BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC

THÀNH PHỐ HỒ CHÍ MINH

ĐỀ TÀI MÔN

QUẢN TRỊ MẠNG

SV: Nguyễn Công Khang - 21DH110770

SV: Phạm Đức Thiên Phúc - 21DH112813

SV: Nguyễn Minh Đức – 21DH113591

GVGD: Th.S Đinh Xuân Lâm

Lời cảm ơn

Trong thời gian học tập dưới mái trường Đại Học Ngoại Ngữ Tin Học Thành Phố Hồ Chí Minh, được sự truyền đạt kiến thức và giúp đỡ tận tình của quý Thầy Cô Giảng viên là hành trang quý báo cho sự nhận thức và hiểu biết của em ngày hôm nay. Em xin ghi nhận nơi này lỏng biết ơn chân thành nhất đối với tất cả các Thầy Cô Giảng viên và đặc biệt là thạc sĩ ***Đinh Xuân Lâm****, giảng viên chuyên ngành Quản trị mạng, người thầy đã tận tình hướng dẫn em hoàn thành bải báo cáo tốt nghiệp này. Do kiến thức còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ cũng chưa hoàn hảo nên bởi báo cáo sẽ còn nhiều thiếu sót, kinh mong sự góp ý và giúp đỡ từ Quý Thầy cô. Một lần nữa, em xin chân thành cảm ơn!*

Lý do chọn đề tài

Việc chọn đề tài về bảo mật Windows Server 2019 là một quyết định có lý do, và có thể có nhiều lợi ích từ việc nghiên cứu về lĩnh vực này. Dưới đây là một số lý do mà nhóm em đã chọn đề tài này:

- **Phổ biến sử dụng:** Windows Server 2019 là một trong những hệ điều hành server phổ biến và được sử dụng rộng rãi. Do đó, nghiên cứu về bảo mật trên nền tảng này có thể mang lại giá trị lớn, đặc biệt là khi nhiều doanh nghiệp và tổ chức sử dụng nó để triển khai ứng dụng và dịch vụ.

- **Thách thức bảo mật:** Bảo mật là một vấn đề quan trọng, và Windows Server 2019 không nằm ngoài tầm ngắm của các hacker và kẻ xâm phạm. Nghiên cứu về bảo mật trên nền tảng này có thể giúp hiểu rõ hơn về các thách thức đặt ra và phát triển các giải pháp để bảo vệ hệ thống.

- **Kỹ thuật tiên tiến:** Windows Server 2019 mang lại nhiều tính năng và công nghệ tiên tiến trong lĩnh vực bảo mật. Nghiên cứu về cách các tính năng như IPSec, Group Policy Object và BitLocker có thể được triển khai và cấu hình để tăng cường bảo mật hệ thống là một lĩnh vực hứa hẹn.

- **Chấp nhận thách thức mới:** Bảo mật là một lĩnh vực đang phát triển liên tục, và Windows Server 2019 không ngừng cập nhật để đối mặt với những thách thức mới. Nghiên cứu về cách nền tảng này đang đối mặt

với các vấn đề an ninh mới có thể đưa ra thông báo cho cộng đồng bảo mật và doanh nghiệp về cách phát triển chiến lược bảo mật hiệu quả.

Chương 1: Tổng quan về đề tài

I. Mục tiêu đề tài

Để đảm bảo an toàn và ổn định cho hệ thống máy chủ Windows Server 2019, việc triển khai các giải pháp bảo mật là hết sức quan trọng. Mục tiêu chính của đề tài này là tìm kiếm và áp dụng các giải pháp hiệu quả để bảo vệ hệ thống trước các mối đe dọa mạng và tăng cường khả năng chống lại các cuộc tấn công.

Một trong những mục tiêu hàng đầu là nâng cao cơ sở hạ tầng bảo mật của Windows Server 2019. Điều này bao gồm việc cài đặt và cấu hình các tường lửa mạng, kiểm soát quyền truy cập, và quản lý chính sách bảo mật để ngăn chặn việc xâm nhập từ các nguồn đáng ngờ. Đồng thời, việc thực hiện các bản vá và cập nhật hệ thống định kỳ cũng là một phần quan trọng để giảm thiểu lỗ hổng bảo mật có thể bị tận dụng bởi những kẻ xâm nhập.

Mục tiêu khác là tối ưu hóa quản lý danh tính và quản lý người dùng. Bằng cách này, hệ thống có thể nhận diện và kiểm soát quyền truy cập của người dùng đến tài nguyên hệ thống, giảm thiểu rủi ro từ những hành động không đúng đắn. Việc triển khai các biện pháp như Multi-Factor Authentication (MFA) cũng có thể được xem xét để cung cấp một lớp bảo mật bổ sung.

Ngoài ra, một phần quan trọng của mục tiêu này là tăng cường khả năng giám sát và phản ứng. Việc triển khai các công cụ theo dõi sự kiện và hệ thống như Windows Event Log, Security Information and Event Management (SIEM) giúp phát hiện sớm các hoạt động bất thường và đưa ra các biện pháp ngăn chặn kịp thời.

Tổng cộng, việc đạt được những mục tiêu này sẽ cung cấp một mức độ bảo mật cao cho hệ thống Windows Server 2019, giúp bảo vệ dữ liệu quan trọng và duy trì sự ổn định của môi trường kinh doanh.

II. Đối tượng và phạm vi

- **Đối tượng:**

- **Quản trị viên hệ thống:** Những người chịu trách nhiệm về quản lý và bảo mật hệ thống Windows Server 2019. Đối tượng này cần hiểu rõ về cấu trúc hệ thống và có khả năng triển khai, cấu hình, và duy trì các giải pháp bảo mật.
- **Nhân viên IT:** Các nhân viên thực hiện các nhiệm vụ cụ thể liên quan đến bảo mật, như cài đặt và cấu hình tường lửa, quản lý quyền truy cập, và thực hiện các biện pháp bảo mật hàng ngày.
- **Người quản lý dự án:** Những người quản lý chịu trách nhiệm về việc đảm bảo rằng dự án triển khai giải pháp bảo mật cho Windows Server 2019 được thực hiện đúng thời hạn, kinh phí, và đạt được các mục tiêu đã đề ra.

- **Phạm vi:**

- **Triển khai tường lửa mạng:** Cài đặt và cấu hình tường lửa để kiểm soát lưu lượng mạng đến và đi từ hệ thống. Phạm vi cũng bao gồm việc thiết lập các quy tắc tường lửa để ngăn chặn các truy cập không ủy quyền.
- **Quản lý danh tính và quyền truy cập:** Bao gồm việc cài đặt và quản lý danh tính người dùng, xác thực người dùng, và kiểm soát quyền truy cập vào tài nguyên hệ thống.
- **Cập nhật và bảo trì hệ thống:** Áp dụng các bản vá và cập nhật hệ thống định kỳ để giảm thiểu lỗ hổng bảo mật. Bảo trì các chính sách bảo mật và theo dõi sự kiện hệ thống.
- **Giám sát và phản ứng:** Triển khai công cụ giám sát sự kiện và hệ thống để theo dõi các hoạt động bất thường và phản ứng nhanh chóng khi phát hiện sự cố bảo mật.

- **Đào tạo người dùng cuối:** Thực hiện các biện pháp đào tạo để nâng cao nhận thức về bảo mật cho người sử dụng cuối, giúp họ tránh những hành động có thể tạo ra rủi ro bảo mật.

III. Ý nghĩa

Ý nghĩa của Đề Tài Bảo Mật Windows Server 2019:

- **Bảo vệ Tài Nguyên Hệ Thống:**

Đề tài này mang lại ý nghĩa lớn trong việc bảo vệ tài nguyên hệ thống trên nền tảng Windows Server 2019 khỏi những mối đe dọa mạng và tấn công từ phía ngoại vi. Qua đó, nó giúp đảm bảo tính an toàn và ổn định của các dữ liệu quan trọng, ứng dụng, và các chức năng kinh doanh khác.

- **Tăng Cường Khả Năng Chống Lại Cuộc Tấn Công:**

Trong bối cảnh môi trường kỹ thuật số ngày càng phức tạp, đề tài này đóng vai trò quan trọng trong việc nâng cao khả năng chống lại các cuộc tấn công từ các mối đe dọa ngày càng tiên tiến. Các giải pháp bảo mật được triển khai từ đề tài này giúp làm giảm thiểu rủi ro và tăng cường sức mạnh bảo mật của hệ thống.

- **Quản lý Danh Tính và Quyền Truy Cập Hiệu Quả:**

Đối với doanh nghiệp, quản lý danh tính và quyền truy cập là yếu tố cực kỳ quan trọng. Đề tài giúp tối ưu hóa quá trình này, đảm bảo rằng người dùng chỉ có quyền truy cập vào những tài nguyên mà họ cần, giảm thiểu rủi ro từ việc sử dụng không đúng đắn.

- **Đảm Bảo Tuân Thủ và Bảo Mật Hợp Pháp:**

Đối với các tổ chức, việc tuân thủ các quy định và luật lệ về bảo mật thông tin là thiết yếu. Đề tài này không chỉ giúp bảo vệ dữ liệu mà còn đảm bảo rằng hệ thống tuân thủ các quy định pháp luật liên quan đến bảo mật thông tin.

- **Nâng Cao Năng Lực Quản lý Sự Cố:**

Bằng cách triển khai các công cụ giám sát và phản ứng, đề tài giúp nâng cao khả năng quản lý sự cố. Việc phát hiện và xử lý sự cố một cách nhanh chóng giúp giảm thiểu thiệt hại và duy trì tính ổn định của hệ thống.

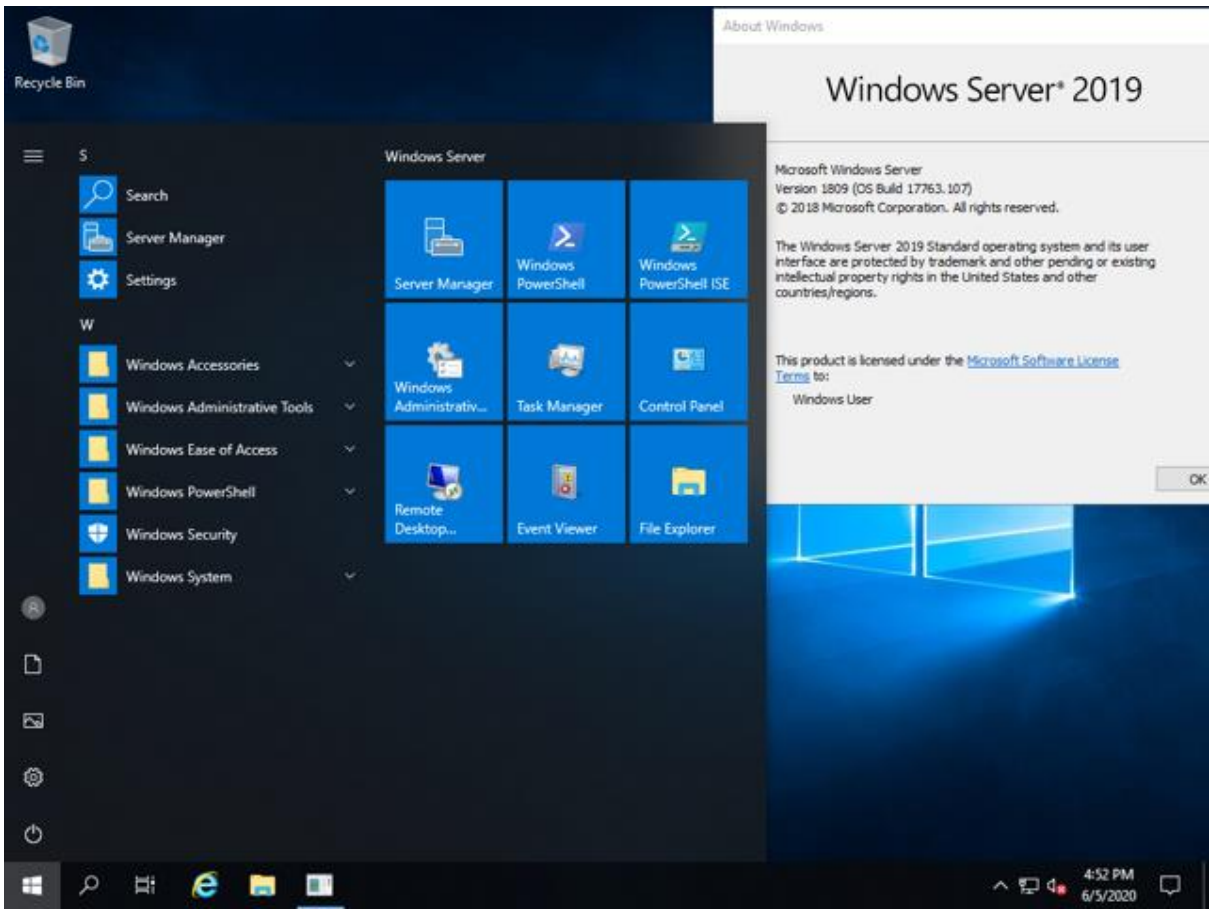
- **Chia Sẻ Kiến Thức và Nâng Cao Năng Lực Cộng Đồng Chuyên Gia:**

Kết quả từ đề tài có thể được chia sẻ với cộng đồng chuyên gia và người quan tâm đến lĩnh vực bảo mật. Điều này đóng góp vào việc nâng cao kiến thức chung và khả năng đối phó với những mối đe dọa mạng hiện đại.

Chương 2: Lý thuyết tổng quan

I. Giới thiệu về hệ điều hành Windows Server 2019

Windows Server 2019 là một hệ điều hành server phổ biến của Microsoft, được thiết kế để cung cấp các dịch vụ, ứng dụng, và giải pháp cho môi trường doanh nghiệp và tổ chức. Đó là hệ điều hành nối tiếp Windows Server 2016, nó được giới thiệu vào ngày 20 tháng 3 năm 2018 và chính thức ra mắt vào ngày 2 tháng 10 năm 2018



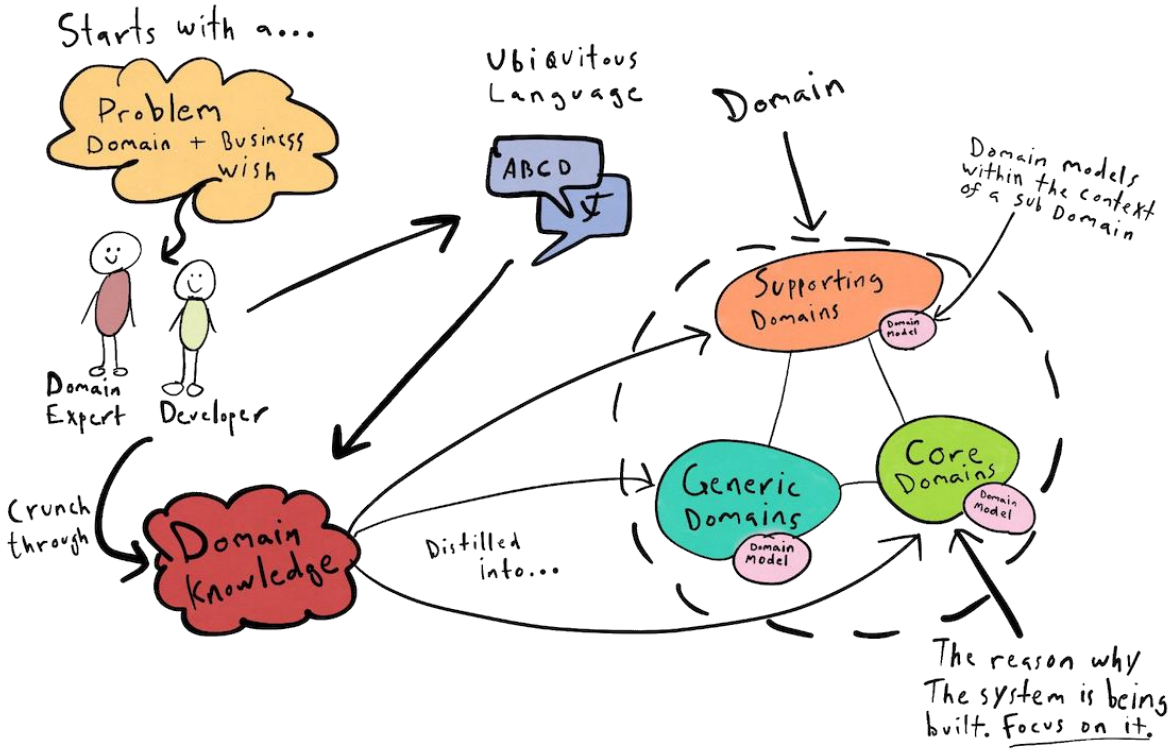
II. Mô hình miền và dịch vụ AD

Mô hình miền (Domain Model) và dịch vụ Active Directory (AD) là hai khái niệm chặt chẽ liên quan trong hệ thống Windows Server.

- **Mô hình miền (Domain Model)**

Mô hình miền là một cách tổ chức người dùng, máy tính, và các đối tượng khác trong một môi trường Windows Server. Một miền là một đơn vị an ninh và quản lý, trong đó tất cả các tài khoản người dùng, máy tính, và đối tượng khác được quản lý và xác định bằng một tên miền chung. Một mô hình miền cung cấp các lợi ích như:

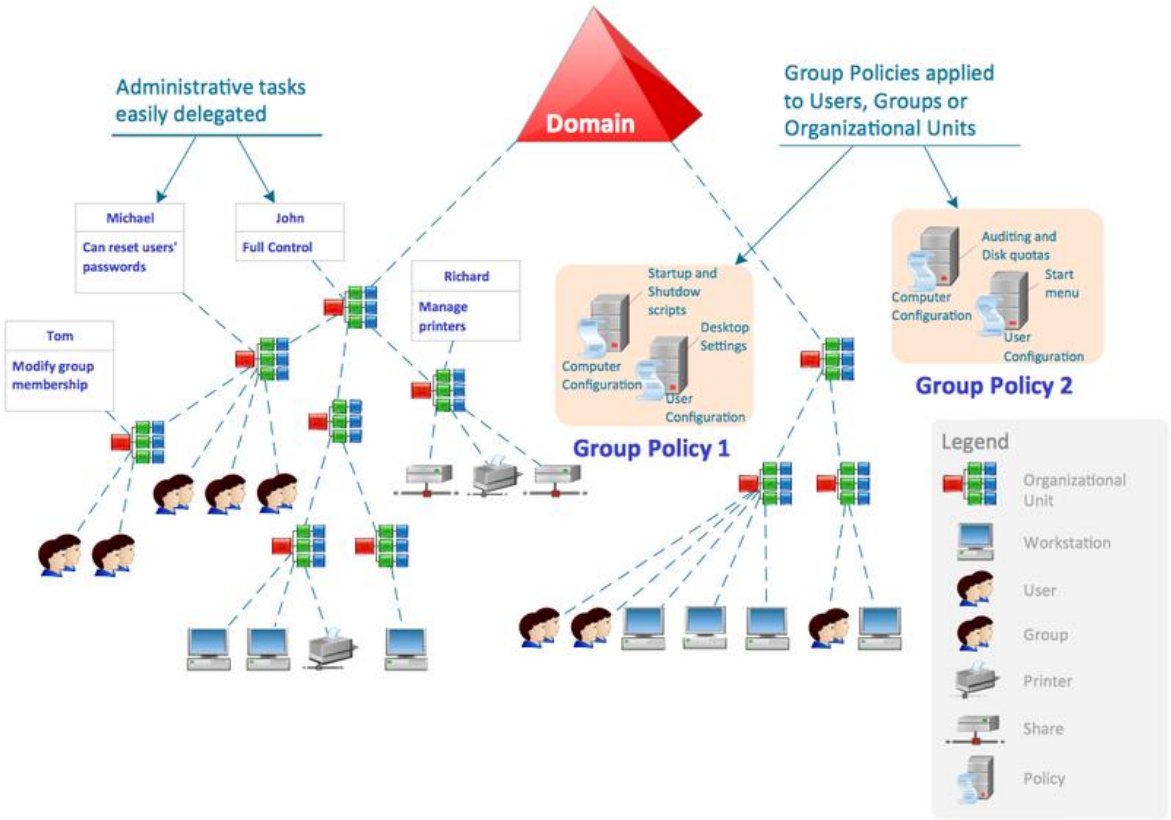
- **Quản lý Tài Khoản Người Dùng:** Người quản trị có thể quản lý và theo dõi tất cả tài khoản người dùng trong một miền duy nhất.
- **Quản lý Tài Khoản Máy Tính:** Máy tính cũng được quản lý trong một miền, giúp dễ dàng triển khai và quản lý các máy tính trong mạng.
- **Quản lý Chính Sách An Toàn:** Chính sách an toàn, như chính sách mật khẩu, chính sách tài khoản, và chính sách nhóm có thể được quản lý tập trung cho toàn bộ miền.
- **Quản lý Tài Nguyên Mạng:** Tài nguyên như máy in, ổ đĩa mạng, và dịch vụ khác có thể được chia sẻ và quản lý một cách hiệu quả.



- **Dịch vụ AD (Active Directory)**

Active Directory là một dịch vụ cơ sở dữ liệu và mô hình xác định, quản lý tài khoản người dùng, máy tính, và các đối tượng khác trong một môi trường miền. Các dịch vụ chính của Active Directory bao gồm:

- **Xác Thực và Ủy Quyền:** Active Directory quản lý quá trình xác thực và ủy quyền người dùng đối với các tài nguyên mạng.
- **Quản Lý Miền và Cây Miền:** Active Directory hỗ trợ quản lý miền và cây miền, nơi mà mỗi miền có thể chứa nhiều máy chủ và máy tính.
- **Dịch Vụ DNS (Domain Name System):** Active Directory sử dụng DNS để giúp xác định vị trí của các máy chủ và dịch vụ trong mạng.
- **Group Policy:** Active Directory cho phép người quản trị triển khai các chính sách an toàn và cấu hình mạng trên toàn bộ miền.
- **Replication:** Cung cấp quá trình sao chép dữ liệu giữa các máy chủ Active Directory để đảm bảo tính nhất quán và sẵn sàng.



III. Giới thiệu các dịch vụ bảo mật trên Windows Server 2019

1. Mã hóa IPSec

IPsec (Internet Protocol Security) là một bộ giao thức an ninh được sử dụng để bảo vệ giao tiếp trên mạng Internet. IPsec cung cấp một cơ chế cho việc xác định và mã hóa dữ liệu trong gói tin IP, giúp bảo vệ tính toàn vẹn, sự bí mật và xác thực của thông tin truyền qua mạng.

IPsec thường được triển khai ở tầng mạng (tầng 3) trong mô hình OSI (Open Systems Interconnection), nó hoạt động trực tiếp trên lớp IP. Có hai chế độ chính của IPsec:

- **Transport mode:** Trong chế độ này, chỉ phần dữ liệu của gói tin IP được bảo vệ và được mã hóa. Điều này thường được sử dụng cho các kết nối điểm-điểm (point-to-point) khi chỉ có một số lượng ít các thiết bị tham gia.
- **Tunnel mode:** Ở chế độ này, toàn bộ gói tin IP được bao gồm và bảo vệ, không chỉ là dữ liệu bên trong. Chế độ này thường được sử dụng khi muốn tạo một kết nối an toàn giữa hai mạng (site-to-site VPN), che giấu thông tin về cả địa chỉ IP và dữ liệu bên trong.

IPsec cung cấp các tính năng như:

- **Xác thực:** Đảm bảo rằng bên gửi và bên nhận là những bên chính xác.
- **Mã hóa:** Bảo vệ dữ liệu khỏi việc đọc trộm bằng cách mã hóa thông tin.
- **Tạo và quản lý kênh an toàn (SA):** Cơ chế để thiết lập và duy trì thông tin về an toàn giữa các nút tham gia truyền thông an toàn.

IPsec thường được sử dụng trong việc triển khai các mạng riêng ảo (VPN), cung cấp các phương tiện để bảo vệ dữ liệu khi truyền qua Internet hoặc mạng công cộng khác.

2. GPO

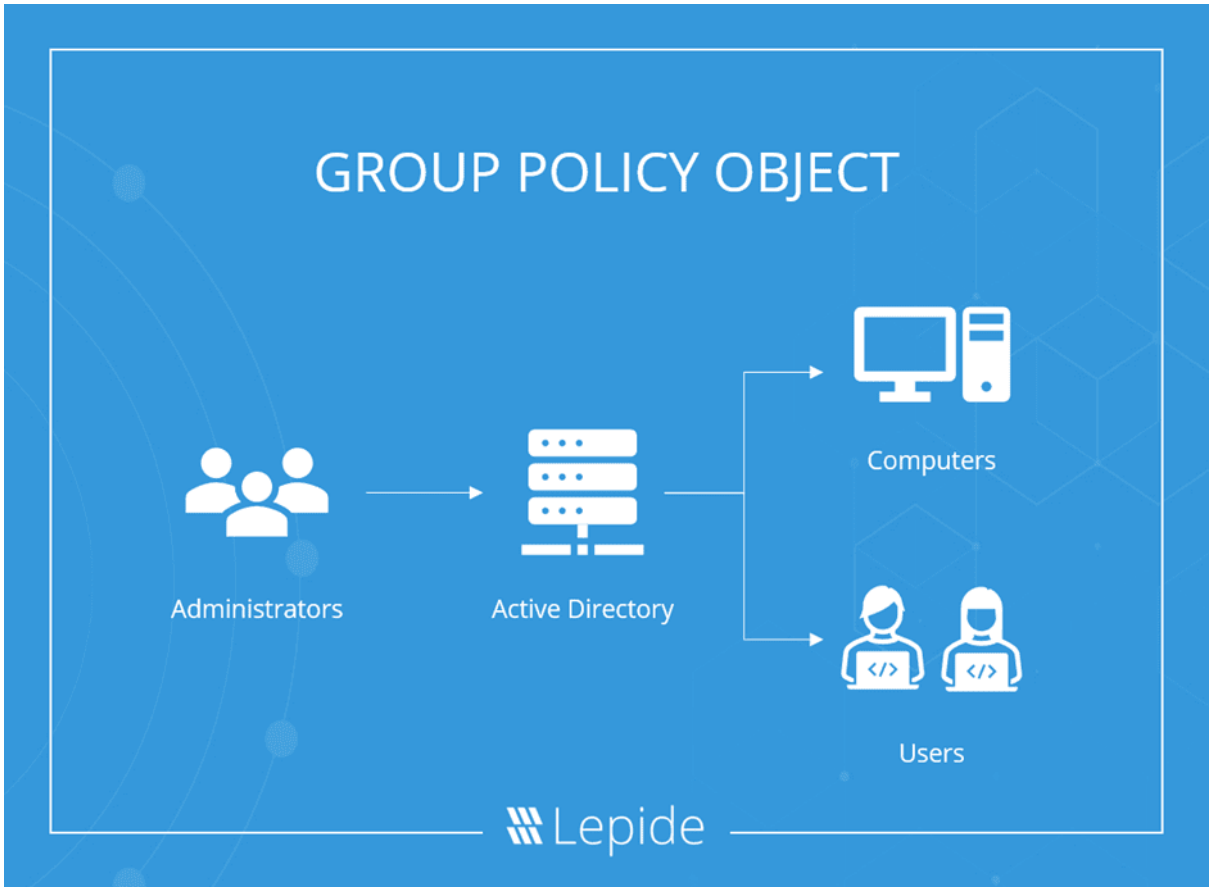
GPO là viết tắt của "Group Policy Object" trong hệ điều hành Windows. Group Policy (Chính sách Nhóm) là một cơ chế quản lý trên nền tảng Windows, cho phép quản trị viên thiết lập và triển khai các cài đặt và chính sách mạng trên các máy tính trong một môi trường Windows doanh nghiệp.

Group Policy Objects (GPOs) là các đối tượng cụ thể trong Active Directory của Windows Server, được sử dụng để áp dụng cài đặt và chính sách cho các người dùng và máy tính trong một miền hoặc một OU (Organizational Unit).

Một số điểm chính về Group Policy và GPOs bao gồm:

- **Tự động hóa quản lý:** GPOs cho phép tự động hóa quản lý môi trường mạng, giúp giảm thiểu sự can thiệp tay và đảm bảo tính nhất quán trong cài đặt mạng.
- **Chính sách an toàn và bảo mật:** GPOs có thể được sử dụng để áp dụng chính sách an toàn như cài đặt mật khẩu, chính sách tài khoản, và cài đặt bảo mật khác trên toàn bộ mạng.
- **Quản lý tài nguyên:** GPOs cũng cho phép quản trị viên quản lý tài nguyên mạng như máy in, ổ đĩa mạng, và các tài nguyên khác.
- **Quản lý ứng dụng:** GPOs có thể được sử dụng để quản lý và triển khai ứng dụng trên các máy tính trong mạng.
- **Quản lý giao diện người dùng:** Cài đặt liên quan đến giao diện người dùng, hình nền, biểu tượng và nhiều cài đặt khác cũng có thể được quản lý bằng GPOs.

GPOs chủ yếu được sử dụng trong môi trường doanh nghiệp và giúp quản trị viên duy trì tính nhất quán và an toàn trong hệ thống mạng Windows.



3. BitLocker

BitLocker là một tính năng mã hóa được tích hợp sẵn trong các phiên bản chuyên nghiệp của hệ điều hành Windows, bắt đầu từ Windows Vista và các phiên bản sau này, bao gồm cả Windows 7, 8, 8.1 và 10. BitLocker được thiết kế để bảo vệ dữ liệu trên các ổ đĩa lưu trữ, đặc biệt là ổ đĩa hệ thống, bằng cách mã hóa toàn bộ phân vùng lưu trữ.

Cụ thể, BitLocker có thể được sử dụng để mã hóa ổ đĩa cứng nội địa, ổ đĩa di động, hoặc các thiết bị lưu trữ khác như USB. Mục tiêu chính của BitLocker là giúp người dùng và tổ chức bảo vệ dữ liệu quan trọng khỏi việc truy cập trái phép hoặc lợi dụng thông tin từ ổ đĩa lưu trữ bằng cách mã hóa dữ liệu và đảm bảo rằng chỉ những người có chứng nhận và quyền truy cập hợp lệ mới có thể giải mã và sử dụng dữ liệu.

BitLocker thường được cấu hình và quản lý thông qua Group Policy trong môi trường Windows Server, và nó sử dụng các phương thức bảo mật như Trusted Platform Module (TPM) để tăng cường tính an toàn.

Chương 3: Khảo sát hệ thống mạng thực tế

I. Giới thiệu doanh nghiệp

Tên công ty: tập đoàn đa quốc gia DKP Gaming

Lĩnh vực kinh doanh: dịch vụ cho thuê sử dụng Internet

Quy mô hoạt động: 3 tầng mỗi tầng 30 máy

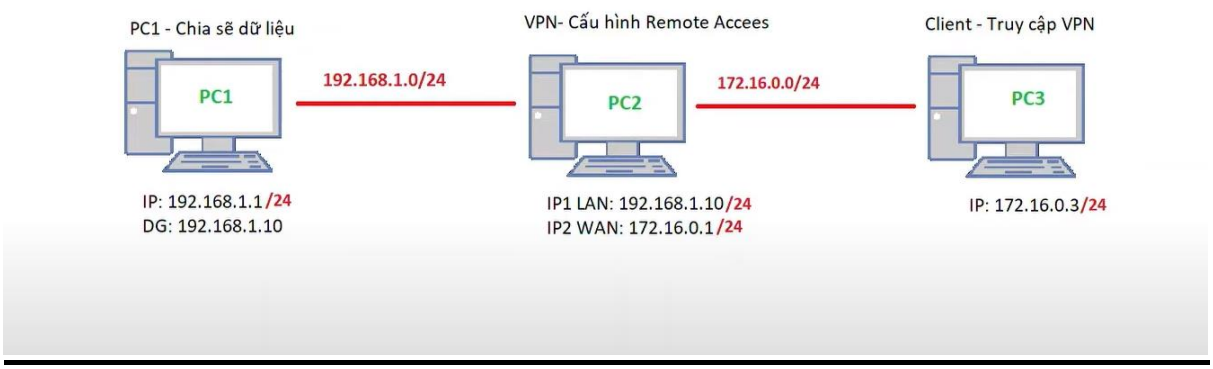
Tổng số chi nhánh: 2

Tổ chức phòng ban: phòng thanh toán sử dụng dịch vụ

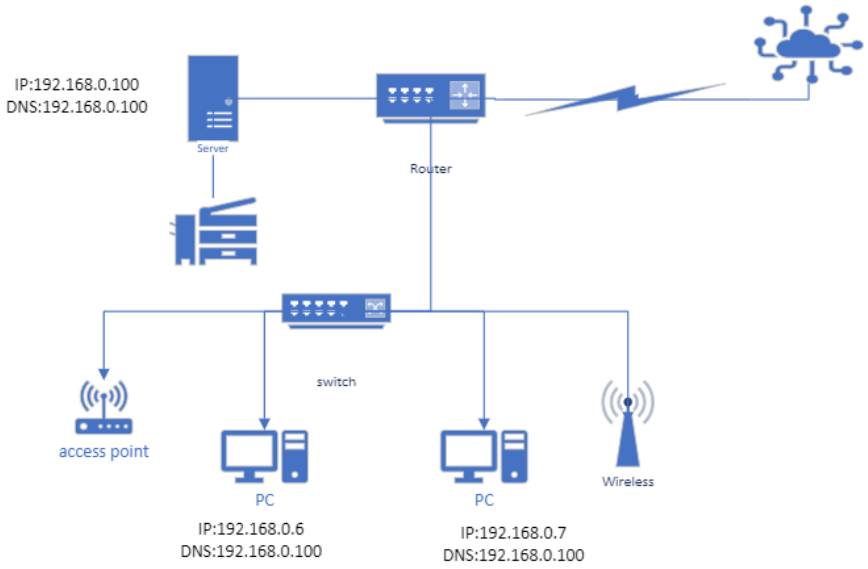
Vai trò của phòng: thanh toán dịch vụ

II. Tổng quan hệ thống mạng

1. Sơ đồ thiết kế mạng vật lý



2. Sơ đồ thiết kế mạng logic



---

3. Số lượng thiết bị sử dụng

- 1 máy window server 2019(DC,IPSEC,FIREWALL,ANTIVIRUS)
- 1 máy client window 10 join vào domain

4. Phân hoạch địa chỉ IP

Dải địa chỉ IP: 192.168.0.0/24

- **Máy chủ Domain:**

Địa chỉ IP tĩnh: 192.168.0.1

Subnet Mask: 255.255.255.0

Gateway (cổng ra): 192.168.0.254

- **Máy khách (Clients):**

Dải địa chỉ IP cho máy khách: 192.168.0.2 đến 192.168.0.101

Subnet Mask: 255.255.255.0

Gateway (cổng ra): 192.168.0.254

Có thể mở rộng dải địa chỉ IP cho máy khách nếu cần thiết.

- **Quản trị DHCP (Dynamic Host Configuration Protocol):**

Dải địa chỉ IP còn lại trong mạng có thể được sử dụng cho DHCP để tự động cấp phát địa chỉ IP cho các máy khách. Ví dụ, 192.168.0.102 đến 192.168.0.254.

Chương 4: Triển khai giải pháp Demo

a. Số lượng chi nhánh: 2

b. Sơ đồ thiết kế logic demo

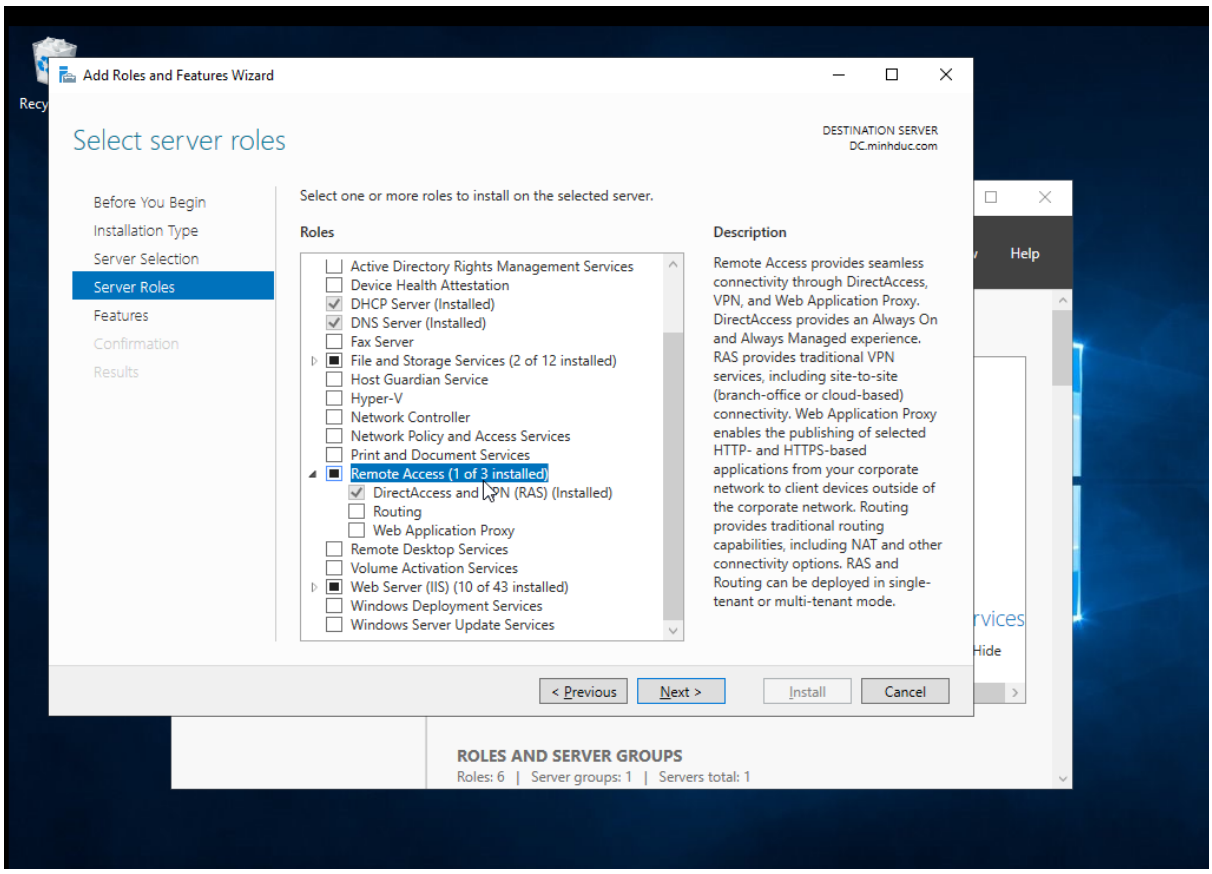
Server01:DC,Firewall,IPSEC

Client01

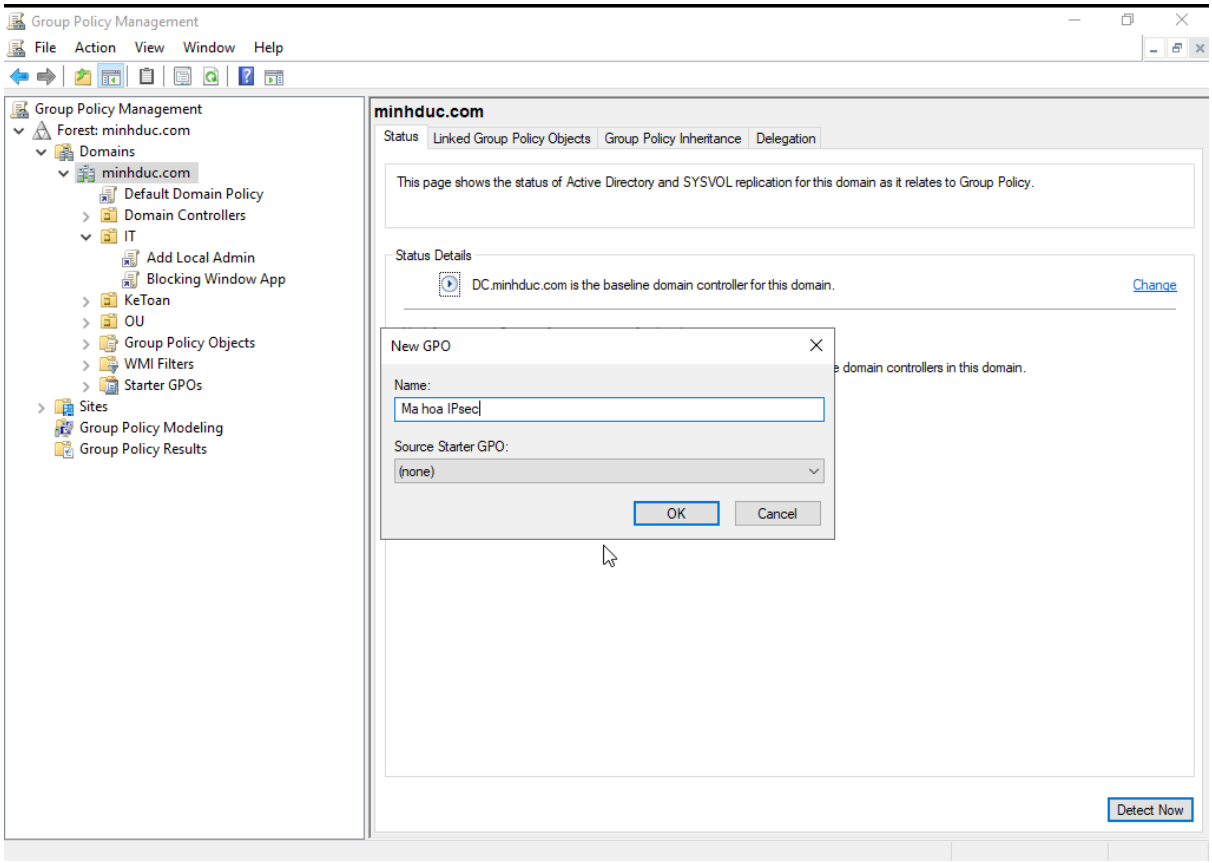
c. Tóm tắt các bước cấu hình

1. Mã hóa Ipsec

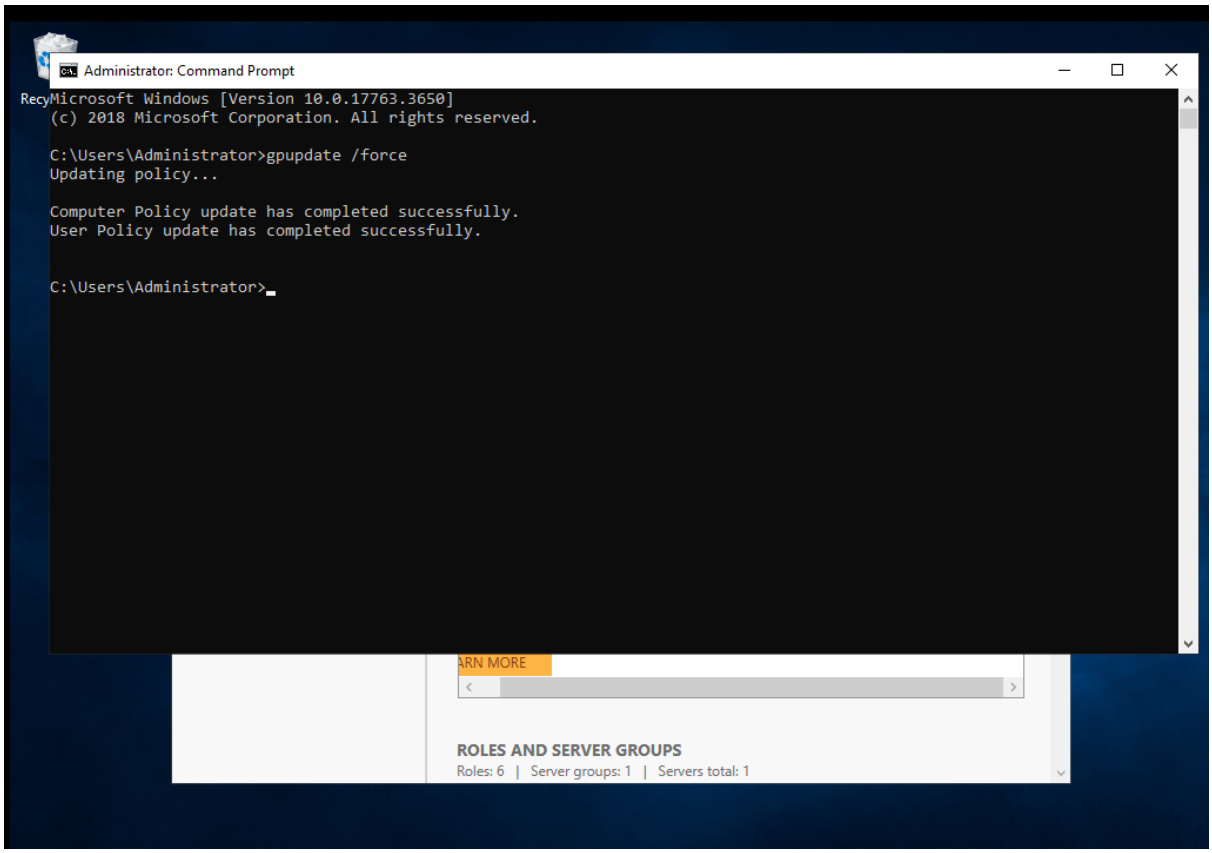
Bước 1: Cài đặt IPsec



Bước 2: Cấu hình IPsec qua Group Policy

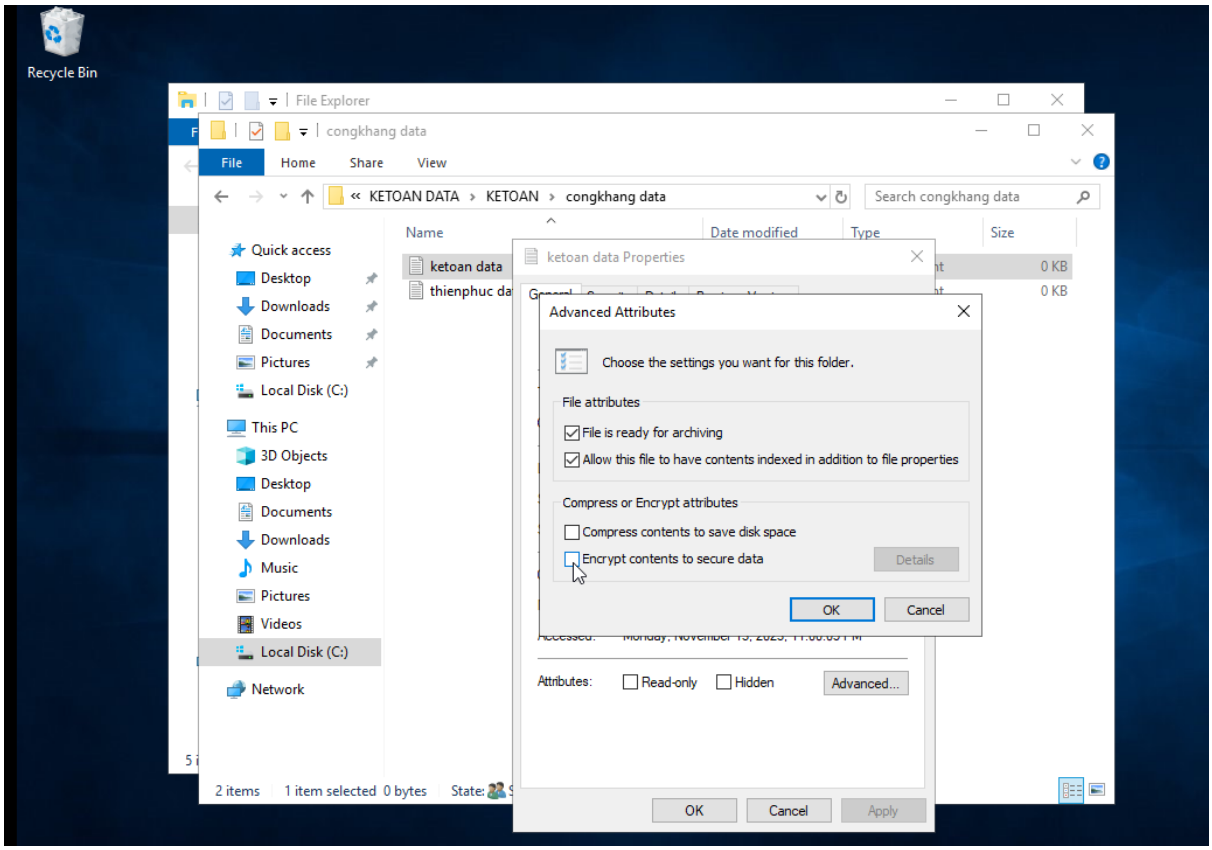


Bước 3: Áp dụng GPO

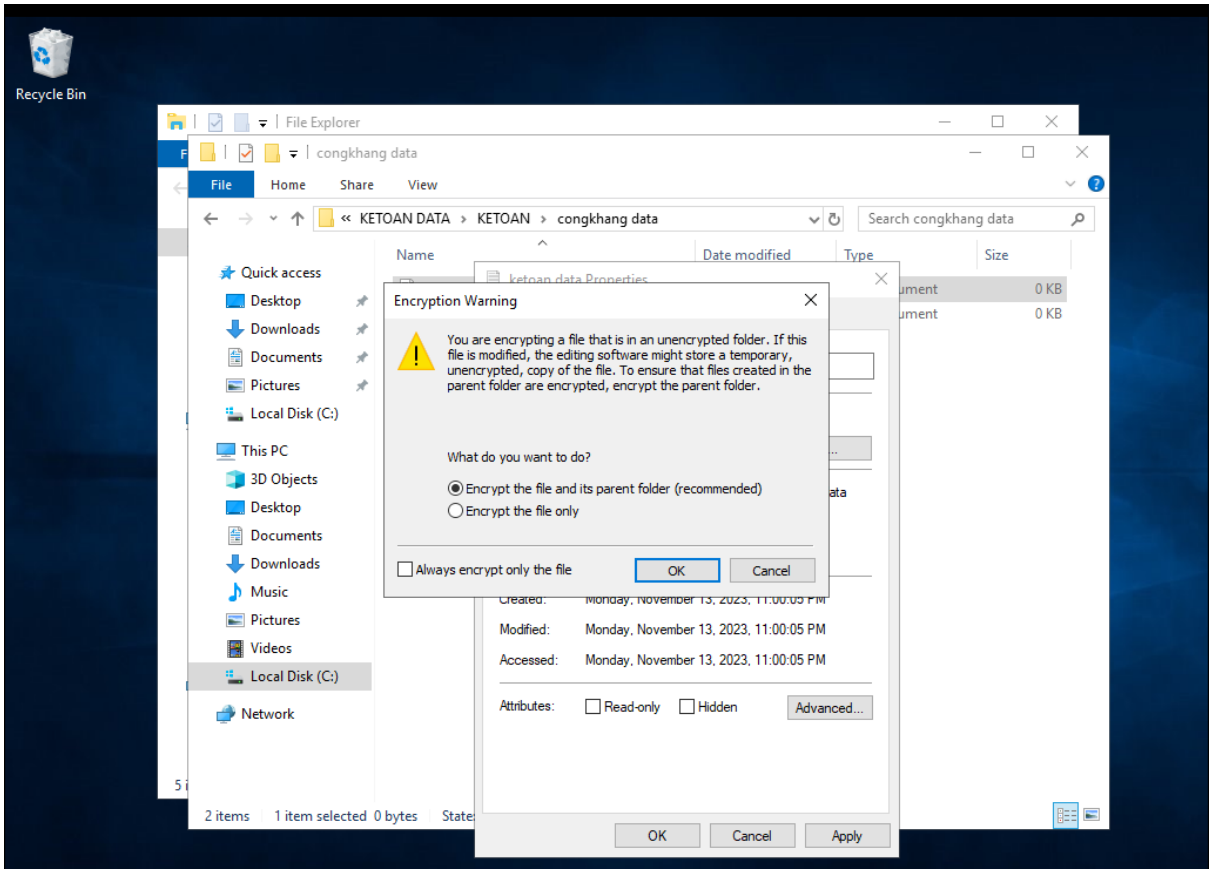


2. Mã hóa EFS

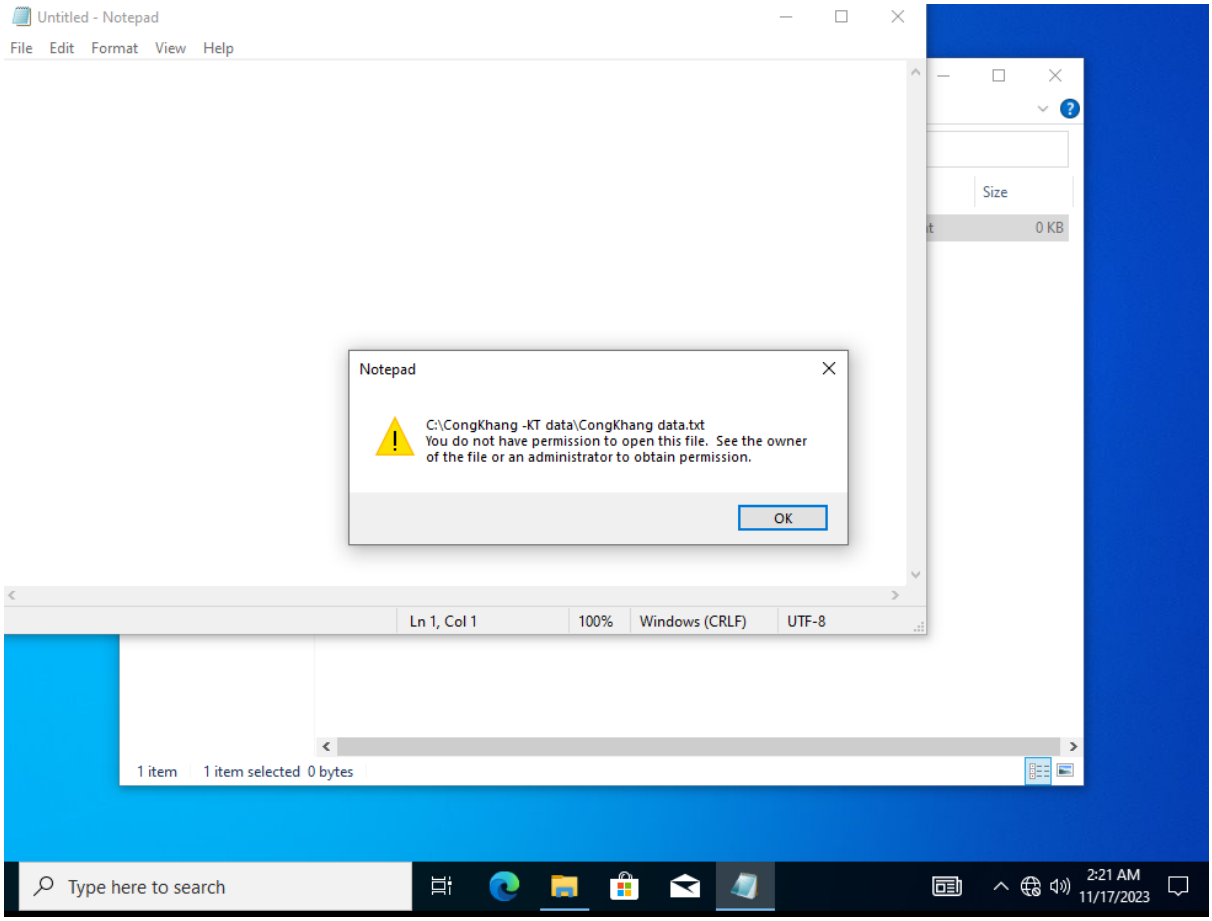
Bước 1: Kiểm tra khả năng sử dụng EFS



Bước 2: Mã hóa tệp tin hoặc thư mục

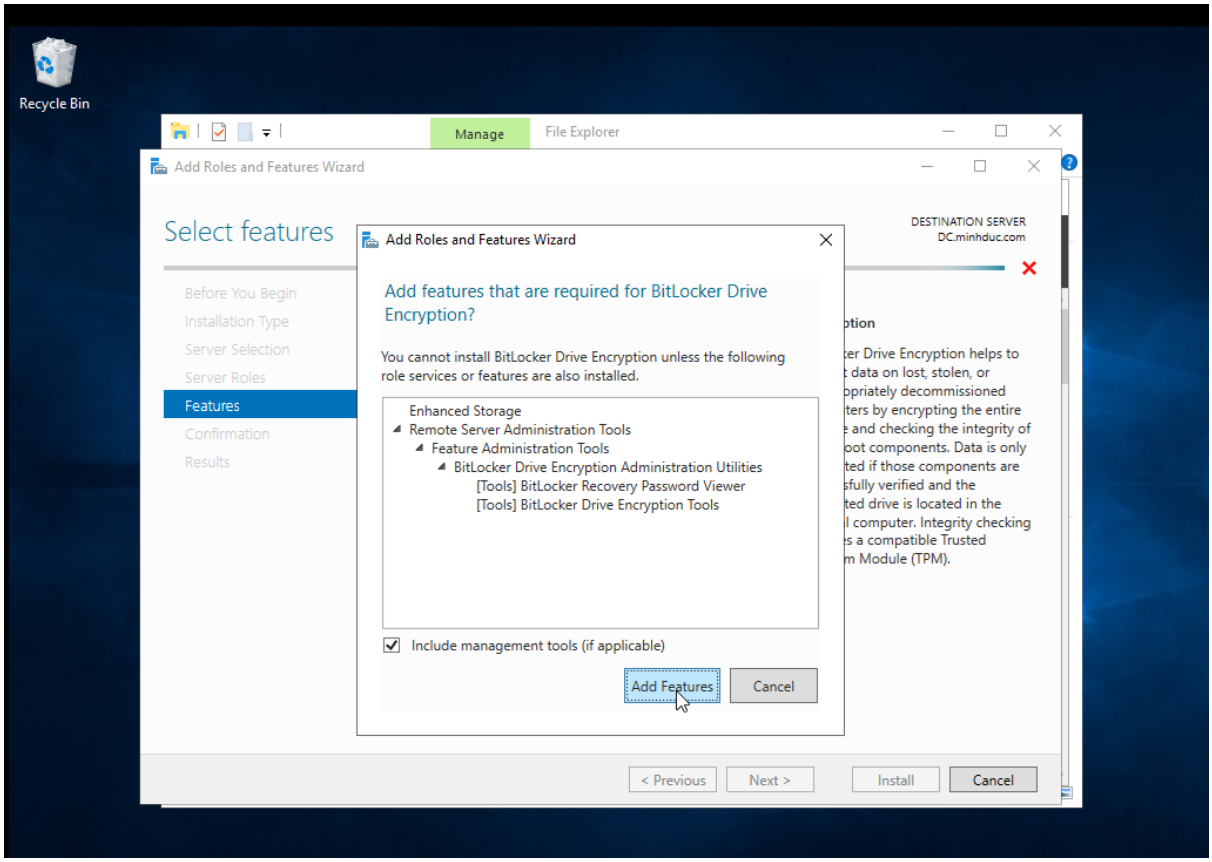


Bước 3: Giải mã tệp tin hoặc thư mục

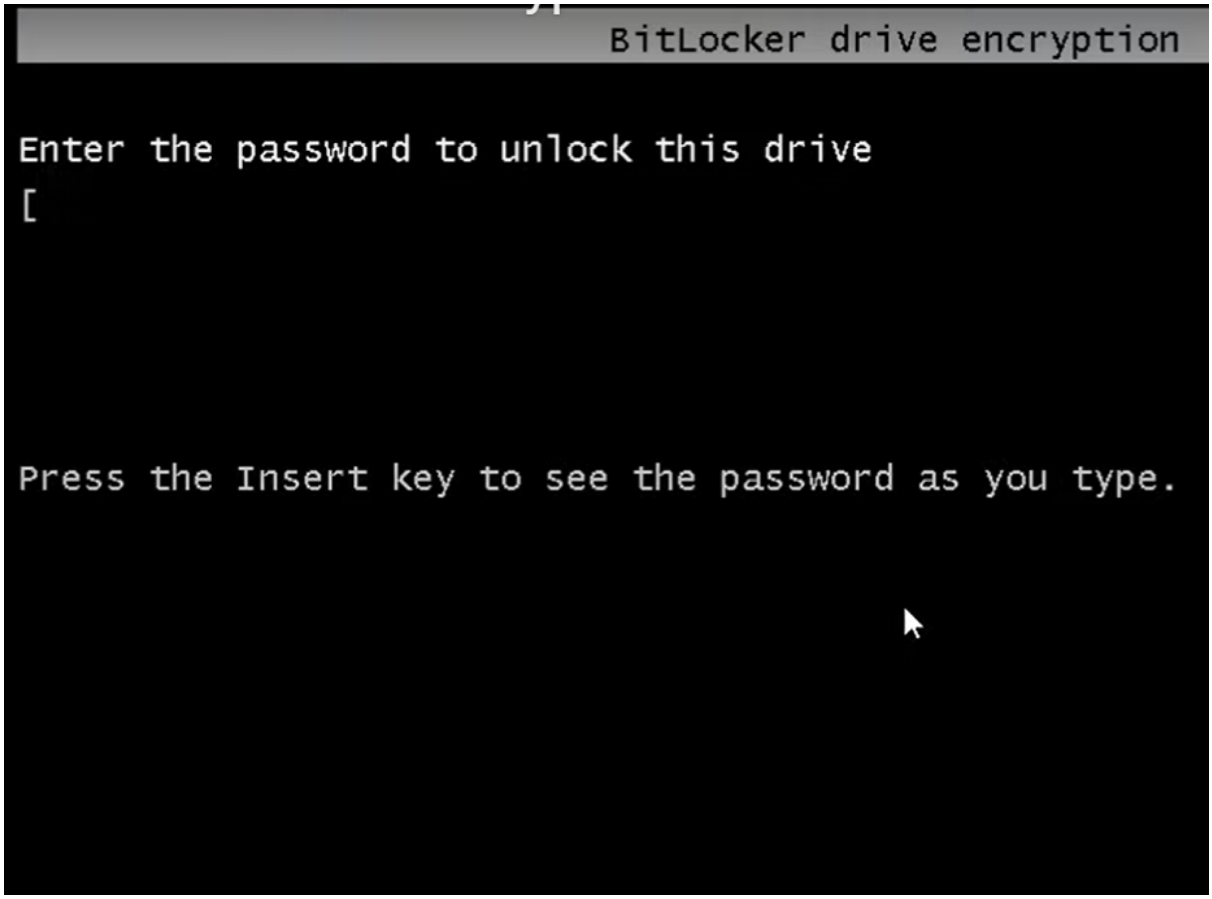


3. Mã hóa Bitlocker

Bước 1: Kiểm tra khả năng sử dụng BitLocker

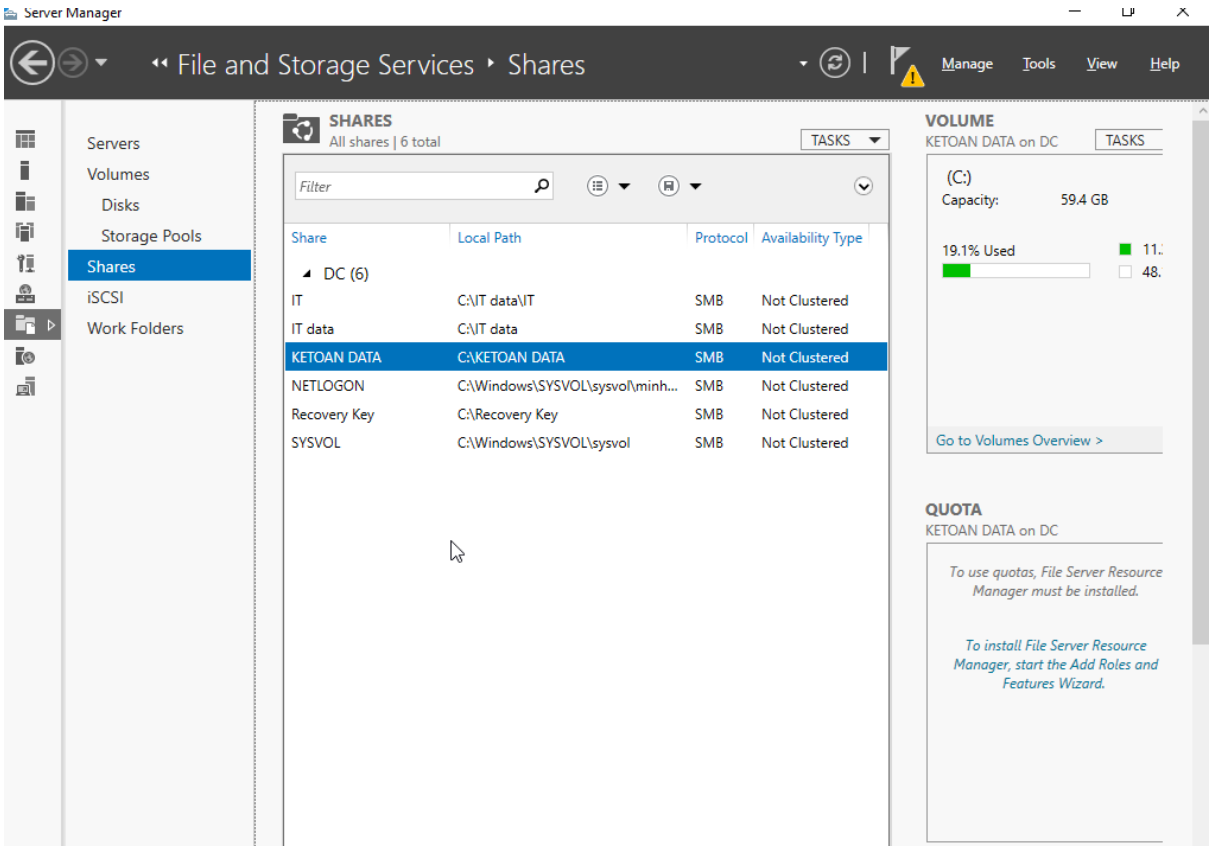


Bước 2: Cấu hình BitLocker qua Server Manager

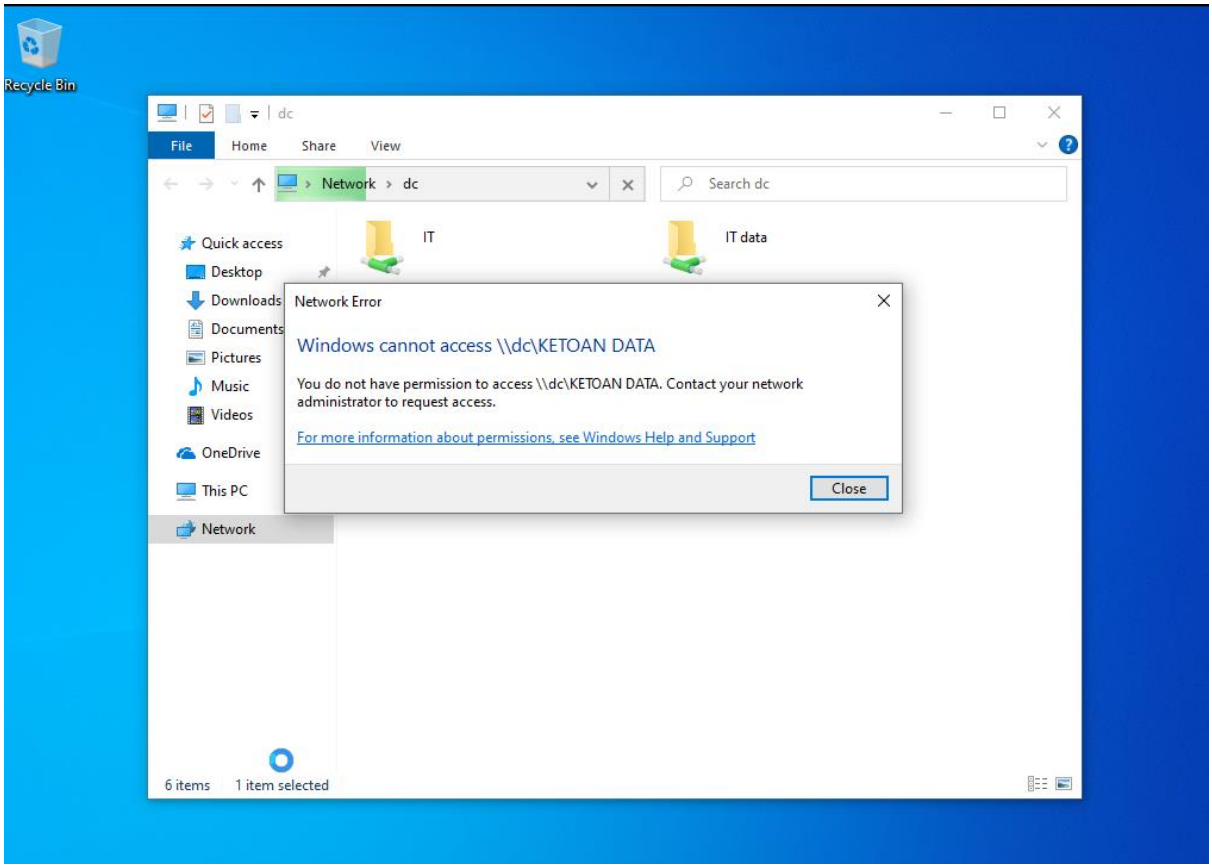


4. Quyền truy cập NTFS và quyền Share

Bước 1: Mở Properties của Thư Mục hoặc Ổ Đĩa

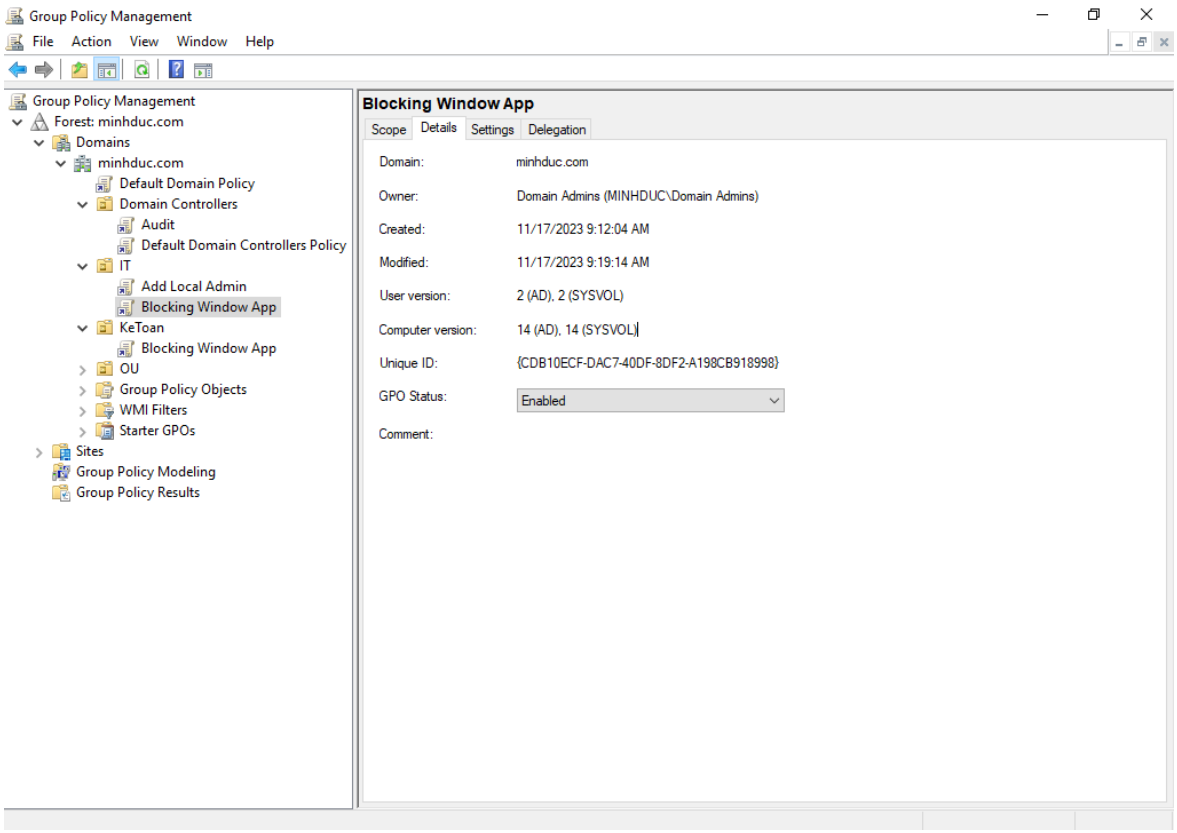


Bước 4: Chỉnh Sửa Quyền Truy Cập trong Tab "Security"



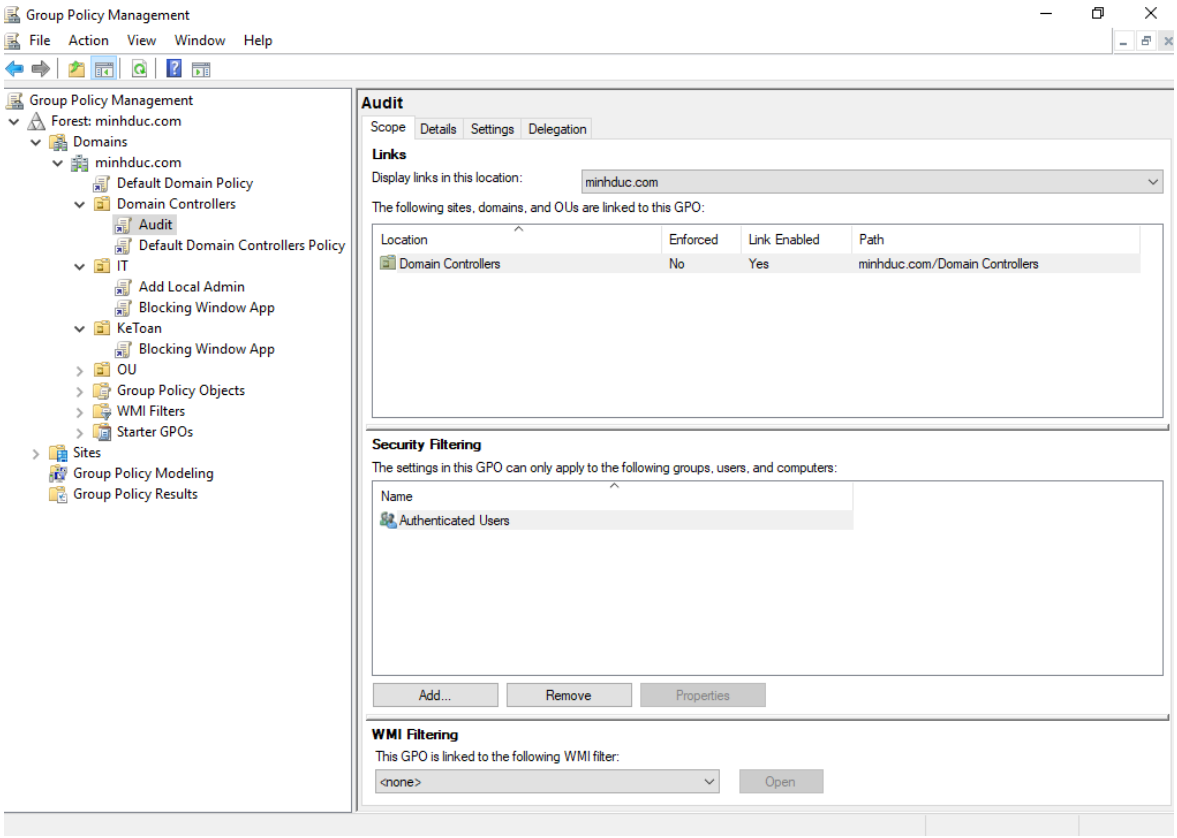
5. Blocking CMD và Control Planel

-Tạo GPO mới trong Group Policy Managemant và thêm vào các OU

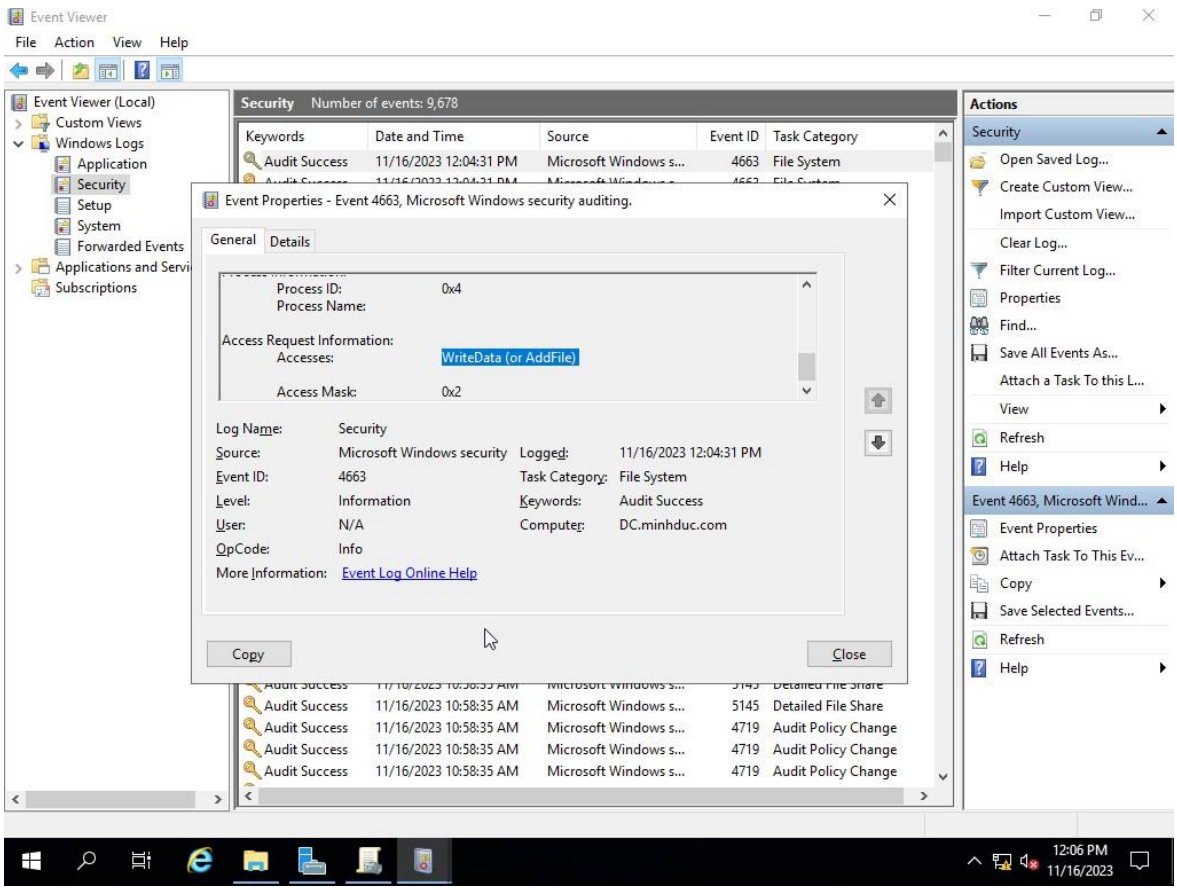


6. Audit Log (Event View)

Bước 1 : Tạo GPO mới trong Group Policy Managemant và thêm Domain Controller

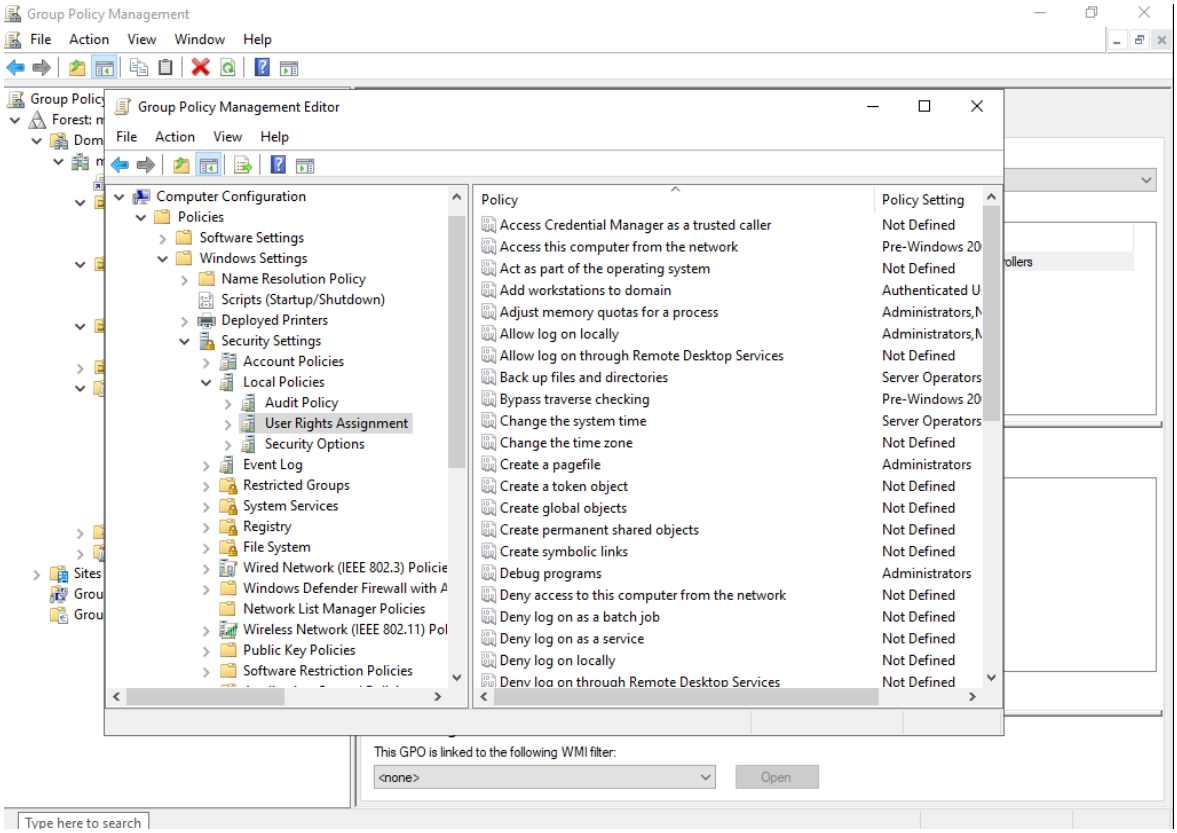


Bước 2 : Truy cập Event Views trong Server Manager để kiểm tra

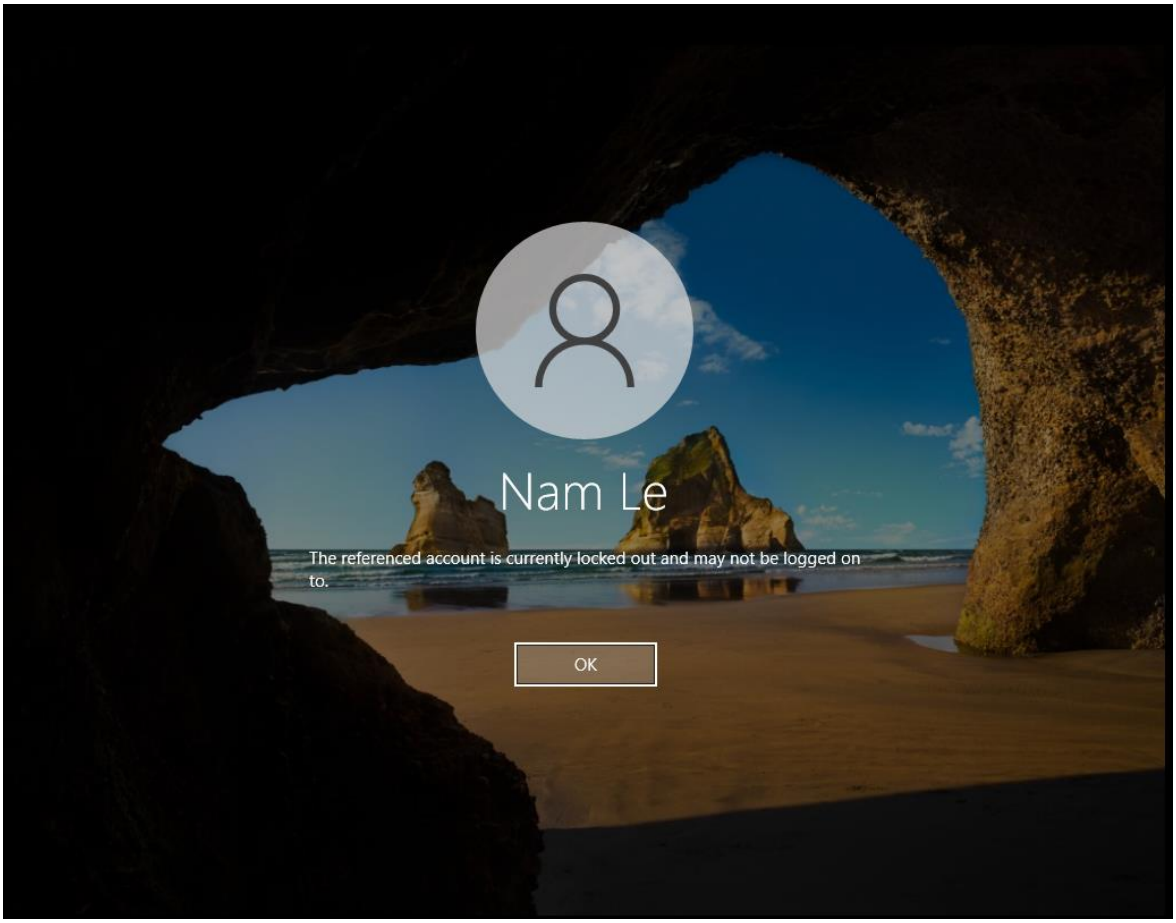


7. Thực hiện Lockout User khi nhập sai mật khẩu

Bước 1 : Truy cập GPO và edit, chọn User Right Assignment



Bước 2 : Thêm vào các OU và thực hiện kiểm tra



Chương 5: Kết quả triển khai

5.1.Kết quả triển khai:

Sau quá trình triển khai đầy thách thức, dự án đã đạt được những kết quả tích cực, hoàn thiện một loạt các mục tiêu quan trọng mà nhóm đã đề ra từ trước. Tính đến thời điểm hiện tại, chúng tôi đã thành công trong việc triển khai và tích hợp hệ thống mới, mang lại những cải tiến đáng kể cho hiệu suất và hiệu quả làm việc của tổ chức.

Một trong những thành tựu nổi bật là sự tích hợp mượt mà của các ứng dụng và hệ thống, tạo nên một môi trường làm việc mạnh mẽ và linh hoạt. Điều

này giúp tăng cường khả năng tương tác giữa các phòng ban và đội ngũ, thúc đẩy sự hợp tác và chia sẻ thông tin một cách hiệu quả.

Hơn nữa, các tiêu chí về hiệu suất đã được đáp ứng đúng như kỳ vọng. Hệ thống mới không chỉ giúp giảm thời gian xử lý công việc mà còn tối ưu hóa tài nguyên, đảm bảo rằng tổ chức đang hoạt động ở mức hiệu suất tối ưu. Điều này không chỉ giúp tiết kiệm chi phí mà còn đảm bảo rằng nguồn lực đang được sử dụng một cách có hiệu quả nhất.

Tuy nhiên, còn một số công việc như cài đặt firewall và quá trình backup restore vẫn đang trong quá trình thực hiện. Các công việc này đòi hỏi sự cẩn trọng và đảm bảo đầy đủ thời gian để đảm bảo tính bảo mật và khả năng phục hồi dữ liệu hiệu quả. Nhóm chúng tôi cam kết hoàn thành những công việc này một cách cẩn thận và chắc chắn để đảm bảo rằng toàn bộ hệ thống hoạt động mạnh mẽ và an toàn.

5.2.Ưu – Nhược điểm:

- **Ưu điểm:**

1. Cập nhật bảo mật định kỳ: Microsoft thường xuyên phát hành các bản cập nhật bảo mật để đối mặt với các lỗ hổng bảo mật mới và cải thiện tính ổn định.
2. Windows Defender: Windows Server 2019 tích hợp sẵn Windows Defender, một phần mềm diệt virus và malware mạnh mẽ.
3. Credential Guard: Chức năng này giúp bảo vệ thông tin xác thực bằng cách cô lập và bảo vệ các thông tin xác thực của người dùng.
4. BitLocker: Cung cấp khả năng mã hóa đĩa để bảo vệ dữ liệu tránh khỏi việc truy cập trái phép nếu thiết bị bị mất hoặc đánh cắp.

5. Advanced Threat Protection (ATP): Cung cấp các tính năng nâng cao như theo dõi và phân tích hành vi để phát hiện và ngăn chặn các mối đe dọa tiên tiến.
6. Firewall tích hợp: Hệ điều hành cung cấp một tường lửa tích hợp giúp kiểm soát luồng dữ liệu giữa các mạng.
7. Quản lý quyền truy cập: Windows Server 2019 hỗ trợ quản lý quyền truy cập chi tiết cho từng người dùng và nhóm.

- **Nhược điểm:**

1. Khả năng chống lại tấn công zero-day: Mặc dù có các cập nhật định kỳ, nhưng vẫn có thể tồn tại lỗ hổng bảo mật chưa được biết đến (zero-day vulnerabilities).
2. Cần cấu hình chặt chẽ: Nếu không cấu hình đúng, các tính năng bảo mật có thể trở nên không hiệu quả.
3. Yêu cầu tài nguyên hệ thống cao: Các tính năng bảo mật mạnh mẽ thường đi kèm với việc tăng tải cho hệ thống, đôi khi có thể làm giảm hiệu suất.
4. Chi phí bản quyền và quản lý: Sử dụng các tính năng bảo mật cao cấp thường đòi hỏi chi phí bản quyền và công sức quản lý đáng kể.
5. Khả năng tương thích: Có thể có vấn đề tương thích với một số ứng dụng hoặc phần cứng cụ thể.
6. Sự phức tạp của các tính năng bảo mật cao cấp: Việc cấu hình và quản lý các tính năng bảo mật phức tạp có thể đòi hỏi kiến thức chuyên sâu và thời gian đào tạo.

5.3.Hướng phát triển:

Đề tài về bảo mật của Windows Server 2019 có nhiều hướng phát triển tiềm năng mà có thể được khám phá để nâng cao khả năng bảo vệ và quản lý hệ thống. Một trong những hướng phát triển quan trọng là nghiên cứu về cách tích hợp công nghệ tiên tiến như trí tuệ nhân tạo và học máy vào hệ thống,

nhằm tăng cường khả năng phát hiện và phòng ngự trước các mối đe dọa ngày càng phức tạp.

Ngoài ra, việc mở rộng nghiên cứu đến lĩnh vực bảo mật trong môi trường đám mây và ảo hóa là một hướng quan trọng để đảm bảo an toàn và đồng bộ giữa các nền tảng khác nhau. Đặc biệt, việc tập trung vào cách quản lý tổn thương và khôi phục hệ thống sau một tấn công cũng là một khía cạnh quan trọng, giúp giảm thiểu thời gian chết của hệ thống và giữ cho doanh nghiệp hoạt động một cách liên tục.

Một hướng phát triển khác có thể bao gồm việc tương tác với Internet of Things (IoT) và ứng phó với những thách thức đặc biệt của việc bảo mật trong môi trường kết nối của các thiết bị thông minh. Đồng thời, việc phát triển chính sách an ninh và đào tạo nguồn nhân lực cũng là yếu tố quan trọng để xây dựng một hệ thống bảo mật toàn diện.

Những hướng phát triển này không chỉ giúp nâng cao đề tài mà còn tạo ra ảnh hưởng tích cực trong việc phát triển các giải pháp bảo mật chống lại các mối đe dọa ngày càng phức tạp trong môi trường doanh nghiệp hiện đại.

Kết luận

Trong quá trình nghiên cứu và triển khai giải pháp bảo mật cho Windows Server 2019, chúng tôi đã đạt được những kết quả quan trọng và tạo ra một hệ thống an toàn, đáng tin cậy. Việc đề tài này không chỉ giúp chúng tôi nắm bắt sâu sắc về các vấn đề bảo mật hiện tại mà còn mang lại cái nhìn rõ ràng về cách tích hợp các giải pháp bảo mật hiệu quả cho môi trường Windows Server 2019.

Chúng tôi đã xác định và triển khai một loạt các biện pháp bảo mật như cập nhật hệ điều hành, cài đặt và cấu hình firewall, áp dụng các chính sách bảo mật nhóm người dùng, và triển khai các công nghệ mã hóa để bảo vệ dữ liệu quan trọng. Ngoài ra, chúng tôi cũng thực hiện theo dõi liên tục và thiết lập các biện pháp phát hiện xâm nhập để đảm bảo sự an toàn và phản ứng nhanh chóng trước bất kỳ mối đe dọa nào.

Kết quả của đề tài này là việc nâng cao đáng kể về mặt bảo mật của hệ thống, giảm thiểu rủi ro từ các mối đe dọa mạng và bảo vệ thông tin quan trọng của tổ chức. Đồng thời, chúng tôi đã chú ý đến khả năng linh hoạt và sự thuận tiện trong quản lý hệ thống, nhằm đảm bảo rằng các biện pháp bảo mật không gây ảnh hưởng đáng kể đến hiệu suất và trải nghiệm người dùng.

Tổng cộng, đề tài này không chỉ là một bước quan trọng để nâng cao bảo mật cho Windows Server 2019 mà còn là một cơ hội để hiểu rõ hơn về quy trình triển khai và quản lý an ninh thông tin trong môi trường doanh nghiệp.

- **Tài liệu tham khảo(References)**

1. **Microsoft Documentation:**

Microsoft Security Documentation - Cung cấp thông tin chi tiết về các biện pháp bảo mật và hướng dẫn triển khai trên nền tảng Microsoft, bao gồm cả Windows Server 2019.

Windows Server Security - Tài liệu cung cấp hướng dẫn và chi tiết về cách cải thiện bảo mật trên Windows Server.

2. **Sách và Tài Liệu Hướng Dẫn:**

"Mastering Windows Server 2019" của Jordan Krause - Sách này cung cấp thông tin chi tiết về cách triển khai, quản lý và bảo mật Windows Server 2019.

"Windows Server 2019 Administration Inside Out" của Orin Thomas - Cung cấp thông tin về quản lý hệ thống và bảo mật trong môi trường Windows Server 2019.

3. **Bài Viết và Hướng Dẫn Trực Tuyến:**

Windows Server Security Best Practices and Strategies - Bài viết này đề cập đến những phương pháp tốt nhất và chiến lược cho bảo mật trên Windows Server.

Best Practices for Securing Active Directory - Tài liệu của Microsoft về các phương pháp tốt nhất để bảo vệ Active Directory, một thành phần quan trọng trên Windows Server.

4. **Tài Liệu Chuyên Sâu và Bài Nghiên Cứu:**

"Security Technical Implementation Guide (STIG)" - Cung cấp các hướng dẫn chi tiết về cách cấu hình và bảo mật nhiều hệ điều hành, bao gồm cả Windows Server.

Bài nghiên cứu từ các tổ chức như SANS Institute, NIST, và ISC² về bảo mật hệ thống Windows Server.