

# MỤC LỤC

<b>Bài 1</b>	<b>CẤU HÌNH ACTIVE DIRECTORY.....</b>	<b>3</b>
<b>Bài 2</b>	<b>KẾT NỐI MÁY TÍNH VÀO MIỀN .....</b>	<b>11</b>
<b>Bài 3</b>	<b>CẤU HÌNH DỊCH VỤ TÊN MIỀN DNS .....</b>	<b>14</b>
3.1	Kiểm tra dịch vụ DNS với NSLOOKUP .....	14
3.2	Cấu hình DNS Server .....	14
<b>Bài 4</b>	<b>TẠO VÀ QUẢN TRỊ GROUP POLICY OBJECT .....</b>	<b>19</b>
<b>Bài 5</b>	<b>CẤU HÌNH DỊCH VỤ DHCP .....</b>	<b>30</b>
<b>Bài 6</b>	<b>CẤU HÌNH DỊCH VỤ IIS .....</b>	<b>36</b>
6.1	Cài đặt dịch vụ IIS.....	36
6.2	Kiểm tra dịch vụ WEB : .....	37
6.3	Cấu hình dịch vụ FTP.....	38
6.4	Kiểm tra dịch vụ FTP .....	40
<b>Bài 7</b>	<b>CẤU HÌNH DỊCH VỤ VPN .....</b>	<b>42</b>
<b>Bài 8</b>	<b>CÂN BẰNG TẢI TRÊN WINDOWS SERVER 2012.....</b>	<b>50</b>
8.1	Cài đặt dịch vụ NLB.....	50
8.2	Kiểm tra NLB .....	52
<b>Bài 9</b>	<b>CẤU HÌNH DỊCH VỤ AD RMS.....</b>	<b>53</b>
<b>Bài 10</b>	<b>ĐỊNH TUYẾN IPv6 TRÊN WINDOWS SERVER 2012.....</b>	<b>59</b>
10.1	Cài đặt IPV6 trên máy chủ .....	59
10.2	Gán địa chỉ IPv6 thủ công .....	61

# **GIỚI THIỆU**

Hệ điều hành Microsoft Windows Server 2012 là thế hệ kế tiếp của hệ điều hành Windows Server, có thể giúp các chuyên gia công nghệ thông tin có thể kiểm soát tối đa cơ sở hạ tầng của họ và cung cấp khả năng quản lý và hiệu lực vượt trội, đảm bảo độ an toàn, khả năng tin cậy và môi trường máy chủ vững chắc hơn các phiên bản trước đây. Windows Server 2012 cung cấp những giá trị mới cho các tổ chức bằng việc bảo đảm tất cả người dùng đều có thể có được những thành phần bổ sung từ các dịch vụ từ mạng, cung cấp nhiều tính năng vượt trội bên trong hệ điều hành và khả năng chuẩn đoán, cho phép các quản trị viên tăng được thời gian hỗ trợ cho các doanh nghiệp.

Các bài hướng dẫn quản trị Windows Server 2012 cung cấp các kỹ năng và kiến thức cần thiết, nhằm giúp cho các người quản trị mạng có được kỹ năng nâng cao để thực hiện nâng cấp, quản lý, bảo trì cơ sở hạ tầng Windows Server 2012 và có thể tham dự chứng chỉ quốc tế Microsoft Certified Solutions Associate (MCSA).

Nội dung các bài hướng dẫn tập trung vào các chủ đề quản trị mạng Windows Server 2012 nâng cao như sau:

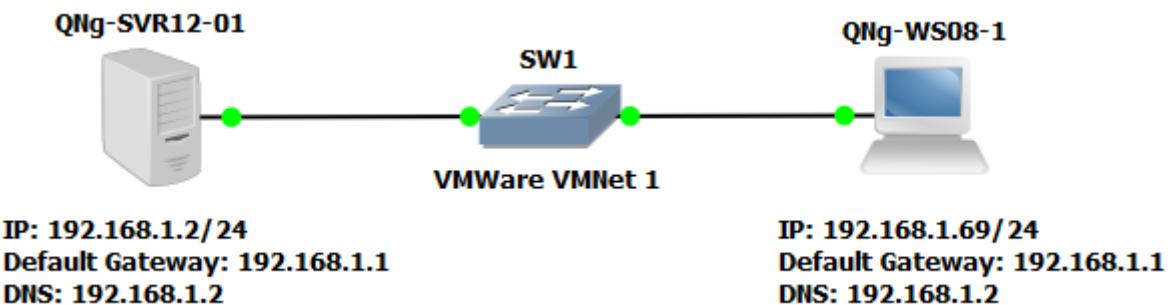
- Lập kế hoạch và thực hiện một AD DS triển khai bao gồm các domain và forests.
- Lập kế hoạch và thực hiện một AD DS triển khai bao gồm các địa điểm.
- Thực hiện triển khai và cấu hình một Active Directory Certificate Services (AD CS).
- Cấu hình các tính năng Dynamic Host Configuration Protocol (DHCP), hệ thống tên miền (DNS), và cấu hình quản lý địa chỉ IP (IPAM) với Windows Server 2012.
- Thực hiện triển khai AD RMS.
- Cung cấp tính sẵn sàng cao và cân bằng tải cho các ứng dụng dựa trên web bằng cách thực hiện cân bằng tải mạng (NLB).
- Thực hiện và xác nhận tính sẵn sàng cao và cân bằng tải cho các ứng dụng dựa trên web bằng cách thực hiện NLB.
- Triển khai dịch vụ IPv6.

TRUNG TÂM TIN HỌC BÁCH KHOA  
TRƯỜNG ĐẠI HỌC BÁCH KHOA - ĐHQGHN

## CẤU HÌNH ACTIVE DIRECTORY

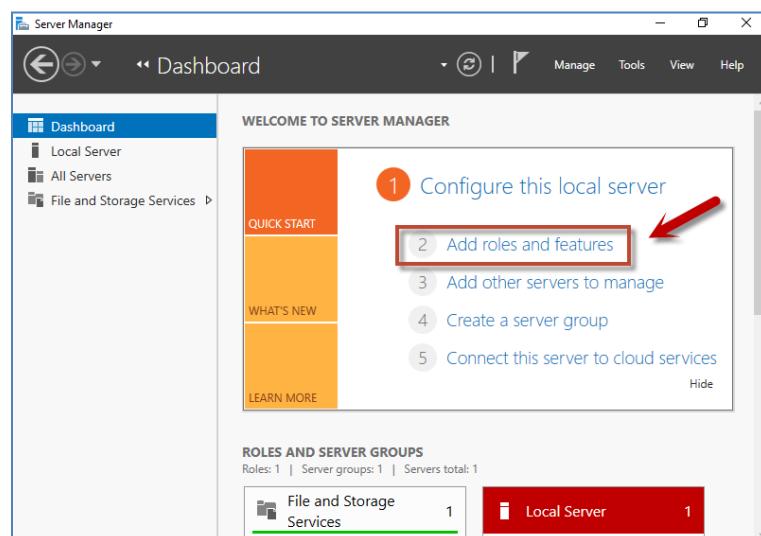
Một domain là tập hợp các tài khoản người dùng và tài khoản máy tính được nhóm lại với nhau để quản lý một cách tập trung. Và công việc quản lý là dành cho domain controller (bộ điều khiển miền) nhằm giúp việc khai thác tài nguyên trở nên dễ dàng hơn.

Mục tiêu: Nâng cấp Server thành Domain Controller.



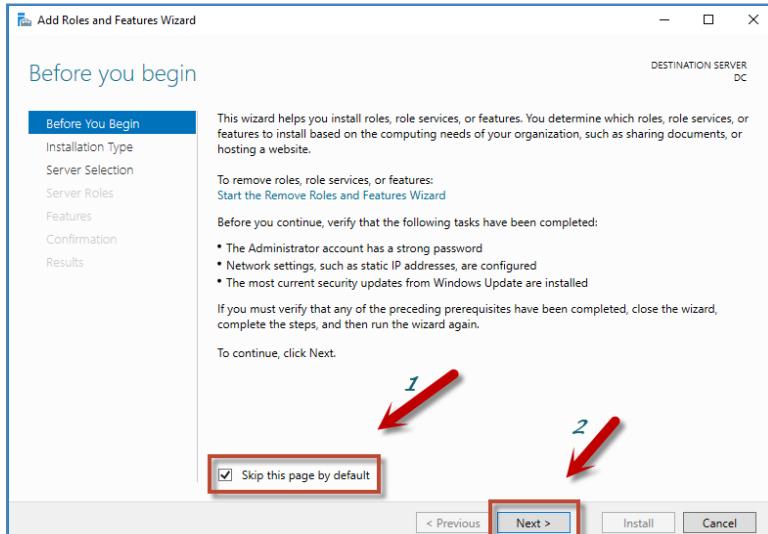
Bước 1. Nhấn chọn công cụ *Server Manager* trên thanh Taskbar

Bước 2. Tại bảng điều khiển của công cụ Server Manager, nhấn chọn mục Add Roles and Features.



Hình 1.1. Mở chức năng cài đặt AD DS.

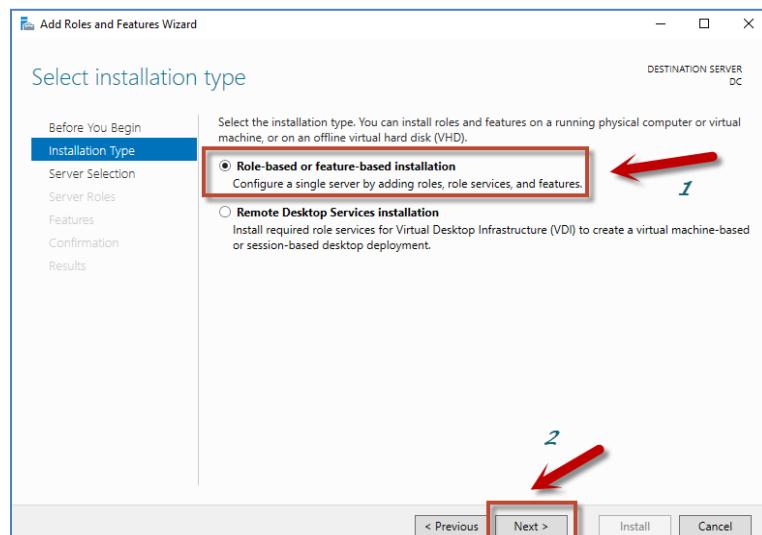
Bước 3. Tại giao diện thêm vai trò và tính năng, nhấn chọn *Skip this page by default* để bỏ qua màn hình giới thiệu cho những lần sử dụng sau. Sau đó nhấn *Next*.



Hình 1.2. Màn hình giới thiệu.

Bước 4. Tại màn hình lựa chọn kiểu cài đặt, nhấn chọn Role-based or feature-based installation. Sau đó nhấn Next.

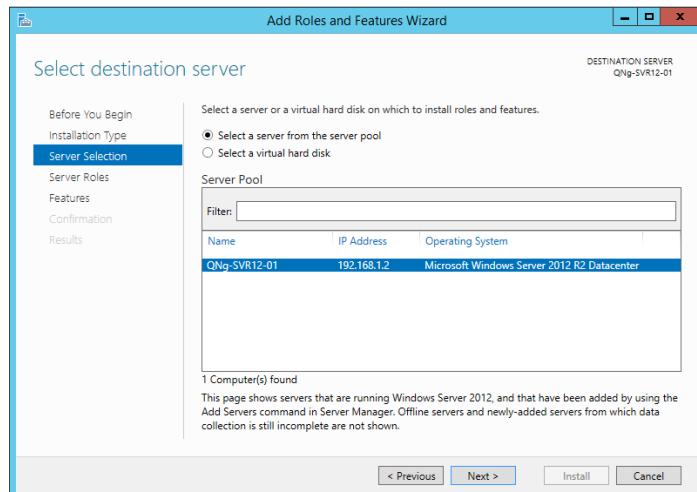
- **Role-based or feature-based installation:** cài đặt và cấu hình cho một máy chủ vật lý.
- **Remote Desktop Services installation:** cài đặt các dịch vụ cần thiết cho máy chủ ảo.



Hình 1.3. Lựa chọn dạng cài đặt.

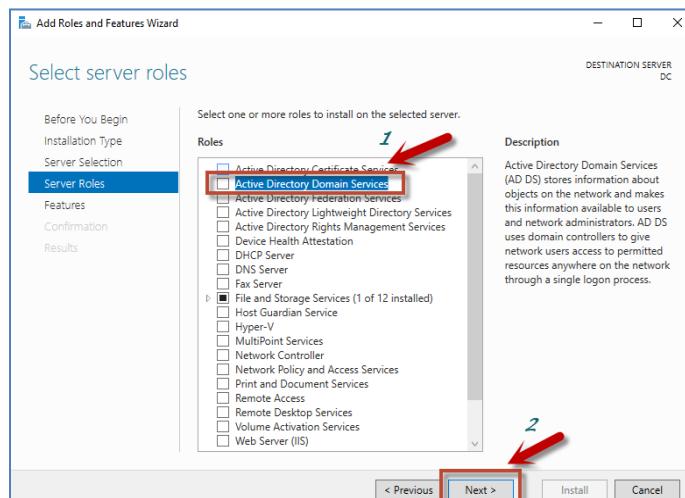
Bước 5. Tại màn hình lựa chọn máy chủ, ta lần lượt thực hiện các bước sau:

- 1) Nhấn chọn Select a server from the server pool.
  - **Select a server from the server pool:** chọn máy chủ từ danh sách các máy chủ được liệt kê.
  - **Select a virtual hard disk:** lựa chọn một đĩa cứng ảo.
- 2) Tại mục Server Pool, chọn máy chủ để cài đặt. Trong hình bên dưới chọn máy chủ có tên là DC để tiến hành cài đặt AD DS.
- 3) Nhấn Next để tiếp tục.



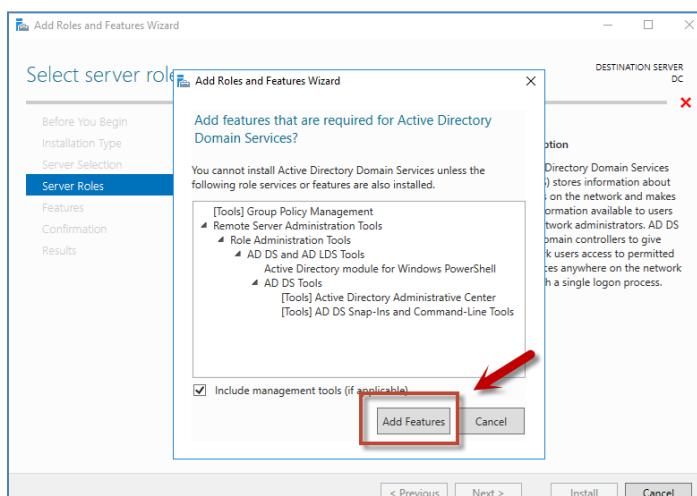
Hình 1.4. Lựa chọn máy chủ cài đặt.

Bước 6. Tại mục lựa chọn các vai trò cần cài đặt, nhấn chọn mục Active Directory Domain Services. Sau đó nhấn Next.



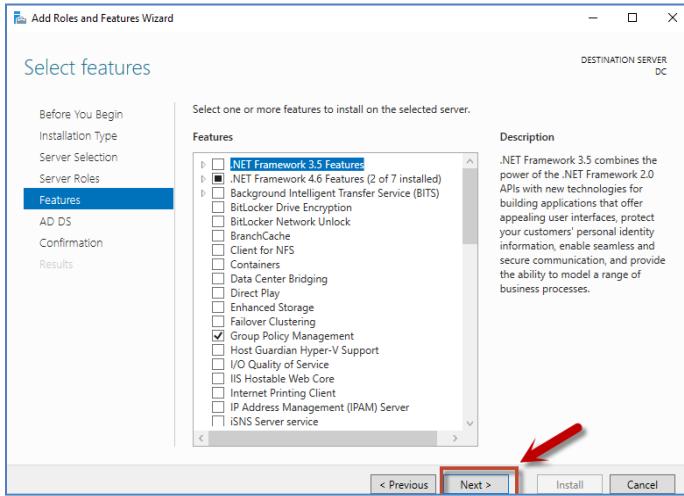
Hình 1.5. Lựa chọn cài đặt AD DS.

Bước 7. Khi lựa chọn cài đặt AD DS, một cửa sổ hiển thị yêu cầu cài đặt thêm các tính năng bổ sung. Nhấn nút Add Features để chấp nhận cài đặt.



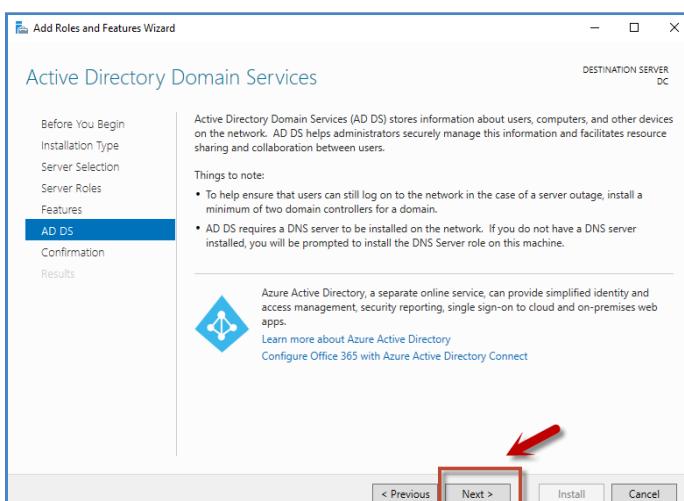
Hình 1.6. Cài đặt các tính năng cần thiết cho AD DS.

Bước 8. Tại màn hình lựa chọn các tính năng bổ sung, nhấn Next để tiếp tục.



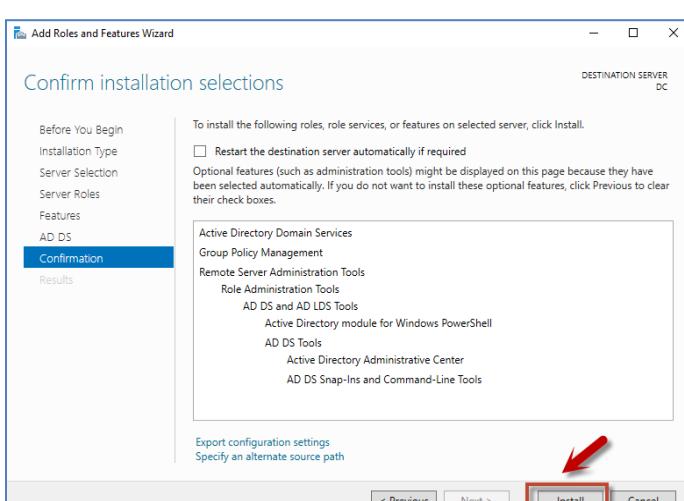
Hình 1.7. Lựa chọn tính năng bổ sung.

Bước 9. Tại màn hình giới thiệu AD DS, nhấn Next để tiếp tục.



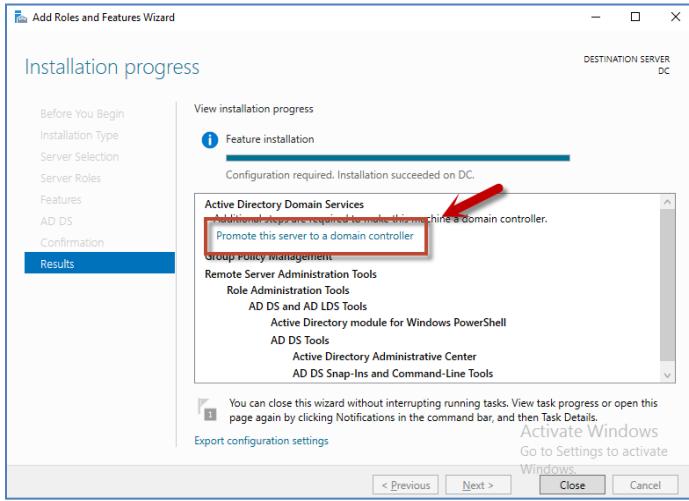
Hình 1.8. Màn hình giới thiệu về AD DS.

Bước 10. Tại màn hình xác nhận cài đặt, kiểm tra lại các lựa chọn cài đặt trước đó. Nếu tất cả hợp lệ, nhấn nút Install để tiến hành cài đặt.



Hình 1.9. Màn hình xác nhận lại các thành phần sẽ cài đặt.

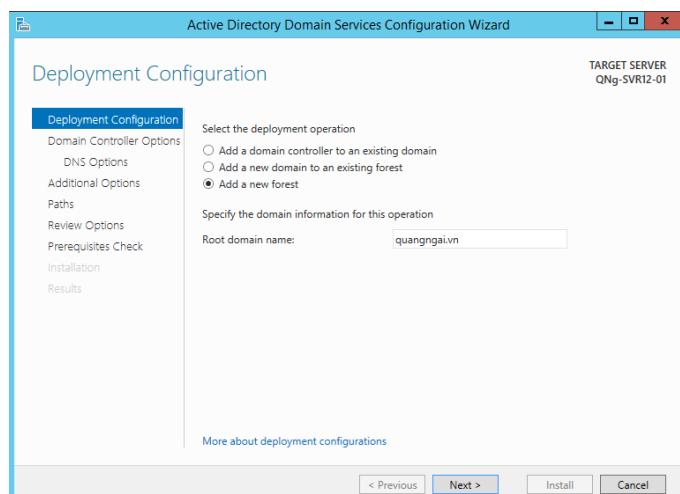
Bước 11. Sau khi AD DS được cài xong, nhấn chọn Promote this server to a domain controller.



Hình 1.10. Nâng cấp máy chủ thành DC.

Bước 12. Tại màn hình cấu hình cài đặt, ta thực hiện lần lượt các thao tác sau:

- 1) Nhấn chọn **Add a new forest**: vì do hệ thống chưa tồn tại bất kỳ forest nào nên ta chọn mục này.
  - **Add a domain controller to an existing domain**: thêm một DC mới vào miền đã tồn tại trước.
  - **Add a new domain to an existing forest**: thêm một miền mới vào một forest đã tồn tại trước.
  - **Add a new forest**: tạo một forest mới.
- 2) Nhập tên miền của hệ thống vào mục **Root domain name**: quangngai.vn
- 3) Nhấn **Next** để tiếp tục.

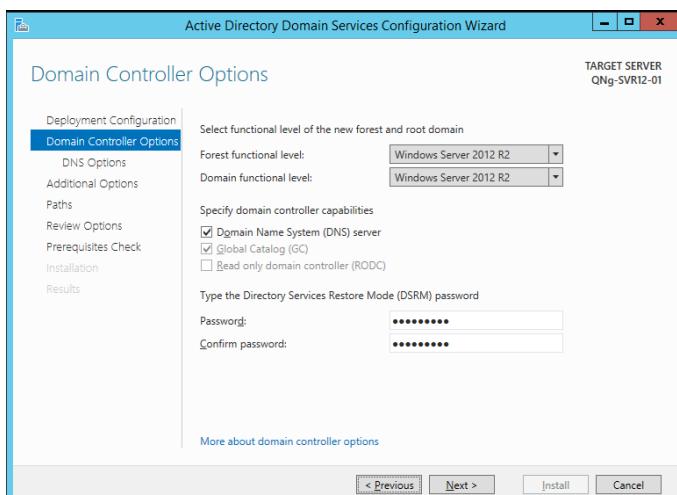


Hình 1.11. Thiết lập cài đặt trước khi nâng cấp lên DC.

Bước 13. Tại mục lựa chọn thiết lập cho DC, ta lần lượt thực hiện các thao tác sau:

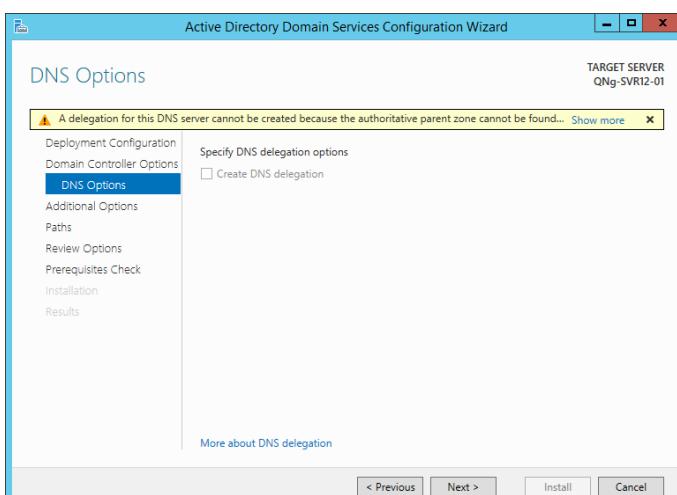
- 1) Chọn **Windows Server 2012** tại mục **Forest functional level**
- 2) Chọn **Windows Server 2012** tại mục **Domain functional level**
- 3) Tại mục **Specify domain controller capabilities**: giữ nguyên các lựa chọn mặc định.
  - **Domain Name System (DNS) server**: lựa chọn này cho phép cài đặt dịch vụ DNS lên chính máy chủ này.
  - **Global Catalog (GC)**: do máy chủ này là DC đầu tiên trong rừng, nên GC sẽ được cài đặt mặc định. Do đó, tại mục này chúng ta không thể thay đổi lựa chọn.

- **Read only domain controller (RODC):** thiết lập cài đặt máy chủ này như là một RODC. Do đây là DC đầu tiên trong miền nên không thể chọn thiết lập này.
- 4) Tiến hành nhập mật khẩu vào hai trường: **Password** và **Confirm password**. Khi cần hạ cấp DC xuống thành máy chủ bình thường, cần phải cung cấp mật khẩu này. Vì khi hạ cấp thì toàn bộ dữ liệu của AD sẽ mất hết. Nên đây là mật khẩu rất quan trọng quản trị viên cần phải thiết lập một mật khẩu có độ phức tạp cao. Một mật khẩu được xem là phức tạp cao khi đáp ứng các tiêu chí sau:
- Có chứa ký tự hoa, thường, số, và ký tự đặc biệt.
  - Nên có chiều dài mật khẩu phải từ 15 ký tự trở lên.



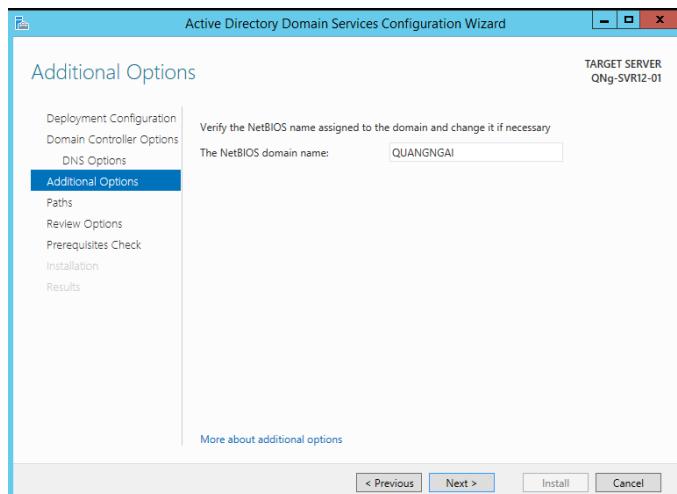
Hình 1.12. Thiết lập cấu hình cho DC.

Bước 14. Tại mục thiết lập cho DNS, nhấn Next để tiếp tục.



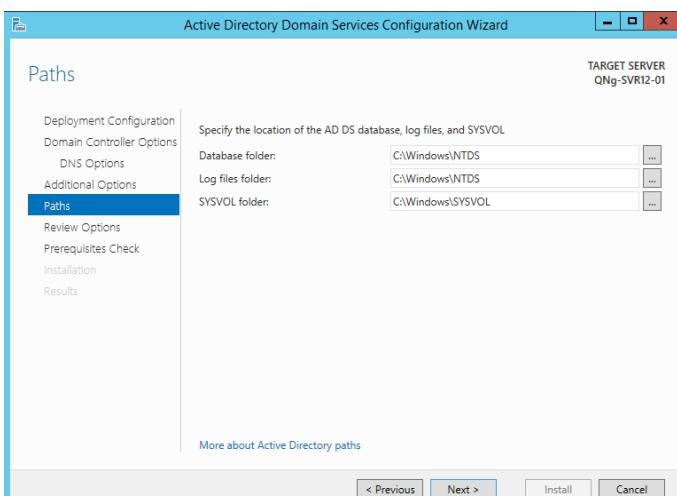
Hình 1.13. Thiết lập ủy quyền DNS.

Bước 15. Tại màn hình thiết lập các tùy chọn bổ sung, hệ thống sẽ tiến hành kiểm tra lại tên NetBIOS của DC. Nếu tên này không tồn tại trong hệ thống thì sau đó nhấn Next để tiếp tục.



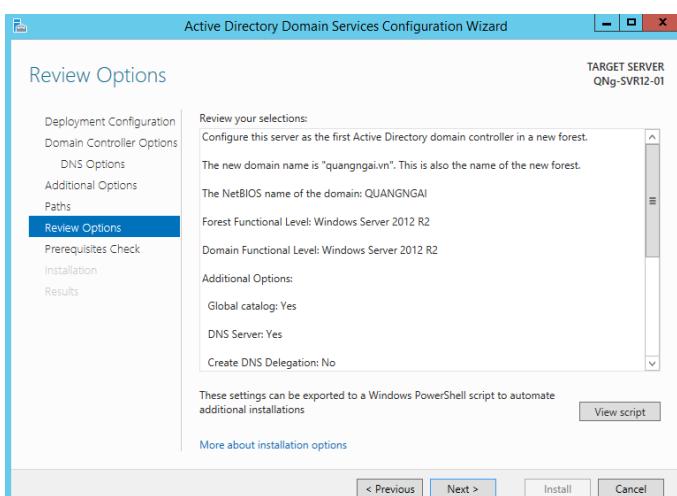
Hình 1.14. Tùy chọn bổ sung.

Bước 16. Tại màn hình thiết lập các đường dẫn lưu trữ, giữ nguyên đường dẫn mặc định và nhấn Next để tiếp tục.



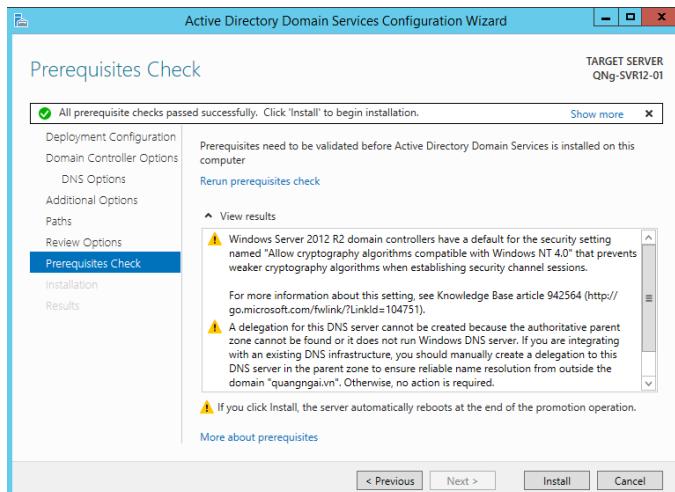
Hình 1.15. Thiết lập đường dẫn nơi lưu trữ thông tin của DC.

Bước 17. Tại màn hình xem lại các thiết lập cài đặt, nếu tất cả đều hợp lệ thì nhấn Next để tiếp tục.



Hình 1.16. Tổng hợp lại các thiết lập cài đặt

Bước 18. Tại bước này hệ thống sẽ tiến hành kiểm tra các điều kiện tiên quyết trước khi tiến hành cài đặt. Nếu tất cả đều hợp lệ, nhấp Install để thực hiện quá trình nâng cấp máy chủ lên DC.



Hình 1.17. Kiểm tra các điều kiện tiên quyết trước khi cài đặt.

Bước 19. Sau khi kiểm tra các điều kiện tiên quyết, hệ thống sẽ tiến hành thực hiện quá trình nâng cấp máy chủ lên DC.

Bước 20. Sau khi nâng cấp thành công, hệ thống sẽ được khởi động lại.

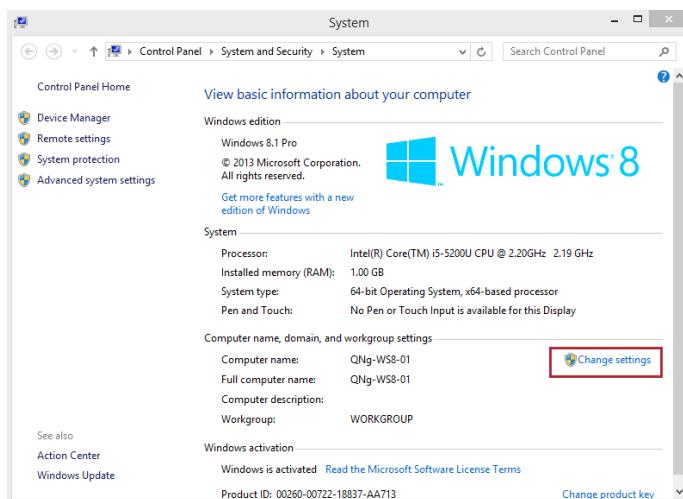
## Bài 2

# KẾT NỐI MÁY TÍNH VÀO MIỀN

Tại mỗi máy sẽ tạo các User Account cho nhân viên truy cập. Tuy nhiên nếu người dùng đăng nhập vào máy 1 để làm việc sau đó sang máy thứ 2 làm việc thì phải tạo các User Account giống nhau mới truy cập được. Tính năng là Domain Controller (DC) cho phép Administrator chỉ việc tạo User Account ngay trên máy DC, nhân viên công ty dù ngồi vào bất cứ máy nào trên Domain đều có thể truy cập vào Account của mình mà các tài nguyên anh ta tạo trước đó đều có thể dễ dàng tìm thấy.

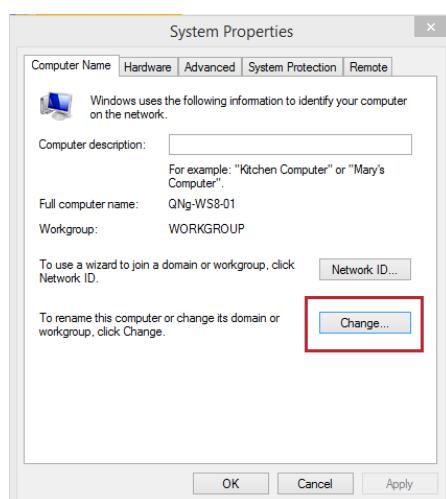
Bước 1. Trên máy người dùng, nhấn chuột phải vào This PC và chọn Properties.

Bước 2. Tại màn hình hiển thị thông tin hệ thống, nhấn chọn Change Settings.



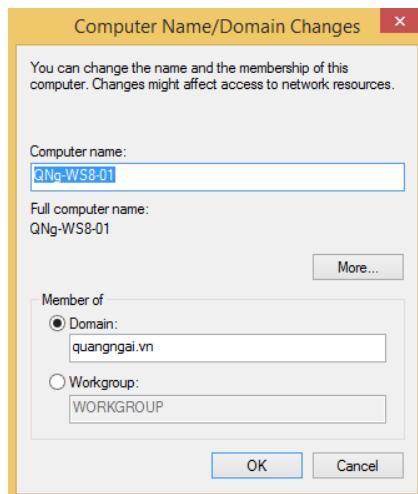
Hình 2.1. Thay đổi thông tin hệ thống.

Bước 3. Tại màn hình thông tin về tên máy tính, nhấn chọn nút Change...



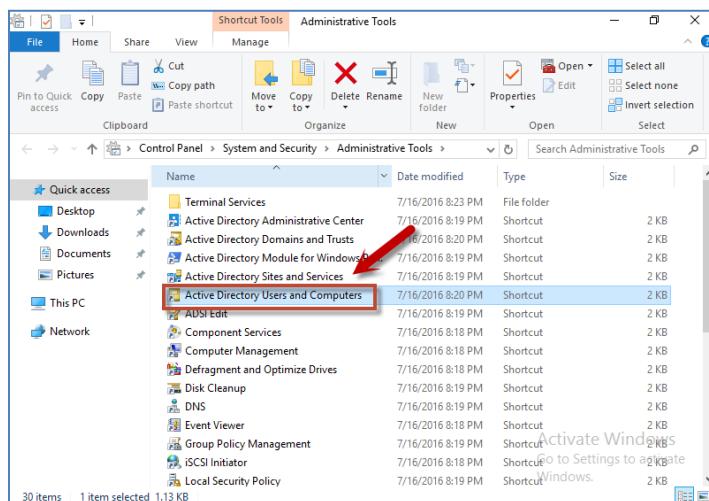
Hình 2.2. Vào mục thay đổi tên máy tính.

Bước 4. Tại mục Member of, nhấn chọn Domain và nhập tên miền cần tham gia. Sau đó nhấn Ok để hoàn tất thiết lập.



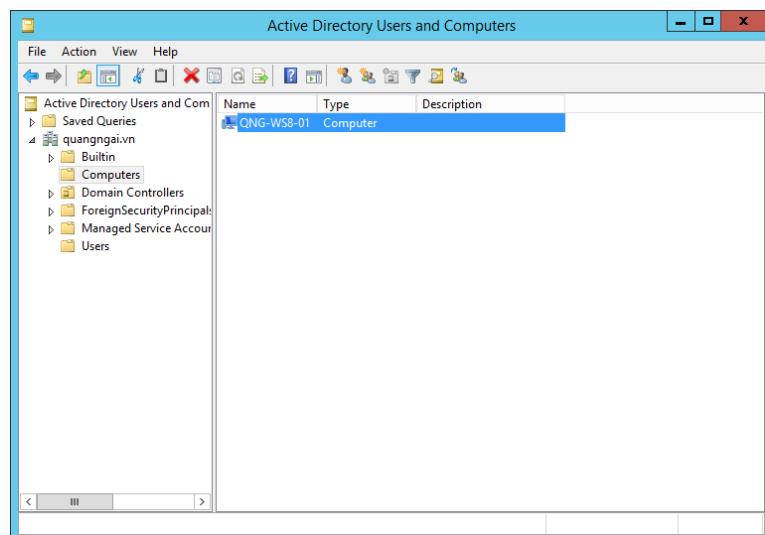
Hình 2.3. Nhập tên miền cần tham gia.

- Bước 5. Một thông báo chứng thực hiển thị, nhập tên đăng nhập và mật khẩu tài khoản quản trị miền và nhấn Ok để tiến hành chứng thực.
- Bước 6. Sau khi chứng thực thành công, một hộp thoại xuất hiện thông báo việc tham gia miền thành công. Nhấn Ok để đóng hộp thoại.
- Bước 7. Đăng nhập thành công, người dùng cần phải khởi động máy tính để việc tham gia miền có hiệu lực.
- Bước 8. Kiểm tra lại việc thêm máy tính vào miền. Trên DC, truy cập vào Administrative tools trong menu Start.
- Bước 9. Trong bộ chia công cụ quản trị, mở công cụ quản lý người dùng và máy tính trong miền: Active Directory Users and Computers.



Hình 2.4. Công cụ quản trị người dùng và máy tính trong miền.

- Bước 10. Truy cập vào OU có tên là Computers, chúng ta sẽ thấy tên của máy tính vừa tham gia vào miền.



Hình 2.5. Kiểm tra thông tin máy tính vừa tham gia miền.

# CẤU HÌNH DỊCH VỤ TÊN MIỀN DNS

DNS (Domain Name System) là một hệ cơ sở dữ liệu phân tán dùng để ánh xạ giữa các tên miền và các địa chỉ IP. DNS đưa ra một phương pháp đặc biệt để duy trì và liên kết các ánh xạ này trong một thể thống nhất. Trong phạm vi lớn hơn, các máy tính kết nối với internet sử dụng DNS để tạo địa chỉ liên kết dạng URL (Universal Resource Locators). Theo phương pháp này, mỗi máy tính sẽ không cần sử dụng địa chỉ IP cho kết nối.

Khi cài Active Directory thì một DNS Server đã được cài.

## 3.1 Kiểm tra dịch vụ DNS với NSLOOKUP

Thực hiện trên Server Active Directory.

Từ cửa sổ Run nhập vào lệnh:

- Tại dấu nháy lệnh, nhập vào **nslookup**
- Nhập vào **set all** tại dấu nháy >. Lệnh này sẽ liệt kê tất cả giá trị hiện hành của các tùy chọn **nslookup**.
- Dùng các lệnh sau để thay đổi giá trị timeout tới 1 giây và làm lại tới 7 giây.

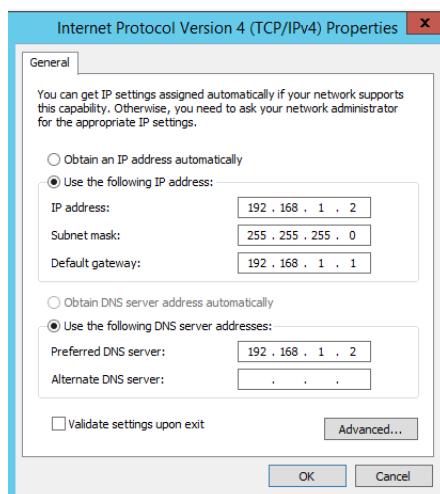
Set ti=1

Set ret=7

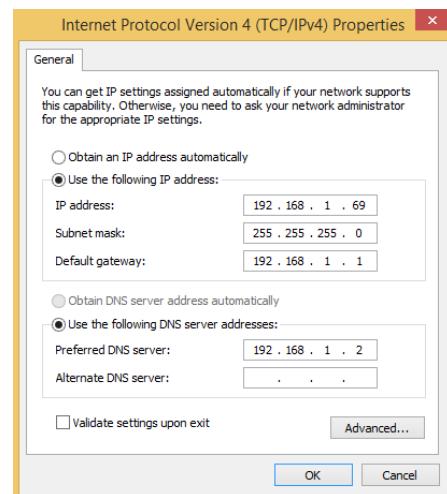
- Dùng **Set All** để kiểm tra các giá trị mặc định được thay đổi.
- Nhập **exit** để thoát.

## 3.2 Cấu hình DNS Server

Cài đặt địa chỉ IP trên máy Server

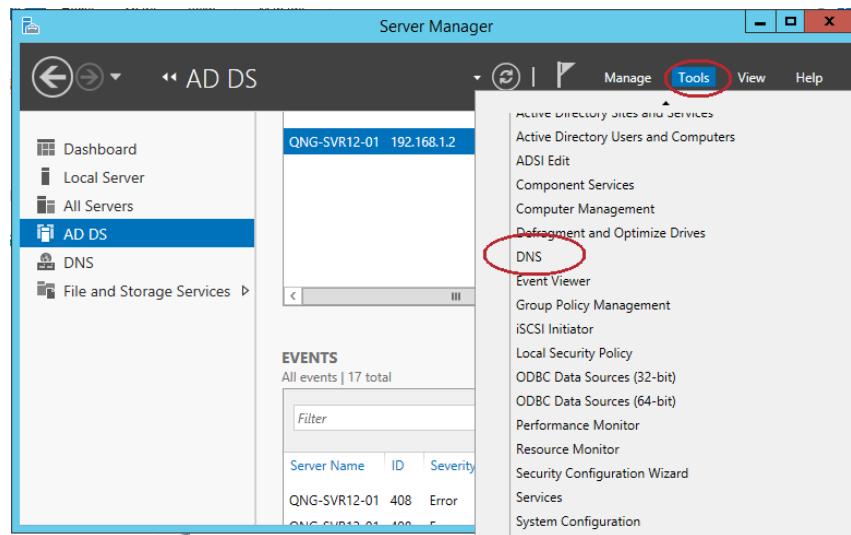


Cài đặt địa chỉ IP trên máy Client

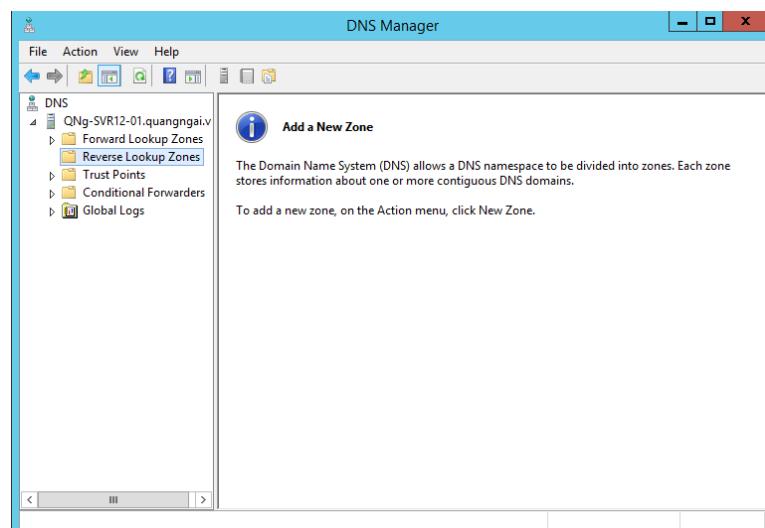


Cấu hình dịch vụ DNS:

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



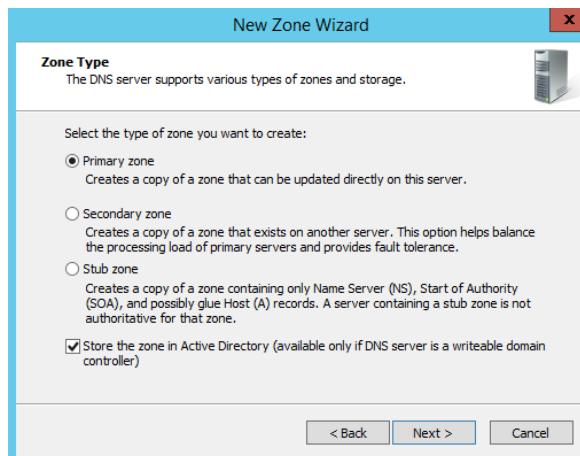
Cửa sổ DNS:



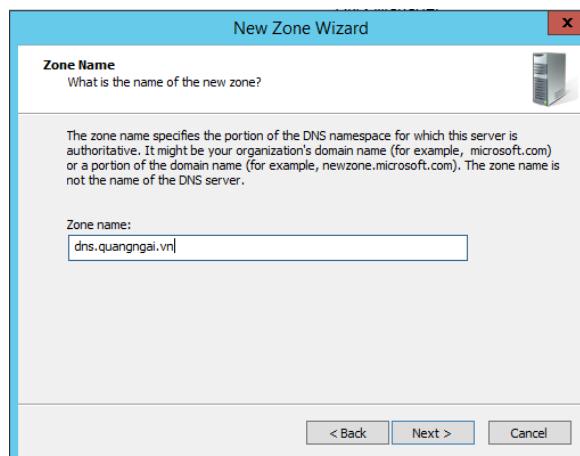
Click chuột phải tại Forward Lookup Zones chọn New Zone. Cửa sổ mới hiện ra, chọn Next



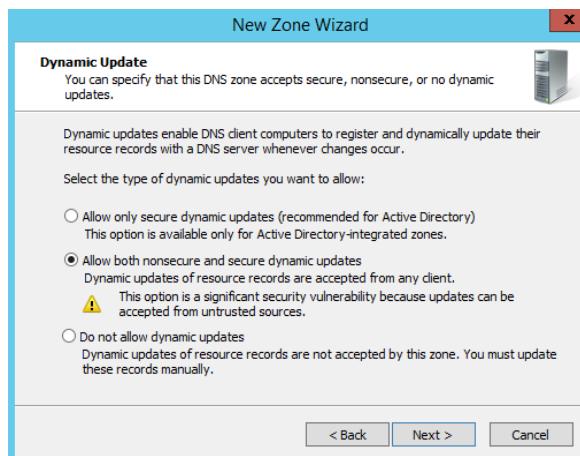
Tại cửa sổ Zone Type, chọn vào Primary zone.



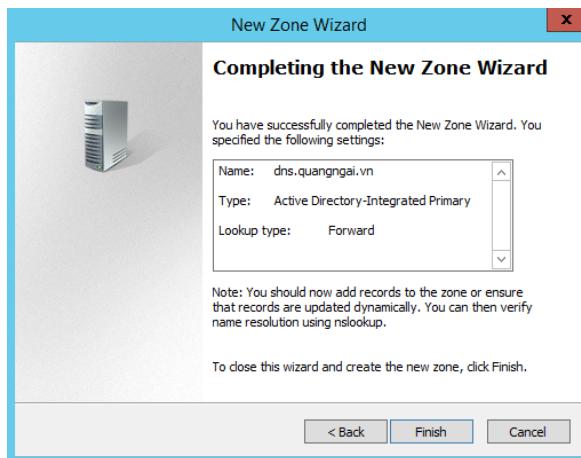
Tại cửa sổ Zone Name, nhập vào tên miền: dns.quangngai.vn



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



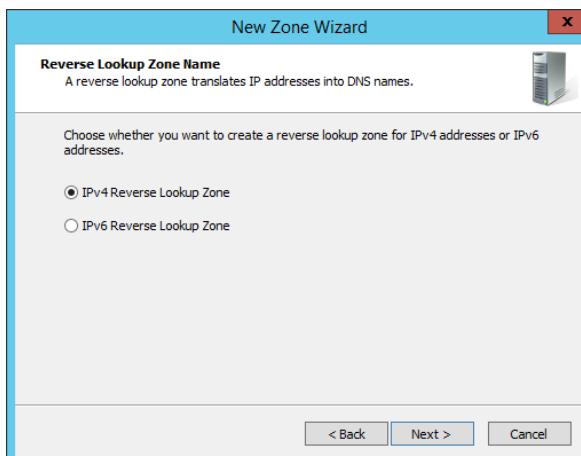
Click vào Finish để kết thúc quá trình cài đặt.



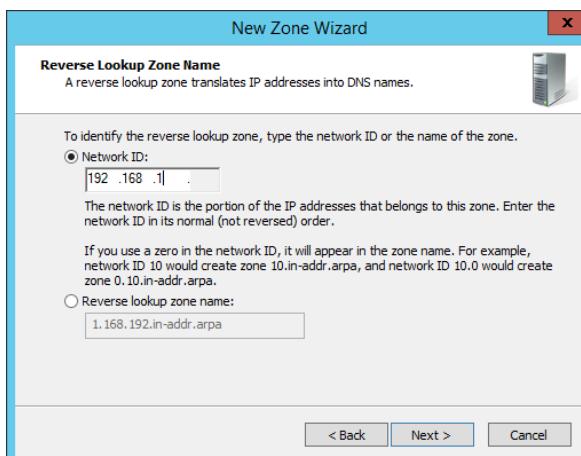
Click chuột phải tại Reverse Lookup Zones, chọn vào New Zone. (tương tự ở trên)

Tại cửa sổ Zone Type, click chọn vào Primary zone (tương tự ở trên)

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



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



Tại cửa sổ Dynamic Update, chọn vào Allow both nonsecure and secure dynamic updates. (tương tự ở trên)

Tại cửa sổ tiếp theo, click chọn vào Finish để kết thúc quá trình cấu hình dịch vụ DNS.

Cáu hình tạo bản ghi cho máy QNG-SVR12-01:

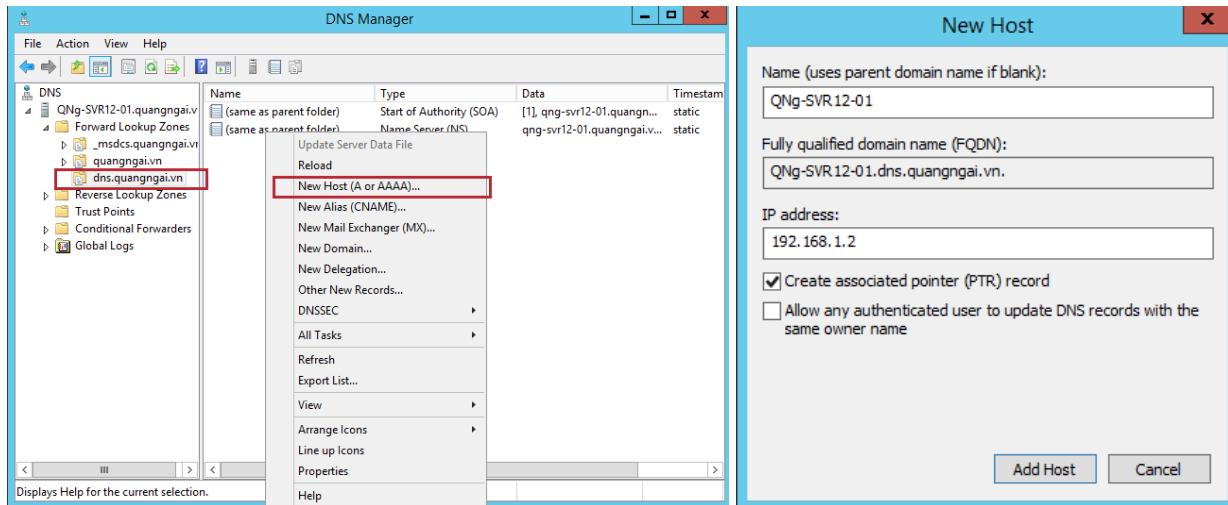
Click vào tên miền dns.quangngai.vn

Click chuột phải chọn New Host (A or AAAA)

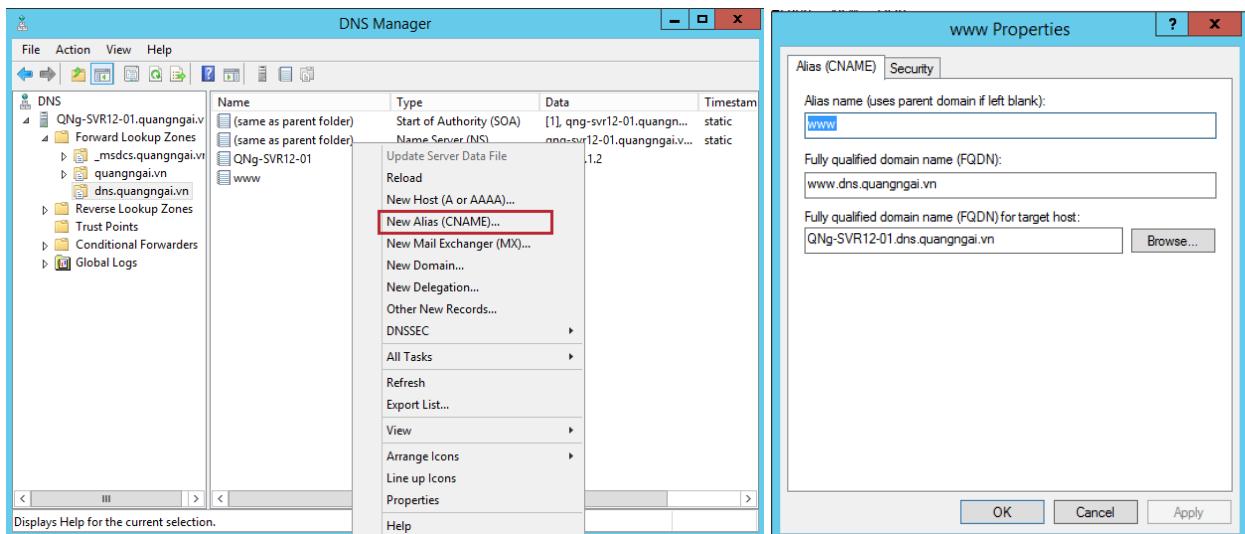
Tại cửa sổ New Host:

- Name (users parent domain name if blank): QNG-SVR12-01
- IP address: 192.168.1.2

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



Tạo bản ghi CNAME:



Chuyển sang máy QNg-WS08-01, kiểm tra phân giải IP sang tên miền.

Vào cmd, gõ lệnh nslookup:

## TẠO VÀ QUẢN TRỊ GROUP POLICY OBJECT

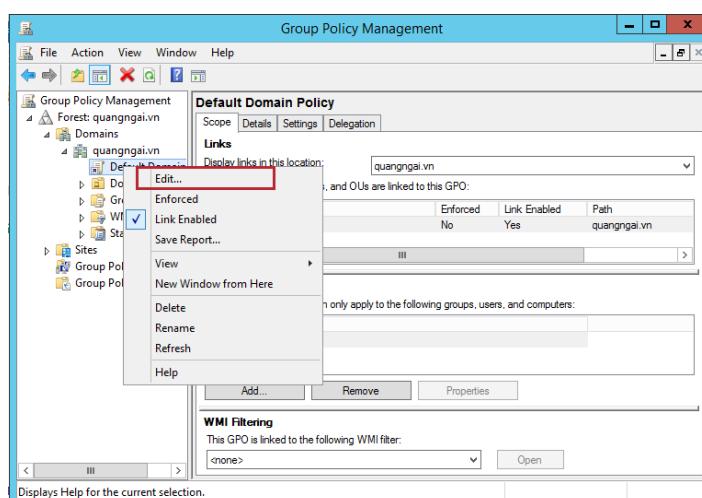
Group Policy có thể dùng để triển khai phần mềm cho một hoặc nhiều máy trạm nào đó một cách tự động; để xác định quyền hạn cho một số người dùng mạng, để giới hạn những ứng dụng mà người dùng được phép chạy; để kiểm soát hạn ngạch sử dụng đĩa trên các máy trạm; để thiết lập các kịch bản (script) đăng nhập (logon), đăng xuất (logout), khởi động (start up), và tắt máy (shut down).

Sau khi xây dựng xong cấu trúc phân cấp OU, tạo xong tài khoản người dùng và nhóm người dùng theo yêu cầu của đơn vị, bạn được yêu cầu thiết lập chính sách để quy định về cách thức đặt mật khẩu của người dùng trong hệ thống như sau.

- Mật khẩu phải có ít nhất 8 ký tự.
- Không phứa tạp.
- Thời gian tối thiểu: 5 ngày.
- Thời gian sử dụng tối đa: 60 ngày.
- Đăng nhập sai 5 lần trong 180 phút thì tài khoản đó sẽ bị khóa 1 ngày.

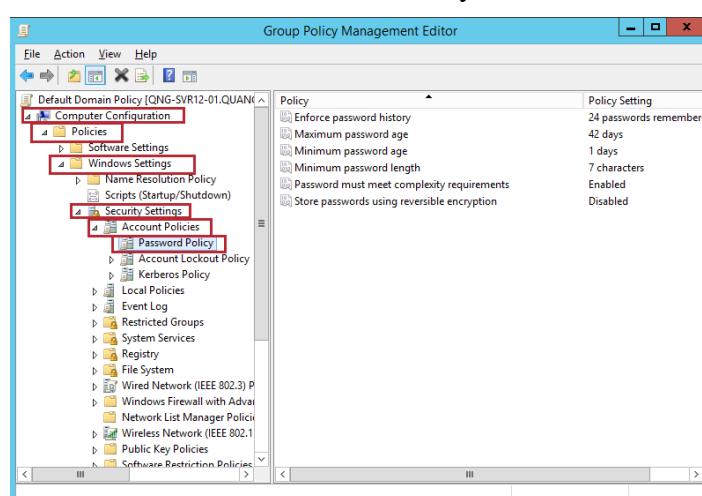
Bước 1. Mở công cụ GPMC.

Bước 2. Nhấn phải chuột lên GPO “Default Domain Policy” và chọn Edit.

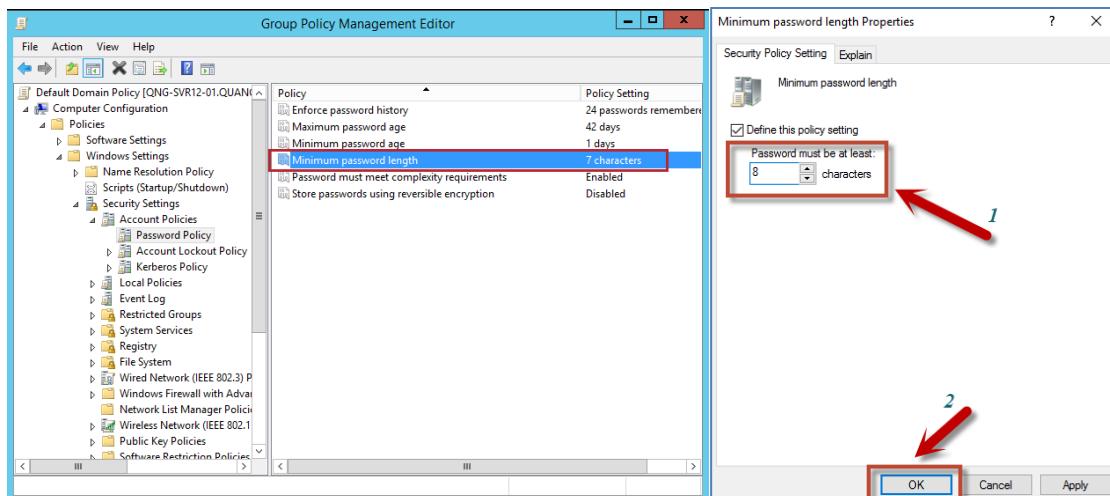


Hình 4.1. Chỉnh sửa lại từ chính sách mặc định.

Bước 3. Tại mục Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy.

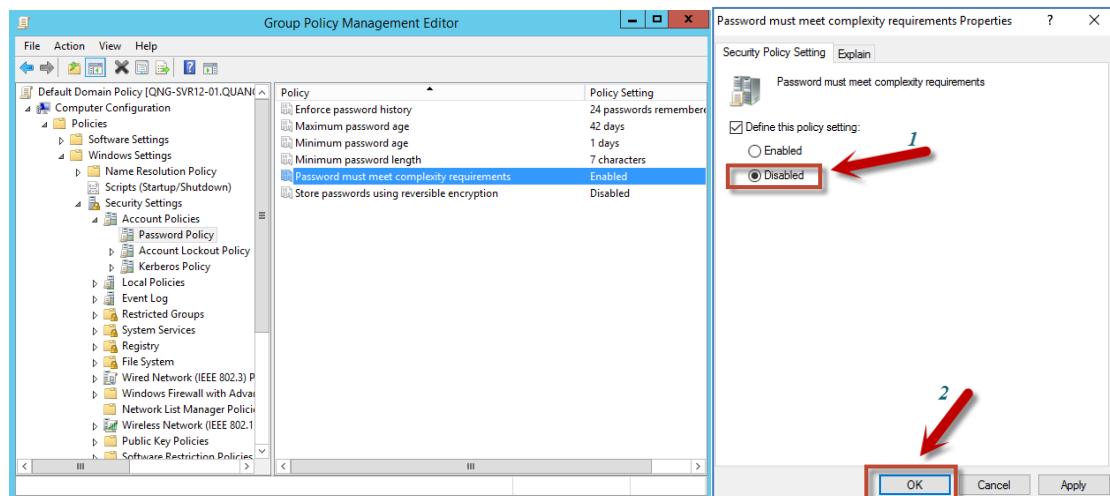


Bước 4. Tại khung chứa bên phải, nhấn đúp chuột lên mục Minimum Password Length để thiết lập chiều dài tối thiểu cho mật khẩu. Nhập số lượng ký tự tối thiểu cho mật khẩu. Nhấn OK.



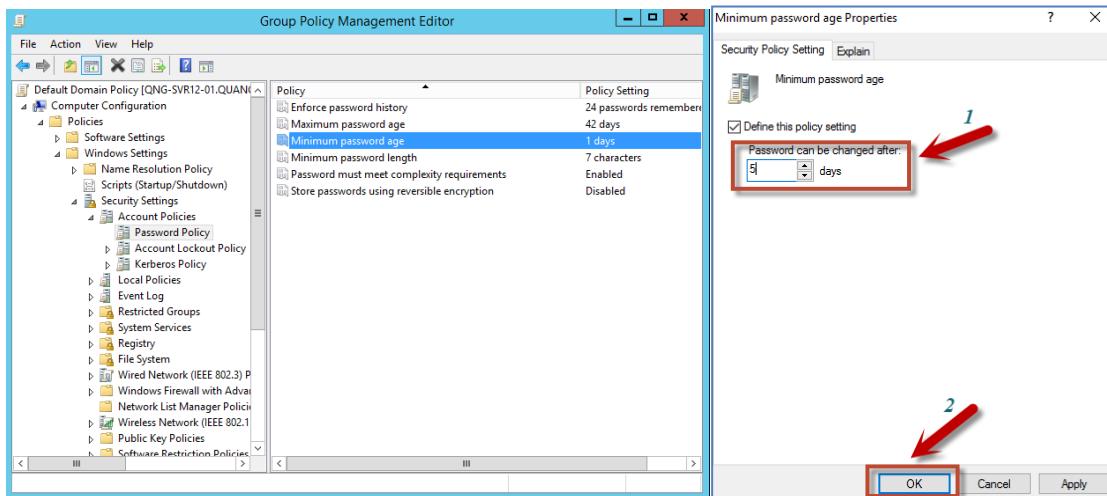
Hình 4.2. Thiết lập chiều dài tối thiểu cho mật khẩu.

Bước 5. Nhấn đúp chuột vào chính sách “Password must meet complexity requirements” để thiết lập độ phức tạp cho mật khẩu → Nhấn OK.



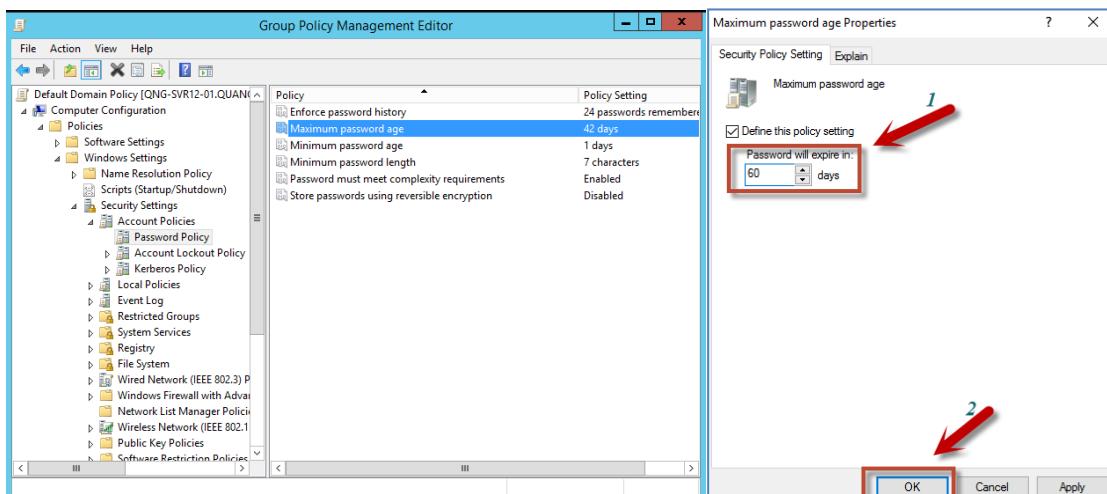
Hình 4.3. Thiết lập chế độ phức tạp cho mật khẩu.

Bước 6. Nhấp đúp chuột vào chính sách “Minimum password age” để thiết lập thời gian tối thiểu cho mật khẩu → Nhấn OK.



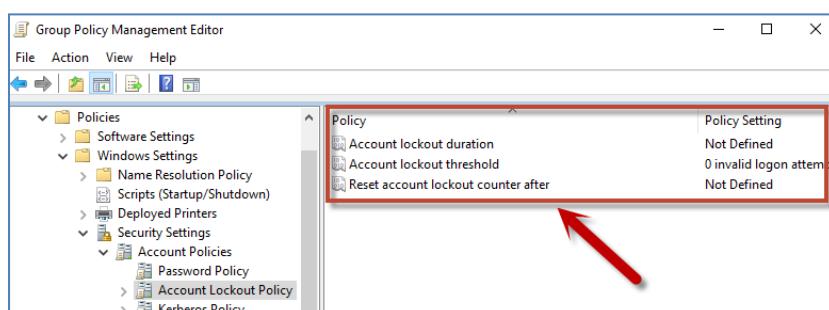
Hình 4.4. Thiết lập thời gian tối thiểu.

Bước 7. Nhấp đúp chuột vào chính sách “Maximum password age” để thiết lập thời gian sử dụng tối đa cho mật khẩu → Nhấn OK.



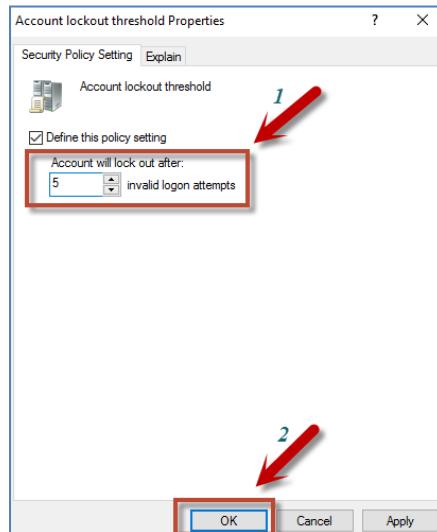
Hình 4.5. Thiết lập thời gian sử dụng tối đa.

Bước 8. Tại khung bên trái, chuyển qua phần Account Lockout Policy để thiết lập các chính sách về khóa tài khoản.



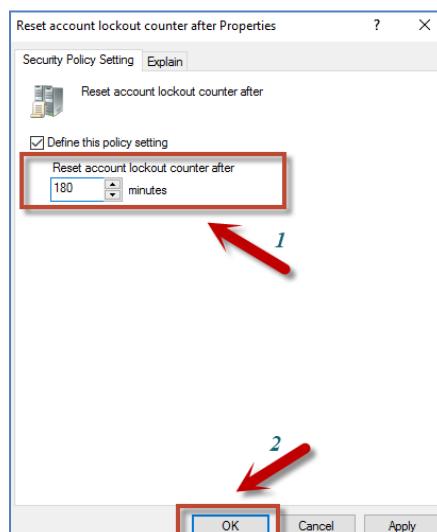
Hình 4.6. Thiết lập các chính sách về khóa tài khoản.

Bước 9. Nhấp đúp chuột vào chính sách “Account lockout threshold” để thiết lập số lần đăng nhập sai sẽ bị khóa tài khoản → Nhấn OK.



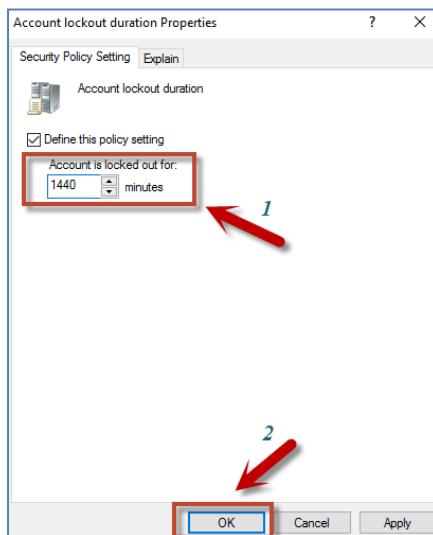
Hình 4.7. Thiết lập số lần đăng nhập sai sẽ bị khóa tài khoản.

Bước 10. Nhấn đúp chuột vào chính sách “Reset account lockout counter after” để thiết lập thời gian sẽ thiết lập lại bộ đếm số lần đăng nhập sai của người dùng → Nhấn OK.



Hình 4.8. Thời gian sẽ thiết lập lại bộ đếm số lần đăng nhập sai

Bước 11. Nhấp đúp chuột lên chính sách “Account lockout duration” để thiết lập thời gian khóa tài khoản nếu người dùng đăng nhập sai quá số lần quy định → Nhấn OK.



Hình 4.9. Thiết lập thời gian khóa tài khoản.

Bước 12. Mở PowerShell, và nhập câu lệnh để thực thi chính sách ngay lập tức: `gpupdate /force`

```
Administrator: Windows PowerShell
PS C:\Users\Administrator> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.
PS C:\Users\Administrator>
```

Hình 4.10. Thực thi chính sách ngay lập tức.

**Bài 2:** Nhằm tăng mức độ an toàn thông tin cho lãnh đạo đơn vị, bạn được yêu cầu xây dựng chính sách mật khẩu dành riêng cho ban giám đốc như sau:

- Mật khẩu phải có ít nhất 15 ký tự.
- Trong 5 lần liên tiếp không được đổi mật khẩu trùng nhau.
- Phải phức tạp.
- Thời gian tối thiểu: 5 ngày.
- Thời gian sử dụng tối đa: 30 ngày.
- Đăng nhập sai 3 lần trong 1 ngày thì tài khoản đó sẽ bị khóa 3 ngày.

Với vai trò là Quản trị viên bạn hãy thực hiện yêu cầu trên.

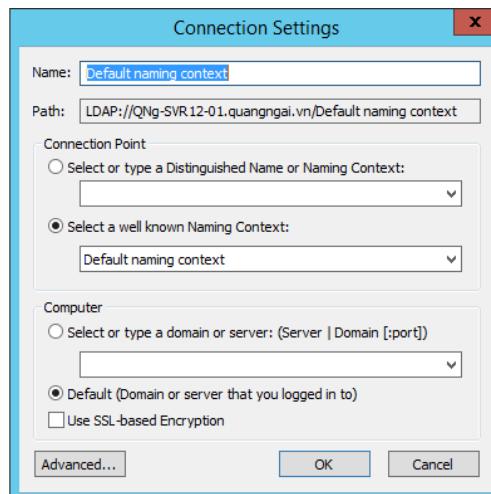
Bước 13. Mở công cụ ADSI Edit trong Administrative tools.

Bước 14. Nhấn phải chuột lên ADSI Edit → Chọn Connect to...



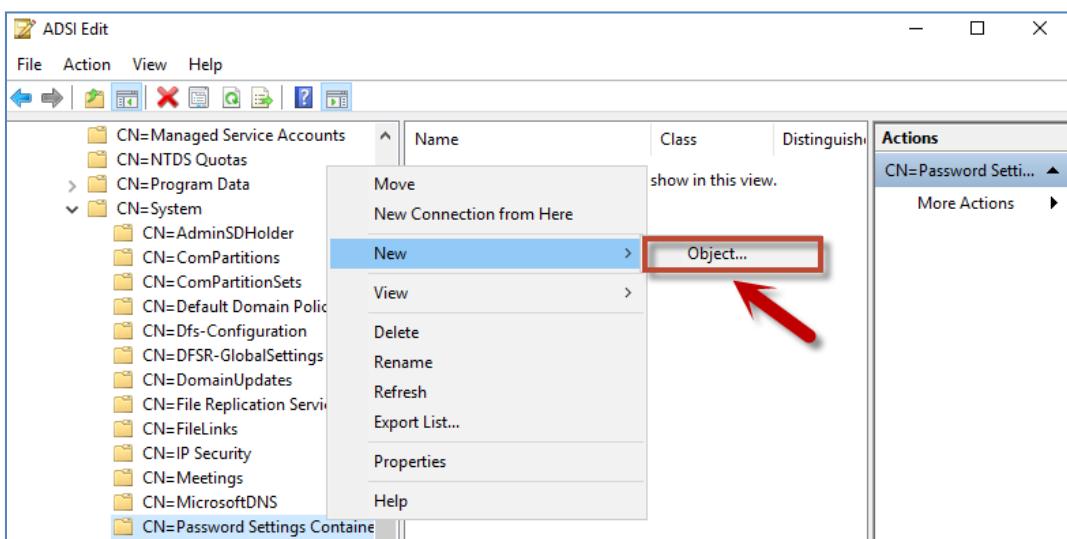
Hình 4.11. Thiết lập kết nối.

Bước 15. Tại hộp thoại Connection Settings, nhấn OK.



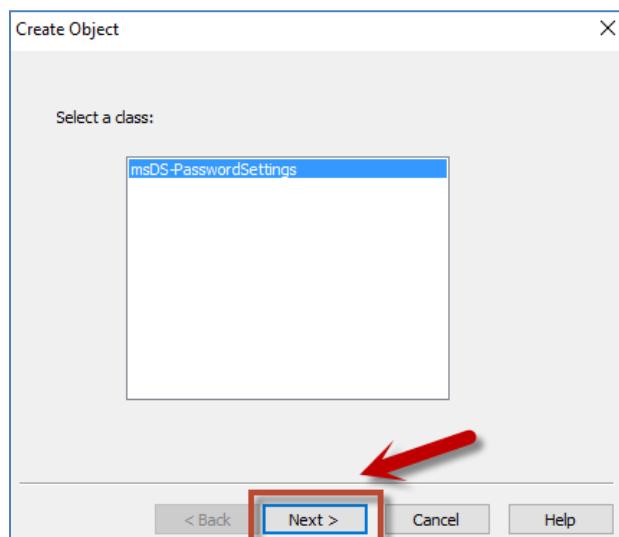
Hình 4.12. Lựa chọn thông tin kết nối.

Bước 16. Tại cấu trúc phân cấp ADSI, di chuyển đến “CN=Password Settings Container” → Nhấn phải chuột lên vùng bên phải chọn → New → Object.



Hình 4.13. Tạo mới một PSO.

Bước 17. Tại hộp thoại Create Object, nhấn Next.

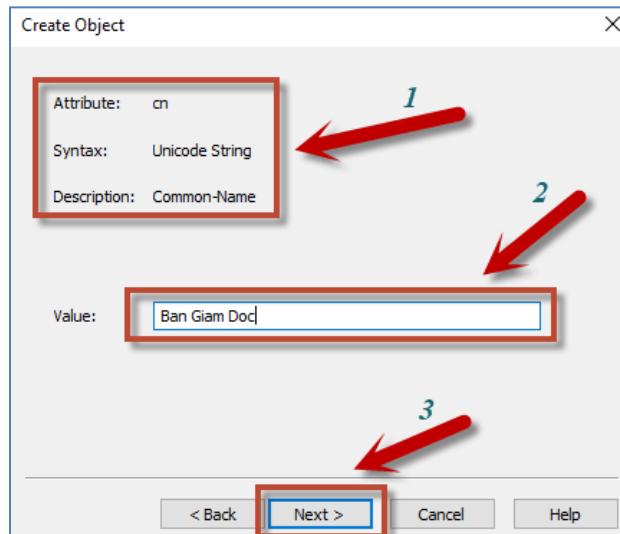


Hình 4.14. Hộp thoại tạo mới PSO.

Bước 18. Tại mục này, ta thấy có 3 thông tin:

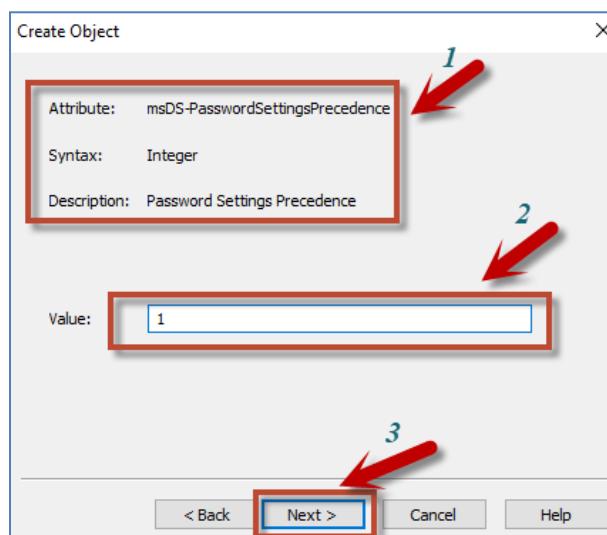
- **Description:** mô tả cho biết chức năng đang thiết lập.
- **Syntax:** cho biết giá trị phải nhập là kiểu dữ liệu gì (chuỗi, số, true/false,...) .
- **Value:** giá trị cần nhập cho mục này.

Tại hộp thoại này, nhập tên của PSO này → Nhấn Next.



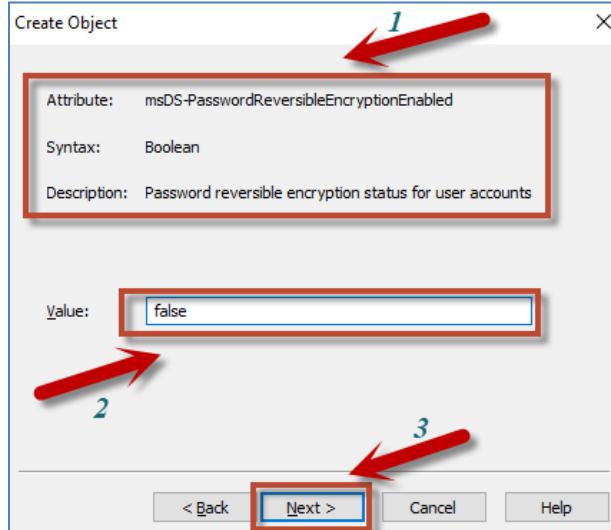
Hình 4.15. Thiết lập tên của PSO.

Bước 19. Thiết lập độ ưu tiên cho PSO. Giá trị càng nhỏ thì độ ưu tiên càng cao. Nhập độ ưu tiên vào mục Value → Nhấn Next.



Hình 4.16. Thiết lập độ ưu tiên cho PSO.

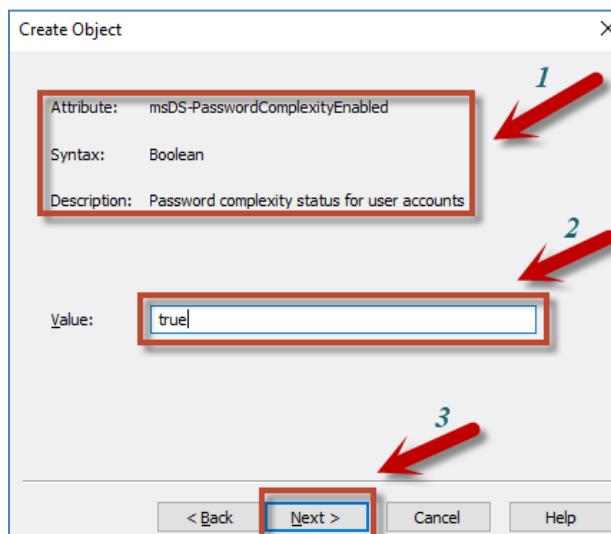
Bước 20. Không thiết lập nên nhập False → Nhấn Next.



Hình 4.17. Thiết lập chế độ mã hóa cho mật khẩu.

Bước 21. Mục này thiết lập lịch sử đổi mật khẩu. Nhập số lần đổi mật khẩu liên tiếp không được trùng → Nhấn Next.

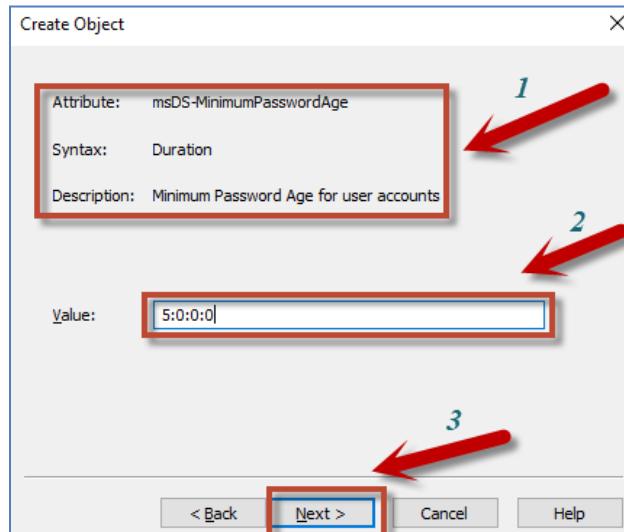
Bước 22. Mục này thiết lập độ phức tạp cho mật khẩu. Nhập true vào ô Value → Nhấn Next.



Hình 4.18. Thiết lập độ phức tạp cho mật khẩu.

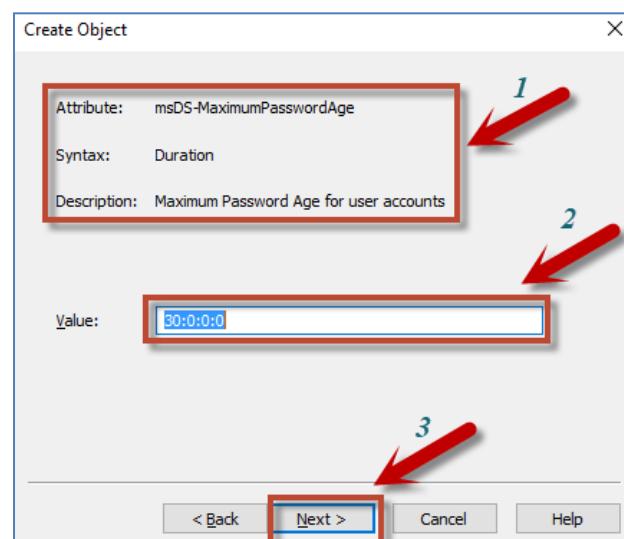
Bước 23. Mục này thiết lập số ký tự tối thiểu của mật khẩu. Nhập giá trị là 15 → Nhấn Next.

Bước 24. Mục này thiết lập thời gian tối thiểu cho mật khẩu. Thời gian (Duration) được biểu diễn theo cú pháp: Ngày:Giờ:Phút:Giây



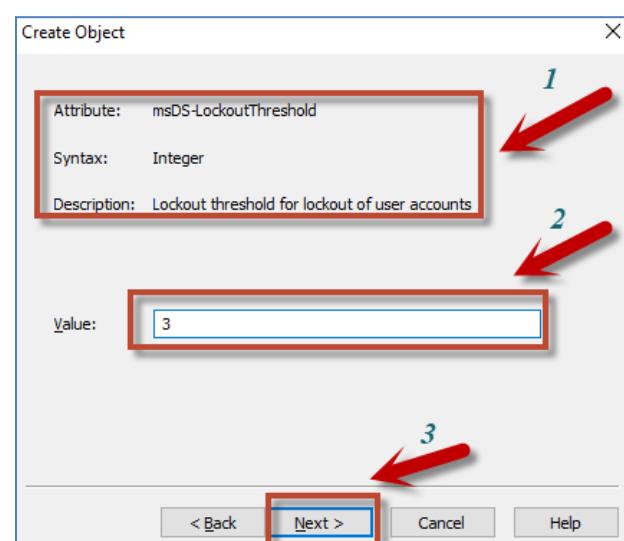
**Hình 2.1 - Thiết lập thời gian tối thiểu cho mật khẩu.**

Bước 25. Mục này thiết lập thời gian sử dụng tối đa cho mật khẩu.



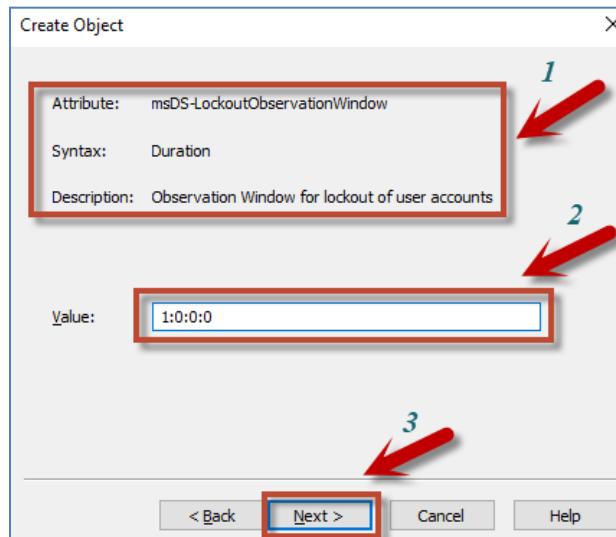
**Hình 2.2 - Thiết lập thời gian tối đa cho mật khẩu.**

Bước 26. Mục này thiết lập số lần đăng nhập sai cho phép.



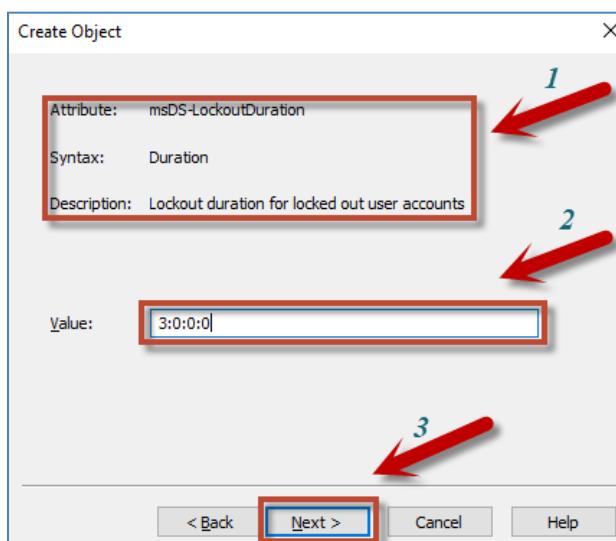
**Hình 2.3 - Thiết lập số lần đăng nhập sai cho người dùng.**

Bước 27. Mục này thiết đặt thời gian sẽ thiết lập lại bộ đếm số lần đăng nhập sai của người dùng.



**Hình 2.4 -** Thiết lập thời gian sẽ làm mới bộ đếm số lần đăng nhập sai.

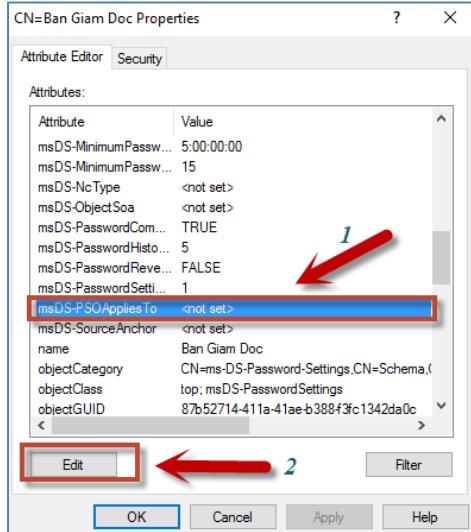
Bước 28. Mục này thiết lập thời gian tài khoản sẽ bị khóa nếu đăng nhập sai vượt quá số lần quy định.



**Hình 2.5 -** Thiết lập thời gian khóa tài khoản.

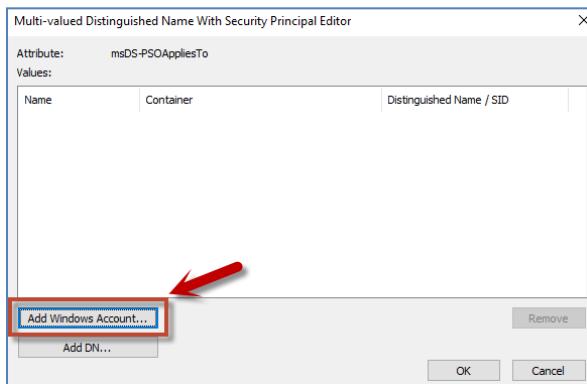
Bước 29. Nhấn Finish để kết thúc quá trình thiết lập cho PSO.

Bước 30. Nhấp đúp chuột lên PSO vừa tạo, chọn msDS-PSOAppliesTo → Edit để lựa chọn đối tượng chịu áp dụng của chính sách này.



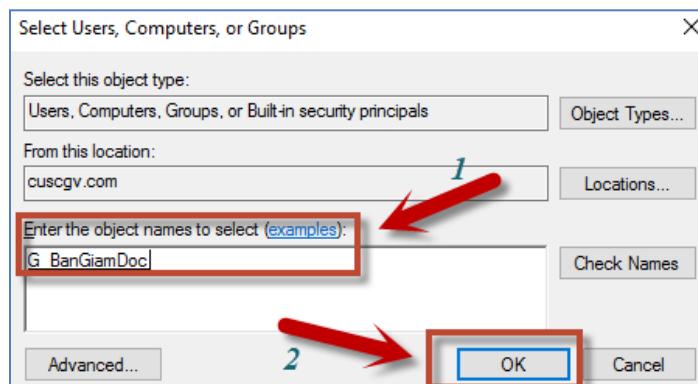
**Hình 2.6 - Thiết lập đối tượng chịu áp dụng của PSO.**

Bước 31. Một hộp thoại thiết lập mở ra, nhấn nút Add Windows Account...



**Hình 2.7 - Lựa chọn các tài khoản Windows.**

Bước 32. Nhập người dùng hoặc nhóm người dùng cần áp dụng chính sách → Nhấn OK 3 lần để kết thúc quá trình tạo và áp dụng PSO lên đối tượng.



Chọn người dùng hoặc nhóm người dùng sẽ chịu áp dụng PSO.

## CẤU HÌNH DỊCH VỤ DHCP

Dịch vụ DHCP (Dynamic Host Configuration Protocol): Là dịch vụ cho phép cấp phát động các thông số cấu hình mạng (địa chỉ IP, Subnet Mask, Default Gateway, Preferred DNS Server) cho các máy trạm (Client).

Trong đơn vị của bạn ngày càng có nhiều nhân viên sử dụng laptop, họ gặp phải rất nhiều khó khăn trong việc kết nối laptop của họ với hệ thống mạng của công ty. Trước tình hình đó, bạn được giao nhiệm vụ cài đặt và cấu hình dịch vụ DHCP server trên server đang chạy hệ điều hành Windows Server 2012 theo các thiết lập như sau:

- Dãy địa chỉ cấp phát: 172.18.206.1 tới 172.18.206.254.
- Dãy địa chỉ loại trừ: 172.18.206.1 tới 172.18.206.150. Đây là dãy địa chỉ IP đã được cấp phát tĩnh cho các máy tính trong hệ thống.
- Địa chỉ mặt nạ mạng con: 255.255.248.0 hay length = 21.
- Thời hạn sử dụng: 15 ngày.

Với vai trò là quản trị viên bạn hãy thực hiện yêu cầu này.

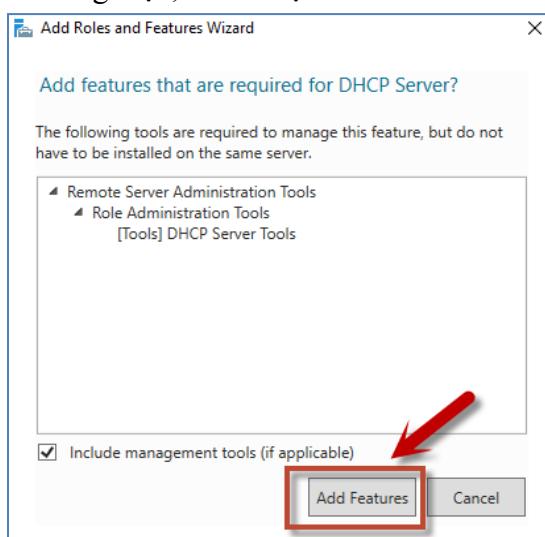
Bước 1. Mở công cụ Server Manager và nhấp vào “Add Roles and Features”.

Bước 2. Tại màn hình “Before you begin”, nhấp Next để tiếp tục.

Bước 3. Tại màn hình “Select installation type”, nhấp chọn “Role-based or feature-based installation” và sau đó nhấp Next.

Bước 4. Tại màn hình “Select destination server”, nhấp chọn “Select a server from the Server pool” và chọn máy chủ cần cài đặt dịch vụ trong mục Server pool. Sau đó nhấp Next.

Bước 5. Nhấp chọn mục “DHCP Server” từ danh sách các dịch vụ. Ngay khi nhấp chọn “DHCP Server”, một cửa sổ xuất hiện, nhấp chọn “Add Features”.



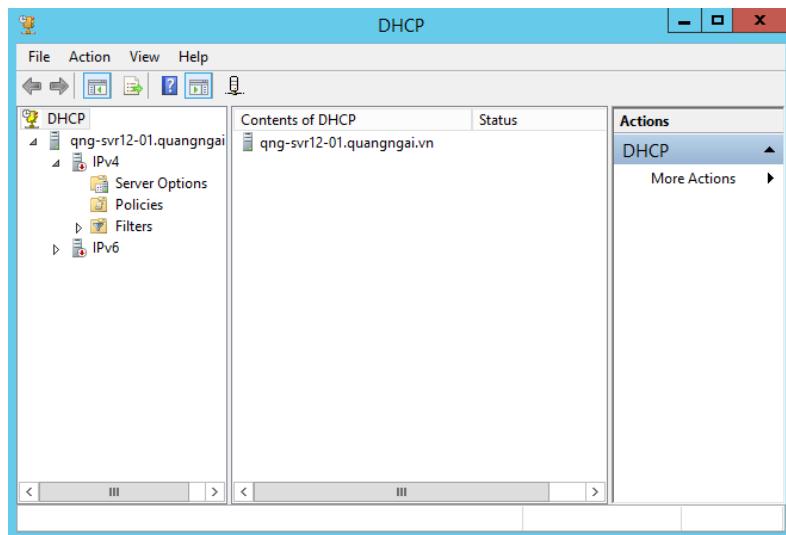
Hình 5.1. Thêm các tính năng bổ sung cho dịch vụ.

Bước 6. Tại màn hình “Select features”, nhấp Next.

Bước 7. Tại màn hình “DHCP Server”, nhấp Next sau khi đã đọc xong.

Bước 8. Nhấp Install để bắt đầu cài đặt.

Bước 9. Mở công cụ Windows Administrative tool → DHCP.

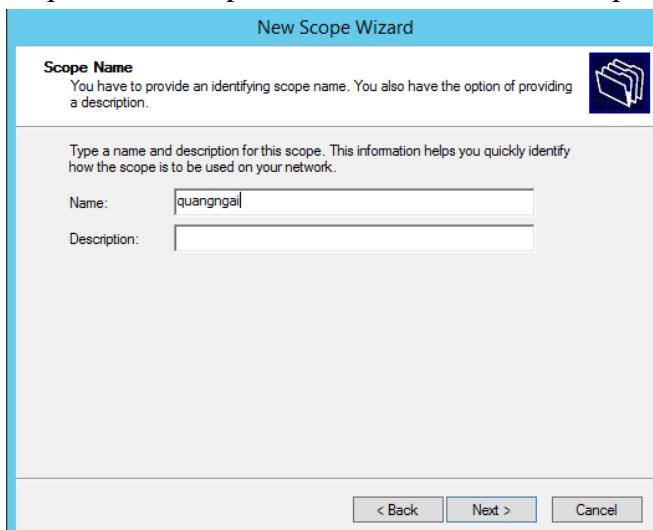


Hình 5.2. Giao diện chính của công cụ quản trị DHCP.

Bước 10. Nhấn phím chuột lên mục IPv4 → chọn New Scope.

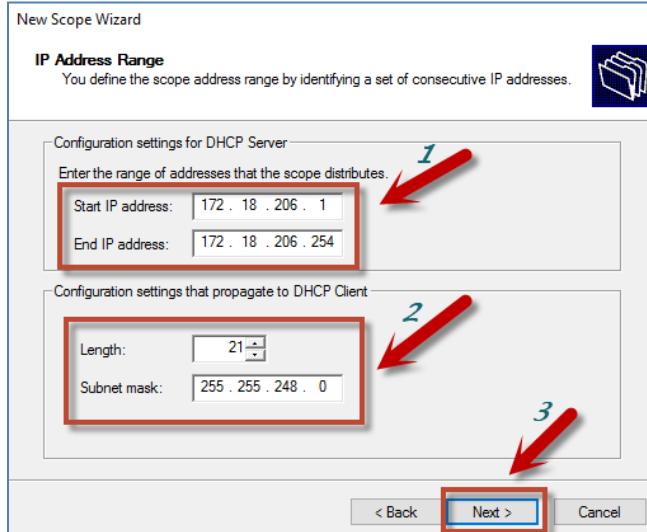
Bước 11. Tại màn hình “Welcome to the New Scope Wizard” → Nhấn Next để tiếp tục.

Bước 12. Nhập tên cho Scope vào ô “Scope Name” và nhấn Next để tiếp tục.



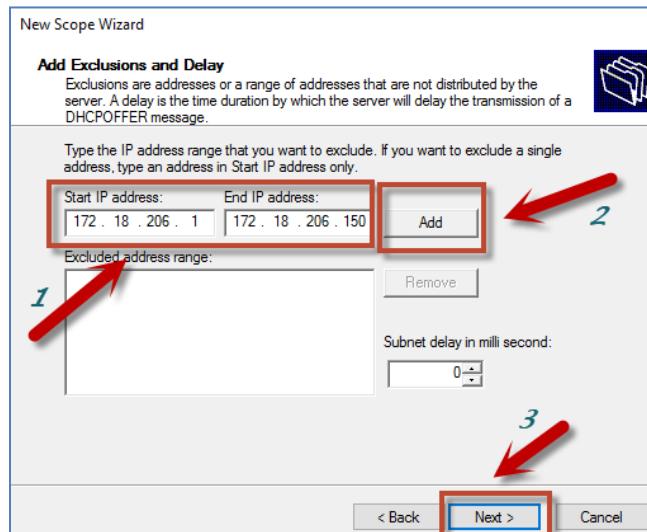
Hình 5.3. Nhập các thông tin cơ bản về Scope.

Bước 13. Tại màn hình thiết lập dãy địa chỉ IP sẽ cấp phát cho người dùng, nhập dãy IP cấp phát vào hai ô “Start IP address” và “End IP address”. Nhập giá trị của cho Subnet Mask vào ô “Length” hoặc ô “Subnet mask”. Sau đó nhấn Next để tiếp tục.



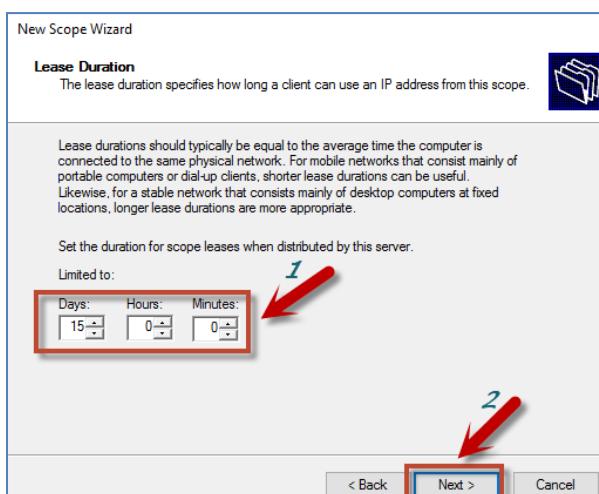
Hình 5.4. Nhập dãy IP sẽ sử dụng để cấp phát.

Bước 14. Tại màn hình thiết lập dãy IP loại trừ, nhập dãy IP sẽ không cấp phát cho người dùng vào hai ô “Start IP address” và “End IP address” → Nhấn nút Add. Sau đó nhấn Next.



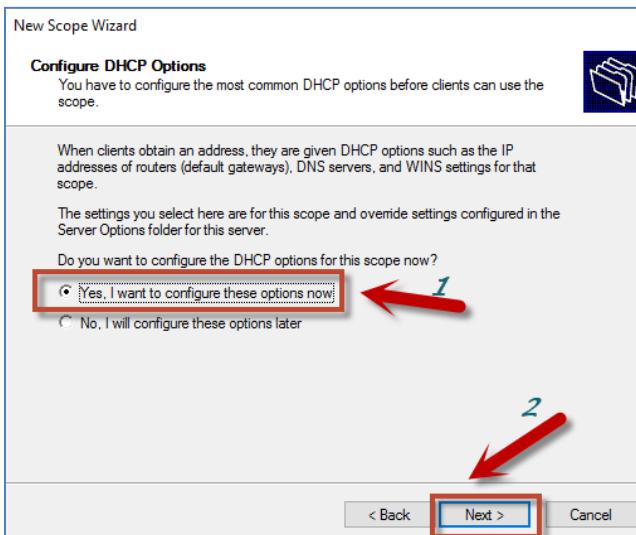
Hình 5.5. Nhập dãy IP không cấp phát cho người dùng.

Thiết lập thời gian hết hạn của địa chỉ IP cấp phát cho người dùng. Sau đó nhấn Next.



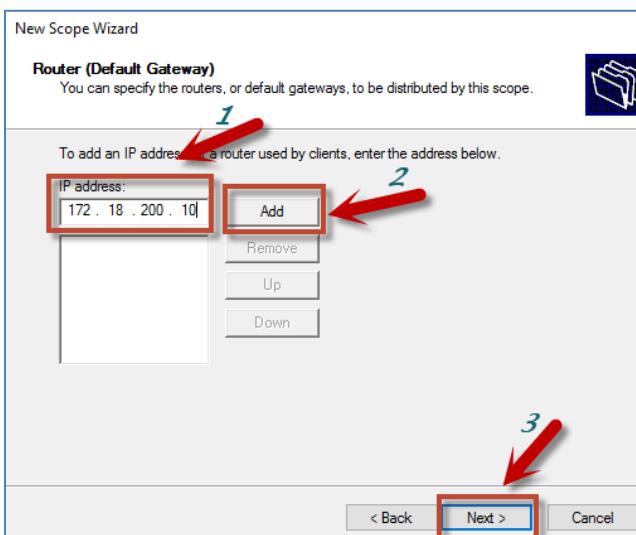
Hình 5.6. Thiết lập thời gian sử dụng của IP động.

Bước 15. Tại màn hình lựa chọn thiết lập các giá trị tùy chọn bổ sung, nhấn chọn “Yes, I want to configure these options now”. Sau đó nhấn Next.



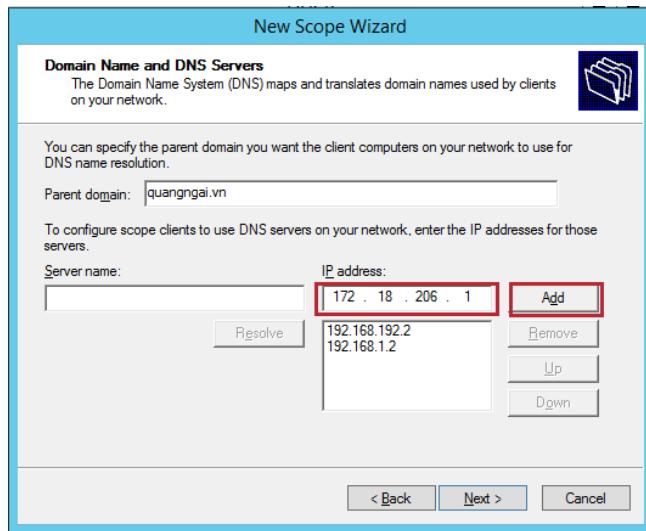
Hình 5.7. Cấu hình các tùy chọn bổ sung

Bước 16. Tại màn hình thiết lập giá trị cho Default Gateway, nhập địa chỉ IP của Router vào ô “IP address” và nhấn Add. Sau đó nhấn Next để tiếp tục.



Hình 5.8. Thiết lập Default Gateway.

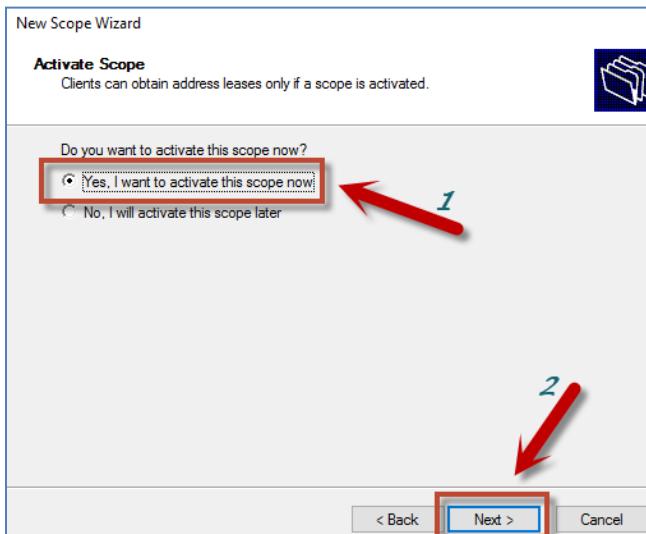
Bước 17. Tại màn hình thiết lập Domain Name and DNS Servers, nhập địa chỉ IP của máy chủ DNS vào ô “IP address” và nhấn Next.



Hình 5.9. Thiết lập DNS.

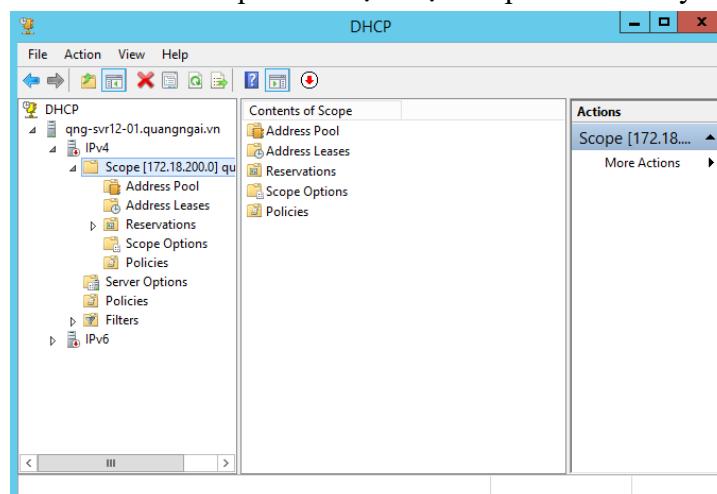
Bước 18. Tại màn hình thiết lập WINS Servers, nhấn nút Next.

Bước 19. Tại màn hình Activate Scope, chọn “Yes, I want to activate this scope now” và nhấn nút Next.



Hình 5.10. Kích hoạt cho Scope vừa tạo.

Bước 20. Nhấn Finish để kết thúc quá trình tạo một Scope và dưới đây là kết quả thu được.



Hình 5.11. Kết quả sau khi tạo xong một Scope.

## **Chia sẻ địa chỉ máy in**

Hiện nay trong đơn vị của bạn có một máy in mạng dùng chung, bạn muốn máy in này cũng sử dụng địa chỉ IP động. Tuy nhiên, nếu một máy in sử dụng địa chỉ IP động sẽ dẫn đến tình huống có thể IP sẽ khác nhau cho mỗi ngày và điều đó sẽ gây khó khăn cho nhân viên khi thực hiện việc in ấn vì không biết địa chỉ IP của máy in là bao nhiêu? Với vai trò là quản trị viên, bạn hãy cấu hình thiết lập để máy in mạng đó chỉ nhận đúng duy nhất một địa chỉ IP do bạn thiết lập trước trên máy chủ DHCP.

*Bước 1.* Tạo một Scope theo các bước ở bài tập 1 của chương này.

*Bước 2.* Tại mục Reservation của Scope, tiến hành tạo mới một địa chỉ.

*Bước 3.* Nhập địa chỉ MAC của máy trạm.

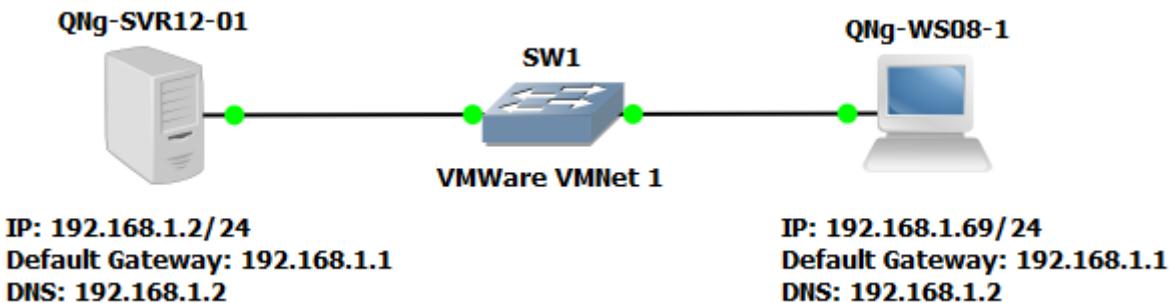
*Bước 4.* Nhập địa chỉ IP sẽ cấp phát cho máy trạm đó.

*Bước 5.* Lưu lại và tiến hành kiểm tra kết quả.

---

## CẤU HÌNH DỊCH VỤ IIS

IIS (Internet Information Services), dịch vụ thông tin Internet, là các dịch vụ dành cho máy chủ chạy trên nền Windows nhằm cung cấp và phân tán nội dung số lên mạng thông qua Web (HTTP) và FTP.



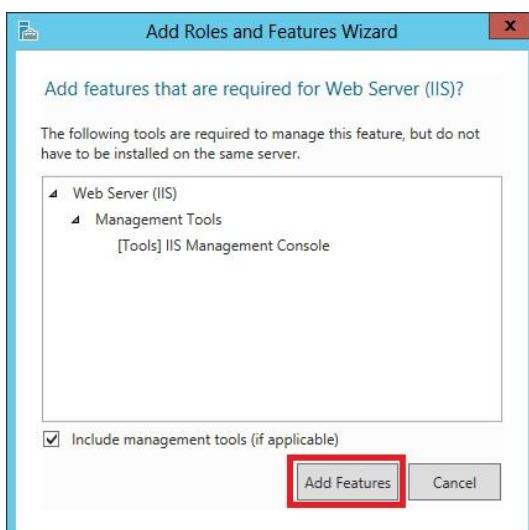
### 6.1 Cài đặt dịch vụ IIS

Với vai trò là quản trị viên bạn hãy thực hiện yêu cầu trên bằng cách cài đặt và cấu hình dịch vụ IIS.

Bước 1. Thăng cấp máy chủ lên DC và cài đặt DNS (quangngai.vn).

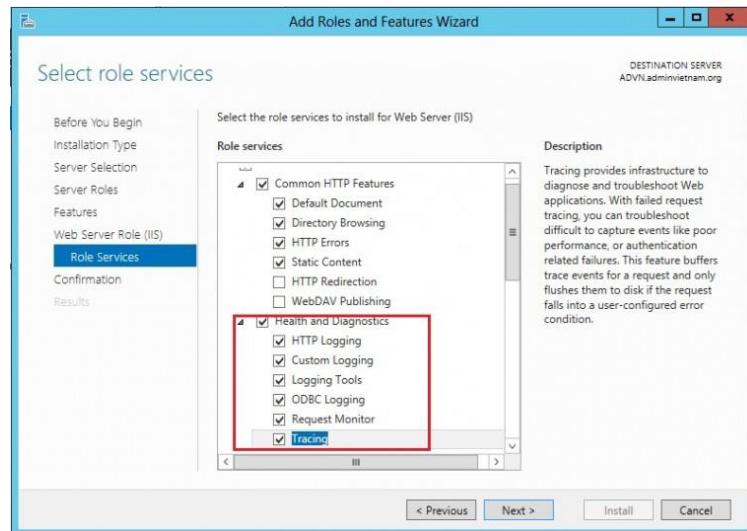
Bước 2. Cài đặt IIS: tại công cụ "Server Manager", chọn "Add roles and features".

Bước 3. Tại màn hình "Select server roles", chọn "Web Server (IIS)" và nhấn Add Features như hình 2.1



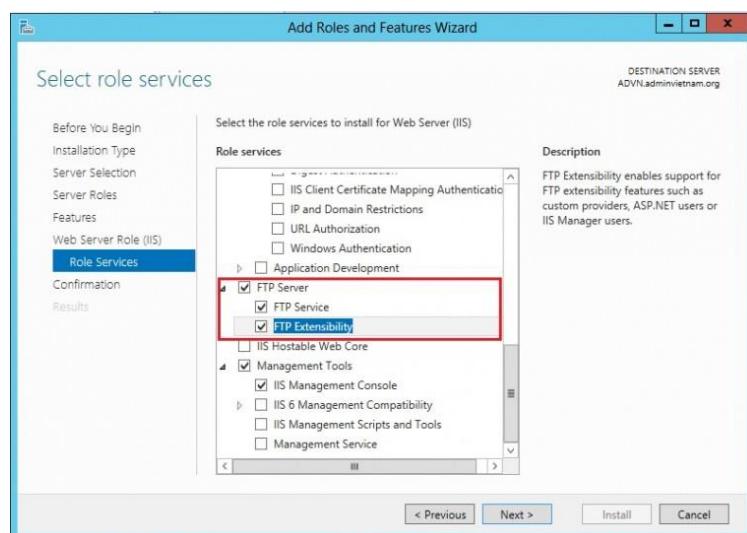
Hình 6.1. Cài đặt dịch vụ IIS.

Bước 4. Nhấn Next và chọn Role Services cho Web (http).



Hình 6.2. Chọn Role Services cho HTTP.

Bước 5. Để cài đặt thêm FTP, kéo thanh cuộn xuống và chọn FTP Server như hình, sau đó nhấn Next và Installation.



Hình 6.3. Chọn Role Services cho FTP.

Bước 6. Chọn IIS trong Server Manager, chuột phải lên Default Website, chọn Properties, chọn địa chỉ IP của máy chủ trong ô IP Address sau đó nhấn OK.

## 6.2 Kiểm tra dịch vụ WEB :

Trên trình duyệt Web của máy chủ hoặc máy trạm gõ địa chỉ IP của máy chủ:



Hình 6.4. Dịch vụ WEB chạy thành công.

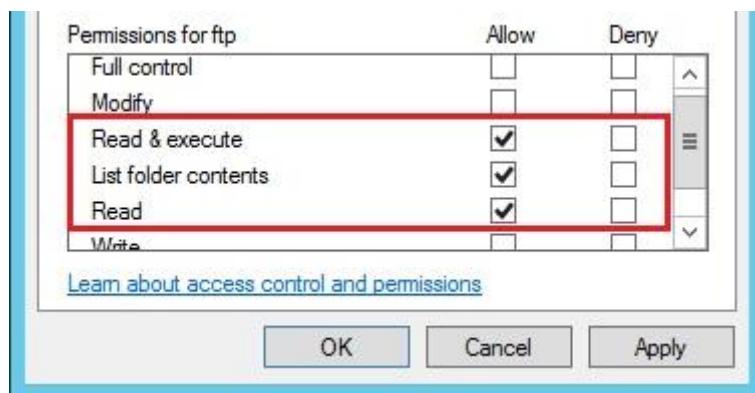
### 6.3 Cấu hình dịch vụ FTP

Bước 1. Tạo 1 thư mục FTP ở ổ đĩa C, trong thư mục này tạo 1 file Test.txt có nội dung ‘Dịch vụ FTP chạy thành công’ để kiểm tra dịch vụ.

Bước 2. Tạo user ftp

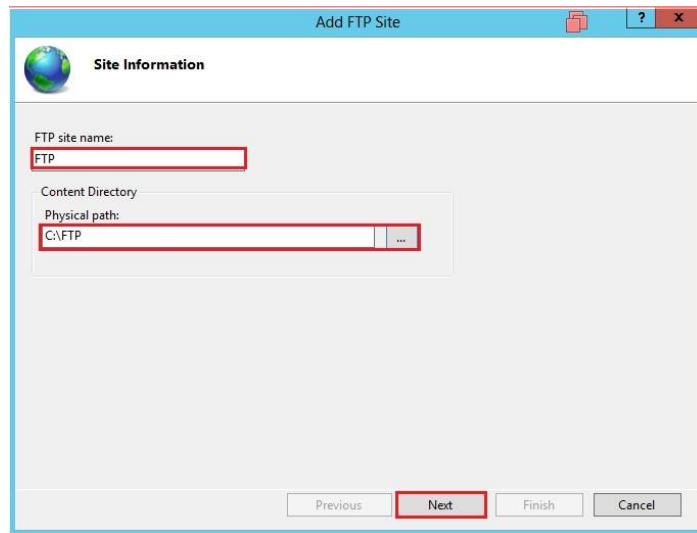
Bước 3. Cấp quyền cho user này truy cập vào thư mục FTP như sau:

- Chuột phải lên thư mục FTP, chọn Properties
- Chọn Security, chọn Edit, chọn Add
- Gõ ftp vào ô **Enter the object names to select**, sau đó chọn OK
- Kiểm tra user ftp được các quyền Đọc (Read), Thực thi (Execute) và Liệt kê thư mục (List), sau đó chọn OK.



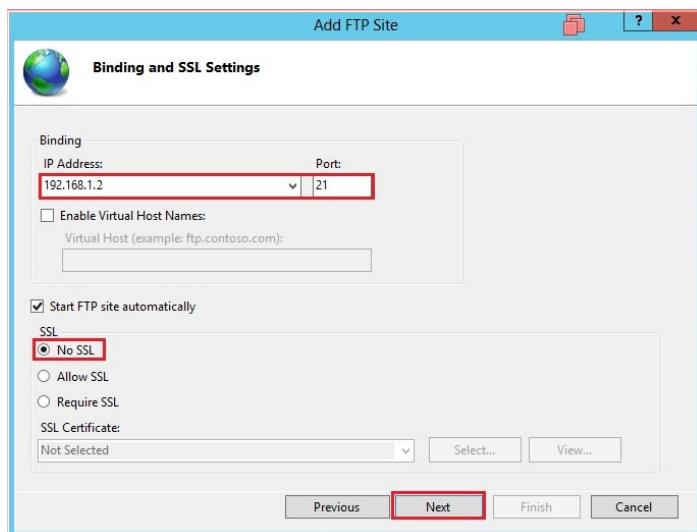
Hình 6.5. Cấp quyền cho user ftp.

Bước 4. Chọn IIS trong Server Manager, chuột phải chọn Internet Information Services (IIS) Manager, chuột phải lên Sites chọn Add FTP Site, nhập vào tên và chọn đường dẫn về thư mục FTP đã tạo, nhấn Next.



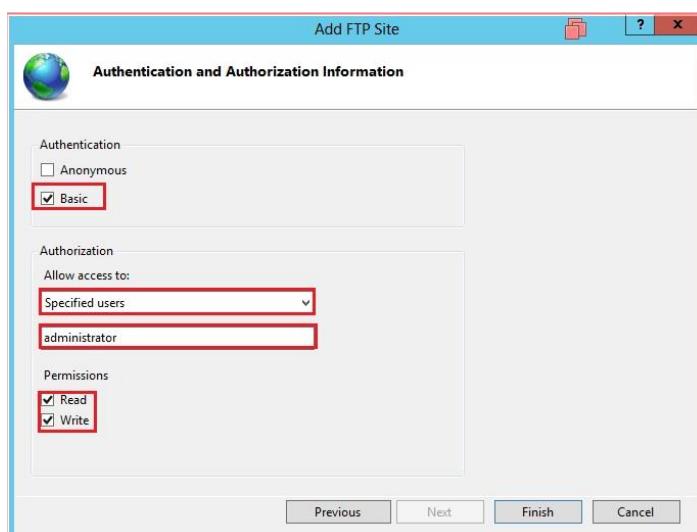
Hình 6.6. Add FTP Site.

Bước 5. Gán địa chỉ IP của máy chủ, chọn các mục như hình dưới đây, sau đó chọn Next.



Hình 6.7. Gán IP và chọn các mục.

Bước 6. Chọn xác thực (Authentication), Cấp quyền (Authorization) và chỉ định người dùng (Specified Users) như hình dưới, sau đó chọn Finish.



Hình 6.8. Authentication, Authorization và Specified users.

Bước 7. Trên IIS Manager, chuột phải lên FTP chọn Add Allow Rule và chỉ định người dùng (Specified Users) ftp như hình dưới, sau đó chọn OK.



Hình 6.9. Chỉ định và cấp quyền cho user ftp.

#### 6.4 Kiểm tra dịch vụ FTP

Bước 1. Mở trình duyệt web trên máy trạm và gõ `ftp://192.168.1.2` để truy cập vào FTP Server, nhập username, password của administrator hoặc ftp.

Bước 2. Nội dung được cung cấp bởi FTP server sẽ hiện ra như sau



Hình 6.10. Dịch vụ FTP chạy thành công.

**LƯU Ý:** trong quá trình đăng nhập bằng tài khoản ftp nếu không login được các bạn có thể viết đầy đủ username gồm user và domain để đăng nhập (ví dụ `ftp@quangngai.vn`)

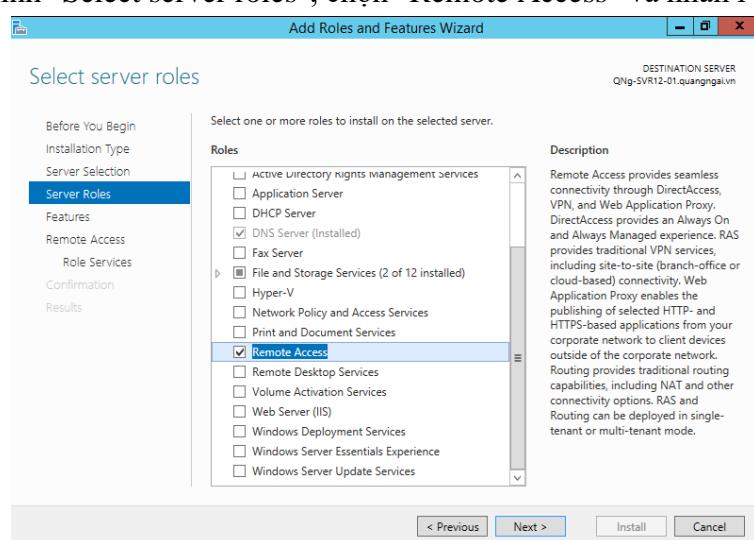


## CẤU HÌNH DỊCH VỤ VPN

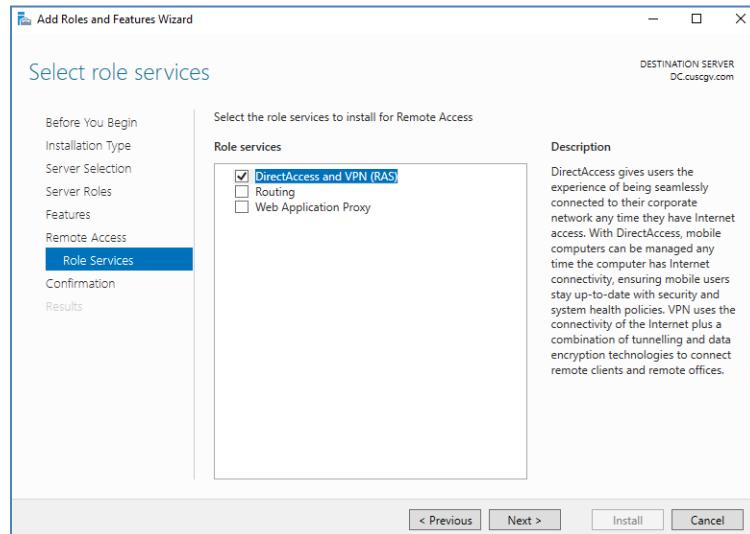
Do nhu cầu mở rộng hoạt động, nên có nhiều nhân viên của đơn vị thường xuyên phải đi công tác. Tuy nhiên, những nhân viên này lại cần phải truy cập vào các tài nguyên được đặt trong hệ thống mạng của công ty. Để đáp ứng nhu cầu này, bạn được yêu cầu cài đặt dịch vụ truy cập từ xa cho những nhân viên thường xuyên đi công tác.

Với vai trò là quản trị viên bạn hãy thực hiện yêu cầu trên.

- Bước 1. Gắn thêm một NIC cho máy Server và thiết lập địa chỉ IP là: 10.0.0.100/24.
- Bước 2. Tại công cụ "Server Manager", chọn "Add roles and features".
- Bước 3. Tại màn hình "Select installation type", chọn "Role-based or feature-based installation". Sau đó nhấn Next.
- Bước 4. Tại màn hình "Select destination server", chọn máy chủ cần cài đặt và nhấn Next.
- Bước 5. Tại màn hình "Select server roles", chọn "Remote Access" và nhấn Next.



- Bước 6. Tại màn hình "Select features", nhấn Next.
- Bước 7. Tại màn hình "Remote Access", xem qua các thông tin mô tả về dịch vụ. Sau đó nhấn Next để tiếp tục.
- Bước 8. Tại màn hình "Select role services", nhấn chọn "DirectAccess and VPN (RAS)". Một hộp thoại yêu cầu cài đặt các công cụ bổ sung xuất hiện, nhấn "Add features". Sau đó nhấn Next để tiếp tục quá trình cài đặt.

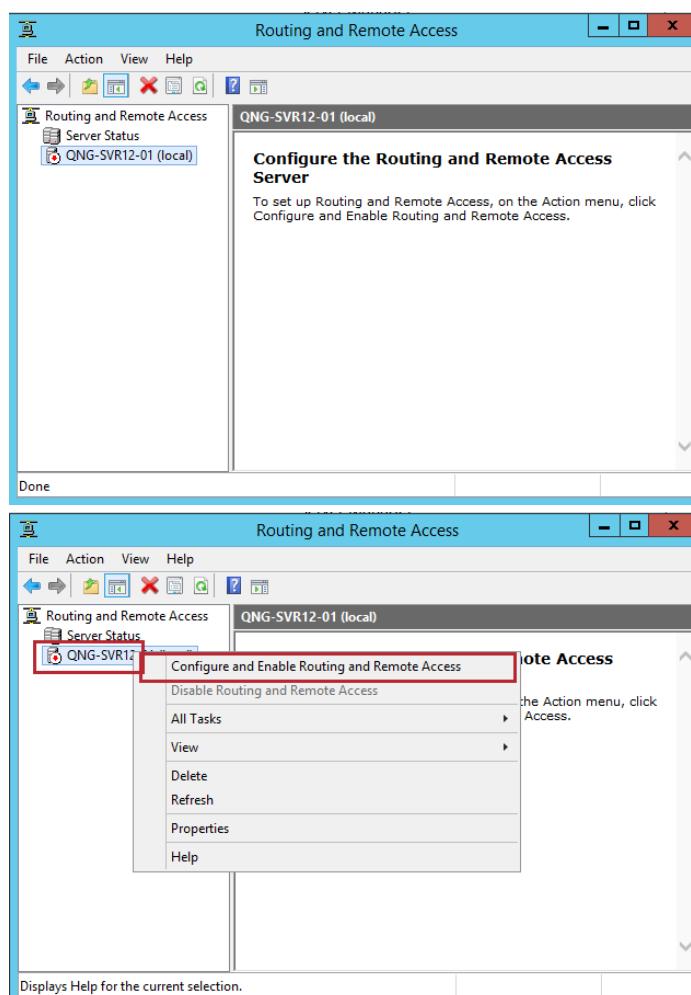


Hình 7.1. Cài đặt dịch vụ VPN.

Bước 9. Nhấn Install để bắt đầu cài đặt.

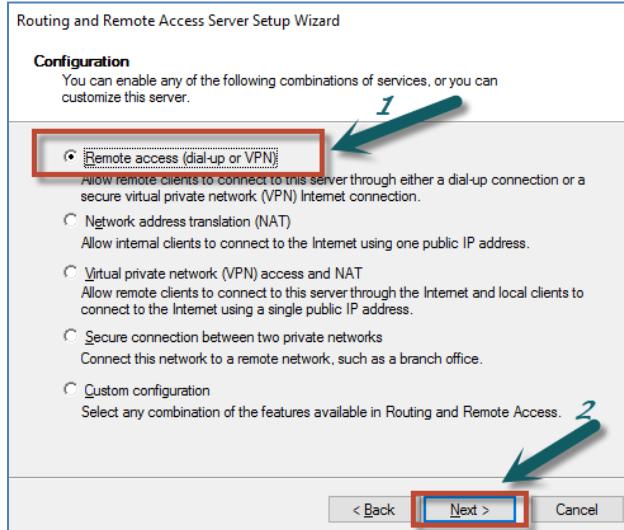
Bước 10. Mở công cụ "Routing and Remote Access" trong Server Manager → Tools

Bước 11. Nhấn phải chuột vào tên máy tính và chọn "Configure and Enable Routing and Remote Access".



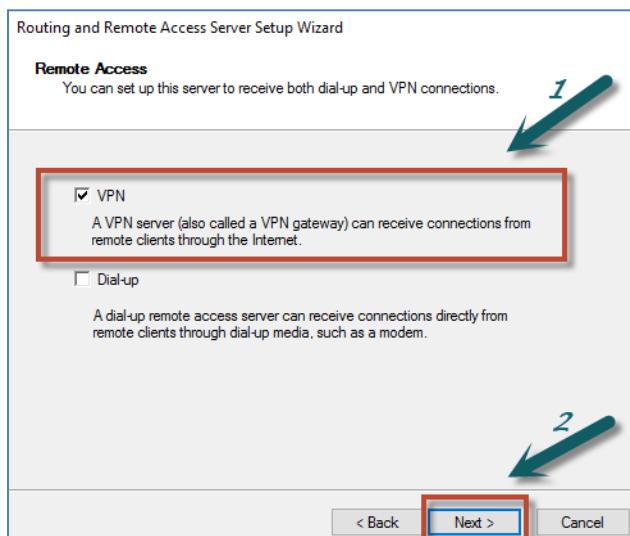
Bước 12. Một hộp thoại xuất hiện, nhấn Next.

Bước 13. Tại màn hình "Configuration", chọn "Remote access (dial-up or VPN)" và nhấn Next.



Hình 7.2. Cấu hình VPN.

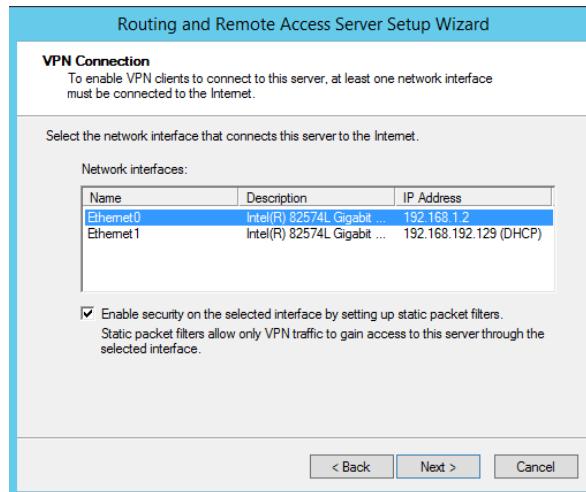
Bước 14. Tại màn hình "Remote Access", nhấn chọn VPN và sau đó nhấn Next.



Hình 7.3. Lựa chọn loại kết nối.

Bước 15. Tại màn hình thiết lập "VPN Connection", thiết lập các thông số như bên dưới. Sau đó nhấn Next.

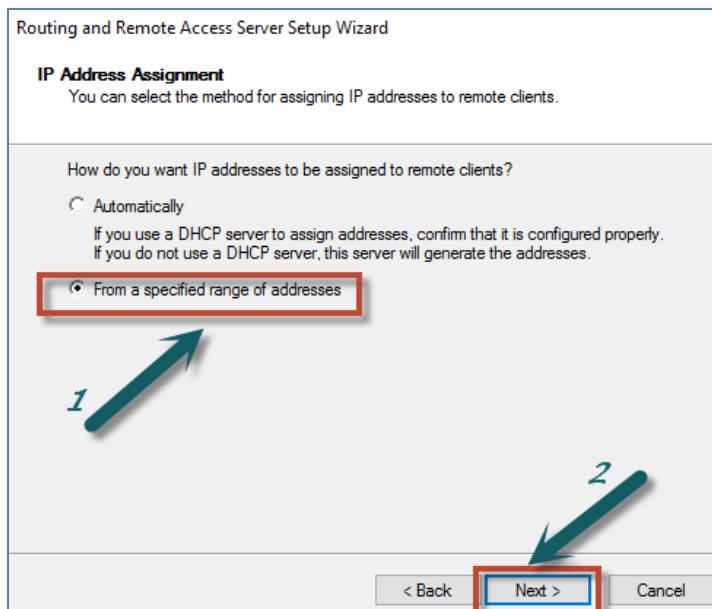
- **Network interfaces** : chọn NIC sẽ kết nối ra bên ngoài Internet.
- Bỏ chọn tại mục "**Enable security on the selected interface by setting up static packet filters**"



Hình 7.4. Thiết lập NIC cho kết nối VPN.

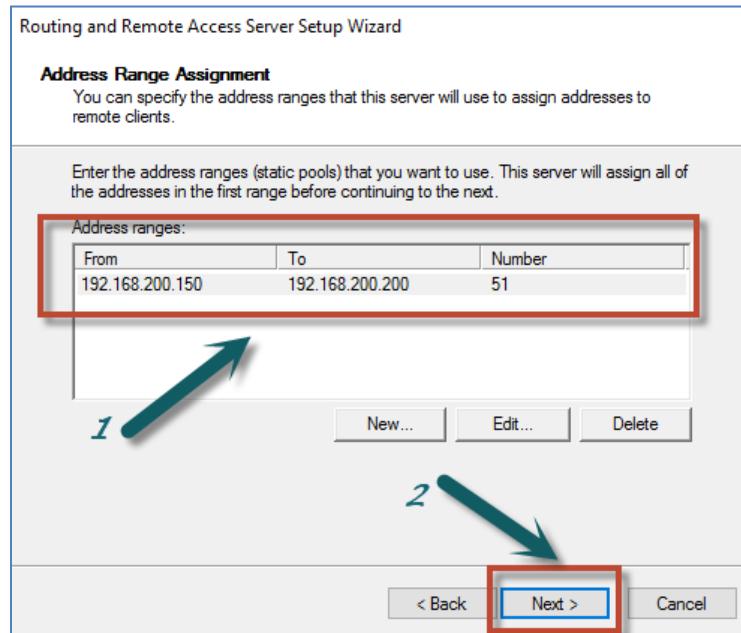
Bước 16. Tại màn hình "IP Address Assignment", chúng ta chọn mục "From a specified range of addresses".

- **Automatically** : chọn mục này khi trong hệ thống đã có sẵn dịch vụ DHCP.
- **From a specified range of address** : chọn mục này khi trong hệ thống chưa có dịch vụ DHCP.



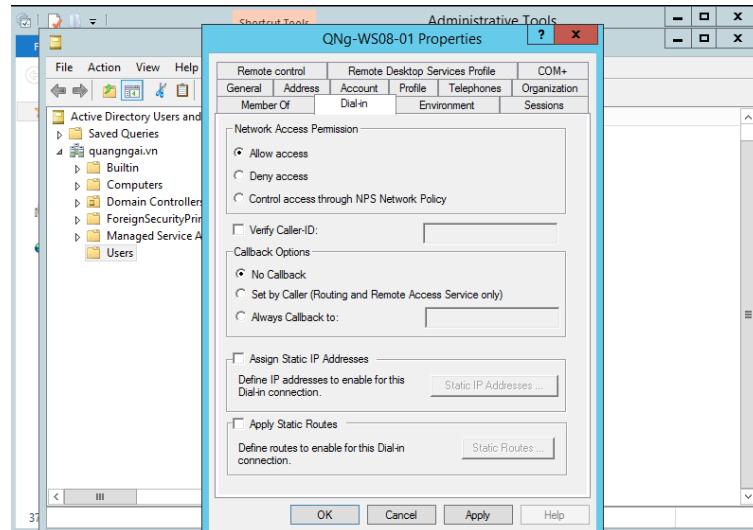
Hình 7.5. Chọn cơ chế cấp phát IP cho VPN Client.

Bước 17. Tại màn hình "Address Range Assingment", nhấn New và nhập dãy IP sẽ cấp phát cho người dùng.



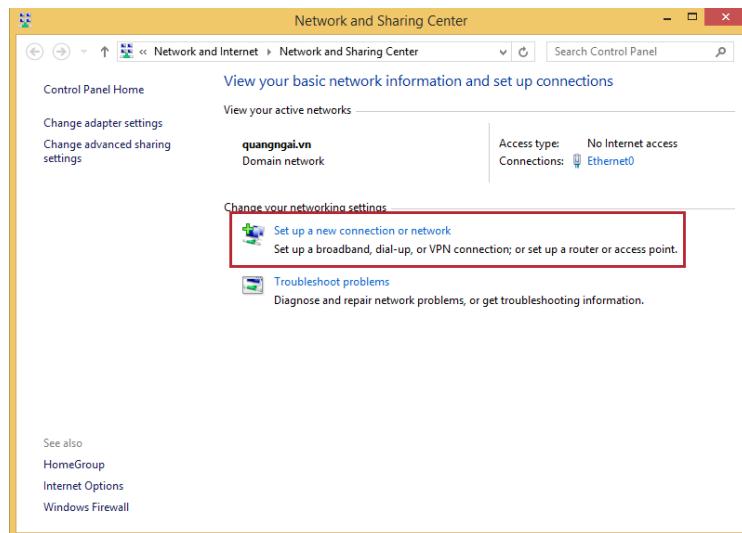
Hình 7.6. Thiết lập dãy IP cấp phát cho VPN Client.

- Bước 18. Tại màn hình "Managing Multiple Remote Access Servers", chọn "No, use Routing and Remote Access to authenticate connection requests". Sau đó nhấn Next.
- Bước 19. Nhấn Finish để kết thúc quá trình cấu hình.
- Bước 20. Nhấn Ok để khởi động dịch vụ.
- Bước 21. Trên máy DC, tại công cụ "Active Directory Users and Computers", nhấp đúp chuột vào tài khoản cho phép sử dụng VPN và di chuyển đến thẻ "Dial-in".
- Bước 22. Tại mục "Network Access Permission", chọn "Allow access".



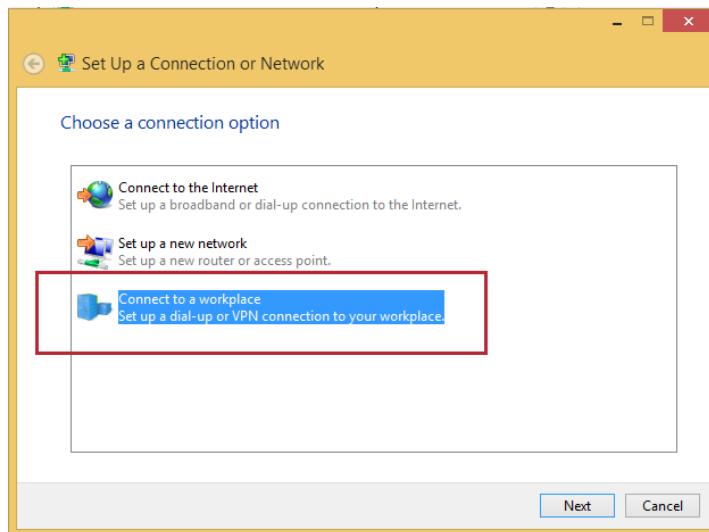
Hình 7.7. Cho phép tài khoản được phép kết nối từ xa.

- Bước 23. Trên máy Client kết nối VPN, mở công cụ "Network and Sharing Center". Nhấn chọn "Set up a new connection or network".

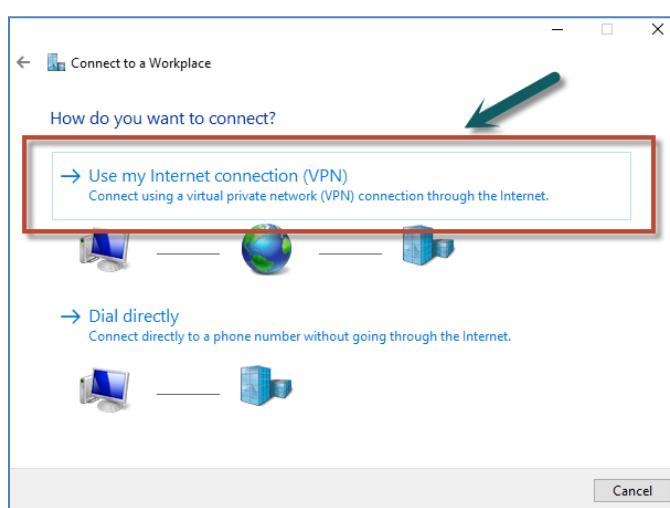


Hình 7.8. Thiết lập kết nối VPN trên máy Client.

Bước 24. Tại màn hình "Choose a connection option", nhấn chọn "Connect to a workplace" → Nhấn Next.

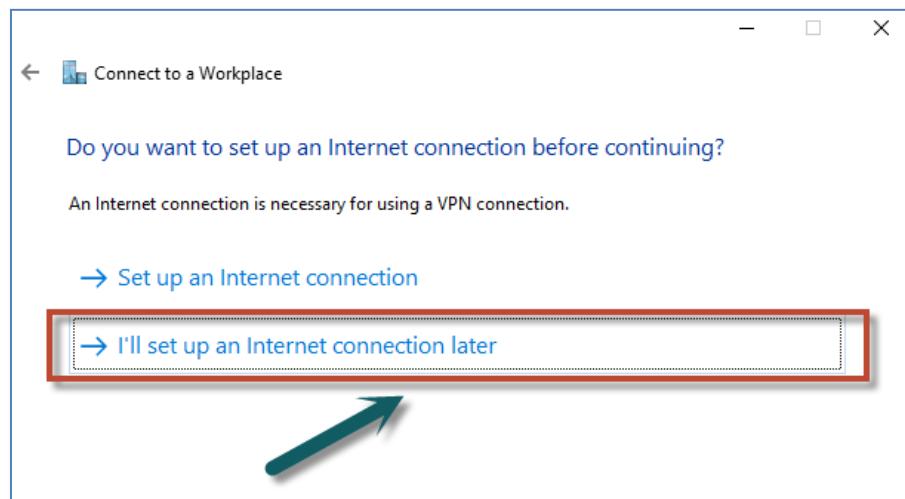


Bước 25. Tại màn hình "How do you want to connect?", nhấn chọn "Use my Internet connection (VPN)".



Hình 7.9. Chọn kết nối VPN.

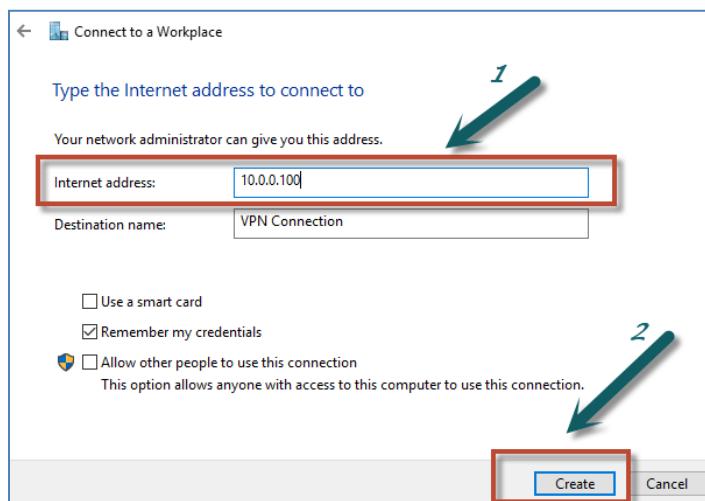
Bước 26. Tại màn hình "Do you want to set up an Internet connection before continuing?", chọn "I'll set up an Internet connection later".



Hình 7.10. Bỏ qua thiết lập Internet.

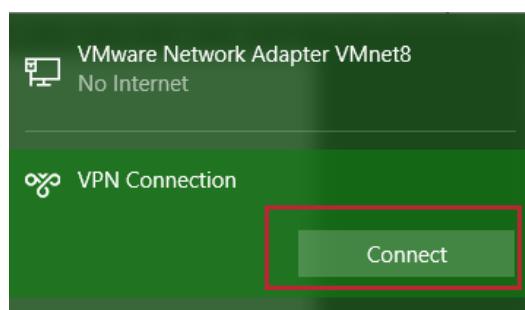
Bước 27. Thiết lập các thông tin cho kết nối VPN.

- **Internet Address** : nhập địa chỉ IP nhánh Internet của VPN Server. Sau đó nhấn **Create**.



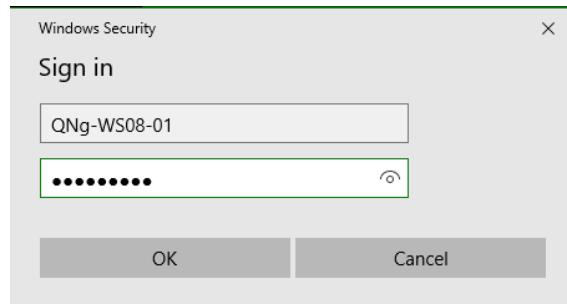
Hình 7.11. Thiết lập cho kết nối VPN.

Bước 28. Tiến hành kết nối VPN.



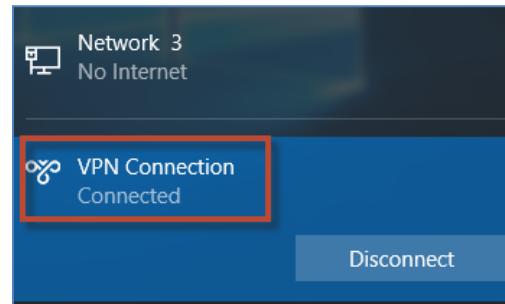
Hình 7.12. Thực hiện kết nối VPN.

Bước 29. Hộp thoại chứng thực xuất hiện, nhập thông tin chứng thực.



Hình 7.13. Chứng thực khi kết nối VPN.

Bước 30. Kết nối thành công.



Hình 7.14. Kết nối VPN thành công.

Bước 31. Kiểm tra địa chỉ IP khi VPN thành công.

```
PPP adapter VPN Connection:

Connection-specific DNS Suffix . :
IPv4 Address . . . . . : 192.168.200.152
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0
```

Hình 7.15. IP nhận được khi kết nối thành công.

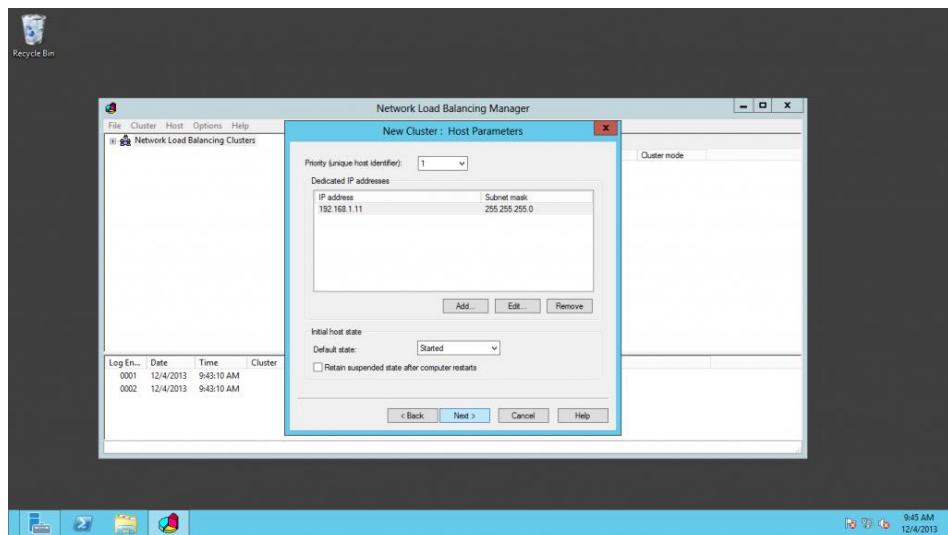
Tại thời điểm ban đầu, các website với khả năng mở rộng lớn thường được thiết kế để phục vụ hàng triệu yêu cầu mỗi ngày, sau đó nó được nâng cấp để phục vụ thêm nếu như có yêu cầu. Để phục vụ được hàng chục triệu lượt truy cập mỗi ngày, website cần phải đáp ứng được yêu cầu về khả năng mở rộng (Scalability), về tính linh hoạt (Flexibility), tính đáp ứng (Responsiveness), tính sẵn sàng cao (High Availability), tránh được thời gian chết của hệ thống (downtime impact), khả năng bảo trì tốt và được xây dựng với giá thành tốt nhất.



Để cân bằng tải (Network Load Balancing), tăng tốc duyệt Web và dự phòng cho máy chủ chính (192.168.1.11/24), công ty thêm 1 máy chủ phụ (192.168.1.12/24) như sơ đồ trên, trong đó IP: 192.168.1.13/24 là IP đại diện cho cả 2 máy chủ. Với vai trò là quản trị viên bạn hãy thực hiện yêu cầu trên bằng cách triển khai dịch vụ cân bằng tải (Network Load Balancing).

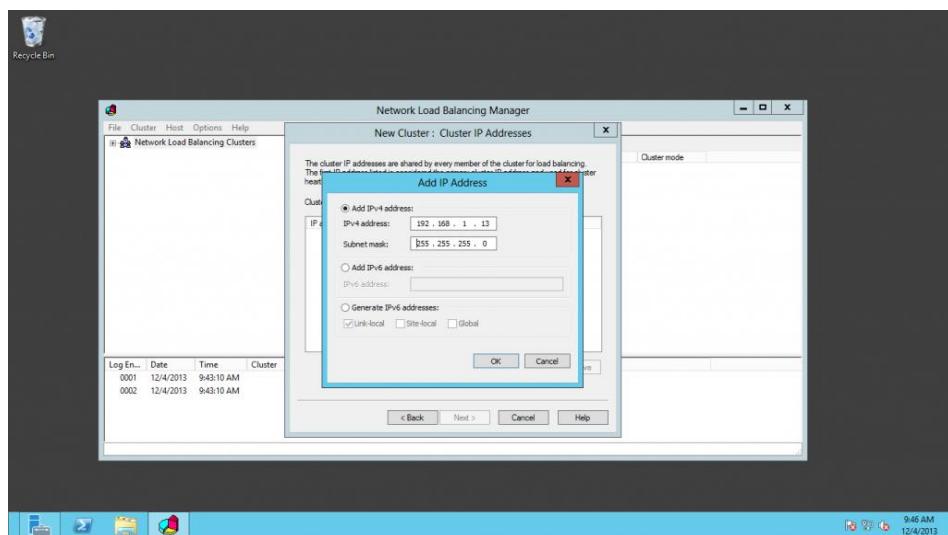
## 8.1 Cài đặt dịch vụ NLB

- Bước 1. Sử dụng chức năng Clone (nhân bản) của VMWare để tạo thêm 1 máy chủ
- Bước 2. Từ máy chủ đã cho. Thay đổi IP các máy chủ theo sơ đồ. Gia nhập các máy trạm và máy chủ vào domain: quangngai.vn
- Bước 3. Cài đặt và kiểm tra dịch vụ IIS trên 2 máy chủ.
- Bước 4. Cài đặt dịch vụ Network Load Balancing : tại công cụ "Server Manager", chọn "Add roles and features".
- Bước 5. Tại màn hình "Select installation type", chọn "Role-based or feature-based installation". Sau đó nhấn Next.
- Bước 6. Tại màn hình "Server Selection", chọn máy chủ cần cài đặt và nhấn Next.
- Bước 7. Tại màn hình "Select server roles", chọn "Network Load Balancing" và nhấn Next.
- Bước 8. Nhấn Install để bắt đầu cài đặt.
- Bước 9. Sau khi cài đặt xong, tìm và mở "Network Load Balancing" trong Server Manager hoặc Administrative Tool hoặc Control Panel.
- Bước 10. Nhấn phải chuột vào "Network Load Balancing Clusters" và chọn New Cluster.
- Bước 11. Nhập IP của máy chủ thứ nhất (192.168.1.11), nhấn Next.
- Bước 12. Thiết lập độ ưu tiên của máy chủ là 1 sau đó nhấn Next



Hình 8.1. Thiết lập độ ưu tiên.

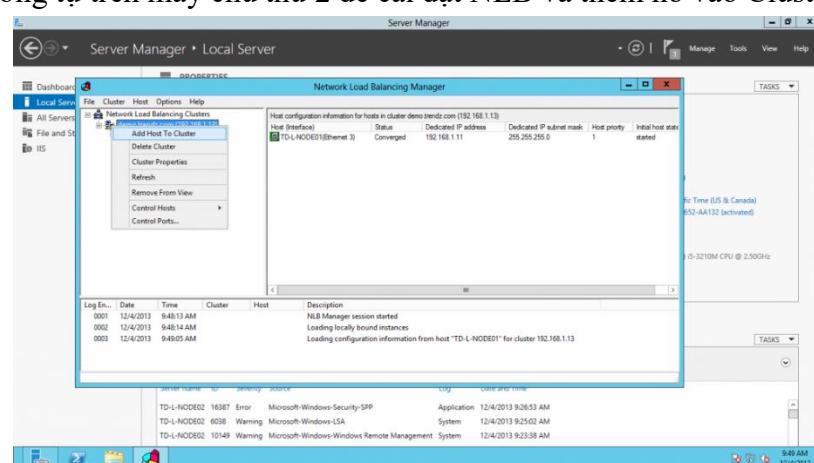
Bước 13. Nhấn Add để thêm địa chỉ đại diện cho 2 máy chủ (192.168.1.13/24) và sau đó nhấn OK.



Hình 8.2. Thiết lập địa chỉ đại diện.

Bước 14. Gõ vào ô Full Internet name tên miền đã thiết lập, chọn Multicast và sau đó nhấn Next.

Bước 15. Làm tương tự trên máy chủ thứ 2 để cài đặt NLB và thêm nó vào Cluster đã tạo.



Hình 8.3. Thêm máy chủ thứ 2 vào Cluster.

Bước 16. Thiết lập chê độ ưu tiên (Priority) là 2, nhấn Next. Sau đó nhấn Finish.

## 8.2 Kiểm tra NLB

Bước 17. Đăng nhập vào Domain Controller, vào DNS, thêm bản ghi Host A cho Cluster đã tạo.

Bước 18. Kiểm tra dịch vụ NLB và IIS trên 2 máy chủ và địa chỉ IP đại diện.



Hình 8.1. Dịch vụ NLB và IIS chạy thành công.

## Bài 9

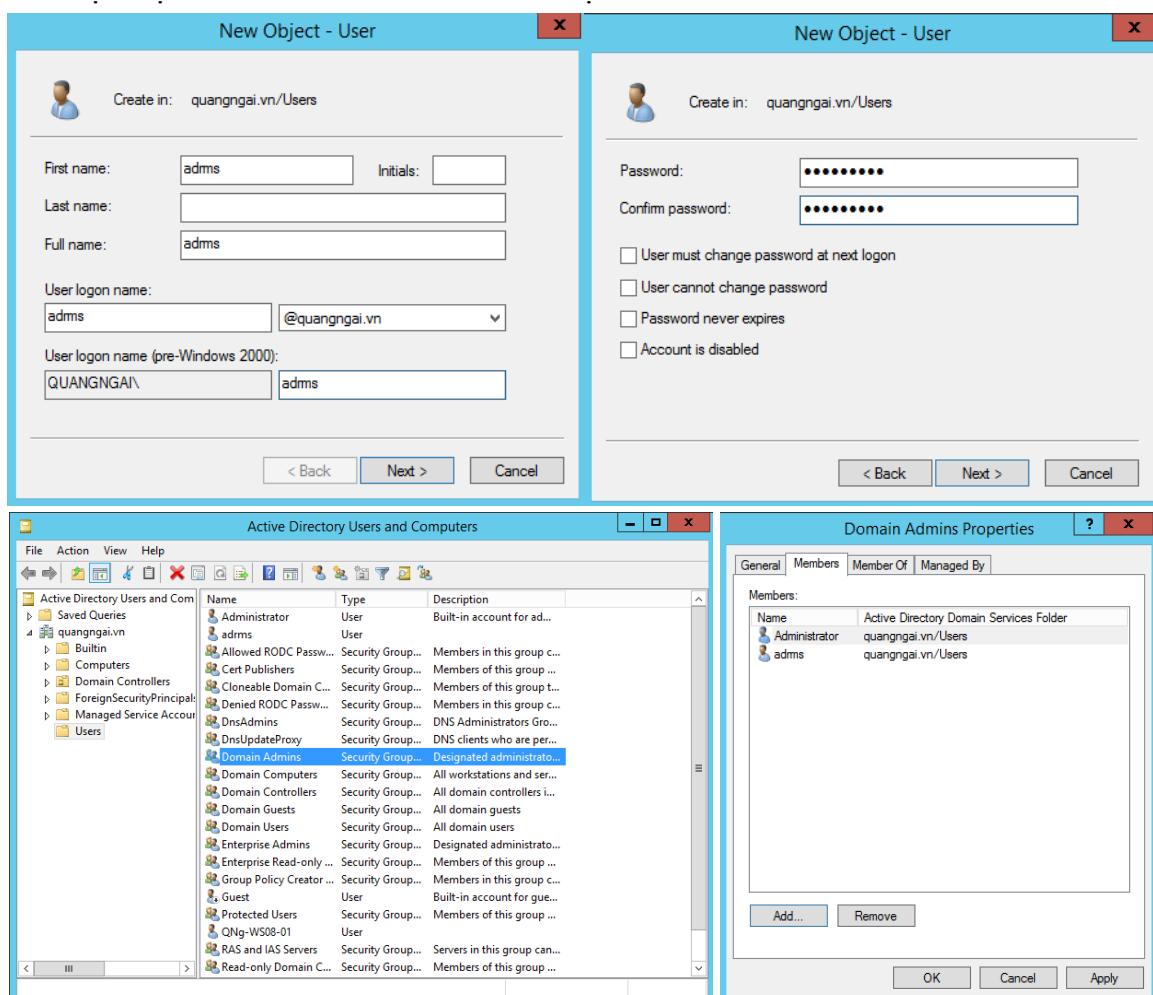
# CẤU HÌNH DỊCH VỤ AD RMS

Active Directory Rights Management Service (AD RMS) là dịch vụ được tích hợp sẵn trong Windows cho phép bảo vệ các tài liệu nhạy cảm trong doanh nghiệp bằng cách cho phép người dùng tùy ý phân quyền trên các tài liệu của mình và ngăn chặn việc đưa các tài liệu nhạy cảm ra khỏi môi trường doanh nghiệp. Phần này trình bày các thao tác cài đặt và cấu hình AD RMS để phân quyền và bảo vệ các tài liệu trong tổ chức, phân quyền cho người dùng thuộc tổ chức khác và tích hợp với Dynamic Access Control (DAC) Jump để tự động bảo vệ các tài liệu nhạy cảm dựa theo điều kiện xác định.

Hiện nay tổ chức của bạn đang có rất nhiều tài liệu chia sẻ với người dùng trong tổ chức, tuy nhiên với các quyền chia sẻ và NTFS khi cho phép người dùng đọc tài liệu thì đồng nghĩa với việc cũng cho những người dùng đó quyền sao chép tài liệu, in ấn, ... Lãnh đạo đơn vị phân công bạn hãy tìm và cài đặt một dịch vụ giúp có thể phân quyền trên tài nguyên được chặt chẽ hơn. Sau một khoảng thời gian tìm hiểu, bạn biết đến dịch vụ AD RMS và báo cáo với lãnh đạo. Sau đó bạn được yêu cầu cài đặt dịch vụ này.

Với vai trò là quản trị viên hệ thống, bạn hãy thực hiện yêu cầu trên.

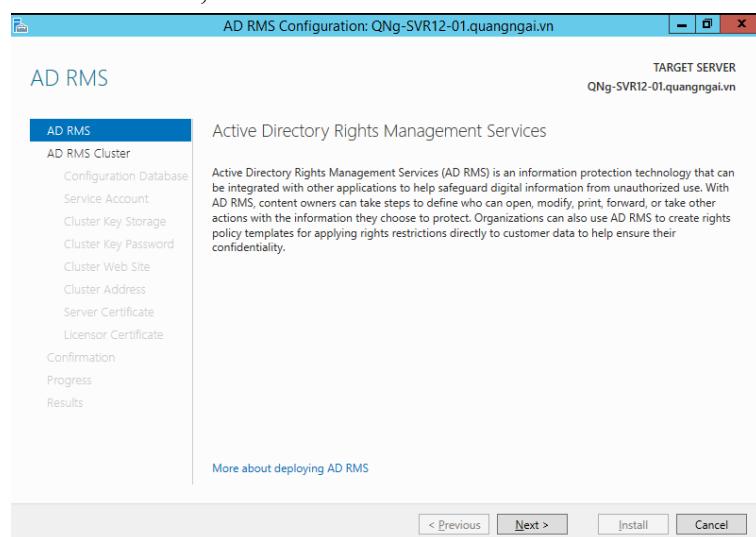
Bước 1. Tạo một tài khoản có tên là "adrms" thuộc nhóm "Domain Admins".



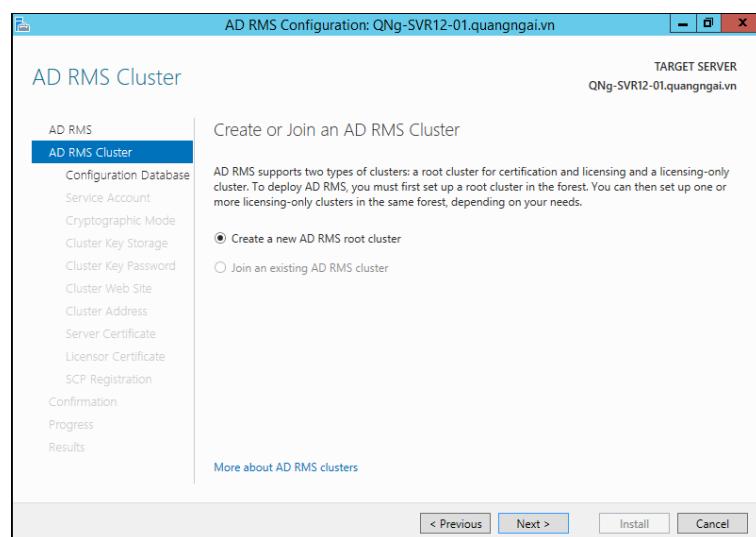
Bước 2. Tại công cụ "Server Manager", nhấn chọn "Add roles and features".

Bước 3. Tại màn hình "Select server roles", nhấn chọn "Active Directory Rights Management

- Bước 4.* Services". Hộp thoại yêu cầu cài đặt các tính năng bổ sung xuất hiện, nhấn "Add Features". Sau đó nhấn Next.
- Bước 5.* Tại màn hình "Select features", nhấn Next.
- Bước 6.* Tại màn hình "Active Directory Rights Management Services", xem qua các thông tin mô tả về dịch vụ. Sau đó nhấn Next.
- Bước 7.* Tại màn hình "Select role services", chọn "Active Directory Rights Management Server" → Nhấn Next.
- Bước 8.* Tại màn hình "Web Server Role (IIS)", nhấn Next.
- Bước 9.* Tại màn hình "Select role services", nhấn Next.
- Bước 10.* Tại màn hình "Confirm installation selections", nhấn Install.
- Bước 11.* Tại màn hình "AD RMS", nhấn Next.

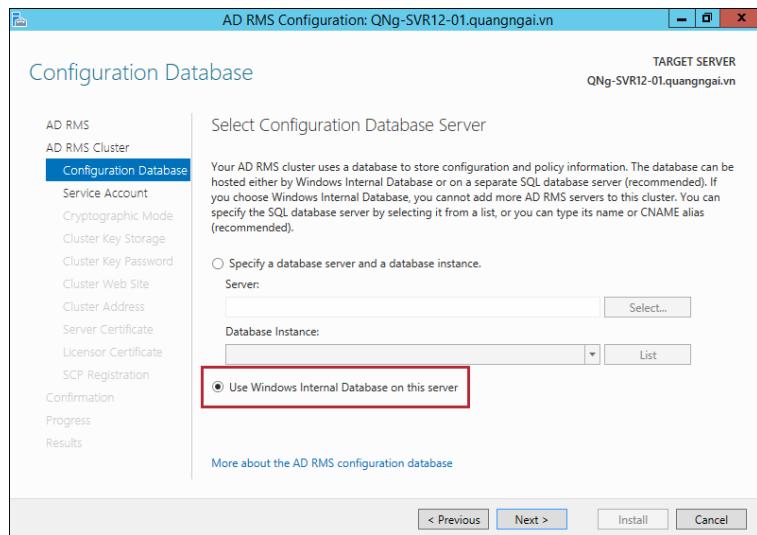


- Bước 12.* Tại màn hình "AD RMS Cluster", chọn "Create a new AD RMS root cluster". Sau đó nhấn Next.



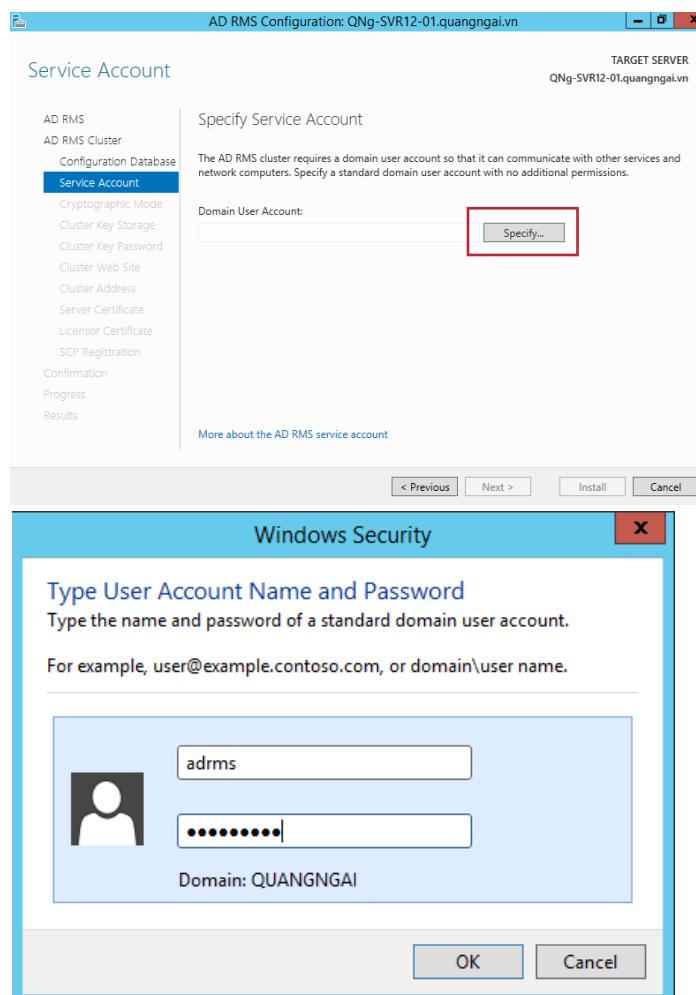
Hình 9.1. Tạo mới một Cluster.

- Bước 13.* Tại màn hình "Configure Database", chọn "Use Windows Internal Database on this server". Sau đó nhấn Next.



Hình 9.2. Cấu hình cơ sở dữ liệu cho AD RMS.

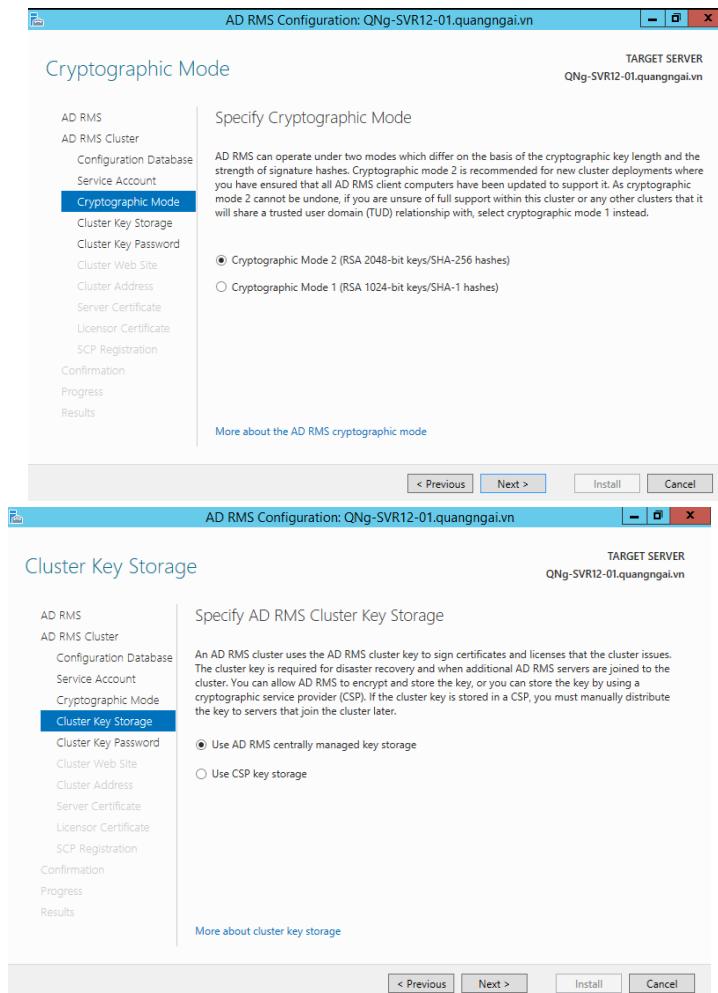
Bước 14. Tại màn hình "Service Account", nhấn vào nút "Specify" và nhập thông tin của tài khoản "adrms". Sau đó nhấn Next.



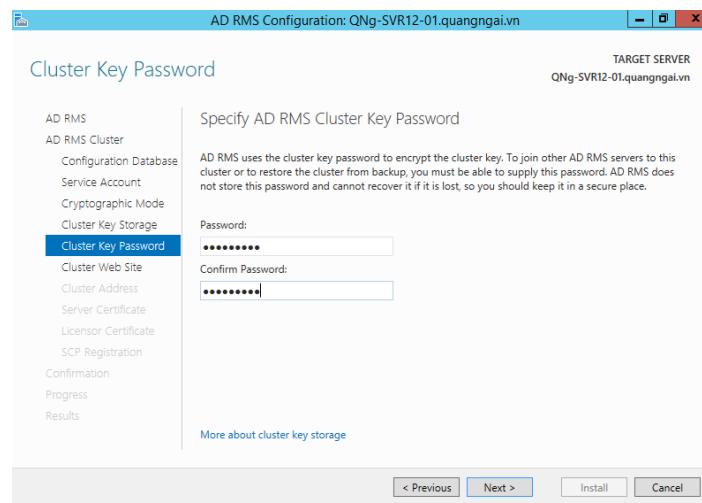
Hình 9.3. Xác nhận tài khoản dịch vụ AD RMS.

Bước 15. Tại màn hình "Cryptographic Mode", chọn "cryptographic Mode 2 (RSA 2048-bit keys/SHA-256 hashes)". Sau đó nhấn Next.

Bước 16. Tại màn hình "Cluster Key Storage", chọn "Use AD RMS centrally managed key storage". Sau đó nhấn Next.



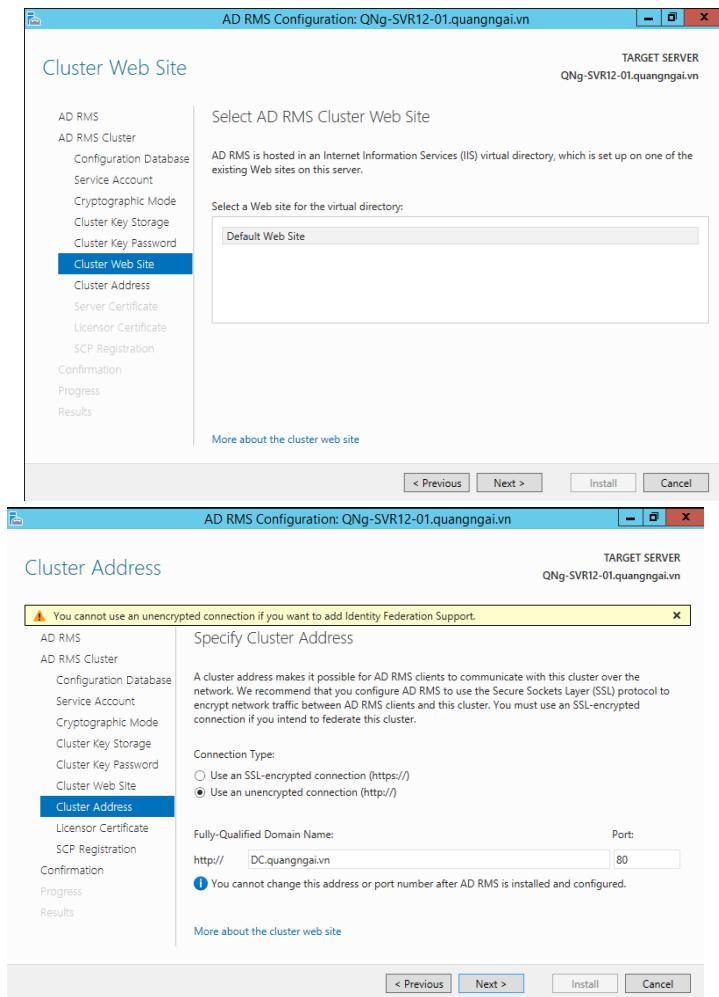
Bước 17. Tại màn hình "Cluster Key Password", nhập mật khẩu vào hai ô "Password" và "Confirm Password". Sau đó nhấn Next.



Hình 9.4. Thiết lập mật khẩu.

Bước 18. Tại màn hình "Cluster Web Site", chấp nhận các thiết lập mặc định và sau đó nhấn Next.

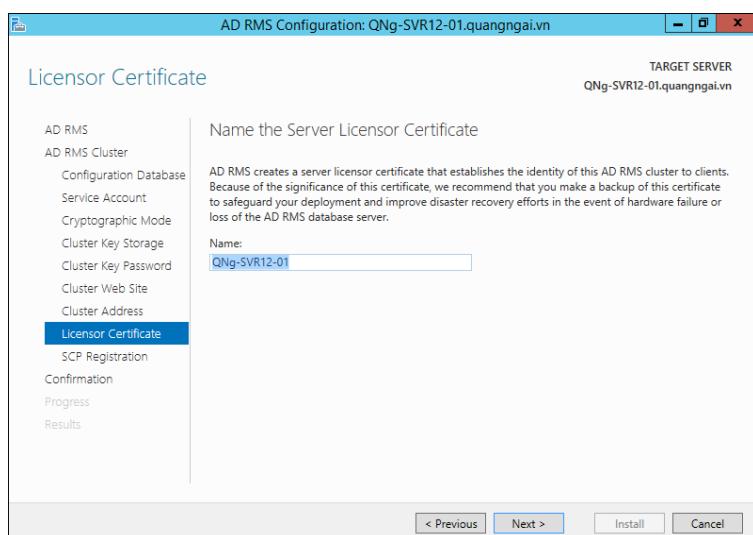
Bước 19. Tại màn hình "Cluster Address", chọn "Use an unencrypted connection (http://)". Tại ô nhập liệu "Fully-Qualified Domain Name" nhập theo cú pháp sau: ***ten\_may\_DC.ten\_mien***. Sau đó nhấn Next.

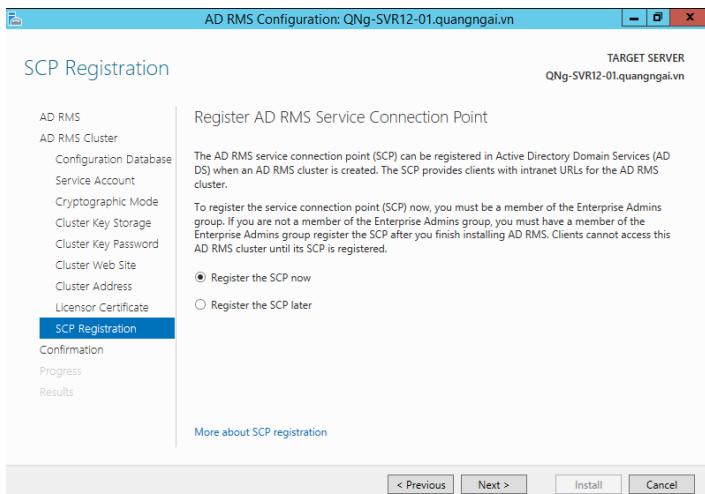


Hình 9.5. Thiết lập địa chỉ Cluster.

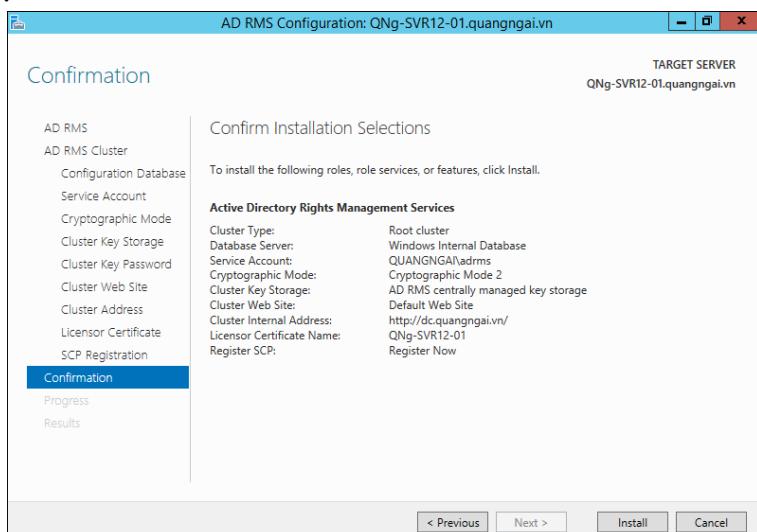
Bước 20. Tại màn hình "**Licensor Certificate**", chấp nhận các thiết lập mặc định và sau đó nhấn **Next**.

Bước 21. Tại màn hình "**SCP Registration**", chọn "**Register the SCP now**" và sau đó nhấn **Next**.





*Bước 22.* Tại màn hình "Confirmation", xem lại thông tin về các thiết lập. Nếu có sai sót nhấn vào nút **Previous** để thực hiện việc thay đổi. Ngược lại nhấn **Install** để hoàn thành quá trình cài đặt.



*Hình 9.6. Xác nhận các thiết lập.*

#### **Bảo vệ tài liệu :**

Hiện nay ở tổ chức của bạn có một số tài liệu cần được bảo vệ. Thông tin về các tài nguyên đó như sau :

Thư mục	Đọc	Sao chép	In
Bao_Cao_Tai_Chinh	Ban giám đốc, kế toán.	Ban giám đốc.	Ban giám đốc, kế toán.
Chi_Tiet_Ky_Thuat	Ban giám đốc, trưởng các nhóm phần mềm	Trưởng các nhóm phần mềm	Trưởng các nhóm phần mềm

*Bước 1.* Mở tập tin cần bảo vệ (Word, Excel, PowerPoint).

*Bước 2.* Nhấn vào menu "**File**".

*Bước 3.* Tại mục Info, nhấp vào biểu tượng "Protect Document" → Chọn "Restricted Access".

*Bước 4.* Nhấp chọn Restrict permission to this document trong hộp thoại Permission. Và thực hiện việc thiết lập quyền cho các tài khoản cần thiết.

## Bài 10 ĐỊNH TUYẾN IPv6 TRÊN WINDOWS SERVER 2012

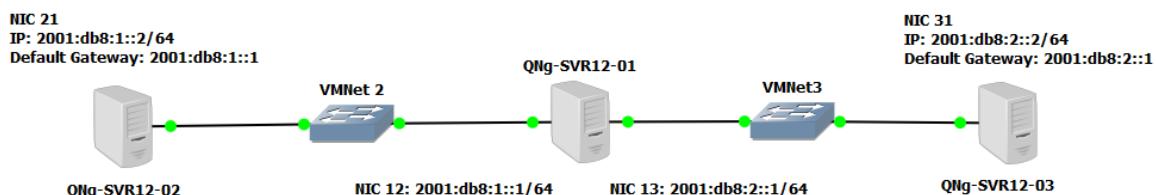
Sự khác biệt chính giữa IPv4 và IPv6 là giao thức IPv6 được thiết kế để tự động cấu hình. Điều này có nghĩa là, trong hầu hết các trường hợp, bạn sẽ không cần gán địa chỉ một cách thủ công, hay triển khai máy chủ DHCPv6, thay vào đó ta sẽ sử dụng tính năng tự động cấu hình địa chỉ phi trạng thái cho hầu hết các máy chủ của mình. NIC trên máy chủ thường được gán 1 địa chỉ IPv4 tĩnh, nhưng với IPv6 thì 1 NIC được gán nhiều địa chỉ. Cụ thể, IPv6 sử dụng ít nhất hai địa chỉ trên 1 NIC:

- Link-local được tạo ra một cách tự động, sử dụng cho traffic trên liên kết nội bộ.
- Địa chỉ Unicast bổ sung, được sử dụng cho traffic cần được định tuyến ngoài liên kết nội bộ.

IPv6 có thể được gán cho 1 NIC theo những cách sau:

- Cấu hình thủ công một hoặc nhiều địa chỉ IPv6
- Cấu hình địa chỉ có trạng thái sử dụng máy chủ DHCPv6
- Cấu hình địa chỉ phi trạng thái - stateless, dựa trên tin nhắn nhận được từ Quảng bá của bộ định tuyến (Router Advertisement)
- Tự động cấu hình cả địa chỉ có trạng thái và phi trạng thái

Ngoài ra, địa chỉ link-local luôn được tự động cấu hình dù địa chỉ có trạng thái hay phi trạng thái (đã cấu hình tự động) đang được sử dụng.



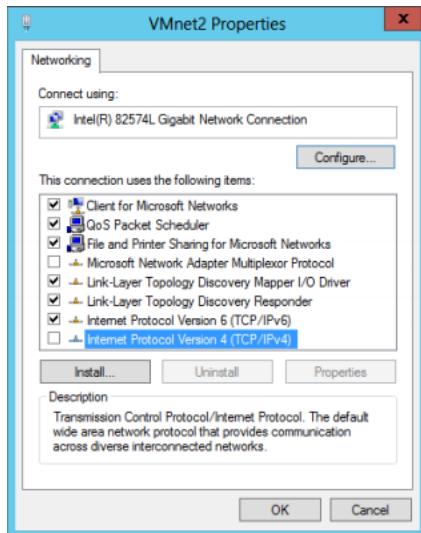
Để hạn chế việc cạn kiệt địa chỉ IPv4, công ty triển khai hệ thống IPv6 như sơ đồ trên, trong đó máy chủ QNG-SVR12-01 thực hiện công việc của 1 bộ định tuyến cho 2 mạng con VMNet2 và VMNet3. Với vai trò là quản trị viên bạn hãy thực hiện yêu cầu trên bằng cách triển khai dịch vụ Định tuyến và Truy cập từ xa (**Routing and Remote Access**).

### 10.1 Cài đặt IPv6 trên máy chủ

*Bước 1.* Có thể dùng chức năng Clone (nhân bản) của VMWare để tạo thêm 2 máy chủ hoặc kết nối 3 máy chủ ảo với nhau thông qua mạng vật lý (Bridged). Thêm 1 card mạng VMNet tương ứng cho máy chủ QNG-SVR12-01.

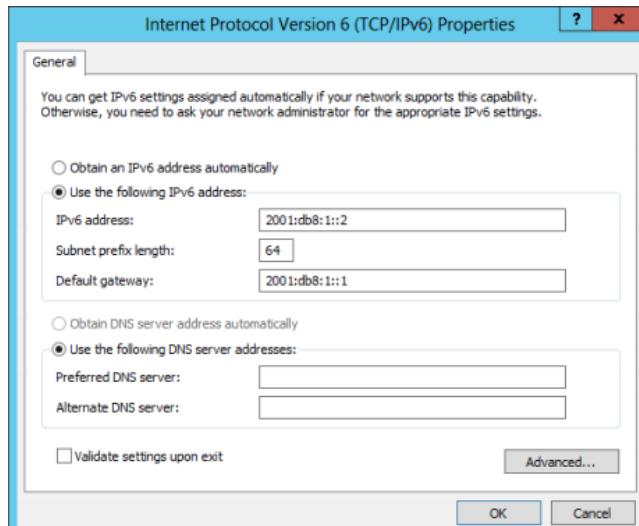
*Bước 2.* Trên mỗi máy chủ :

- Kích chuột phải để đặt lại tên card mạng (**Rename**) theo sơ đồ đã cho
- Tiếp tục kích chuột phải chọn **Properties** và bỏ dịch vụ IPv4



Hình 10.1 – Bỏ dịch vụ IPv4

- Chọn dịch vụ IPv6 và gán IP như sơ đồ đã cho, ví dụ đối với NIC 21 như hình 2.2. **Chú ý** trên máy chủ **QNG-SVR12-01** không gán Default Gateway



Hình 10.2 – NIC 21 gán IPv6

Bước 3. Trên máy chủ QNG-SVR01-12, kiểm tra kết nối đến 2 máy chủ còn lại bằng lệnh ping

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 2001:db8:1::2

Pinging 2001:db8:1::2 with 32 bytes of data:
Reply from 2001:db8:1::2: time<1ms
Reply from 2001:db8:1::2: time<1ms

Ping statistics for 2001:db8:1::2:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
C:\Users\Administrator>ping 2001:db8:2::2

Pinging 2001:db8:2::2 with 32 bytes of data:
Reply from 2001:db8:2::2: time<1ms
Reply from 2001:db8:2::2: time<1ms
Reply from 2001:db8:2::2: time<1ms
Reply from 2001:db8:2::2: time<1ms

Ping statistics for 2001:db8:2::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

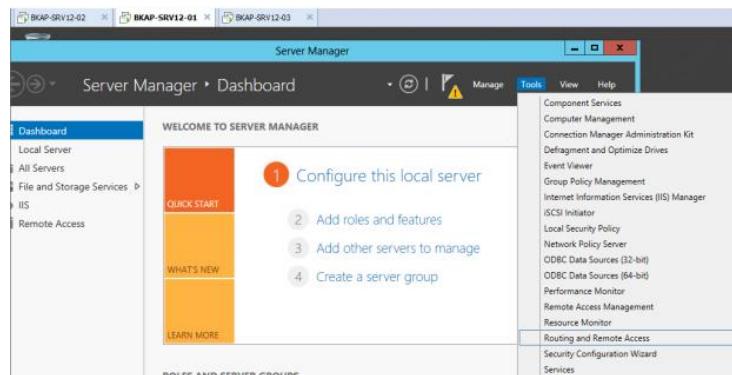
C:\Users\Administrator>
```

Hình 10.3 – Ping IPv6 từ QNG-SVR12-01

Bước 4. Thực hiện cài đặt và cấu hình **Routing and Remote Access (RRAS)** trên máy chủ QNG-SVR12-01

- Vào Server Manager → Add roles and features. Tại cửa sổ Select server roles, chọn Remote Access.
- Tại cửa sổ Select role services, click chọn vào Routing.
- Click Install / Finish tại các cửa sổ tiếp theo để Server bắt đầu cài đặt và kết thúc tiến trình cài đặt dịch vụ.

Bước 5. Cấu hình dịch vụ **RRAS**: Server Manager → Tools → Routing and Remote Access.



Hình 10.4 – Lựa chọn Routing and Remote Access

- Tại cửa sổ Routing and Remote Access, chuột phải lên QNg-SRV12-01 (local), chọn Configure and Enable Routing and Remote Access.
- Tại cửa sổ Configuration, chọn Custom configuration.
- Tại cửa sổ Custom Configuration, chọn Lan routing.
- Nhấn Finish / Start Services tại các cửa sổ tiếp theo để kết thúc cấu hình.

Bước 6. Trên máy chủ QNG-SVR12-02, ping đến máy chủ QNG-SVR12-03 và ngược lại

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 2001:db8:1::2

Pinging 2001:db8:1::2 with 32 bytes of data:
Reply from 2001:db8:1::2: time=1ms
Reply from 2001:db8:1::2: time<1ms
Reply from 2001:db8:1::2: time<1ms
Reply from 2001:db8:1::2: time<1ms

Ping statistics for 2001:db8:1::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Administrator>

```

Hình 10.5 – Ping thành công giữa QNG-SVR12-02 và 03

## 10.2 Gán địa chỉ IPv6 thủ công

Việc gán địa chỉ IPv6 thủ công nói chung thường được thực hiện trong 2 trường hợp:

- Cho các máy chủ hiện tại trên mạng
- Trên hầu hết các cổng của bộ định tuyến (router)

Trên máy chạy Windows Server 2012 ta có thể gán địa chỉ IPv6 bằng cách sử dụng một trong những phương án sau:

- Sử dụng Internet Protocol Version 6 (TCP/IPv6) Properties
- Sử dụng các cmdlet New-NetIPAdress và Set-DnsClientServerAddress của Windows PowerShell
- Sử dụng các lệnh netsh từ menu ngữ cảnh của tiện ích dòng lệnh Netsh.exe

### Cách 1: Sử dụng Internet Protocol Version 6 (TCP/IPv6) Properties

Chuột phải vào biểu tượng mạng trên thanh taskbar → Open network and sharing center → nhấp sang bên trái chọn Change adapter settings → chuột phải lên biểu tượng mạng chọn Properties → Chọn Internet Protocol Version 6 (TCP/IPv6) → Properties để mở hộp thoại Internet Protocol Version 6 (TCP/IPv6) Properties. Tại đây bạn cấu hình địa chỉ IPv6, độ dài tiền tố mạng con, gateway mặc định và địa chỉ máy chủ DNS.

### Cách 2: Sử dụng Windows PowerShell

Ví dụ dưới đây sẽ sử dụng Windows PowerShell để cấu hình thủ công 1 địa chỉ IPv6 trên NIC của máy chủ chạy Windows Server 2012/2012 R2. Đầu tiên, chạy lệnh Ipconfig trên máy chủ, đây là kết quả:

```
PS C:\> ipconfig  
NIC có tên Ethernet được gán 2 địa chỉ:  
IPv4: 172.16.11.75  
Link-local IPv6: fe80::2025:61fb:b68:c266%12
```

%12 ở cuối địa chỉ link-local được gọi là Zone identifier, sử dụng để xác định các liên kết trên địa chỉ được đặt. Trên Windows, Zone identifier tương đương với chỉ mục của NIC, bạn có thể sử dụng cmdlet Get-NetAdapter để hiển thị danh sách tên và chỉ mục của các NIC trên máy chủ chạy Windows Server 2012 hoặc 2012 R2 như bên dưới:

```
PS C:\> Get-NetAdapter | fl Name,ifIndex
```

Thay vì sử dụng lệnh Ipconfig, ta cũng có thể sử dụng cmdlet Get-NetIPAdress như dưới đây để hiển thị thông tin địa chỉ cho Interface có tên là Ethernet:

```
PS C:\> Get-NetIPAddress | where {$_.InterfaceAlias -eq "Ethernet"}  
Lệnh này trả về nhiều thông tin hơn so với Ipconfig.
```

Sử dụng cmdlet NewNetIPAdress để gán địa chỉ Unicast IPv6 global mới với độ dài tiền tố là 64 và địa chỉ gateway mặc định cho Interface Ethernet như sau:

```
PS C:\> New-NetIPAddress -InterfaceAlias "Ethernet" -IPAddress 2001:DB8:3FA9::D3:9C5A `
```

Để xác nhận kết quả, ta cần sử dụng Get-NetIPAddress với tham số AddressFamily để chỉ hiển thị thông tin IPv6 như dưới đây:

```
PS C:\> Get-NetIPAddress -AddressFamily IPv6 | where {$_.InterfaceAlias -eq "Ethernet"}  
NIC bây giờ đã được multihomed (kết nối nhiều mạng) vì nó có địa chỉ IPv6 link-local và IPv6 global. Mở hộp thoại Internet Protocol Version 6 (TCP/IPv6) Properties ta sẽ thấy những thông tin địa chỉ được cấu hình thủ công như mong muốn.
```