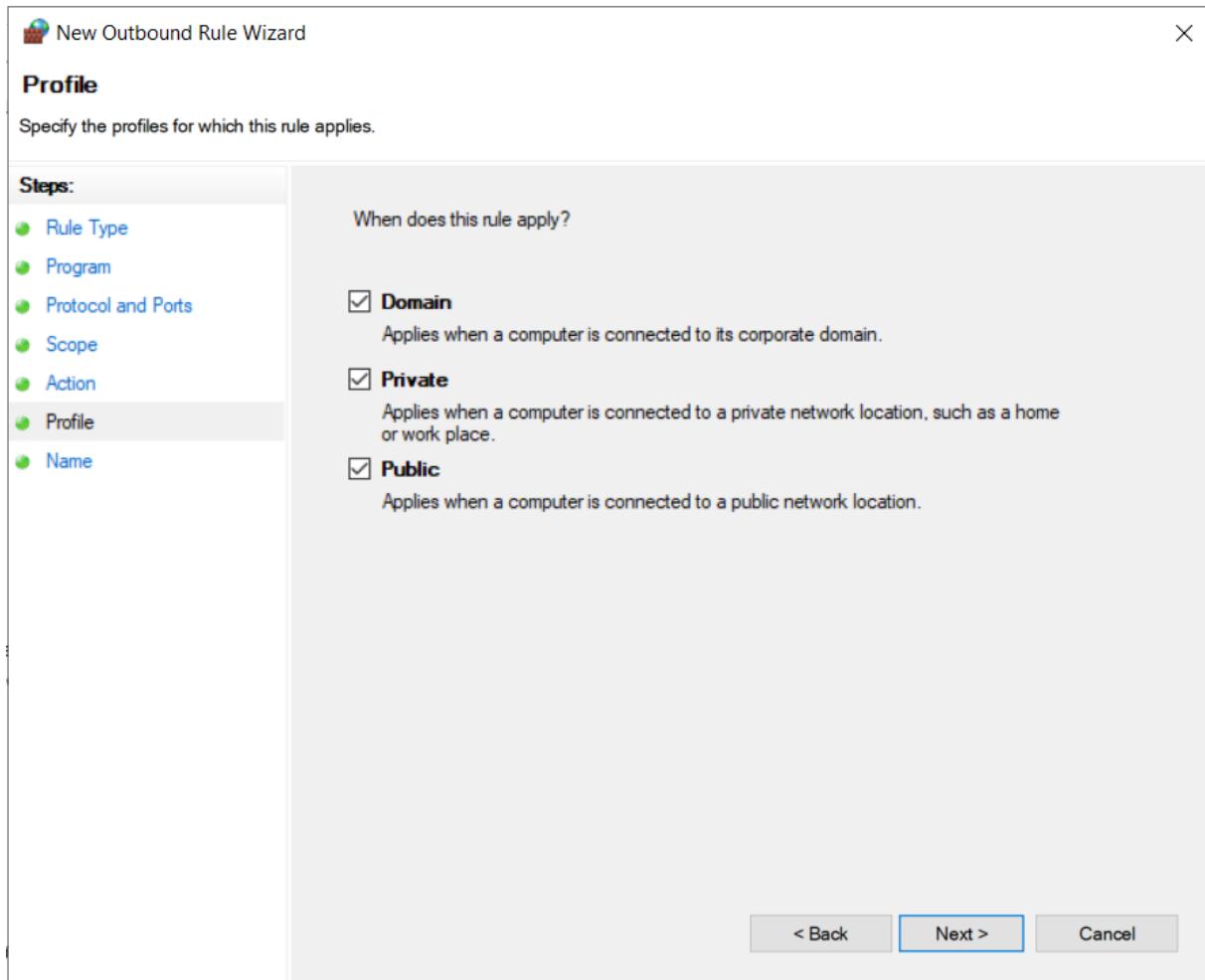
Hình 104: Cài đặt IP

## Tại Action > Block the connection



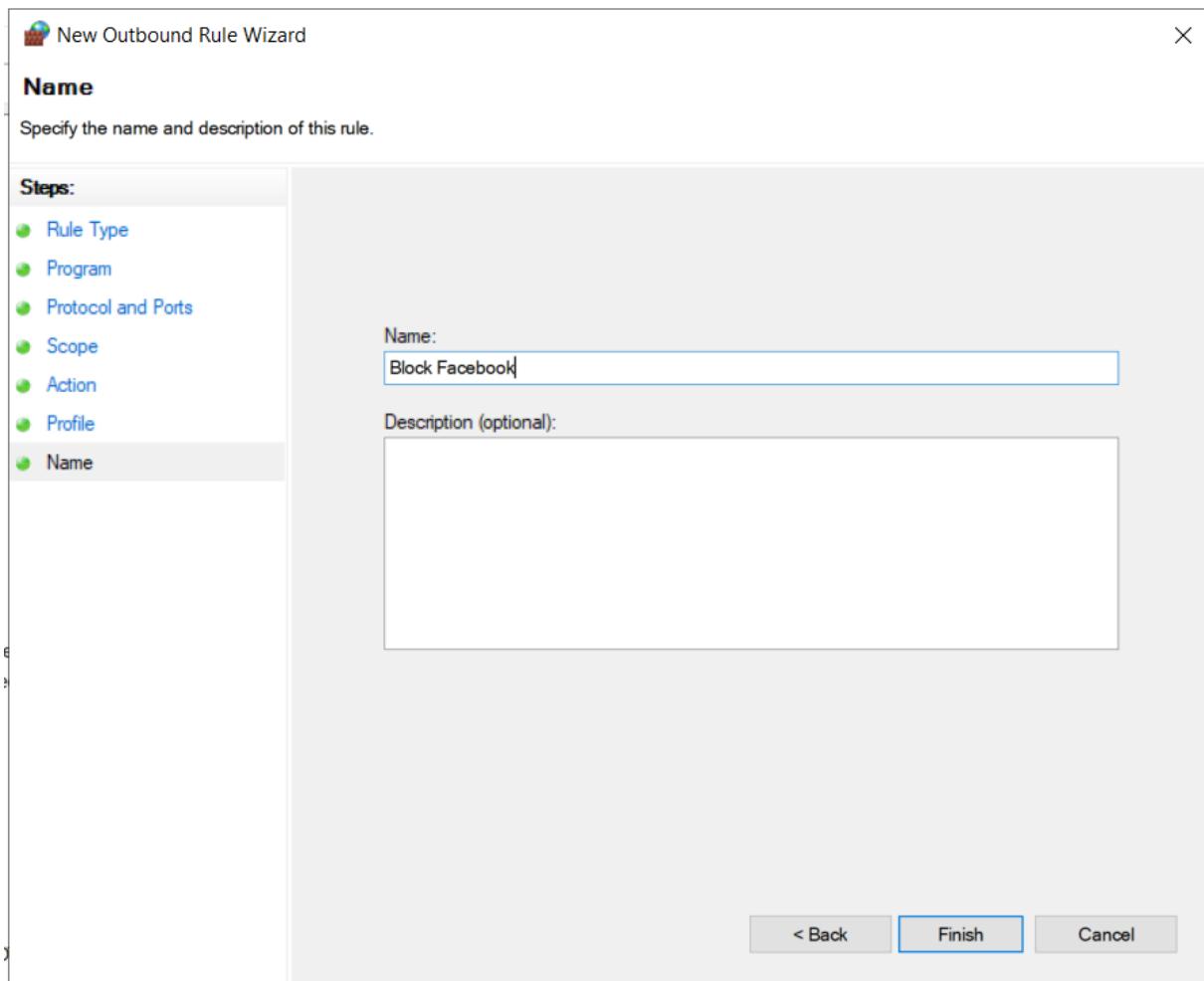
Hình 105: Chặn kết nối

## Tại Profile chọn hết



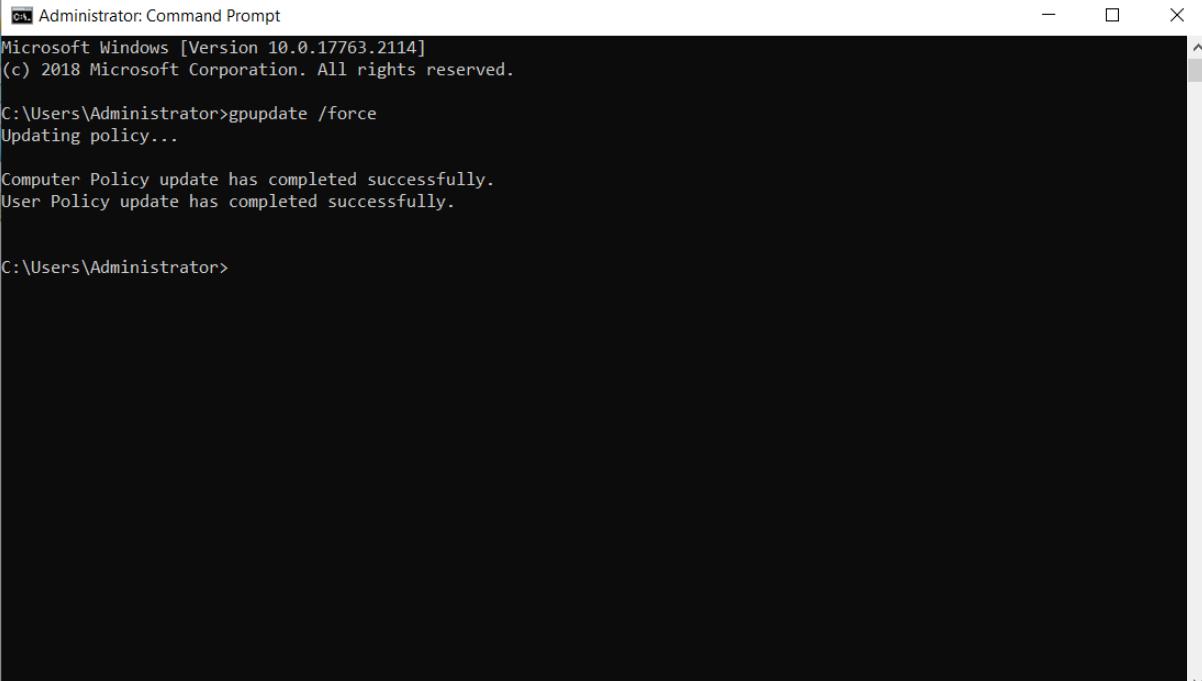
Hình 106: Áp dụng rule

## Tại Name điền tên rule "Block Facebook"



Hình 107: Đặt tên

**Vào máy Server và Client1 mở cmd với quyền administrator rồi chạy lệnh gpupdate /force**



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.2114]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>gpupdate /force
Updating policy...

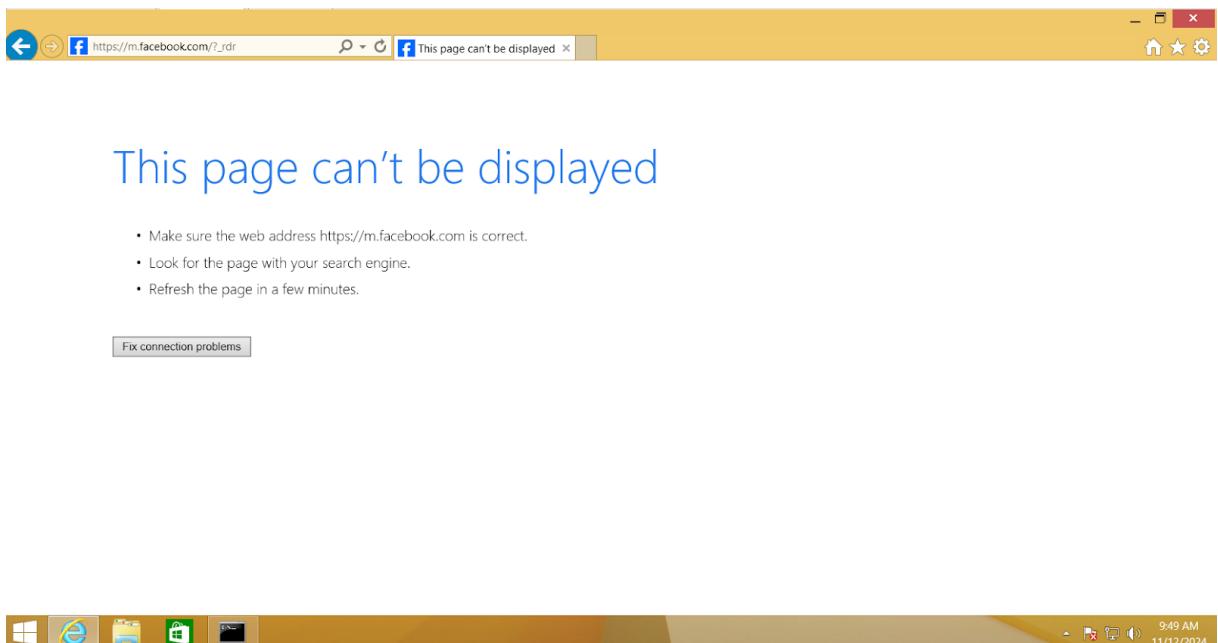
Computer Policy update has completed successfully.
User Policy update has completed successfully.

C:\Users\Administrator>

```

Hình 108: gpupdate /force

**Kiểm tra: Thử vào facebook thì không được**

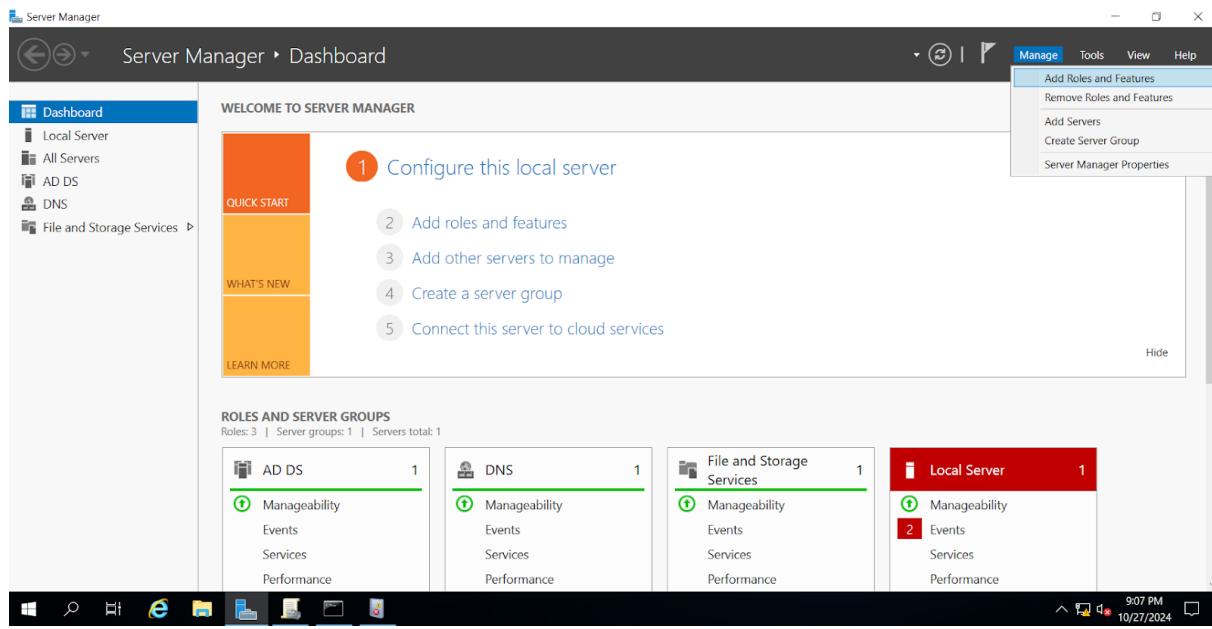


Hình 109: Facebook đã bị chặn

### 3.6 Kịch bản 6: Cấu hình phòng chống DDoS và giám sát IP truy cập vào Web Server

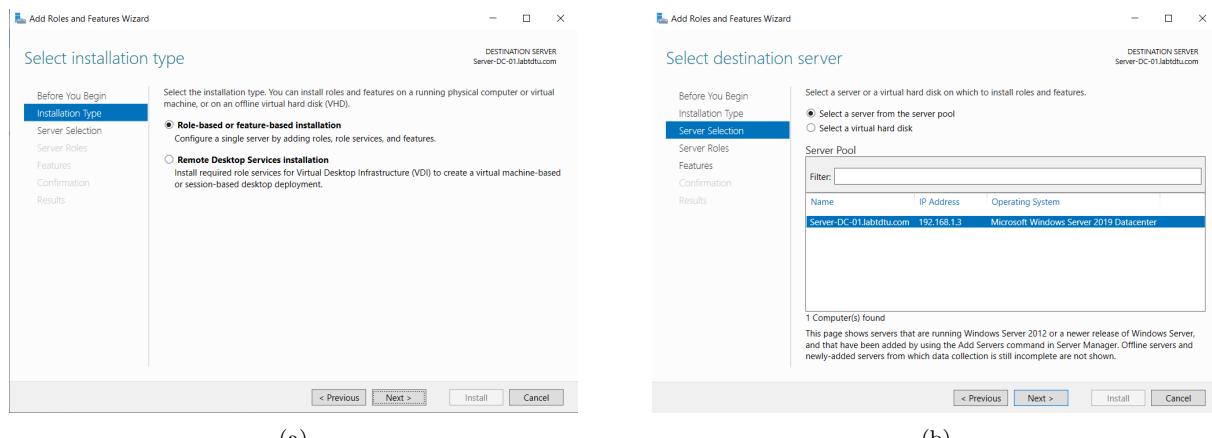
#### 1. Cài đặt dịch vụ Web Server IIS

- Vào Server Manager > Dashboard chọn Manager > Add Role and Features



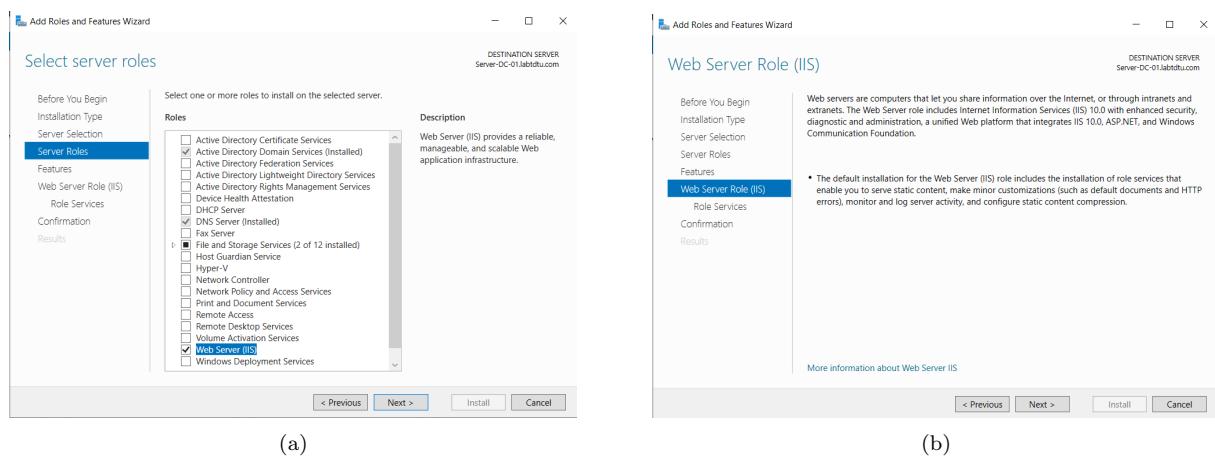
Hình 110: Server Manager

- Chọn Next



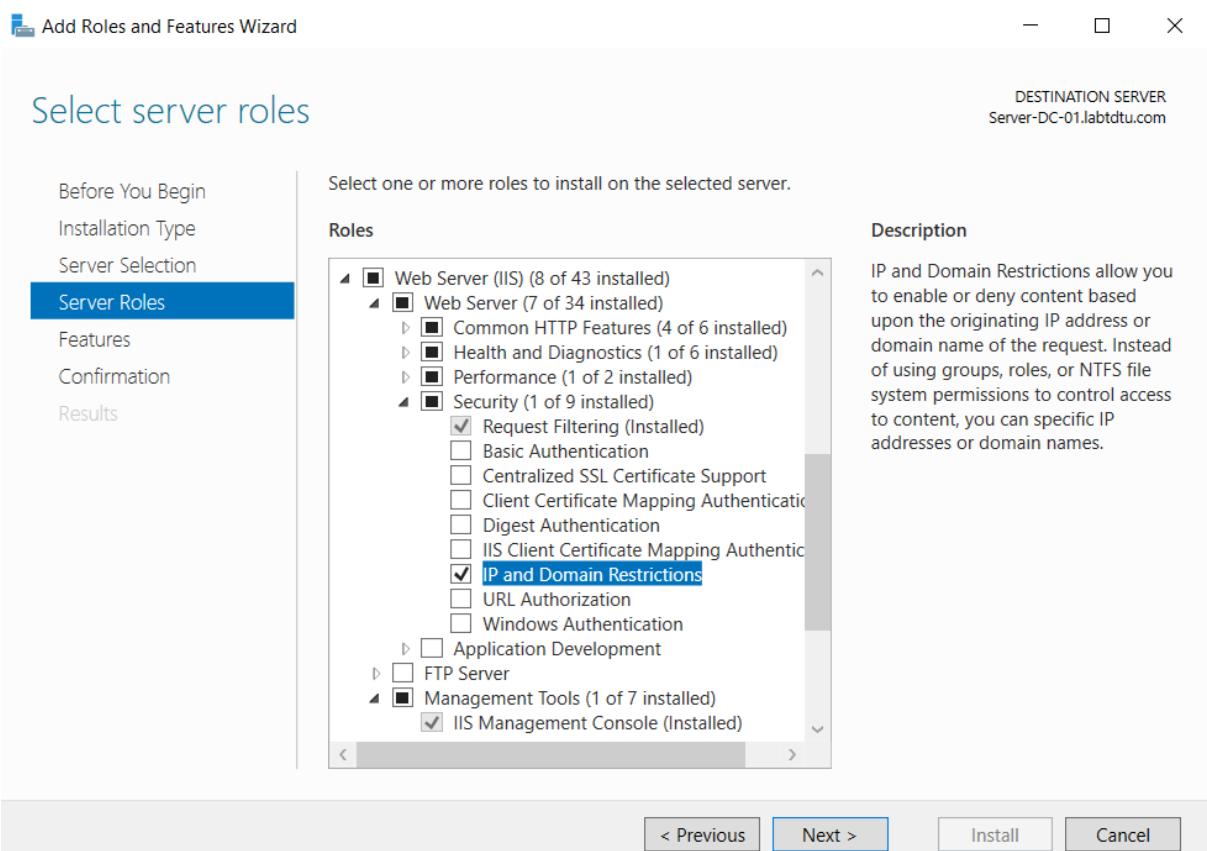
Hình 111: Cài đặt Web Server IIS

- Chọn Web Server (IIS) > Next Chọn Web Server (IIS) > Next



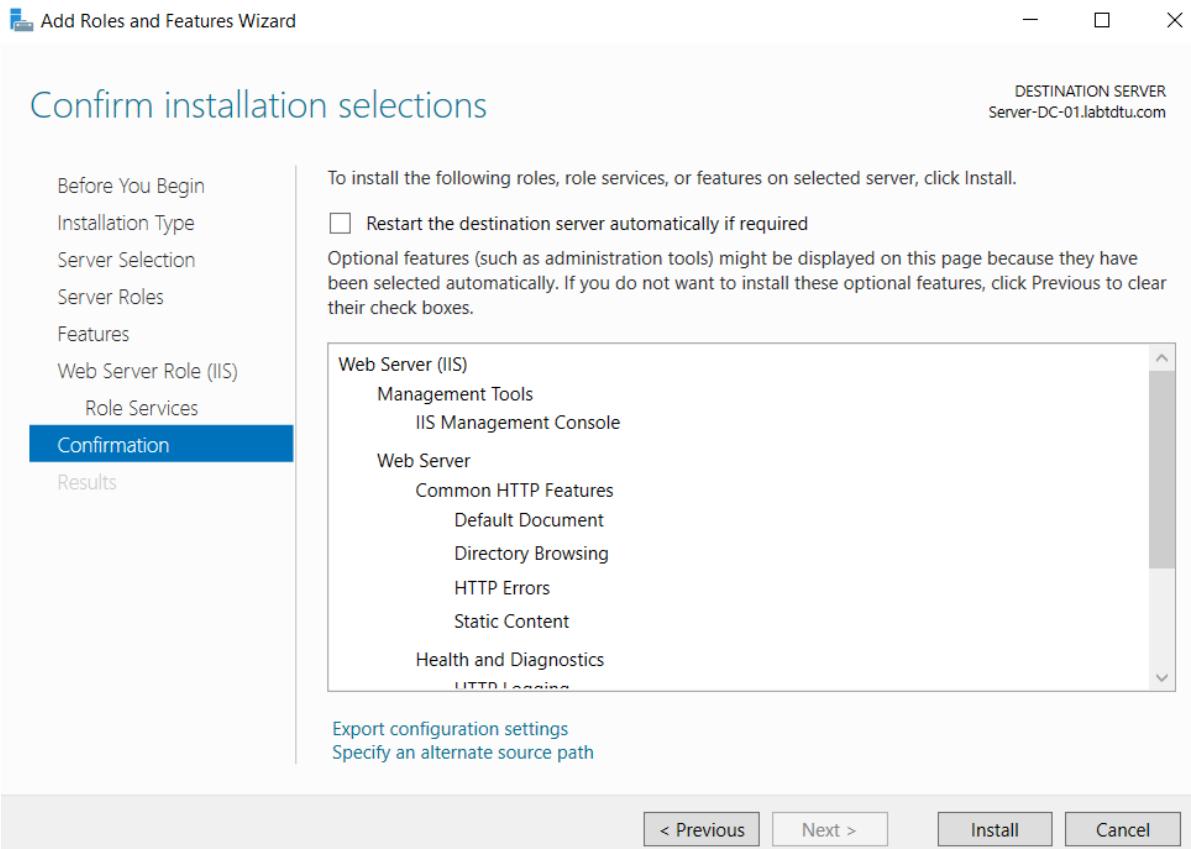
Hình 112: Tiếp tục cài đặt Web Server IIS

- Tại **Server Roles** Diều hướng **Web Server (IIS)** > **Web Server** > **Security**
- Tích chọn **IP and Domain Restrictions**



Hình 113: IP and Domain Restrictions

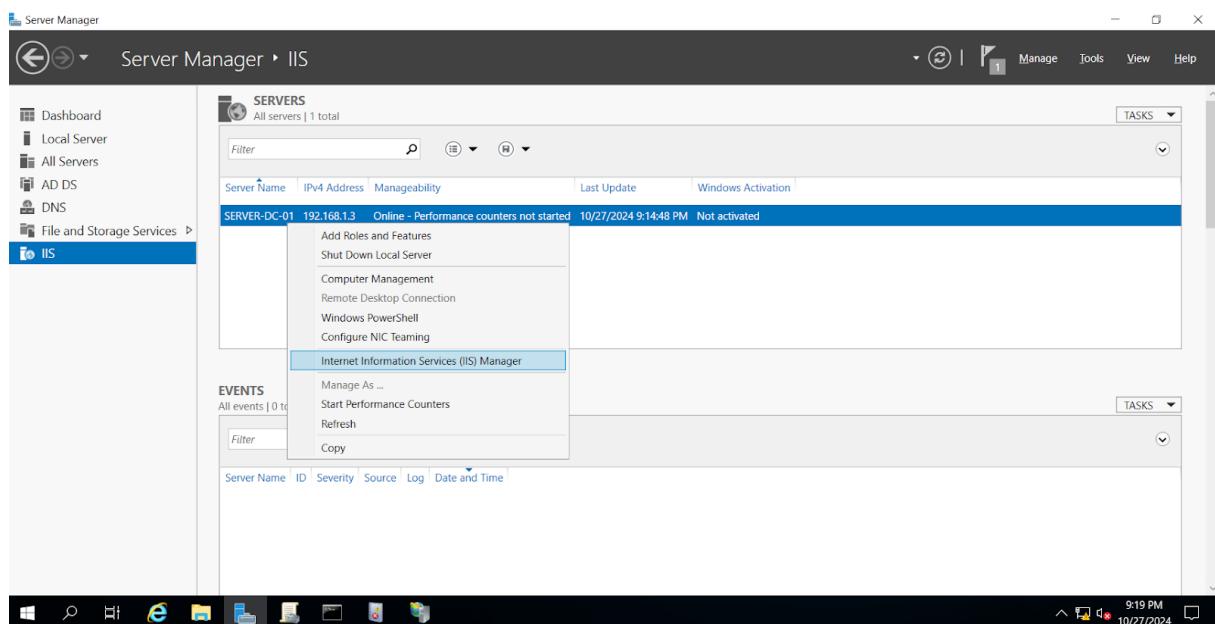
## ● Chọn Install



Hình 114: Cài đặt

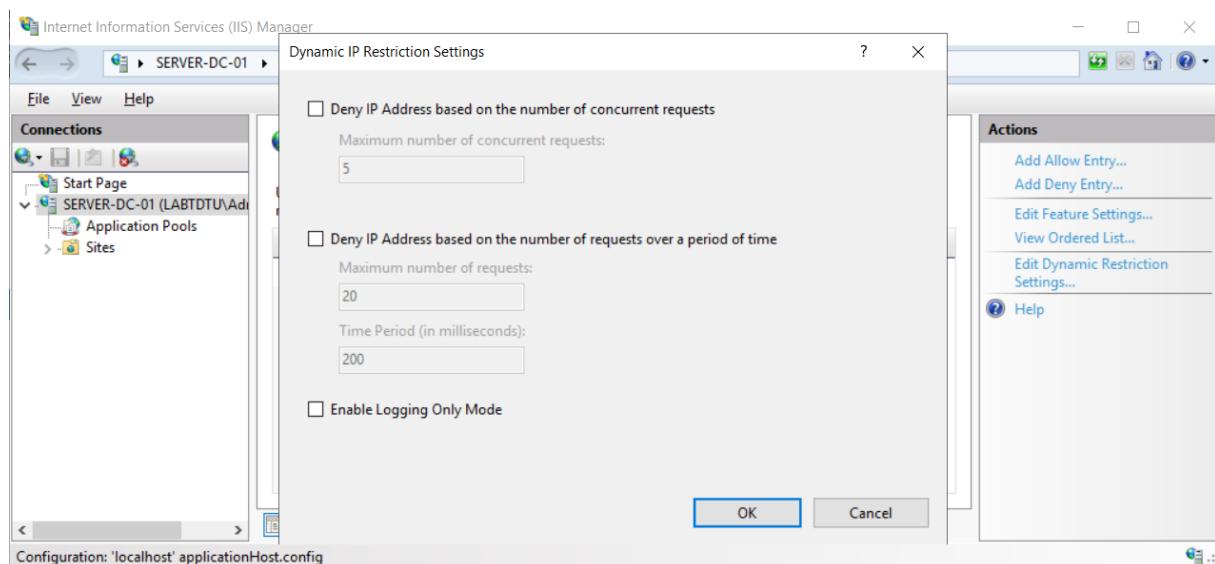
## 2. Cấu hình Web Server IIS

- Vào **Server Manager > IIS** rồi nhấp chuột phải vào **Server-DC-01** chọn **Internet Information Services (IIS) Manager**



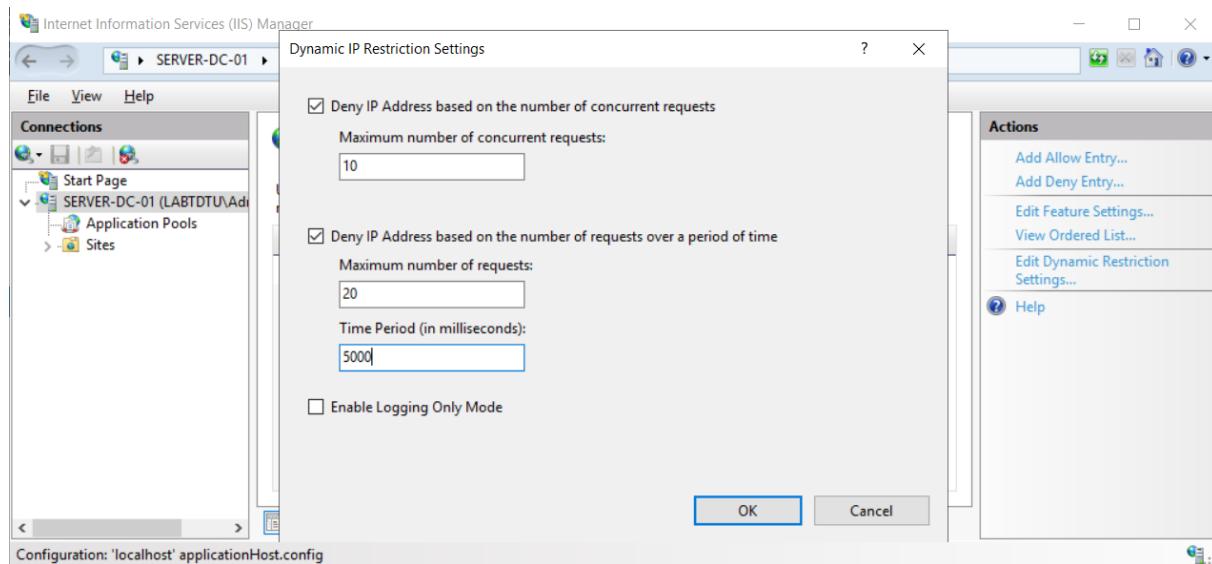
Hình 115: Internet Information Services (IIS) Manager

- Chọn **SERVER-DC-01 > IP Address and Domain Restriction > Edit Dynamic Restriction Setting**



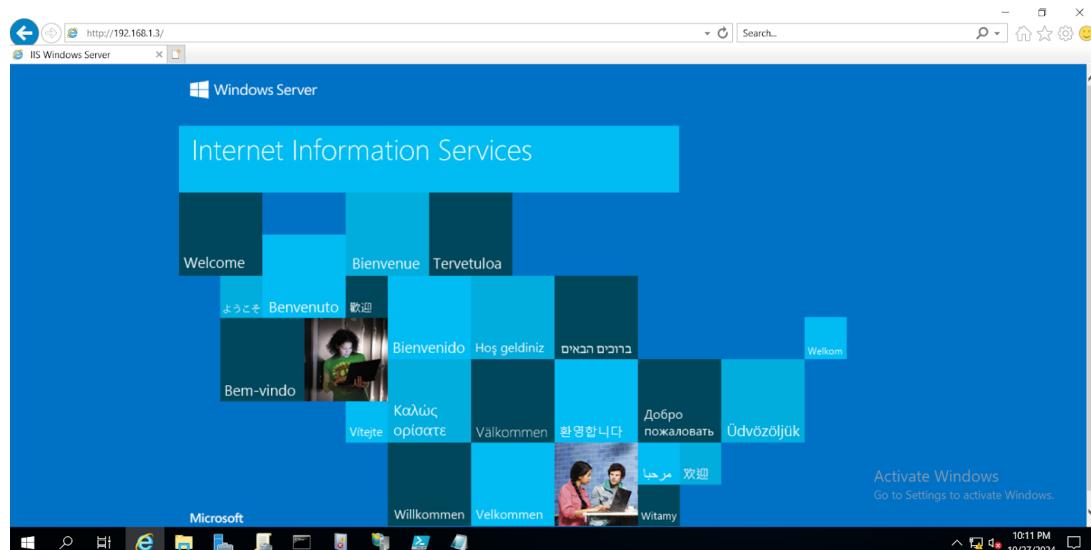
Hình 116: Vào Edit Dynamic Restriction Setting

- Deny IP Address Based on the Number of Concurrent Requests:** Tùy chọn này cho phép chặn các IP gửi quá nhiều yêu cầu cùng một lúc.
- Deny IP Address Based on the Number of Requests Over a Period of Time:** Chặn các IP gửi quá nhiều yêu cầu trong một khoảng thời gian ngắn.



Hình 117: Cấu hình Dynamic Restriction

- Để kiểm tra xem cấu hình thành công chưa thì vào trình duyệt tìm kiếm địa chỉ IP của Web vừa tạo.



Hình 118: Kiểm tra P của Web vừa tạo

- Để kiểm tra xem cấu hình chống DDoS thì vào Powershell chạy lệnh

```
while ($true) {
```

```
try {
```

```
Invoke-WebRequest -Uri "http://192.168.1.3" -TimeoutSec 3 -  
ErrorAction Stop
```

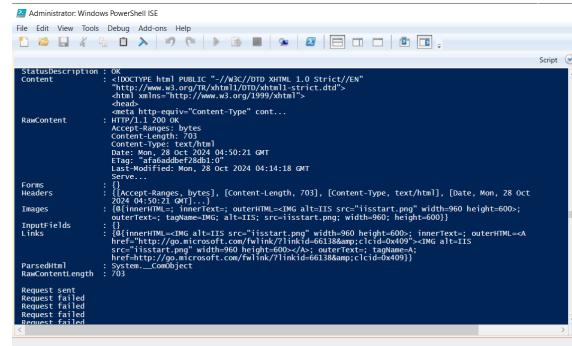
```
Write-Host "Request sent"
```

}

```
catch {Write-Host "Request failed"}
```

}

- Ta sẽ thấy Request sent được 20 lần rồi Request failed là đã cấu hình thành công.



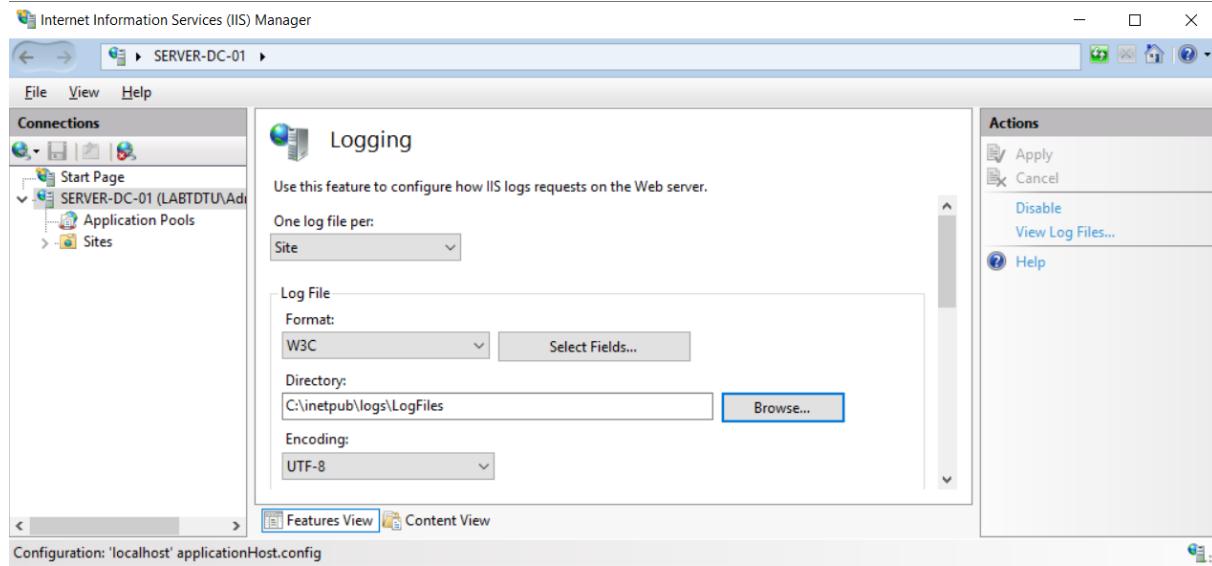
(a)

(b)

Hình 119: Request Failed

### 3. Quan sát những IP truy cập vào Web

- Vào Internet Information Services (IIS) Manager chọn SERVER-DC-01 > Logging



Hình 120: Nhấn **Browse** để chọn nơi lưu trữ file thông tin. Rồi chọn **Apply**

- Mở File vừa lưu

```
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-10-28 04:33:32
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-s
2024-10-28 04:33:32 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT+10.0;+WOW64;+Trident/7.0;+rv:11.0)+like+Gecko
2024-10-28 04:33:32 192.168.1.3 GET /iisstart.png - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT+10.0;+WOW64;+Trident/7.0;+rv:11.0;+MSIE+11.0)
2024-10-28 04:33:32 192.168.1.3 GET /favicon.ico - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT+10.0;+WOW64;+Trident/7.0;+rv:11.0;+MSIE+11.0)
#Software: Microsoft Internet Information Services 10.0
#Version: 1.0
#Date: 2024-10-28 04:50:19
#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-username c-ip cs(User-Agent) cs(Referer) sc-status sc-s
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:19 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:20 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
2024-10-28 04:50:20 192.168.1.3 GET / - 80 - 192.168.1.3 Mozilla/5.0+(Windows+NT;+Windows+NT+10.0;+en-US)+WindowsPowerShell/
```

Hình 121: Lịch sử các IP đã truy cập vào web

## TÀI LIỆU THAM KHẢO

1. "Fix Can't Create Tasks to Display Messages in Windows 8 Task Scheduler"  
<https://www.askvg.com/fix-cant-create-tasks-to-display-messages-in-windows-8-task-scheduler/>.

2. "How to Fix Windows Task Scheduler Display Message Option Not Available"  
<https://www.youtube.com/watch?v=EHnAihz3lo&t=552s>.

3. "Windows Task Scheduler Tutorial"  
<https://www.youtube.com/watch?v=pqJCnvQ3Aw0&t=128s>.

4. "Task Scheduler in Windows - Automate Your Tasks"  
<https://www.youtube.com/watch?v=0Hu0bJLfb7U>.