# **HƯỚNG DẪN THỰC HÀNH**

# 

# **1. Windows Server 2022**

- Tải trực tiếp từ Website của Microsoft, link: <https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2022>

- Tải từ Google Drive, link: <https://drive.google.com/drive/folders/1rkLRlR4eoknWwIW5rOfRqO4eOqiLebeS?usp=sharing>

# **2. Sử dụng công cụ tạo máy ảo**

Các bạn có thể sử dụng VMWare, hoặc VirtualBox hoặc Hyper-V

## **2.1. VMWare**

Tải trực tiếp từ Website VMware, link: <https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>

Tải từ Google Drive, link: <https://drive.google.com/drive/folders/1rkLRlR4eoknWwIW5rOfRqO4eOqiLebeS?usp=sharing>

## **2.2. VirtualBox**

Link: <https://www.virtualbox.org/wiki/Downloads>

## **2.3. Hyper-V**

Link: <https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-hyper-v?pivots=windows>

# **3. Tạo máy ảo và cài Windows Server 2022**

- B1: Mở VMware

- B2: File/Mew Virtual Machine

- B3: Chọn Typical, Next

- B4: Chọn I will install the operating system later

- B5: Chọn Microsoft Windows, Chọn Version: Windows Server 2022, Next

- B6: Đặt tên Virtual machine, nên đặt tên dễ nhớ để buổi sau thực hành, Chọn đường dẫn đến ổ D để lưu trữ, vì khi lưu vào ổ C máy khởi động sẻ mất, Next

- B7: Chọn Maximum disk size 60GB, Chọn Split virtual disk into multipe files, Next

- B8: Finish

- B9: Click chuột phải vào tên Virtual Machine vừa đặt bên cửa sổ tay trái, Chọn Settings …

- B10: Click vào CD/DVD (SATA), chọn Use ISO image file và click Brower… để dẫn đến file Windows Server 2022.ISO vừa tải về, Nhấp vào Ok

- B11: Click chuột phải vào tên Virtual Machine vừa tạo và bấm Powrer/Power On Hoặc có thể thực hiện bằng cách click vào nút tam giác màu xanh

LƯU Ý:

- Nếu máy không báo lỗi thì qua B12.

- Nếu máy tính báo lỗi *“This host supports Intel VT-x, but Intel VT-x is disabled”*.

+ Khởi động lại máy tính,

+ Khi máy tính tắt, và bắt đầu bật màn hình đen thực hiện nhấp F2 liên tục để vào BIOS setting (hoặc phím khác theo hướng dẫn trên màn hình)

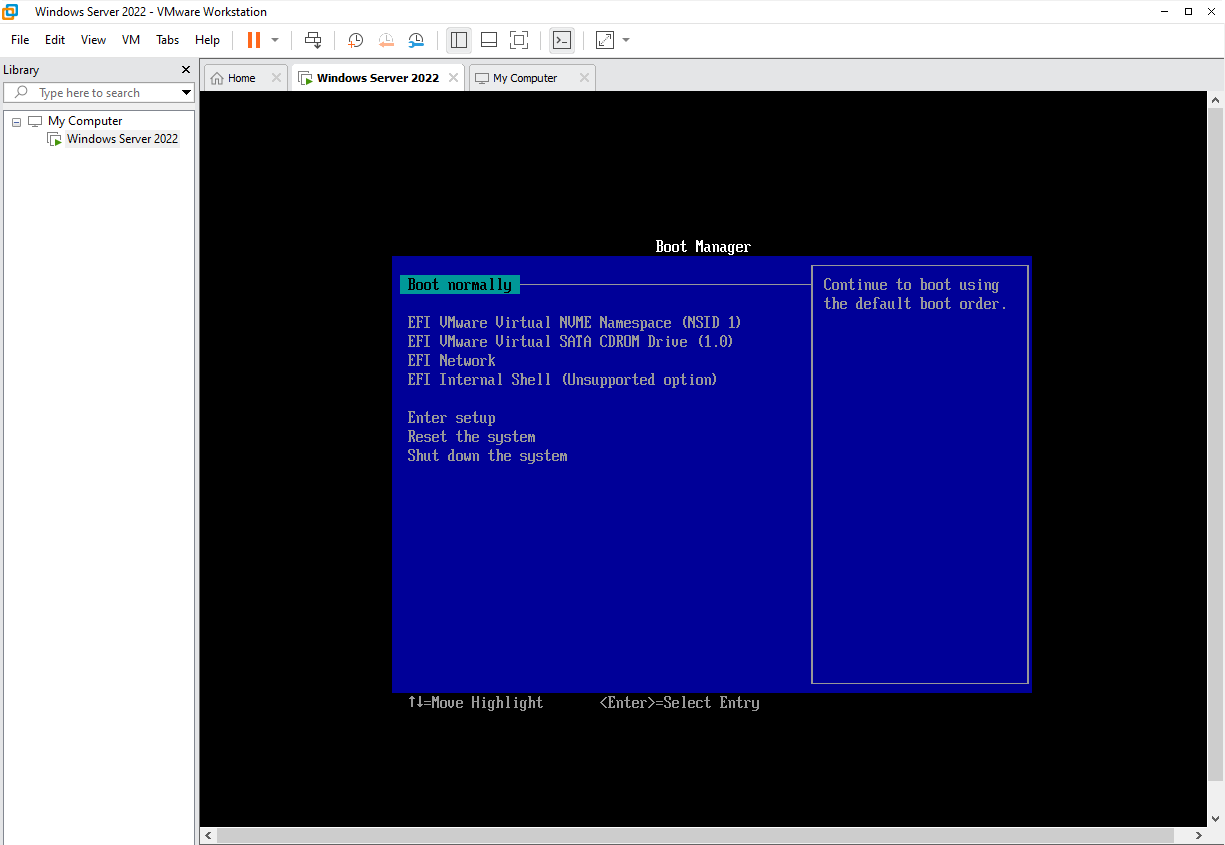
+ Sau khi vào BIOS Setting thực hiện các bước sau:

+ Vào Advanced Model/Advanced/CPU Configuration/Intel Virtualization Technology, thay đổi từ “Disabled” thành “Enabled” trong listbox bên tay phải.

+ Sau đó bấm F10 để lưu kết quả thiết lập

+ Bấm Ok để lưu và khởi động Windows

+ Mở VMware và khởi động lại Máy ảo vừa tạo ở B11.



* B12: khi vào màn hình đen, có hiển thị hàng chữ bấm phím bất kỳ để vào Setup,

Lưu ý: nếu quên bấm phím bất kỳ thì sẻ vào màn hình màu xanh chọn “EFI VMware virtual CDROM”

- B13: Trog giao diện màn hình Setup bấm Next

- B14: Nhấp chuột vào Install now

- B15: Giao diện hiển thì 4 tuỳ chọn Windows Server các bạn chọn Windows Server 2022 Datacenter Evaluation (Desktop Experience), chọn Next

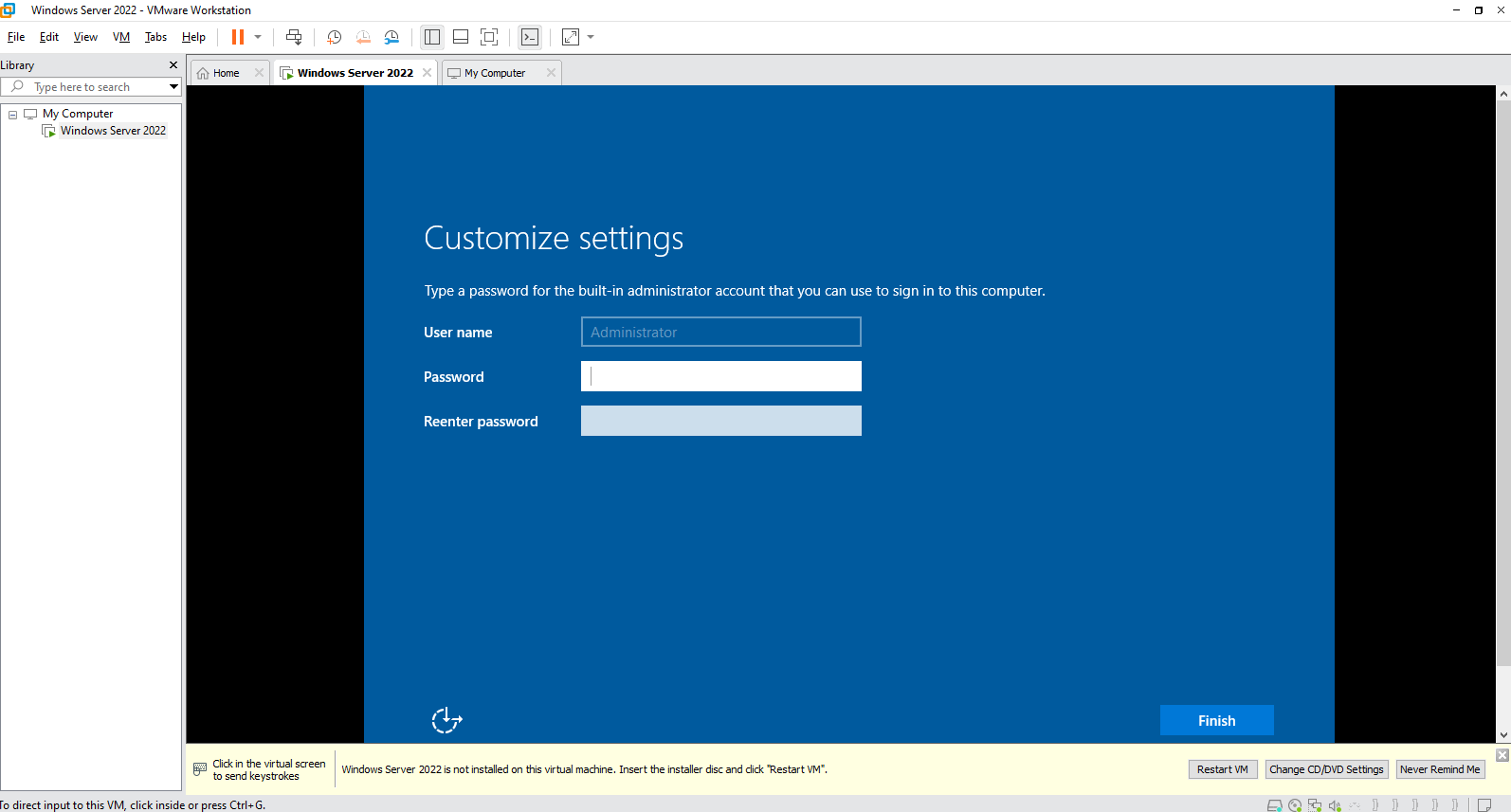
- B16: Chọn vào Checkbox “I accept the Microsoft….”, Next

- B17: Màn hình Which type of installation do you want?, chọn Custom: Install Micorsoft Server ….

Lưu ý: Bước này nếu chọn Upgrade thì khi cài máy thật có thể mất dữ liệu

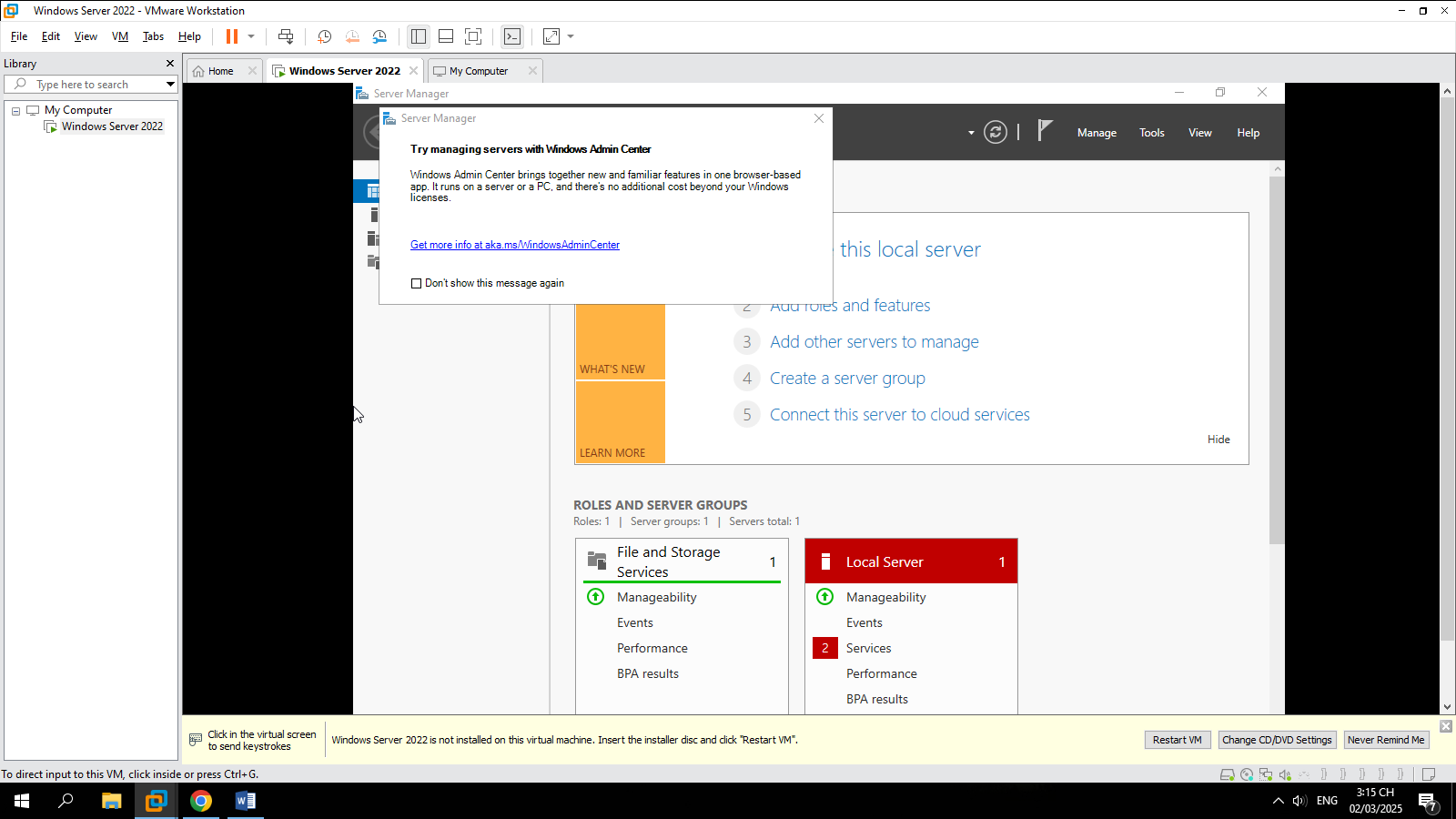
- B18: tại nước này chon New để tạo ổ đỉa mới, Chọn Apply, Chọn Ok, Chọn Next.

Lưu ý: Bước này nếu cài máy thật, đã có các phân vùng thì không thực hiện chọn New mà click vào phần vùng chứa hệ điều hành đã cài trước để cài đè lên hoặc xoá dữ liệu trước khi cài lên.



- B19: Đặt mật khẩu phải có ký tự hoa, ký tự thường, ký tự số và ký tự đặc biệt.

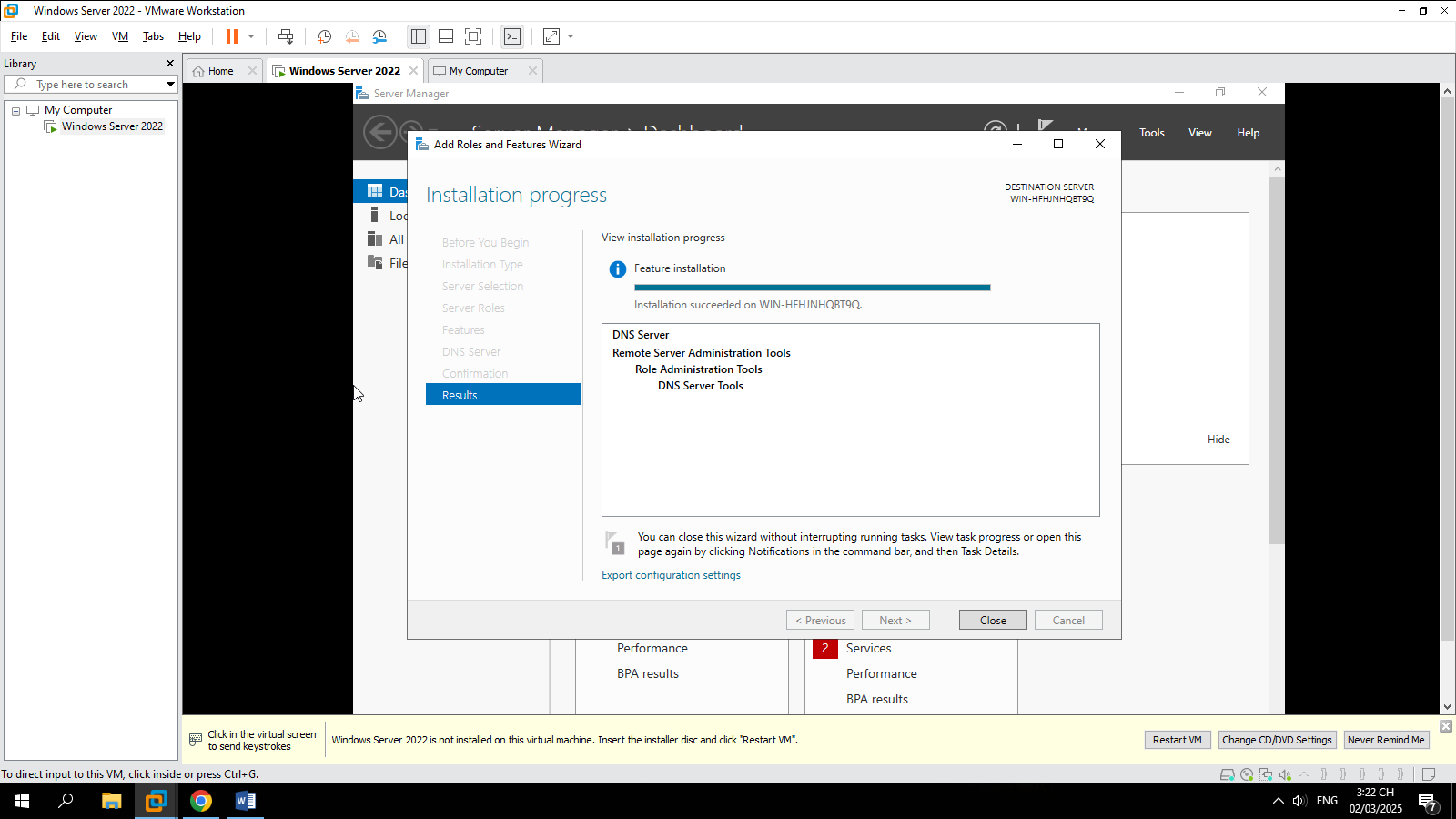
- B20: Trên thanh công cụ VMware vào VM/Send Ctrl + Alt + Del



# **4. DNS Server**

## **4.1. Installing and Configuring the DNS Service**

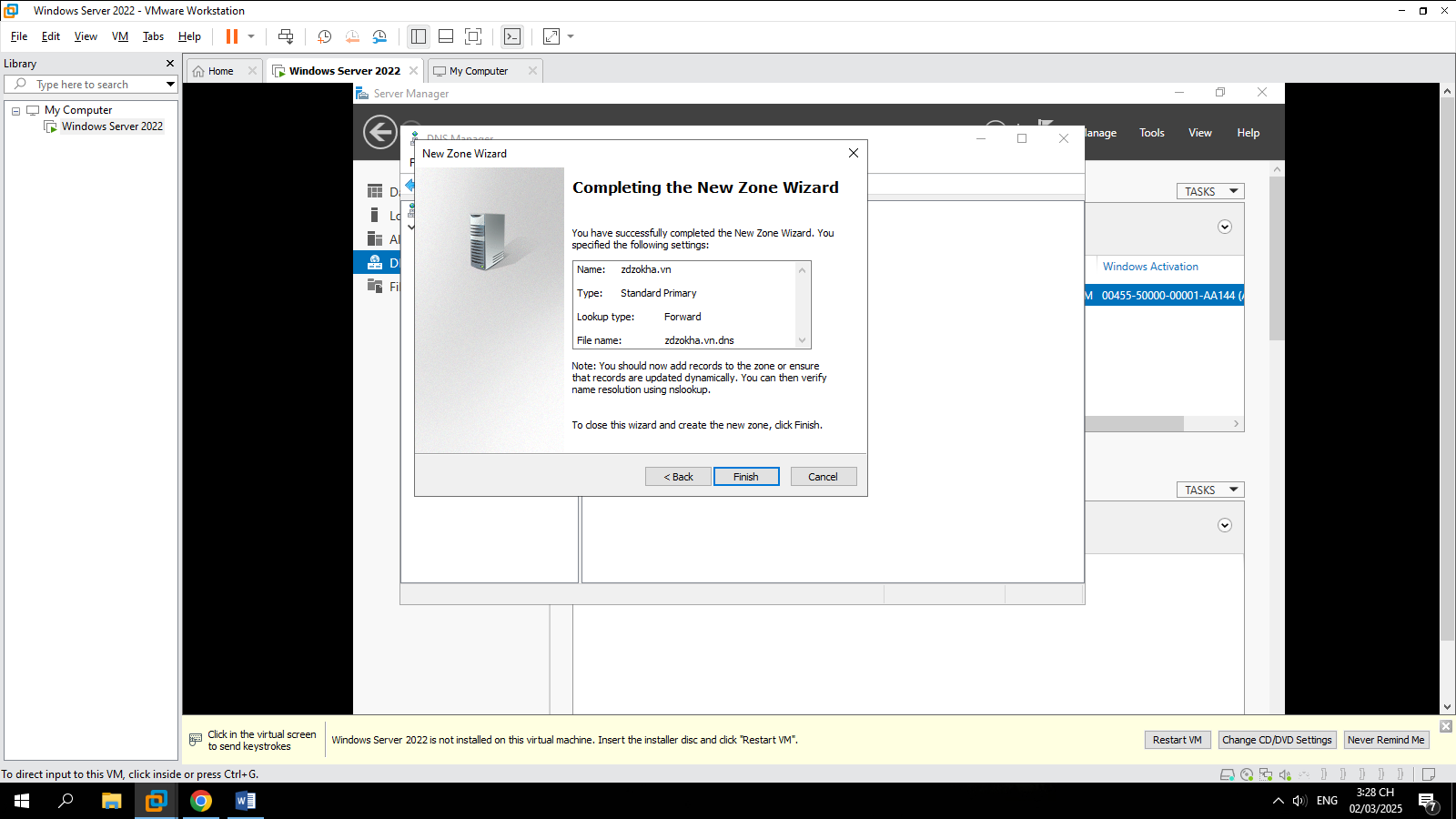
1. Mở Server Manager.
2. Trên bảng điều khiển Server Manager, nhấp vào liên kết Add Roles And Features.
3. Nếu màn hình Before You Begin xuất hiện, hãy nhấp vào Next.
4. Trên trang Selection type, chọn Role-Based Or Feature-Based Installation và nhấp vào Next.
5. Nhấp vào nút radio Select A Server From The Server Pool và chọn máy chủ trong phần Server Pool. Nhấp vào Next.
6. Nhấp vào DNS Server Item trong danh sách Server Role. Nếu cửa sổ bật lên xuất hiện thông báo rằng bạn cần thêm các tính năng bổ sung, hãy nhấp vào nút Add Features. Nhấp vào Next để tiếp tục.
7. Trên trang Add Features, chỉ cần nhấp vào Next.
8. Nhấp vào Next trên màn hình thông tin DNS Server.
9. Trên màn hình Confirm Installation, chọn hộp kiểm Restart The Destination Server Automatically If Required rồi nhấp vào nút Install.
10. Tại màn hình Installation progress, hãy nhấp vào Close sau khi máy chủ DNS được cài đặt.



1. Đóng Server Manager.

## **4.2. Configuring a Zone for Dynamic Updates**

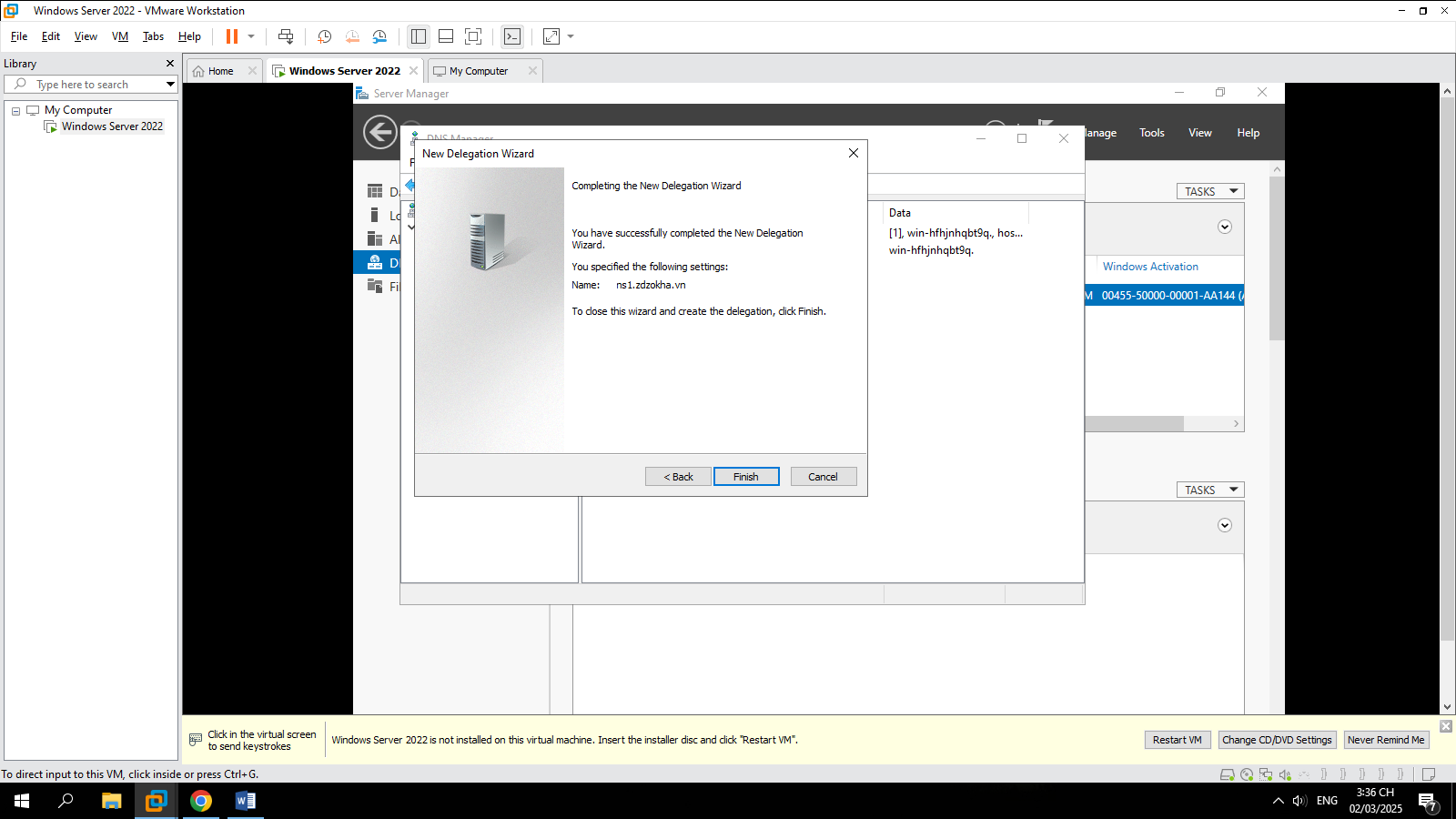
1. Mở snap-in quản lý DNS bằng cách chọn Server Manager. Khi đã vào Server Manager, hãy nhấp vào DNS ở phía bên trái. Trong cửa sổ Servers (màn hình trung tâm), nhấp chuột phải vào tên máy chủ của bạn và chọn DNS Manager.
2. Nhấp DNS Server để mở rộng và sau đó nhấp vào thư mục Forward Lookup Zones. Nhấp chuột phải vào thư mục Forward Lookup Zones và chọn New Zone
3. Tại màn hình New Zone Welcome, nhấp vào Next.
4. Tại màn hình Zone Type, chọn tùy chọn Primary Zone. Nếu máy chủ DNS của bạn cũng là bộ điều khiển miền, không đánh dấu vào hộp để lưu trữ vùng trong Active Directory. Nhấp vào Next khi bạn đã sẵn sàng.
5. Nhập tên vùng mới vào trường Zone Name và nhấp vào Next. (zdzokha.vn)
6. Để nguyên tên tệp vùng mặc định và nhấp vào Next.
7. Chọn nút radio Do Not Allow Dynamic Updates và nhấp vào Next.
8. Nhấp vào Finish để kết thúc trình hướng dẫn.



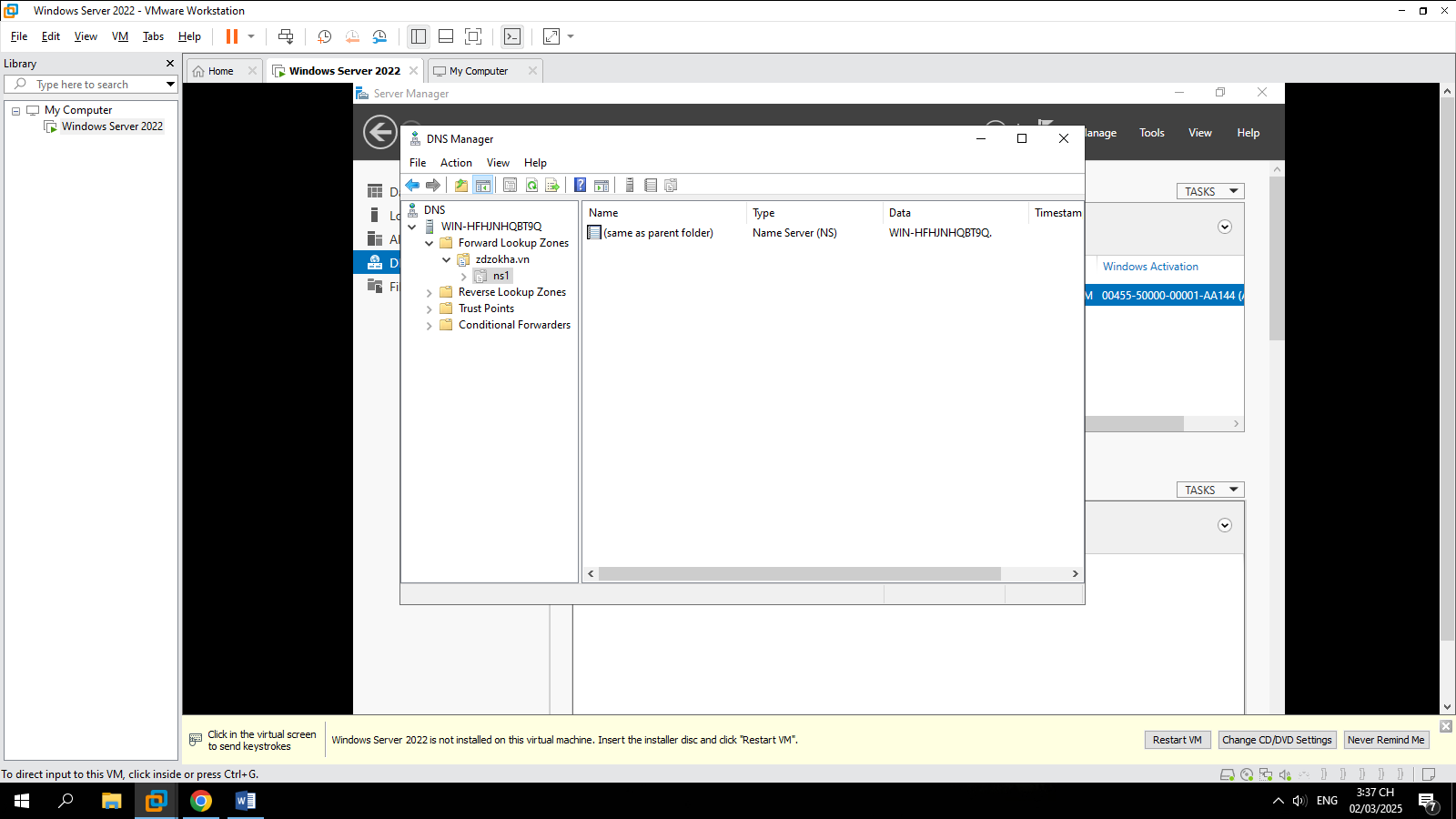
1. Nhấp chuột phải vào vùng bạn vừa tạo và chọn lệnh Properties.
2. Nhấp vào mũi tên xuống bên cạnh Dynamic Updates. Lưu ý rằng chỉ có hai tùy chọn (None và Nonsecure And Secure). Tùy chọn Secure Only không khả dụng vì bạn không sử dụng Active Directory Integrated. Đảm bảo Nonsecure And Secure được chọn.
3. Nhấp vào OK để đóng hộp Properties.
4. Đóng snap-in quản lý DNS.
5. Đóng snap-in Server Manager.

## **4.3. Creating a Delegated DNS Zone**

1. Mở snap-in quản lý DNS bằng cách chọn Server Manager. Khi đã vào Server Manager, hãy nhấp vào DNS ở phía bên trái. Trong cửa sổ Servers (màn hình ở giữa), nhấp chuột phải vào tên máy chủ của bạn và chọn DNS Manager.
2. Mở rộng DNS Server và định vị vùng bạn đã tạo
3. Nhấp chuột phải vào vùng và chọn lệnh New Delegation.
4. Trình hướng dẫn New Delegation xuất hiện. Nhấp vào Next để đóng trang trình hướng dẫn ban đầu.
5. Nhập ns1 (hoặc bất kỳ tên nào khác mà bạn thích) vào trường Delegated Domain của trang Delegated Domain Name. Đây là tên miền mà bạn muốn ủy quyền cho máy chủ DNS khác. Nó phải là một miền phụ của miền chính. Nhấp vào Next để hoàn tất bước này.
6. Khi trang Name Servers xuất hiện, hãy nhấp vào nút Add để thêm tên và địa chỉ IP của các máy chủ sẽ lưu trữ vùng mới được ủy quyền. Đối với mục đích của bài tập này, hãy nhập tên máy chủ mà bạn đã sử dụng trong bài tập trên. Nhấp vào nút Resolve để tự động giải quyết địa chỉ IP của tên miền này vào trường địa chỉ IP. Nhấp vào OK khi bạn hoàn tất. Nhấp vào Next để tiếp tục với trình hướng dẫn.



1. Nhấp vào nút Finish. Trình hướng dẫn New Delegation sẽ biến mất và bạn sẽ thấy vùng mới mà bạn vừa tạo xuất hiện bên dưới vùng bạn đã chọn ở bước 3. Biểu tượng thư mục của vùng mới được ủy quyền được vẽ màu xám để chỉ ra rằng quyền kiểm soát vùng đã được ủy quyền.



## **4.4. Manually Creating DNS Records**

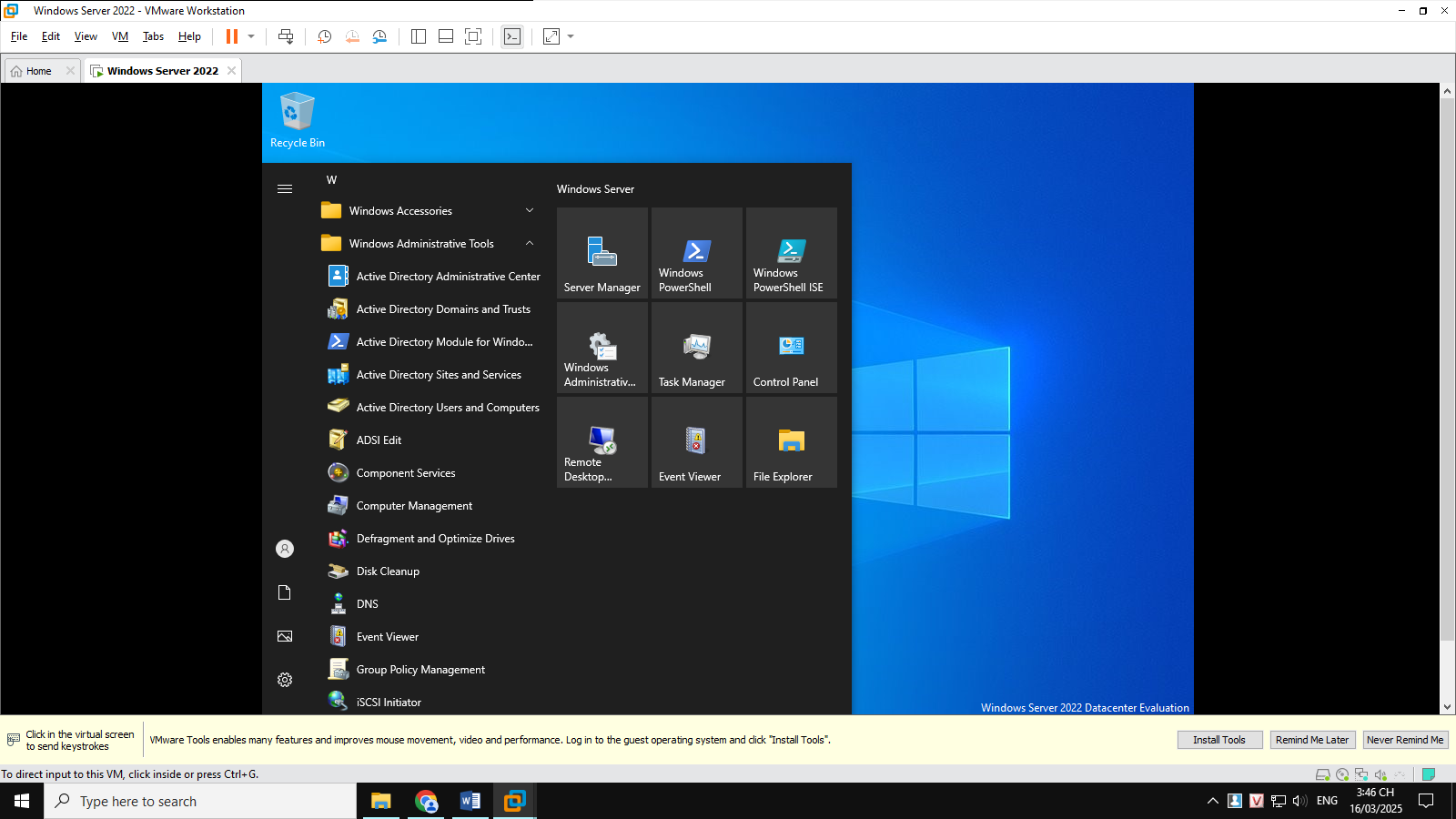
1. Mở snap-in quản lý DNS bằng cách chọn Server Manager. Khi đã vào Server Manager, hãy nhấp vào DNS ở phía bên trái. Trong cửa sổ Servers (màn hình trung tâm), nhấp chuột phải vào tên máy chủ của bạn và chọn DNS Manager.
2. Mở rộng DNS của bạn, nhấp chuột phải vào vùng của nó và chọn New Host (A record).
3. Nhập mailtest vào trường Name. Nhập địa chỉ IP vào trường IP Address. Nhấp vào nút Add Host.
4. Một hộp thoại xuất hiện thông báo rằng bản ghi máy chủ đã được tạo thành công. Nhấp vào OK. Nhấp vào Xong.
5. Nhấp chuột phải vào tên vùng của bạn và chọn New Mail Exchanger (MX).
6. Nhập mailtest vào trường Host Or Child Domain và nhập mailtest.zdzokha.vn (hoặc bất kỳ tên miền nào bạn đã sử dụng trong Bài tập trước) vào trường Fully-Qualified Domain Name (FQDN) Of Mail Server rồi nhấp vào OK. Lưu ý rằng bản ghi mới đã hiển thị.
7. Tiếp theo, tạo một bản ghi bí danh (hoặc CNAME) để trỏ đến máy chủ thư. (Giả sử rằng bạn đã có bản ghi A cho mailtest trong vùng của mình.) Nhấp chuột phải vào vùng của bạn và chọn New Alias ​​(CNAME).
8. Nhập mail vào trường Alias ​​Name.
9. Nhập mailtest.zdzokha.vn vào trường Fully-Qualified Domain Name (FQDN) For Target Host.
10. Nhấp vào nút OK.
11. Đóng snap-in quản lý DNS.

# 

# **5. Active Directory**

## **5.1. Promoting a Domain Controller**

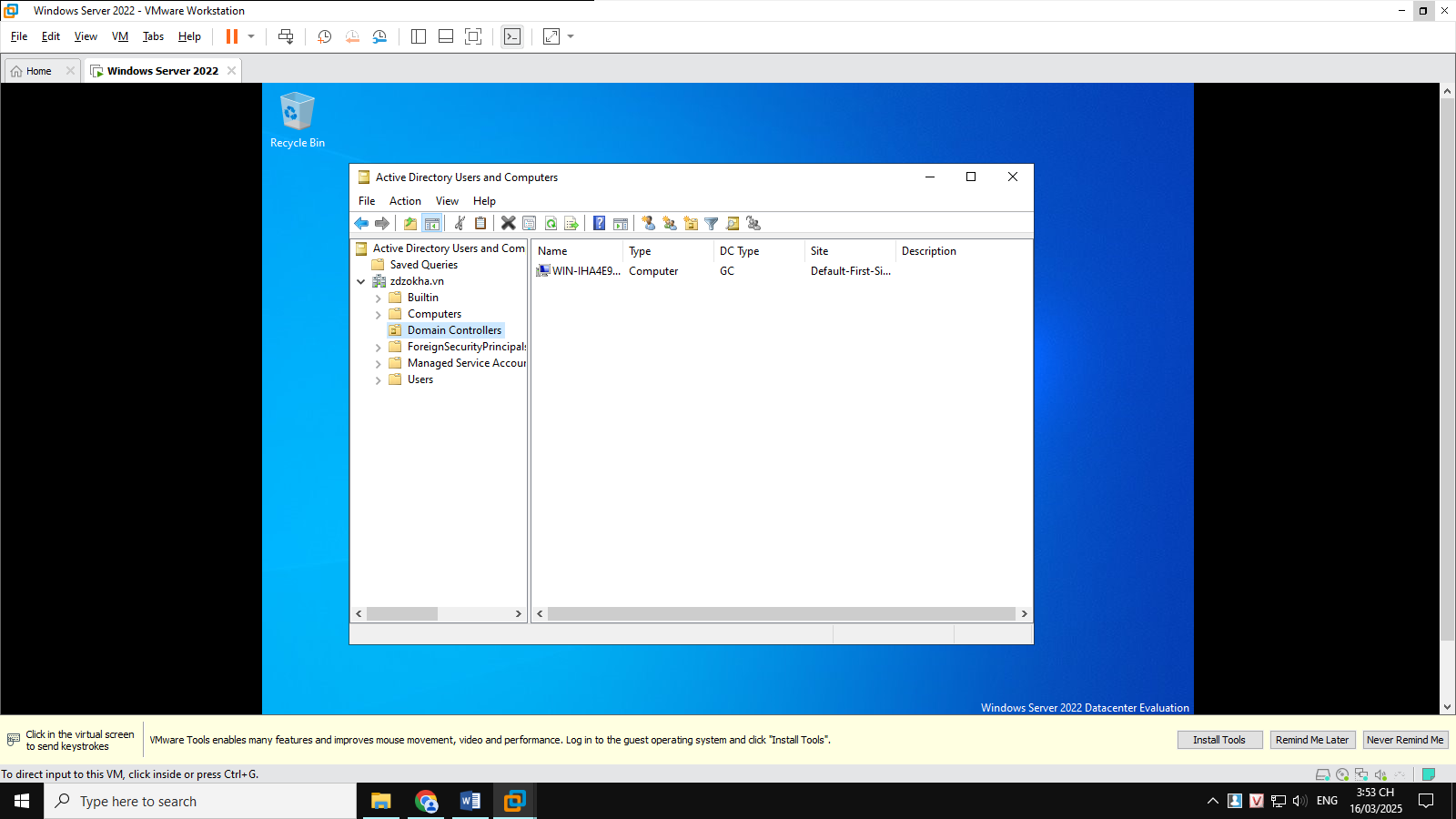
1. Cài đặt Active Directory Domain Services bằng cách nhấp vào liên kết Add Roles And Features trong chế độ xem Dashboard của Server Manager.
2. Tại màn hình Before You Begin, nhấp vào Next.
3. Màn hình Select Installation Type sẽ xuất hiện tiếp theo. Đảm bảo rằng nút radio Role-Based được chọn và nhấp vào Next.
4. Tại màn hình Select Destination Server, chọn Select a server from the server pool, chọn Server. Nhấp vào Next.
5. Tại màn hình Select Server Roles, nhấp vào hộp kiểm cho Active Directory Domain Services.
6. Sau khi bạn chọn hộp Active Directory Domain Services, một menu bật lên sẽ xuất hiện yêu cầu bạn cài đặt các tính năng bổ sung. Nhấp vào nút Add Features.
7. Nhấp vào Next.
8. Tại màn hình Select Features, chấp nhận các mặc định và nhấp vào Next.
9. Nhấp vào Next tại màn hình thông tin.
10. Nhấp vào nút Install tại màn hình Confirmation Installation.
11. Màn hình Installation Progress sẽ hiển thị cho bạn quá trình cài đặt đang diễn ra như thế nào.
12. Sau khi cài đặt hoàn tất, nhấp vào nút Close.
13. Ở cửa sổ bên trái, nhấp vào liên kết AD DS.
14. Nhấp vào liên kết More bên cạnh Configuration Required for Active Directory Domain Services.
15. Trong phần Post-­Deployment Configuration , hãy nhấp vào liên kết Promote This Server To A Domain Controller.
16. Tại thời điểm này, bạn sẽ cấu hình bộ điều khiển miền này. Bạn sẽ cài đặt bộ điều khiển miền mới trong một miền mới trong một khu rừng mới. Tại màn hình Deployment Configuration , hãy chọn nút radio Add A New Forest radio. Sau đó, bạn cần thêm tên miền gốc (ví dụ: dzokha.vn). Nhấp vào Next.
17. Tại màn hình Domain Controller Options, hãy đặt các tùy chọn sau:
    1. Function level: Windows Server 2012 R2 (cho cả hai).
    2. Xác minh rằng các hộp kiểm DNS và Global Catalog đã được chọn. Lưu ý rằng hộp kiểm RODC có màu xám. Điều này là do RODC cần lấy cơ sở dữ liệu Active Directory của chúng từ một bộ điều khiển miền khác. Vì đây là bộ điều khiển miền đầu tiên trong rừng nên không thể có RODC.
    3. Nhập P@ssw0rd làm mật khẩu. Sau đó, nhấp vàoNext.
18. Tại màn hình DNS Option, nhấp Next.
19. Tại màn hình Additional Options, chấp nhận tên miền NetBIOS mặc định và nhấp vào Next.
20. Tại màn hình Paths, chấp nhận các vị trí tệp mặc định và nhấp vào Next.
21. Tại màn hình Review Options, xác minh cài đặt của bạn và nhấp vào Next. Tại màn hình này, có nút View Script. Nút này cho phép bạn lấy tập lệnh PowerShell dựa trên các tính năng bạn vừa thiết lập.
22. Tại màn hình Prerequisites Check, hãy nhấp vào nút Install (miễn là không có lỗi). Cảnh báo vẫn ổn miễn là không có lỗi.
23. Sau khi cài đặt hoàn tất, máy sẽ tự động khởi động lại. Đăng nhập với tư cách là administrator.
24. Đóng Server Manager.
25. Nhấp vào nút Start trên bàn phím và chọn Administrative Tools.
26. Bạn sẽ thấy các snap-in MMC mới cho Active Directory.
27. Đóng cửa sổ Administrative Tools.



## **5.2. Viewing the Active Directory Event Log**

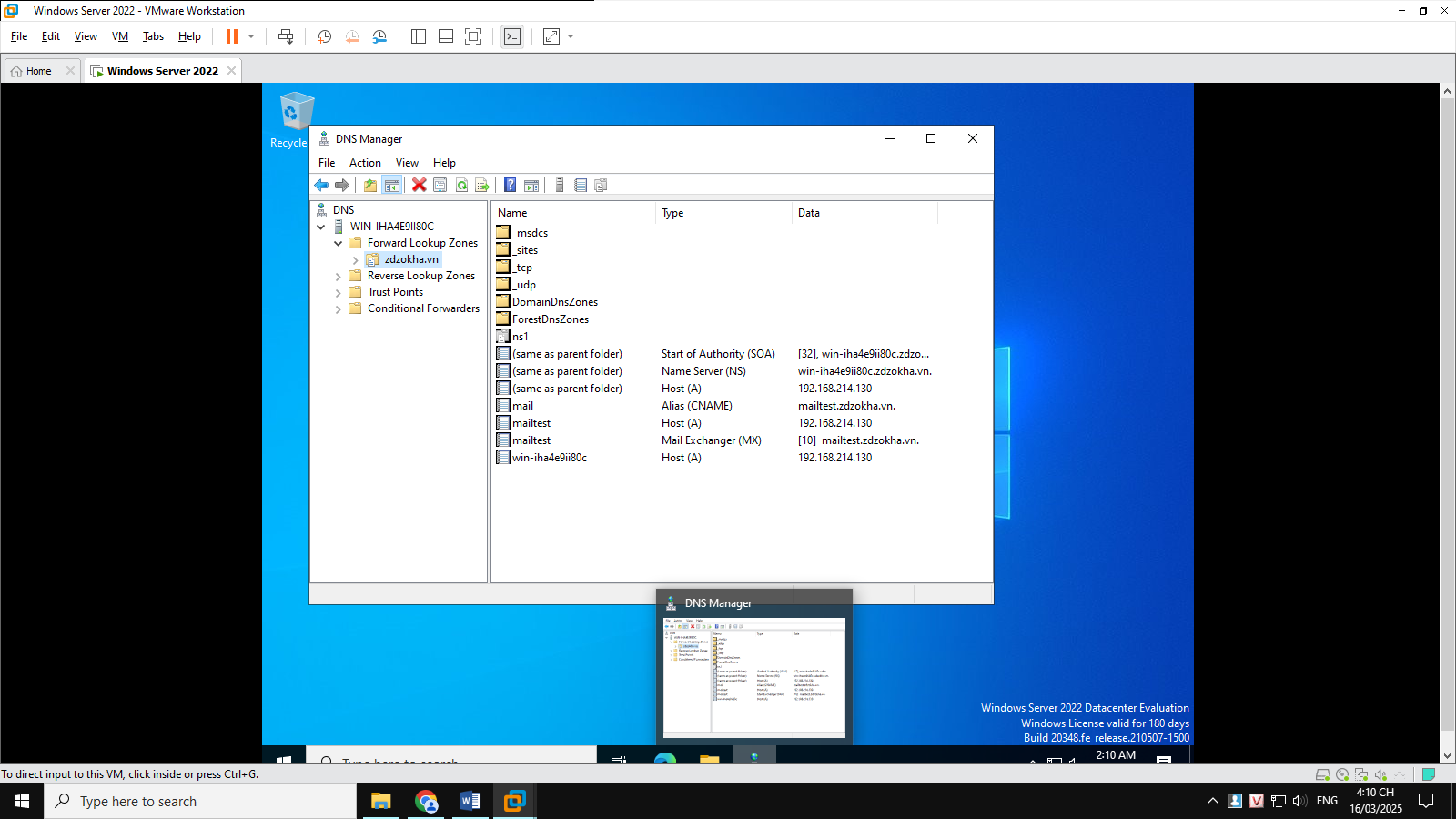
1. Mở Administrative Tools bằng cách nhấn phím Windows và chọn Administrative Tools.
2. Mở snap-in Event Viewer từ nhóm chương trình Administrative Tools.
3. Trong ngăn bên trái, bên dưới Applications And Services Logs, chọn Directory Service.
4. Trong ngăn bên phải, bạn có thể sắp xếp thông tin bằng cách nhấp vào tiêu đề cột. Ví dụ: bạn có thể nhấp vào cột Source để sắp xếp theo dịch vụ hoặc quy trình đã báo cáo sự kiện.
5. Nhấp đúp vào một sự kiện trong danh sách để xem thông tin chi tiết cho mục đó. Lưu ý rằng bạn có thể nhấp vào nút Copy để sao chép thông tin sự kiện vào Clipboard. Sau đó, bạn có thể dán dữ liệu vào tài liệu để tham khảo sau. Ngoài ra, bạn có thể di chuyển giữa các mục bằng cách sử dụng các mũi tên lên và xuống. Nhấp vào OK khi bạn đã xem xong một sự kiện.
6. Lọc danh sách sự kiện bằng cách nhấp chuột phải vào mục Directory Service trong ngăn bên trái và chọn Filter Current Log. Lưu ý rằng việc lọc không xóa các mục khỏi nhật ký sự kiện, nó chỉ hạn chế việc hiển thị chúng.
7. Để xác minh cài đặt Active Directory, hãy tìm các sự kiện liên quan đến việc khởi động đúng Active Directory, chẳng hạn như ID sự kiện. Ngoài ra, hãy đảm bảo kiểm tra bất kỳ thông báo lỗi hoặc cảnh báo nào vì chúng có thể chỉ ra sự cố với DNS hoặc các dịch vụ cần thiết khác.
8. Khi bạn đã xem xong thông tin trong Event Viewer, hãy đóng ứng dụng.

Một cách tốt để đảm bảo rằng Active Directory có thể truy cập được và hoạt động bình thường là chạy công cụ Active Directory Users and Computers. Bạn nên đảm bảo rằng tên miền bạn đã tạo xuất hiện trong danh sách. Bạn cũng nên nhấp vào thư mục Domain Controllers và đảm bảo rằng tên máy chủ cục bộ của bạn xuất hiện trong ngăn bên phải. Nếu cấu hình của bạn vượt qua hai lần kiểm tra này, Active Directory sẽ có mặt và được cấu hình.



## **5.5. Configuring DNS Integration with Active Directory**

1. Mở Administrative Tools bằng cách nhấn phím Windows và chọn Administrative Tools.
2. Mở snap-in DNS từ nhóm chương trình Administrative Tools.
3. Nhấp chuột phải vào biểu tượng của máy chủ DNS cục bộ và chọn Properties. Nhấp vào tab Security. Lưu ý rằng bây giờ bạn có thể chỉ định người dùng và nhóm nào có quyền truy cập để sửa đổi cấu hình của máy chủ DNS. Thực hiện bất kỳ thay đổi cần thiết nào và nhấp vào OK.
4. Mở rộng nhánh máy chủ cục bộ và thư mục Forward Lookup Zones.
5. Nhấp chuột phải vào tên miền Active Directory mà bạn đã tạo và chọn Properties.
6. Trên tab General, hãy xác minh rằng loại là Active Directory-Integrated và thông báo Data Is Stored In Active Directory được hiển thị. Nếu tùy chọn này hiện chưa được chọn, bạn có thể thay đổi bằng cách nhấp vào nút Change bên cạnh Type và chọn hộp kiểm Store The Zone In Active Directory ở phía dưới.
7. Xác minh rằng tùy chọn Dynamic Updates được đặt thành Secure Only. Điều này đảm bảo rằng tất cả các bản cập nhật cho cơ sở dữ liệu bản ghi tài nguyên DNS được thực hiện thông qua các tài khoản và quy trình Active Directory đã xác thực. Các tùy chọn khác là Nonsecure And Secure (chấp nhận tất cả các bản cập nhật) và None (để không cho phép cập nhật động).
8. Cuối cùng, hãy lưu ý rằng bạn có thể xác định quyền bảo mật ở cấp vùng bằng cách nhấp vào tab Security. Thực hiện bất kỳ thay đổi cần thiết nào và nhấp vào OK.



## **5.6. Creating an OU Structure**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/ Active Directory Users And Computers.
2. Nhấp chuột phải vào tên miền cục bộ và chọn New/Organizational Unit.
3. Nhập North America cho tên của OU đầu tiên. Bỏ chọn hộp Protect Container From Accidental Deletion và nhấp vào OK để tạo đối tượng này.
4. Tạo các OU cấp cao nhất sau bằng cách nhấp chuột phải vào tên miền và chọn New/Organizational Unit. Ngoài ra, hãy đảm bảo bỏ chọn Protect Container From Accidental Deletion cho tất cả các OU trong các bài tập này vì bạn sẽ xóa một số OU này trong các bài tập sau.
   1. Africa
   2. Asia
   3. Europe
   4. South America

Lưu ý rằng thứ tự bạn tạo OU không quan trọng. Trong bài tập này, bạn chỉ sử dụng phương pháp nhấn mạnh mối quan hệ phân cấp.

1. Tạo các OU cấp độ thứ hai sau đây trong OU North America bằng cách nhấp chuột phải vào OU North America và chọn New/Organizational Unit:
   1. Austin
   2. Boston
   3. Canada
   4. Chicago
   5. Corporate
   6. Los Angeles
   7. Mexico
   8. New York
   9. San Francisco
2. Tạo các OU sau theo OU Asia:
   1. China
   2. India
   3. Malaysia
   4. Vietnam
3. Tạo các OU sau theo OU Europe:
   1. France
   2. Germany
   3. Spain
   4. UK
4. Tạo các OU sau theo OU South America:
   1. Argentina
   2. Brazil
   3. Chile
   4. Peru
5. Tạo các OU cấp ba sau đây trong OU India bằng cách nhấp chuột phải vào India trong OU Asia và chọn New/Organizational Unit:
   1. Bombay
   2. New Delhi
6. Với Corporate của North America, tạo các OUs:
   1. Engineering
   2. HR
   3. Marketing
   4. Research
   5. Sales
7. Khi bạn hoàn tất việc tạo OU, hãy đóng Active Directory.

## **5.7. Modifying OU Structure**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Nhấp chuột phải vào OU Engineering (nằm trong North America/ Corporate) và nhấp vào Delete. Khi bạn được nhắc xác nhận, hãy nhấp vào Yes. Lưu ý rằng nếu OU này chứa các đối tượng, tất cả chúng cũng sẽ tự động bị xóa.
3. Nhấp chuột phải vào OU Research và chọn Rename. Nhập RD để đổi tên OU và nhấn Enter.
4. Nhấp chuột phải vào OU Sales và chọn Move. Trong hộp thoại Move, hãy mở rộng nhánh North America và nhấp vào OU New York. Nhấp vào OK để di chuyển OU.
5. Bạn sẽ sử dụng một phương pháp thay thế để di chuyển OU Marketing. Kéo OU Marketing và thả vào OU Chicago.
6. Khi bạn hoàn tất, hãy đóng công cụ quản trị Active Directory Users and Computers.

## **5.8. Using the Delegation of Control Wizard**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Nhấp chuột phải vào Corporate OU trong OU North America và chọn Delegate Control. Thao tác này sẽ khởi chạy Trình hướng dẫn Delegation of Control. Nhấp vào Next để bắt đầu cấu hình cài đặt bảo mật.
3. Trong trang Users Or Groups, nhấp vào nút Add. Trong trường Enter The Object Names To Select, nhập Account Operators và nhấp vào nút Check Names. Nhấp vào OK. Nhấp vào Next để tiếp tục.
4. Trong trang Tasks To Delegate, chọn Delegate The Following Common Tasks và đánh dấu kiểm bên cạnh các mục sau:
   1. Create, Delete, And Manage User Accounts
   2. Reset User Passwords And Force Password Change At Next Login
   3. Read All User Information
   4. Create, Delete, And Manage Groups
   5. Modify The Membership Of A Group
5. Nhấp vào Next để tiếp tục.
6. Sau đó, trang Completing The Delegation Of Control Wizard sẽ tóm tắt các thao tác bạn đã chọn. Để triển khai các thay đổi, hãy nhấp vào Finish.

## **5.9. Delegating Custom Tasks**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Nhấp chuột phải vào Corporate OU trong North America OU và chọn Delegate Control. Thao tác này sẽ khởi chạy Trình hướng dẫn Delegation of Control. Nhấp vào Next để bắt đầu thực hiện cài đặt bảo mật.
3. Trong trang Users Or Groups, nhấp vào nút Add. Trong trường Enter The Object Names To Select, nhập Server Operators và nhấp vào nút Check Names. Nhấp vào OK rồi nhấp vào Next để tiếp tục.
4. Trong trang Tasks To Delegate, chọn nút radio Create A Custom Task To Delegate và nhấp vào Next để tiếp tục.
5. Trong trang Active Directory Object Type, chọn Only The Following Objects In The Folder và đánh dấu kiểm bên cạnh các mục sau. (Bạn sẽ phải cuộn xuống để xem tất cả.)
   1. User Objects
   2. Computer Objects
   3. Contact Objects
   4. Group Objects
   5. Organizational Unit Objects
   6. Printer Objects
6. Nhấp vào Next để tiếp tục.
7. Trong trang Permissions, hãy đánh dấu kiểm bên cạnh tùy chọn General và đảm bảo các tùy chọn khác không được chọn. Lưu ý rằng nếu các đối tượng khác nhau trong lược đồ Active Directory của bạn có cài đặt thuộc tính cụ thể, bạn sẽ thấy các tùy chọn đó ở đây. Đánh dấu kiểm bên cạnh các mục sau:
   1. Create All Child Objects
   2. Read All Properties
   3. Write All Properties

Điều này cung cấp cho các thành viên của nhóm Server Operators khả năng tạo các đối tượng mới trong OU của Corporate và các quyền để đọc và ghi tất cả các thuộc tính cho các đối tượng này.

1. Nhấp vào Next để tiếp tục.
2. Trang Completing The Delegation Of Control Wizard cung cấp tóm tắt các thao tác bạn đã chọn. Để triển khai các thay đổi, hãy nhấp vào Finish.

## **5.10. Creating Active Directory Objects**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Mở rộng miền hiện tại để liệt kê các đối tượng hiện có trong đó. Đối với bài tập này, bạn sẽ sử dụng OU cấp hai và cấp ba có trong OU cấp cao nhất của North America.
3. Nhấp chuột phải vào OU Corporate và chọn New/User. Điền thông tin sau:
   1. First Name: Maria
   2. Initial: D
   3. Last Name: President
   4. Full Name: (giữ nguyên mặc định)
   5. User Logon Name: mdpresident (giữ nguyên tên miền mặc định) Nhấp vào Next để tiếp tục.
4. Nhập P@ssw0rd làm mật khẩu cho người dùng này rồi xác nhận. Lưu ý rằng bạn cũng có thể thay đổi cài đặt mật khẩu tại đây. Nhấp vào Next.
5. Bạn sẽ thấy tóm tắt thông tin người dùng. Nhấp vào Finish để tạo người dùng mới.
6. Nhấp vào container RD và tạo một người dùng khác trong vùng chứa đó với thông tin sau:
   1. First Name: John
   2. Initial: Q
   3. Last Name: Adams
   4. Full Name: (giữ nguyên mặc định)
   5. User Logon Name: jqadams (giữ nguyên tên miền mặc định)

Nhấp vào Next để tiếp tục.

1. Gán mật khẩu P@ssw0rd. Nhấp vào Next rồi nhấp vào Finish để tạo người dùng.
2. Nhấp chuột phải vào OU RD và chọn New/Contact. Sử dụng thông tin sau để điền vào các thuộc tính của đối tượng Contact:
   1. First Name: Jane
   2. Initials: R
   3. Last Name: Admin
   4. Display Name: jradmin

Nhấp vào OK để tạo đối tượng Contact mới.

1. Nhấp chuột phải vào RD OU và chọn New/Shared Folder. Nhập Software cho tên và \\server1\applications cho đường dẫn mạng (còn được gọi là đường dẫn Universal Naming Convention [UNC]). Lưu ý rằng bạn có thể tạo đối tượng ngay cả khi tài nguyên này (máy chủ vật lý) không tồn tại. Nhấp vào OK để tạo đối tượng Shared Folder
2. Nhấp chuột phải vào OU HR và chọn New/Group. Nhập All Users cho tên nhóm. Không thay đổi giá trị trong trường Group Name (Pre–Windows 2000). Đối với Group Scope, chọn Global và đối với Group Type, chọn Security. Để tạo nhóm, nhấp vào OK.
3. Nhấp chuột phải vào OU Sales và chọn New/Computer. Nhập Workstation1 cho tên máy tính. Lưu ý rằng Computer name (pre–Windows 2000) được tự động điền và theo mặc định, các thành viên của nhóm Domain Admins là những người duy nhất có thể thêm máy tính này vào miền. Đánh dấu kiểm vào hộp Assign This Computer Account As A PreWindows 2000 Computer rồi nhấp vào OK để tạo đối tượng Computer.
4. Đóng công cụ Active Directory Users and Computers.

## **5.11. Creating a User Template**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Mở rộng miền hiện tại để liệt kê các đối tượng có trong đó. Đối với bài tập này, bạn sẽ sử dụng Sales OU. Nhấp chuột phải vào Sales OU và chọn New/User.
3. Sử dụng các thuộc tính sau:
   1. First Name: Sales
   2. Last Name: Template
   3. Username: sales\_template
   4. Password: P@ssw0rd
4. Nhấp vào Next rồi nhấp vào Finish.
5. Trong cửa sổ bên phải, nhấp đúp vào người dùng Sales Template để mở properties..
6. Trên tab General, hãy hoàn thành các mục sau:
   1. Description: Template Account
   2. Office: Corporate
   3. Telephone: 999-999-9999
   4. Email: Sales@abc.com
   5. Web: www.abc.com
7. Nhấp vào tab e Profile. Trong trường Profile Path, nhập \\ServerA\%username%.
8. Trên tab Members Of, nhấp vào nút Add. Tại hộp Enter The Object Name To Select, nhập Administrator và nhấp vào nút Check Names. (Thông thường, bạn sẽ không thêm nhân viên bán hàng vào nhóm Administrators, nhưng bạn đang làm như vậy chỉ dành cho bài tập này.) Nhấp vào OK.
9. Nhấp vào tab Account. Cuộn xuống trong hộp Account Options và chọn hộp kiểm Account Is Disabled.
10. Nhấp vào OK trong cửa sổ Properties của người dùng để quay lại Sales OU.
11. Nhấp chuột phải vào tài khoản Sales Template và chọn Copy.
12. Nhập thông tin sau:
    1. First Name: Jenny
    2. Last Name: Sales
    3. Username: jsales
    4. Password: P@ssw0rd Bỏ chọn hộp kiểm Account Is Disabled.
13. Trong cửa sổ bên phải, nhấp đúp vào người dùng Jenny Sales để mở properties.
14. Xem tab Members Of, tab General và tab Profile, bạn sẽ thấy một số trường đã được điền sẵn (bao gồm cả nhóm Administrators).
15. Đóng Jenny Sales Properties và thoát khỏi Active Directory Users and Computers.

## **5.12. Managing Object Properties**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Mở rộng tên miền và chọn vùng chứa RD. Nhấp chuột phải vào tài khoản người dùng John Q. Adams và chọn Properties.
3. Tại đây, bạn sẽ thấy các tab Properties khác nhau cho tài khoản Người dùng. Thực hiện một số thay đổi cấu hình dựa trên sở thích cá nhân của bạn. Nhấp vào OK để tiếp tục.
4. Chọn OU RD. Nhấp chuột phải vào nhóm All Users và nhấp vào Properties. Trong hộp thoại All Users Properties, bạn sẽ có thể sửa đổi tư cách thành viên của nhóm. Nhấp vào tab Members rồi nhấp vào Add. Thêm tài khoản người dùng Maria D. President và John Q. Adams vào nhóm. Nhấp vào OK để lưu cài đặt rồi nhấp vào OK để chấp nhận các sửa đổi của nhóm.
5. Chọn OU Sales. Nhấp chuột phải vào đối tượng Workstation1 Computer. Lưu ý rằng bạn có thể chọn disable tài khoản hoặc reset tài khoản (để cho phép máy tính khác tham gia miền dưới cùng tên đó). Từ menu ngữ cảnh, chọn Properties. Bạn sẽ thấy các thuộc tính cho đối tượng Computer. Kiểm tra các tùy chọn khác nhau và thực hiện thay đổi dựa trên sở thích cá nhân của bạn. Sau khi bạn đã kiểm tra các tùy chọn có sẵn, hãy nhấp vào OK để tiếp tục.
6. Chọn Corporate OU. Nhấp chuột phải vào tài khoản người dùng Maria D. President và chọn Reset Password. Bạn sẽ được nhắc nhập mật khẩu mới, sau đó bạn sẽ được yêu cầu xác nhận. Lưu ý rằng bạn cũng có thể buộc người dùng thay đổi mật khẩu này khi đăng nhập lần tiếp theo và bạn cũng có thể mở khóa tài khoản của người dùng từ đây. Đối với bài tập này, không nhập mật khẩu mới; chỉ cần nhấp vào Cancel.
7. Đóng công cụ Active Directory Users and Computers.

## **5.13. Moving Active Directory Objects**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Mở rộng tên miền.
3. Chọn Sales OU (bên dưới New York OU), nhấp chuột phải vào Workstation1 và chọn Move. Một hộp thoại xuất hiện. Chọn RD OU và nhấp vào OK để di chuyển đối tượng Computer đến vùng chứa đó.
4. Nhấp vào RD OU và xác minh rằng Workstation1 đã được di chuyển.
5. Đóng công cụ Active Directory Users and Computers.

## **5.14. Resetting an Existing Computer Account**

1. Mở Active Directory Users and Computers bằng cách nhấp vào Start/ Administrative Tools/Active Directory Users And Computers.
2. Mở rộng tên miền.
3. Nhấp vào RD OU rồi nhấp chuột phải vào tài khoản máy tính Workstation1.
4. Chọn Reset Account từ menu ngữ cảnh. Nhấp vào Yes để xác nhận lựa chọn của bạn. Nhấp vào OK tại dấu nhắc thành công.
5. Khi bạn đặt lại tài khoản, bạn sẽ ngắt kết nối giữa máy tính và miền. Vì vậy, sau khi thực hiện bài tập này, hãy kết nối lại máy tính với miền nếu bạn muốn máy tính tiếp tục hoạt động trên mạng.

Để kếy nối lại máy tính với tên miền chạy lệnh sau trên máy tính cục bộ:

Test-ComputerSecureChannel -Repair -Server \_msdcs.dzokha.vn

## **5.15. Creating and Publishing a Printer bỏ**

1. Nhấp vào phím Windows trên bàn phím và chọn Control Panel.
2. Nhấp vào Devices And Printers/Add A Printer. Thao tác này sẽ khởi chạy Add Printer Wizard. Sau đó, nhấp vào nút Next.
3. Trong trang Choose A Local Or Network Printer, chọn Add A Local Printer. Thao tác này sẽ tự động đưa bạn đến trang tiếp theo. Nếu không, hãy nhấp vào Next.
4. Trên trang Choose A Printer Port, chọn Use An Existing Port. Từ danh sách thả xuống bên cạnh tùy chọn đó, hãy đảm bảo LPT1: (Printer Port) được chọn. Nhấp vào Next.
5. Trên trang Install The Printer Driver, chọn Generic cho nhà sản xuất. Đối với máy in, hãy tô sáng Generic/Text Only. Nhấp vào Next.
6. Trên trang Type A Printer Name, nhập Text Printer. Bỏ chọn hộp Set As The Default Printer rồi nhấp vào Next.
7. Màn hình Installing Printer xuất hiện. Sau khi hệ thống hoàn tất, trang Printer Sharing xuất hiện. Đảm bảo hộp có nhãn “Share this printer so that others on your network can find and use it” được chọn và chấp nhận tên chia sẻ mặc định là Text Printer.
8. Trong phần Location, nhập Building 203 và trong phần Comment, thêm chú thích sau: This is a text-only Printer. Nhấp vào Next.
9. Trên trang You’ve Successfully Added Text Printer, nhấp vào Finish.
10. Tiếp theo, bạn cần xác minh rằng máy in sẽ được liệt kê trong Active Directory. Nhấp chuột phải vào biểu tượng Text Printer và chọn Printer Properties.
11. Chọn tab Sharing và đảm bảo rằng hộp List In The Directory được chọn. Lưu ý rằng bạn cũng có thể thêm trình điều khiển máy in bổ sung cho các hệ điều hành khác bằng cách sử dụng tab này. Nhấp vào OK để chấp nhận các thiết lập.

## **5.16. Creating and Publishing a Shared Folder**

1. Tạo một thư mục mới trong thư mục gốc của phân vùng C: và đặt tên là Test Share. Để thực hiện việc này, hãy nhấp vào liên kết File Explorer trên thanh công cụ.
2. Nhấp chuột phải vào thư mục Test Share. Chọn Give access to/Specific People...
3. Trong hộp thoại Network access, nhập tên của những người dùng mà bạn muốn chia sẻ thư mục này. Trong hộp trên cùng, nhập Everyone rồi nhấp vào Add. Lưu ý rằng Everyone xuất hiện trong hộp dưới cùng. Nhấp vào cột Permission Level bên cạnh Everyone và chọn Read/Write. Chọn Share
4. Bạn sẽ thấy thông báo rằng thư mục của bạn đã được chia sẻ. Nhấp vào Done.
5. Nhấp vào phím Windows trên bàn phím và chọn Administrative Tools.
6. Mở công cụ Active Directory Users and Computers. Mở rộng tên miền hiện tại và nhấp chuột phải vào RD OU. Chọn New/Shared Folder
7. Trong hộp thoại New Object - Shared Folder, nhập Shared Folder Test cho tên thư mục. Sau đó nhập đường dẫn UNC đến chia sẻ (ví dụ: \\server1\Test Share). Nhấp vào OK để tạo chia sẻ.

# **6. DHCP**

## **6.1. Installing the DHCP Service**

1. Chọn Server Manager bằng cách nhấp vào biểu tượng Server Manager trên Taskbar.
2. Nhấp vào Add Roles And Features.
3. Chọn cài đặt Role-based or feature-based installation và nhấp vào Next.
4. Chọn máy chủ của bạn và nhấp vào Next.
5. Chọn DHCP Server và nhấp vào Next.
6. Tại màn hình Features, nhấp vào Next.
7. Nhấp vào Next tại màn hình DHCP Server.
8. Tại màn hình confirmation DHCP, nhấp vào nút Install.
9. Khi quá trình cài đặt hoàn tất, nhấp vào nút Close.
10. Ở phía bên trái, nhấp vào liên kết DHCP.
11. Nhấp vào liên kết More bên cạnh Configuration Required For DHCP Server.
12. Trong Action, nhấp vào Complete DHCP Configuration.
13. Tại trang DHCP Description, nhấp vào Commit.
14. Nhấp vào Close tại màn hình Summary.
15. Đóng Server Manager.

## **6.2. Authorizing a DHCP Server**

1. Từ Administrative Tools, chọn DHCP để mở DHCP snap-in.
2. Nhấp chuột phải vào máy chủ bạn muốn cấp quyền và chọn lệnh Authorize.
3. Đợi vài giây rồi nhấn F5. Thao tác này sẽ làm mới máy chủ. Bây giờ bạn sẽ thấy các mũi tên xuống màu đỏ giờ đã chuyển sang màu xanh lá cây.

## **6.3. Unauthorizing a DHCP Server**

1. 1. Từ Administrative Tools, chọn DHCP để mở DHCP snap-in.
2. Nhấp chuột phải vào máy chủ bạn muốn cấp quyền và chọn lệnh Unauthorize.
3. Đợi vài giây rồi nhấn F5. Thao tác này sẽ làm mới máy chủ. Bây giờ bạn sẽ thấy các mũi tên màu xanh lá cây giờ đã chuyển sang màu đỏ.
4. Bây giờ chúng ta hãy cấp lại quyền cho máy chủ. Nhấp chuột phải vào máy chủ và chọn lệnh Authorize. Đợi vài giây rồi nhấn F5.

## **6.4. Creating a New Scope**

1. Mở snap-in DHCP bằng cách chọn Administrative Tools/DHCP.
2. Nhấp chuột phải vào thư mục IPv4 và chọn New Scope. New Scope Wizard xuất hiện.
3. Nhấp vào nút Next trên trang chào mừng.
4. Nhập tên và mô tả cho phạm vi mới của bạn và nhấp vào nút Next.
5. Trên trang IP Address Range, nhập 192.168.0.2 làm địa chỉ IP bắt đầu cho phạm vi và 192.168.0.250 làm địa chỉ IP kết thúc. Giữ nguyên các điều khiển mặt nạ mạng con (mặc dù khi tạo phạm vi trên mạng sản xuất, bạn có thể cần thay đổi chúng). Nhấp vào nút Next.
6. Trên trang Add Exclusions And Delay, nhấp vào Next mà không thêm bất kỳ địa chỉ hoặc độ trễ nào bị loại trừ.
7. Trên trang Lease Duration, đặt lease duration là 3 ngày và nhấp vào nút Next.
8. Trên trang Configure DHCP Options, nhấp vào nút Next để cho biết bạn muốn cấu hình các tùy chọn mặc định cho phạm vi này.
9. Trên trang Router (Default Gateway), nhập 192.168.0.1 cho địa chỉ IP của router rồi nhấp vào nút Add. Sau khi thêm địa chỉ, nhấp vào nút Next.
10. Trên trang Domain Name And DNS Servers, nhập địa chỉ IP của máy chủ DNS trên mạng của bạn vào trường IP Address (ví dụ: bạn có thể nhập 192.168.0.251) và nhấp vào nút Add. Nhấp vào nút Next.
11. Trên trang WINS Servers, nhấp vào nút Next để bỏ chọn tùy chọn WINS.
12. Trên trang Activate Scope, nếu mạng của bạn hiện đang sử dụng phạm vi 192.168.0.x, hãy chọn Yes, I Want To Activate This Scope Now. Nhấp vào nút Next.
13. Khi trang tóm tắt của trình hướng dẫn xuất hiện, hãy nhấp vào nút Finish để tạo phạm vi

## **6.5. Creating a Superscope**

1. Mở snap-in DHCP bằng cách chọn Administrative Tools/DHCP.
2. Làm theo hướng dẫn trong Bài tập trên để tạo hai scopes: một cho 192.168.0.2 đến 192.168.0.127 và một cho 192.168.1.12 đến 192.168.1.127.
3. Nhấp chuột phải vào IPv4 và chọn lệnh New Superscope. New Superscope Wizard xuất hiện. Nhấp vào nút Next.
4. Trên trang Superscope Name, đặt tên cho siêu phạm vi của bạn và nhấp vào nút Next.
5. Trang Select Scopes xuất hiện, liệt kê tất cả các phạm vi trên máy chủ hiện tại. Chọn hai phạm vi bạn đã tạo ở bước 2, sau đó nhấp vào nút Next.
6. Trang tóm tắt của trình hướng dẫn xuất hiện. Nhấp vào nút Finish để tạo phạm vi của bạn.
7. Xác minh rằng siêu phạm vi mới của bạn xuất hiện trong snap-in DHCP.

## **6.6. Creating a New Multicast Scope**

1. Mở snap-in DHCP bằng cách chọn Administrative Tools/DHCP.
2. Nhấp chuột phải vào IPv4 và chọn New Multicast Scope. New Multicast Scope Wizard xuất hiện. Nhấp vào nút Next trên trang chào mừng.
3. Trong trang Multicast Scope Name, hãy đặt tên cho phạm vi multicast của bạn (và thêm mô tả nếu bạn muốn). Nhấp vào nút Next.
4. Trang IP Address Range xuất hiện. Nhập địa chỉ IP bắt đầu là 224.0.0.0 và địa chỉ IP kết thúc là 224.255.0.0. Điều chỉnh TTL thành 1 để đảm bảo không có gói multicast nào thoát khỏi phân đoạn mạng cục bộ của bạn. Nhấp vào nút Next khi bạn hoàn tất.
5. Trang Add Exclusions xuất hiện; nhấp vào nút Next của trang này.
6. Trang Lease Duration xuất hiện. Vì các địa chỉ đa hướng được sử dụng cho video và âm thanh, thông thường bạn sẽ để các chỉ định phạm vi đa hướng lâu hơn một chút so với phạm vi đơn hướng thông thường, do đó lease mặc định là 30 ngày (thay vì 8 ngày đối với phạm vi đơn hướng). Nhấp vào nút Next.
7. Trình hướng dẫn sẽ hỏi bạn xem bạn có muốn kích hoạt phạm vi ngay bây giờ không. Nhấp vào nút tùy chọn Không rồi nhấp vào nút Next.
8. Trang tóm tắt của trình hướng dẫn sẽ xuất hiện; nhấp vào nút Hoàn tất để tạo phạm vi của bạn
9. Xác minh rằng phạm vi đa hướng mới của bạn xuất hiện trong snap-in DHCP.

## **6.7. Enabling DHCP-DNS Integration**

1. Mở snap-in DHCP bằng cách chọn Administrative Tools/DHCP.
2. Nhấp chuột phải vào mục IPv4 và chọn Properties.
3. Hộp thoại Server Properties xuất hiện. Nhấp vào tab DNS.
4. Xác minh rằng hộp kiểm có nhãn Enable DNS Dynamic Updates According To The Settings Below được chọn và xác minh rằng nút radio có nhãn Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients được chọn.
5. Xác minh rằng hộp kiểm có nhãn Discard A And PTR Records When Lease Is Deleted được chọn. Nếu không, hãy chọn hộp kiểm đó.
6. Nhấp vào nút OK để áp dụng các thay đổi của bạn và đóng hộp thoại Server Properties.

## **6.8. Configuring DHCP Filtering**

1. Mở DHCP Management Console.
2. Mở rộng IPv4 cho đến khi bạn đến đối tượng bộ lọc Deny trong phân cấp DHCP của bạn.
3. Nhấp chuột phải vào đối tượng bộ lọc Deny và chọn New Filter.
4. Nhập địa chỉ MAC của thiết bị bạn muốn loại trừ khỏi mạng của mình, cung cấp mô tả như Unwanted Device, nhấp vào Add, sau đó nhấp vào Close.
5. Nhấp chuột phải vào bộ lọc Deny và chọn Enable để hoàn tất bài tập này.

## **6.9. Enabling DHCP Name Protection**

1. Mở DHCP Management Console.
2. Nhấp chuột phải vào IPv4 và chọn Properties.
3. Hộp thoại Server Properties xuất hiện. Nhấp vào tab DNS.
4. Xác minh rằng tùy chọn Enable DNS Dynamic Updates According To The Settings Below được chọn và xác minh rằng nút radio có nhãn Dynamically Update DNS A And PTR Records Only If Requested By The DHCP Clients được chọn.
5. Xác minh rằng tùy chọn Discard A And PTR Records When Lease Is Deleted được chọn. Nếu không, hãy chọn tùy chọn này.
6. Nhấp vào Configure bên dưới Name Protection và chọn Enable Name Protection.
7. Nhấp vào OK hai lần để hoàn tất bài tập này.

Bảo vệ tên của máy được DHCP cho thuê khỏi bị ghi đè bởi máy khác có cùng tên trong quá trình cập nhật động DNS.

# **10. Group Policy**

## **10.1. Creating a Group Policy Object Using the GPMC**

1. Nhấp vào nút Windows và chọn Administrative Tools/Group Policy Management. Công cụ Group Policy Management sẽ mở ra.
2. Mở rộng các vùng chứa Forest, Domains, tên miền của bạn và North America. Nhấp chuột phải vào Corporate OU rồi chọn Create A GPO In This Domain, And Link It Here.
3. Khi hộp thoại New GPO xuất hiện, nhập Warning Box vào trường Name. Nhấp OK.
4. New GPO sẽ được liệt kê ở bên phải cửa sổ Group Policy Management. Nhấp chuột phải vào GPO và chọn Edit.
5. Trong Group Policy Management Editor, hãy mở rộng các mục sau: Computer Configuration/Policies/Windows Settings/Security Settings/ Local Policies/Security Options. Ở bên phải, cuộn xuống và nhấp đúp vào Interactive Logon: Message Text For Users Attempting To Log On.
6. Nhấp vào hộp Define This Policy Setting In The Template. Trong hộp văn bản, nhập Unauthorized use of this machine is prohibit rồi nhấp OK. Đóng GPO và trở về màn hình chính của GPMC.
7. Bên dưới tên miền (trong GPMC), nhấp chuột phải vào Group Policy Objects và chọn New.
8. Khi hộp thoại New GPO xuất hiện, nhập Unlinked Test GPO vào trường Name. Nhấp OK.
9. Ở bên phải, GPO mới sẽ xuất hiện. Nhấp chuột phải vào Unlinked Test GPO và chọn Edit.
10. Trong phần User Configuration, nhấp Policies/Administrative Templates/ Desktop. Ở bên phải, nhấp đúp vào Hide And Disable All Items On The Desktop rồi nhấp vào Enabled. Nhấp OK rồi đóng GPMC.

## **10.2. Linking Existing GPOs to Active Directory**

1. Mở Group Policy Management Console.
2. Mở rộng các container Forest và Domain và nhấp chuột phải vào Africa OU.
3. Chọn Link An Existing GPO.
4. Hộp thoại Select GPO xuất hiện. Nhấp vào Unlinked Test GPO và nhấp vào OK.
5. Đóng Group Policy Management Console.

## **10.3. Filtering Group Policy Using Security Groups**

1. Mở công cụ quản trị Active Directory Users and Computers.
2. Tạo một OU mới có tên là Group Policy Test.
3. Tạo hai nhóm bảo mật toàn cầu mới trong OU Group Policy Test và đặt tên là PolicyEnabled và PolicyDisabled.
4. Thoát khỏi Active Directory Users and Computers và mở GPMC.
5. Nhấp chuột phải vào OU Group Policy Test và chọn Link An Existing GPO.
6. Chọn Unlinked Test GPO và nhấp vào OK.
7. Mở rộng OU Group Policy Test để bạn có thể thấy GPO (Unlinked Test GPO) bên dưới OU.
8. Nhấp vào tab Delegation rồi nhấp vào nút Advanced ở góc dưới bên phải của cửa sổ.
9. Nhấp vào nút Add và nhập PolicyEnabled vào trường Enter The Object Names To Select. Nhấp vào nút Check Names. Sau đó nhấp vào OK.
10. Thêm một nhóm có tên PolicyDisabled theo cách tương tự.
11. Làm nổi bật nhóm PolicyEnabled và chọn Allow cho quyền Read và Apply Group Policy. Điều này đảm bảo rằng người dùng trong nhóm PolicyEnabled sẽ bị ảnh hưởng bởi chính sách này.
12. Làm nổi bật nhóm PolicyDisabled và chọn Deny cho quyền Read và Apply Group Policy. Điều này đảm bảo rằng người dùng trong nhóm PolicyDisabled sẽ không bị ảnh hưởng bởi chính sách này.
13. Nhấp vào OK. Bạn sẽ thấy một thông báo nêu rằng bạn đang chọn sử dụng quyền Deny và quyền Deny có quyền ưu tiên hơn các mục Allow. Nhấp vào nút Yes để tiếp tục.
14. Khi bạn hoàn tất, hãy đóng công cụ GPMC.

## **10.4. Delegating Administrative Control of Group Policy**

1. Mở công cụ Active Directory Users and Computers.
2. Mở rộng miền cục bộ và tạo người dùng có tên Policy Admin trong OU Group Policy Test.
3. Thoát khỏi Active Directory Users and Computers và mở GPMC.
4. Nhấp vào OU Group Policy Test và chọn tab Delegation.
5. Nhấp vào nút Thêm. Trong trường Enter The Object Name To Select, nhập Policy Admin và nhấp vào nút Check Names.
6. Hộp thoại Add Group Or User xuất hiện. Trong danh sách thả xuống Permissions, hãy đảm bảo rằng mục có nhãn Edit Settings, Delete, Modify Security được chọn. Nhấp vào OK.
7. Tại thời điểm này, bạn sẽ thấy cửa sổ Group Policy Test Delegation. Nhấp vào nút Nâng cao ở góc dưới bên phải.
8. Đánh dấu tài khoản Policy Admin và chọn hộp Allow Full Control. Người dùng này hiện có toàn quyền kiểm soát các OU này và tất cả các OU con và GPO cho các OU này. Nhấp vào OK. Nếu bạn chỉ muốn cấp cho người dùng này các quyền riêng lẻ, thì trong cửa sổ Thuộc tính (bước 8), hãy nhấp vào nút Advanced rồi đến tab Effective Permission. Đây là nơi bạn cũng có thể chọn một người dùng và chỉ cấp cho họ các quyền mà bạn muốn họ có.
9. Khi hoàn tất, hãy đóng công cụ GPMC.

## **10.5. Configuring Automatic Certificate Enrollment in Group Policy**

1. Mở công cụ Group Policy Management Console.
2. Nhấp chuột phải vào OU North America mà bạn đã tạo trong các bài tập trước.
3. Chọn Create A GPO In This Domain And Link It Here và đặt tên là Test CA. Nhấp vào OK.
4. Nhấp chuột phải vào Test CA GPO và chọn Edit.
5. Mở Computer Configuration/Policies/Windows Settings/Security Settings/ Public Key Policies.
6. Nhấp đúp vào Certificate Services Client – Auto-Enrollment trong ngăn bên phải.
7. Hộp thoại Certificate Services Client – Auto-Enrollment Properties sẽ xuất hiện.
8. Hiện tại, đừng thay đổi bất cứ điều gì. Chỉ cần làm quen với các cài đặt trong hộp thoại này. Nhấp vào OK để đóng hộp thoại.

**10.6. Configuring Folder Redirection in Group Policy**

1. Mở công cụ GPMC.
2. Mở OU North America rồi chỉnh sửa GPO Test CA.
3. Mở User Configuration/Policies/Windows Settings/Folder Redirection/ Documents.
4. Nhấp chuột phải vào Documents và chọn Properties.
5. Trên tab Target của hộp thoại Documents Properties, chọn lựa chọn Basic – Redirect Everyone’s Folder To The Same Location từ danh sách thả xuống Settings.
6. Để nguyên tùy chọn mặc định cho danh sách thả xuống Target Folder Location và chỉ định đường dẫn mạng trong trường Root Path.
7. Nhấp vào tab Settings. Tất cả các thiết lập mặc định đều tự giải thích và thường nên để nguyên thiết lập mặc định. Nhấp vào OK khi bạn hoàn tất

## **10.7. Creating a Software Deployment Share**

1. Sử dụng Windows Explorer, tạo một thư mục có tên là Software mà bạn có thể sử dụng với chia sẻ ứng dụng. Đảm bảo rằng ổ đĩa mà bạn tạo thư mục này có ít nhất 2.000 MB dung lượng đĩa trống.
2. Tạo một thư mục có tên là Office 2016 trong thư mụcSoftware.
3. Sao chép tất cả các tệp cài đặt cho Microsoft Office 2016 từ DVD hoặc chia sẻ mạng chứa các tệp vào thư mục Office 2016 mà bạn đã tạo ở bước 2. Nếu muốn, bạn có thể sử dụng công tắc để cài đặt tất cả các tệp cài đặt Office 2016.
4. Nhấp chuột phải vào thư mục Software (đã tạo ở bước 1) và chọn Give access to/Specific People… Trong hộp thoại Choose People On Your Network To Share With, nhập Everone và nhấp vào nút Add. Tiếp theo, nhấp vào nút Share. Khi bạn thấy thông báo cho biết quá trình chia sẻ đã hoàn tất, hãy nhấp vào Done.

# **11. Configuring Security**

## **11.1. Windows Defender Security Center**

1. Nhấp vào Start/Settings/Update & Security/Windows Security rồi chọn Virus & Threat Protection.
2. Chọn liên kết Scan options
3. Đảm bảo nút radio ở chế độ Full scan và chọn nút Scan now
4. Quá trình quét sẽ mất một lúc. Sau khi quá trình quét hoàn tất, hãy đóng Defender Security Center.

## **11.2. Configuring Windows Firewall**

1. Nhấp vào Start/Settings/Update & Security/Windows Security rồi chọn Firewall & Network Protection.
2. Sau đó, bạn có thể quyết định tùy chọn tường lửa nào bạn muốn đặt, như thay đổi thông báo tường lửa, bật hoặc tắt Tường lửa Windows, khôi phục mặc định, cấu hình cài đặt nâng cao và khắc phục sự cố
3. Hộp thoại cài đặt Tường lửa Windows cho phép bạn bật hoặc tắt Tường lửa Windows cho cả mạng riêng và mạng công cộng. Cài đặt Bật sẽ chặn các nguồn đến và cài đặt Tắt Tường lửa Windows sẽ cho phép các nguồn đến kết nối.

## **11.3. Windows Firewall with Advanced Security (WFAS)**

1. Nhấp vào Start/Settings/Update & Security/Windows Security/ Firewall & Network Protection
2. Click vào Advanced Settings.
3. Nhấp chuột phải vào Inbound Rules và chọn New Rule.
4. Chọn một loại quy tắc. Đối với bài tập này, hãy chọn Custom để bạn có thể thấy tất cả các tùy chọn có sẵn cho mình. Sau đó, nhấp vào Next.
5. Tại màn hình Program, hãy chọn All Programs. Sau đó, nhấp vào Next.
6. Chọn loại giao thức cũng như số cổng cục bộ và từ xa bị ảnh hưởng bởi quy tắc này. Đối với bài tập này, hãy chọn TCP và đảm bảo rằng All Ports được chọn cho cả Local Port và Remote Port. Nhấp vào Next để tiếp tục.
7. Tại màn hình Scope, hãy chọn Any IP Address cho cả local và remote. Sau đó, nhấp vào Next.
8. Tại màn hình Action, hãy chọn Allow The Connection Only If It Is Secure. Nhấp vào Next.
9. Tại màn hình Users, bạn có thể thử nghiệm các tùy chọn này nếu muốn bằng cách nhập người dùng vào cả hai phần. Khi bạn nhấp vào một trong các hộp kiểm, các nút Add và Remove sẽ khả dụng. Nhấp vào Next để tiếp tục.
10. Tại màn hình Computers, bạn có thể chọn máy tính nào bạn sẽ ủy quyền hoặc cho phép thông qua quy tắc này (ngoại lệ). Một lần nữa, bạn có thể thử nghiệm các tùy chọn này nếu muốn. Nhấp vào Next để tiếp tục.
11. Tại màn hình Profile, hãy chọn hồ sơ nào sẽ bị ảnh hưởng bởi quy tắc này. Chọn một hoặc nhiều hồ sơ và nhấp vào Next.
12. Đặt tên và mô tả cho hồ sơ của bạn, sau đó nhấp vào Finish. Quy tắc tùy chỉnh của bạn sẽ xuất hiện trong danh sách các quy tắc đến và quy tắc sẽ được bật.
13. Nhấp đúp vào quy tắc mới tạo của bạn. Lưu ý rằng bạn có thể thay đổi các tùy chọn mà bạn đã định cấu hình trước đó.
14. Xóa quy tắc bằng cách nhấp chuột phải vào quy tắc mới và chọn Delete. Một hộp thoại sẽ xuất hiện hỏi bạn có chắc chắn không. Nhấp vào Yes.
15. Đóng Tường lửa Windows.

## **11.4. Installing Windows Defender Application Guard**

1. Nhấp chuột phải vào Start/Apps and Features, tại cửa sổ bên phải chọn Programs And Features.
2. Nhấp vào liên kết Turn Windows Features On Or Off.
3. Cuộn xuống và đánh dấu vào ô Windows Defender Application Guard, sau đó nhấp vào nút OK. Nếu đang cài trên Windows Server 2022 thì qua bước 4.
4. Tại màn hình Before You Begin, nhấp vào Next.
5. Màn hình Select Installation Type sẽ xuất hiện tiếp theo. Đảm bảo rằng nút radio Role-Based được chọn và nhấp vào Next.
6. Tại màn hình Select Destination Server, chọn Select a server from the server pool, chọn Server. Nhấp vào Next.
7. Tại màn hình Select Server Roles, nhấp vào hộp kiểm cho Windows Defender Application Guard.
8. Sau khi Windows Defender Application Guard được cài đặt, hãy đóng Control Panel.

## **11.5. Using Windows Defender Application Guard**

1. Mở Microsoft Edge.
2. Từ menu tùy chọn, chọn New Application Guard Window
3. Bạn sẽ cần phải đợi Application Guard thiết lập môi trường bị cô lập. Quá trình này có thể mất vài phút.
4. Mở trang web của Microsoft ở chế độ Application Guard và bạn có thể thấy điều đó ở góc trên bên trái của cửa sổ. Đóng Edge

## **11.6. Windows Defender Application Guard Enterprise**

1. Cài đặt Application Guard bằng cách sử dụng đối tượng Group Policy, System Center hoặc MDM.
2. Trong Group Policy, hãy đặt các thiết lập Network Isolation mà bạn muốn tuân theo. Để đặt tùy chọn này, trong trình soạn thảo GPO của bạn, hãy đi tới Administrative Templates\Network\Network Isolation\Enterprise Resource Domains Hosted In The Cloud.
3. Tiếp theo, hãy vào Administrative Templates\Network\Network Isolation\Domains được phân loại là cả thiết lập công việc và cá nhân. Nhập các trang web mà bạn tin tưởng.
4. Tiếp theo, hãy vào Computer Configuration\Administrative Templates\Windows Components\Windows Defender Application Guard\Turn On Windows Defender Application Guard In Enterprise Mode.
5. Chọn nút tùy chọn Enabled, chọn Option 1 (xem Hình 17.16) và nhấp vào OK.
6. Close the GPO editor.

## **11.7. Windows Defender Credential Guard**

1. Mở Group Policy Management Console trên Windows Server 2022.
2. Tạo GPO mới và nhấp vào GPO rồi chọn Edit.
3. Đi tới Computer Configuration/Administrative Templates/System/Device Guard.
4. Nhấp đúp vào tùy chọn Turn On Virtualization Based Security rồi chọn tùy chọn Enabled.
5. Trong tùy chọn Turn On Virtualization Based Security, hãy chọn hộp Platform Security Level, chọn Secure Boot hoặc Secure Boot and DMA Protection.
6. Trong hộp Credential Guard Configuration, hãy nhấp vào Enabled with UEFI lock, rồi nhấp vào nút OK.
7. Đóng Group Policy Management Console.

## **11.8. Windows Defender Exploit Guard**

1. Mở trung tâm Cài đặt bằng cách nhấp vào nút Start và nhấp vào biểu tượng Settings (biểu tượng spoke).
2. Chọn Update And Security.
3. Nhấp vào n Windows Security và chọn e Virus & Threat Protection.
4. Chọn Ransomware Protection và đảm bảo cài đặt được bật.
5. Nhấp vào Protected Folders để xem những thư mục nào hiện đang được bảo vệ. Bạn có thể nhấp vào + Add A Protected Folder để thêm các thư mục khác.
6. Nếu bạn muốn một ứng dụng có quyền truy cập, bạn có thể nhấp vào liên kết Allow An App Through Controlled Folder Access. Sau khi nhấp vào liên kết, bạn có thể thêm ứng dụng sẽ được phép truy cập.
7. Đóng Security Center (khởi động lại nếu bạn thực hiện bất kỳ thay đổi nào).