iLAB TECHNOLOGY & TRAINING CENTER
0909 455 982
info@ilab.vn
www.ilab.vn
ilab.vn
+ilabvncenter
ilabvncenter

UPGRADING TECHNOLOGY EVERYDAY

MCSE SERVER INFRASTRUCTURE

70-413

MỤC LỤC

Bài 1: Lập kế hoạch nâng cấp máy chủ và chuyển đổi hệ thống. 4

Bài 2: Lập kế hoạch và triển khai cơ sở hạ tầng máy chủ. 19

Bài 3: Thiết kế hệ thống DHCP và giải pháp quản lý địa chỉ IP. 48

Bài 4: Thiết kế và triển khai hệ thống DNS. 81

Bài 5: Thiết kế và triển khai mô hình Active Directory Forest. 105

Bài 6: Thiết kế và triển khai mô hình Active Directory Domain. 127

Bài 7: Thiết kế cấu trúc OU và triển khai mô hình ủy quyền quản lý Active Directory. 141

Bài 8: Thiết kế và triển khai Group Policy Object (GPO). 166

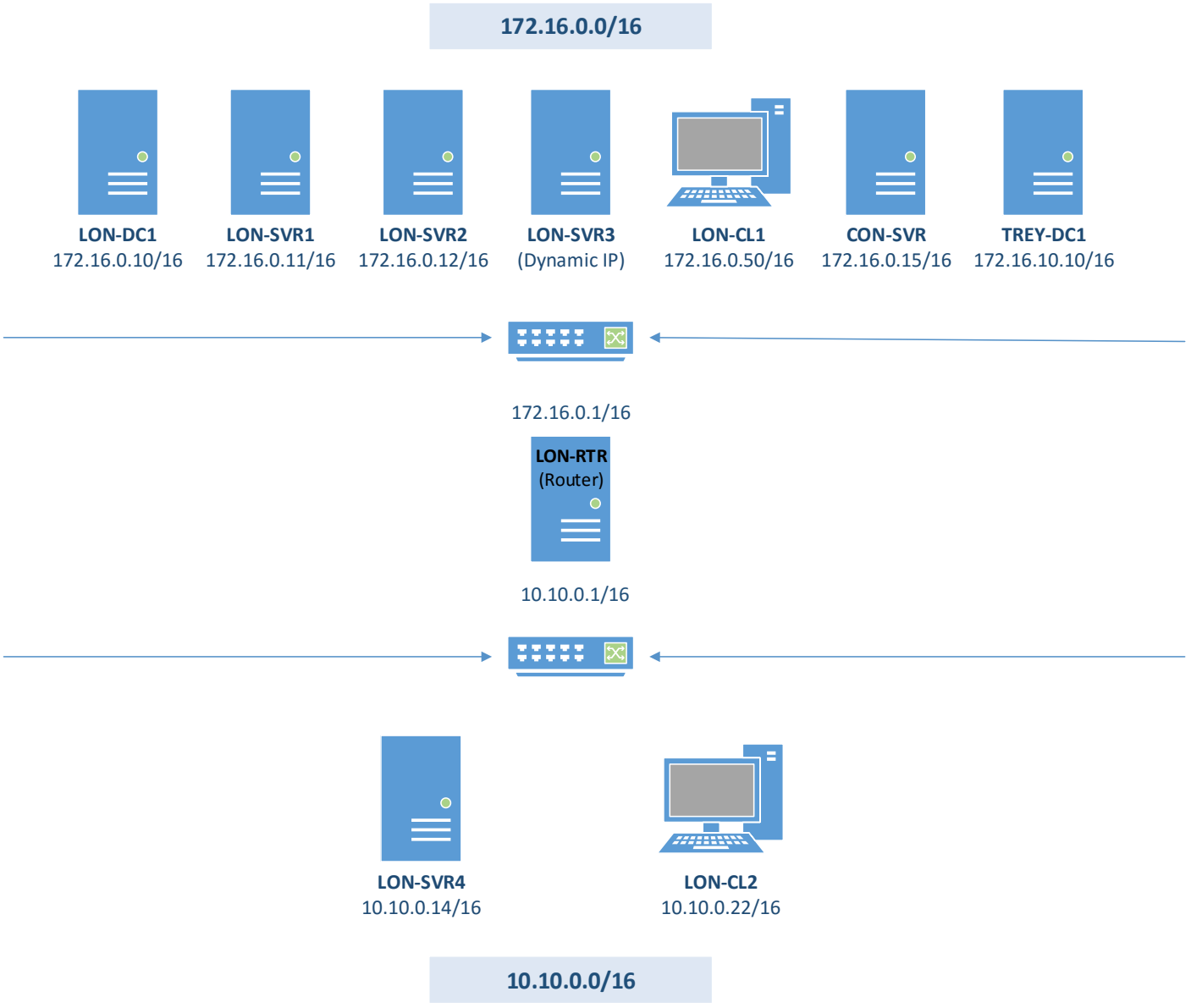
Bài 9: Thiết kế và triển khai mô hình Active Directory Sites. 203

Bài 10: Lập kế hoạch và triển khai giải pháp lưu trữ dữ liệu. 229

Bài 11: Thiết kế và triển khai giải pháp bảo vệ hệ thống mạng. 267

Bài 12: Thiết kế và triển khai giải pháp truy cập từ xa (Direct Access & VPN). 330

Mô hình LAB:


172.16.0.0/16
LON-DC1
172.16.0.10/16
LON-SVR1
172.16.0.11/16
LON-SVR2
172.16.0.12/16
LON-SVR3
(Dynamic IP)
LON-CL1
172.16.0.50/16
CON-SVR
172.16.0.15/16
TREY-DC1
172.16.10.10/16
172.16.0.1/16
LON-RTR
(Router)
10.10.0.1/16
LON-SVR4
10.10.0.14/16
LON-CL2
10.10.0.22/16
10.10.0.0/16

Chức năng của các máy ảo trong mô hình LAB

Máy ảo (VM)	Chức năng
20413C-LON-DC	Domain Controller chạy Windows Server 2012 R2 của domain Adatum.com
20413C-LON-SVR1	Member Server chạy Windows Server 2012 R2 của domain Adatum.com
20413C-LON-SVR2	Member Server chạy Windows Server 2012 R2 của domain Adatum.com
20413C-LON-SVR3	Máy ảo chưa cài đặt hệ điều hành (trong bài Lab sẽ cài Windows Server 2012)
20413C-LON-SVR4	Member Server chạy Windows Server 2012 R2 của domain Adatum.com. Server này đặt ở subnet thứ 2 (10.10.0.0/16)
20413C-LON-RTR	Router có chức năng kết nối & định tuyến cho 2 net
20413C-TREY-DC1	Domain Controller chạy Windows Server 2012 R2 của domain Treyresearch.net. Sẽ được sử dụng trong các bài tập có nhiều domain.
20413C-CON-SVR	Stand-Alone server chạy Windows Server 2012 R2
20413C-LON-CL1 **20413C-LON-CL2**	2 máy Client chạy Windows 8.1 có cài sẵn Microsoft Office 2013 của domain Adatum.com

Bài 1: Lập kế hoạch nâng cấp máy chủ và chuyển đổi hệ thống

I. Mục tiêu của bài học:

- Lập kế hoạch nâng cấp máy chủ và chiến lược chuyển đổi.
- Sử dụng công cụ MAP để đánh giá Server nào phù hợp cho giải pháp ảo hóa.

II. Kịch bản:

Công ty A. Datum có trụ sở chính tại London. Hệ thống Active Directory của A.Datum sử dụng Windows Server 2008 và Windows Server 2008 R2. Domain Controller chạy trên nền Windows Server 2008 R2.

Các chi nhánh ở Toronto and Sydney đều là hệ thống nhỏ và chủ yếu sử dụng Windows Server 2008. Trung tâm phân phối có sử dụng ứng dụng hỗ trợ ngành nghề kinh doanh (LOB)

Đội ngũ quản lý của A. Datum yêu cầu cơ sở hạ tầng CNTT mới phải giải quyết hiệu quả hơn đối với việc sử dụng phần cứng và điện năng tiêu thụ. Điều này cho thấy giải pháp hợp nhất và ảo hóa máy chủ là một phần quan trọng của việc nâng cấp hệ thống.

Bạn đã tham gia các cuộc thảo luận xung quanh khả năng A. Datum mua lại hai công ty. Thông tin này chưa được công bố chính thức, nhưng có thể xảy ra trong những tháng tới. Bạn biết rằng một trong hai công ty này không có cơ sở hạ tầng Windows Server, và bạn có thể được yêu cầu phát triển một chiến lược tốt nhất để triển khai Windows Server 2012 cho công ty đó. Công ty còn lại thì có một Forest chạy trên nền Windows Server 2008.

Tuy nhiên, trước khi bắt đầu triển khai máy chủ, bạn phải lập kế hoạch nâng cấp máy chủ và chiến lược chuyển đổi hệ thống. Kế hoạch này sẽ liên quan đến việc xác định vai trò máy chủ sẽ di chuyển, bạn có thể hợp nhất vào một máy chủ duy nhất, và liệu khối lượng công việc có phù hợp cho ảo hóa. Ban đầu, bạn sẽ thực hiện phân tích này trên các máy chủ ở London, và sau đó là các máy chủ ở Toronto và Sydney.

Trong quá trình này, bạn phải tiếp tục tập trung vào việc tối ưu hóa tài nguyên và năng lực của máy chủ. Ngoài những nhận xét chủ yếu là kỹ thuật, bạn phải xem xét vấn đề bản quyền của máy chủ.

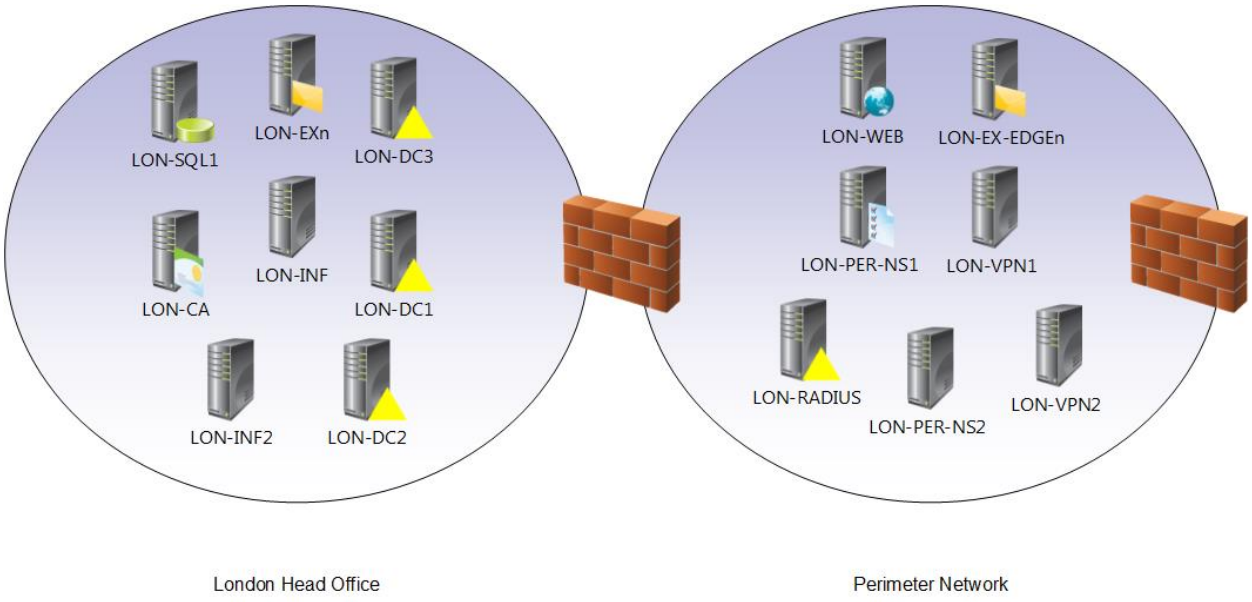
Tất cả các máy chủ hiện tại được cài đặt với bộ vi xử lý đơn hoặc kép. Bảng dưới đây liệt kê cấu hình hiện tại của các máy chủ.

Tên Server	**HĐH**	**Chức năng**	**CPU / sử dụng trung bình**	**RAM/sử dụng trung bình**
Trụ sở chính				
LON-EX1	Windows Server 2008 R2	Exchange Server 2010: Client Access and Hub Transport	Dual processor/75%	32 GB/16 GB
LON-EX2	Windows Server 2008 R2	Exchange Server 2010: Mailbox	Dual processor/75%	32 GB/24 GB
LON-EX3	Windows Server 2008 R2	Exchange Server 2010: Mailbox	Dual processor/75%	24 GB/18 GB
LON-SQL1	Windows Server 2008	SQL Server (clustered)	Dual processor/80%	32 GB/28 GB
LON-CA	Windows Server 2008 R2	Active Directory Certificate Services (AD CS): Enterprise Root CA	Single processor/25%	16 GB/4 GB
LON-DC1	Windows Server 2008 R2	AD DS	Single processor/60%	8 GB/3 GB
LON-DC2	Windows Server 2008 R2	AD DS	Single processor/60%	8 GB/3 GB
LON-DC3	Windows Server 2008 R2	AD DS	Single processor/60%	8 GB/3 GB

LON-INF1	Windows Server 2008	DHCP, DNS	Single processor/50%	8 GB/4 GB
LON-INF2	Windows Server 2008	DHCP, DNS	Single processor/50%	8 GB/4 GB

Perimeter network				
LON-PER-NS1	Windows Server 2008	DNS	Single processor/25%	8 GB/2 GB
LON-PER-NS2	Windows Server 2008	DNS	Single processor/25%	8 GB/2 GB
LON-RADIUS	Windows Server 2008 R2	Network Policy Server	Single processor/35%	8 GB/4 GB
LON-WEB	Windows Server 2008	Multiple websites hosted with Internet Information Services (IIS)	Dual processor/75%	16 GB/10 GB
LON-VPN1 LON-VPN2	Windows Server 2008 R2	Routing and Remote Access Service (RRAS)	Single processor/25%	6 GB/3 GB
LON-EX-EDGE1	Windows Server 2008 R2	Exchange Server 2010 Edge Transport server	Dual processor/40%	16 GB/8 GB

III. Mô hình:



IV. Yêu cầu tổng quan:

Thiết kế nâng cấp máy chủ và chiến lược chuyển đổi để hỗ trợ các mục tiêu sau đây:

- Đảm bảo rằng cơ sở hạ tầng mới phải hiệu quả hơn trong việc sử dụng phần cứng và điện năng tiêu thụ.
- Hợp nhất máy chủ và ảo hóa là một phần quan trọng của việc nâng cấp.
- Phát triển một chiến lược triển khai Windows Server 2012 trong một kịch bản mà chúng ta có thêm một forest sử dụng Windows Server 2008.
- Xác định vai trò máy chủ sẽ di chuyển.
- Xác định vai trò của các máy chủ để hợp nhất vào một máy chủ duy nhất và phù hợp cho ảo hóa.
- Xác định hệ điều hành máy chủ lưu trữ mà bạn sẽ sử dụng để hỗ trợ ảo hóa.
- Xem xét các tác động liên quan đến bản quyền.

V. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-CL1**
User name	Adatum\Administrator
Password	Pa$$w0rd

VI. Chuẩn bị:

1. Trên máy thật, bung Start menu, mở **Hyper-V Manager**.
2. Trong cửa sổ Hyper-V Manager, nhấn phải chuột lên máy ảo **20413C-LON-DC1** chọn **Start.**
3. Nhấn phải chuột lên lại máy ảo **20413C-LON-DC1** chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiện từ bước 2 đến bước 4 cho máy ảo **20413C-LON-CL1.**

VII. Thực hành:

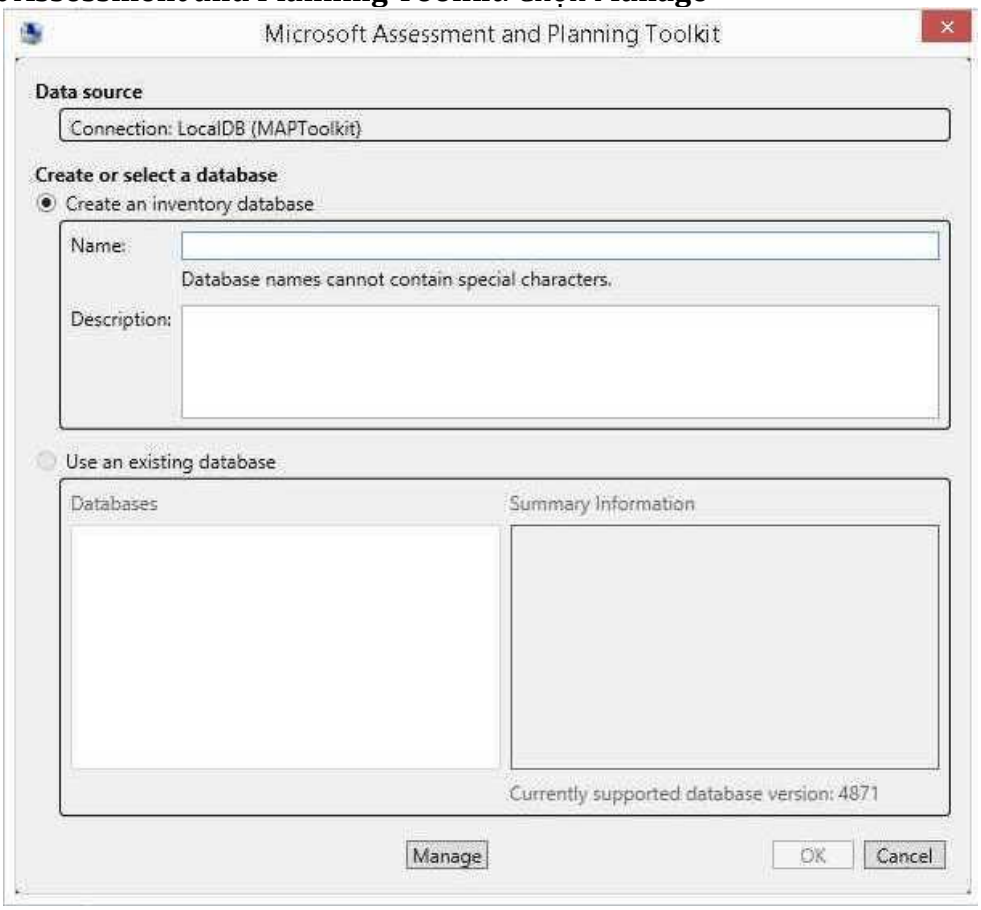
Thời gian thực hành: 40 phút

Bài thực hành sau đây sẽ hướng dẫn chúng ta sử dụng công cụ MAP để đánh giá các Server nào phù hợp cho giải pháp ảo hóa.

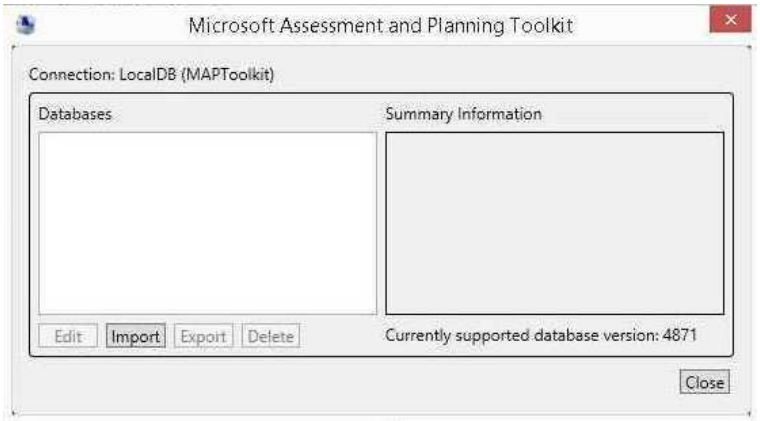
1. Trên máy **LON-CL1**, bung **Start** menu, chọn **Microsoft Assessment and Planning Toolkit.**



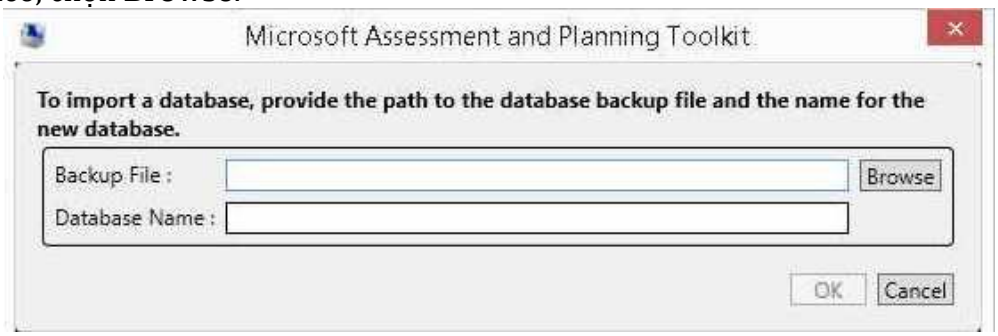
2. Trong cửa sổ **Microsoft Assessment and Planning Toolkit** xuất hiện hộp thoại **Microsoft Assessment and Planning Toolkit**. Chọn **Manage**



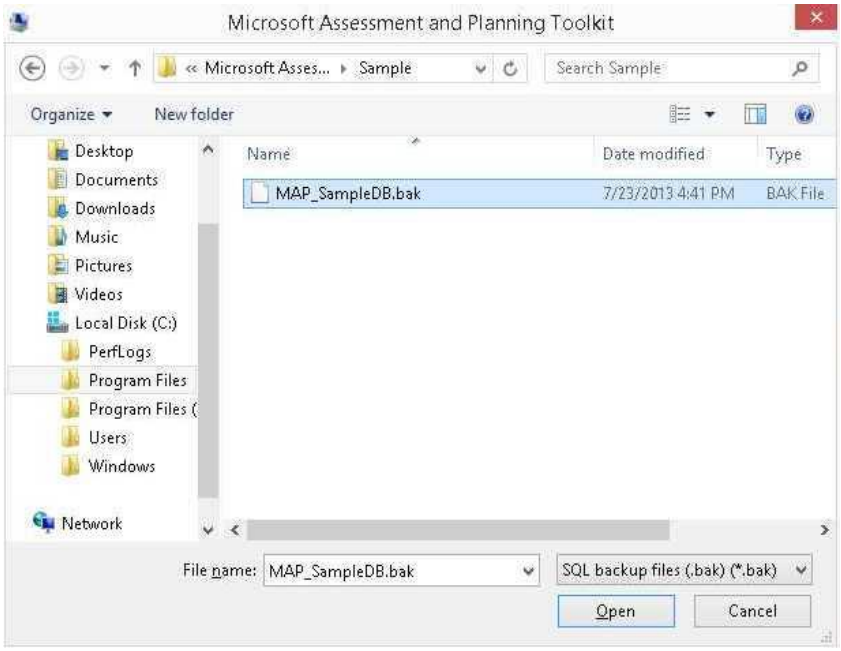
3. Trong hộp thoại **Microsoft Assessment and Planning Toolkit,** chọn **Import**



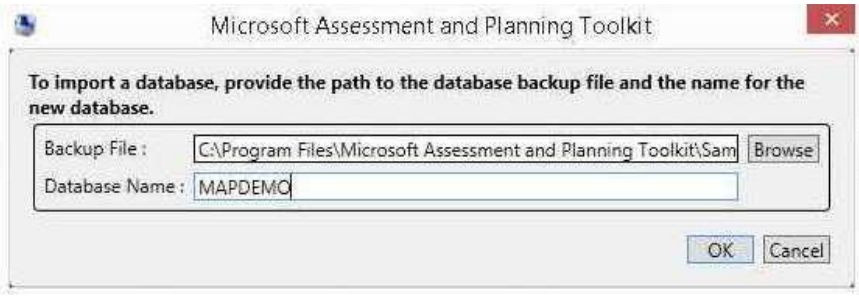
4. Tiếp theo, chọn **Browse**.



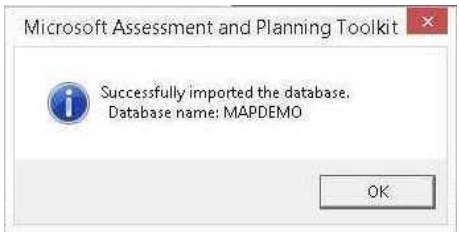
5. Chỉ tới đường dẫn **C:\Program Files\ Microsoft Assessment and Planning Toolkit\Sample**, chọn file **MAP_SampleDB.bak** và chọn **Open**.



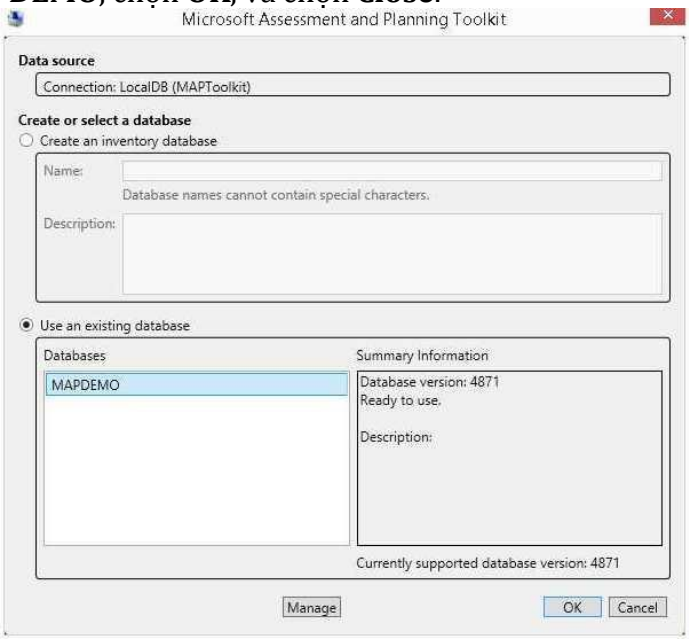
6. Trong hộp thoại **Microsoft Assessment and Planning Toolkit**, nhập tên **MAPDEMO** vào ô **Database Name**, chọn **OK**.



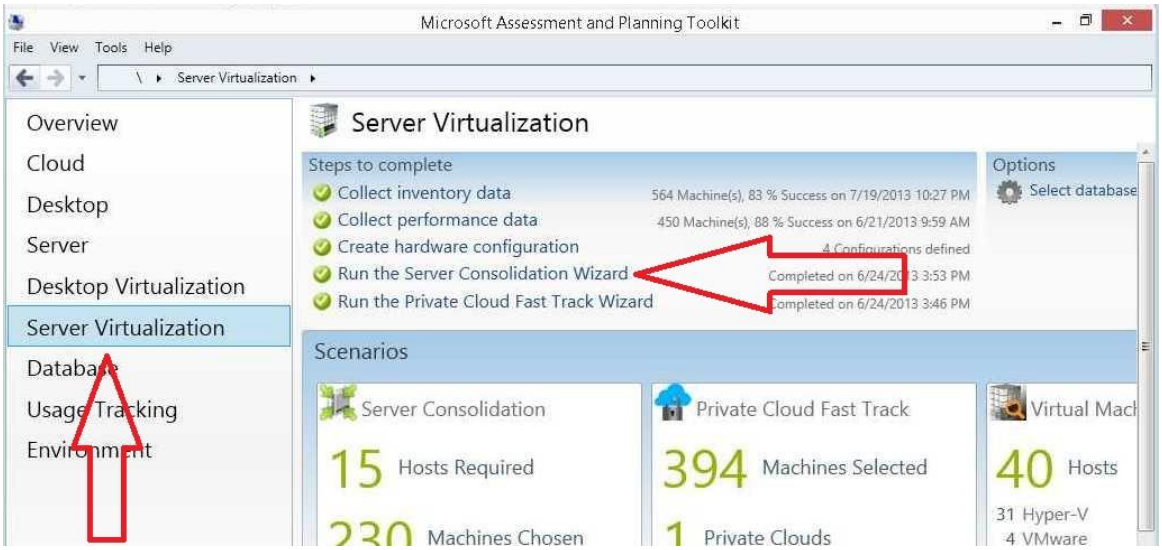
7. Khi nhận được thông báo Successfully imported, chọn **OK**, và chọn **Close**.



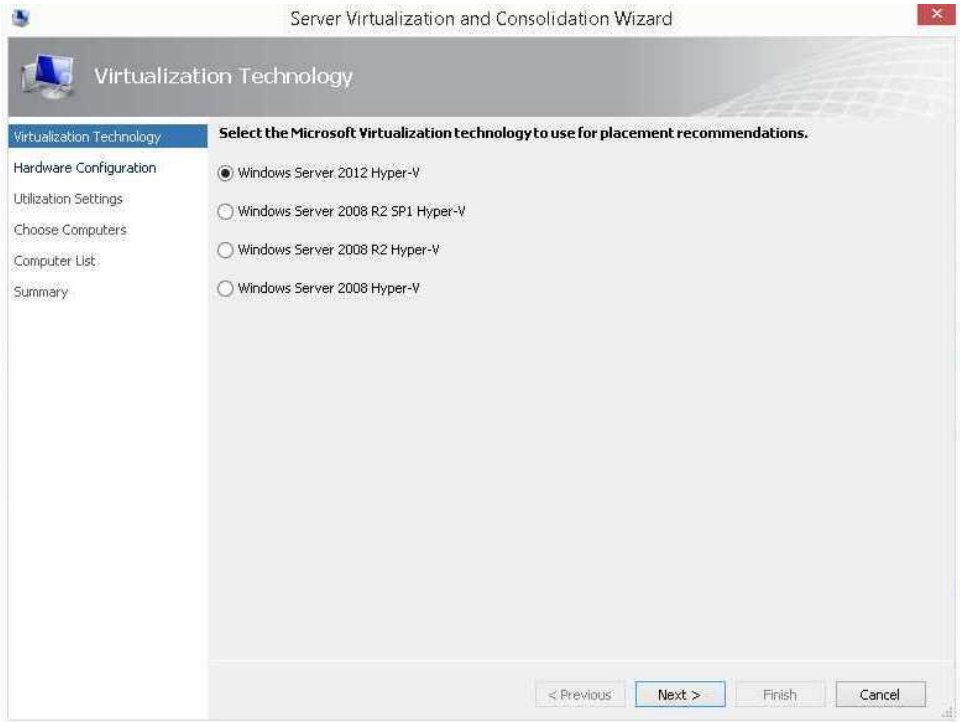
8. Trong hộp thoại **Microsoft Assessment and Planning Toolkit**, chọn **Use an existing database**, chọn **MAPDEMO**, chọn **OK**, và chọn **Close**.



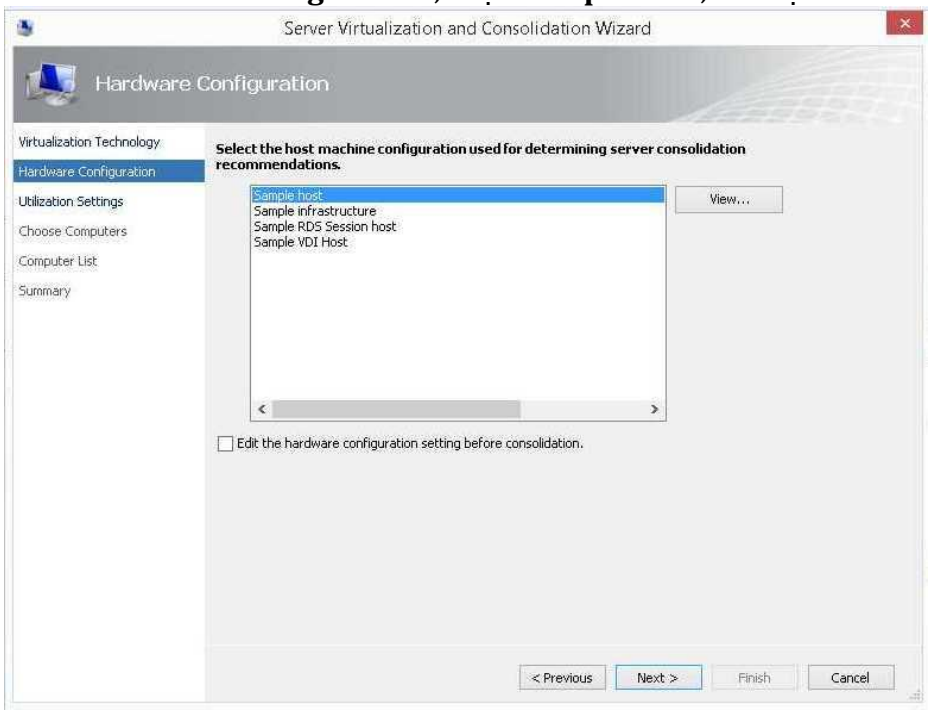
9. Trong cửa sổ **Microsoft Assessment and Planning Toolkit**, chọn vào mục **Server Virtualization** bên trái. Trong phần **Steps to complete**, chọn **Run the Server Consolidation Wizard**.



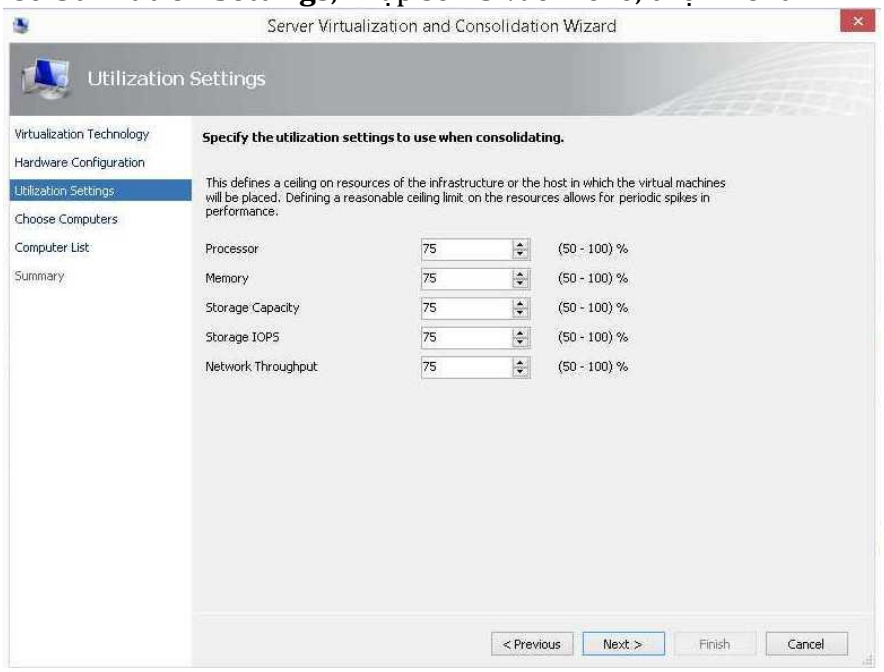
10. Trong cửa sổ **Virtualization Technology**, chọn **Windows Server 2012 Hyper-V**, và chọn **Next**.



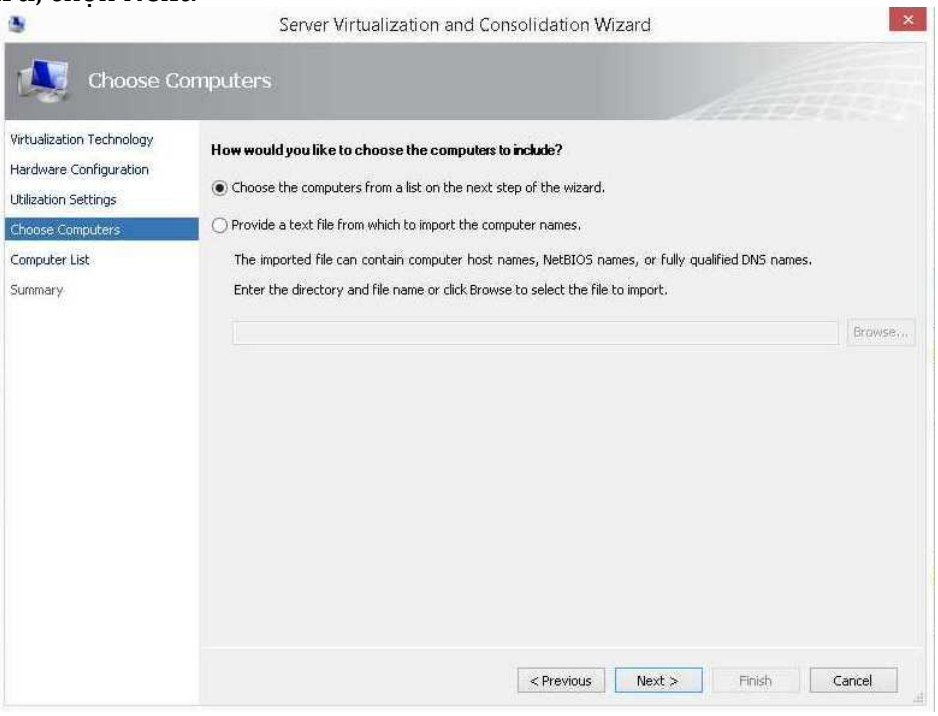
11. Trong cửa sổ **Hardware Configuration**, chọn **Sample host**, và chọn **Next**.



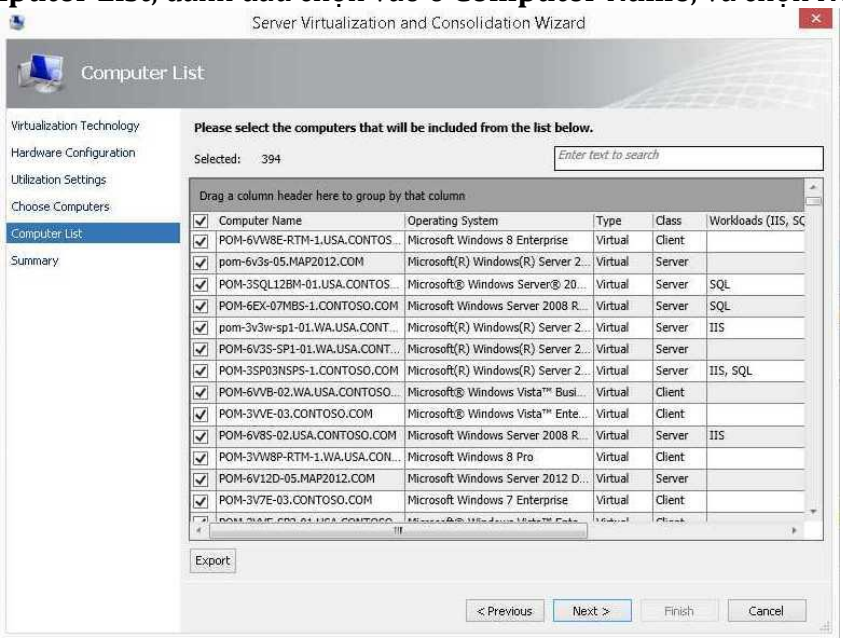
12. Trong cửa sổ **Utilization Settings**, nhập số **75** vào mỗi ô, chọn **Next**.



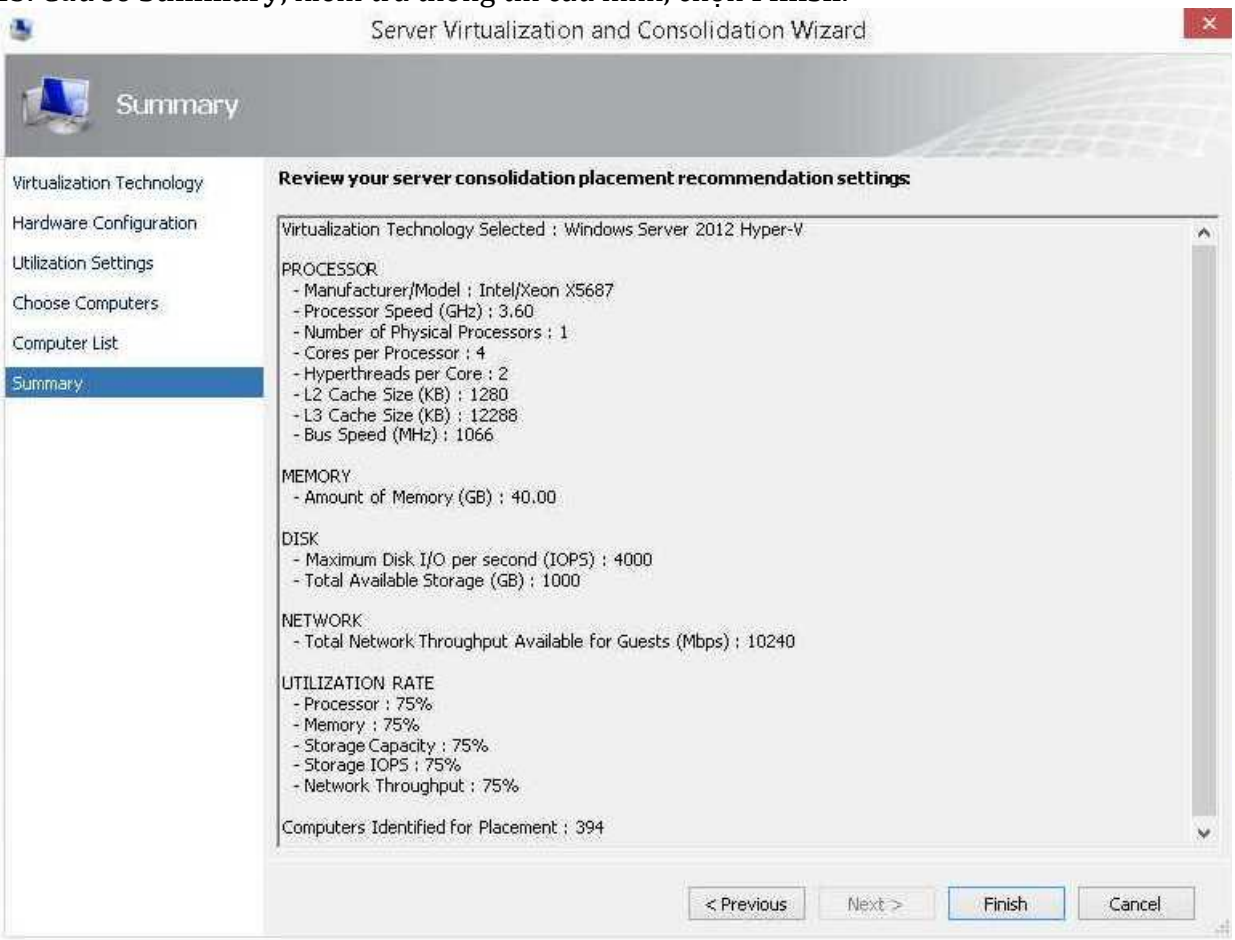
13. Cửa sổ **Choose Computers**, chọn **Choose the computers from a list on the next step of the wizard**, chọn **Next**.



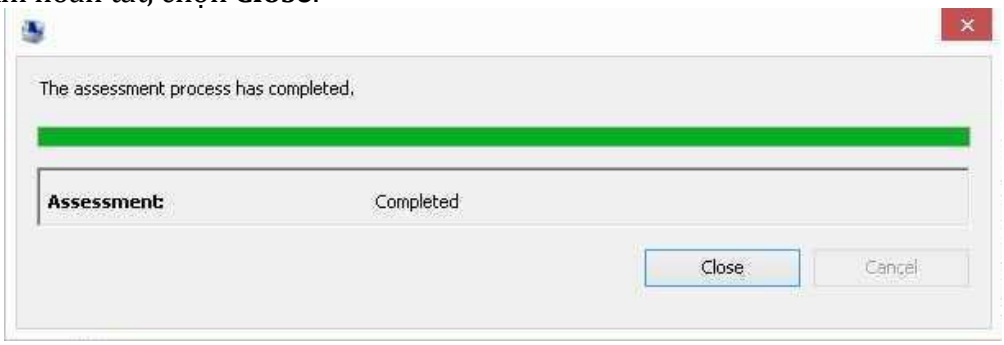
14. Cửa sổ **Computer List**, đánh dấu chọn vào ô **Computer Name**, và chọn **Next**.



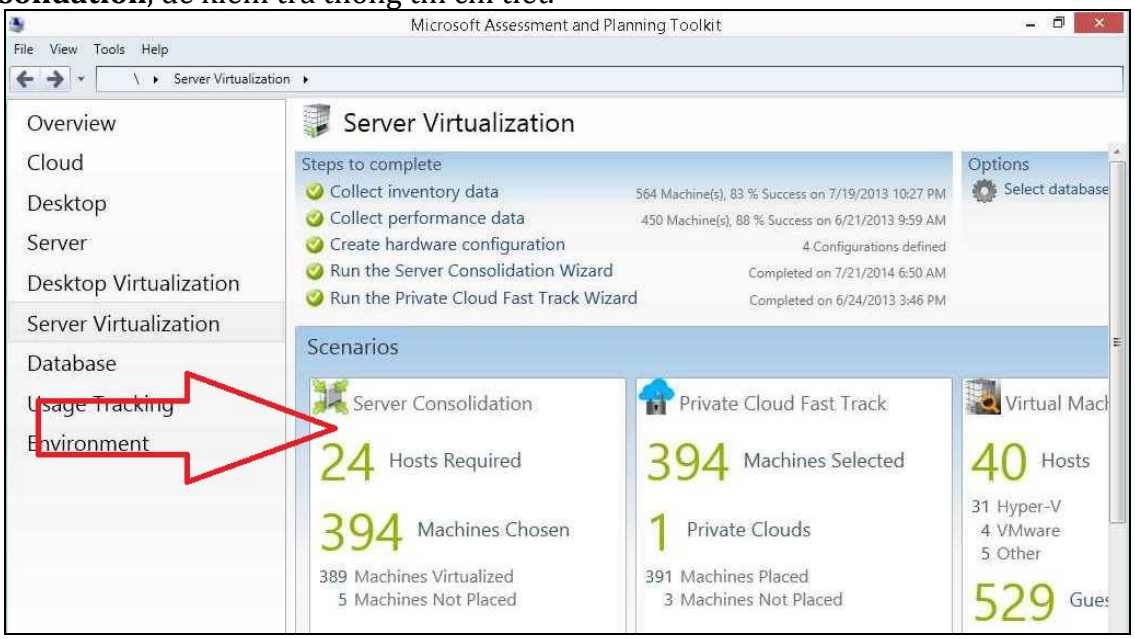
15. Cửa sổ **Summary**, kiểm tra thông tin cấu hình, chọn **Finish**.



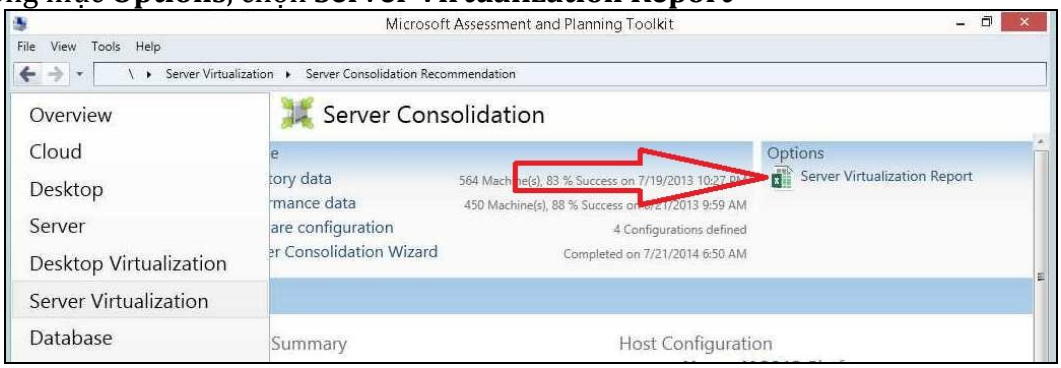
16. Sau khi hoàn tất, chọn **Close**.



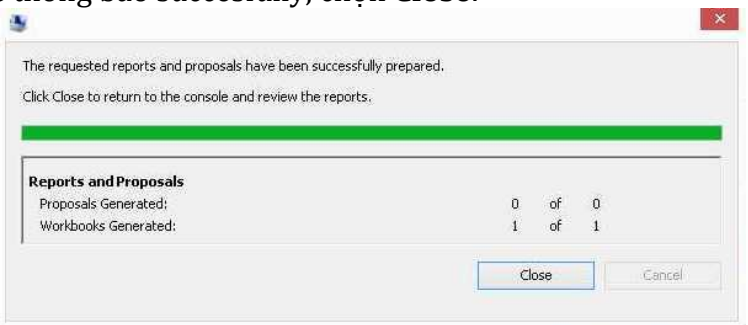
17. Trong cửa sổ MAP, vào mục **Server Virtualization**, trong ô Scenarios, chọn **Server Consolidation**, để kiểm tra thông tin chi tiết.



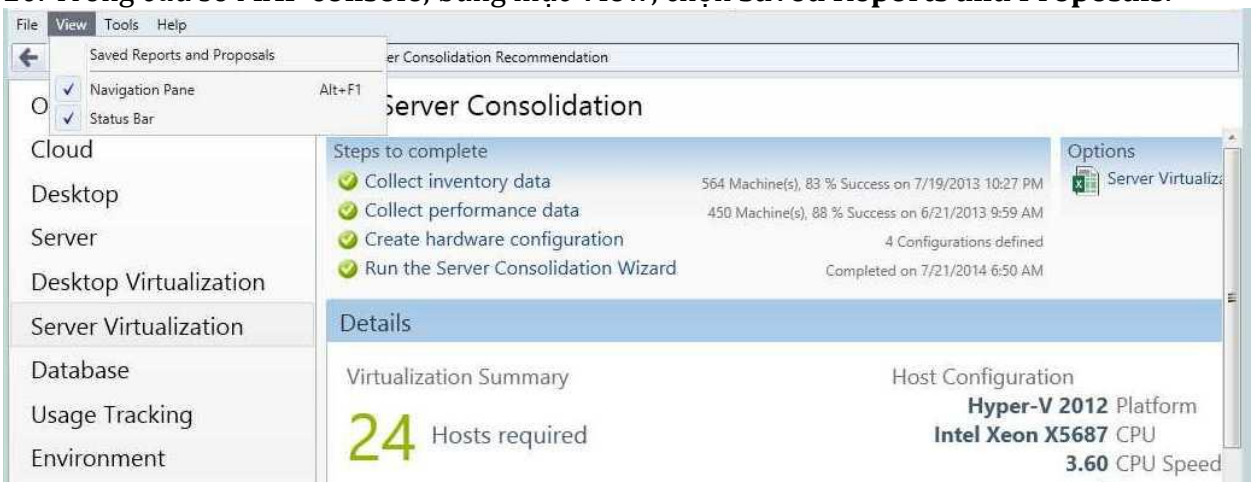
18. Trong mục **Options**, chọn **Server Virtualization Report**



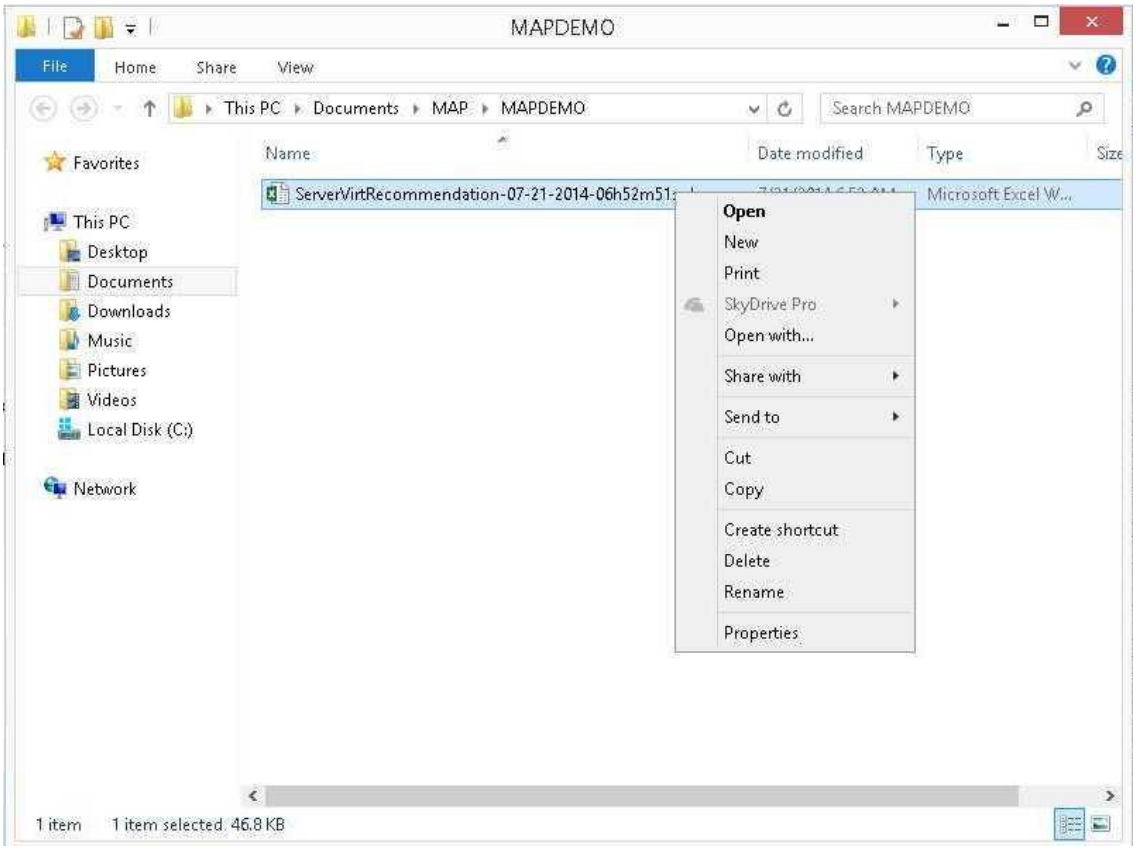
19. Khi nhận được thông báo succesfully, chọn **Close**.



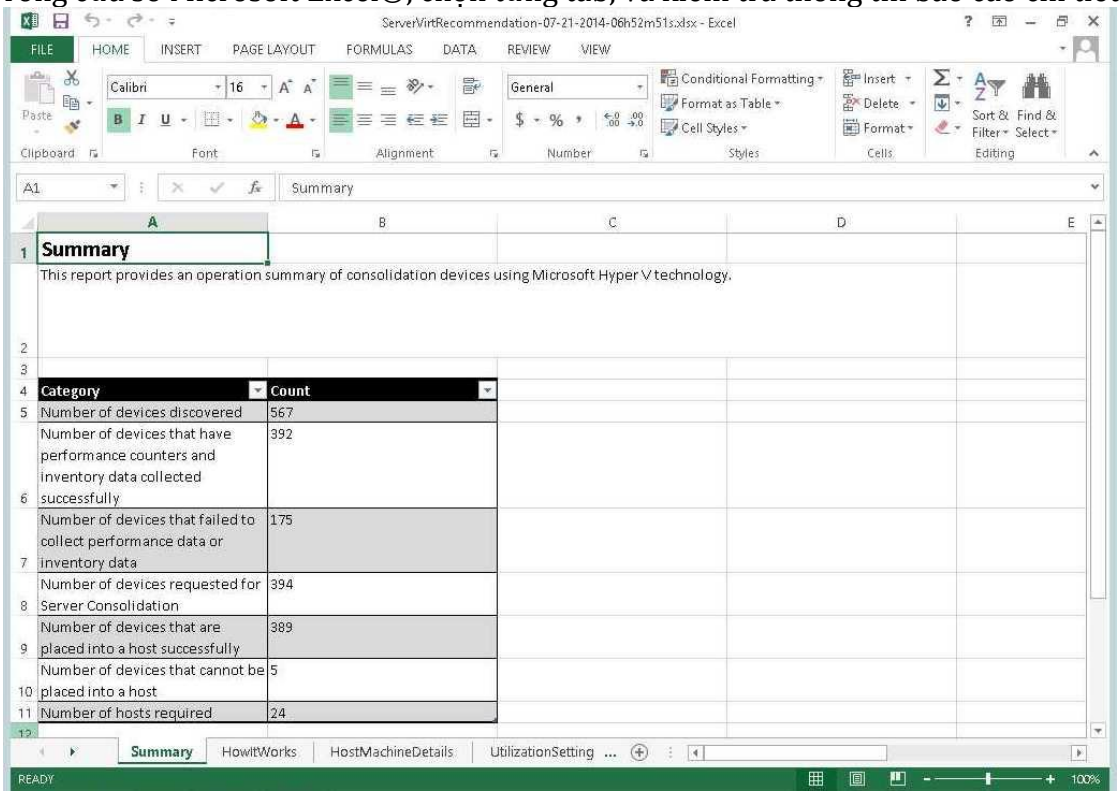
20. Trong cửa sổ **MAP console**, bung mục **View**, chọn **Saved Reports and Proposals**.



21. Trong cửa sổ File Explorer, nhấn chuột phải lên file **ServerVirtRecommendation**, chọn **Open**.



22. Trong cửa sổ Microsoft Excel®, chọn từng tab, và kiểm tra thông tin báo cáo chi tiết.



23. Tắt **Excel** và **File Explorer**.

Kết quả: Trong bài tập này, các bạn đã cài đặt công cụ MAP và sử dụng cơ sở dữ liệu mẫu để đánh giá các server nào phù hợp với giải pháp ảo hóa.

VIII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ Hyper-V Manager.
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20413C-LON-CL1.**

Bài 2: Lập kế hoạch và triển khai cơ sở hạ tầng máy chủ

I. Mục tiêu:

- Lập kế hoạch và chiến lược triển khai cài đặt máy chủ bằng dịch vụ Windows Deployment Services (WDS).
- Chuẩn bị các hình ảnh cài đặt Windows Server 2012 R2.
- Triển khai cài đặt Windows Server 2012 R2 bằng dịch vụ WDS.

II. Kịch bản:

Công ty A. Datum đã lựa chọn sử dụng Windows Server 2012 R2 trong tổ chức của họ. Các máy chủ ở trụ sở chính tại London đang sử dụng Windows Server 2008 và Windows Server 2003. Trong đó, các Domain Controller sử dụng Windows Server 2008.

Kế hoạch thiết kế là bạn phải triển khai Windows Server 2012 R2 tại trụ sở chính để thay thế cho các máy chủ và Domain Controller chạy Windows Server 2008. Ngoài ra, các máy chủ trong các văn phòng trung tâm phải được thay thế bằng các máy chủ chạy Windows Server 2012 R2.

Các văn phòng chi nhánh và các trung tâm phân phối có một ứng dụng hỗ trợ kinh doanh (LOB), ứng dụng này đã được chuyển từ UNIX sang Windows Server 2012 R2. Mỗi địa điểm đã được trang bị máy chủ riêng để hỗ trợ ứng dụng này. Ngoài ra, các dịch vụ cơ sở hạ tầng mạng phải được chuyển qua Windows Server 2012 R2.

Đội ngũ thiết kế mạng đã quy định rằng một số máy chủ, bao gồm cả Domain Controller, phải được ảo hóa nếu có thể. Kế hoạch triển khai của bạn nên bao gồm khả năng A. Datum sẽ mua lại hai công ty mới trong tương lai gần, và khả năng sẽ triển khai thêm các máy chủ chạy Windows Server 2012 R2. Ngoài ra, bạn phải tạo ra một hình ảnh máy chủ (Server Image) tiêu và chuẩn bị các công cụ phù hợp để thực hiện kế hoạch triển khai của bạn.

III. Yêu cầu tổng quan:

Để thiết kế một chiến lược triển khai cài đặt máy chủ tự động, hãy xem xét các yếu tố thiết kế như sau:

- Quen thuộc với việc quản lý hình ảnh hệ điều hành (OS Image) bởi các nhân viên IT.
- Số lượng máy chủ được triển khai.
- Những thay đổi trong cấu hình máy chủ.
- Sử dụng giấy phép bản quyền (License) của hệ điều hành.
- Cấu hình mạng, cả về sự phân bố của các máy chủ cho việc triển khai, và trong điều khoản của dịch vụ được cài đặt hiện tại để hỗ trợ quá trình triển khai.

Các nhân viên IT đang có kế hoạch để triển khai Windows Server 2012 R2 cho các văn phòng khác nhau, và một số đã có kinh nghiệm với việc triển khai và quản lý hình ảnh hệ điều hành (OS Image).

Không có yêu cầu nâng cấp các cài đặt từ các máy chủ hiện tại vì có kế hoạch giới thiệu phần cứng máy chủ mới và ảo hóa nếu có thể.

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1** **20413C-LON-SVR3**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung Start menu, mở **Hyper-V Manager**.
2. Trong cửa sổ Hyper-V Manager, nhấn phải chuột lên máy ảo **20413C-LON-DC1** chọn **Start.**
3. Nhấn phải chuột lên lại máy ảo **20413C-LON-DC1** chọn **Connect**.
4. Logon vào máy ảo với thông tin sau:

- User name: **Adatum\Administrator**
- Password: **Pa$$w0rd**

5. Thực hiện lại từ bước 2 đến bước 4 cho máy ảo **20413C-LON-SVR1.**
6. **Chú ý:** Không khởi động máy **20413C-LON-SVR3** cho tới khi có yêu cầu

VI. Thực hành:

Thời gian thực hành: 60 phút

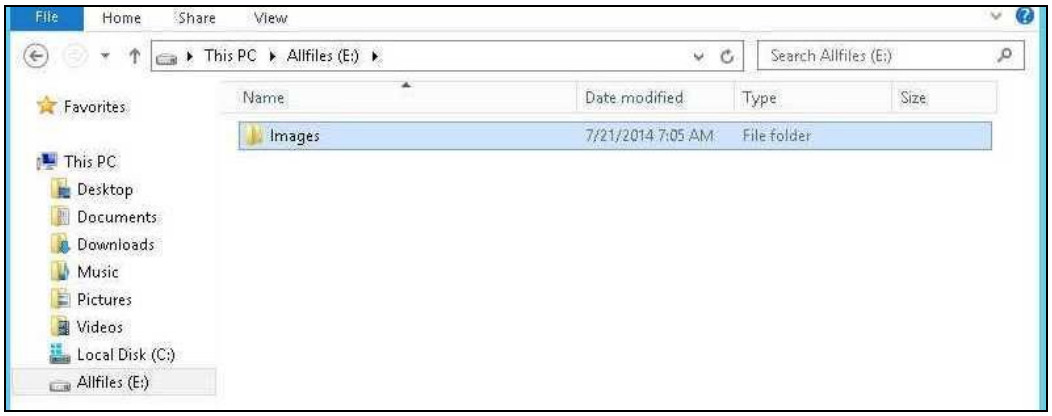
Bài tập 1: Chuẩn bị hình ảnh cài đặt Windows Server 2012 (OS Image)

Bước 1: Tạo nơi lưu trữ file Image, và Map ổ đĩa tới đường dẫn lưu file Image.

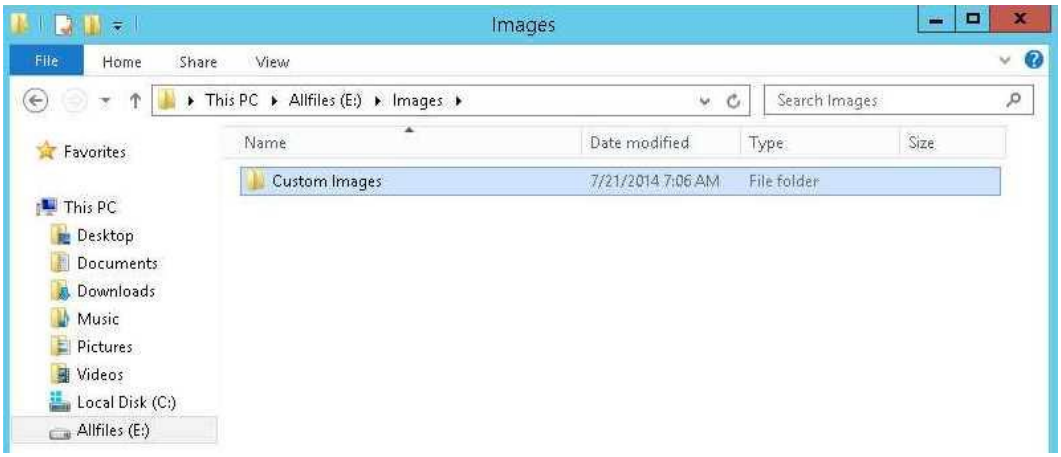
1. Logon vào máy LON-SVR1, trong thanh taskbar, mở **File Explorer**.



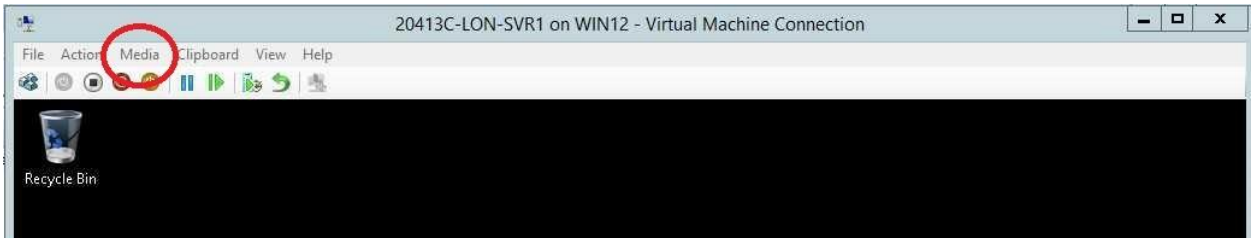
2. Trong cửa sổ File Explorer, vào ổ đĩa **Allfiles (E:)**, tạo folder mới, đặt tên folder là **Images**.



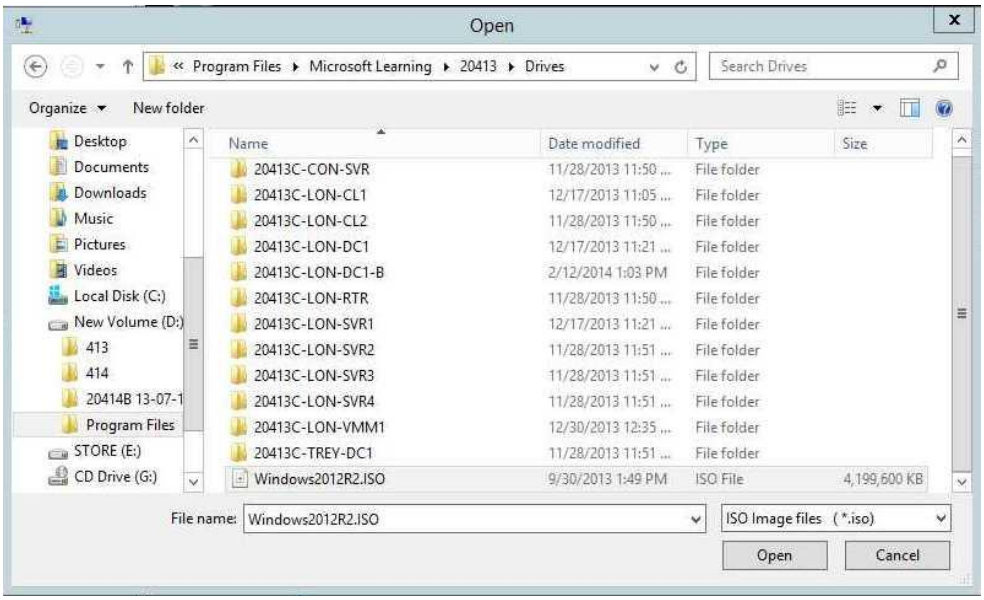
3. Trong cửa sổ File Explorer, mở folder **Images**, tạo folder con tên **Custom Images**



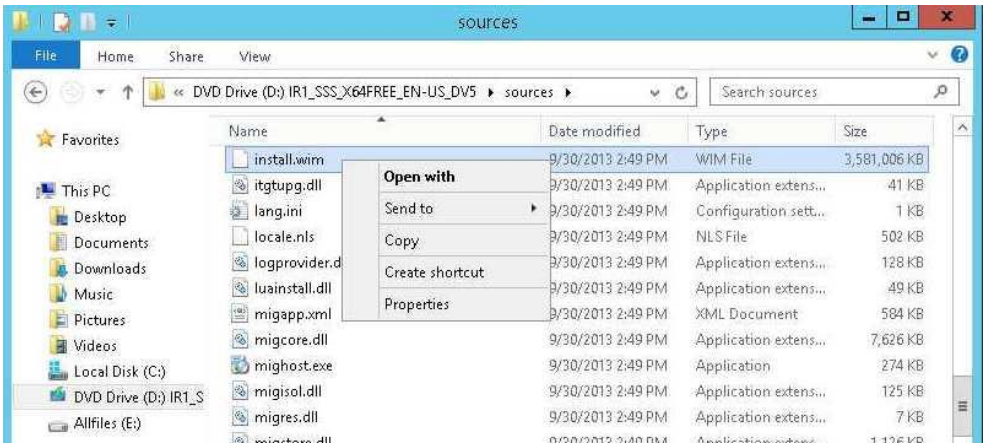
4. Trong cửa sổ máy ảo 20413C-LON-SVR1, bung menu **Media**, chọn **DVD Drive**, chọn **Insert Disk**.



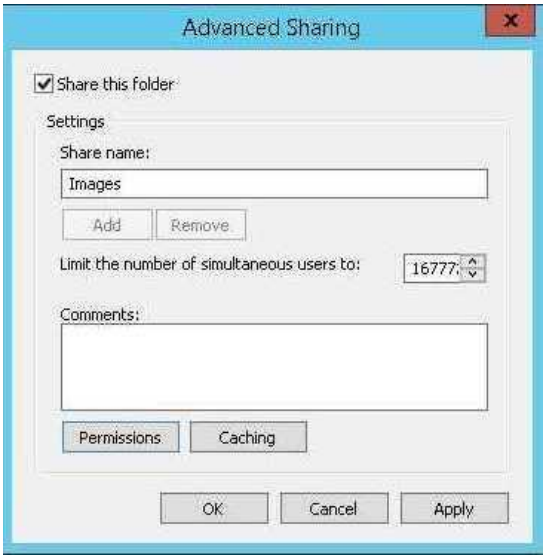
5. Trong hộp thoại **Open**, trỏ đến đường dẫn **D:\Program Files\Microsoft Learning\20413\Drives,** chọn file **Windows2012R2.iso**, chọn **Open**.



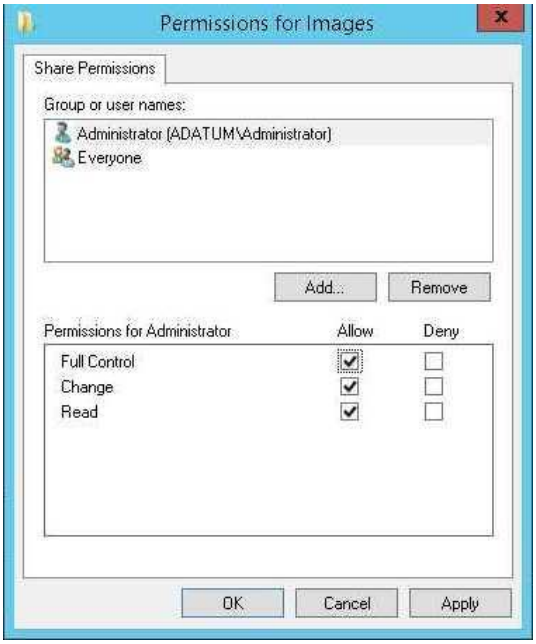
6. Vào đường dẫn **D:\sources,** copy file **install.wim** qua đường dẫn **E:\Images\Custom Images.**



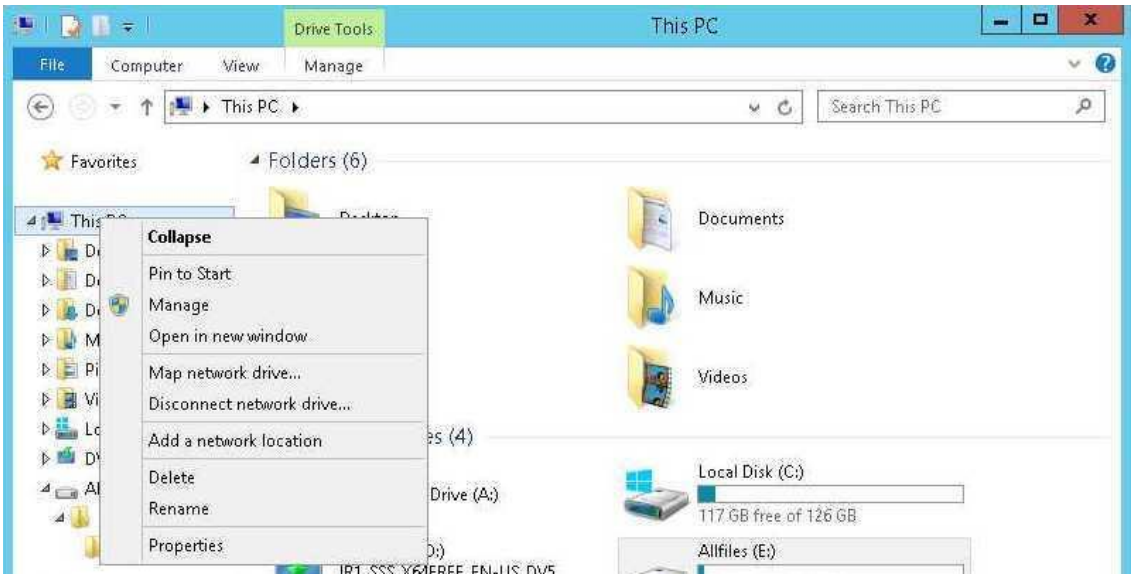
7. Vào ổ đĩa **E:,** nhấn chuột phải lên folder **Images**, chọn **Properties**. Trong hộp thoại **Images Properties**, qua tab **Sharing**, chọn **Advanced Sharing**. Hộp thoại **Advanced Sharing**, đánh dấu chọn **Share this folder,** và chọn **Permission**



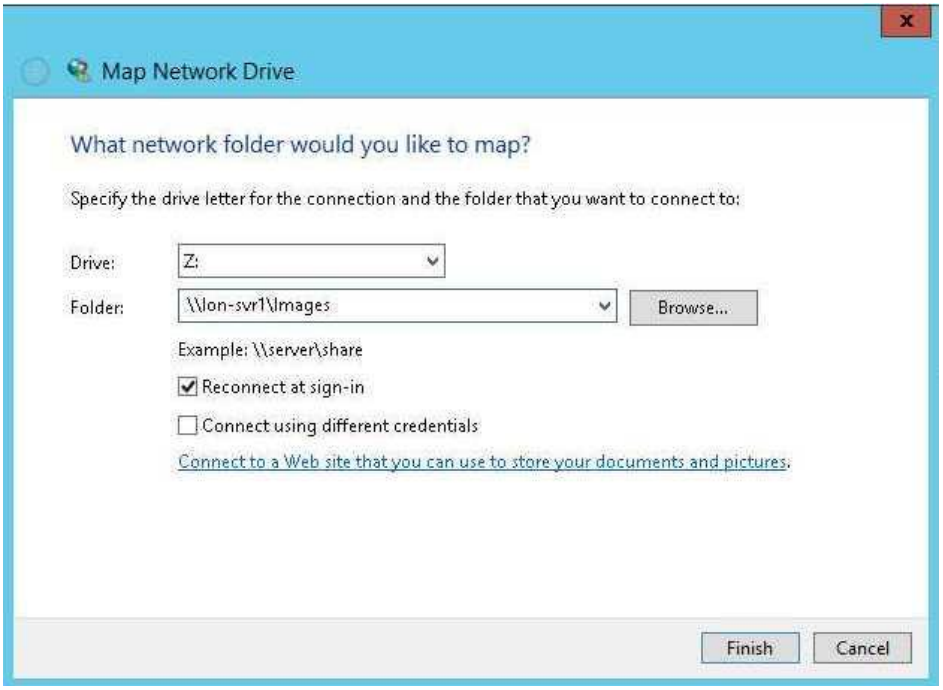
8. Trong hộp thoại **Permissions for Images**, chọn **Add**. Trong hộp thoại **Select Users, Computers, Service Accounts, or Groups** nhập **Administrator**, chọn **OK**. cấp cho **Administrator** quyền **Full Control** (cột Allow), chọn **OK** tất cả hộp thoại và chọn **Close**.



9. Trong cửa sổ File Explorer, nhấn chuột phải **This PC**, chọn **Map network drive**.

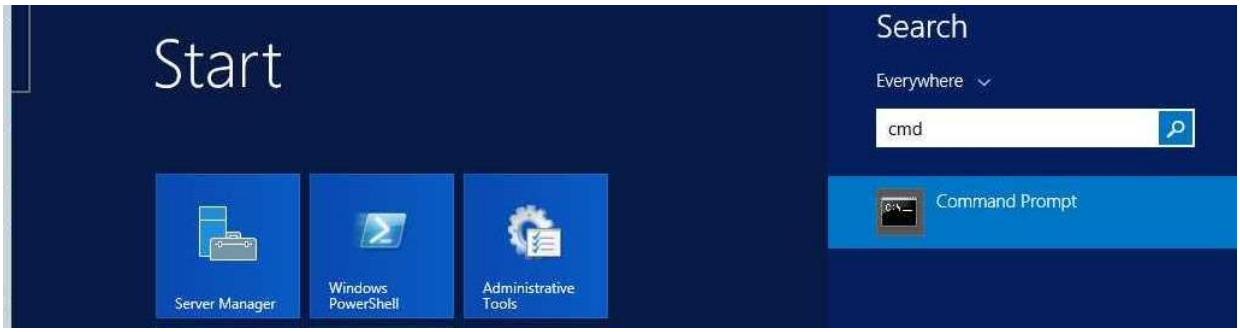


10. Trong hộp thoại **Map network**, nhập **\\lon-svr1\Images** vào ô **Folder**, chọn **Finish**.



Bước 2: Gắn kết file Image

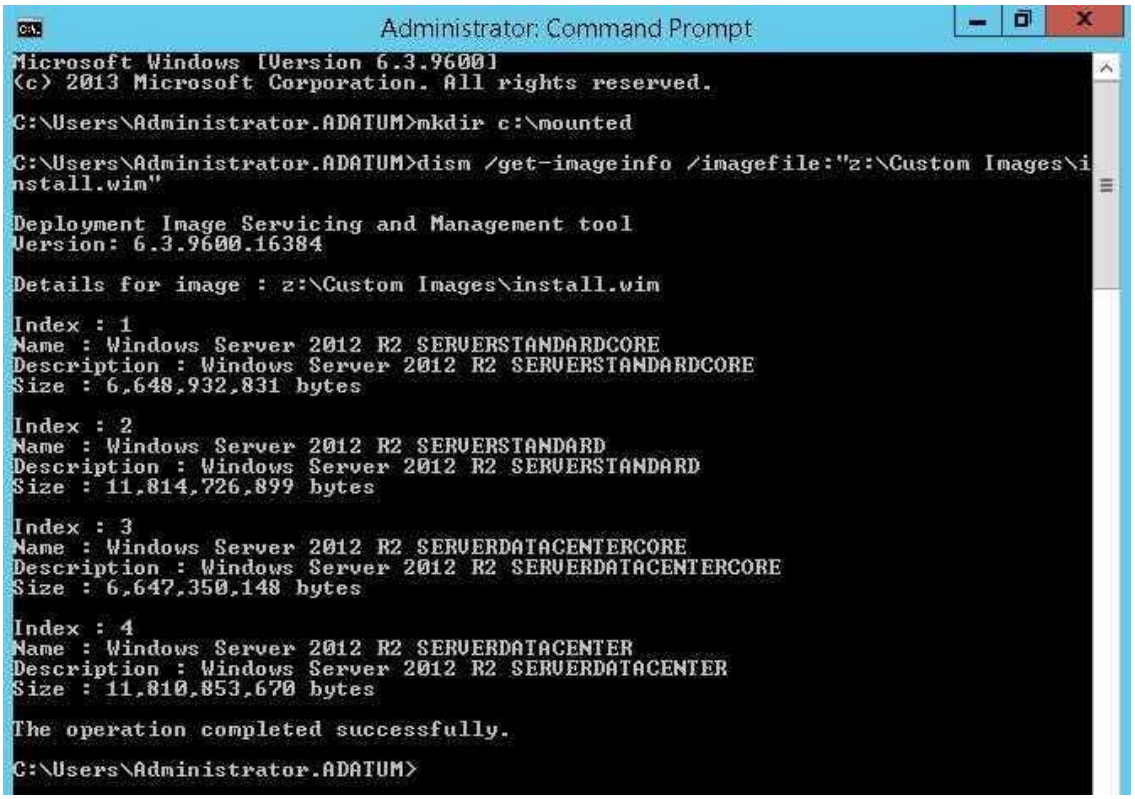
1. Trên máy **LON-SVR1**, bung **Start** menu, gõ **cmd.exe**, mở **Command Prompt**



2. Trong cửa sổ command prompt, gõ lệnh: **Mkdir c:\mounted**

3. Sau đó gõ tiếp lệnh :

Dism /get-imageinfo /imagefile:"z:\Custom Images\install.wim"



Đảm bảo nhận được thông báo **The operation completed successfully**.

Chú thích: Lệnh này liệt kê tất cả các phiên bản Windows trong file install.wim. Chú ý chỉ số của Windows Server 2012 R2 Datacenter có Index là 4.

4. Trong command prompt, gõ lệnh:

Dism /mount-wim /wimfile:"z:\Custom Images\install.wim" /index:4 /mountdir:c:\mounted



Đảm bảo nhận được thông báo **The operation completed successfully**.

Bước 3: Add Web Server (IIS) role vào file image

1. Trong command prompt, gõ lệnh:

Dism /image:c:\mounted /get-features

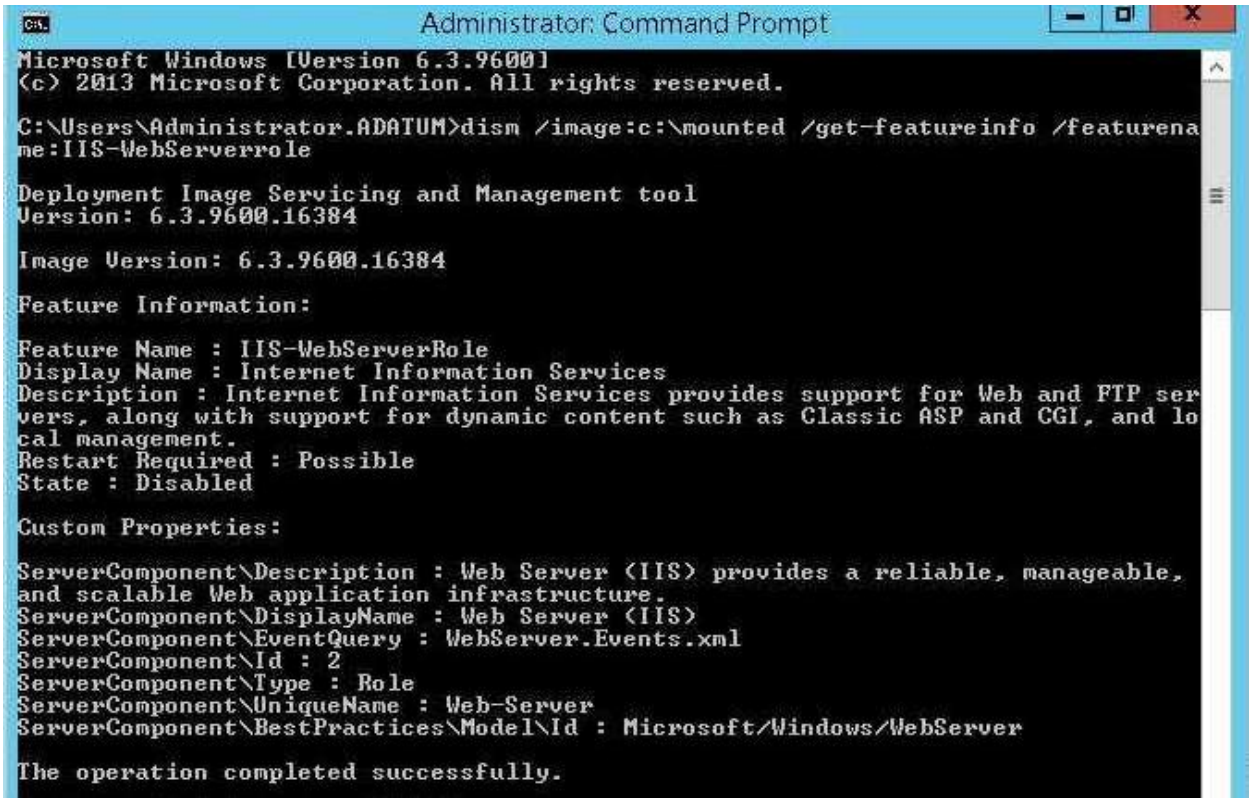


Chú thích: Lệnh này liệt kê các tính năng có sẵn trong file Image. Nếu bạn muốn xem tất cả thông tin của file Image, bạn có thể xuất thông tin ra file txt bằng lệnh:

Dism /image:c:\mounted /get-features > c:\All Features.txt

2. Trong command prompt, gõ lệnh:

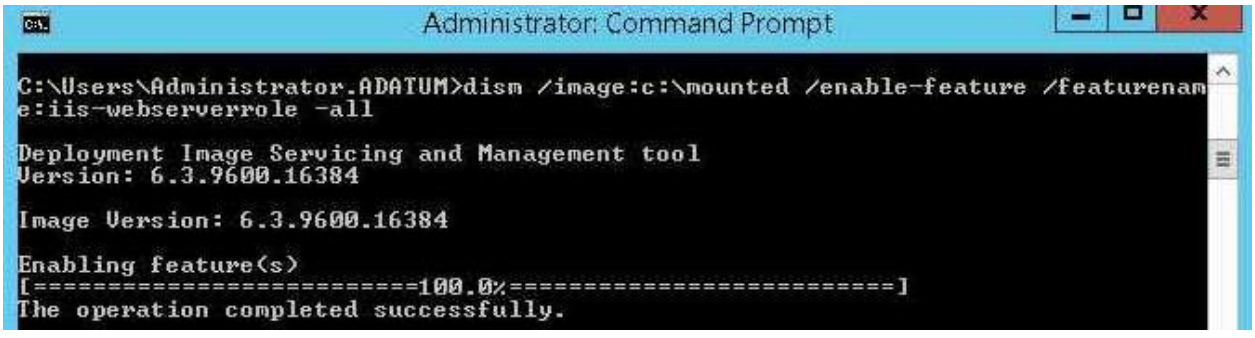
Dism /image:c:\mounted /get-featureinfo /featurename:IIS-WebServerRole



Chú ý: Web Server (IIS) role đang ở trạng thái disabled.

3. Trong command prompt, gõ lệnh:

Dism /image:c:\mounted /enable-feature /featurename:IIS-WebServerRole –all

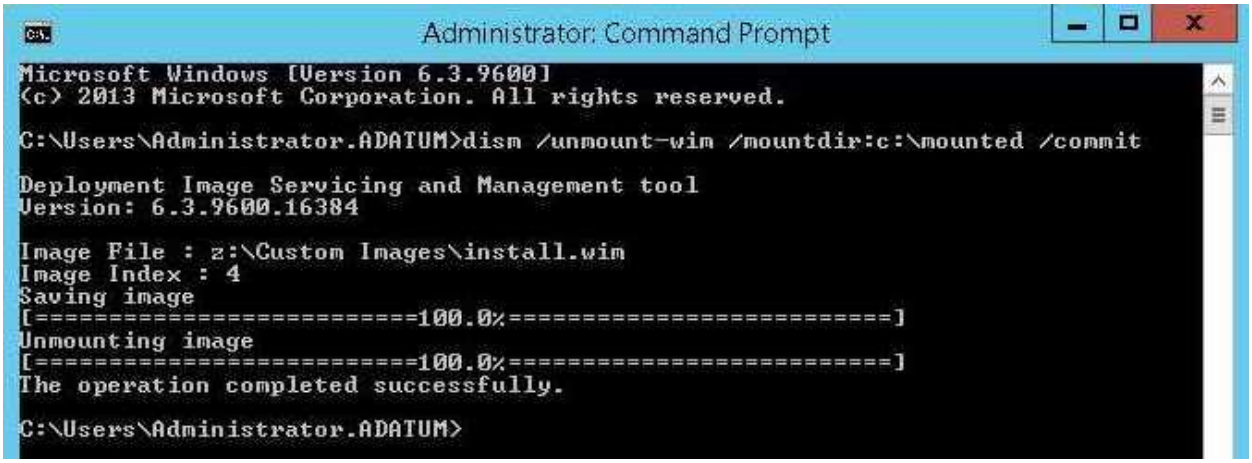


Đảm bảo nhận được thông báo **The operation completed successfully**.

Chú thích: Lệnh này có chức năng cài đặt Web Server (IIS) role.

4. Trong command prompt, gõ tiếp lệnh:

Dism /unmount-wim /mountdir:c:\mounted /commit



Đảm bảo nhận được thông báo **The operation completed successfully**.

Chú thích: Lệnh này có chức năng cập nhật sự thay đổi của file install.wim.

Kết quả: Sau khi hoàn thành bài tập này, bạn đã chuẩn bị được file hình ảnh hệ điều hành (Install.wim), và thêm tính năng Web Server (IIS) role vào file hình ảnh.

Bài tập 2: Triển khai cài đặt Windows Server 2012 R2 từ file Image

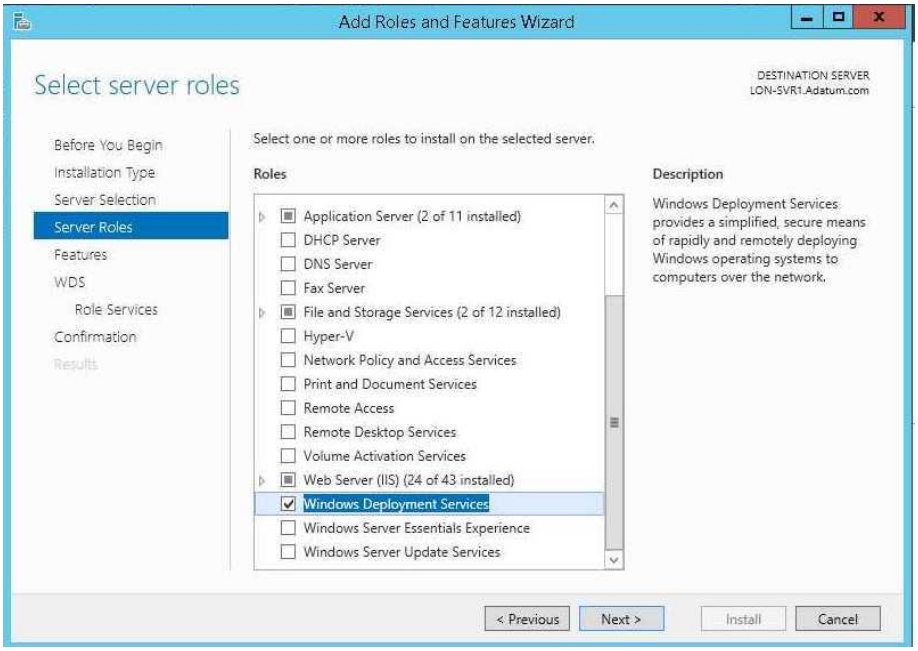
Bước 1: Cài đặt Windows Deployment Service role

1. Trên máy **LON-SVR1**, mở **Server Manager**, bung **Manage**, chọn **Add Roles and Features**.



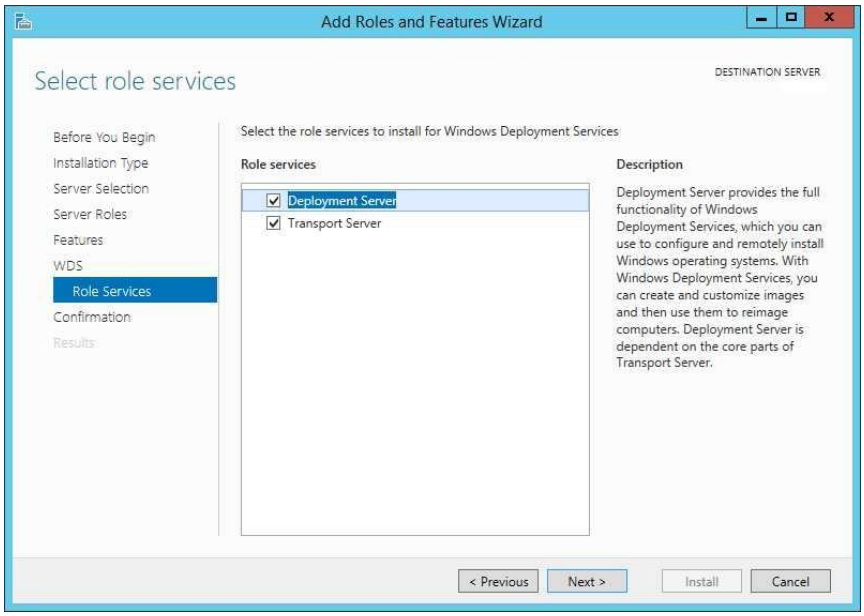
2. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.

3. Trong cửa sổ **Select server roles**, đánh dấu chọn **Windows Deployment Services** . Trong hộp thoại **Add Roles and Features Wizard**, chọn **Add Features**, chọn **Next**.

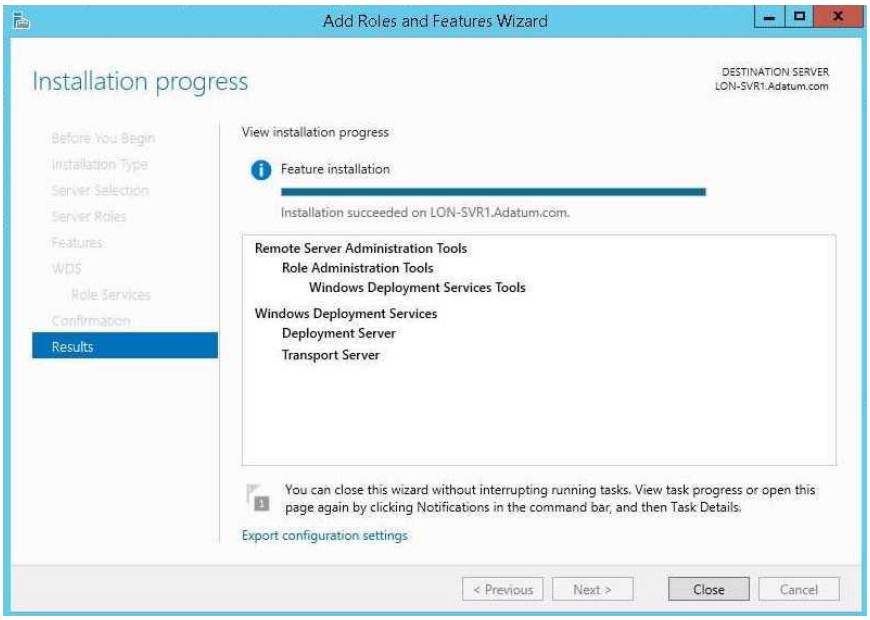


4. Cửa sổ **Select features**, chọn **Next** 2 lần.

5. Cửa sổ **Select role services**, kiểm tra có đánh dấu chọn cả 2 mục **Deployment Server** và **Transport Server**, chọn **Next**, chọn **Install**

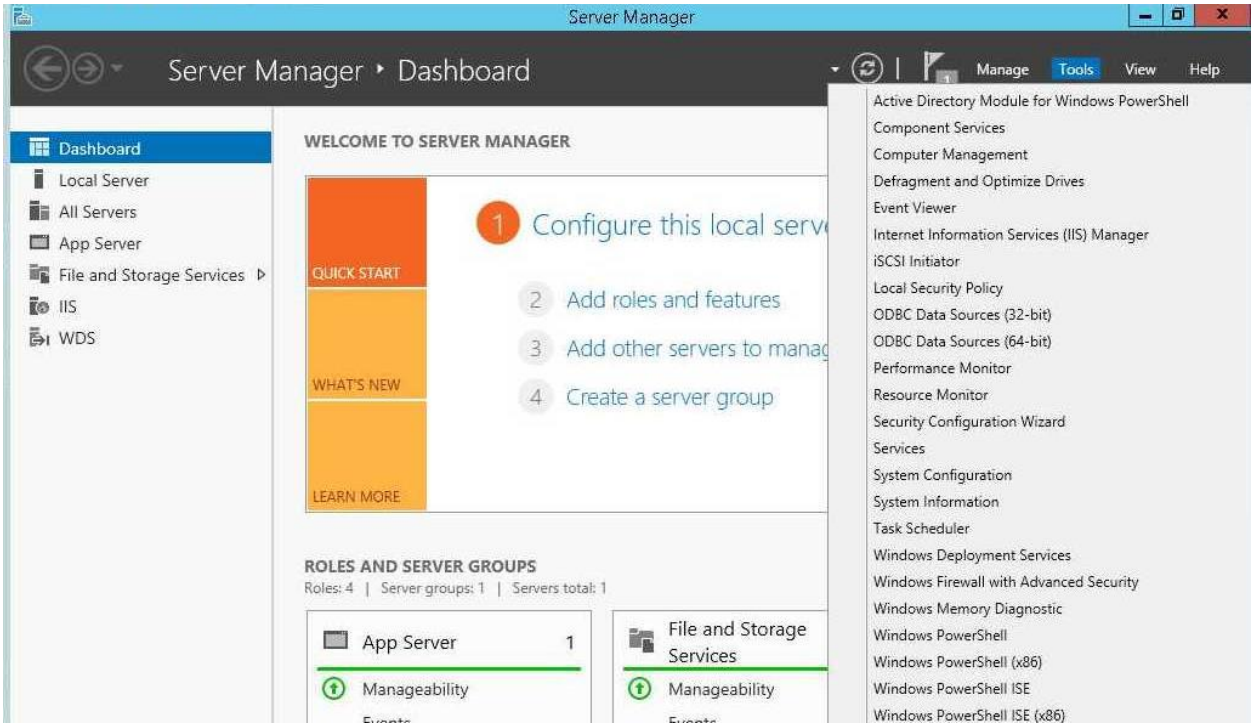


6. Sau khi cài đặt thành công, chọn **Close**.

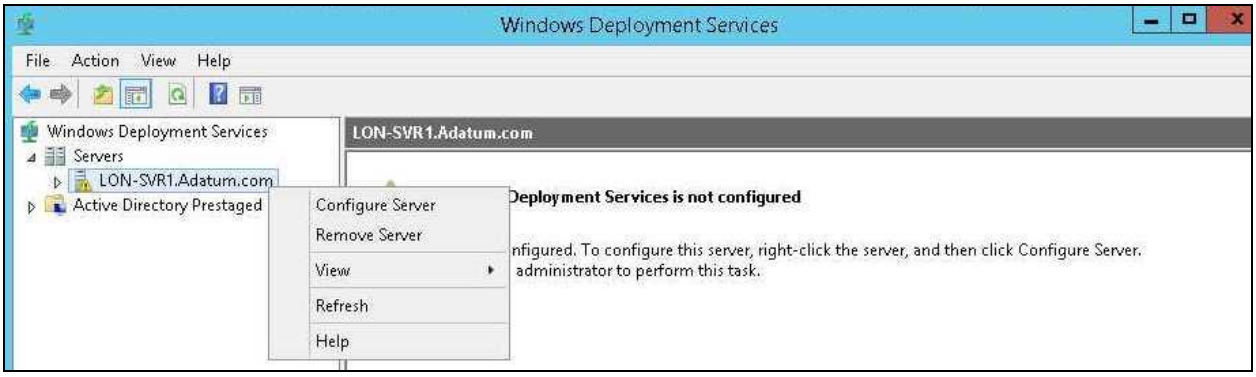


Bước 2: Cấu hình Windows Deployment Services (WDS)

1. Trong **Server Manager**, bung menu **Tools**, chọn **Windows Deployment Services**.

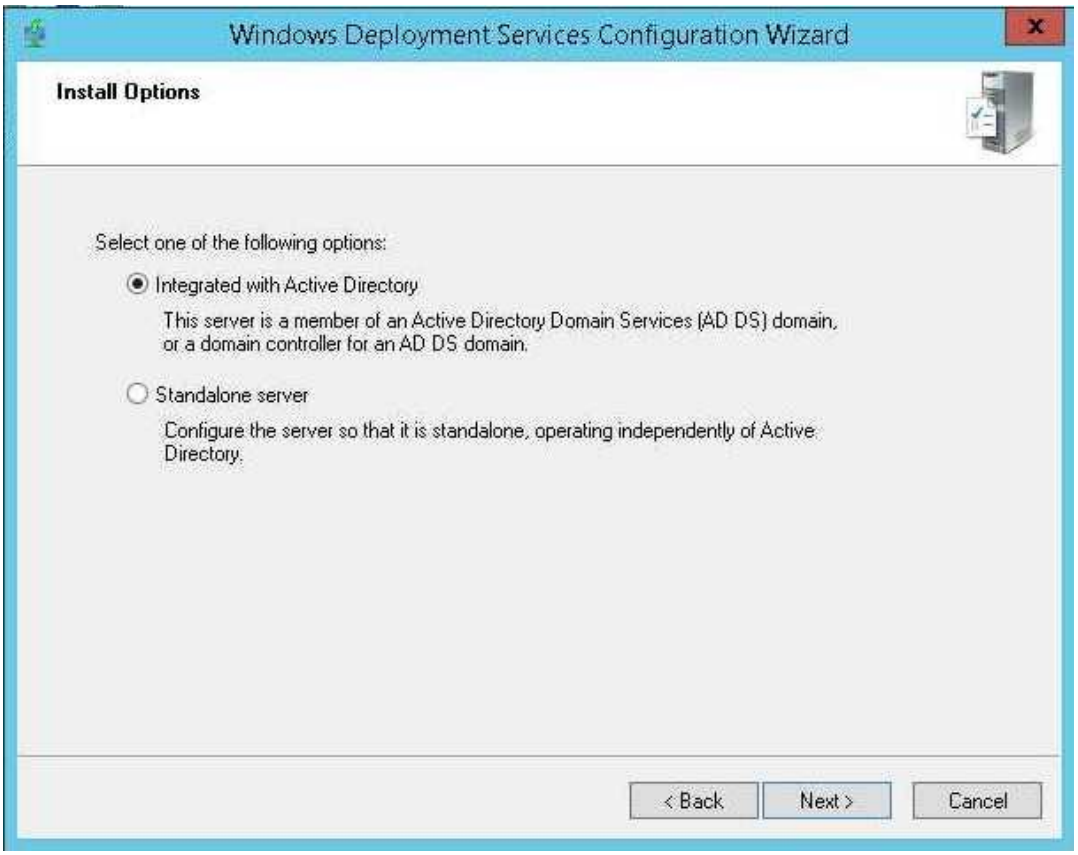


2. Trong cửa sổ **Windows Deployment Services**, bung **Servers**, nhấn chuột phải **LON-SVR1.Adatum.com**, chọn **Configure Server**.

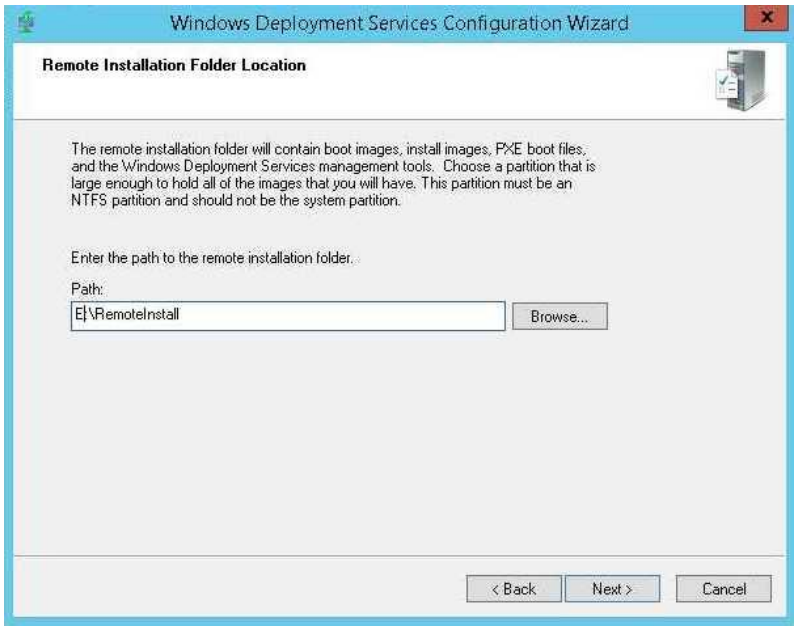


3. Cửa sổ **Before You Begin** ,chọn **Next**.

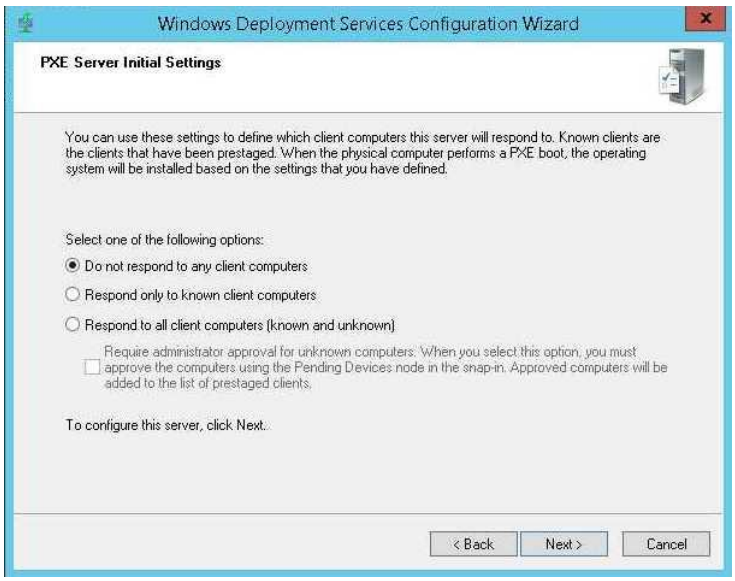
4. Cửa sổ **Install Options**, kiểm tra chọn **Integrated with Active Directory**, chọn **Next**.



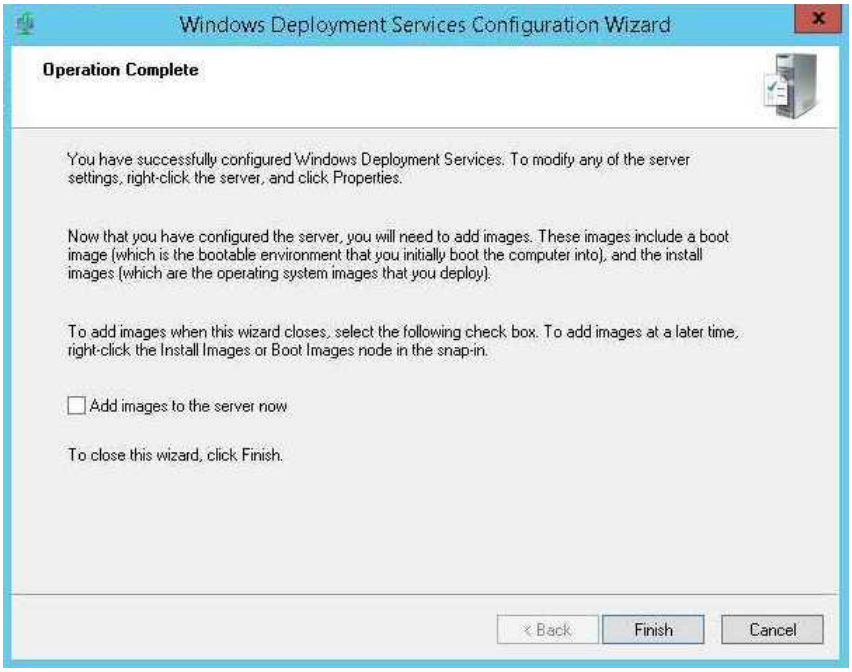
5. Cửa sổ **Remote Installation Folder Location**, nhập **E:\RemoteInstall** vào ô **Path**, chọn **Next**.



6. Cửa sổ **PXE Server Initial Settings.** kiểm tra chọn **Do not respond to any client computers,** chọn **Next**.



7. Cửa sổ **Operation Complete**, bỏ dấu chọn **Add images to the server now,** chọn **Finish**.



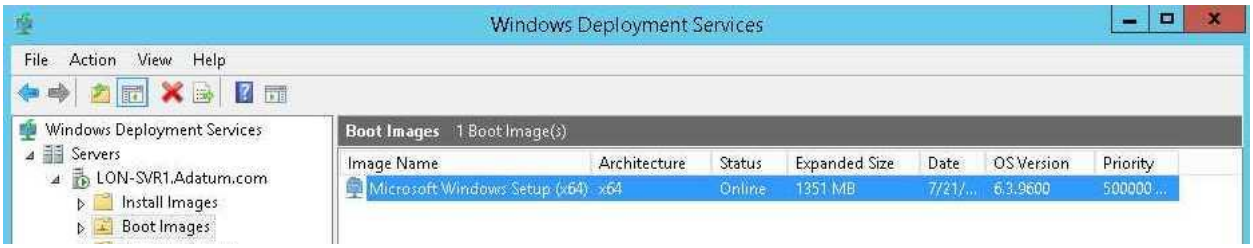
Bước 3: Sử dụng công cụ WDSUtil để add file Boot image

1. Mở Command Prompt. gõ lệnh:

Wdsutil /add-image /ImageFile:"d:\sources\boot.wim" /ImageType:boot

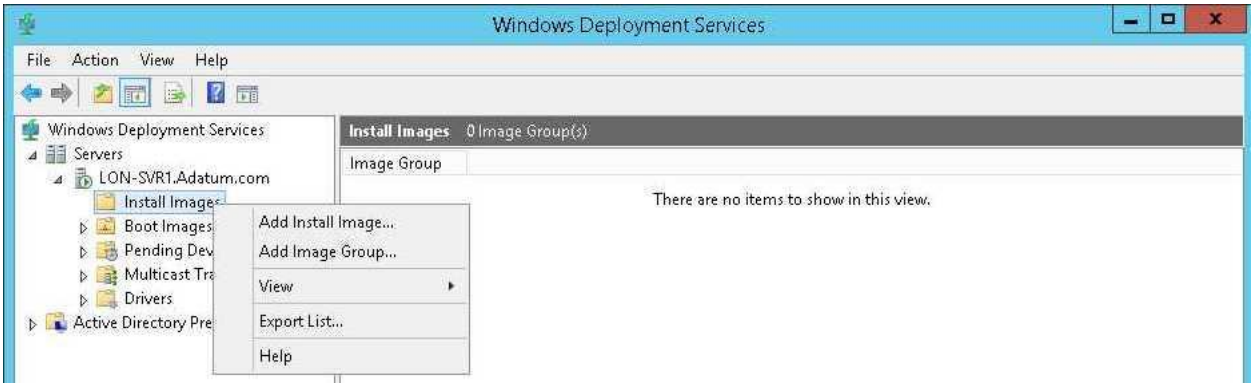


2. Mở công cụ **Windows Deployment Services**, bung **LON-SVR1.Adatum.com**, bung **Boot Images**. Kiểm tra đã có một boot image: **Microsoft Windows Setup (x64).**

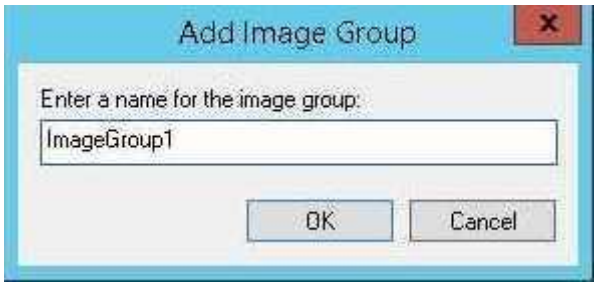


Bước 4: Add file Install image

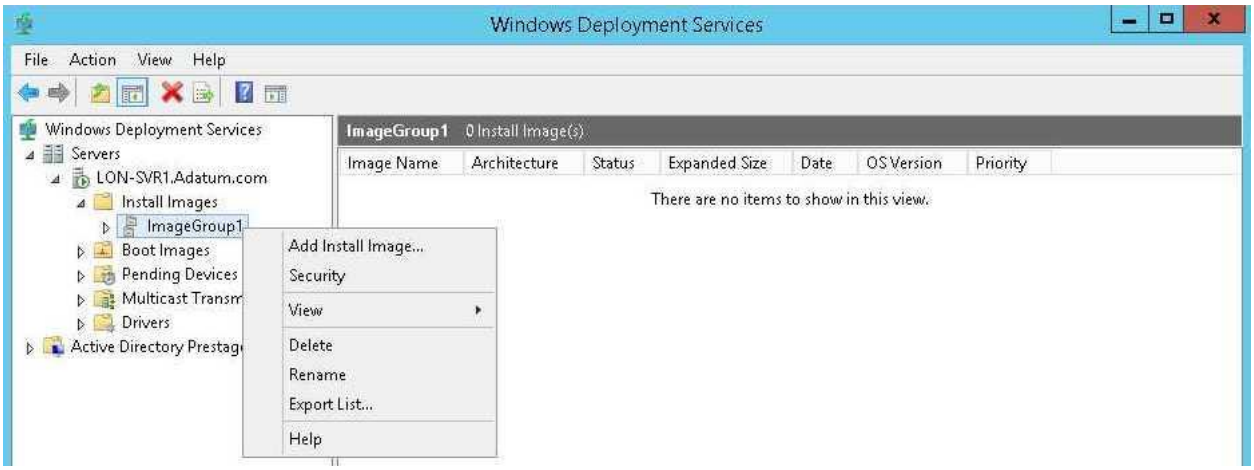
1. Trong cửa sổ **Windows Deployment Services**, nhấn chuột phải **Install Images**, chọn **Add Image Group**.



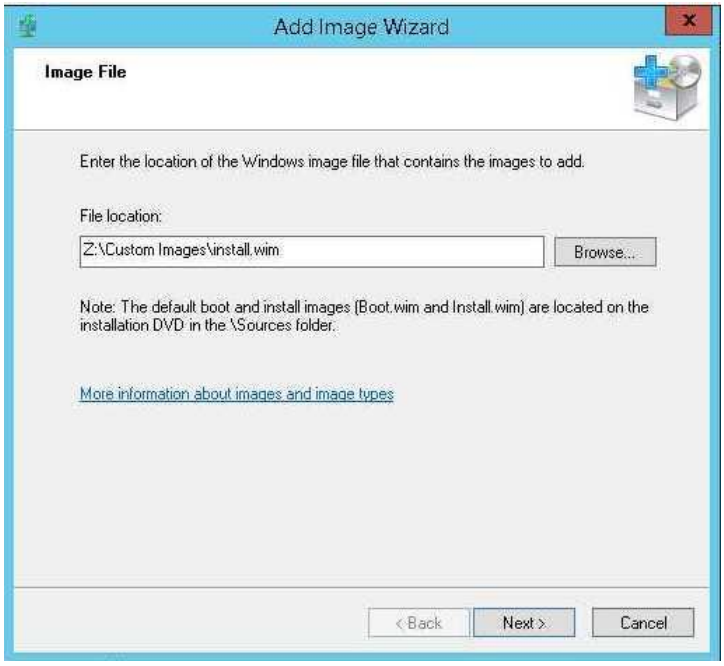
2. Trong hộp thoại **Add Image Group**, nhập **ImageGroup1** vào ô **Name,** chọn **OK**.



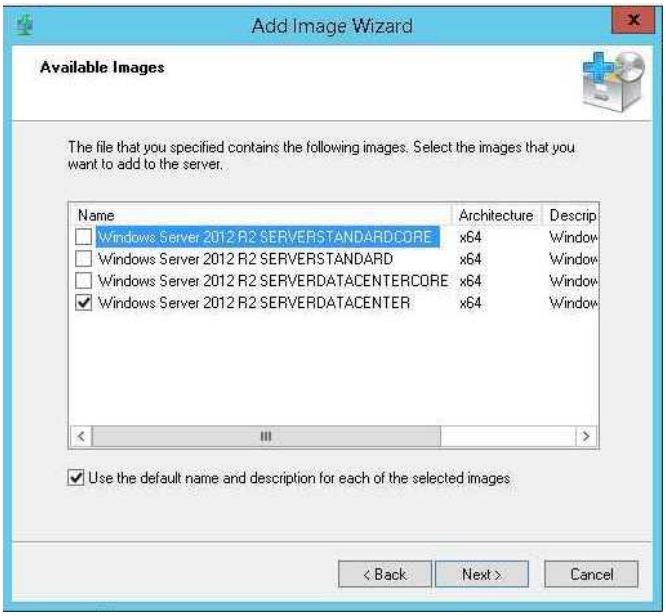
3. Trong cửa sổ **Windows Deployment Services** Nhấn chuột phải **ImageGroup1**, chọn **Add Install Image**.



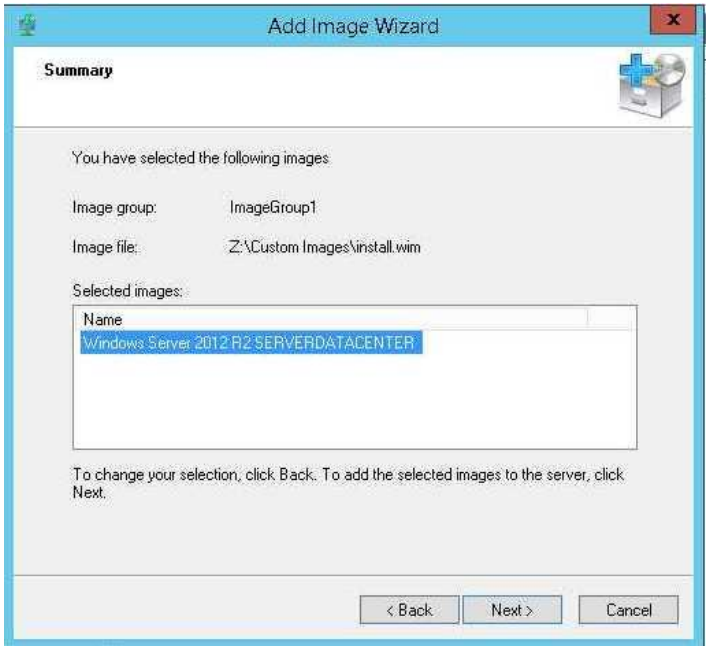
4. Cửa sổ **Add Image Wizard**, nhập **Z:\custom images\install.wim** vào ô **File location,** chọn **Next**.



5. Cửa sổ **Available Images**, bỏ trắng tất cả các lựa chọn, sau đó đánh dấu chọn **Windows Server 2012 SERVERDATACENTER** , chọn **Next**.



6. Cửa sổ **Summary**, chọn **Next**, và chọn **Finish**.

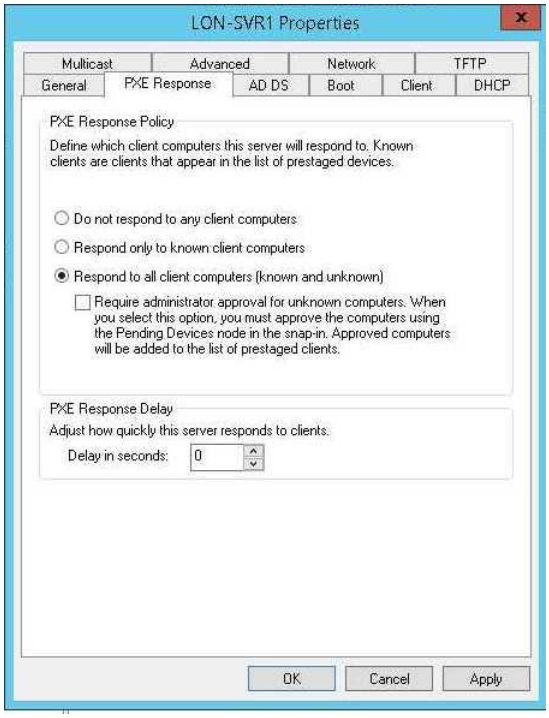


Bước 5: Cấu hình chức năng tự động đặt Computer Name

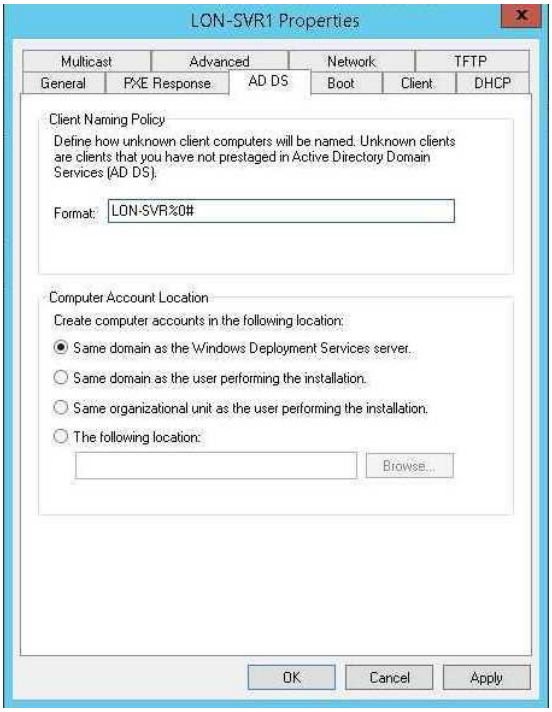
1. Trong cửa sổ **Windows Deployment Services**, nhấn chuột phải **LON-SVR1.Adatum.com**, chọn**Properties**.



2. Trong hộp thoại **Properties,** qua tab **PXE Response**, chọn **Respond to all client computers (known and unknown)**.



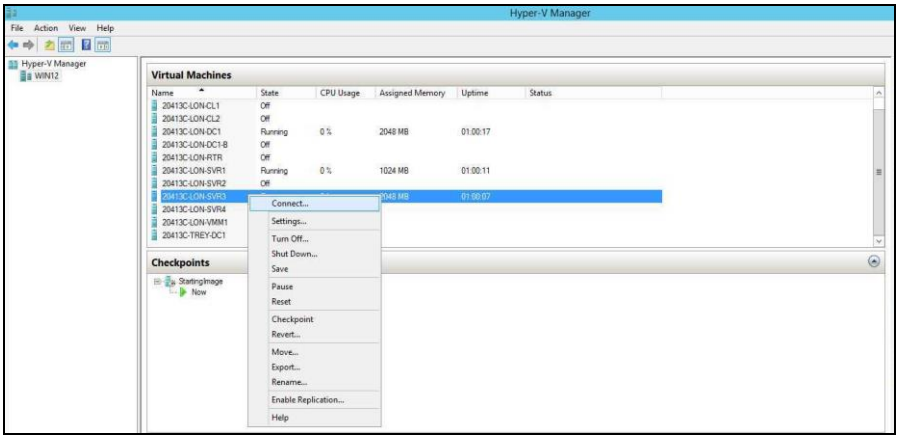
3. Qua tab **AD DS**, nhập **LON-SVR%0#** vào ô **Format,** chọn **OK**.



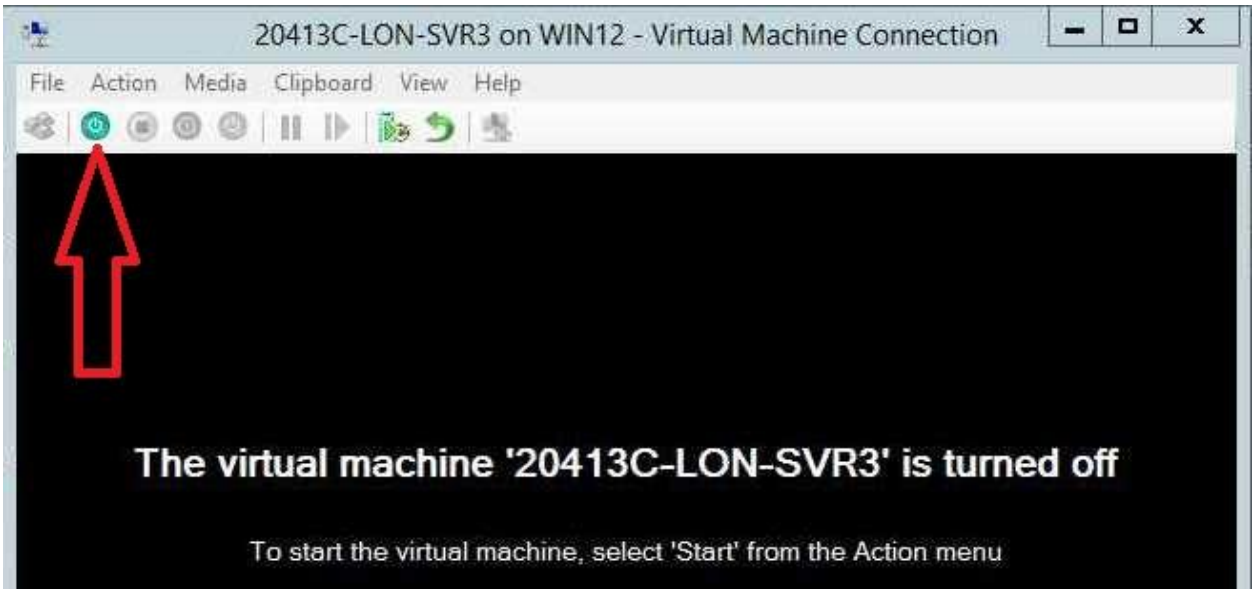
Bước 6: Khởi động quá trình triển khai

1. Trên **máy thật**, mở công cụ **Hyper V Manager**.

2. Trong cửa sổ **Hyper V Manager**, nhấn chuột phải lên máy ảo **20413C-LON-SVR3**, chọn **Connect**.



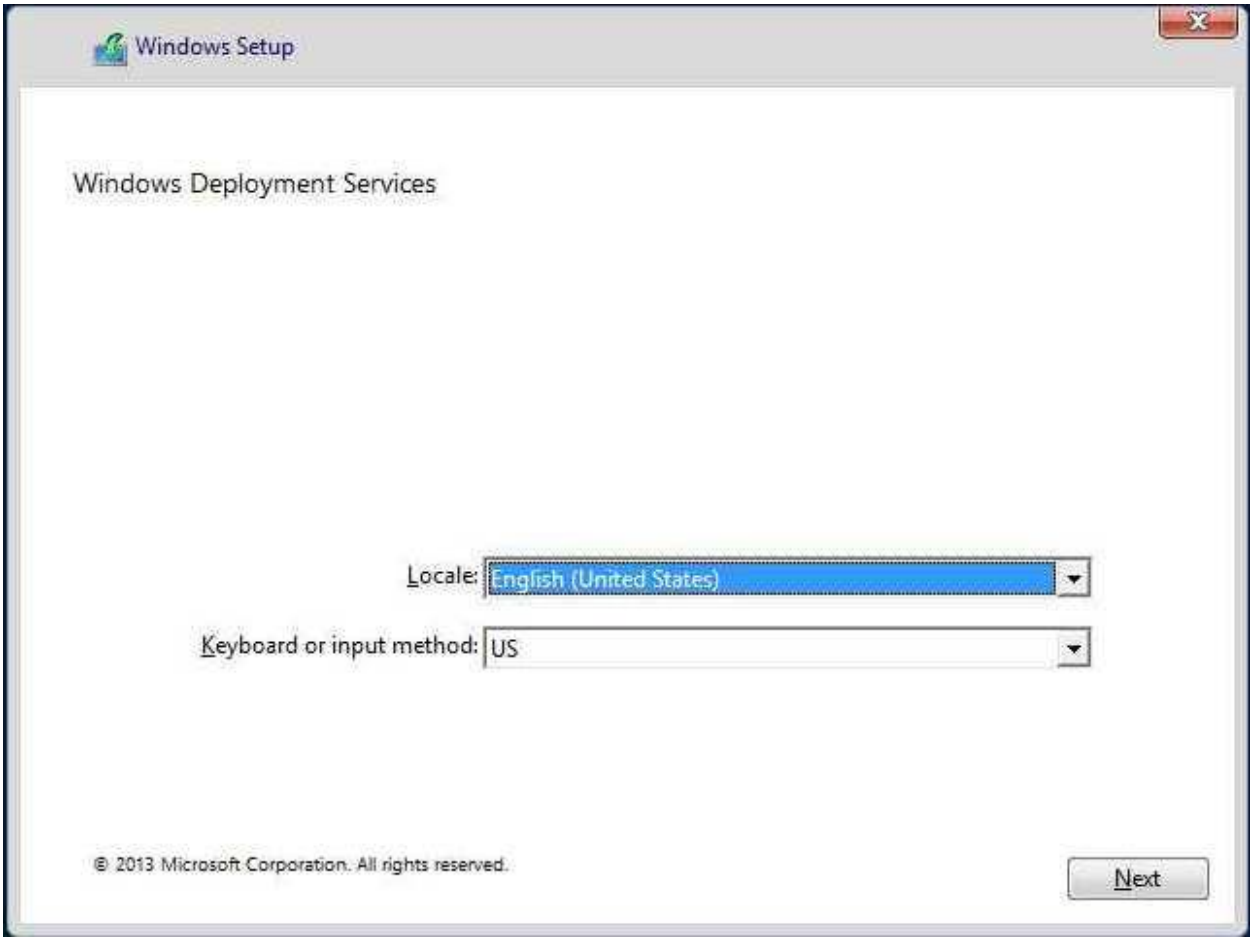
3. Trong cửa sổ máy ảo **20413C-LON-SVR3 – Virtual Machine Connection**, chọn **Start** để khởi động máy ảo.



4. Trong cửa sổ máy ảo **20413C-LON-SVR3**, nhấn phím **F12** khi nhận được thông báo.

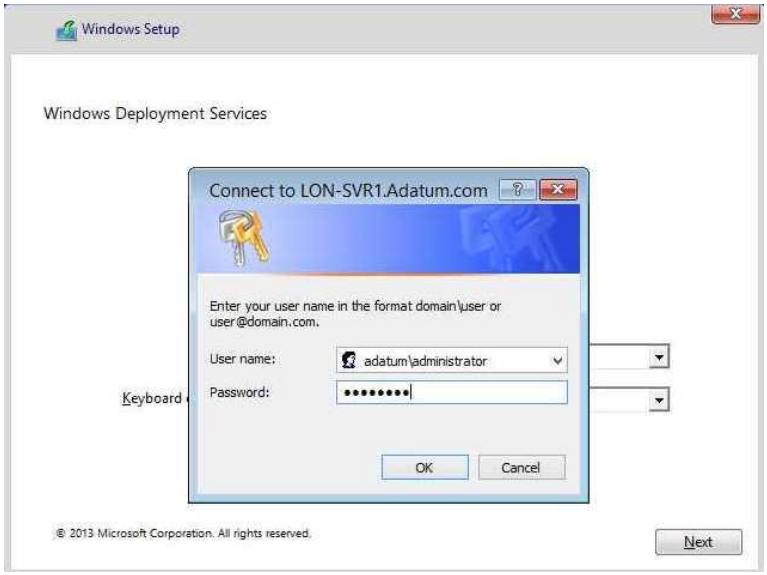


5. Trong cửa sổ **Windows Deployment Services**, chọn **Next**.

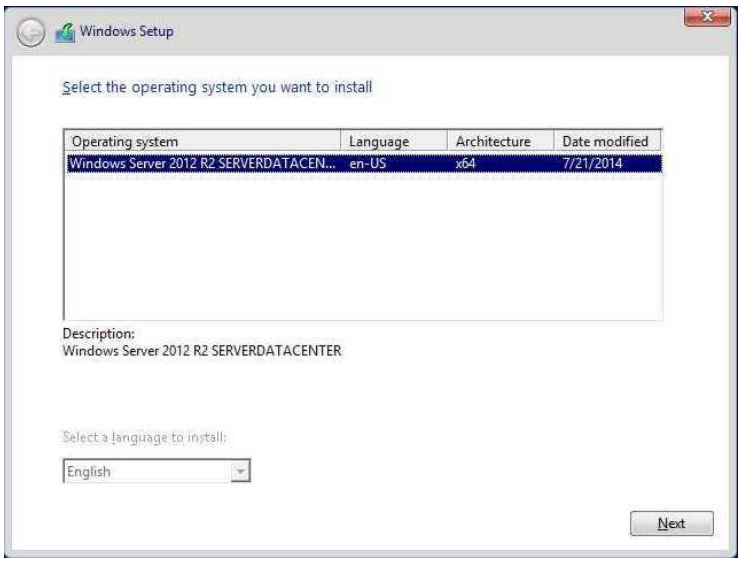


6. Trong hộp thoại chứng thực, nhập username và password bên dưới, và chọn **OK**:

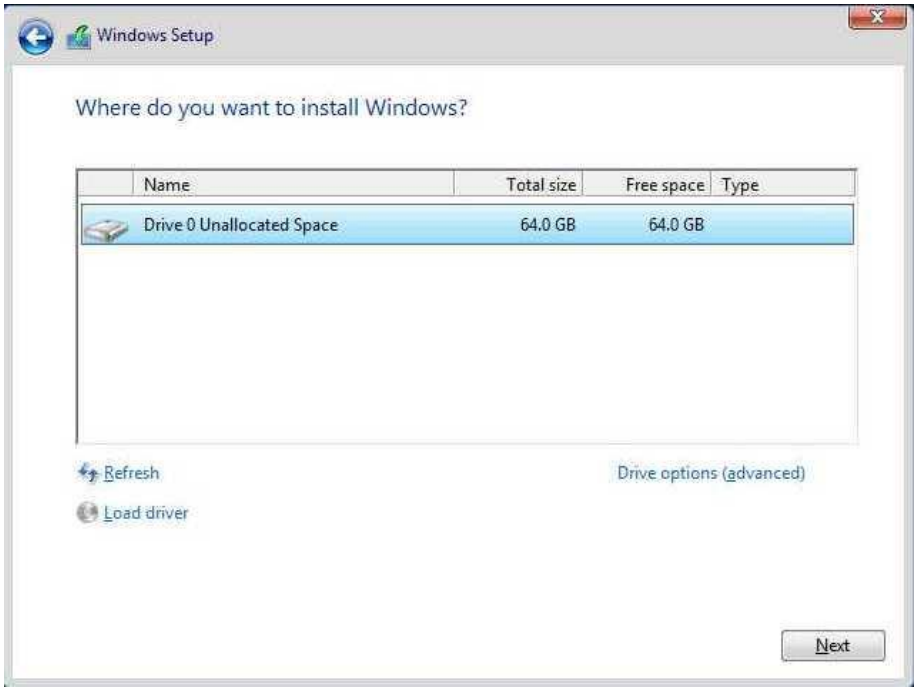
- Username: **Adatum\Administrator**
- Password: **Pa$$w0rd**



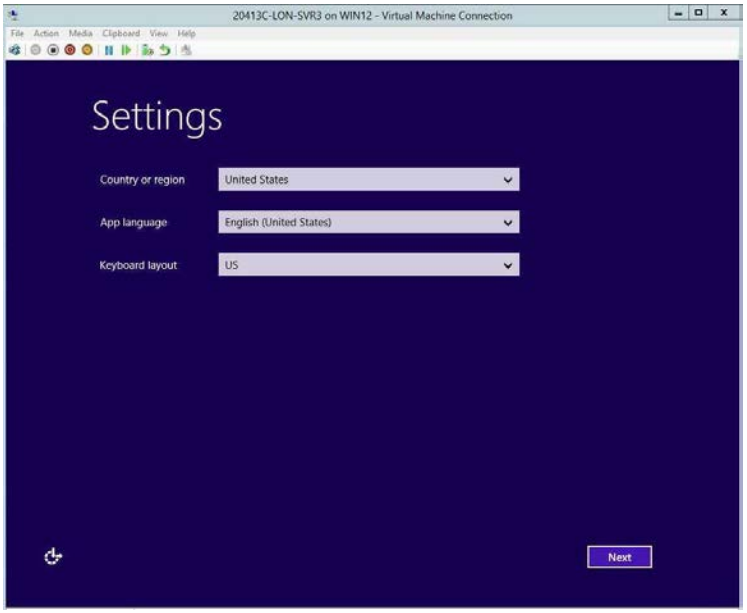
7. Cửa sổ **Select the operating system you want to install**, chọn **Windows Server 2012 R2 SERVERDATACENTER**, chọn **Next**.



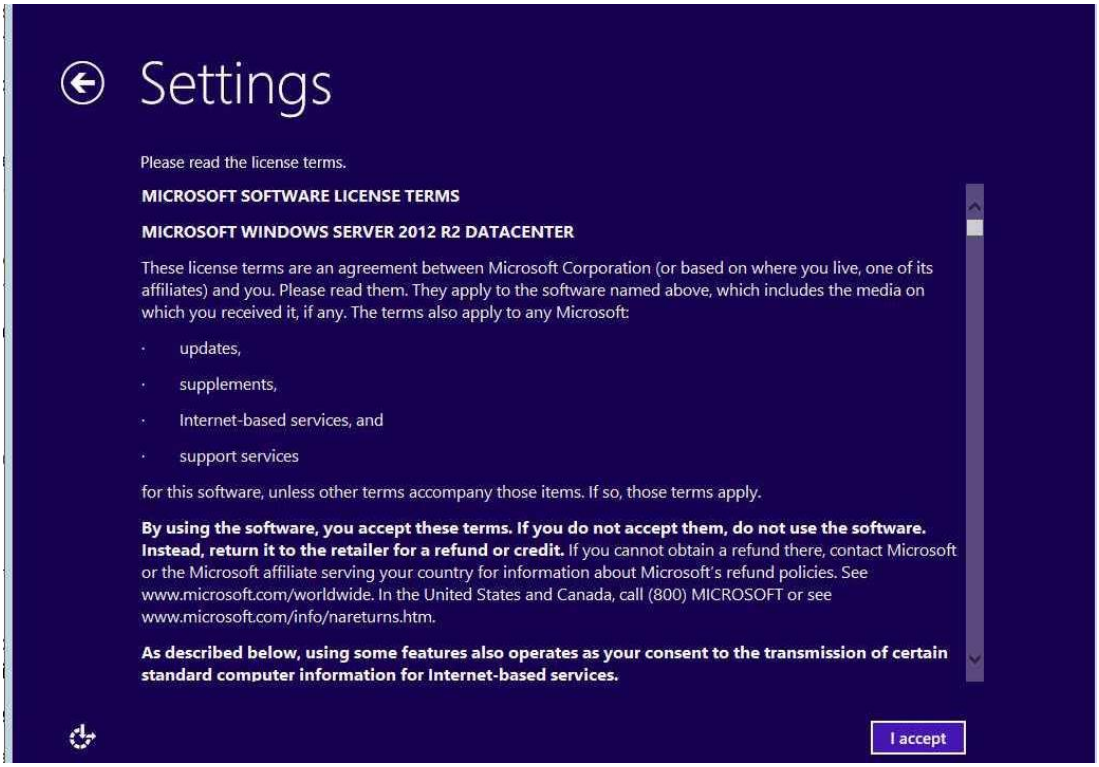
8. Cửa sổ **Where do you want to install Windows**, chọn ổ cứng mặc định. chọn **Next**.



9. Sau quá trình cài đặt, cửa sổ **Settings**, chọn **Next**.

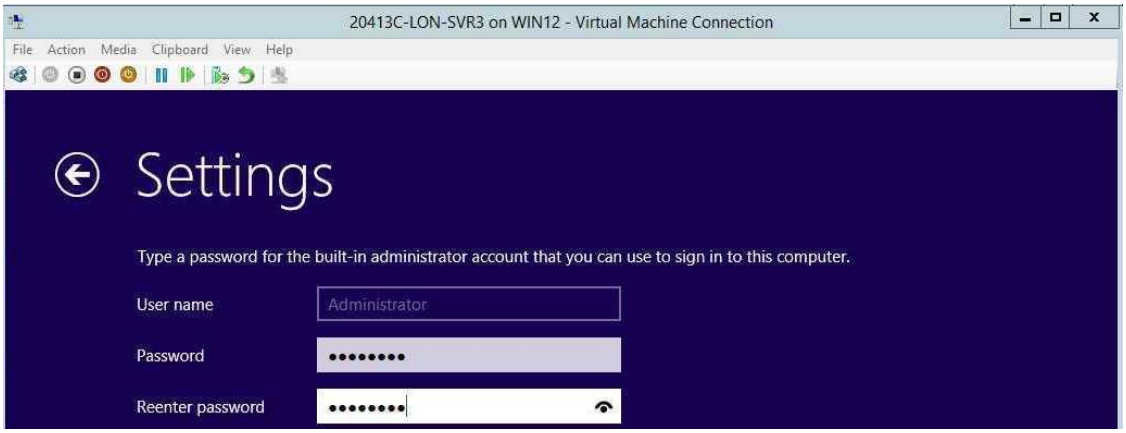


10. Cửa sổ **License**, chọn **I accept**.



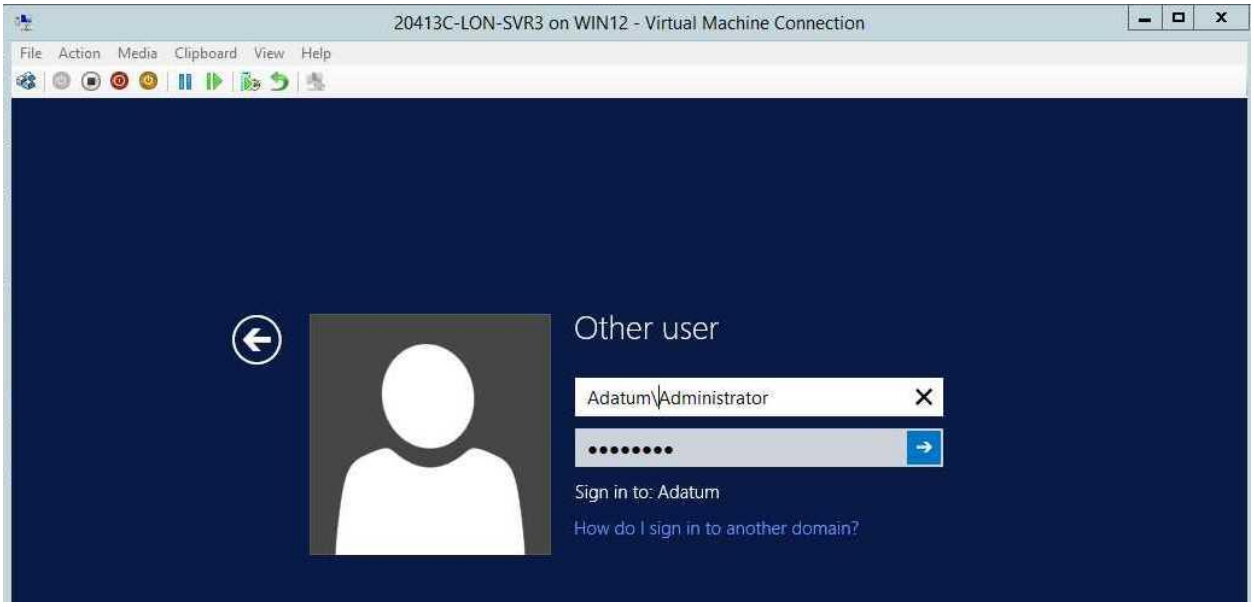
11. Cửa sổ **Region and Language,** chọn **Next**.

12. Cửa sổ **Built-in administrator account**, nhập **Pa$$w0rd** vào cả 2 ô **Password** và **Reenter password,** chọn **Finish**.

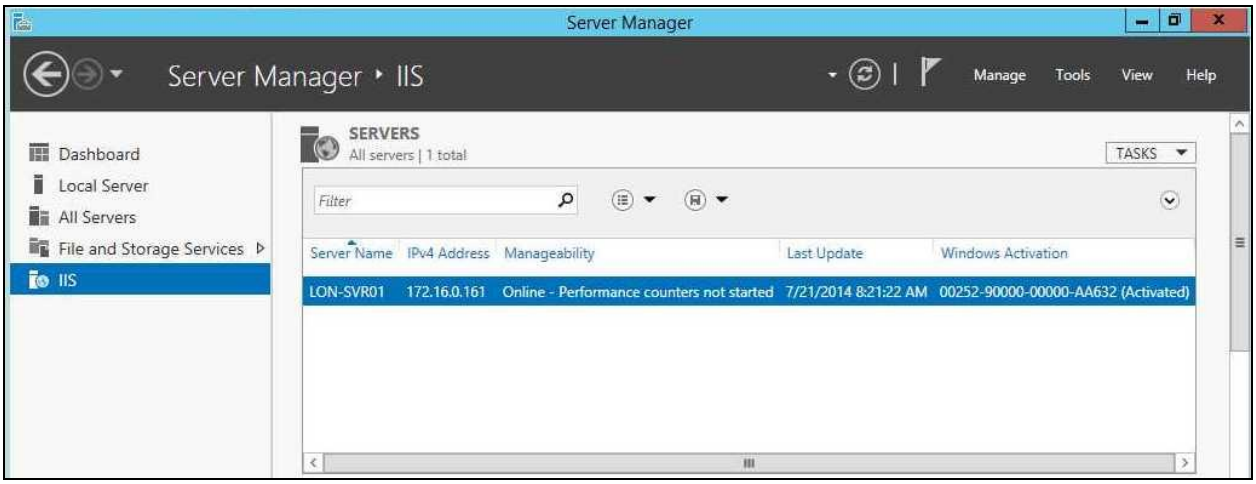


13. Log on vào máy ảo **LON-SVR3** bằng Username và Password sau:

- Username: **Adatum\Administrator**
- Password: **Pa$$w0rd**



14. Trong cửa sổ **Server Manager**, kiểm tra máy ảo **LON-SVR3** đã có cài đặt **Web Server (IIS)** role.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai Windows Server 2012 R2 bằng cách sử dụng tính năng Windows Deployment Services (WDS).

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ Hyper-V Manager.
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Lập lại bước 2 và 3 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-SVR3**.

Bài 3: Thiết kế hệ thống DHCP và giải pháp quản lý địa chỉ IP

I. Mục tiêu:

- Lập kế hoạch triển khai DHCP.
- Lập kế hoạch triển khai IPAM.
- Thực hiện triển khai DHCP và IPAM.

II. Kịch bản:

Trong những năm qua, việc cấu hình và quản lý địa chỉ IP tại công ty A. Datum được thực hiện chủ yếu trên nền tảng cơ bản. Gần đây, A. Datum đã mua một máy chủ mới, và máy chủ này sẽ được sử dụng để phân bổ địa chỉ IP cho hệ thống. DHCP đã được giới thiệu để giúp tự động hóa và quản lý tập trung cho việc phân bổ địa chỉ IP, nhưng dịch vụ cơ sở hạ tầng này chưa được quy hoạch tốt. Điều này đã dẫn đến một số rắc rối trong việc cấu hình và quản lý địa chỉ IP.

Trong quá trình thực hiên kế hoạch nâng cấp lên Windows Server 2012 R2, người quản lý của bộ phận CNTT đã nhìn thấy một cơ hội để triển khai chức năng IPAM trên Windows Server 2012 R2. Sau khi bạn đã chọn một lược đồ địa chỉ thích hợp cho các hệ thống mạng ở công ty Contoso, bạn phải lập kế hoạch tốt nhất cho viêc triển khai chức năng IPAM để quản lý IP trong hệ thống của bạn. Bạn phải xem xét nên chọn mô hình tập trung hoặc cấu trúc phân phối, những gì có thể tích hợp với IPAM (DNS hoặc DHCP), và cách tốt nhất để bảo mật IPAM.

Sau khi lựa chọn một cấu hình IPAM phù hợp, bạn cũng phải xem xét làm thế nào để phân bổ địa chỉ IP cho các máy Server và máy Client bằng cách sử dụng DHCP. Điều quan trọng là các dịch vụ DHCP phải có tính sẵn sàng cao.

III. Yêu cầu tổng quan:

- Lập kế hoạch triển khai DHCP cho Contoso để hỗ trợ các mục tiêu sau đây:

- Tất cả các máy clients và servers phải được cung cấp một cấu hình IPv4 tự động.
- Phải đảm bảo hệ thống DHCP của bạn có khả năng sẵn sàng cao.

- Lập kế hoạch triển khai IPAM ở A. Datum để hỗ trợ các mục tiêu sau đây:

- Đầu tiên, bạn phải triển khai IPAM cho A. Datum.
- Sau đó, bạn sẽ triển khai IPAM cho Contoso và Trey Research trong tương lai gần.

IV. Các thông tin liên quan:

- Các thiết bị Router có bật chức năng DHCP.
- Hiện nay không có yêu cầu cung cấp IPv6.
- Bạn phải triển khai càng ít DHCP Server càng tốt.
- Các Network Policy Servers được triển khai tại A. Datum để hỗ trợ kết nối (VPN).
- Windows Server 2012 R2 và Windows Server 2008 R2 được triển khai tại A. Datum. Tất cả Domain Controller được cài đặt Windows Server 2012 R2.
- Trey Research là 1 forest riêng biệt sử dụng Windows Server 2008 R2.
- Hiện nay, Contoso đang chạy UNIX. Kế hoạch đưa ra để triển khai Windows Server 2012 tại Contoso.

V. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1** **20413C-LON-SVR2**
User name	Adatum\Administrator
Password	Pa$$w0rd

VI. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.

2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.

3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.

4. Logon vào máy ảo với thông tin sau:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**
5. Thực hiên lại từ bước 2 đến 4 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-SVR2.**

VII. Thực hành:

Thời gian thực hành: 75 phút

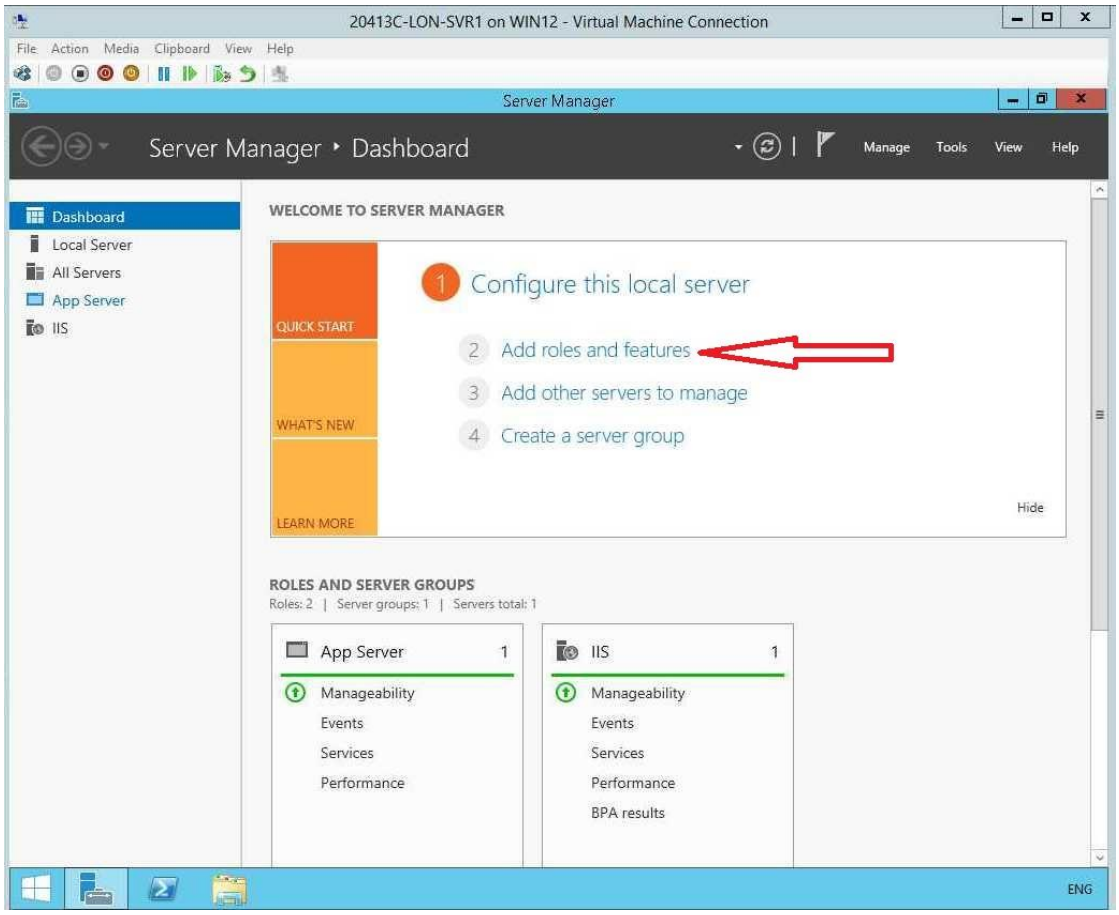
Bài thực hành bao gồm các bước:

1. Cài đặt DHCP Server role.
2. Cấu hình DHCP failover relationship.
3. Cài đặt IPAM.
4. Cấu hình Group Policy Object (GPO).
5. Cấu hình IP management server discovery.
6. Cấu hình chức năng quản lý Server.
7. Cấu hình và kiểm tra DHCP scope với IPAM.
8. Cấu hình IP address blocks, record IP addresses, và tạo DHCP reservations.

Bước 1. Cài đặt DHCP Server role.

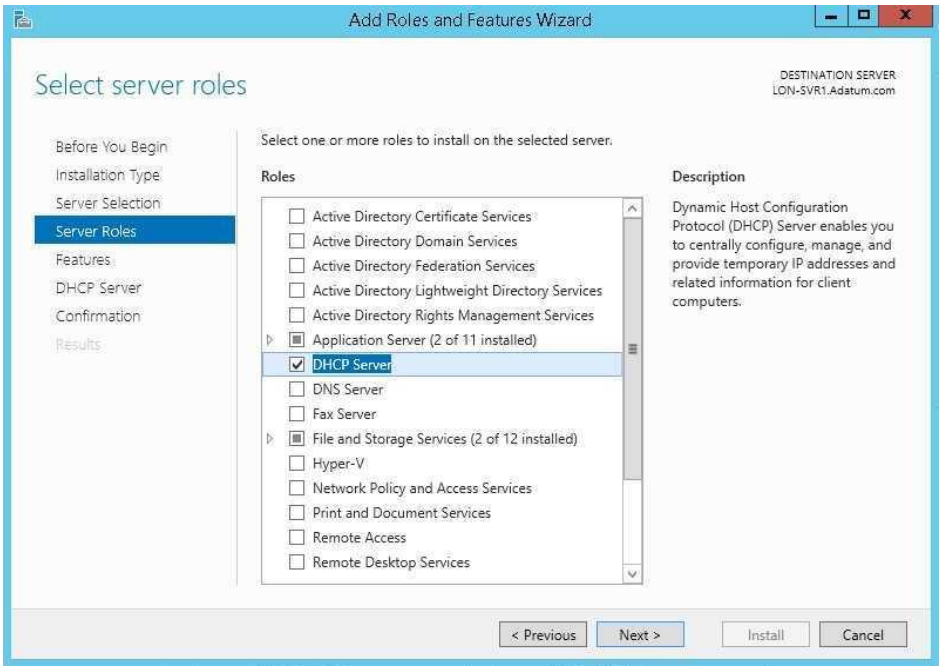
1. Trên máy **LON-SVR1,** mở công cụ **Server Manager.**

2. Trong cửa sổ Server Manager, chọn **Add roles and features**.

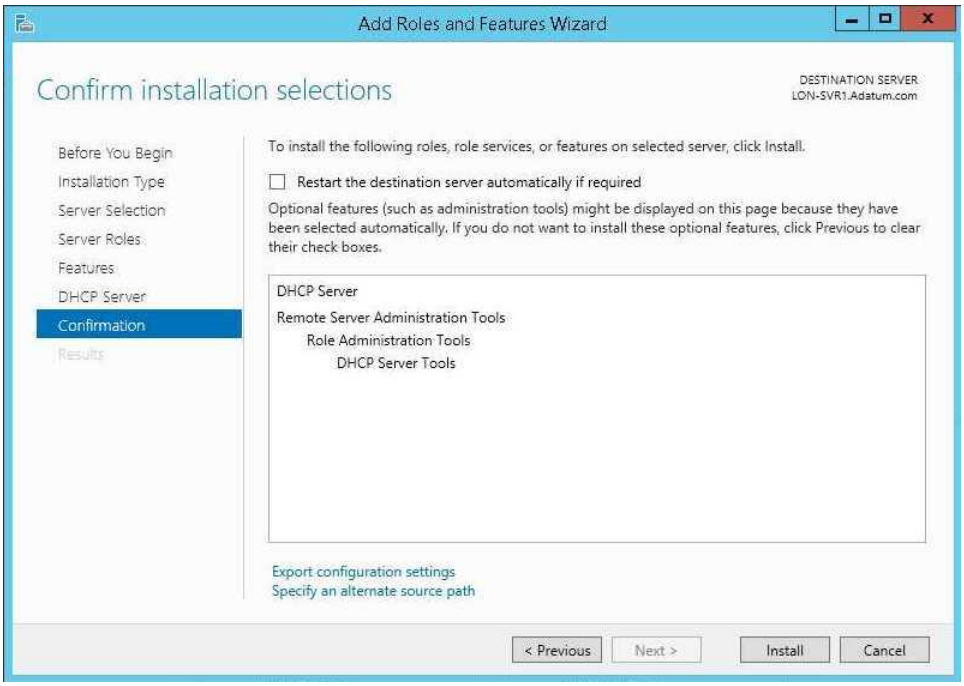


3. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.

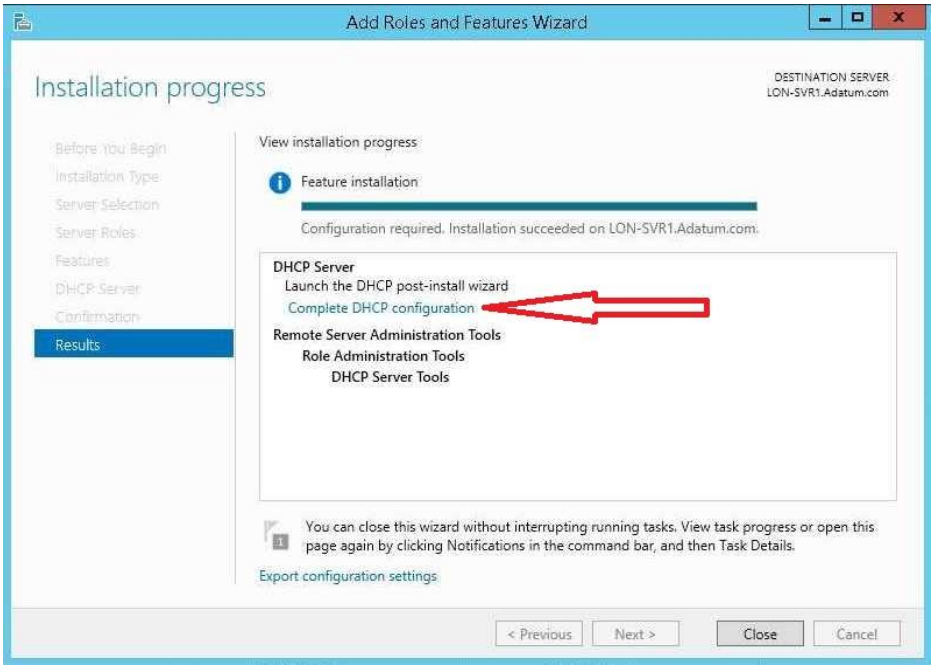
4. Trong cửa sổ **Select server roles**, chọn **DHCP Server**, chọn **Add Features**.



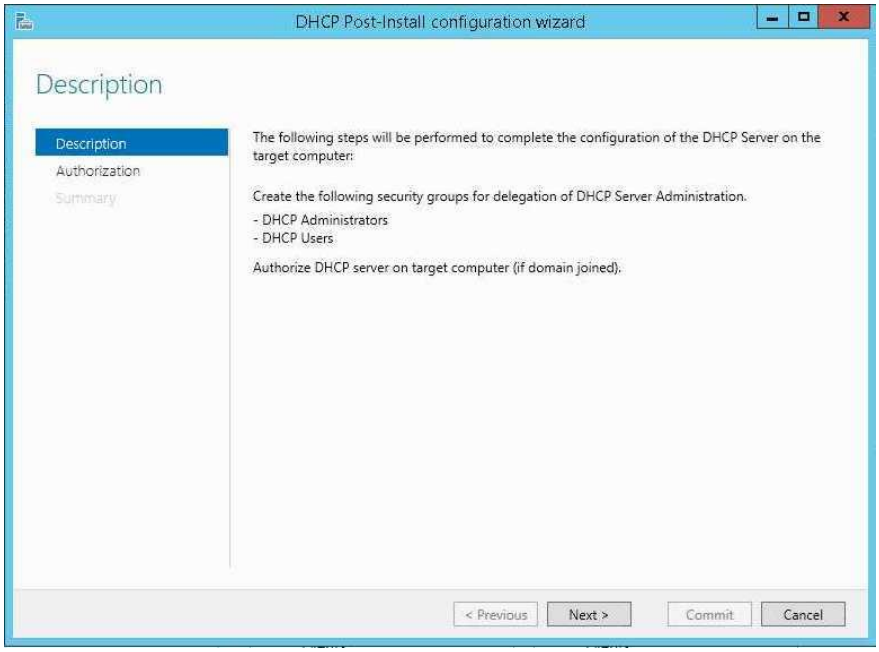
5. Sau đó chọn **Next** 3 lần, và chọn **Install**.



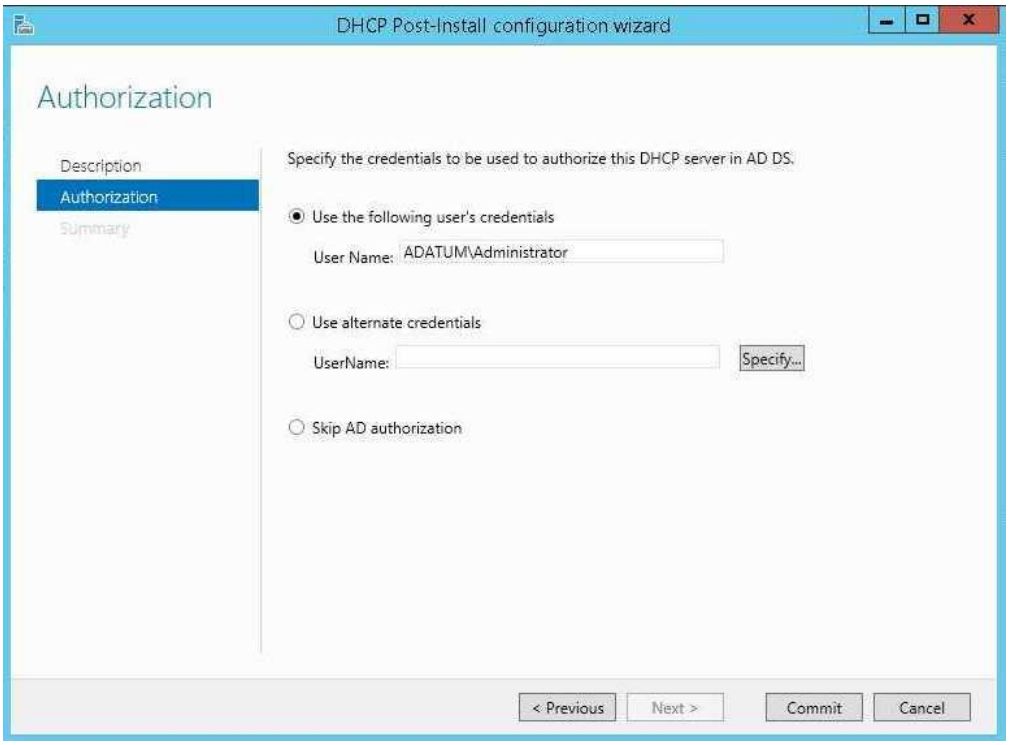
6. Sau khi cài đặt thành công, trong cửa sổ **Installation progress**, chọn dòng **Complete DHCP configuration**.



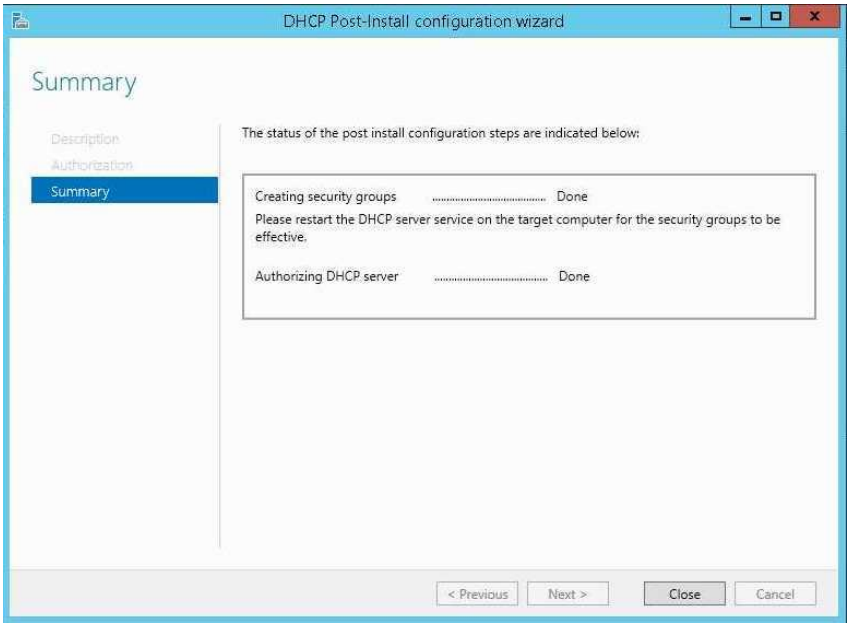
7. Cửa sổ **DHCP Post-Install Configuration Wizard**, chọn **Next**.



8. Cửa sổ **Authorization**, chọn **Commit**.



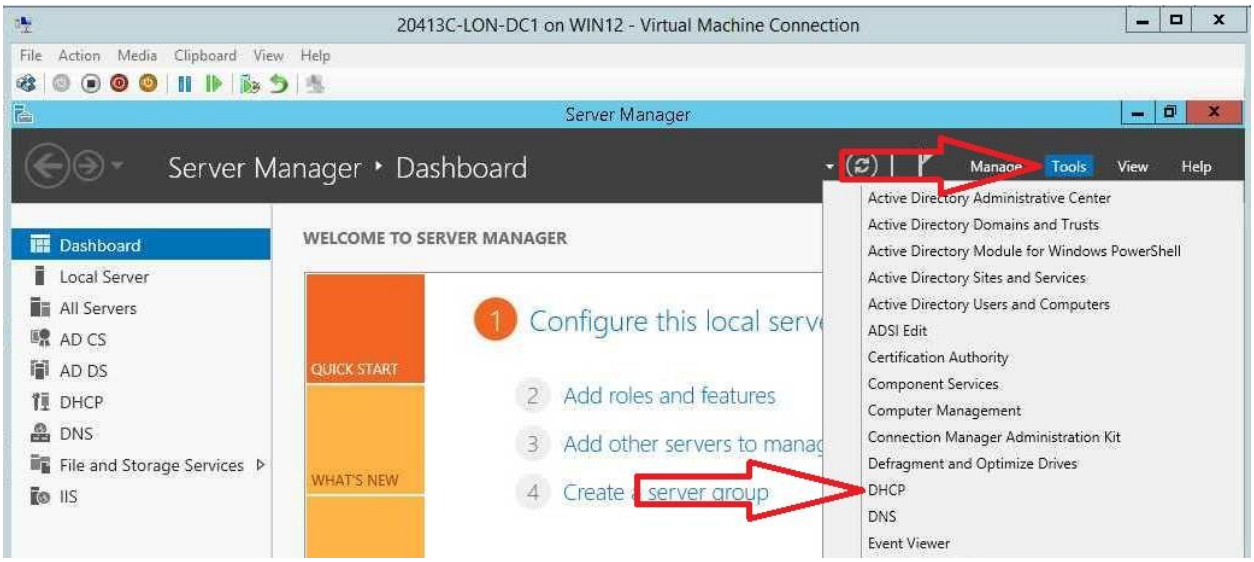
9. Cửa sổ **Summary**, chọn **Close**.



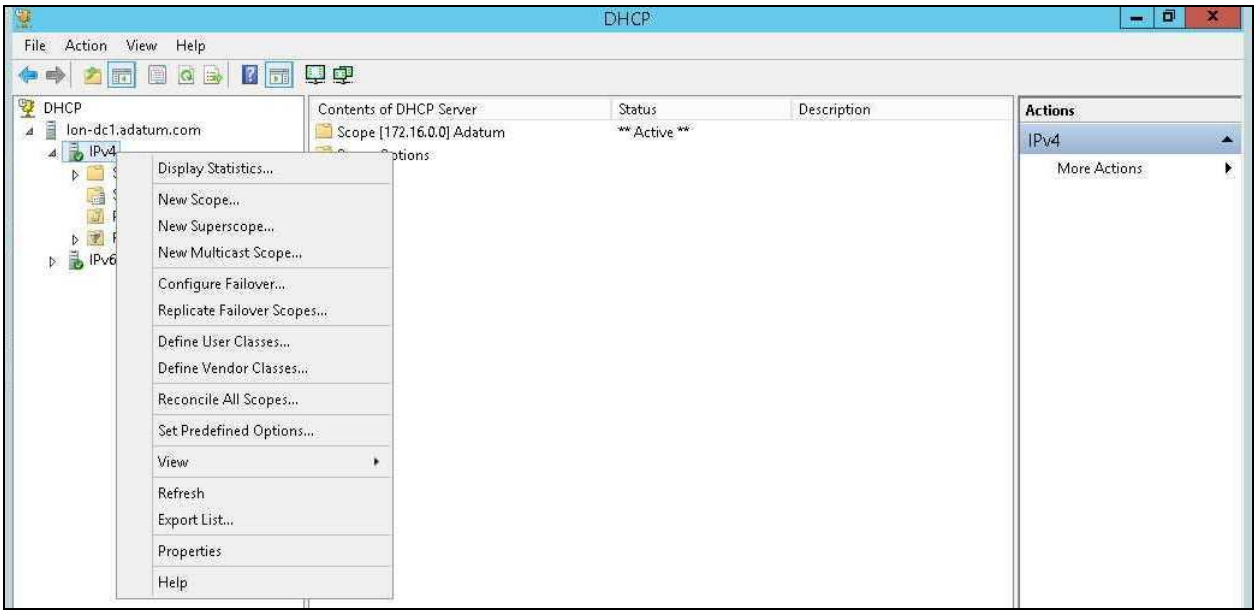
Bước 2. Cấu hình DHCP failover relationship.

1. Qua máy **LON-DC1.**

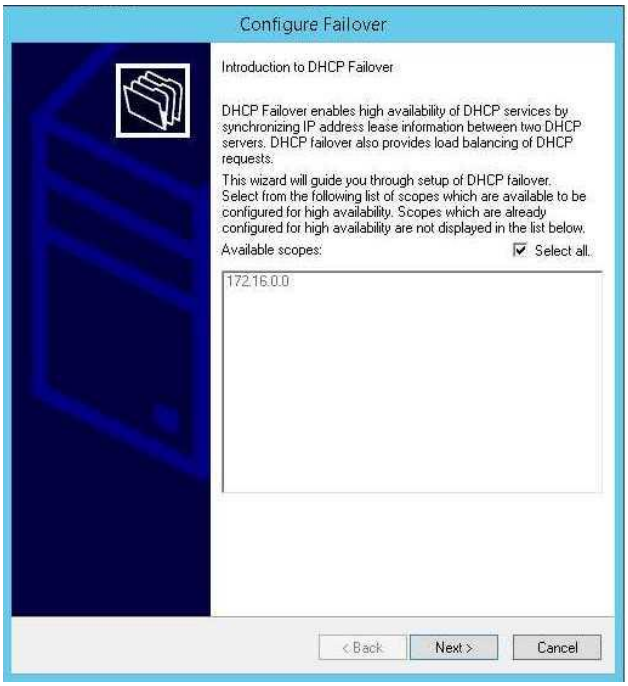
2. Mở công cụ **Server Manager**, bung mục **Tools**, chọn **DHCP**.



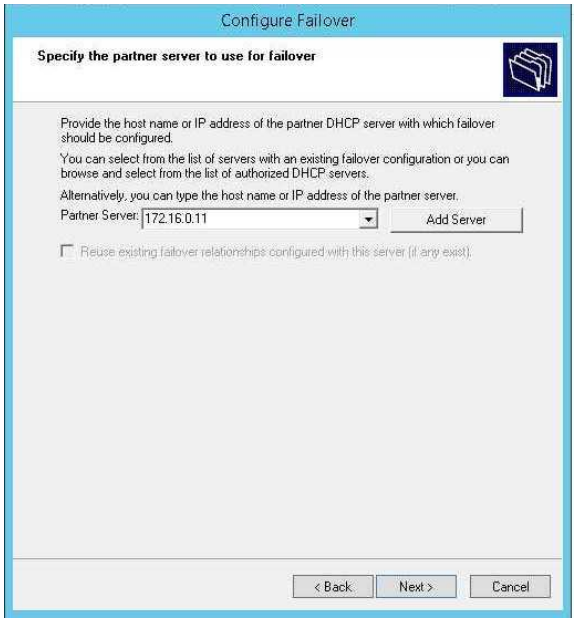
3. Trong cửa sổ **DHCP**, bung **lon-dc1.adatum.com**, chọn và nhấn chuột phải **IPv4**, chọn **Configure Failover**.



4. Cửa sổ **Configuration Failover Wizard**, chọn **Next**.

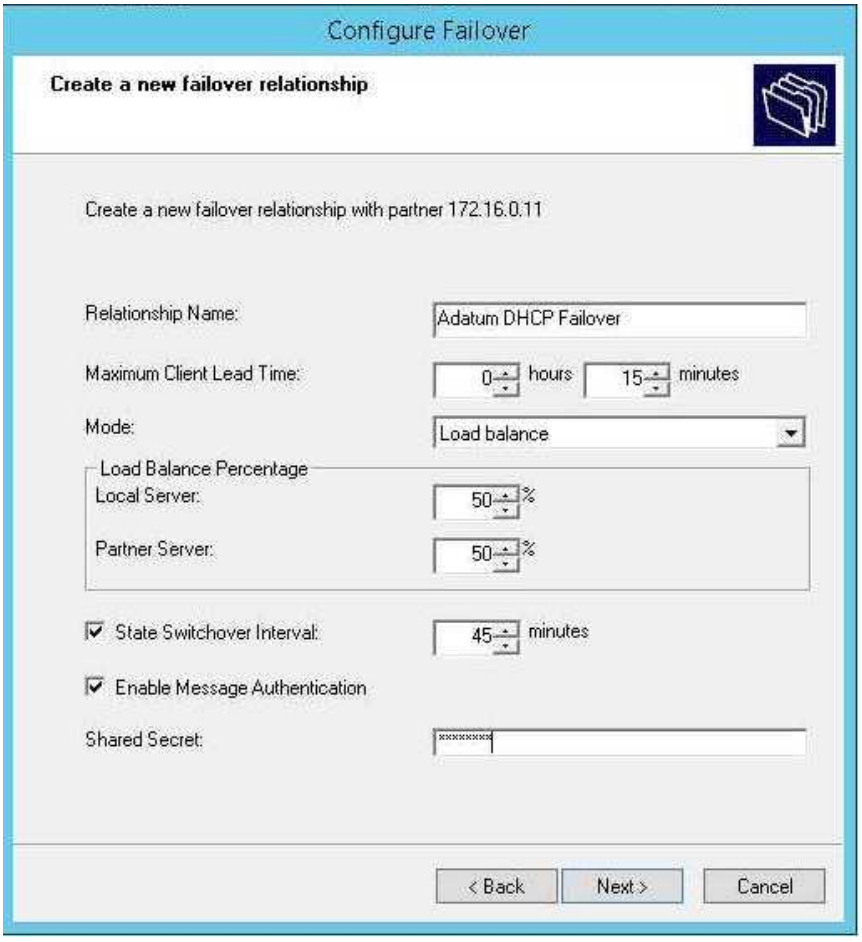


5. Cửa sổ **Specify the partner server to use for failover**, nhập **172.16.0.11** vào ô **Partner Server,** chọn **Next**.



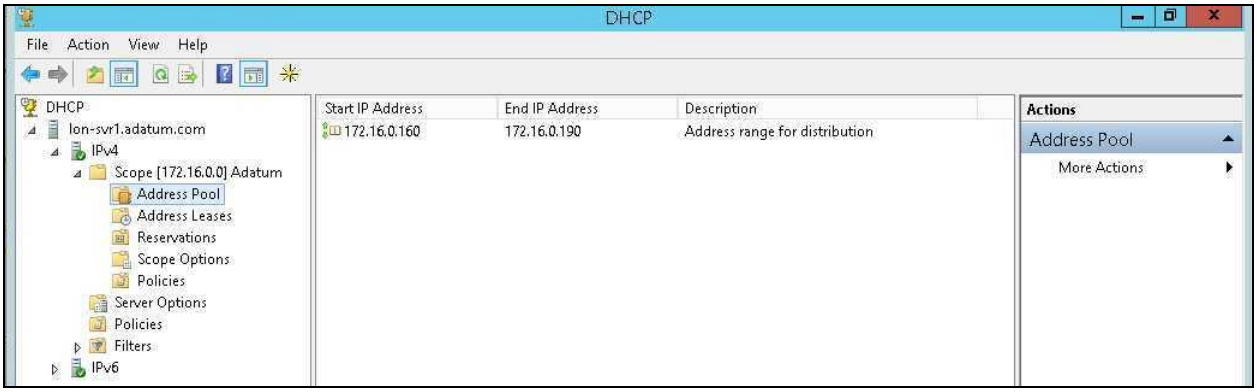
6. Trong cửa sổ **Create a new failover relationship**, nhập thông tin như sau, và sau đó chọn **Next**.

- Relationship Name: **Adatum DHCP Failover**
- Maximum Client Lead Time: **0 hours, 15 minutes**
- Mode: **Load balance**.
- Load Balance Percentage: **50%**.
- Đánh dấu chọn **Enable Message Authentication**
- Shared Secret: **Pa$$w0rd**

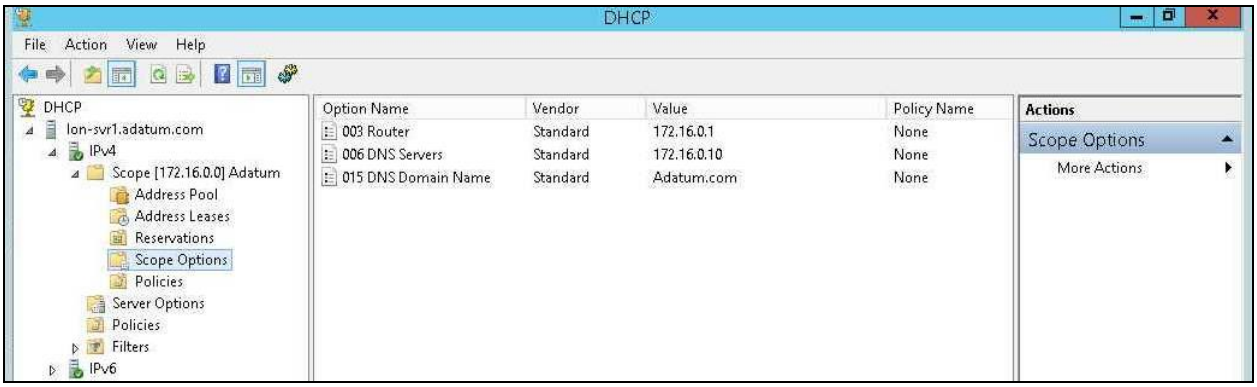


7. Cửa sổ **Configure Failover**, chọn **Finish**, và chọn **Close**.

8. Qua máy **LON-SVR1**, mở công cụ **DHCP**, chú ý mục **IPv4** đang ở trạng thái **active**. Bung **IPv4**, bung **Scope**. chọn **Address Pool**, chú ý cấu hình của address pool.



9. Chọn **Scope Options**, chú ý cấu hình của scope options.

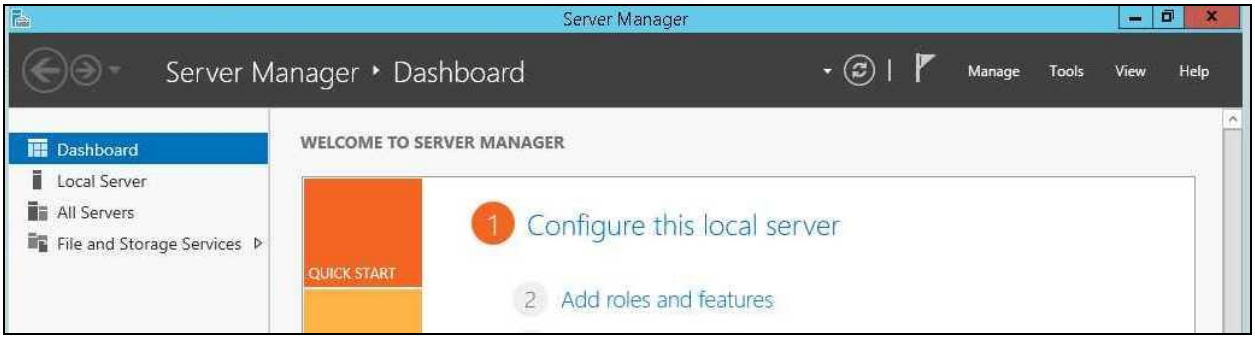


10. Tắt công cụ **DHCP** của máy **LON-SVR1** và **LON-DC1.**

Bước 3. Cài đặt IPAM.

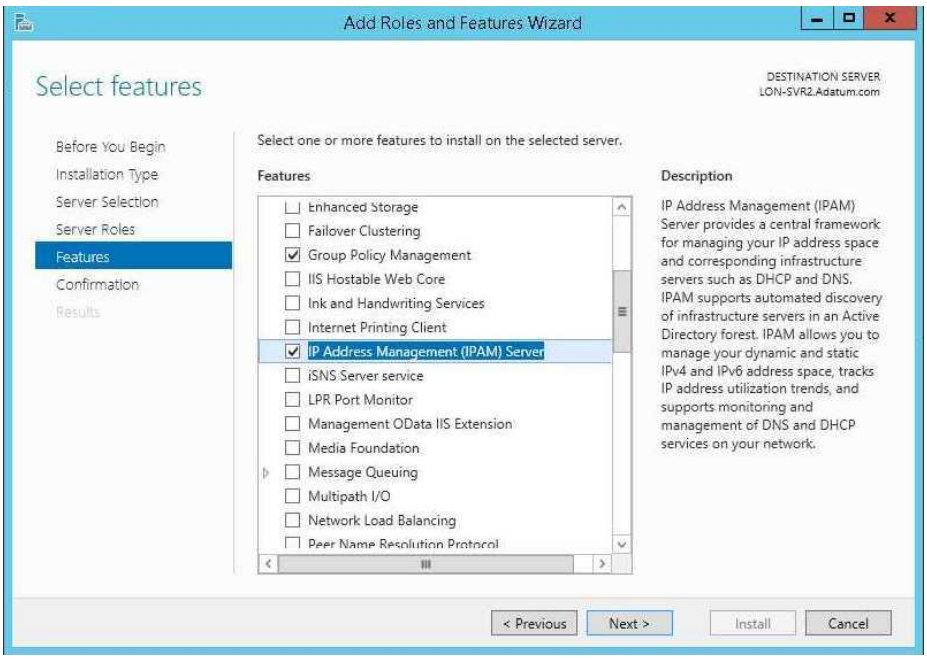
1. Qua máy **LON-SVR2**, logon **Adatum\Administrator** với password là **Pa$$w0rd**.

2. Trong **Server Manager**, chọn **Add roles and features**.

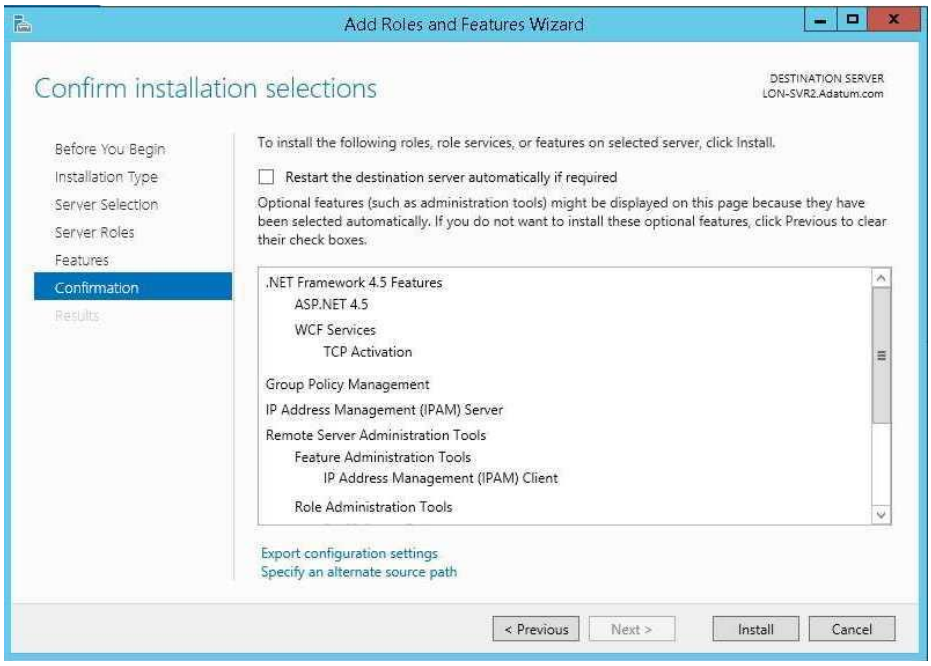


3. Trong cửa sổ **Add Roles and Features Wizard**, chọn **Next** 4 lần.

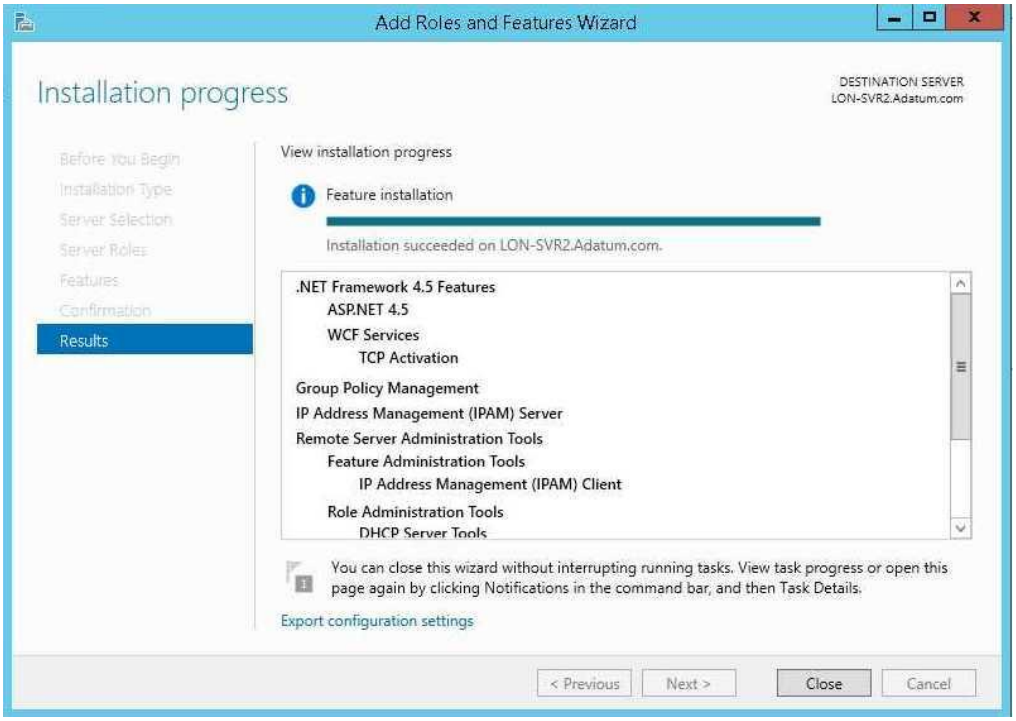
4. Cửa sổ **Select features**, đánh dấu chọn **IP Address Management (IPAM) Server**. Trong hộp thoại **Add features that are required for IP Address Management (IPAM) Server**, chọn **Add Features**, chọn **Next**.



5. Cửa sổ **Confirm installation selections,** chọn **Install**.

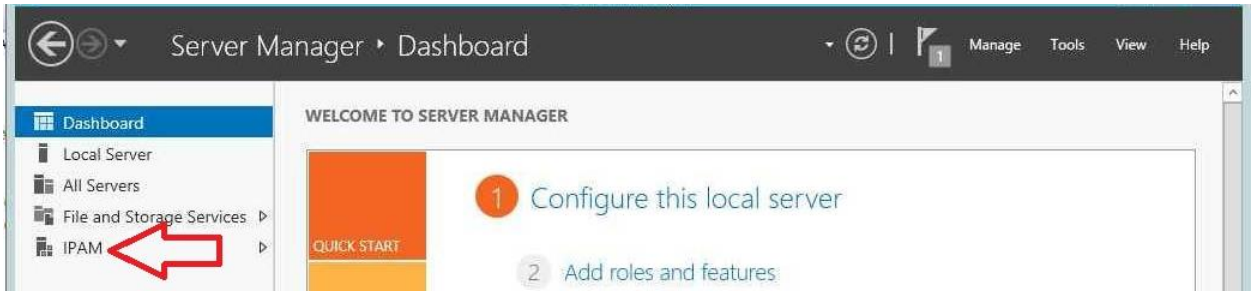


6. Sau khi cài đặt thành công, chọn **Close**



Bước 4. Cấu hình Group Policy Object (GPO).

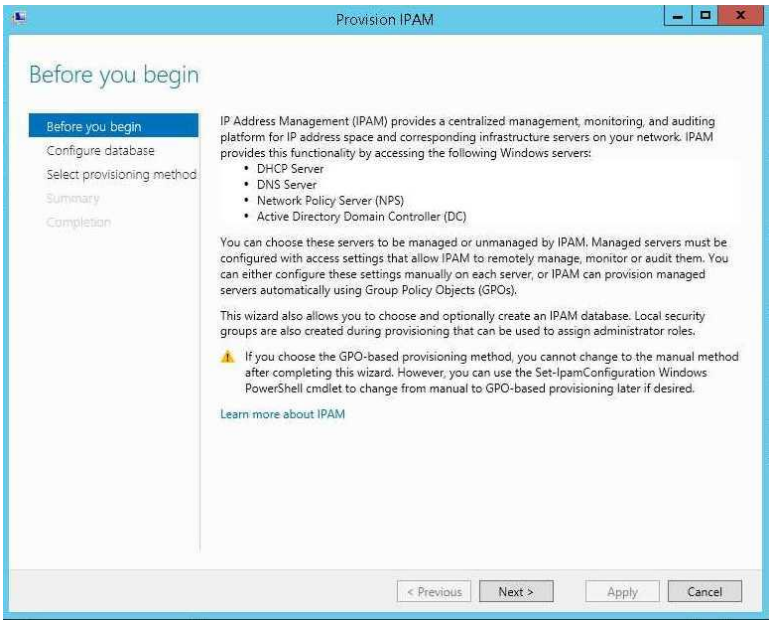
1. Trong cửa sổ Server Manage, chọn **IPAM**.



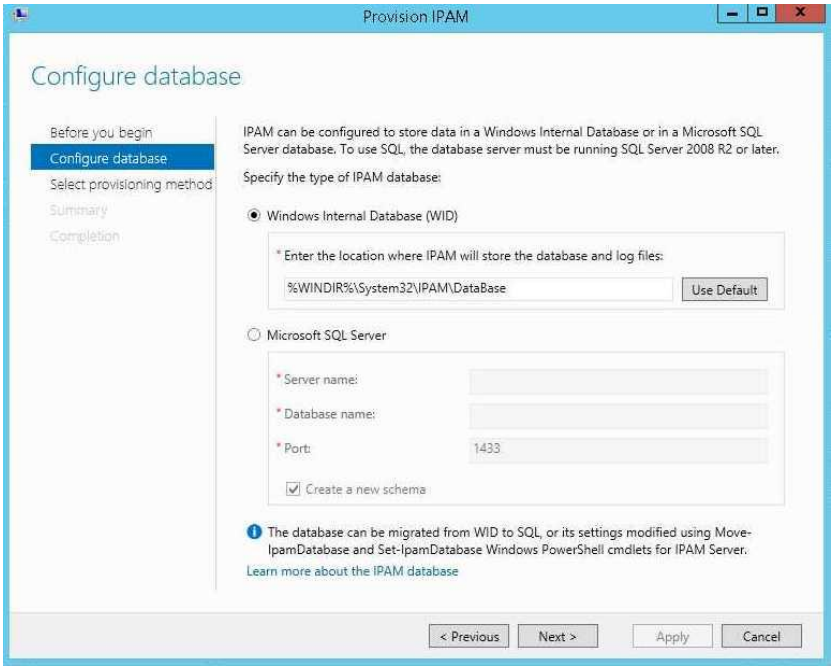
2. Chọn **Provision the IPAM server**.



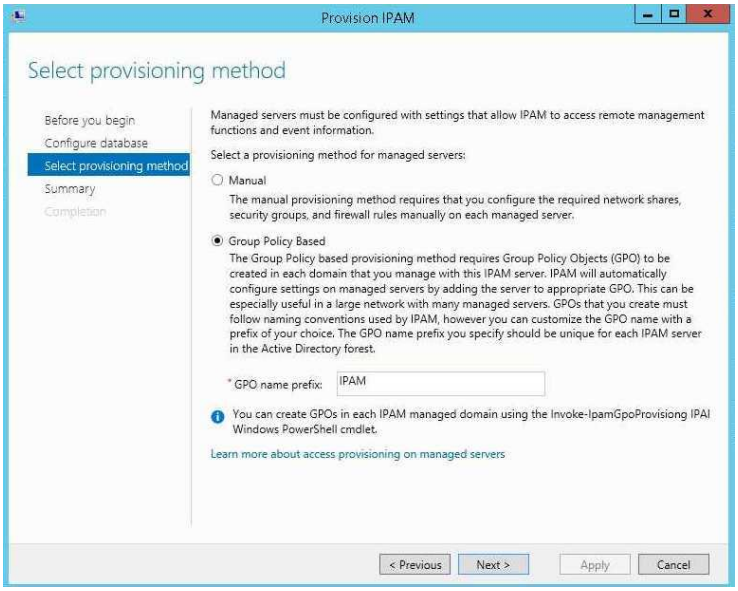
3. Trong cửa sổ **Before you begin**, chọn **Next**.



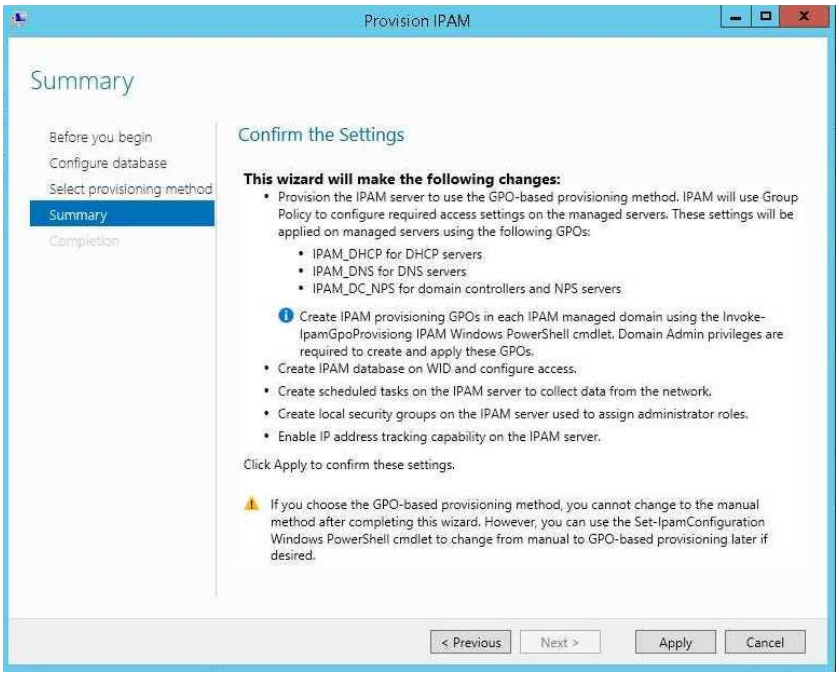
4. Cửa sổ **Configure database**, đảm bảo chọn **Windows Internal Database (WID)**, chọn **Next**.



5. Cửa sổ **Select provisioning method**, đảm bảo chọn **Group Policy Based**, nhập **IPAM** vào ô **GPO name prefix**, chọn **Next**.

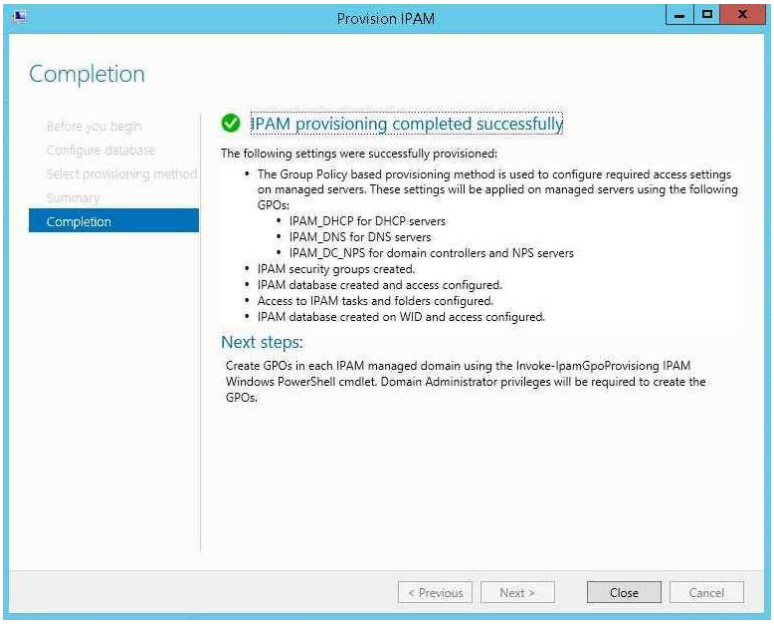


6. Cửa sổ **Summary**, chọn **Apply**.



Chú ý: Cấu hình sẽ hoàn tất trong khoảng 5 phút.

7. Cửa sổ **Completion**, chọn **Close**.

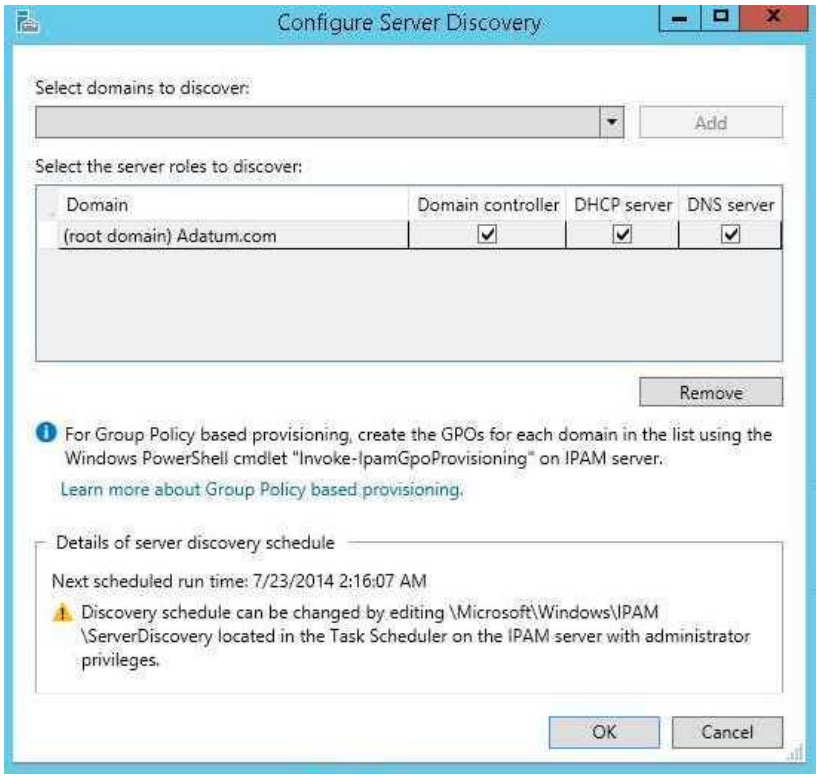


Bước 5. Cấu hình IP management server discovery.

1. Trong **IPAM Overview**, chọn **Configure server discovery**.



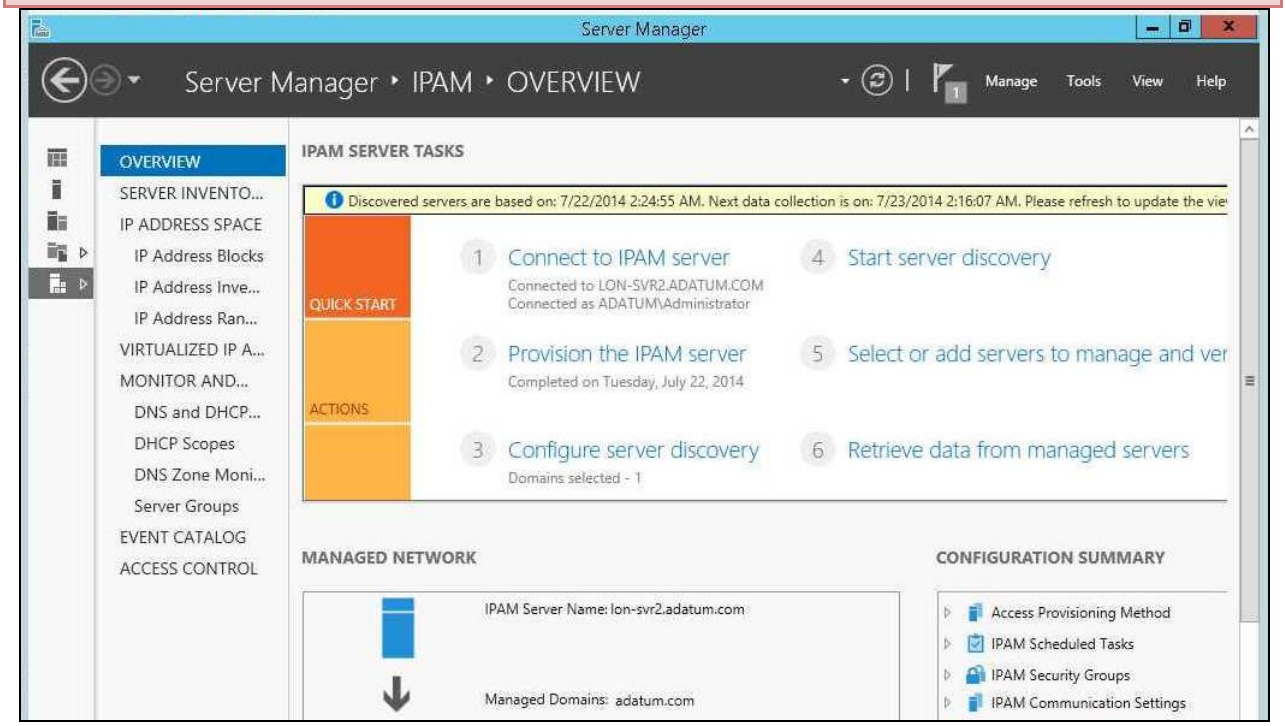
2. Trong hộp thoại **Configure Server Discovery**, chọn **Add** để add domain **Adatum.com** vào danh sách **Select the server roles to discover**, chọn **OK**.



3. Trong **IPAM Overview**, chọn **Start server discovery**.

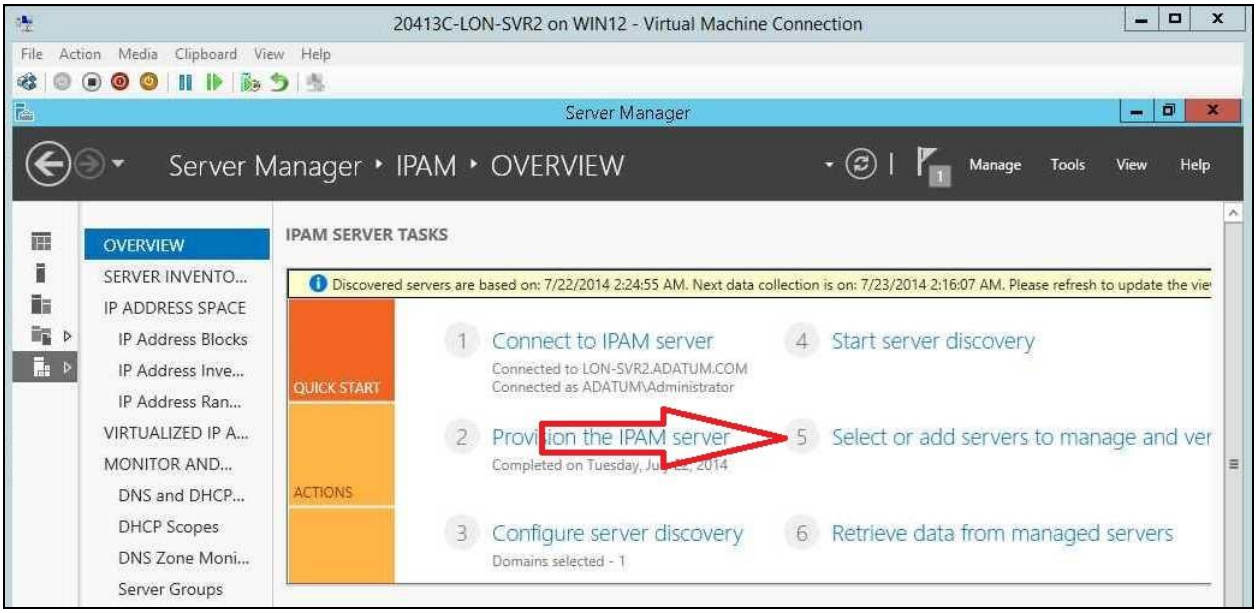


Chú ý: Quá trình Discovery chạy khoảng từ 5 đến 10 phút. Thanh màu vàng sẽ cho biết quá trình Discovery hoàn tất.

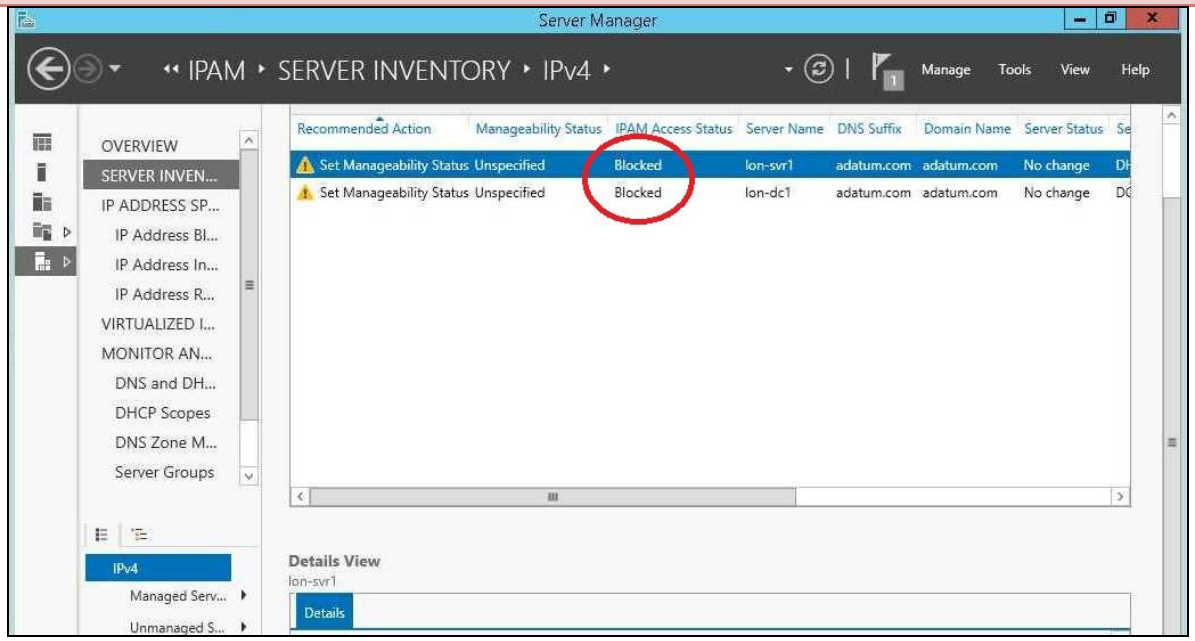


Bước 6. Cấu hình chức năng quản lý Server.

1. Trong cửa sổ **IPAM Overview**, chọn **Select or add servers to manage and verify IPAM access**.



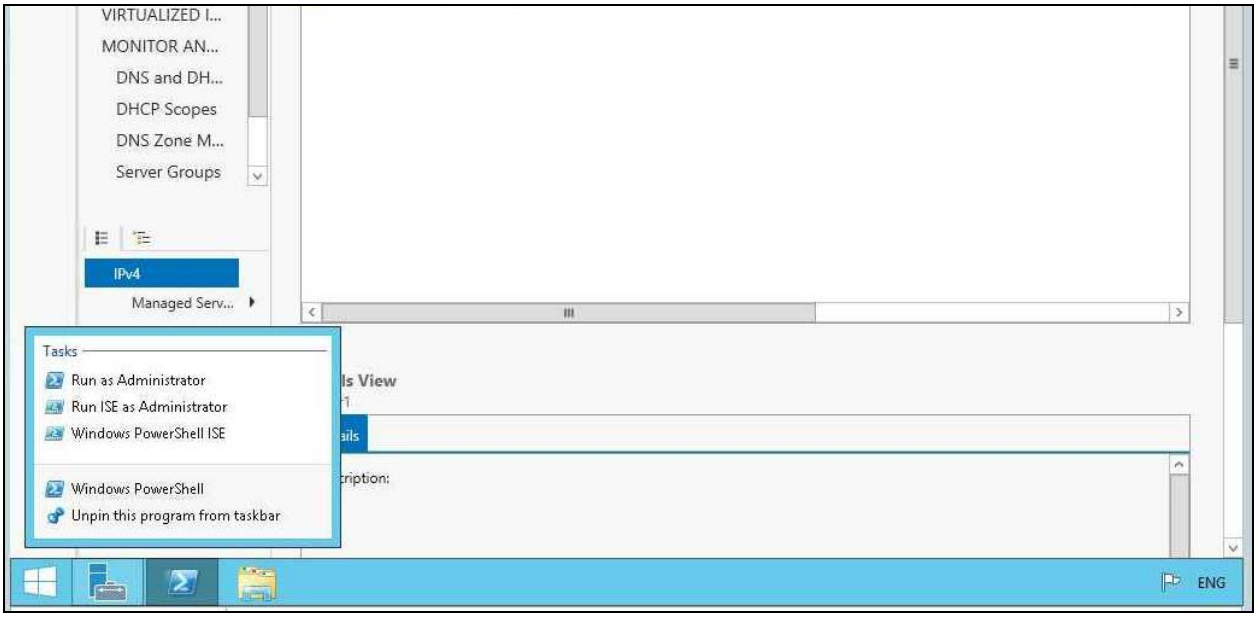
Chú ý: Trạng thái IPAM Access của cả 2 server là Blocked.



2. Kéo thanh trượt qua mục **Details**, kiểm tra status report.

Chú ý: IPAM Server chưa được phép quản lý **LON-DC1** và **LON-SVR1** thông qua Group Policy.

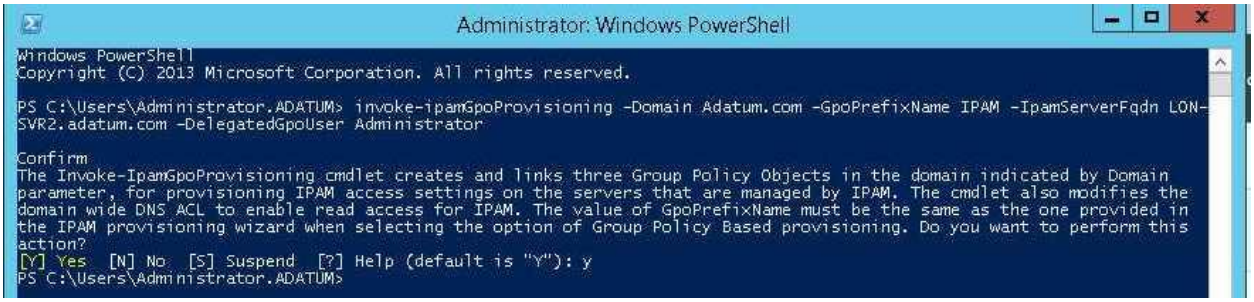
3. Trên thanh taskbar, nhấn chuột phải lên biểu tượng **Windows PowerShel**, chọn **Run as Administrator**.



4. Trong cửa sổ Windows PowerShell® prompt, gõ lệnh:

Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn LON-SVR2.adatum.com –DelegatedGpoUser Administrator

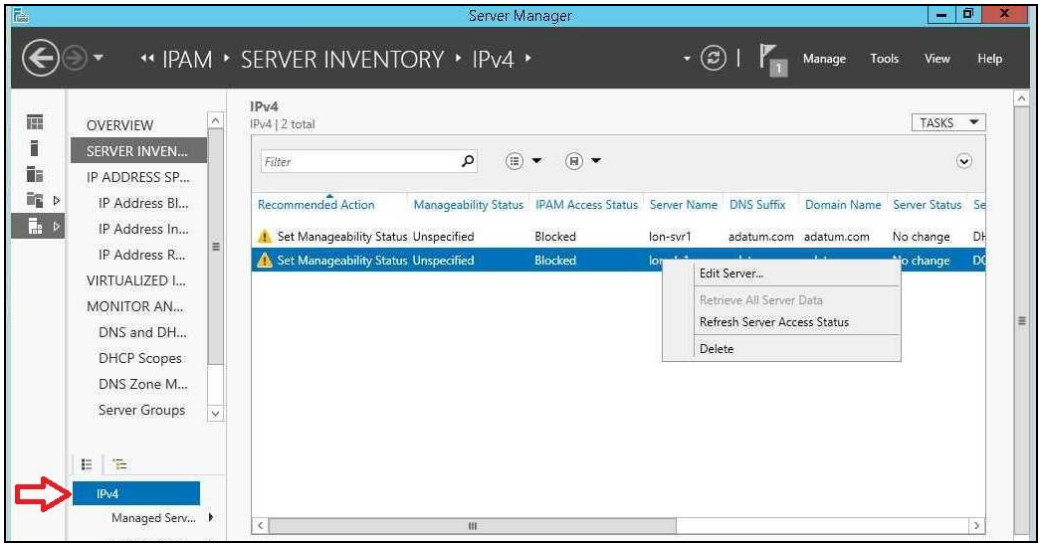
Khi nhận yêu cầu xác nhận, nhập **Y**, chọn **Enter**.



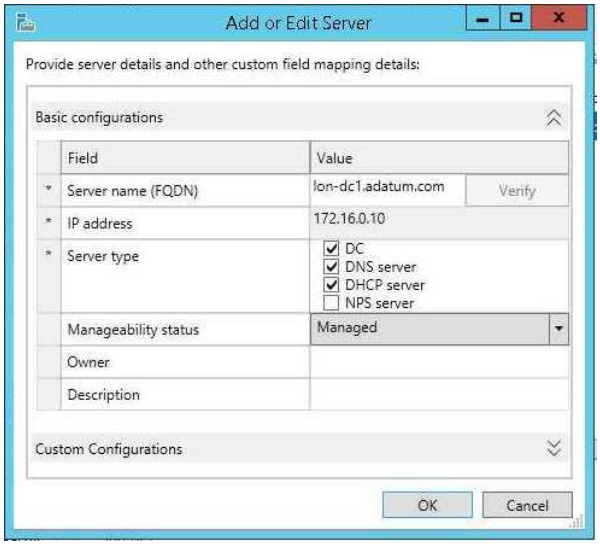
Chú ý: Lệnh này có thể hoàn thành trong vòng 5 phút hoặc hơn.

5. Tắt Windows PowerShell.

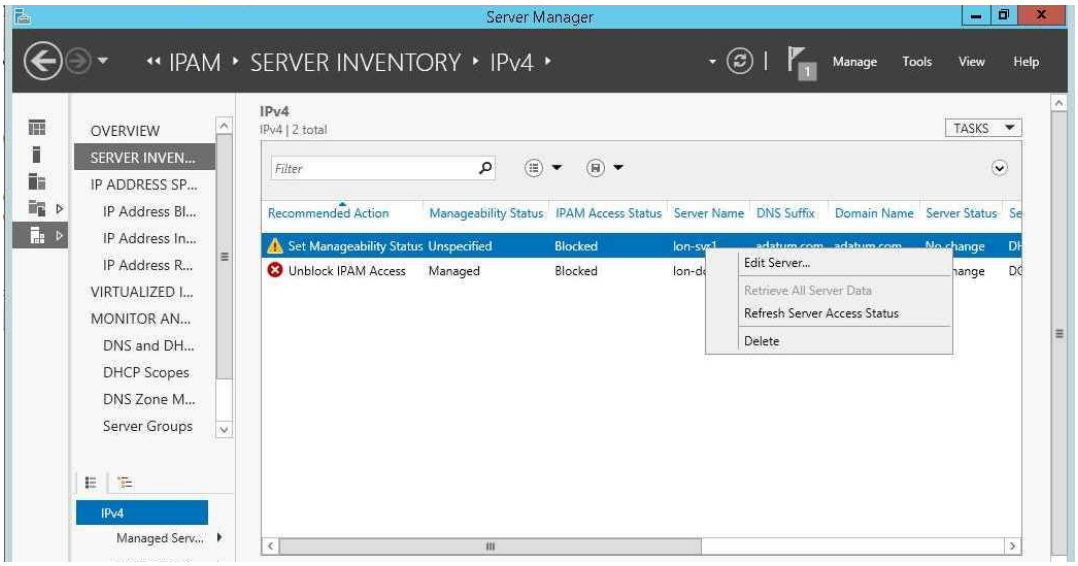
6. Quay lại cửa sổ **Server Manager**, trong cửa sổ **IPv4**, nhấn chuột phải lên dòng **lon-dc1**, chọn **Edit Server**.



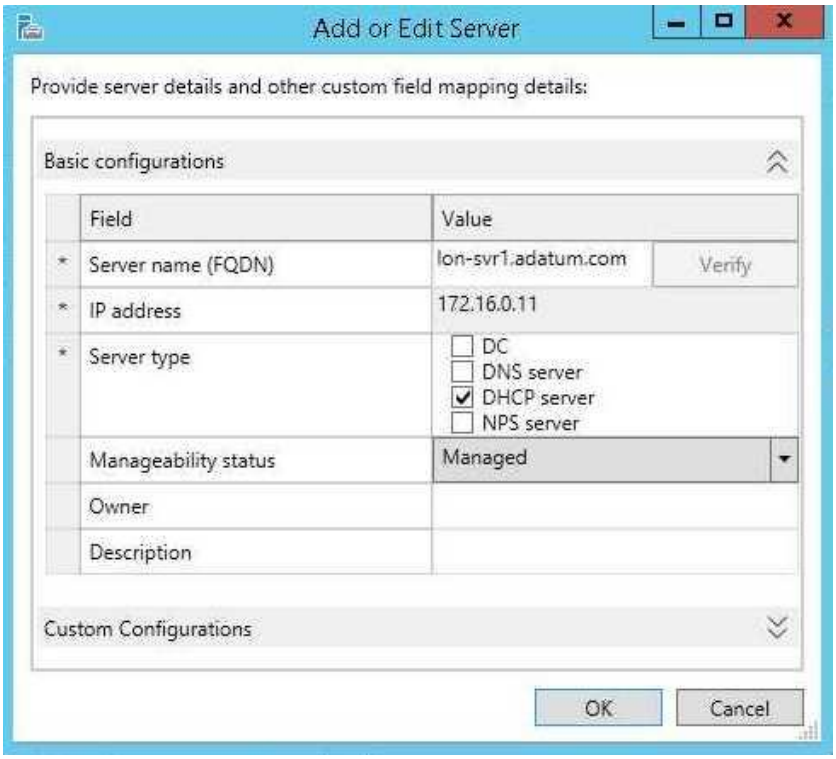
7. Trong hộp thoại **Add or Edit Server**, bung ô **Manageability status**, chọn chế độ **Managed**, và chọn **OK**.



8. Tương tự, trong **IPv4**, nhấn chuột phải lên dòng **lon-svr1**, chọn **Edit Server**.



9. Hộp thoại **Add or Edit Server**, bung ô **Manageability status**, chọn chế độ **Managed**, và chọn **OK**.



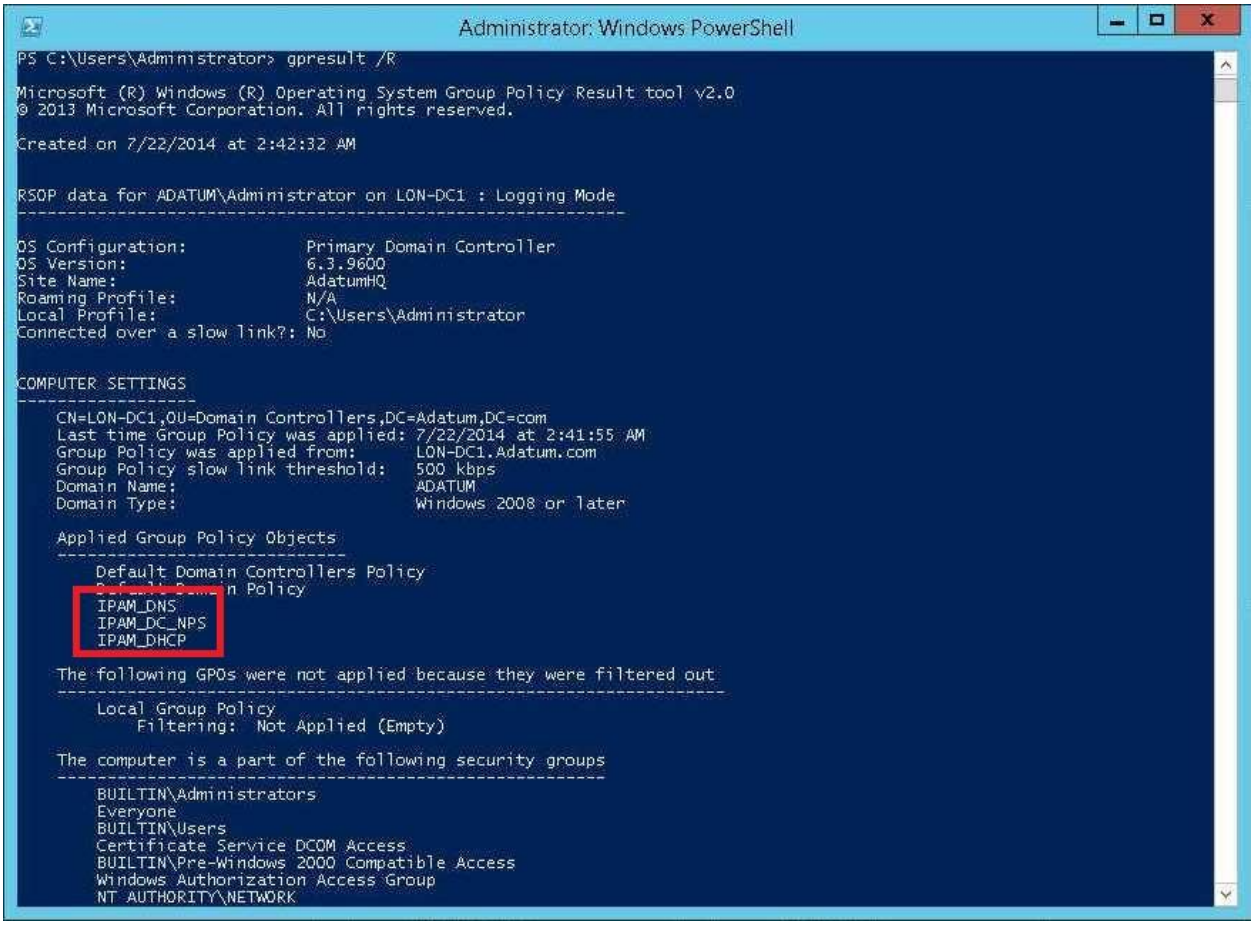
10. Qua máy **LON-DC1.**

11. Trên thanh taskbar, mở **Windows PowerShell**.

12. Trong cửa sổ Windows PowerShell, gõ lệnh: **Gpupdate /force**

13. Sau khi thành công, trong Windows PowerShell, gõ lệnh: **Gpresult /R**

14. Kiểm tra **IPAM_DNS, IPAM_DC_NPS,** và **IPAM_DHCP GPOs** đã được áp dụng.



15. Tắt Windows PowerShell.

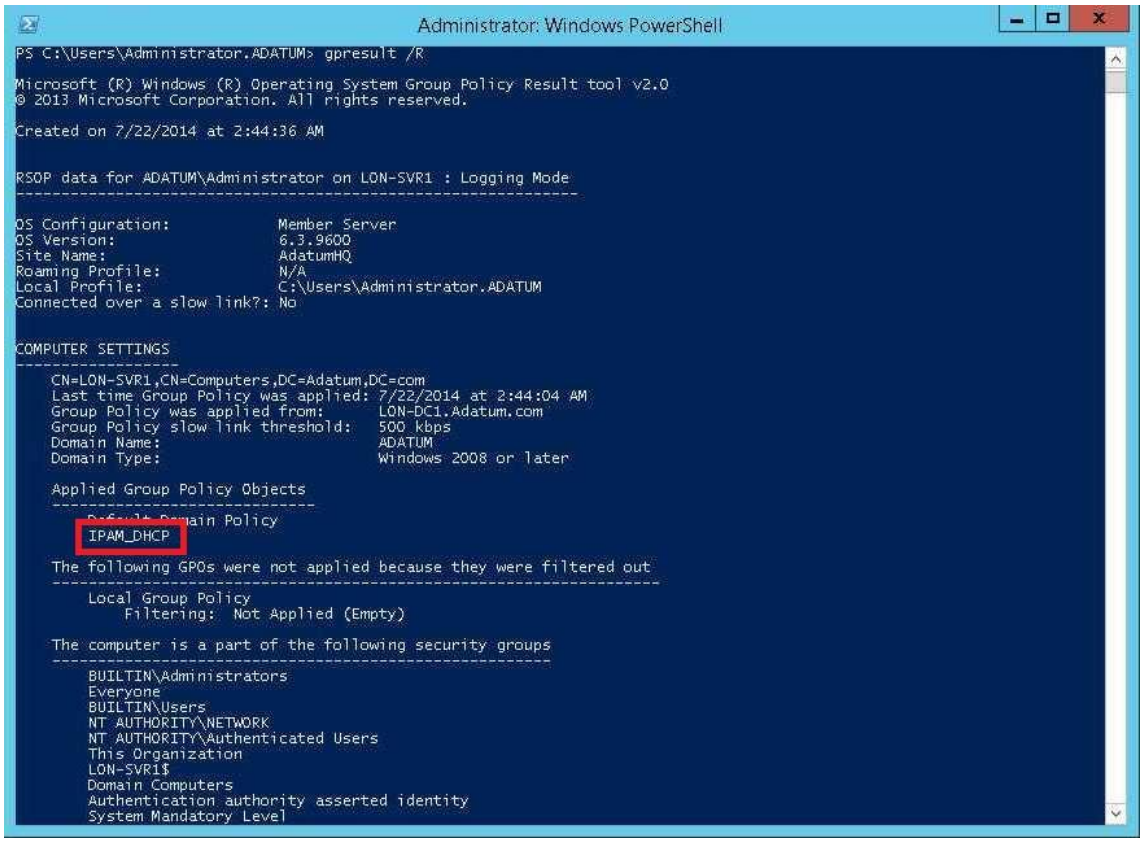
16. Qua máy **LON-SVR1.**

17. Trên thanh taskbar, mở **Windows PowerShell**.

18. Trong cửa sổ Windows PowerShell, gõ lệnh: **Gpupdate /force**

19. Sau khi thành công, trong Windows PowerShell, gõ lệnh: **Gpresult /R**

20. Kiểm tra **IPAM_DHCP** GPO đã được áp dụng.

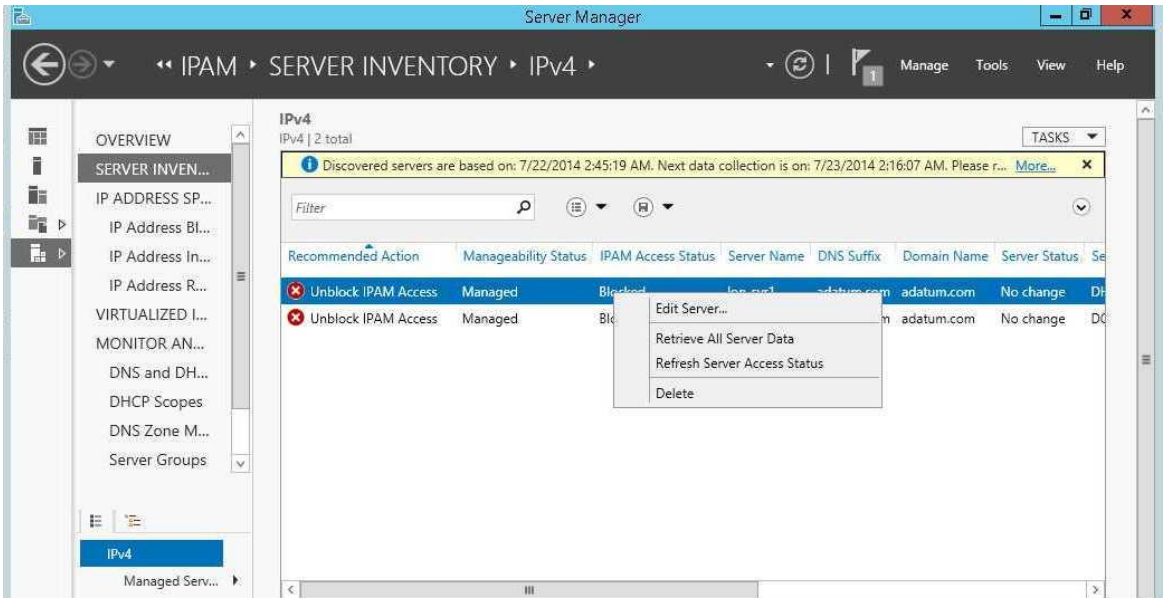


21. Qua máy **LON-SVR2.**

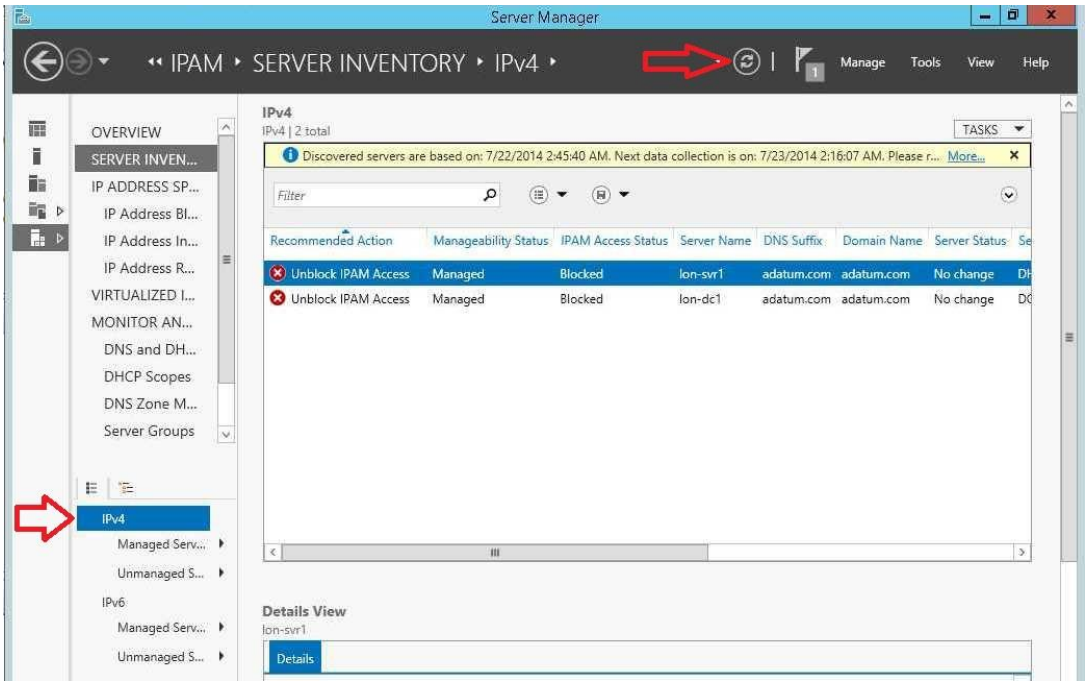
22. Quay lại cửa sổ **Server Manager**, vào mục **IPv4**, nhấn chuột phải **LON-DC1**, chọn **Refresh Server Access Status**.



23. Tương tự, nhấn chuột phải **LON-SVR1**, chọn **Refresh Server Access Status**.

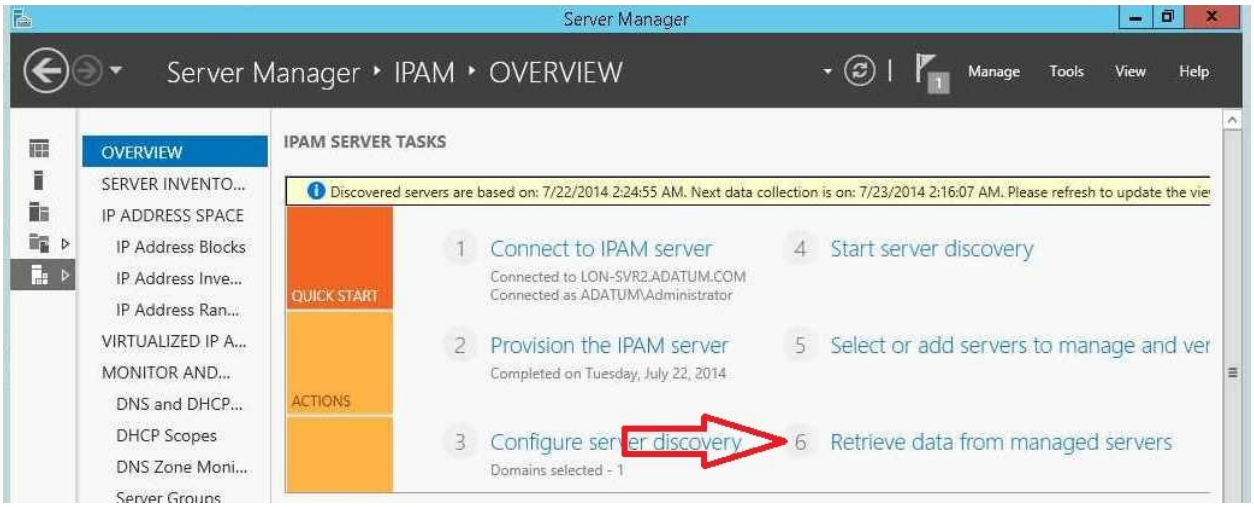


24. Trong **Server Manager**, chọn **IPv4**, chọn vào biểu tượng **Refresh**.



Chú ý: Thời gian Refresh sự thay đổi khoảng 5 phút.

25. Trong cửa sổ **IPAM Overview**, chọn **Retrieve data from managed servers**.



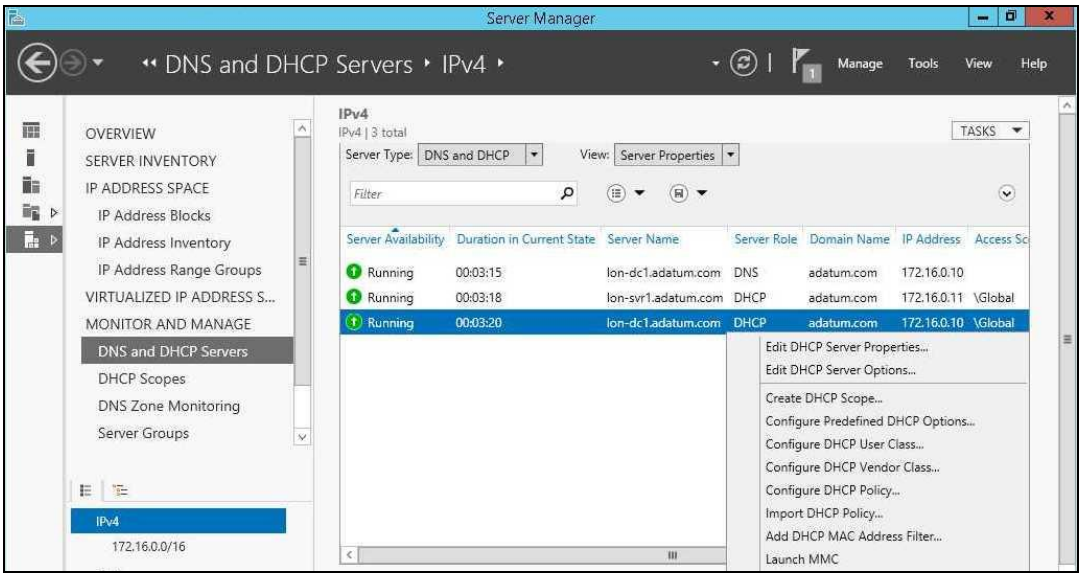
Chú ý: Hành động này sẽ hoàn thành trong khoảng 5 phút hoặc hơn.

Bước 7. Cấu hình và kiểm tra DHCP scope với IPAM.

1. Qua máy **LON-SVR2**.

2. Mở **Server Manager**, trong **IPAM**, chọn **DNS and DHCP Servers**.

3. Nhấn chuột phải lên dòng **lon-dc1.adatum.com** có server role là **DHCP**, chọn **Create DHCP scope**.



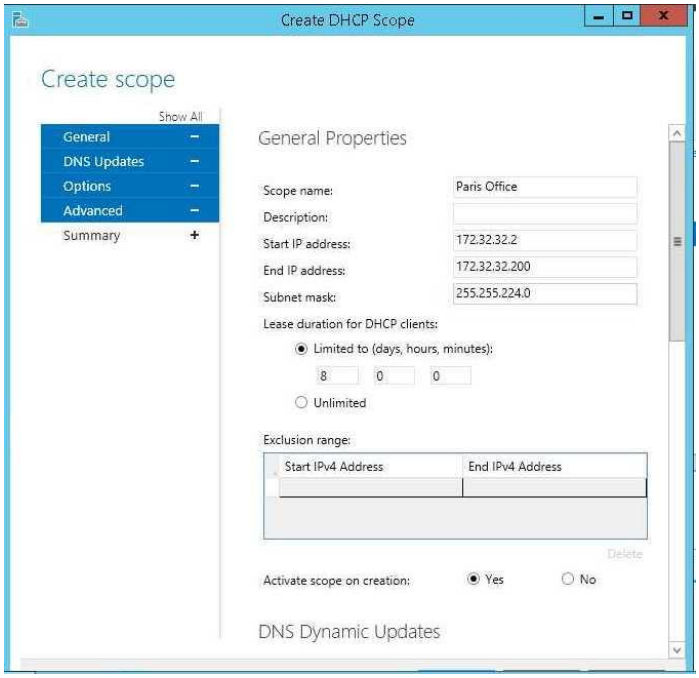
4. Trong hộp thoại **Create DHCP Scope**, nhập thông tin như sau:

- Scope name: Paris Office

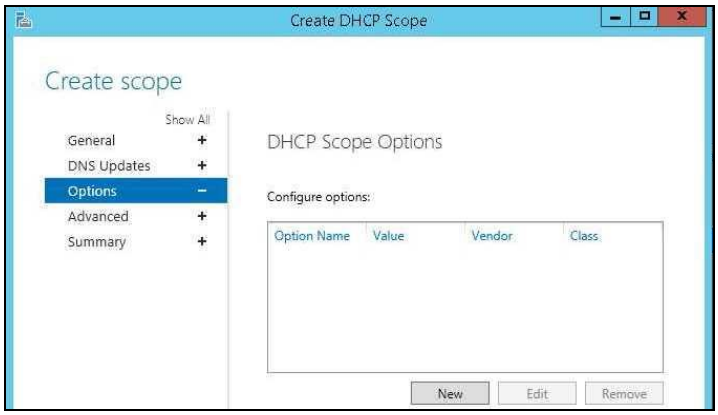
- Start IP address: 172.32.32.2

- End IP address: 172.32.32.200

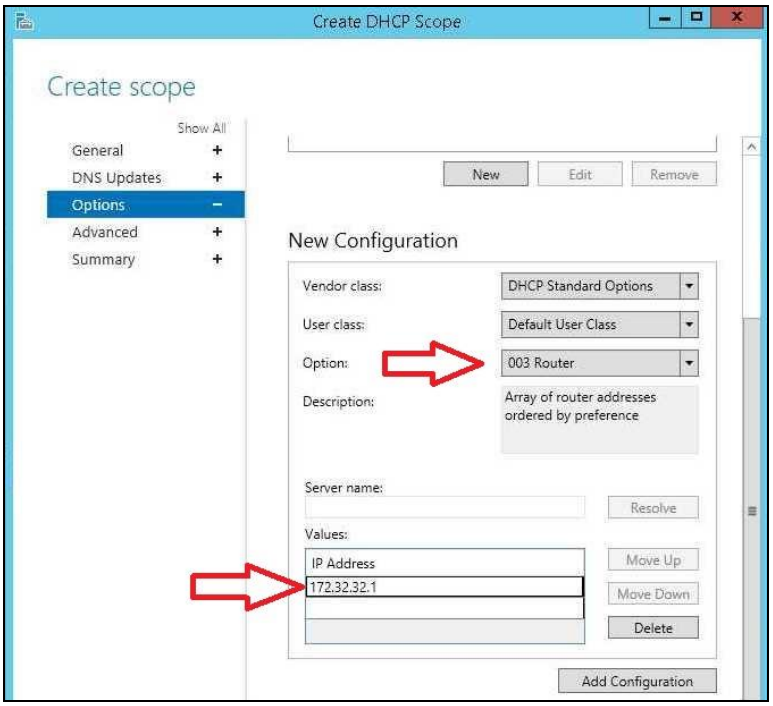
- Subnet mask: 255.255.224.0



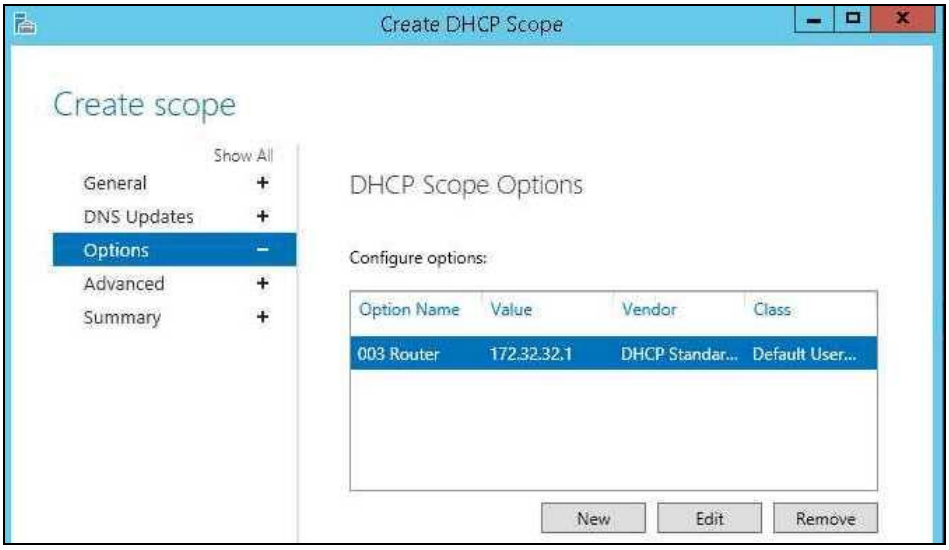
5. Vào mục **Options** bên trái, chọn **New**.



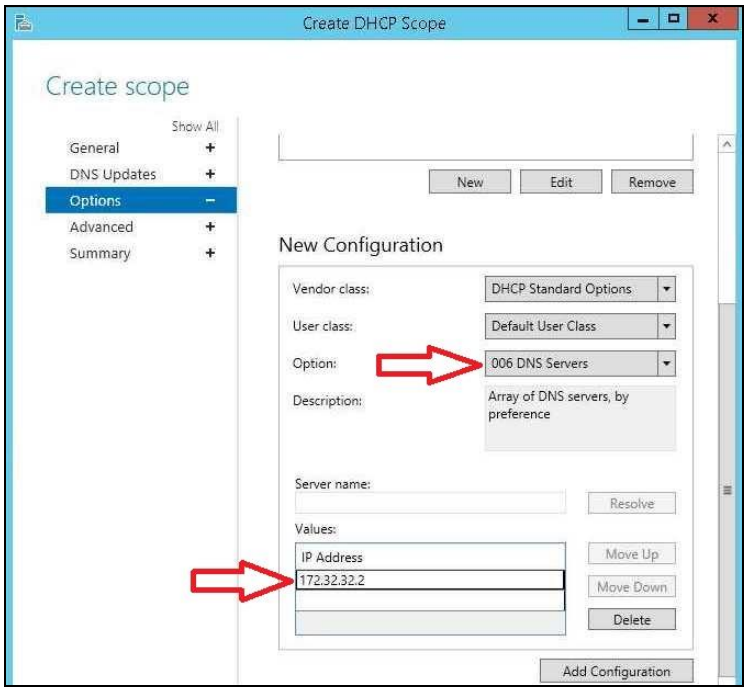
6. Trong phần **New Configuration**, bung **Option**, chọn **003 Router**. Trong mục **Values**, nhập **172.32.32.1** vào ô **IP address**, và chọn **Add Configuration**.



7. Tương tự, trong hộp thoại **DHCP Scope Options**, chọn **New**.



8. Trong phần **New Configuration**, bung **Option**, chọn **006 DNS Servers**. Trong mục **Values**, nhập **172.32.32.2** vào ô **IP address**, và chọn **Add Configuration**, và chọn **OK**.



9. Trong **Server Manager**, vào mục **IPAM**, chọn **DHCP Scopes**.

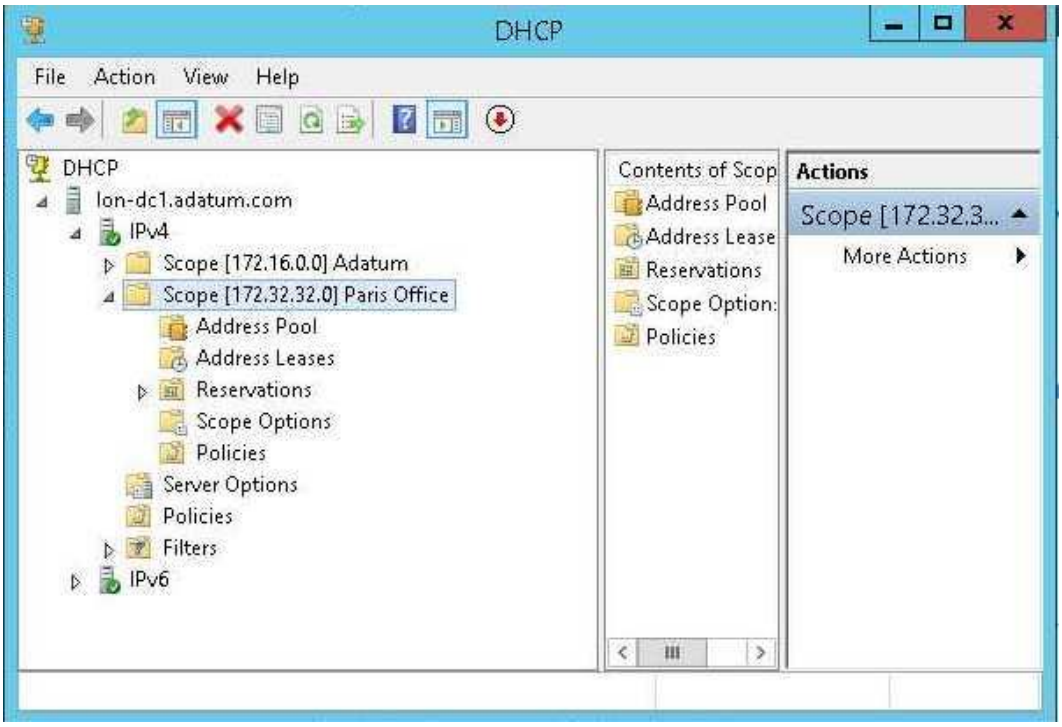
Chú ý: DHCP scope mới tạo đã được hiển thị.

10. Qua máy **LON-DC1.**

11. Mở **Server Manager**, bung mục **Tools**, mở công cụ **DHCP**.



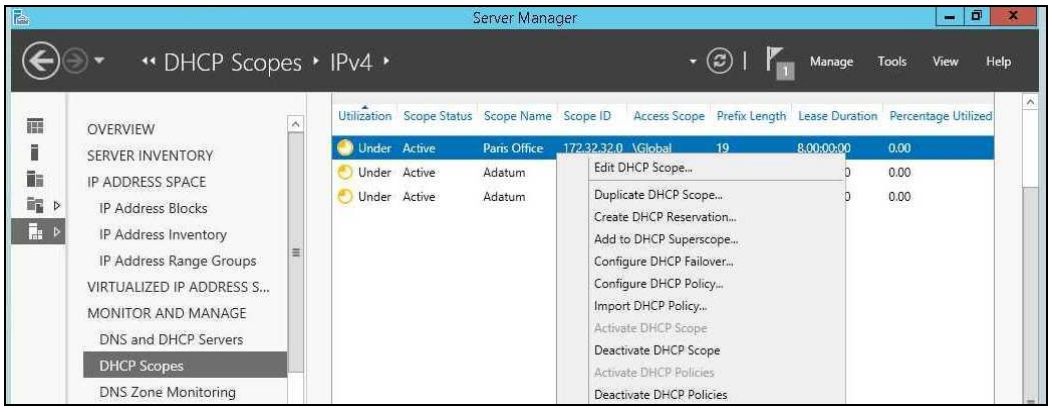
12. Trong cửa sổ **DHCP**, bung **lon-dc1.adatum.com**, bung **IPv4**.



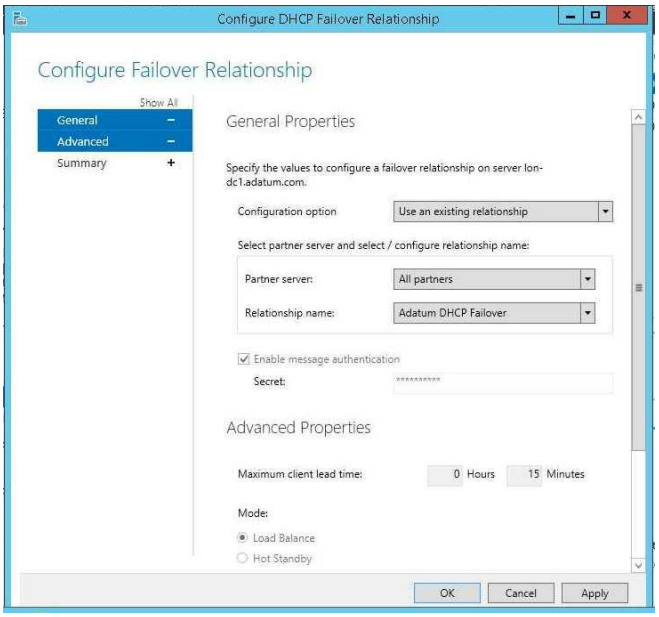
Chú ý: Đã có scope Paris Office.

13. Qua máy **LON-SVR2.**

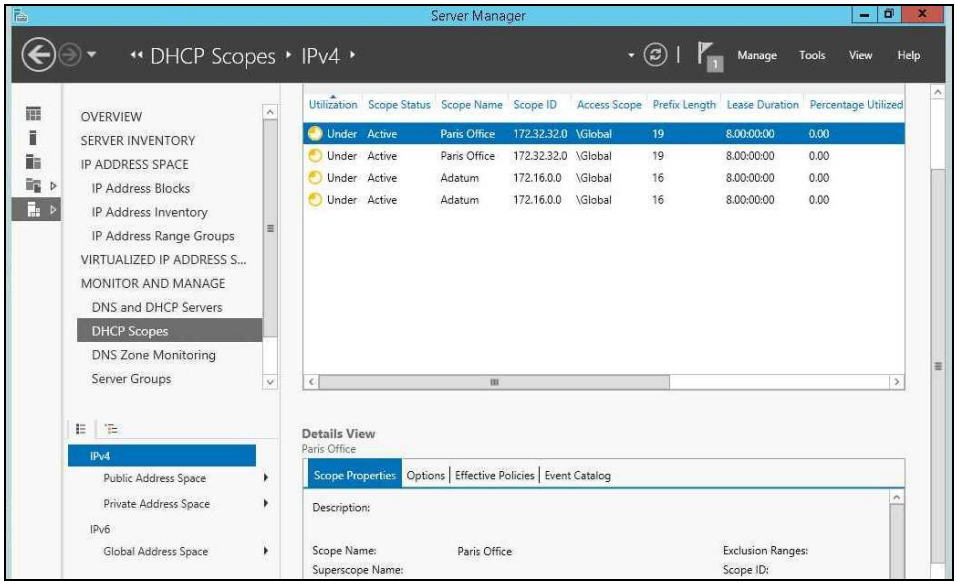
14. Mở **Server Manager**, vào mục **IPAM**, chọn **DHCP Scopes**, nhấn chuột phải lên scope **Paris Office**, chọn **Configure DHCP Failover**.



15. Trong hộp thoại **Configure DHCP Failover Relationship**, bung **Configuration option**, chọn **Use an existing relationship**. Trong **Relationship name**, chọn **Adatum DHCP Failover**, chọn **OK**.

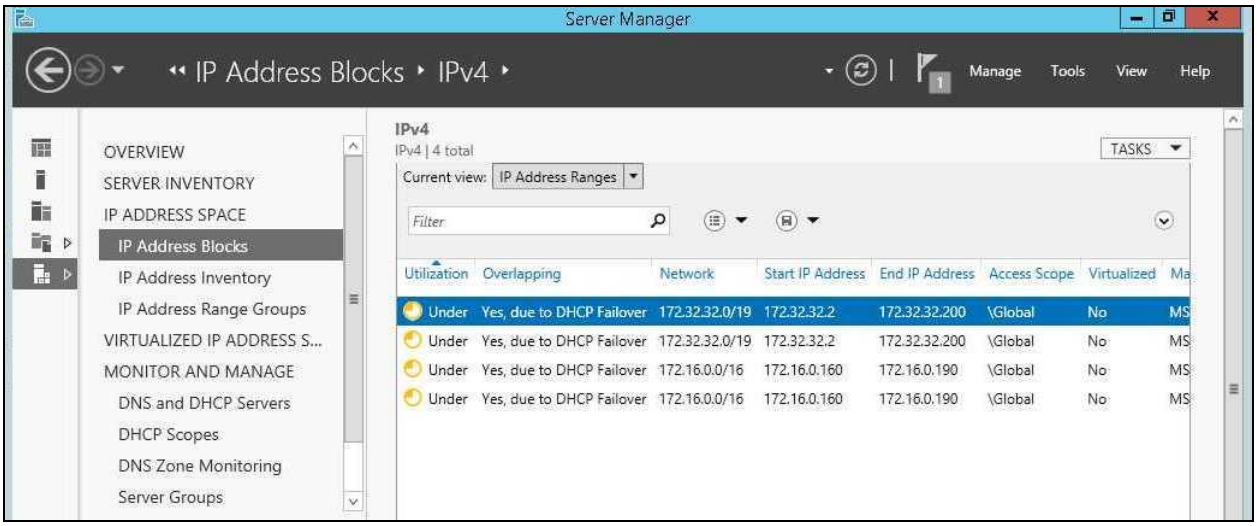


Chú ý: Scope **Paris Office** đã hiển thị trong danh sách các scopes.

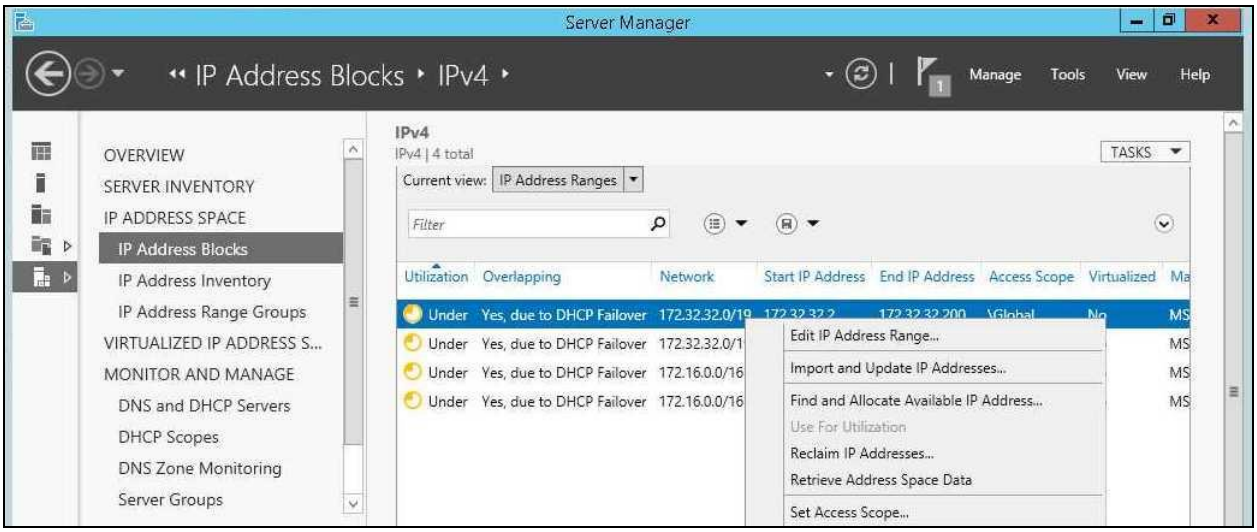


Bước 8. Cấu hình IP address blocks, record IP addresses, và tạo DHCP reservations.

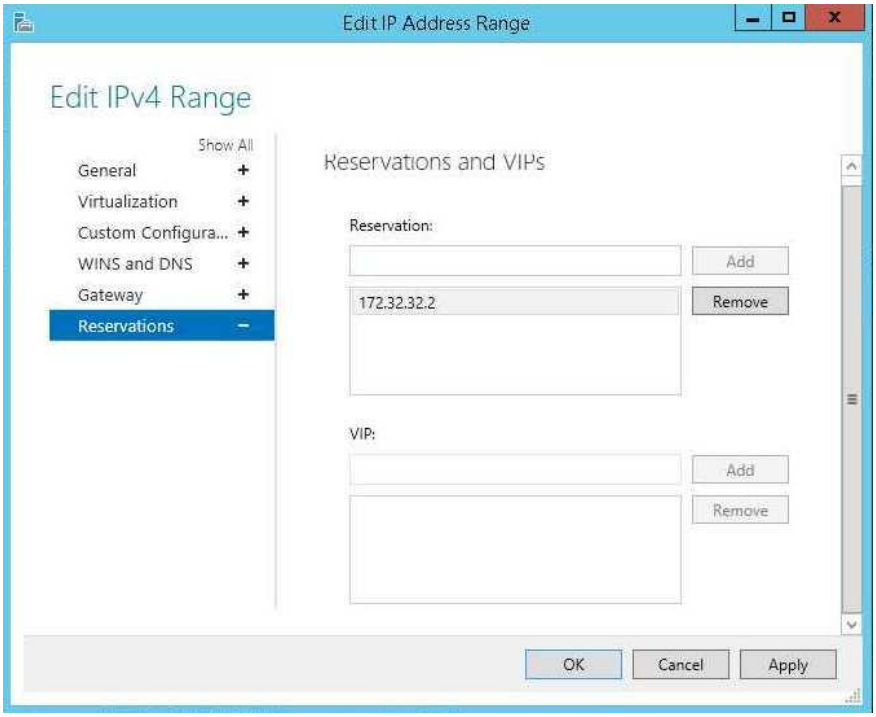
1. Qua máy **LON-SVR2**, mở **Server Manager**, vào mục **IPAM**, chọn **IP address Blocks**. Bung ô **Current view**, chọn **IP Address Ranges**. Kiểm tra có 2 dòng **DHCP failover 172.32.32.0** đã được liệt kê.



2. Nhấn chuột phải lên dòng **172.32.32.0/19** của **lon-dc1.adatum.com**, chọn **Edit IP Address Range**.



3. Trong hộp thoại **Edit IP Address Range**, chọn **Reservations**. Trong ô **Reservation**, , chọn **Add**, và chọn **OK**



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai được DHCP và IPAM cho hệ thống.

VIII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiện bước 2 và 3 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-SVR2**.

Bài 4: Thiết kế và triển khai hệ thống DNS

I. Mục tiêu:

- Thiết kế hệ thống phân giải tên DNS.
- Thiết kế DNS Zone và giải pháp đồng bộ DNS Zone.
- Triển khai hệ thống DNS.

II. Kịch bản:

Công ty A. Datum đã nhanh chóng phát triển và chuyển đổi sang Windows Server 2012, việc này cung cấp một cơ hội lý tưởng để A. Datum thiết kế và cấu hình lại cơ sở hạ tầng DNS. Với việc sắp mua lại công ty Contoso, bạn phải xem xét lại cơ sở hạ tầng DNS của công ty Contoso, và nếu cần thiết, bạn sẽ đề nghị thay đổi thiết kế DNS.

Bảng dưới đây cung cấp một số thông tin bổ sung về các địa điểm khác nhau tại Contoso:

Trụ sở chính và Văn phòng trung tâm khu vực

Vị trí	**Chức năng**	**Đặc điểm**
Paris, Pháp	Trụ sở chính. Có vai trò là bán hàng, tiếp thị và trung tâm phân phối cho châu âu	Nhân viên hiện tại: 1,800 (nhân viên dự trù: 4,700)
Rome, Ý	Văn phòng trung tâm khu vực	Nhân viên: 250
Barcelona, Tây Ban Nha	Văn phòng trung tâm khu vực	Nhân viên: 200
Munich, Đức	Văn phòng trung tâm khu vực	Nhân viên: 200
Athens, Hy Lạp	Văn phòng trung tâm khu vực	Nhân viên: 200

Chi nhánh và các trung tâm phân phối khu vực

Vị trí	Số lượng servers	Số người sử dụng (tổng cộng trên tất cả các chi nhánh)	Chi nhánh
Đức	1 tại mỗi chi nhánh	100	3
Tây Ban Nha	1 tại mỗi chi nhánh	250	5
Ý	1 tại mỗi chi nhánh	250	5
Hy Lạp	1 tại mỗi chi nhánh	75	2

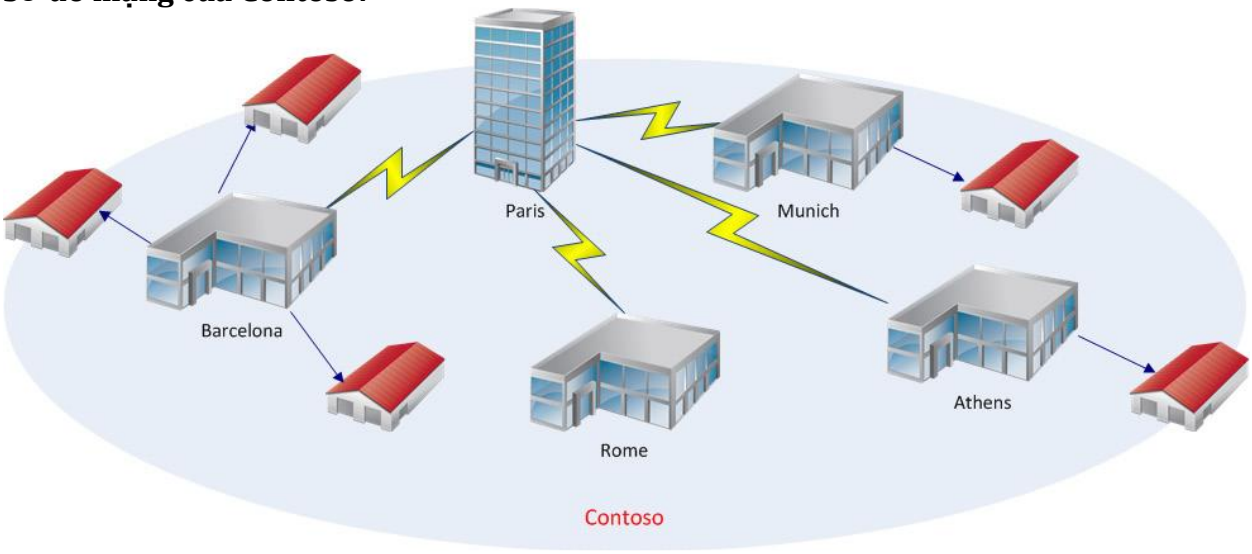
Hiên nay công ty Contoso không có server chạy Windows. Các server hiện tại chạy UNIX và kết hợp với client chạy Windows. UNIX cung cấp dịch vụ phân giải tên. Công ty có đăng ký tên miền Internet là Contoso.com, tên miền này được sử dụng cả trong nội bộ và bên ngoài.

Một DNS Zone duy nhất quản lý cấu trúc này, các server thứ cấp (Secondary Server) phân phối cho các văn phòng trung tâm khu vực. Văn phòng chi nhánh và trung tâm phân phối hiện không có DNS Server, và tất cả các máy clients tại các văn phòng được cấu hình để sử dụng DNS Server tại trung tâm khu vực gần nhất.

Contoso có danh sách các DNS Records bên ngoài mà quản trị viên phải đồng bộ bằng tay với cấu trúc DNS nội bộ. Những DNS Records thay đổi trung bình ít nhất một lần mỗi năm. Bảng sau đây liệt kê những DNS Records này:

External DNS records	Mục đích
www.contoso.com	Public website
Customer.contoso.com	Trang web an toàn cho khách hàng
Vpn.contoso.com	VPN server
Mail.contoso.com	Internet mail server
Dns1.contoso.com	External DNS server
Dns2.contoso.com	External DNS server

Sơ đồ mạng của Contoso:



III. Yêu cầu tổng quan:

Thiết kế một chiến lược phân giải tên DNS mới theo các yêu cầu sau:

- Có khả năng chịu lỗi và phân giải được các tên quan trọng (Single-Label Name).
- Kế hoạch phải hỗ trợ bất kỳ sự tăng trưởng dự kiến hoặc những thay đổi trong cơ sở hạ tầng mạng.
- Có khả năng là sẽ triển khai AD DS cho Contoso khi công ty này được mua lại trong tương lai gần. Thiết kế DNS nên tính đến sự thay đổi này.
- Mặc dù việc dự kiến sáp nhập A Datum, Trey Research và Contoso chưa xảy ra, nhưng người dùng giữa hai tổ chức đã chia sẻ được tài nguyên. Việc giám sát hệ thống gần đây cho thấy số lượng các truy vấn phân giải tên của adatum.com và treyresearch.net đã tăng đáng kể. Việc thiết kế phải phù hợp thực tế này.

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1** **20413C-LON-CL1**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy ảo với thông tin sau:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**
5. Thực hiên từ bước 2 đến 4 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-CL1.**

VI. Thực hành:

Thời gian thực hành: 60 phút

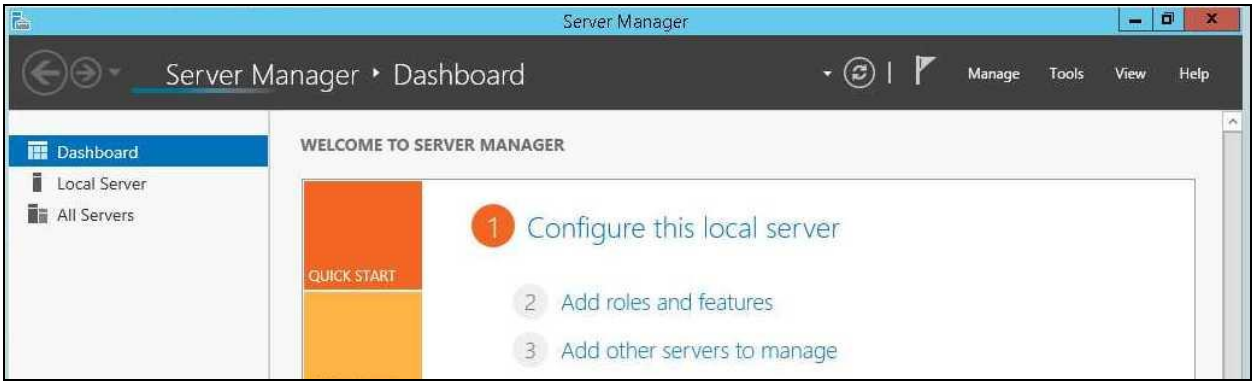
Bài thực hành bao gồm các bước:

1. Cài đặt DNS Server role .
2. Tạo Secondary Zones và cấu hình Zone Transfers.
3. Cấu hình Forwarder và Global Names Zone.
4. Client kiểm tra phân giải tên.

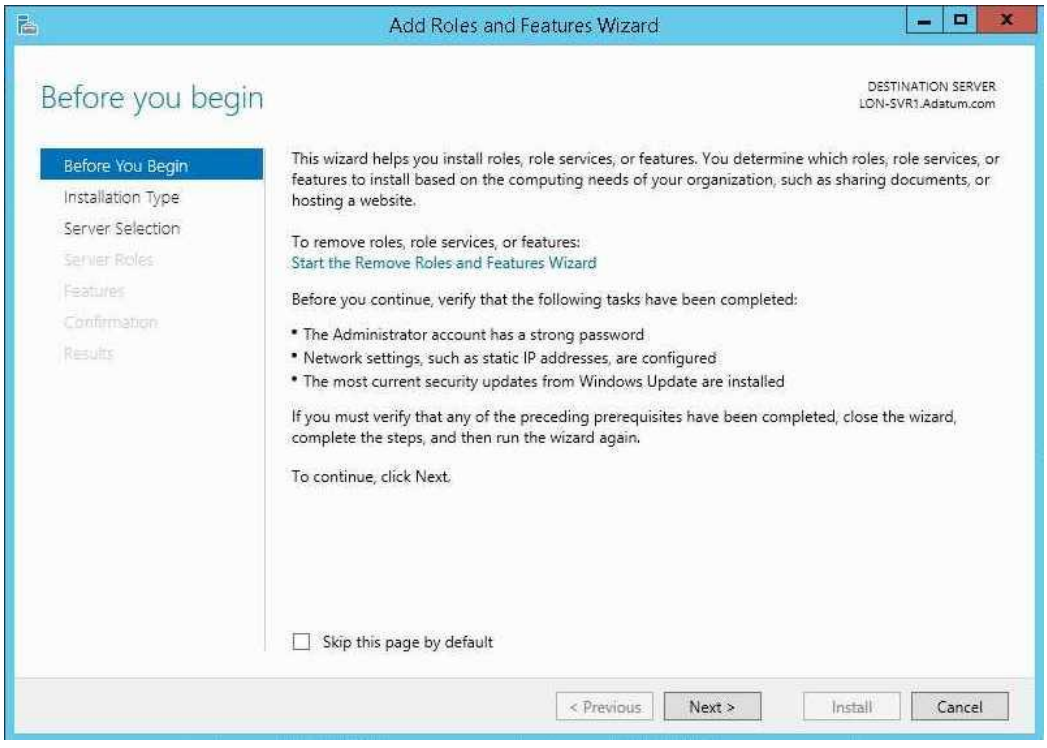
Bước 1: Cài đặt DNS Server role .

1. Qua máy **LON-SVR1.**

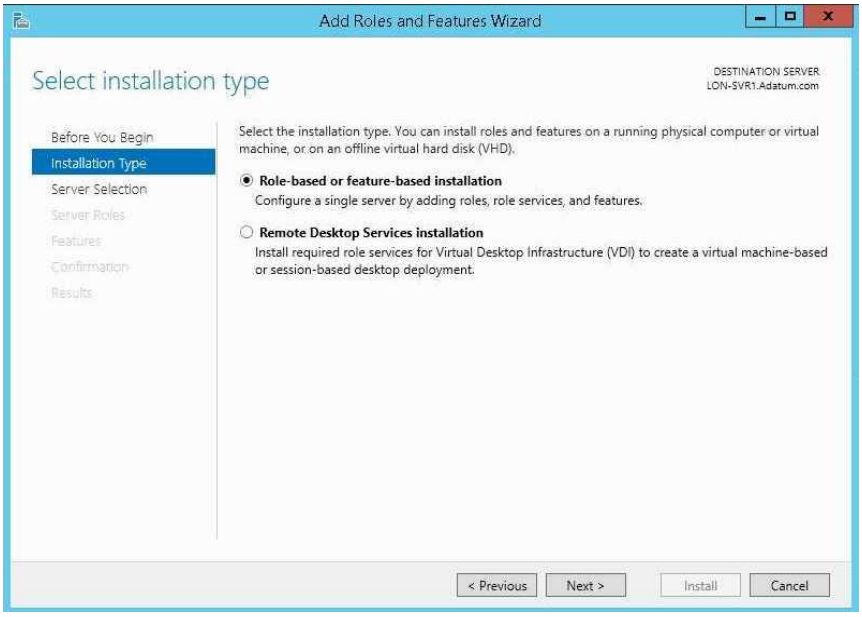
2. Mở công cụ **Server Manager**, chọn **Add roles and features**.



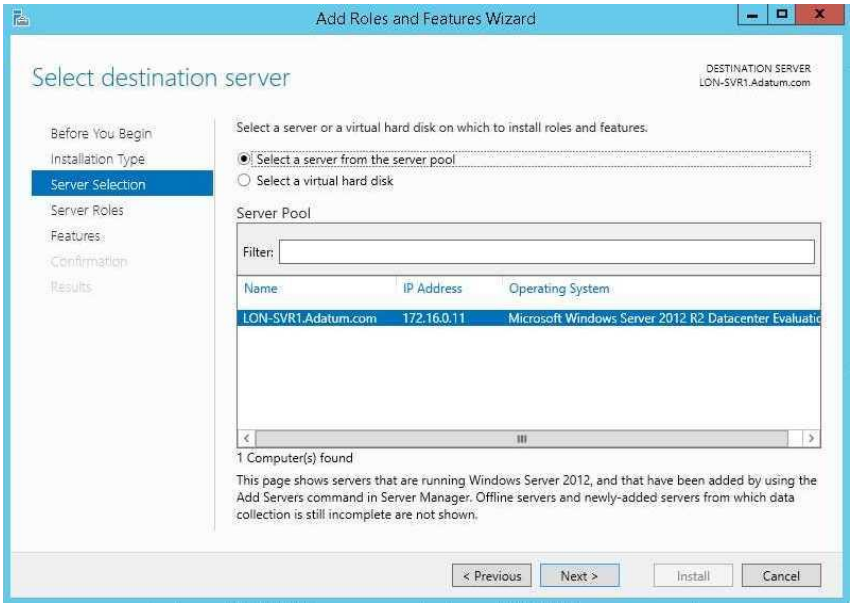
3. Cửa sổ **Before you begin,** chọn **Next**.



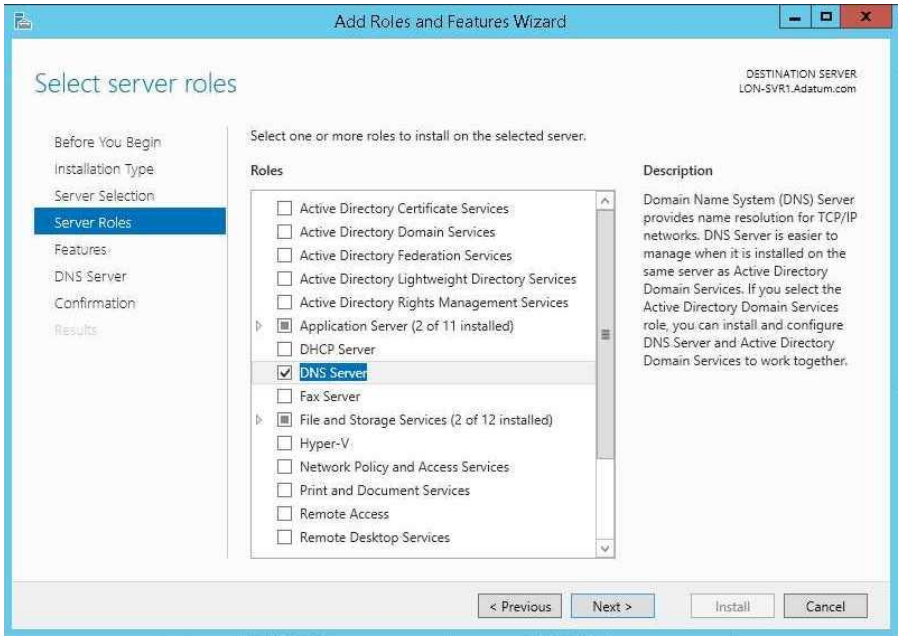
4. Cửa sổ **Select installation type**, chọn **Role-based or feature-based installation**, và chọn **Next**.



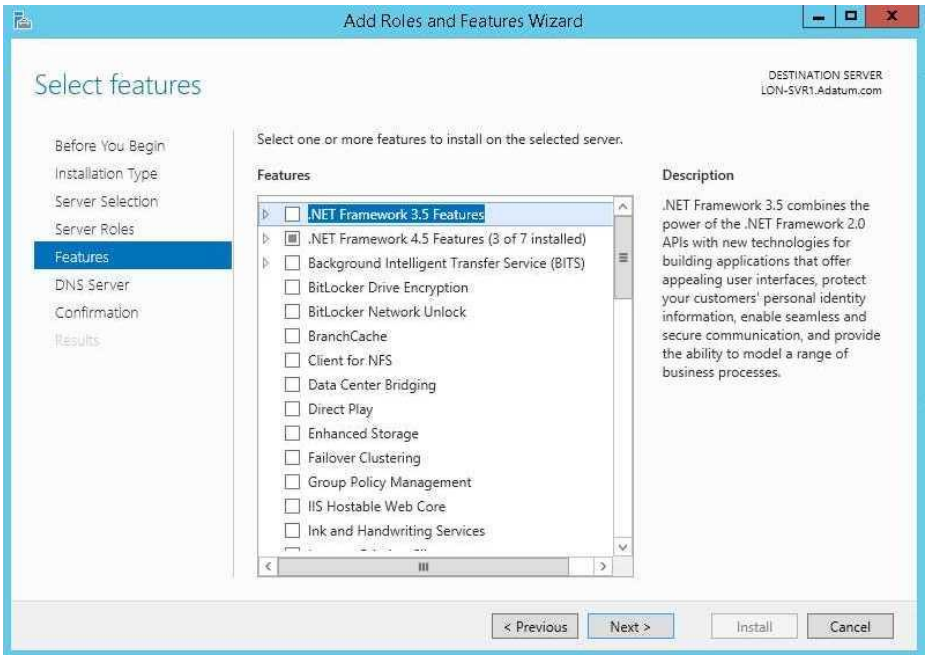
5. Cửa sổ **Select destination server**, chọn **Select a server from the server pool**, và chọn **Next**.



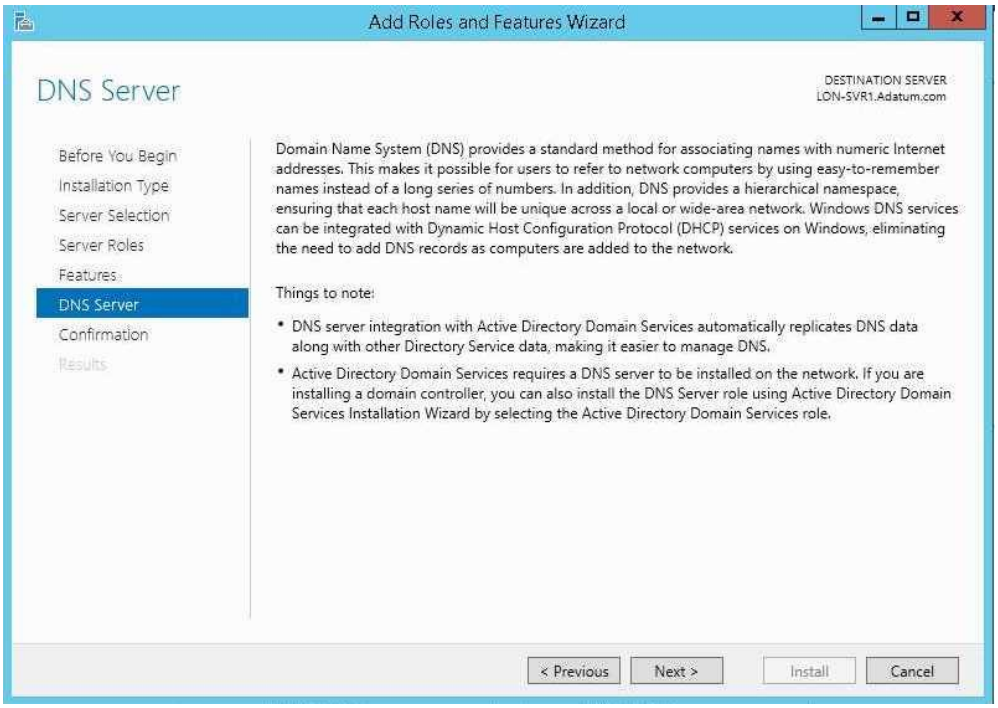
6. Cửa sổ **Select server roles**, đánh dấu chọn **DNS Server**, chọn **Add Features**, và chọn **Next**.



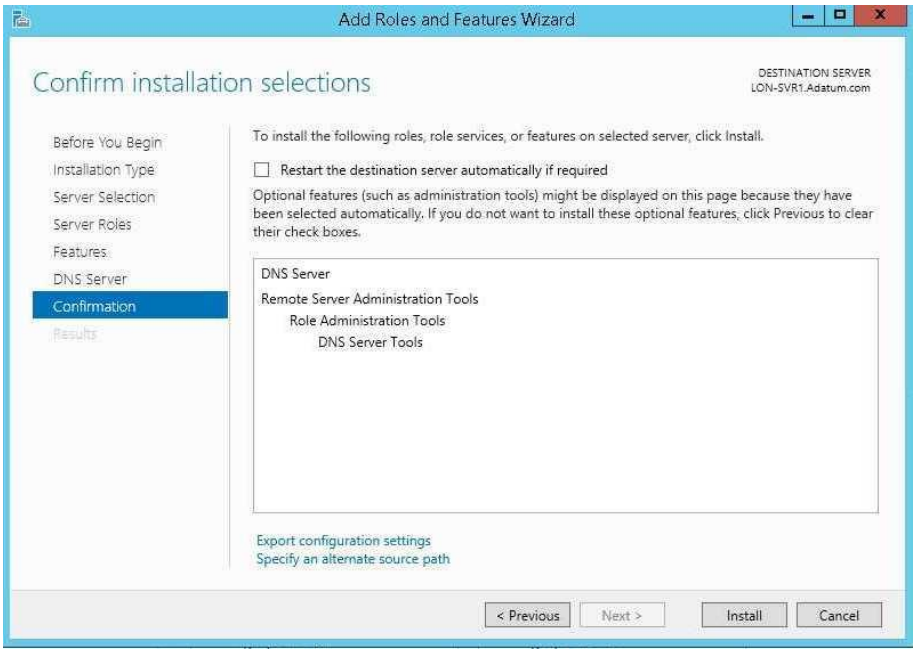
7. Cửa sổ **Select features**, chọn **Next**.



8. Cửa sổ **DNS Server**, chọn **Next**.



9. Cửa sổ **Confirm installation selections**, chọn **Install**.



10. Sau khi cài đặt thành công, chọn **Close**.

Bước 2: Tạo Secondary Zones và cấu hình Zone Transfers.

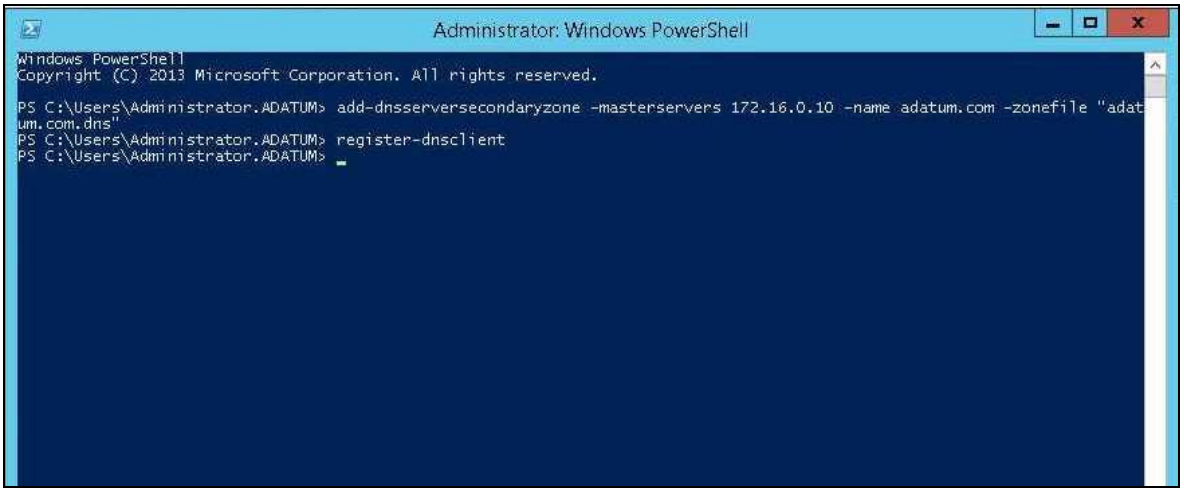
1. Trên máy **LON-SVR1**, trong thanh taskbar, mở **Windows PowerShell**.

2. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

add-dnsserversecondaryzone –masterservers 172.16.0.10 –Name Adatum.com –Zonefile "Adatum.com.dns"

- Sau đó gõ lệnh:

Register-DnsClient



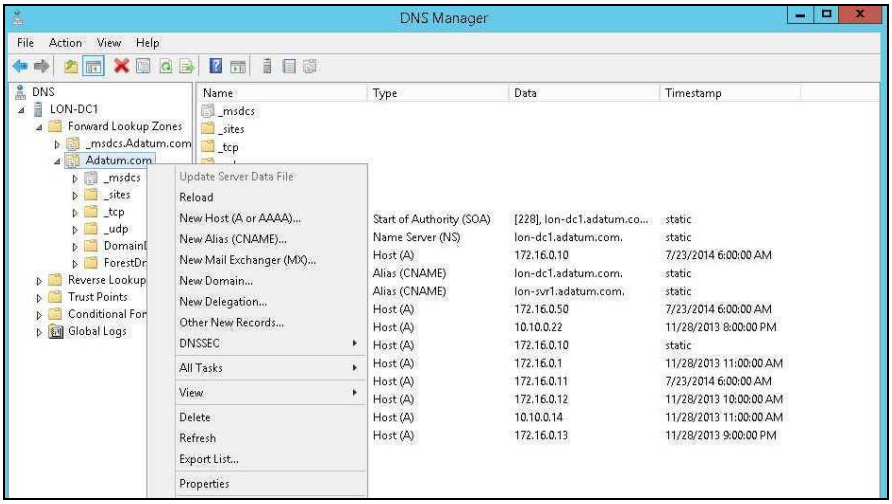
3. Qua máy **LON-DC1**.

4. Mở **Server Manager**, bung menu **Tools**, mở công cụ **DNS**.

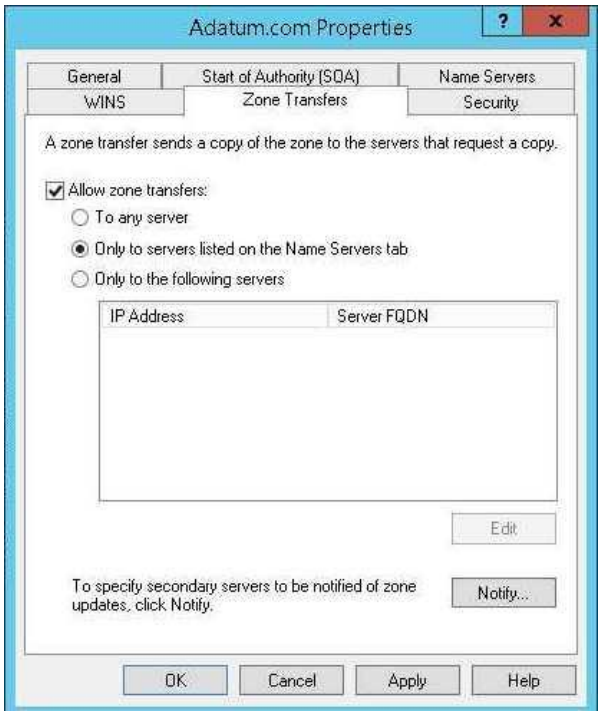


5. Trong cửa sổ **DNS Manager**, bung **Forward Lookup Zones**, bung **Adatum.com**.

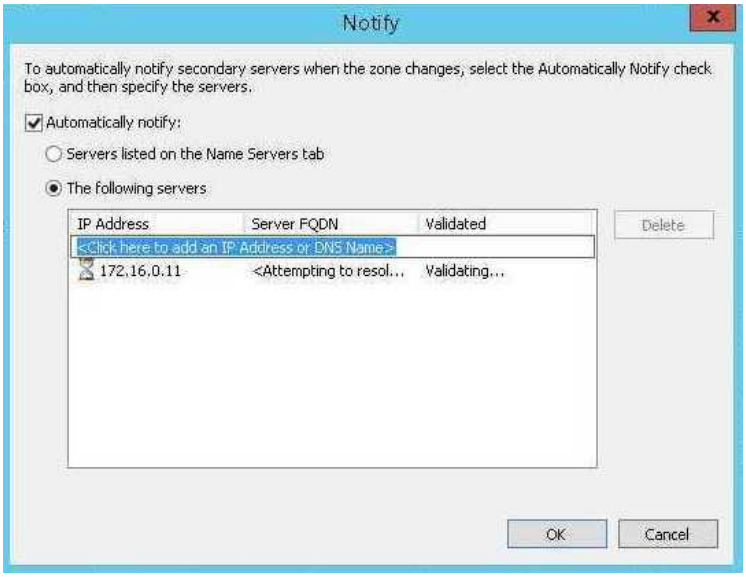
6. Nhấn chuột phải **Adatum.com**, chọn **Properties**.



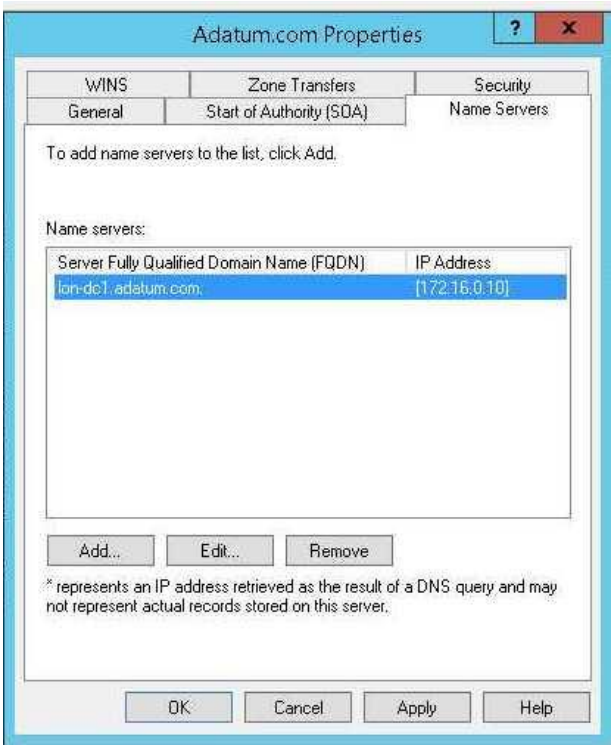
7. Trong hộp thoại **Adatum.com Properties**, qua tab **Zone Transfers**. Đánh dấu chọn **Allow zone transfers**, chọn **Only to servers listed on the Name Servers tab**, và chọn **Notify**.



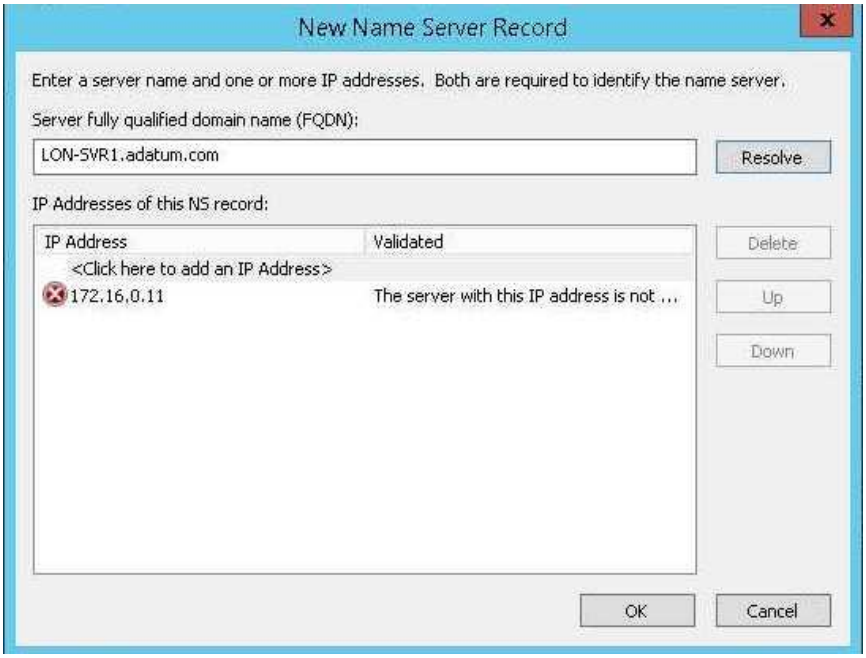
8. Trong hộp thoại **Notify**, nhập **172.16.0.11** vào danh sách **The following servers**, nhấn phím **Enter**, và chọn **OK**



9. Qua tab **Name Servers**, chọn **Add**.



10. Hộp thoại **New Name Server Record**, nhập **LON-SVR1.Adatum.com** vào ô **Server fully qualified domain name (FQDN)**, chọn **Resolve**, chọn **OK** 2 lần.

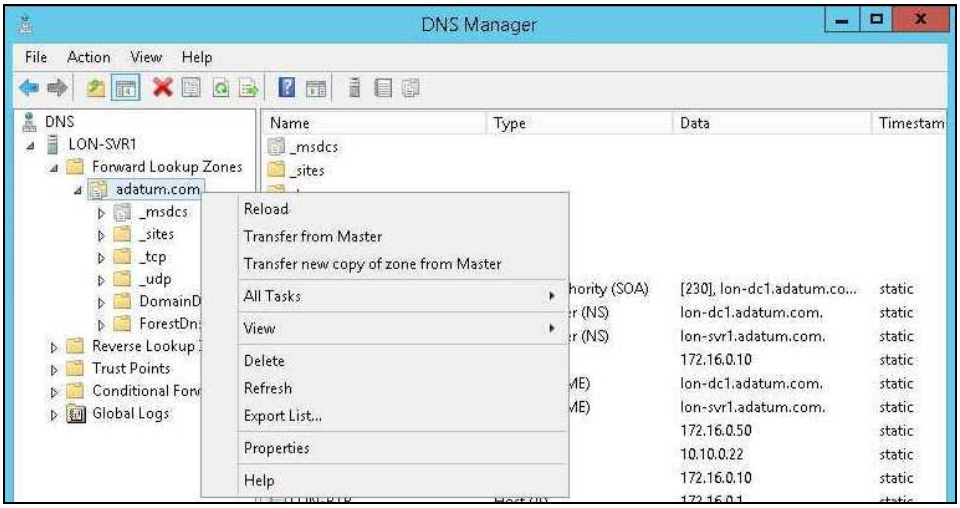


11. Qua máy **LON-SVR1**.

12. Trong cửa sổ **Server Manager**, bung **Tools**, mở **DNS**.



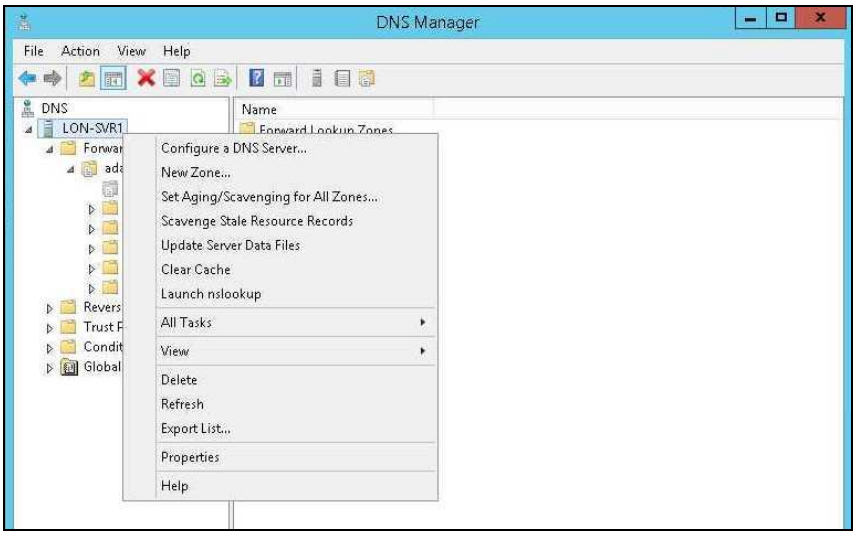
13. Trong cửa sổ **DNS Manager**, bung **LON-SVR1**, bung **Forward Lookup Zones**, bung **Adatum.com**. Nhấn chuột phải **Adatum.com**, chọn **Transfer from Master**.



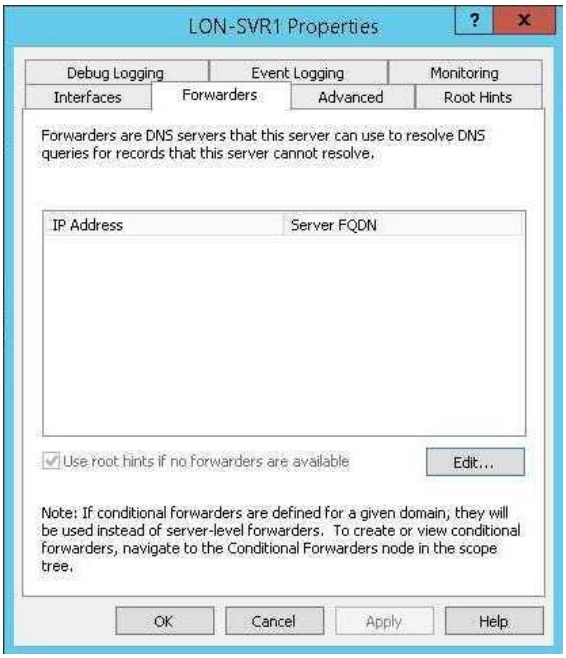
14. Chọn zone **Adatum.com,** nhấn phím **F5** . Kiểm tra dữ liệu trong zone **Adatum.com** đã được hiển thị. (Nếu chưa có, lập lại bước 13 & 14).

Bước 3: Cấu hình Forwarder và Global Names Zone.

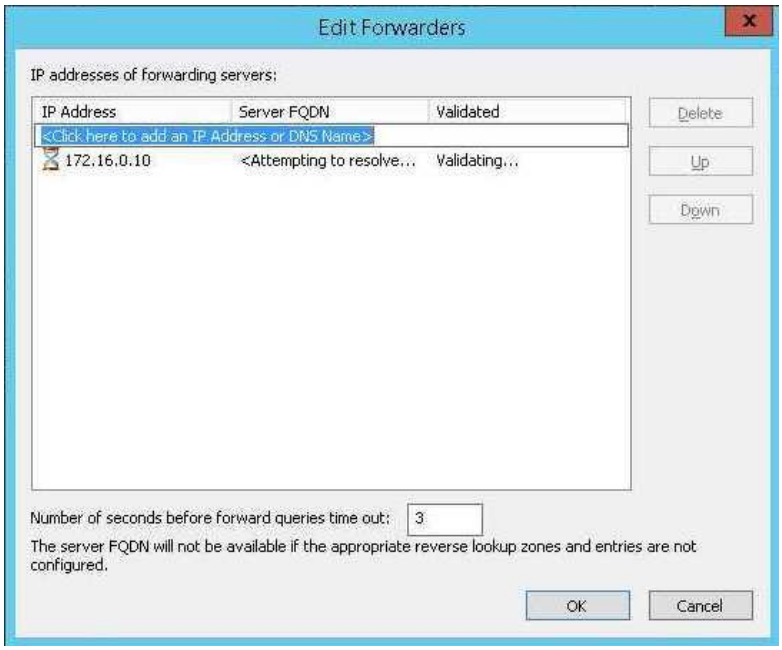
1. Qua máy **LON-SVR1**, trong cửa sổ **DNS Manager**, nhấn chuột phải **LON-SVR1**, chọn **Properties**.



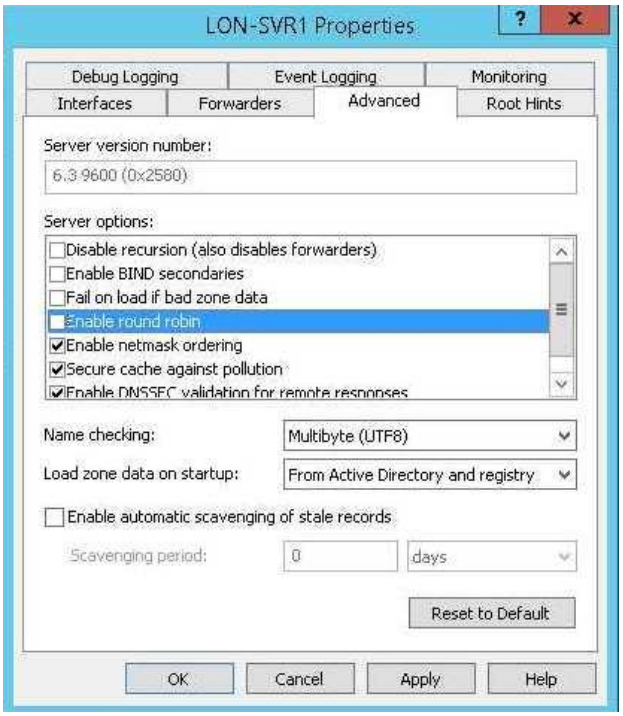
2. Trong hộp thoại **LON-SVR1 Properties**, qua tab **Forwarders**, chọn **Edit**.



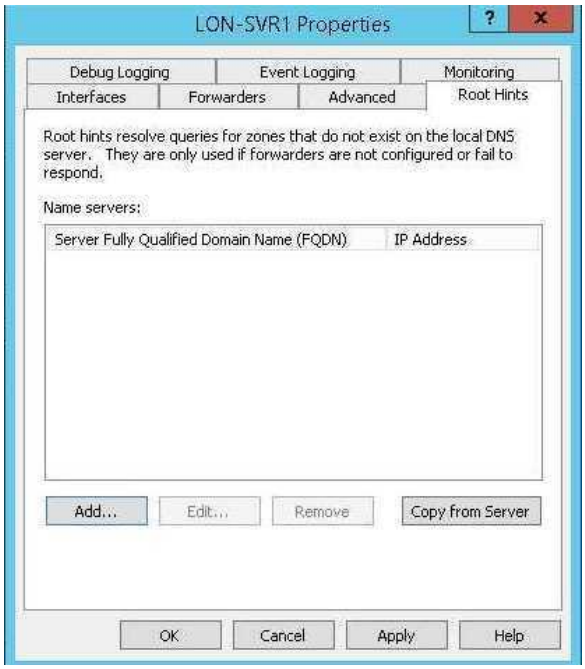
3. Hộp thoại **Edit Forwarders**, nhập **172.16.0.10** vào ô **IP Address**, nhấn phím **Enter**, và chọn **OK**.



4. Qua tab **Advanced**. bỏ dấu chọn **Enable round robin**, chọn **Apply**.



5. Qua tab **Root Hints**. chọn **Remove** để xóa trắng danh sách **Name servers**, chọn **OK**.

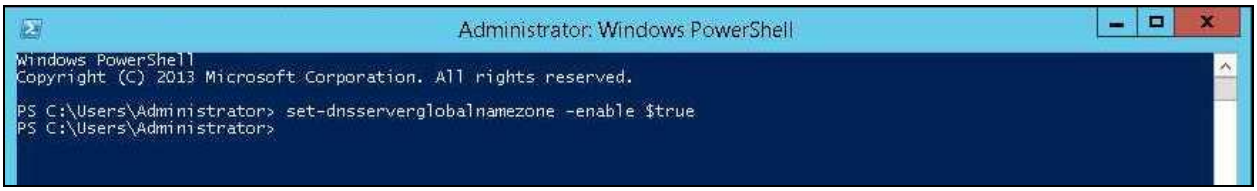


6. Qua máy **LON-DC1**. Trên thanh taskbar, nhấn chuột phải lên biểu tượng **Windows PowerShell**, chọn **Run as administrator**.

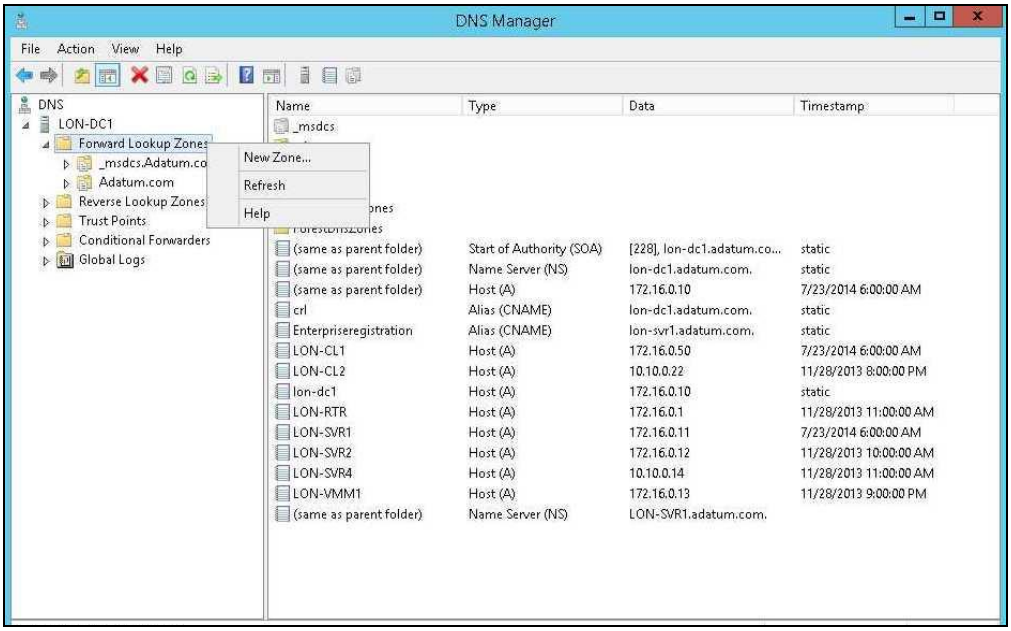


7. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

set-dnsserverglobalnamezone –enable $true



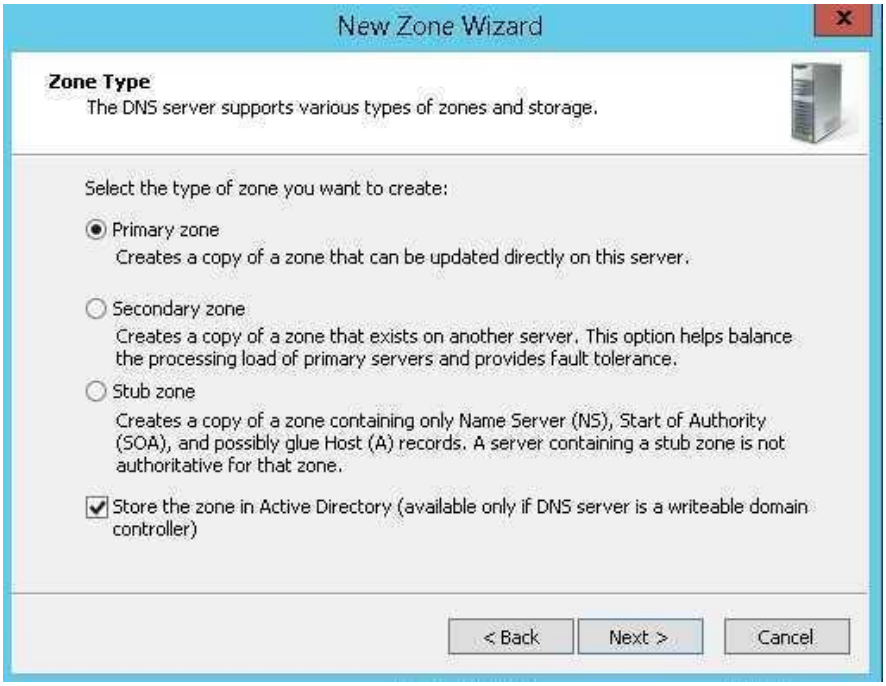
8. Mở công cụ **DNS Manager**, bung **LON-DC1**, bung **Forward Lookup Zones**, nhấn chuột phải **Forward Lookup Zones**, chọn **New Zone**.



9. Cửa sổ **Welcome**, chọn **Next**.



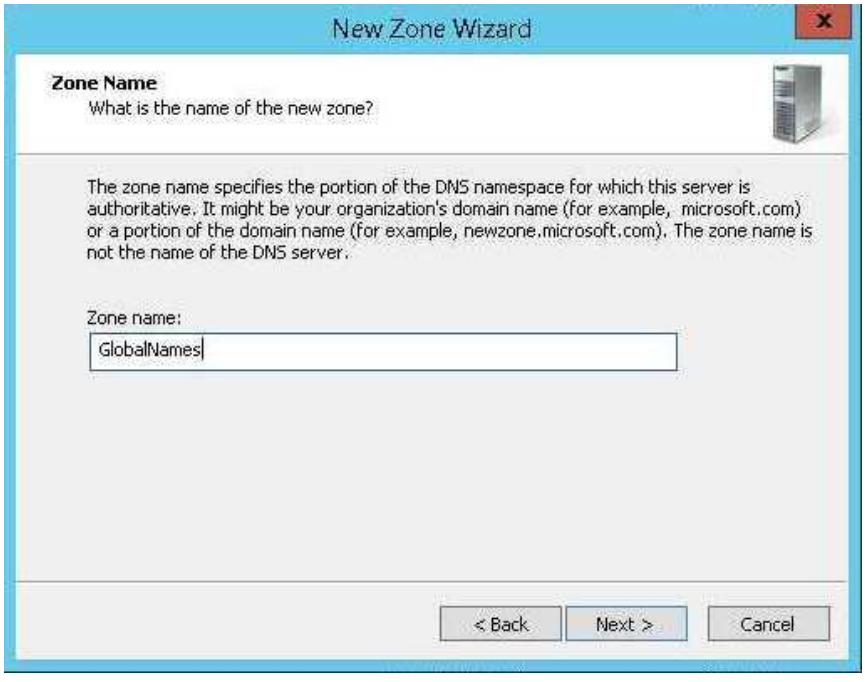
10. Cửa sổ **Zone Type**, chọn **Primary zone**, và chọn **Next**.



11. Cửa sổ **Active Directory Zone Replication Scope**, chọn **To all DNS server running on domain controllers in this forest: Adatum.com**, và chọn **Next**.



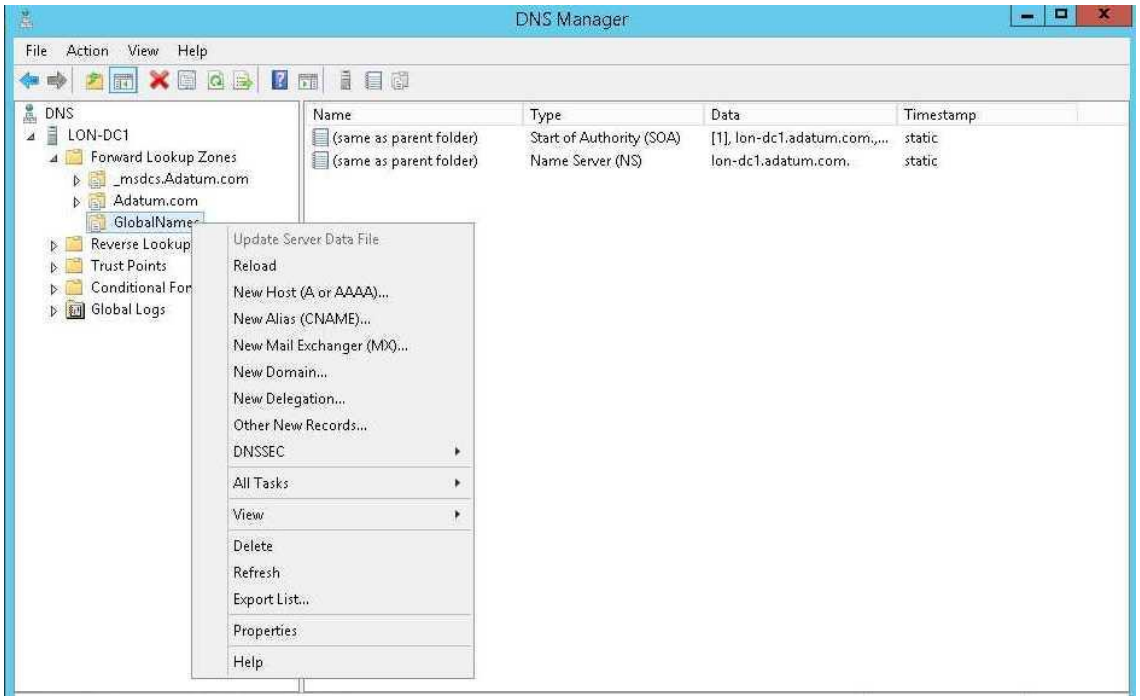
12. Cửa sổ **Zone Name**, nhập tên **GlobalNames** vào ô **Zone name**, chọn **Next**.



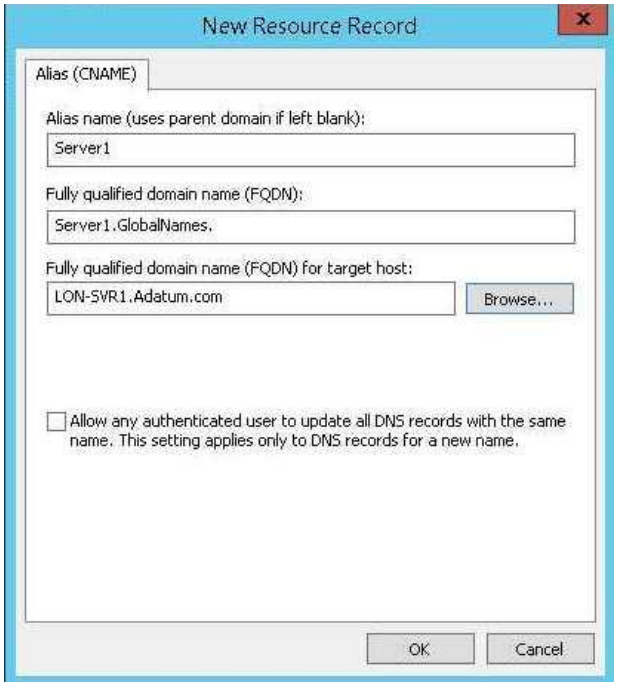
13. Cửa sổ **Dynamic Update**, chọn **Next**, và chọn **Finish**.



14. Trong cửa sổ **DNS Manager**, nhấn chuột phải lên zone **GlobalNames**, chọn **New Alias**.



15. Hộp thoại **New Resource Records,** trong ô **Alias name** nhập **Server1**, trong ô **Fully qualified domain name (FQDN) for the target host**, nhập **lon-svr1.adatum.com**, chọn **OK**.

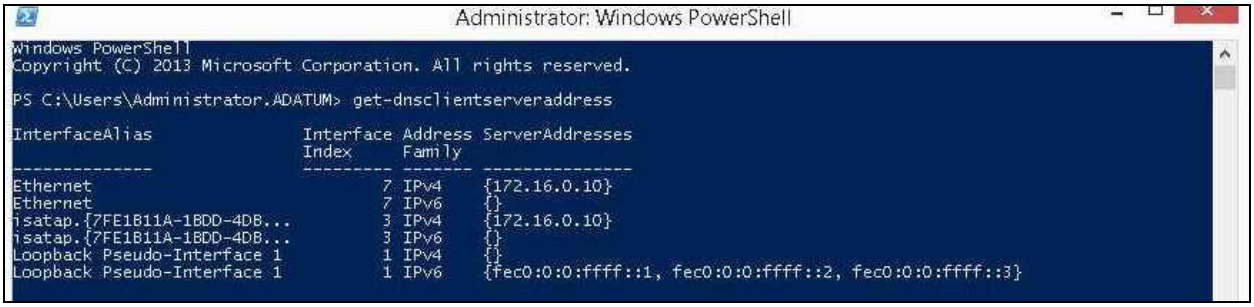


Bước 4: Client kiểm tra phân giải tên.

1. Qua máy **LON-CL1**

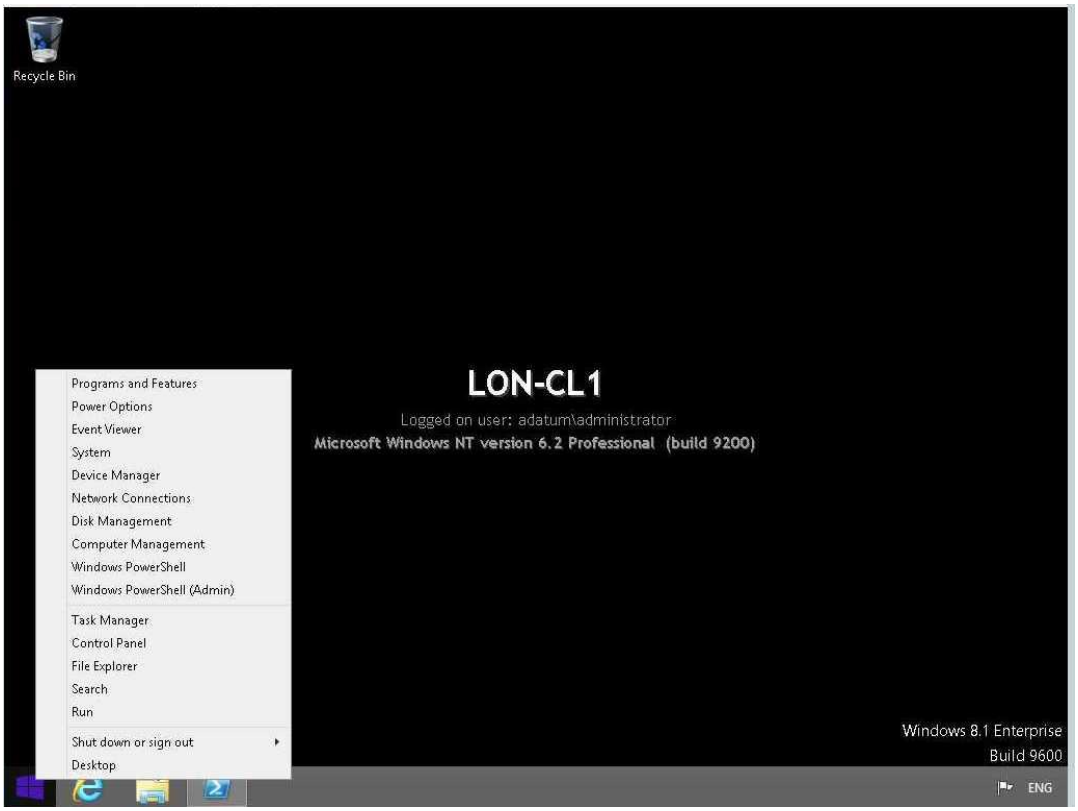
2. Mở **Windows PowerShell**, gõ lệnh:

Get-DnsClientServerAddress

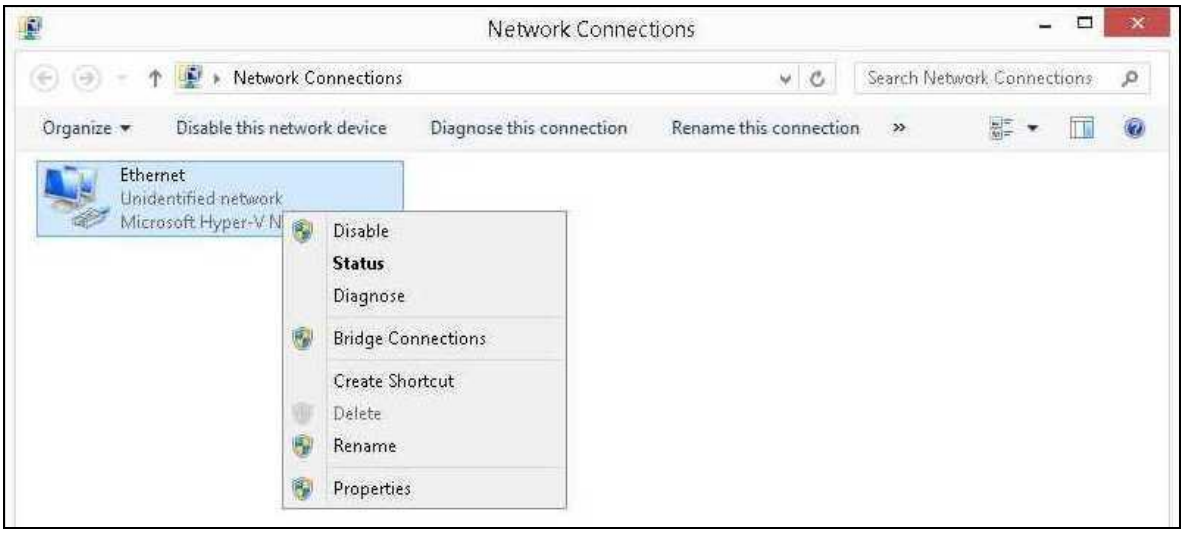


Chú ý: Chỉ có một DNS Server (172.16.0.10) được hiển thị

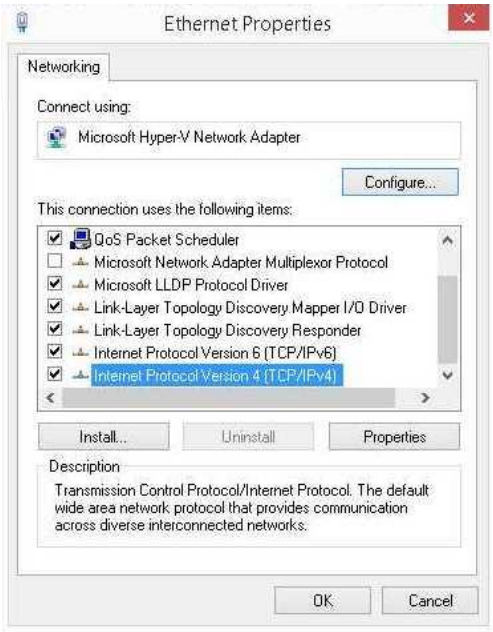
3. Nhấn chuột phải lên Start menu, chọn **Network Connections**.



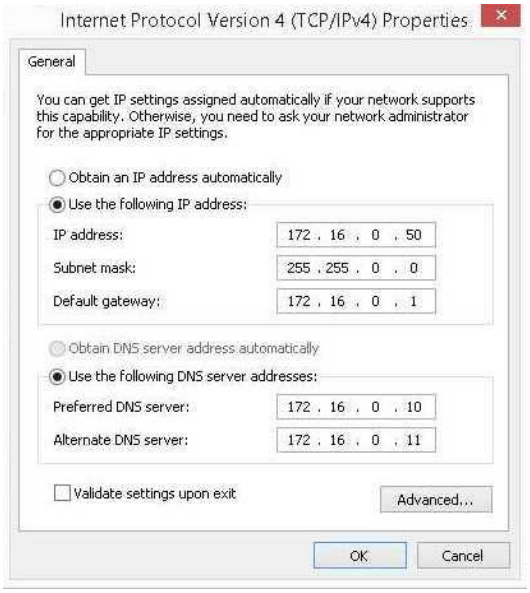
4. Nhấn chuột phải lên card **Ethernet**, chọn **Properties**.



5. Trong hộp thoại **This connection uses the following items**, chọn **Internet Protocol Version 4 (TCPIPv4)**, và chọn **Properties**.



6. Hộp thoại **Internet Protocol Version 4 (TCPIPv4) Properties**, nhập **172.16.0.11** vào ô **Alternate DNS server address**, chọn **OK**, chọn **Close**, tắt **Network Connections**.



7. Quay lại cửa sổ **Windows PowerShell**, gõ lệnh:

Get-DnsClientServerAddress



Chú ý: Bạn sẽ thấy có thêm địa chỉ IP của máy LON-SVR1.

8. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

Get-DnsClientCache



Chú ý: Bạn sẽ thấy DNS Server là **Lon-dc1**, nhưng không có **lon-svr1**.

9. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

Resolve-DnsName LON-SVR1



Chú ý: Kết quả sẽ phân giải được **A** record của **LON-SVR1**.

10. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

Get-DnsClientCache



Chú ý: Bây giờ bạn sẽ thấy tên và địa chỉ của cả 2 DNS Server.

Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai hệ thống DNS thành công.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-CL1**.

Bài 5: Thiết kế và triển khai mô hình Active Directory Forest

I. Mục tiêu:

- Thiết kế mô hình Active Directory Forest.
- Cấu hình Active Directory Forest Trust.

II. Kịch bản:

Hiện tại môi trường Active Directory của công ty A. Datum là một Forest duy nhất, các Domain Controller chạy Windows Server 2008 R2. Tất cả các Domain Controller đều được triển khai tại trụ sở chính ở London.

A. Datum muốn tích hợp hệ thống của công ty Contoso và Trey Research vào hệ thống hiện tại của họ. Contoso hiện đang chạy UNIX, còn Trey Research hiện đang chạy Windows Server 2008 R2 Active Directory.

A. Datum đang có kế hoạch mở rộng số lượng nhân viên tại văn phòng Contoso ở Paris. Lý do là văn phòng ở Paris sẽ đóng vai trò chính trong việc bán hàng, tiếp thị, giao hàng để công ty phát triển mạnh mẽ vào thị trường châu Âu.

Ngoài ra, A. Datum có kế hoạch triển khai một số ứng dụng và dịch vụ cho khách hàng bên ngoài. Những tài nguyên này sẽ được đặt trong một mạng vành đai (perimeter network) , và độc lập với Active Directory của công ty. Tuy nhiên, các quản trị viên cũng sẽ quản lý các tài nguyên trong mạng vành đai.

Khi tích hợp hệ thống của 2 công ty mới vào hệ thống hiện tại, thì yêu cầu quan trọng nhất là sự dễ dàng. Trey Research hiện đang có một Forest duy nhất, cả Contoso và Trey Research hiện đã có hệ thống thư điện tử. Sau khi sát nhập, tất cả người dùng trong các công ty có thể truy cập và sử dụng tài nguyên của toàn bộ hệ thống thông qua một lần chứng thực duy nhất. Yêu cầu thứ hai trong việc tích hợp ba công ty là phải tiết kiệm chi phí.

Tóm tắt thông tin của 3 công ty:

- A. Datum:

- Có một Active Directory Forest duy nhất (Windows Server 2012).
- Có hệ thống Exchange Server
- Mạng vành đai (perimeter network) có Exchange Edge Transport Server

- Trey Research:

- Có một Active Directory Forest duy nhất (Windows Server 2008 R2).
- Schema đã được sửa đổi cho phù hợp với một ứng dụng kinh doanh (LOB).
- Có chuyên môn về việc quản lý Active Directory.
- Phải dược cô lập trong việc quản lý.

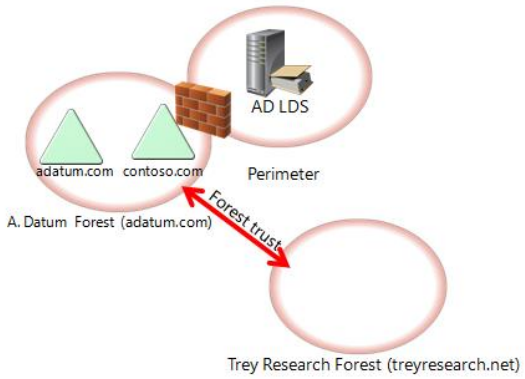
- Contoso:

- Không có Active Directory.
- Không có chuyên môn quản lý Active Directory.
- Ban đầu cần phải được quản lý từ London.
  Không có ứng dụng tích hợp với Active Directory, có khả năng trong tương lai sẽ triển khai Exchange Server (email hiện nay đang sử dụng dịch vụ hosting).

III. Yêu cầu tổng quan:

Thiết kế cơ sở hạ tầng Active Directory cho công ty A. Datum, Trey Research và Contoso theo các yêu cầu sau:

- Thiết kế nên đơn giản.
- Thiết kế phải phản ánh nhu cầu hỗ trợ CNTT của các bộ phận tương ứng.
- Chi phí của việc tái cơ cấu phải được giảm thiểu.
- Hệ thống của Trey Research phải được bảo mật. Điều bắt buộc là chỉ người dùng được ủy quyền mới được truy cập tài nguyên nghiên cứu.



IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-TREY-DC1**
User name	Adatum\Administrator TreyResearch\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**
5. Thực hiên lại bước 2 và 3 cho máy ảo **20413C-TREY-DC1**.
6. Logon vào máy **20413C-TREY-DC1** với thông tin sau:
    - User name: **TreyResearch\Administrator**
    - Password: **Pa$$w0rd**

VI. Thực hành:

Thời gian thực hành: 40 phút

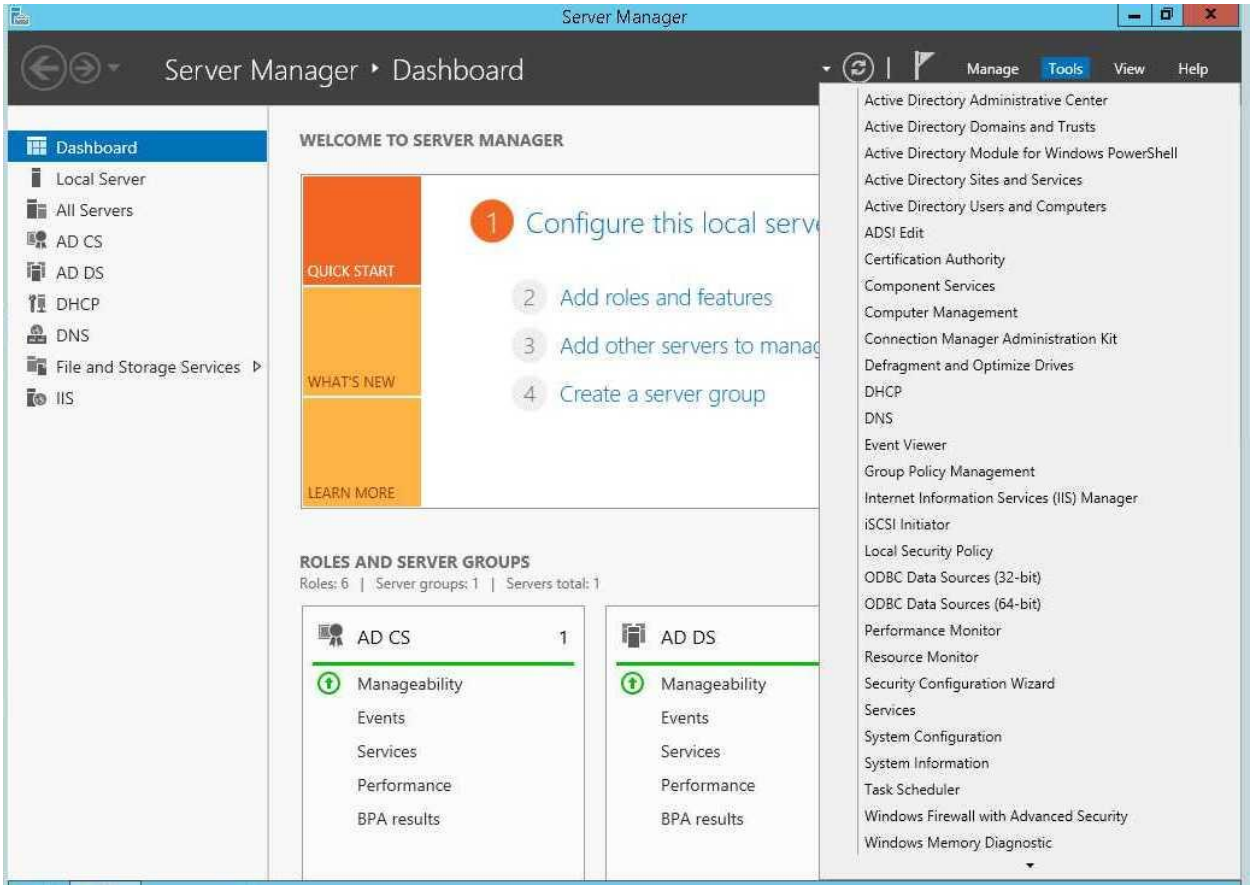
Bài thực hành bao gồm các bước:

1. Cấu hình DNS Conditional Forwarder để hỗ trợ Forest Trust.
2. Tạo Forest Trust giữa A. Datum và Trey Research.
3. Kiểm tra kết quả Forest Trust

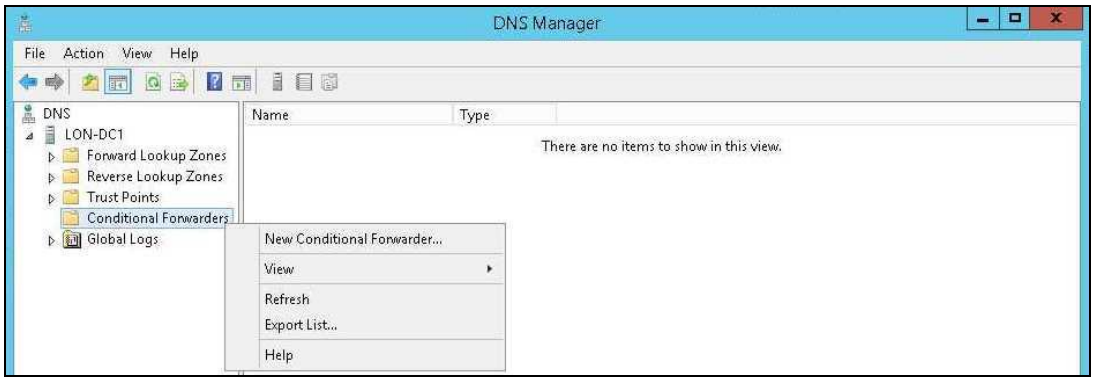
Bước 1. Cấu hình DNS Conditional Forwarder để hỗ trợ Forest Trust.

1. Trên máy **LON-DC1**.

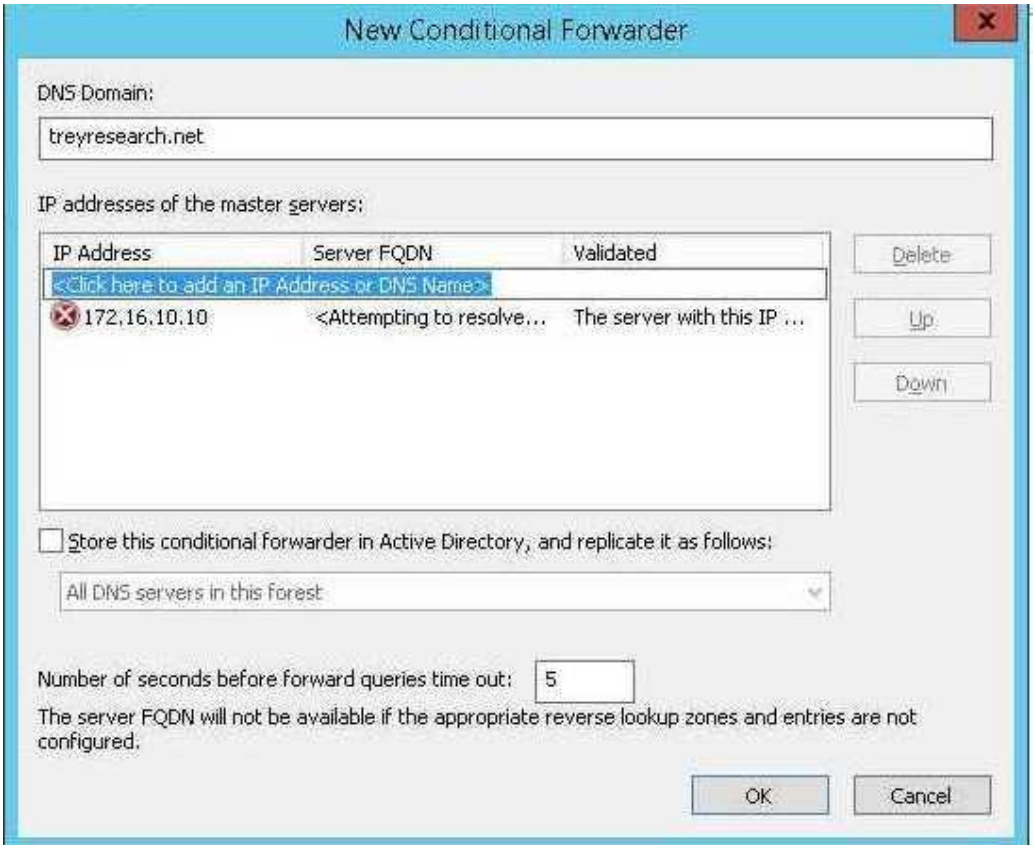
2. Mở **Server Manager**, bung menu **Tools**, mở công cụ **DNS**.



3. Trong cửa sổ **DNS Manager**, bung **LON-DC1**, nhấn chuột phải **Conditional Forwarders**, chọn **New Conditional Forwarder**.



4. Hộp thoại **New Conditional Forwarder**, nhập **treyresearch.net** vào ô **DNS Domain**, nhập **172.16.10.10** vào ô **IP Address**, nhấn phím **Enter**, và chọn **OK**.



5. Bung **Start** menu, gõ **cmd.exe**, nhấn phím **Enter**.

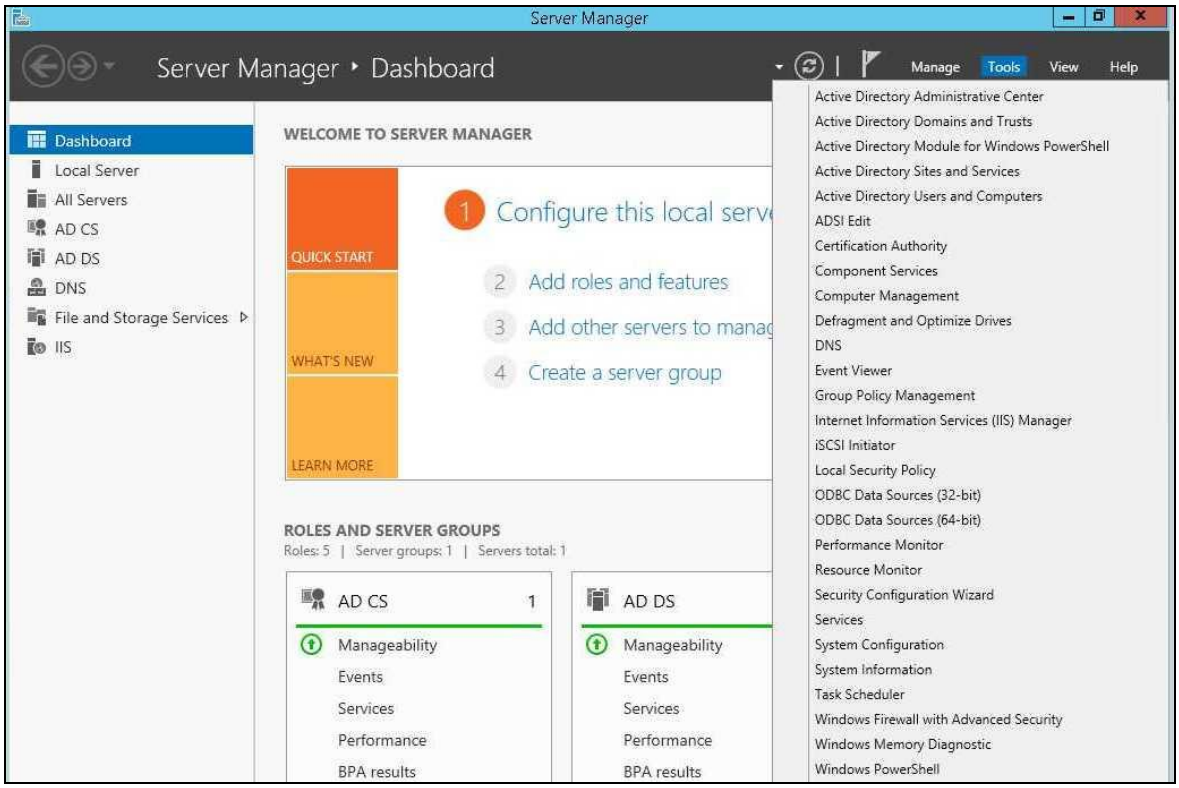
6. Trong command prompt, gõ lệnh: **nslookup trey-dc1.treyresearch.net**

7. Kiểm tra phân giải thành công, **trey-dc1.treyresearch.net** có IP tương ứng **172.16.10.10.**

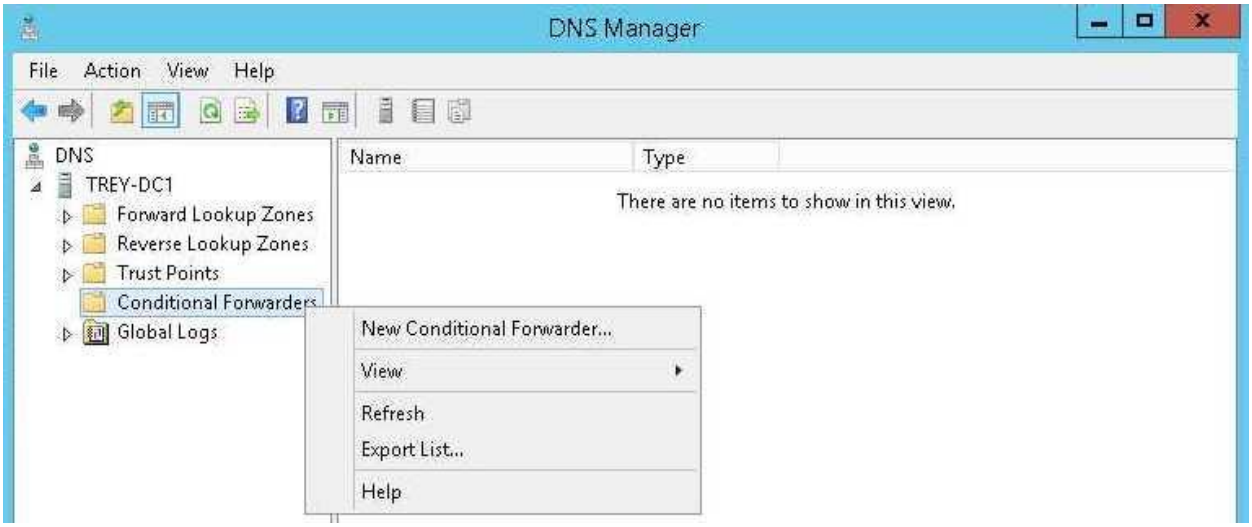


8. Qua máy **TREY-DC1**.

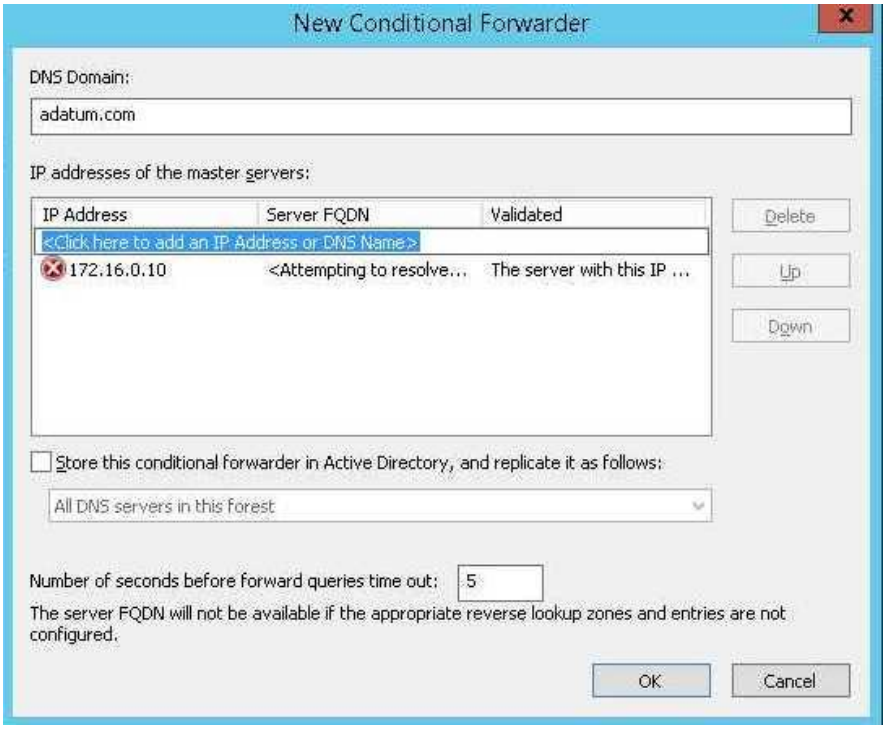
9. Mở **Server Manager**, bung menu **Tools**, mở công cụ **DNS**.



10. Trong cửa sổ **DNS Manager**, bung **LON-DC1**, nhấn chuột phải **Conditional Forwarders**, chọn **New Conditional Forwarder**.



11. Hộp thoại **New Conditional Forwarder**, nhập **Adatum.com** vào ô **DNS Domain**, nhập **172.16.0.10** vào ô **IP Address**, nhấn phím **Enter**, và chọn **OK**.



12. Bung **Start** menu, gõ **cmd.exe**, nhấn phím **Enter**.

13. Trong command prompt, gõ lệnh: **nslookup lon-svr1.adatum.com**

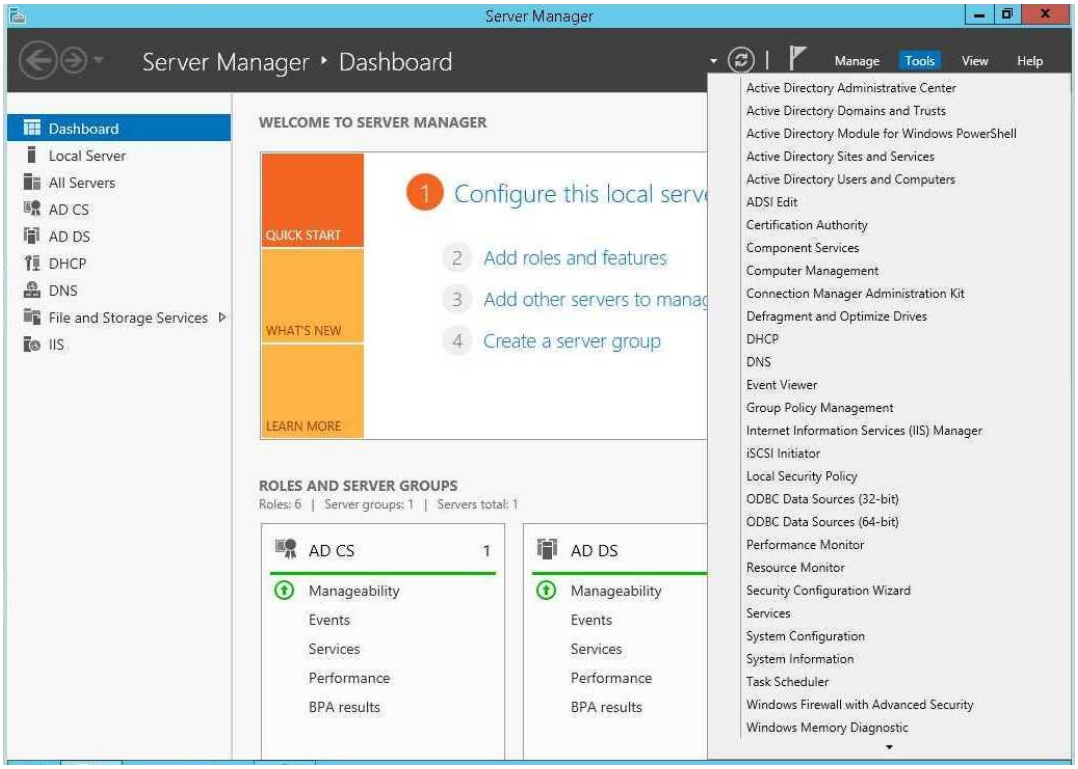
14. Kiểm tra phân giải thành công, **lon-svr1.adatum.com** có IP tương ứng **172.16.0.11.**



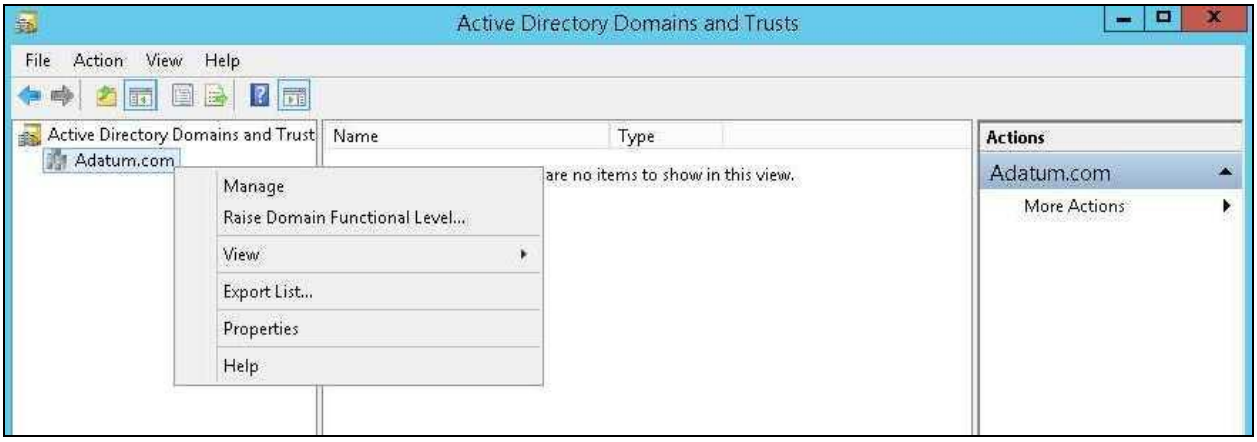
Bước 2. Tạo Forest Trust giữa A. Datum và Trey Research.

1. Qua máy **LON-DC1**.

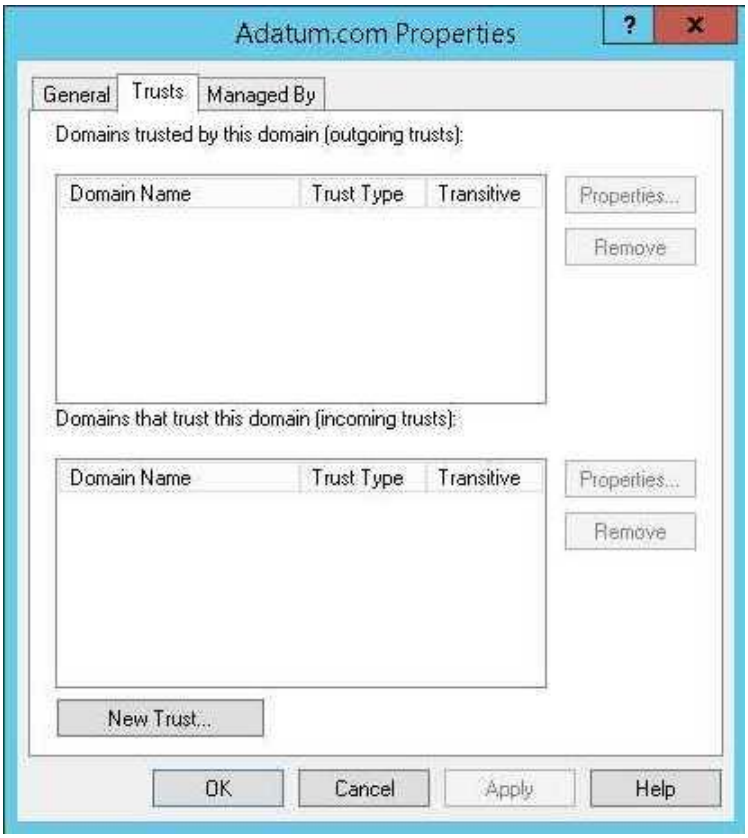
2. Mở **Server Manager**, bung menu **Tools**, mở **Active Directory Domains and Trusts**.



3. Trong cửa sổ **Active Directory Domains and Trusts**, nhấn chuột phải **Adatum.com**, chọn **Properties**.



4. Trong hộp thoại **Adatum.com Properties**, qua tab **Trusts**, chọn **New Trust**.



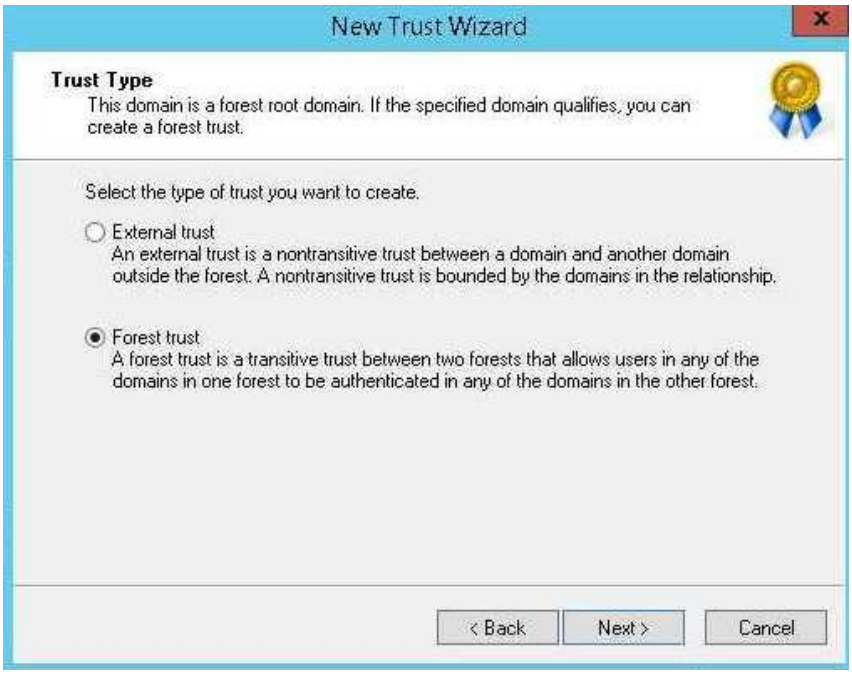
5. Cửa sổ **Welcome**, chọn **Next**.



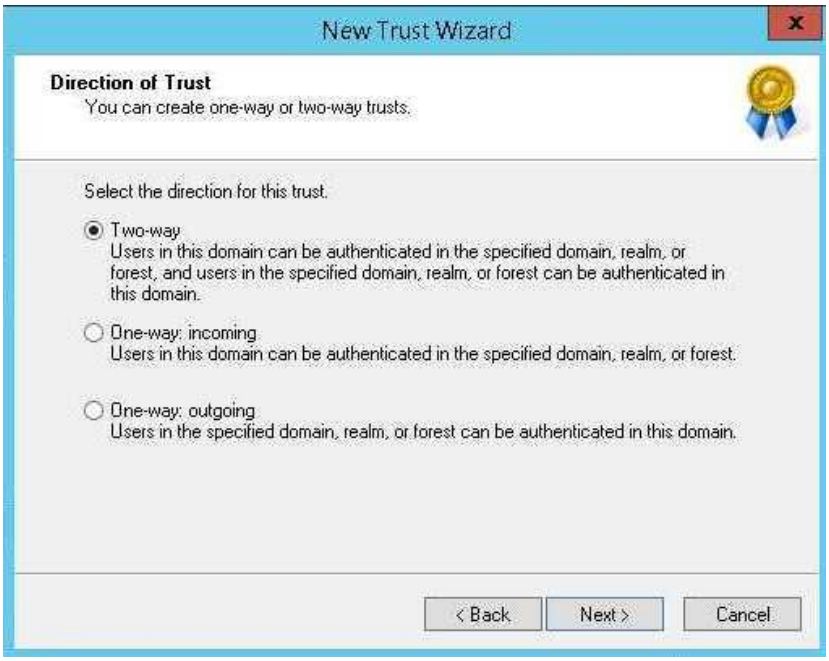
6. Cửa sổ **Trust Name**, nhập **treyresearch.net** vào ô **Name**, chọn **Next**.



7. Cửa sổ **Trust Type**, chọn **Forest trust**, và chọn **Next**.



8. Cửa sổ **Direction of Trust**, chọn **Two-way**, và chọn **Next**.



9. Cửa sổ **Sides of Trust**, chọn **Both this domain and the specified domain**, chọn **Next**.



10. Cửa sổ **User Name and Password**, nhập thông tin như bên dưới, sau đó chọn Next:

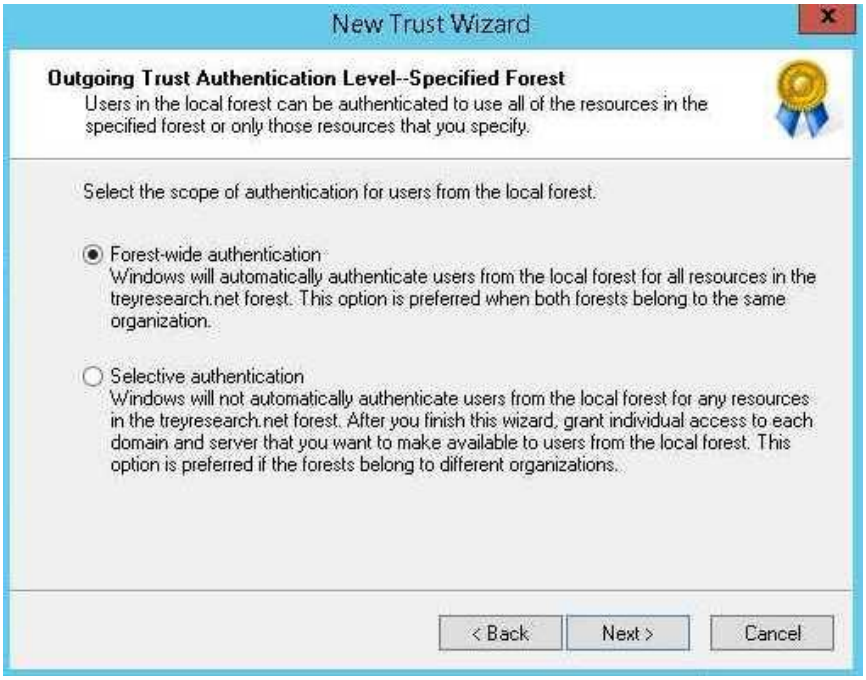
- **User name: Treyresearch\administrator**.
- **Password**: **Pa$$w0rd**



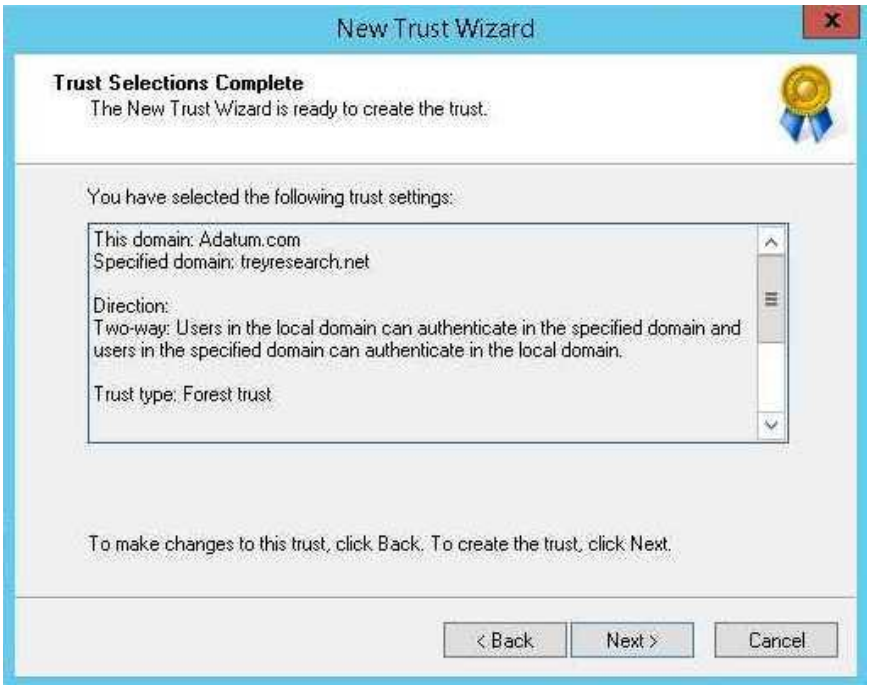
11. Cửa sổ **Outgoing Trust Authentication Level--Local Forest**, chọn **Next**.



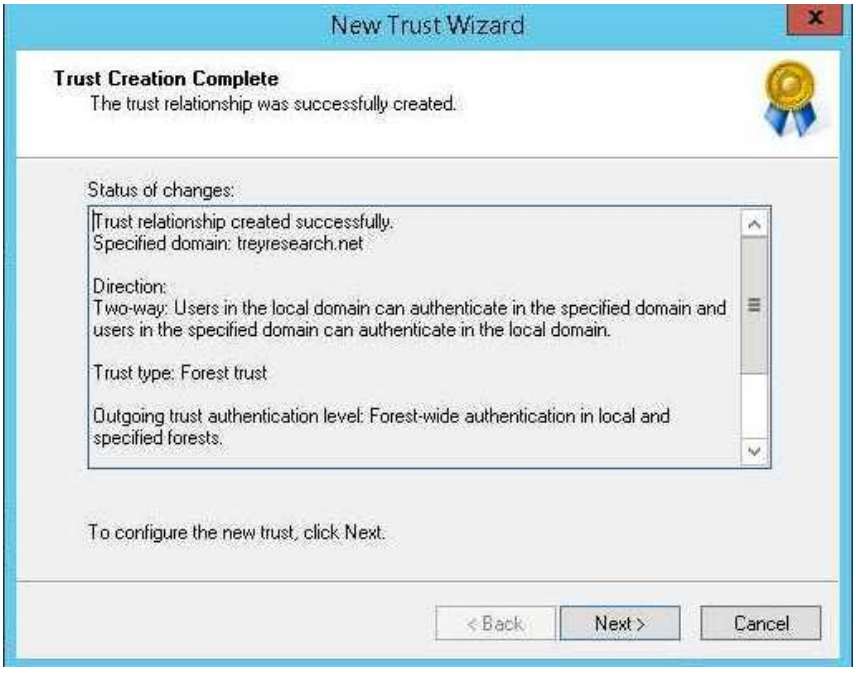
12. Cửa sổ **Outgoing Trust Authentication Level--Specified Forest**, chọn **Next**.



13. Cửa sổ **Trust Selections Complete**, chọn **Next**.



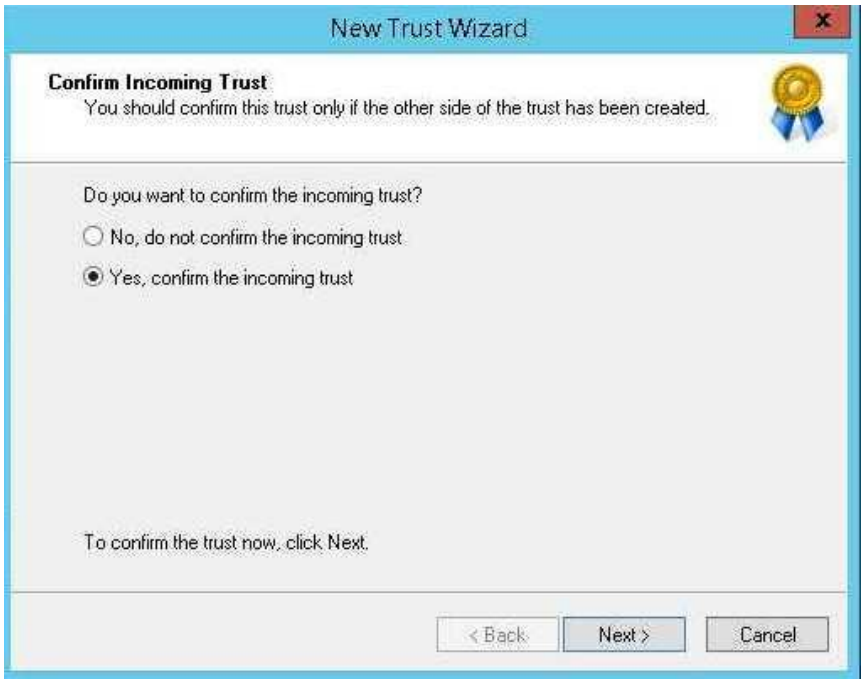
14. Cửa sổ **Trust Creation Complete**, chọn **Next**.



15. Cửa sổ **Confirm Outgoing Trust**, chọn **Yes, confirm the outgoing trust**, và chọn **Next**.



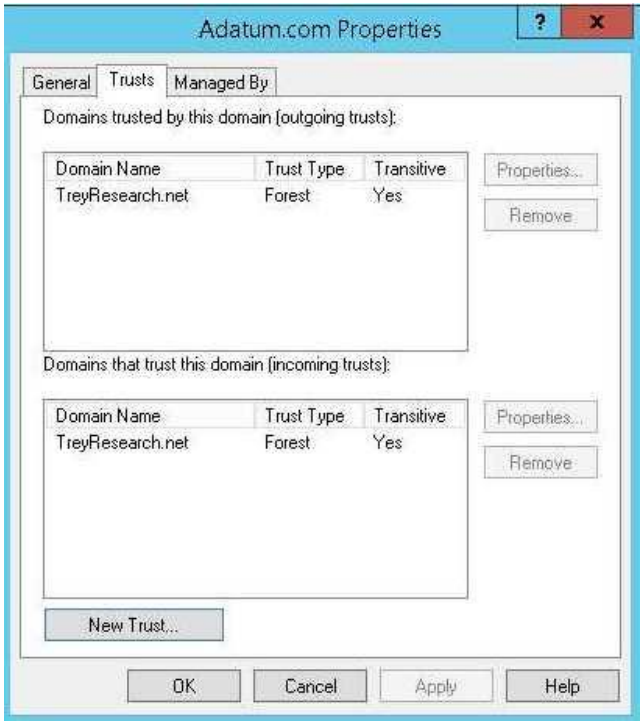
16. Cửa sổ **Confirm Incoming Trust**, chọn **Yes, confirm the incoming trust**, và chọn **Next**.



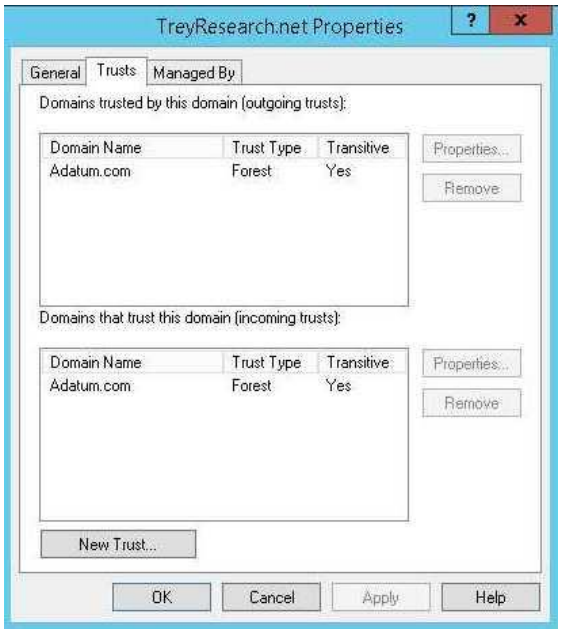
17. Cửa sổ **Completing the New Trust Wizard**, chọn **Finish**.



18. Hộp thoại **Adatum.com Properties**, chọn **OK**.



19. Tương tự, qua máy **TREY-DC1**, mở **Active Directory Domains and Trusts**, nhấn chuột phải **TreyResearch.net** chọn **Properties**, qua tab **Trust**, kiểm tra đã có trust với domain **Adatum.com**

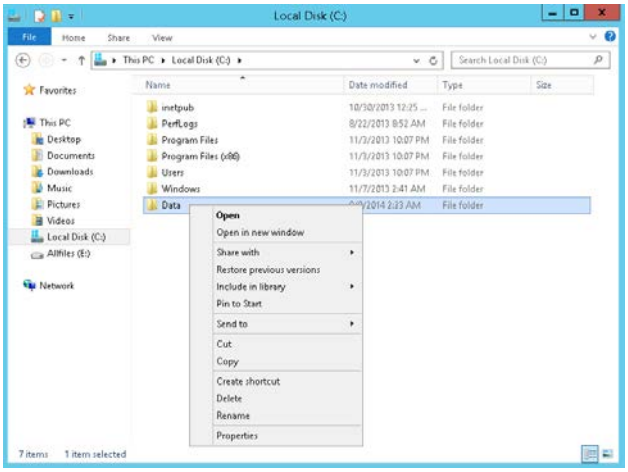


Bước 3: Kiểm tra kết quả Forest Trust

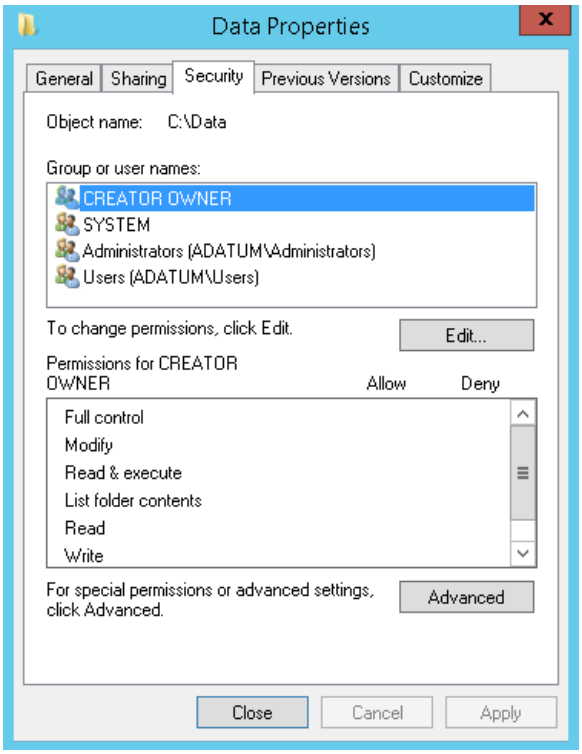
1. Qua máy **LON-DC1**.

2. Mở **File Explorer**, vào ổ đĩa **C:**, tạo folder mới, đặt tên **Data**

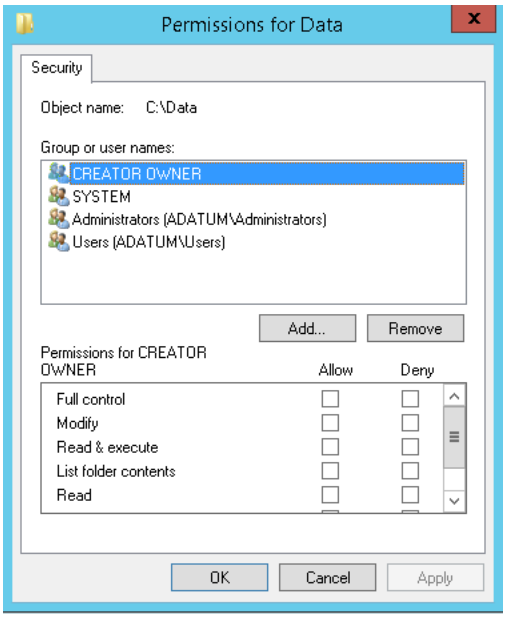
3. Nhấn chuột phải folder **Data**, chọn **Properties**.



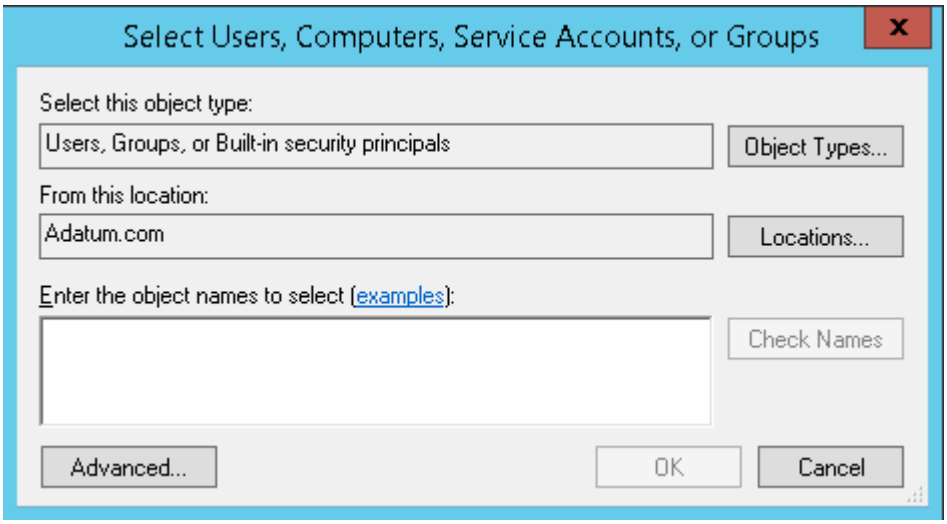
4. Trong hộp thoại **Data Properties**, qua tab **Security**, chọn **Edit**



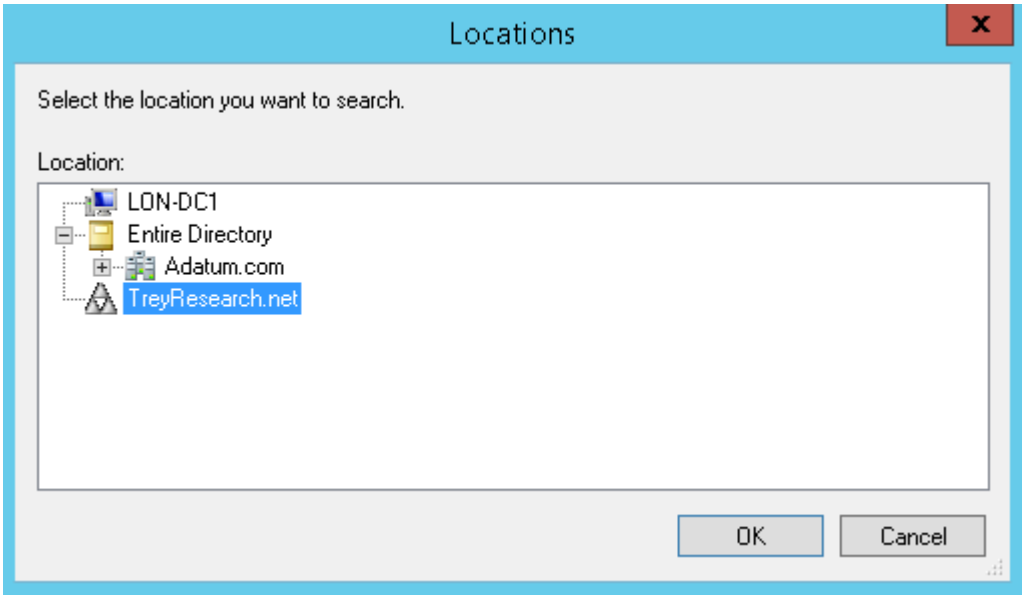
5. Trong hộp thoại, **Permission for Data**, chọn **Add**



6. Hộp thoại **Select Users**, chọn **Locations**

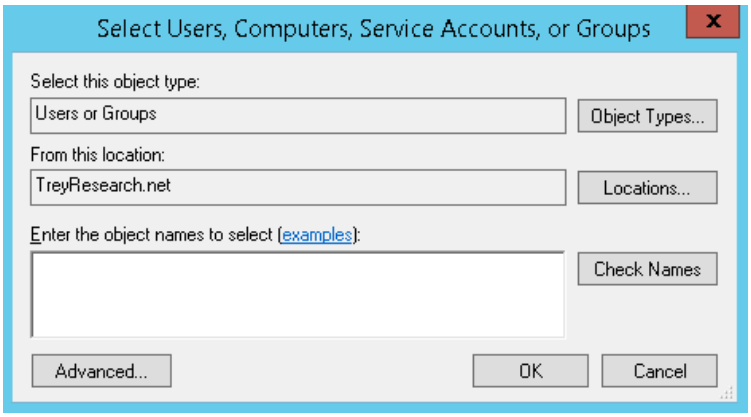


7. Hộp thoại **Location**, chọn forest **TreyResearch.net,** chọn **OK**

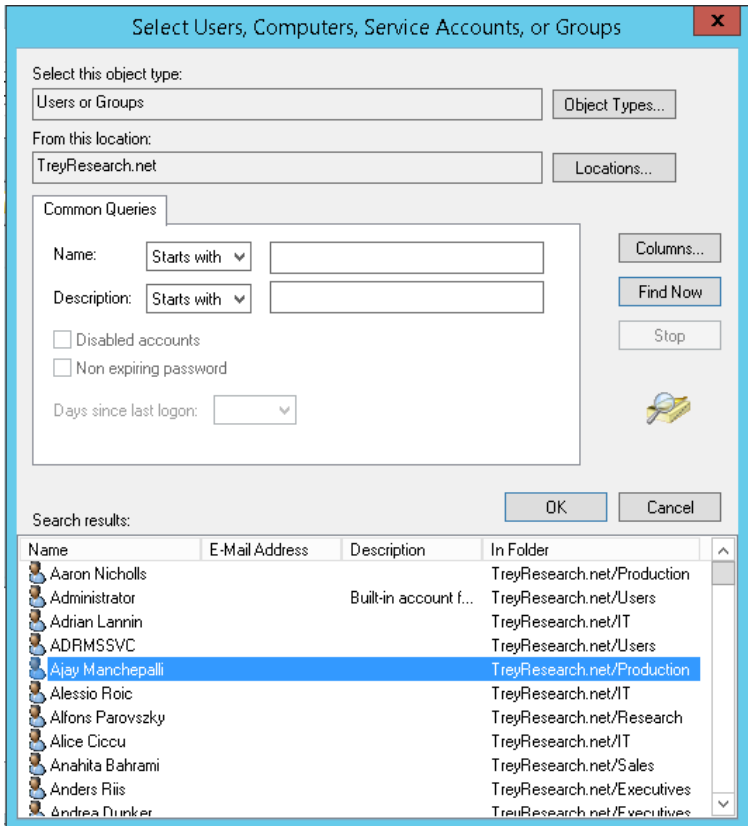


Chú ý: Sau khi cấu hình Forest Trust thành công thì forest TreyResearch.net mới được hiển thị trong hộp thoại Location.

8. Hộp thoại **Select Users**, chọn **Advanced**



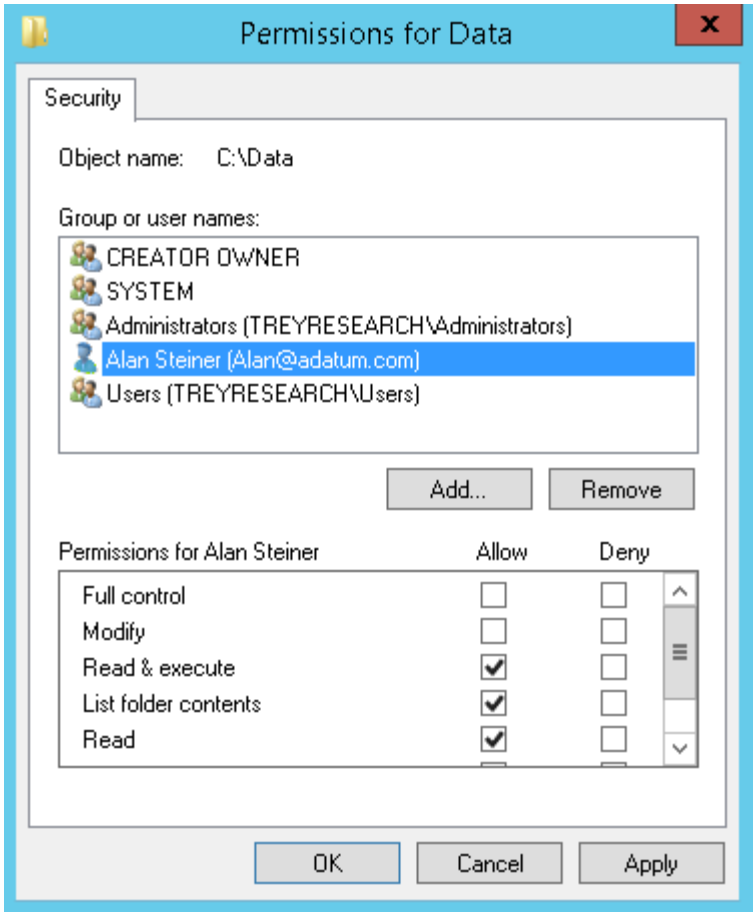
9. Hộp thoại **Select Users**, chọn **Find Now**



Chú ý: Các users và groups của forest TreyResearch.net đã được hiển thị.

Kết quả: Chúng ta đã cấp quyền được cho user của TreyResearch.net trên tài nguyên của Adatum.com, nói cách khác user của TreyResearch.net có thể truy cập tài nguyên của Adatum.com với cơ chế chứng thực Single Sign On

10. Tương tự, trên máy **TREY-DC1**, thực hiện lại từ bước 1 đến 9



Kết quả: Chúng ta đã cấp quyền được cho user của Adatum.com trên tài nguyên của TreyResearch.net, nói cách khác user của TreyResearch.net có thể truy cập tài nguyên của Adatum.com với cơ chế chứng thực Single Sign On.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-TREY-DC1**.

Bài 6: Thiết kế và triển khai mô hình Active Directory Domain

I. Mục tiêu:

- Thiết kế mô hình Active Directory Domain.
- Triển khai mô hình Active Directory có nhiều Domain Tree.

II. Kịch bản:

Trong quá trình thiết kế mô hình Active Directory Forest cho công ty A. Datum, các thành viên trong nhóm thiết kế đã quyết định rằng họ cần phải duy trì một Forest riêng biệt là treyresearch.net để đáp ứng yêu cầu cách ly bộ phận nghiên cứu của công ty Trey Research. Tuy nhiên, đội ngũ thiết kế hiện đang xem xét cách thức tốt nhất để tích hợp hệ thống của công ty Contoso vào cơ sở hạ tầng của A. Datum. Tại thời điểm này, Contoso chưa triển khai AD DS.

Công ty Contoso có trụ sở duy nhất tại Paris, và là một đối tác cũ của công ty A. Datum. Mục tiêu chính trong việc mua Contoso là để tích hợp hai dòng sản phẩm của công ty. Bạn phải xem xét kịch bản và quyết định cách tốt nhất để triển khai AD DS cho Contoso, và làm thế nào để tích hợp hệ thống của Contoso vào hệ thống hiện tại của A. Datum.

Các thông tin khác:

- Datum đang có kế hoạch thuê thêm một số lượng lớn nhân viên khác ở Paris. Những nhân viên mới sẽ làm việc trong phòng bán hàng, tiếp thị, phân phối tại Paris.
- Nhân viên IT của Contoso không có kinh nghiệm quản trị Active Directory, mặc dù nhân viên của công ty đã được huấn luyện cho việc này.
- Văn phòng Paris và London được kết nối bởi một đường truyền có tốc độ 6Mbps, được sử dụng cho tất cả các thông tin liên lạc và chia sẻ dữ liệu. Nhóm IT tại A. Datum quan tâm đến việc sử dụng băng thông giữa Paris và London.
- A. Datum đã triển khai giải pháp VoIP và hội nghị trực tuyến bằng Lync Server 2010, và đang có kế hoạch mở rộng triển khai cho các server của London. Nhóm IT mong muốn rằng hệ thống Active Directory mới phải sử dụng ít băng thông nhất có thể trong việc đồng bộ dữ liệu AD DS.

III. Yêu cầu tổng quan:

Thiết kế một mô hình Active Directory Domains để hỗ trợ các mục tiêu sau đây:

- Nhân viên bán hàng, tiếp thị, và các nhóm sản xuất tại hai công ty sẽ hợp tác chặt chẽ với nhau, và họ phải có khả năng chia sẻ thông tin dễ dàng.
- Người sử dụng trong cả hai công ty A. Datum và Contoso phải có khả năng truy cập một số thông tin trong forest Adatum.com. Ngoài ra, họ phải có khả năng truy cập vào hộp thư người dùng (User Mailbox) trên các máy chủ Exchange được triển khai ở London, và các dữ liệu trên File Server (LON-SVR1) ở London. Người sử dụng phải sử dụng một tài khoản đăng nhập duy nhất để truy cập các tài nguyên và dịch vụ trong hệ thống.
- Một số người dùng của Contoso yêu cầu được phép truy cập đến các tài nguyên của Trey Research. Kế hoạch của bạn là phải tạo điều kiện cho việc này. Giải pháp này không thỏa yêu cầu bảo mật của forest Treyresearch.net.

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-CON-SVR**
User name	Adatum\Administrator Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.

2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.

3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.

4. Logon vào máy **20413C-LON-DC1** với thông tin sau:

   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**

5. Thực hiên lại bước 2 và 3 cho máy ảo **20413C-CON-SVR**.

6. Logon vào máy **20413C-CON-SVR** với thông tin sau:

- User name: **Administrator**
- Password: **Pa$$w0rd**

VI. Thực hành:

Thời gian thực hành: 45 phút

Bài thực hành bao gồm các bước:

1. Cài đặt Active Directoy Domain Services.

2. Cấu hình **CON-SVR** làm Domain Controller của Domain Tree mới trong Forest đang có.

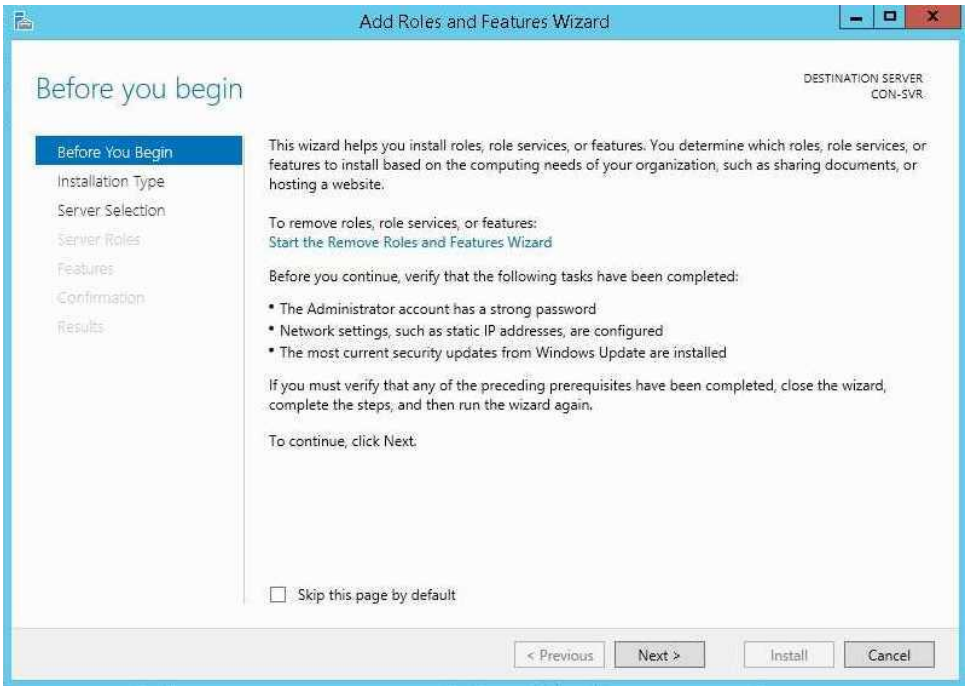
Bước 1. Cài đặt Active Directoy Domain Services.

1. Vào máy **CON-SVR.**

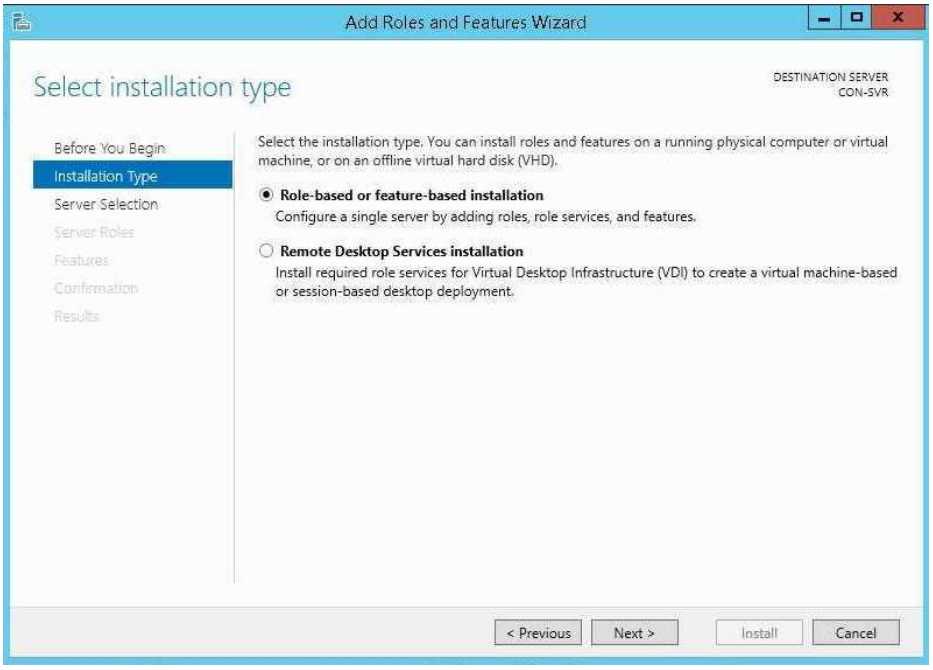
2. Mở **Server Manager**, chọn **Add roles and features**.



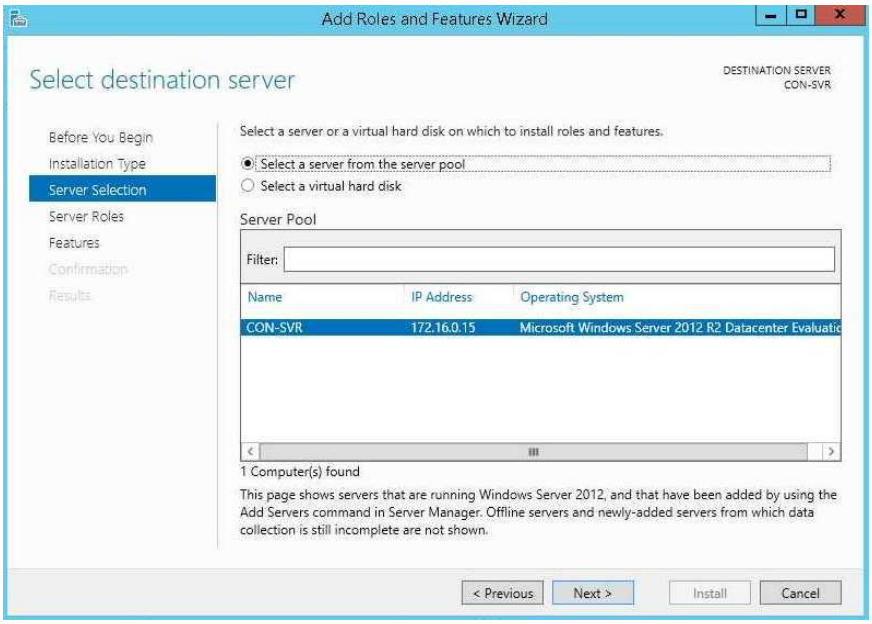
3. Trong cửa sổ **Before you begin**, chọn **Next**.



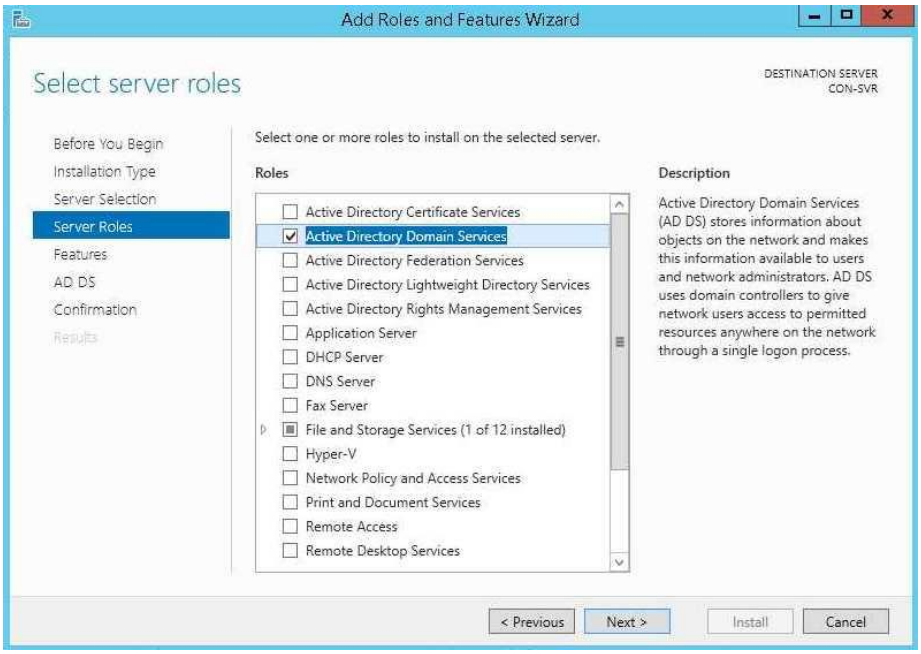
4. Cửa sổ **Select installation type**, chọn **Next**.



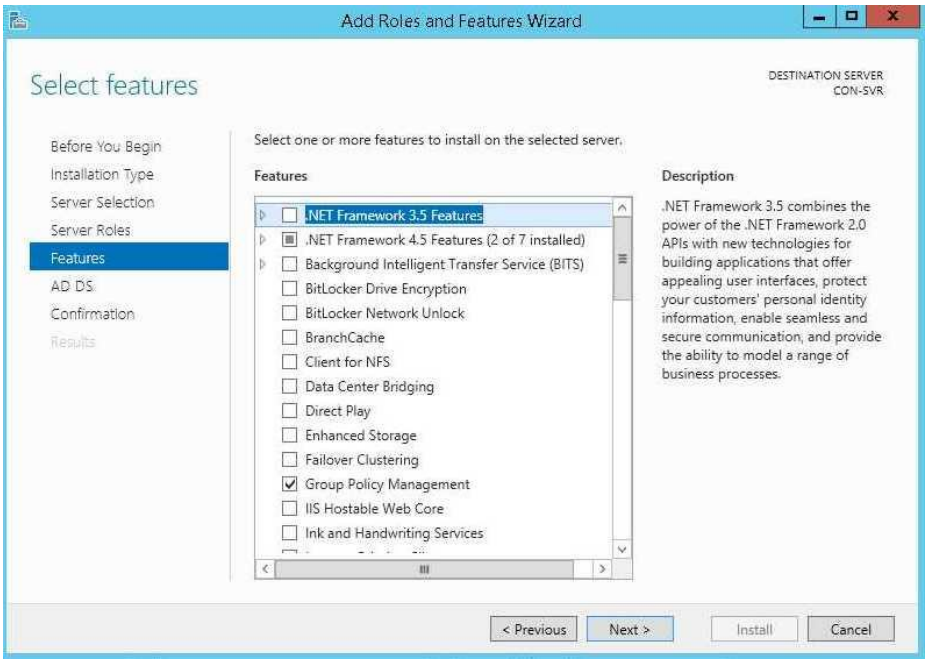
5. Cửa sổ **Select destination server**, chọn **Next**.



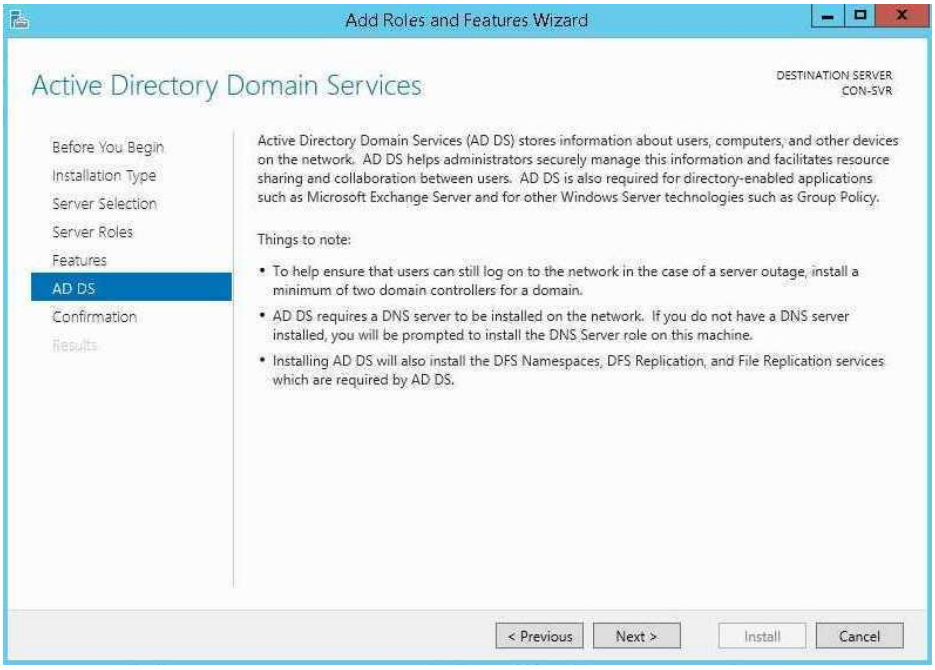
6. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Domain Services**, chọn **Add Features**, chọn **Next**.



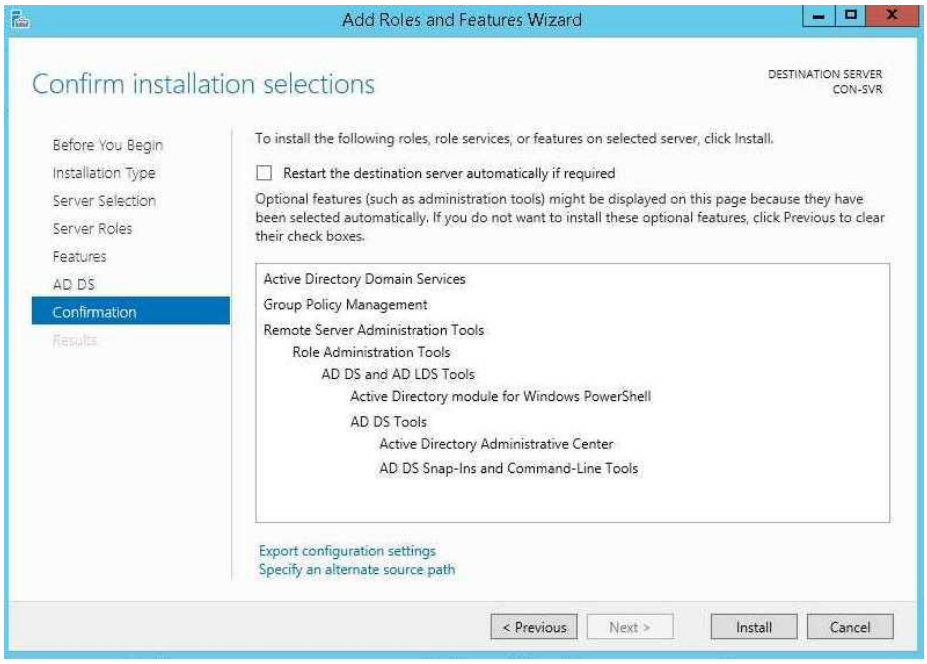
7. Cửa sổ **Select features**, chọn **Next**.



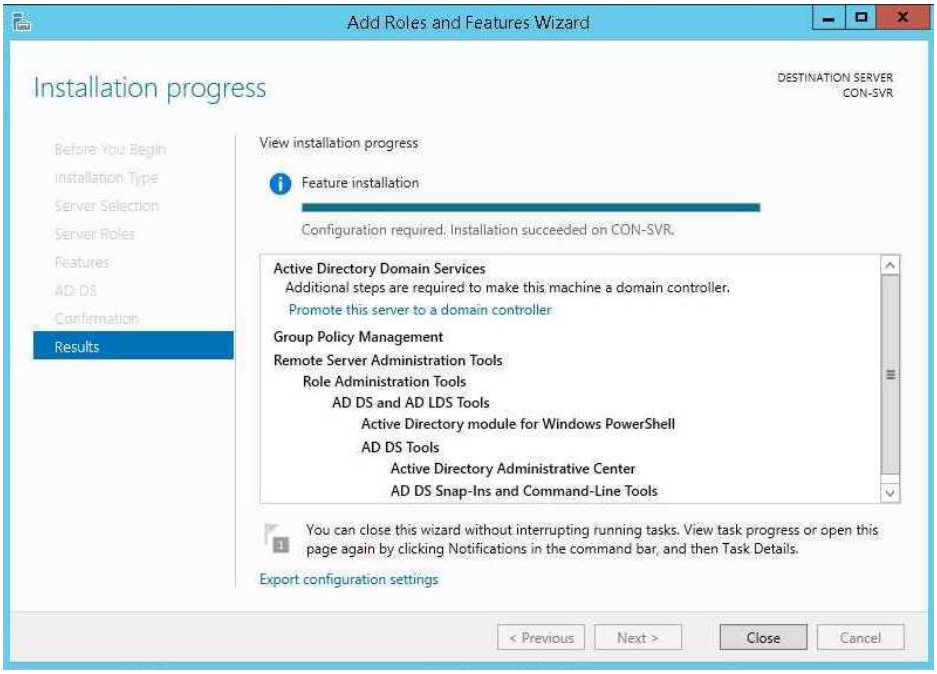
8. Cửa sổ **Active Directory Domain Services**, chọn **Next**.



9. Cửa sổ **Confirm installation selections**, chọn **Install**.

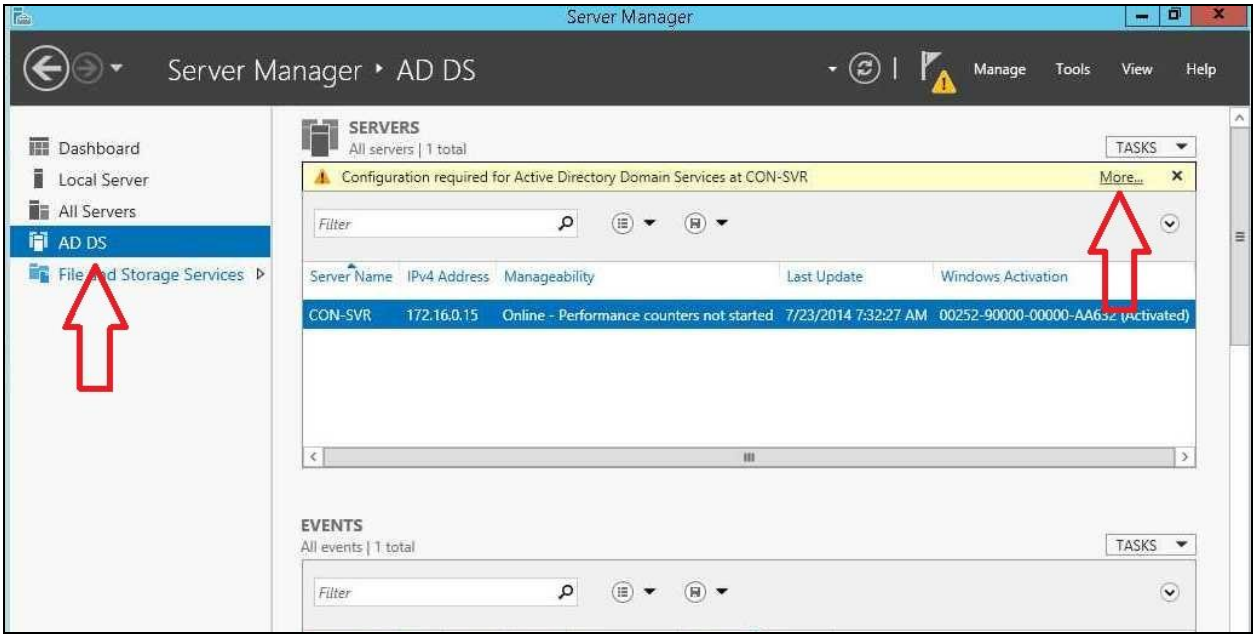


10. Sau khi cài đặt thành công, chọn **Close**.

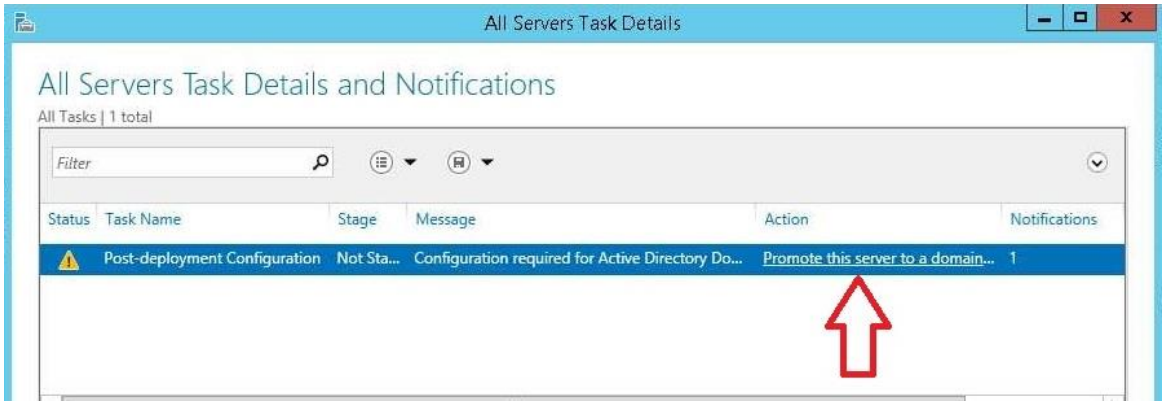


Bước 2. Cấu hình CON-SVR làm Domain Controller của Domain Tree mới trong Forest đang có.

1. Trên máy **CON-SVR**, trong cửa sổ **Server Manager**, chọn **AD DS**, và chọn **More**.



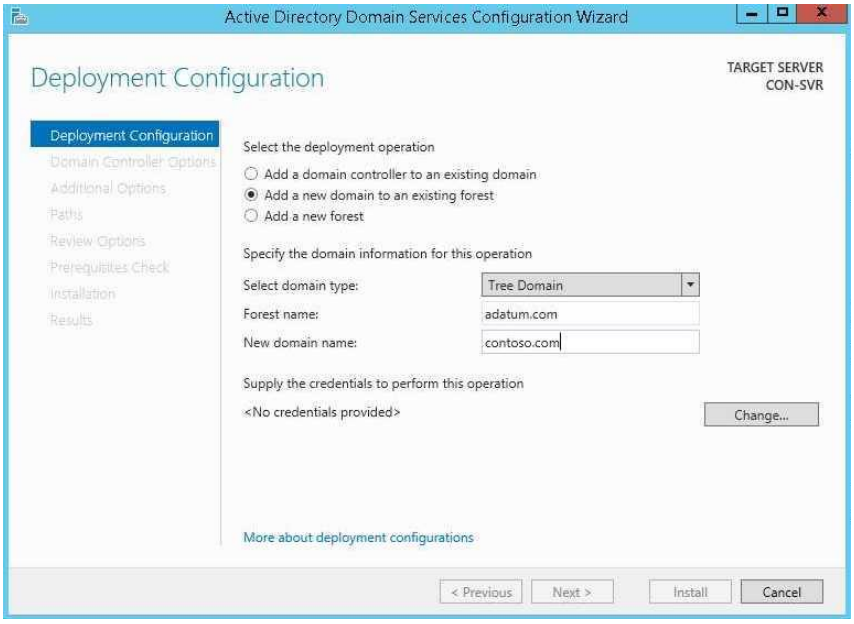
2. Trong hộp thoại **All Servers Task Details and Notifications**, chọn **Promote this server to a domain controller**.



3. Trong cửa sổ **Deployment Configuration**, chọn **Add a new domain to an existing forest**. Khai báo thông tin như sau:

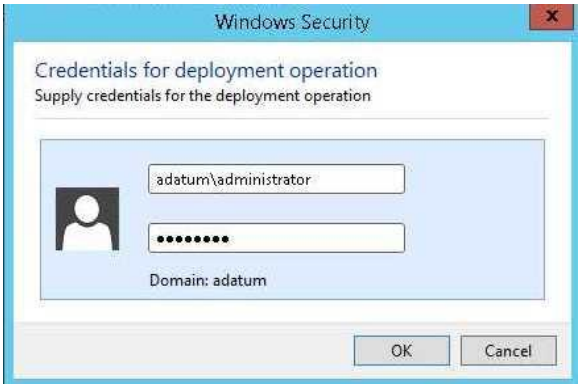
- **Select domain type**: Tree Domain.
- **Forest name**: adatum.com
- **New domain name**: contoso.com

Và chọn **Change**.

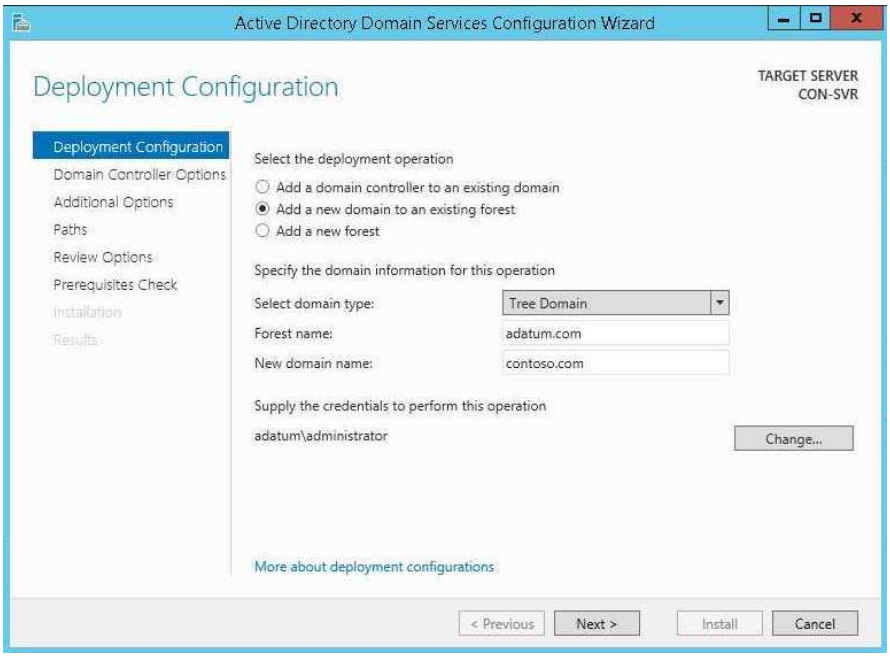


4. Hộp thoại **Windows Security**, nhập thông tinh như bên dưới, và chọn **OK**

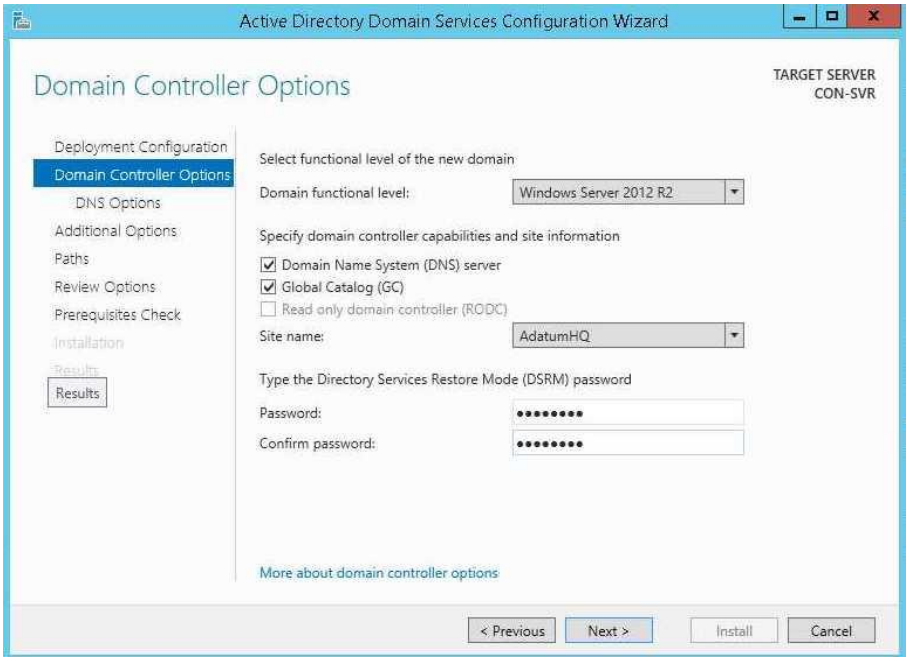
- **User name**: Adatum\Administrator
- **Password**: Pa$$w0rd



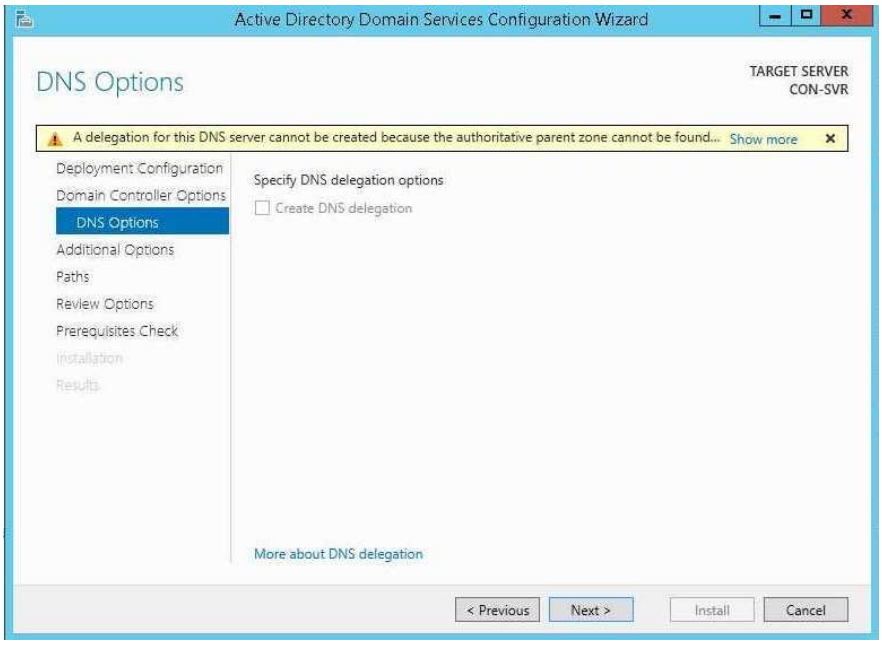
5. Cửa sổ **Deployment Configuration,** chọn **Next**



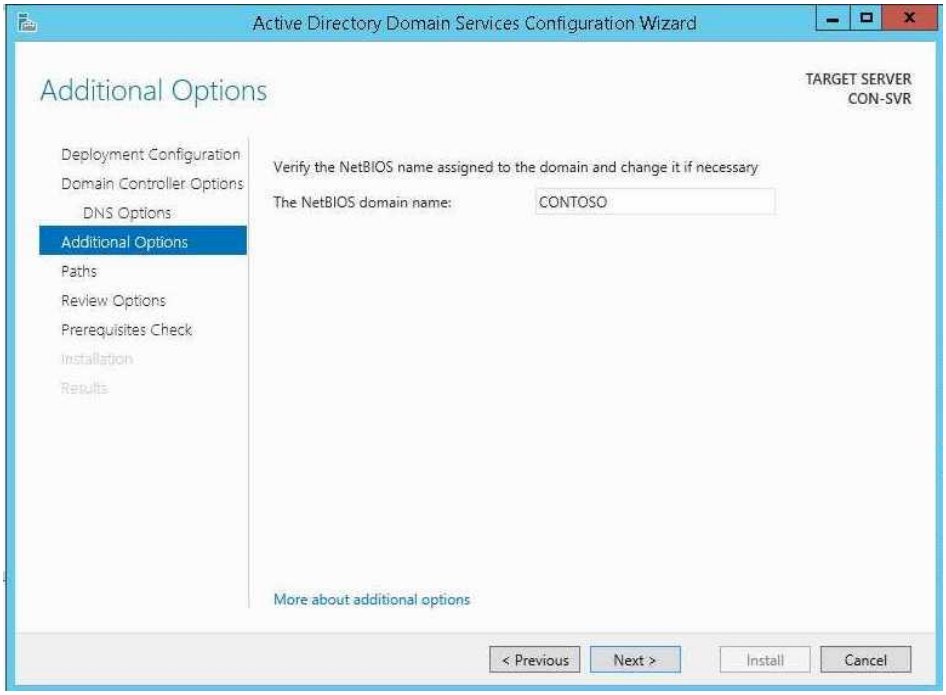
6. Cửa sổ **Domain Controller Options**, trong ô **Password** và **Confirm password**, nhập **Pa$$w0rd**, chọn **Next**.



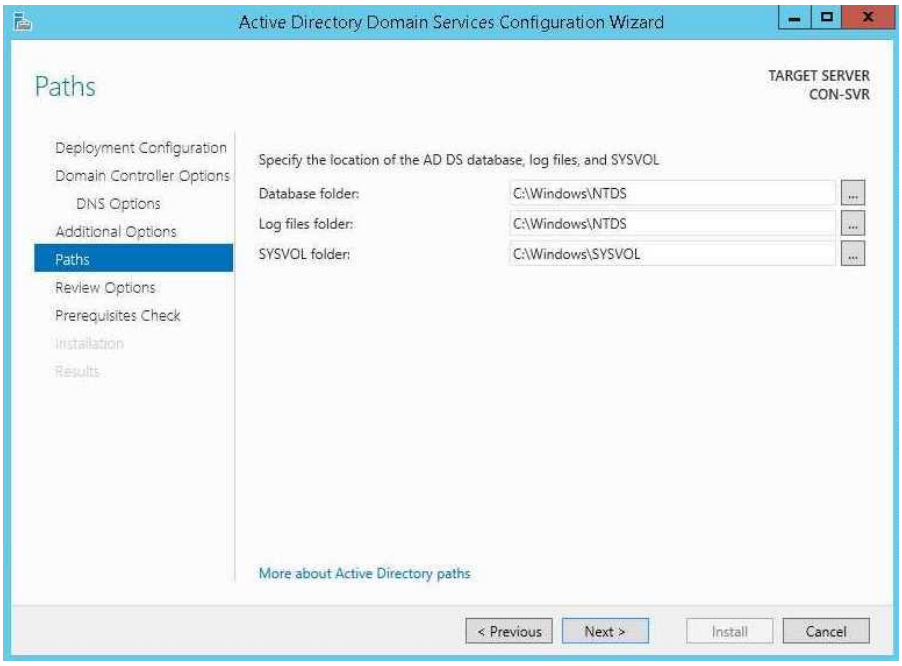
7. Cửa sổ **DNS Options**, chọn **Next**.



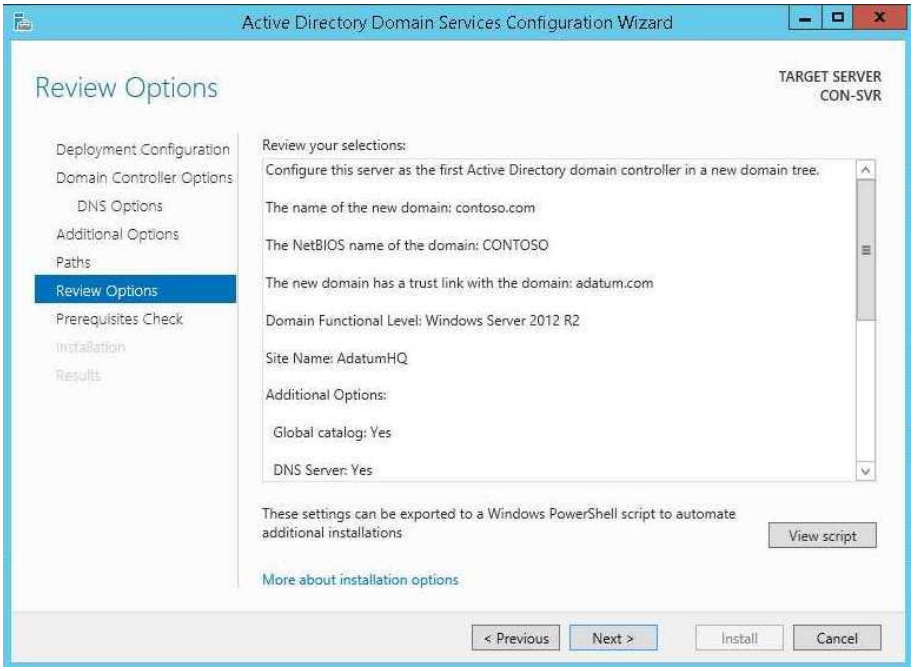
8. Cửa sổ **Additional Options**, chọn **Next**.



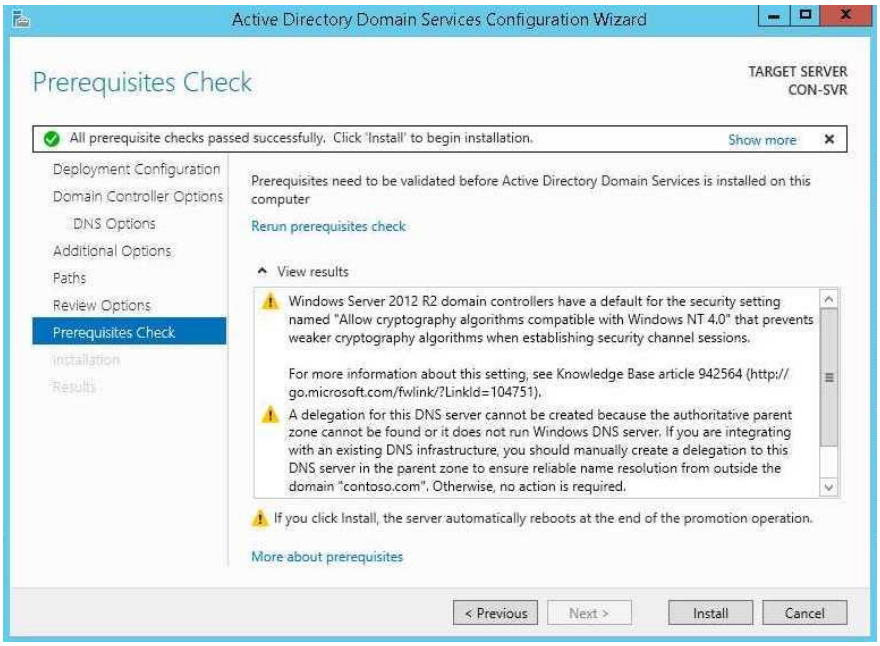
9. Cửa sổ **Paths**, chọn **Next**.



10. Cửa sổ **Review Options**, chọn **Next**.



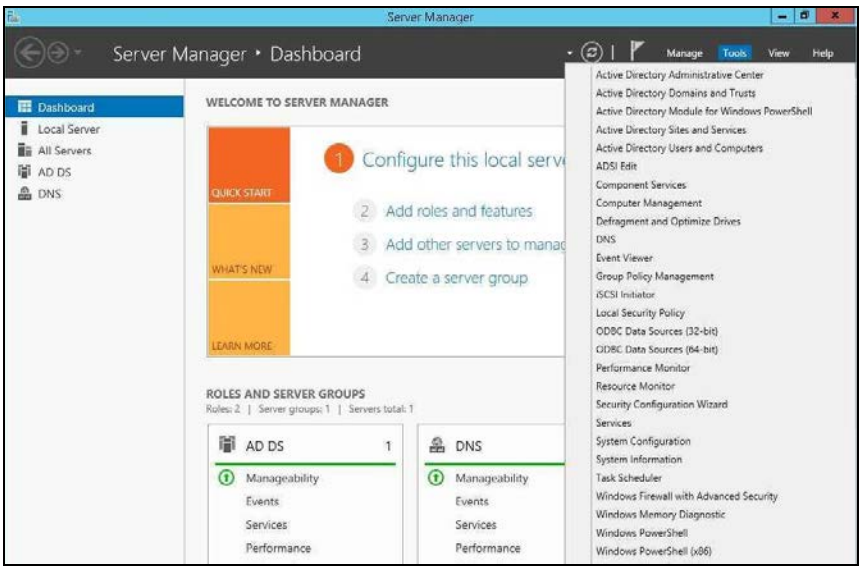
11. Cửa sổ **Prerequisites Check**, chọn **Install**.



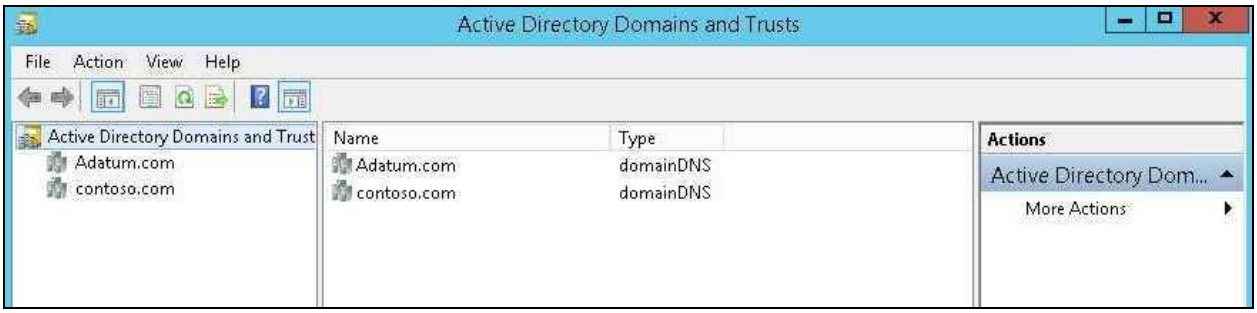
13. Khi **CON-SVR** khởi động thành công, logon bằng tài khoản:

- User name: **Contoso\Administrator**
- Password: **Pa$$w0rd**.

13. Trong **Server Manager**, bung menu **Tool**, mở **Active Directory Domains and Trusts**



14. Kiểm tra trong forest có thêm domain tree mới - **Contoso.com**



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công mô hình Active Directory có nhiều tree.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-CON-SVR**.

Bài 7: Thiết kế cấu trúc OU và triển khai mô hình ủy quyền quản lý Active Directory

I. Mục tiêu:

- Thiết kế cấu trúc OU.
- Triển khai cấu trúc OU.
- Triển khai mô hình ủy quyền quản trị hệ thống AD DS.

II. Kịch bản:

Trong quá khứ, công ty A. Datum sử dụng cách tiếp cận tập trung để quản lý cơ sở hạ tầng CNTT của mình. Tuy nhiên, do công ty đã mở rộng sang các nước khác, cách tiếp cận tập trung này không còn hiệu quả. Vì vậy, giám đốc IT mong muốn đội ngũ thiết kế Active Directory đưa ra giải pháp thay đổi cơ cấu quản lý Active Directory để đáp ứng yêu cầu mới.

Công ty A. Datum đã mở rộng hoạt động kinh doanh của mình thông qua thương vụ mua lại công ty Contoso và Trey Research. Giám đốc IT của họ đang quan tâm đến sự đảm bảo đồng bộ Active Directory và phân giải tên giữa các công ty. Tuy nhiên, giám đốc IT cũng đang có kế hoạch cho phép các nhóm IT của mỗi địa điểm tự quản lý các đối tượng Active Directory trong hệ thống của mình.

Tóm tắt thông tin của ba công ty:

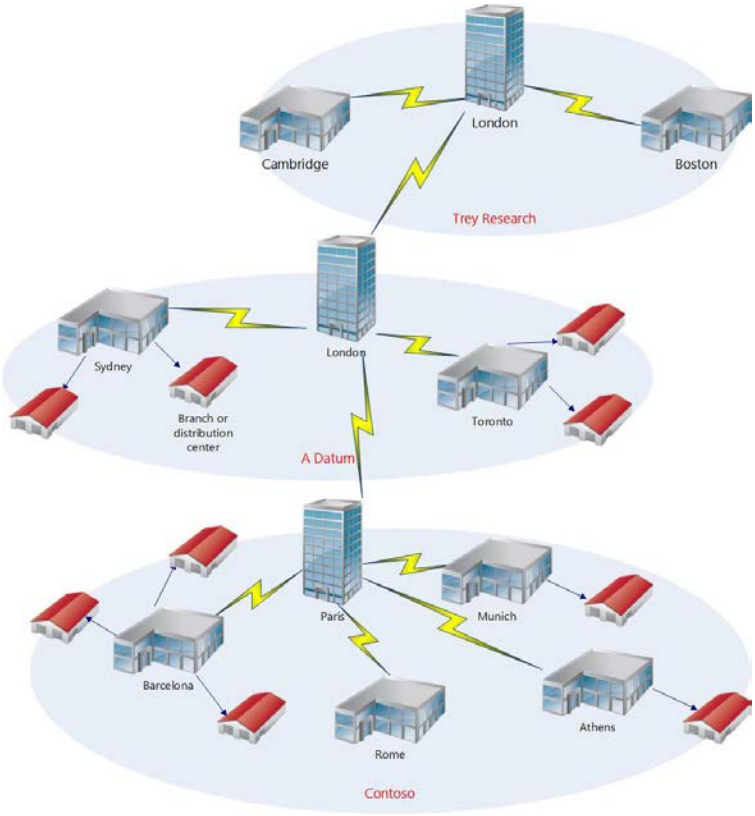
- **A. Datum:**

- Chịu trách nhiệm về cơ sở hạ tầng Active Directory.
- Quản lý tài khoản quản trị (Administrator) và các nhóm liên quan.
- Có ba địa điểm chính: London, Toronto, và Sydney. (Địa điểm nhỏ hơn sẽ không được đưa vào dự thảo thiết kế.)
- Cung cấp một số máy chủ doanh nghiệp.
- Có một đội ngũ chuyên dụng để tạo hoặc xóa User account.
- Có đội ngũ hỗ trợ người dùng, chẳng hạn như thiết lập lại mật khẩu.
- Có bộ phận IT trung tâm, những người chịu trách nhiệm quản lý của các máy client và server nội bộ.

- **Trey Research:**
  - Sau này sẽ sáp nhập vào Adatum.com, cấu trúc OU nên hỗ trợ cho việc này.
  - Sẽ không tích hợp research.treyresearch.net.
- **Contoso:**
  - Sau này sẽ sáp nhập vào Adatum.com, cấu trúc OU nên hỗ trợ cho việc này.
  - Có một File server, cung cấp nơi lưu trữ cho tất cả người dùng trong doanh nghiệp.

III. Yêu cầu tổng quan:

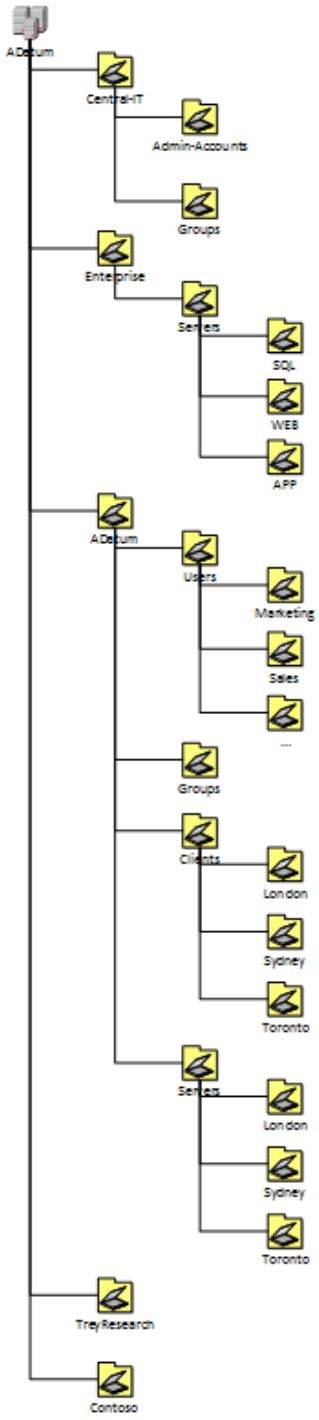
Thiết kế một cấu trúc OU đáp ứng các yêu cầu sau:



- Đối với mục đích quản lý, chỉ sử dụng tài khoản quản trị cá nhân.
- Nhóm IT của A. Datum phải là nhóm duy nhất có thể thay đổi cấu hình của domain, như cấu hình các site, tạo OU cấp 1, quản lý domain controller, tạo và quản lý tài khoản quản trị.
- Tạo điều kiện hội nhập trong tương lai của Contoso và Trey Research vào cấu trúc OU của A. Datum (không bao gồm domain research.treyresearch.net).
- Một nhóm IT trong văn phòng London có thể tạo và xóa tất cả User và Group trong domain Adatum.com.
- Mỗi văn phòng trung tâm khu vực phải có một nhóm IT, có trách nhiệm khắc phục sự cố máy tính và hỗ trợ người dùng trong khu vực mà họ quản lý. Các nhóm IT này phải có quyền truy cập vào tất cả các server trong văn phòng của họ (trừ domain controller).

- Mỗi bộ phận phải có một nhóm IT có quyền thiết lập lại mật khẩu cho người dùng của họ.
- Nhóm IT của A. Datum có trách nhiệm quản lý các máy chủ ứng dụng của toàn doanh nghiệp, phải quản lý quyền truy cập vào các ứng dụng và tài nguyên được lưu trữ trên các máy chủ này. Kế hoạch có ba máy chủ sau đây: SQL, WEB, và APP.
- Người sử dụng từ Contoso.com và người sử dụng từ tất cả các văn phòng khác phải có khả năng truy cập dữ liệu trên File server ở Paris.
- Quy trình để tạo thêm nhiều tài khoản người dùng cùng một lúc, hoặc thay đổi thuộc tính cho một số lượng lớn các tài khoản (User, Group, Computer Account) phải được tự động hóa.

Cấu trúc OU cần tạo như sau:



Danh sách các goup cần tạo như sau:

Tên Group	Loại	Thành viên	Mô tả
London- UserGroupProvisioning	Global		Tạo, xóa User và Group trong Adatum
acl_adatum-users_ccdc	Domain Local	London-UserGroupProvisioning	
acl_adatum-groups_ccdc	Domain Local	London-UserGroupProvisioning	
Enterprise-ServerOps	Global		Quản lý các application servers
acl_enterprise_serveroperator	Domain Local	Enterprise-ServerOps	
Marketing-Admins	Global		Quản lý user Marketing
acl_Users-Marketing_resetpwd	Domain Local	Marketing-Admins	
Xyz-Department-Admins	Global		Quản lý user của phòng ban xyz
acl_xyzDepartment_resetpwd	Domain Local	Xyz-Department-Admins	
London-Admins	Global		Quản lý máy client và server ở London
acl_clients- London_computer_ccdc	Domain Local	London-Admins	
acl_servers- London_computer_ccdc	Domain Local	London-Admins	

Ủy quyền quản lý cho các group theo bảng sau:

Group	**Ở đâu**	**Quyền**	**Áp dụng cho**
acl_adatum-users_ccdc	Adatum\Users	**Create User objects** và **Delete User objects**	**All descendant objects**
acl_adatum-groups_ccdc	Adatum\Group	**Create Group objects** và **Delete Group objects**	**All descendant objects**
acl_enterprise-serveroperator		Dùng GPO để cấp quyền quản lý Server	
acl_Users-Marketing_resetpwd	Adatum\Users \Marketing	**Reset passwords**	**Descendant User objects**
acl_clients-London_computer_ccdc	Adatum\Clients\London	**Create Computer objects** và **Delete Computer objects.** Ngoài ra, dùng GPO để cấp quyền local admin	
acl_servers-London_computer_ccdc	Adatum\Servers\London	**Create Computer objects** và **Delete Computer objects**, Ngoài ra, dùng GPO để cấp quyền quản lý	

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**

VI. Thực hành:

Thời gian thực hành: 120 phút

Bài thực hành bao gồm các bước:

1. Tạo cấu trúc OU mới.
2. Di chuyển đối tượng vào cấu trúc OU mới.
3. Tạo các Group theo yêu cầu.
4. Cấp quyền quản lý cho các group.

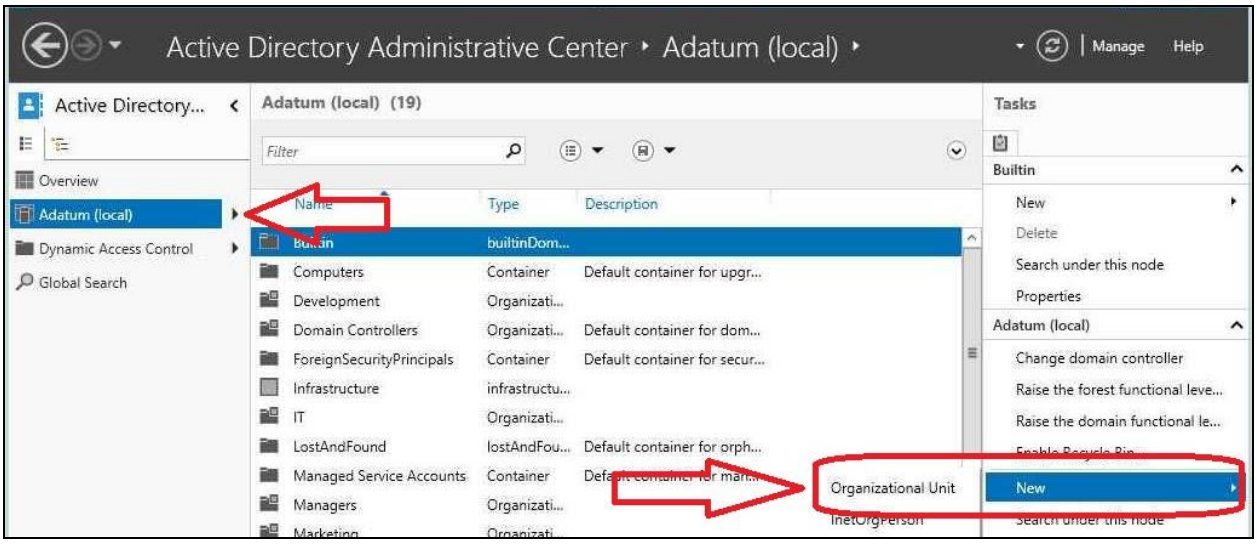
Bước 1. Tạo cấu trúc OU mới.

1. Logon vào máy **LON-DC1**.

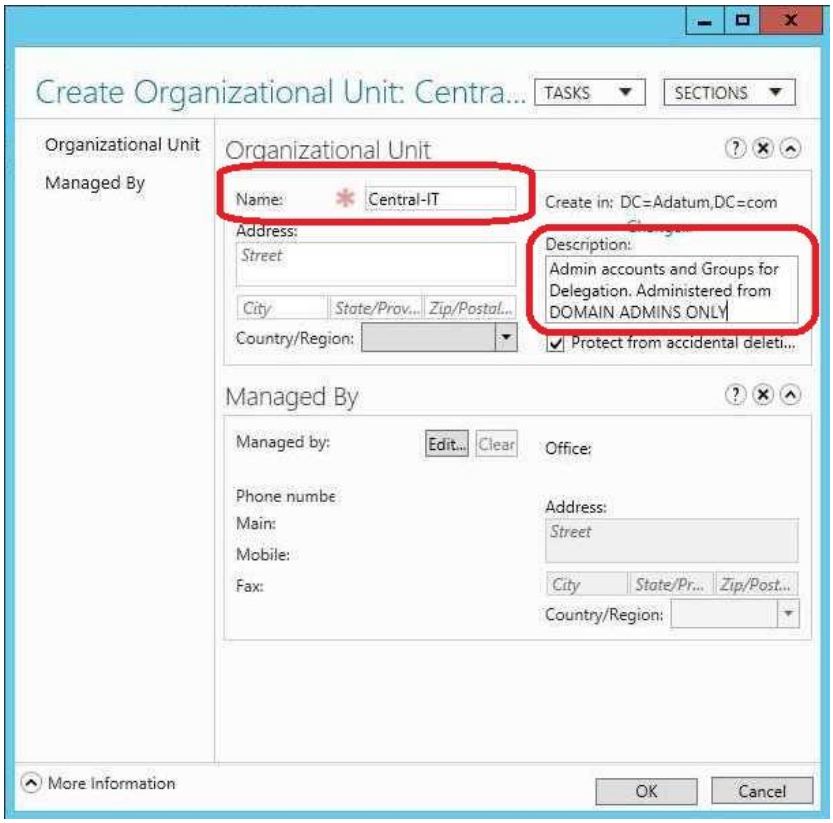
2. Mở **Server Manager**, bung menu **Tools**, mở **Active Directory Administrative Center**.



3. Trong cửa sổ **Active Directory Administrative Center**, chọn **Adatum (local)**, bung **New**, và chọn **Organizational Unit**.



4. Hộp thoại **Create Organizational Unit**, nhập thông tin như bên dưới, sau đó chọn OK
   - Name: **Central-IT**
     - Description: **Admin accounts and Groups for Delegation. Administered from DOMAIN ADMINS ONLY**

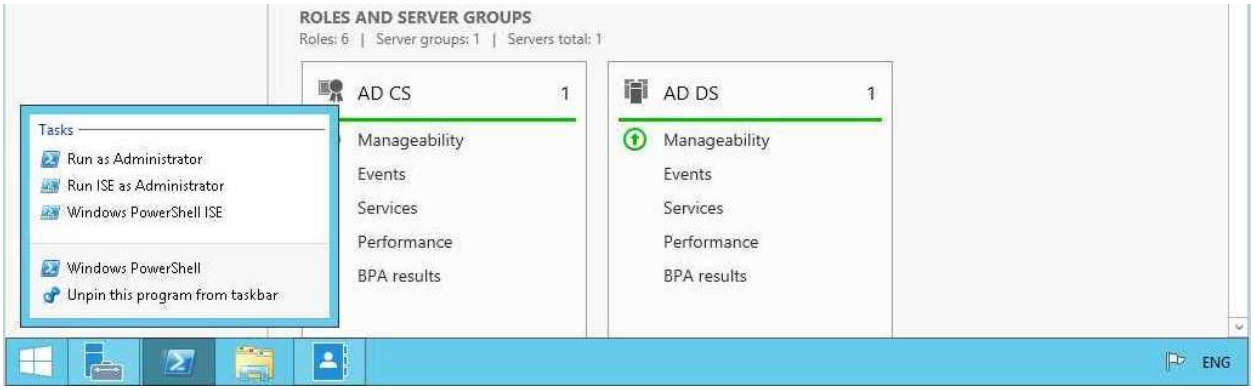


5. Lập lại từ bước 3 và 4 để tạo các OU sau:
   - Name: **Enterprise**
     - Description: **Enterprise-wide managed objects**
   - Name: **Adatum**
     - Description: **Regular objects for A. Datum**
   - Name: **Contoso**
     - Description: **Regular objects for Contoso**
   - Name: **TreyResearch**

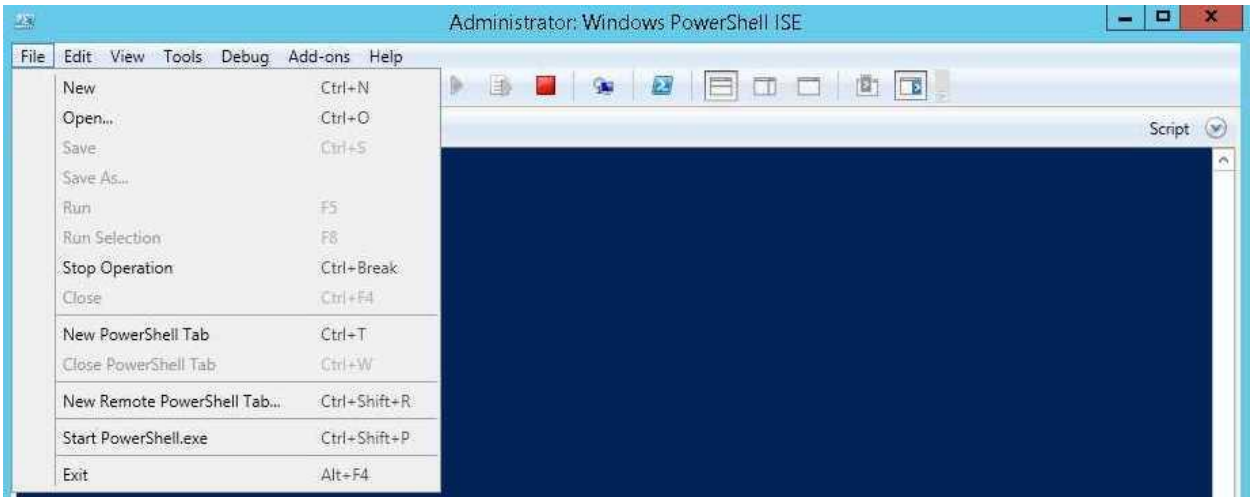
- Description: **Regular objects for Trey Research**

6. Sử dụng file Windows PowerShell Script để tạo các OU con:

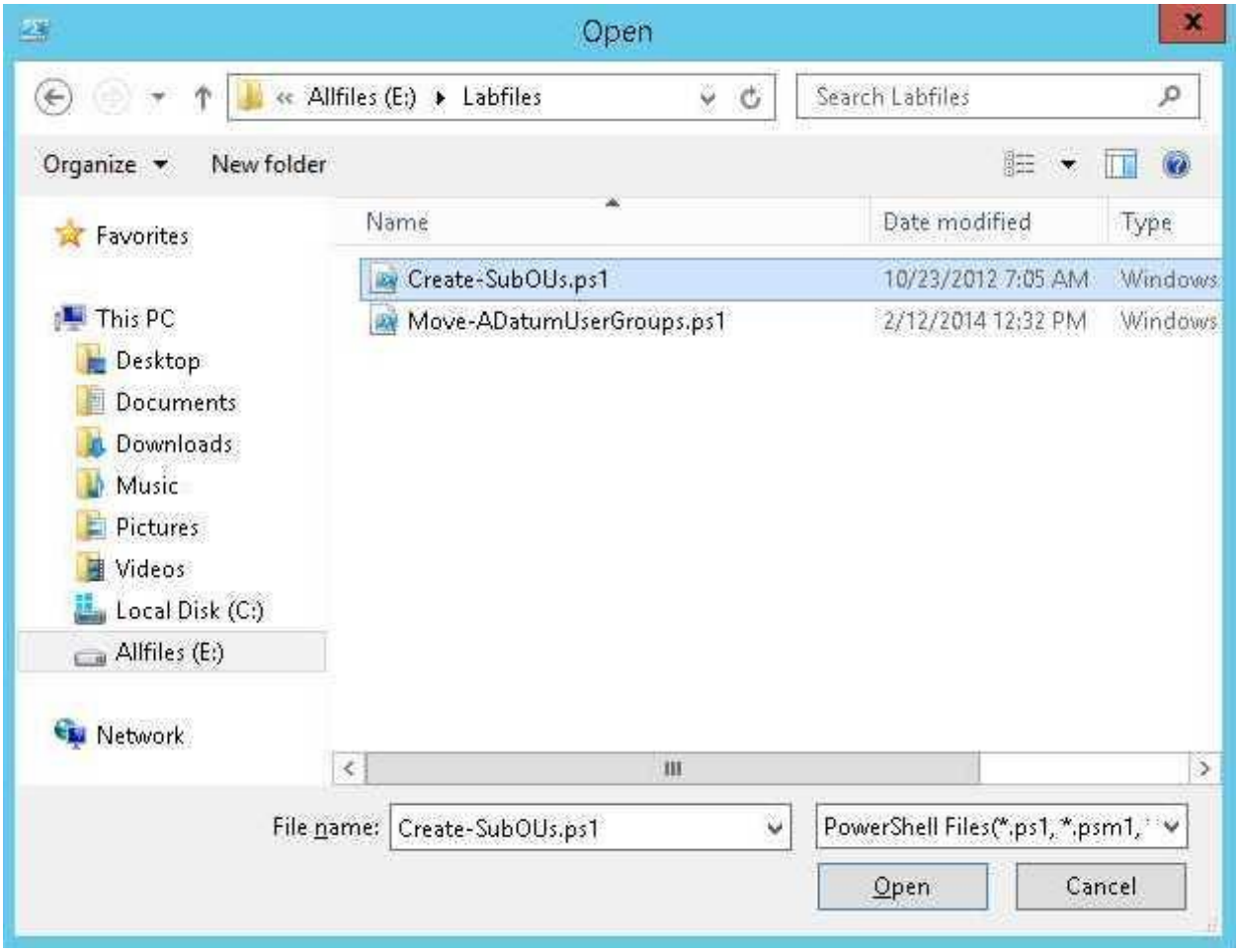
a. Trên thanh taskbar, nhấn chuột phải **Windows PowerShell**, chọn **Run ISE as Administrator**.



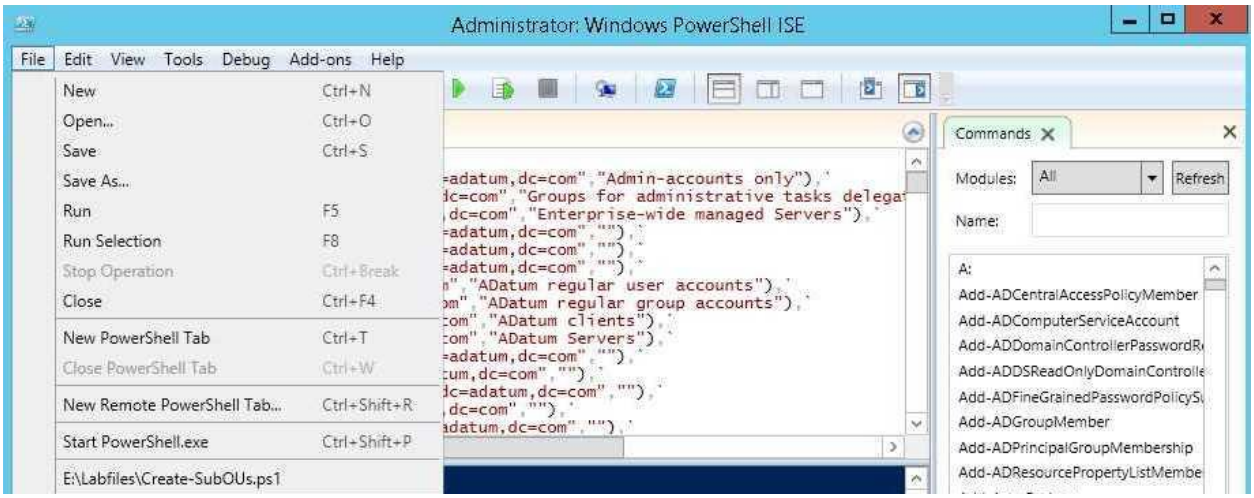
b. Trong cửa sổ **Administrator: Windows PowerShell ISE**, bung menu **File**, chọn **Open**.



c. Trong hộp thoại **Open,** trỏ vào đường dẫn **E:\Labfiles,** chọn file **Create-SubOUs.ps1**, chọn **Open**.



d. Bung menu **File**, chọn **Run**.

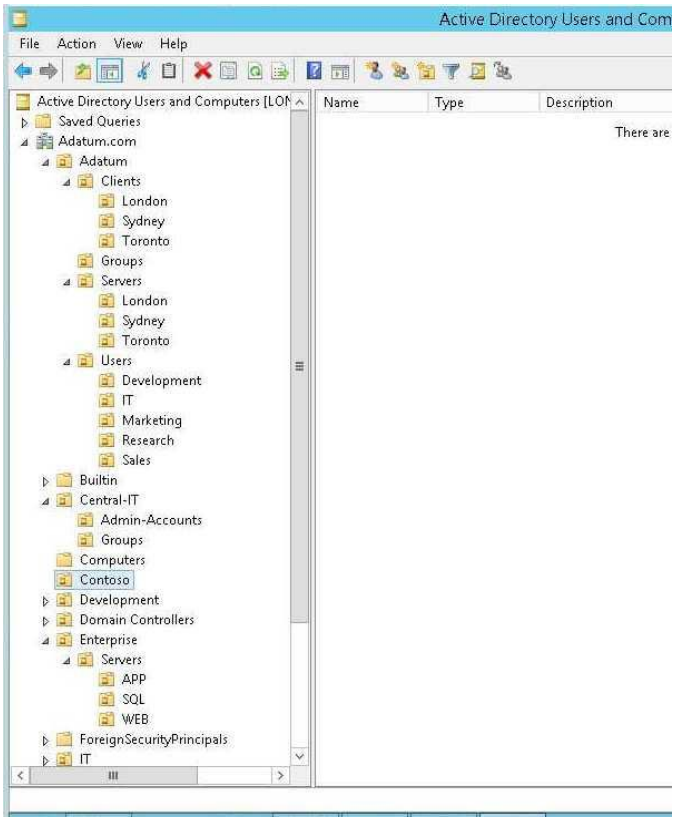


Chú thích: Nội dung của file Create-SubOUs.ps1

```
$subous = @(`
("Admin-Accounts","ou=Central-IT,dc=adatum,dc=com","Admin-accounts only"),`
("Groups","ou=Central-IT,dc=adatum,dc=com","Groups for administrative tasks
delegation"),`
("Servers","ou=Enterprise,dc=adatum,dc=com","Enterprise-wide managed Servers"),`
("SQL","ou=Servers,ou=Enterprise,dc=adatum,dc=com",""),`
("WEB","ou=Servers,ou=Enterprise,dc=adatum,dc=com",""),`
("APP","ou=Servers,ou=Enterprise,dc=adatum,dc=com",""),`
("Users","ou=Adatum,dc=adatum,dc=com","Adatum regular user accounts"),`
("Groups","ou=Adatum,dc=adatum,dc=com","Adatum regular group accounts"),`
("Clients","ou=Adatum,dc=adatum,dc=com","Adatum clients"),`
("Servers","ou=Adatum,dc=adatum,dc=com","Adatum Servers"),`
("Marketing","ou=Users,ou=Adatum,dc=adatum,dc=com",""),`
("Sales","ou=Users,ou=Adatum,dc=adatum,dc=com",""),`
("Development","ou=Users,ou=Adatum,dc=adatum,dc=com",""),`
```

```
("IT","ou=Users,ou=Adatum,dc=adatum,dc=com",""),`
("Research","ou=Users,ou=Adatum,dc=adatum,dc=com",""),`
("London","ou=Clients,ou=Adatum,dc=adatum,dc=com",""),`
("Sydney","ou=Clients,ou=Adatum,dc=adatum,dc=com",""),`
("Toronto","ou=Clients,ou=Adatum,dc=adatum,dc=com",""),`
("London","ou=Servers,ou=Adatum,dc=adatum,dc=com",""),`
("Sydney","ou=Servers,ou=Adatum,dc=adatum,dc=com",""),`
("Toronto","ou=Servers,ou=Adatum,dc=adatum,dc=com",""))
$subous | %{New-ADOrganizationalUnit -Name $_[0] -Path $_[1] -Description $_[2]}
```

7. Mở công cụ **Active Directory Users and Computers**, kiểm tra các OU đã được tạo thành công theo yêu cầu của A. Datum đưa ra.

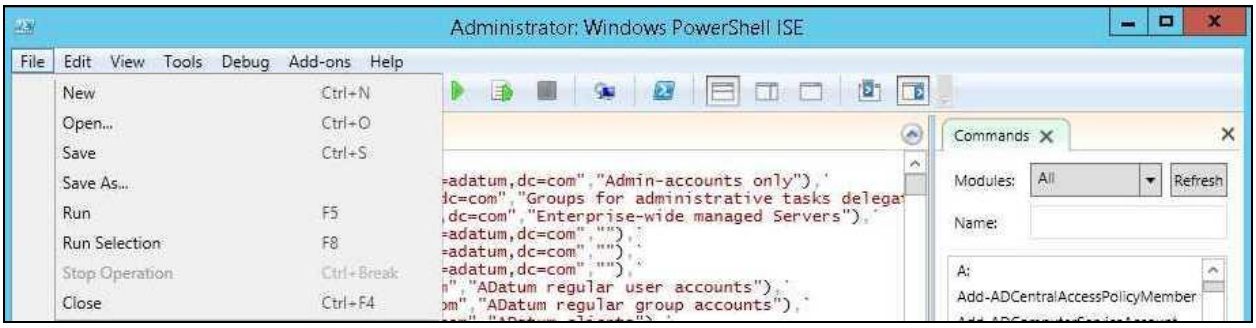


Bước 2. Di chuyển đối tượng vào cấu trúc OU mới.

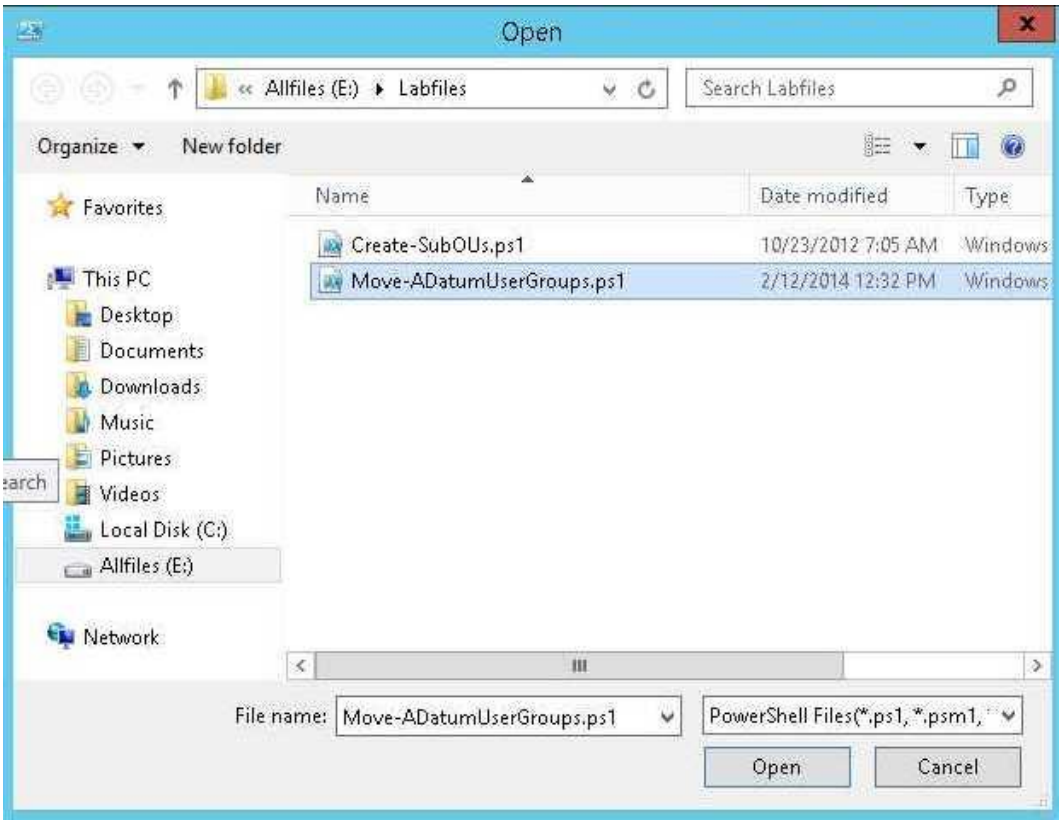
Sử dụng file Windows PowerShell script để di chuyển users và groups vào các OU mới tạo.

1. Quay lại cửa sổ **Windows PowerShell** (ISE), bung menu **File**, chọn **Close**.

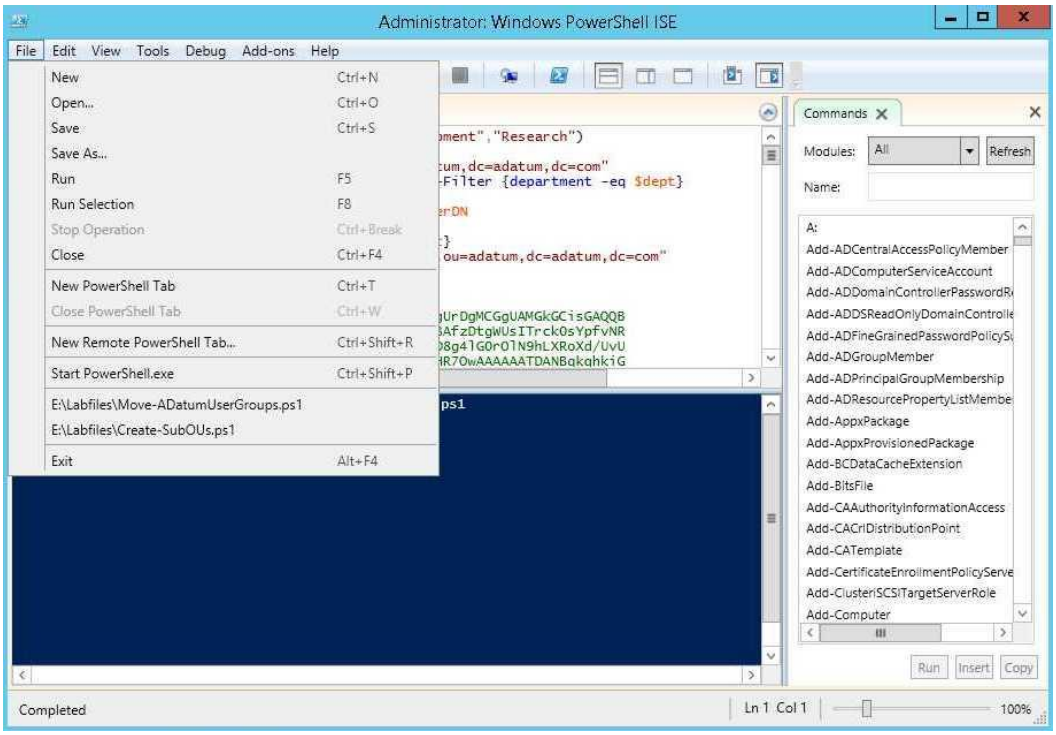
2. Tiếp theo, bung menu **File**, chọn **Open**.



3. Trong hộp thoại **Open**, trỏ vào đường dẫn **E:\Labfiles,** chọn file **Move-AdatumUserGroups.ps1**, chọn **Open**.



4. Bung menu **File**, chọn **Run**.



Chú thích: Nội dung của file Move-AdatumUserGroups.ps1

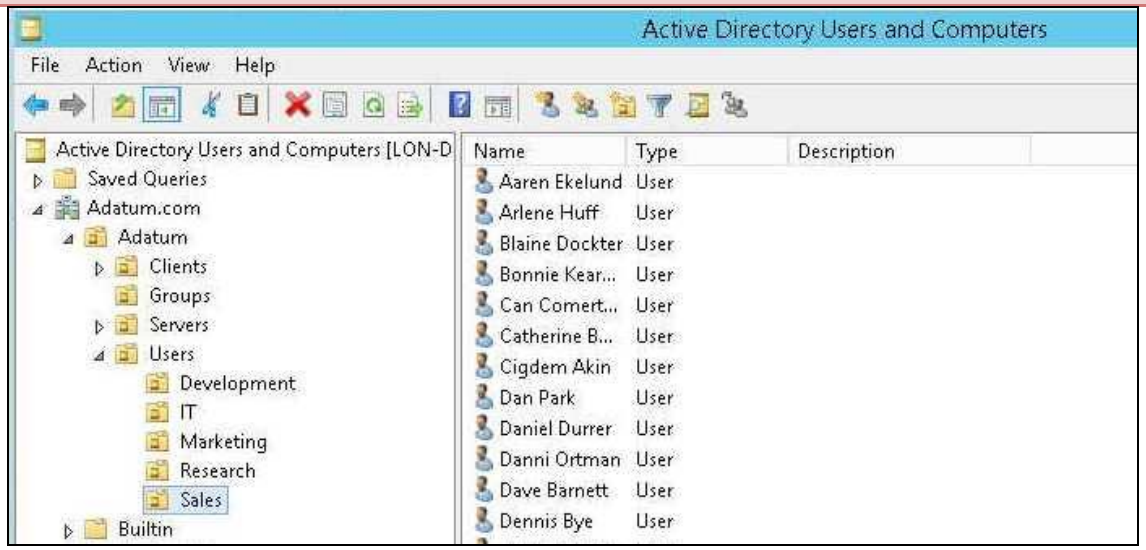
```
$depts = @("Marketing","Sales","IT","Development","Research")
ForEach ($dept in $depts) {
$userDN = "OU=" + $dept + ",ou=users,ou=adatum,dc=adatum,dc=com"
$users = Get-ADUser -Properties Department -Filter {department -eq $dept}
ForEach ($user in $users) {
Move-ADObject $user -TargetPath $userDN
}
$group = Get-ADGroup -Filter {Name -eq $dept}
Move-ADObject $group -TargetPath "ou=groups,ou=adatum,dc=adatum,dc=com"
}
```

5. Qua cửa sổ **Active Directory Administrative Center**, kiểm tra các user và group được di chuyển vào các OU thành công.

a. Bung OU **Adatum**.

b. Bung OU **Users**, vào OU **Sales**.

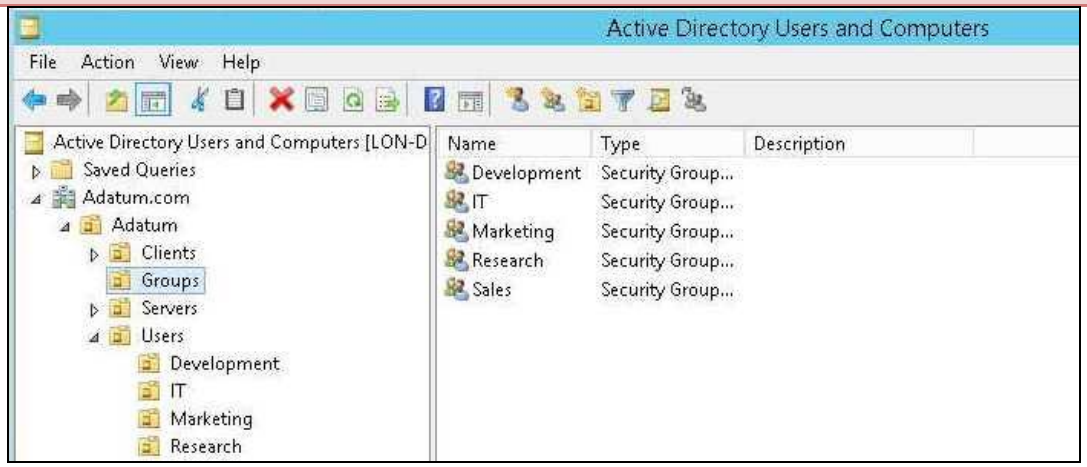
Chú ý: Trong OU Sales có các user như hình bên dưới.



c. Bung OU **Adatum**.

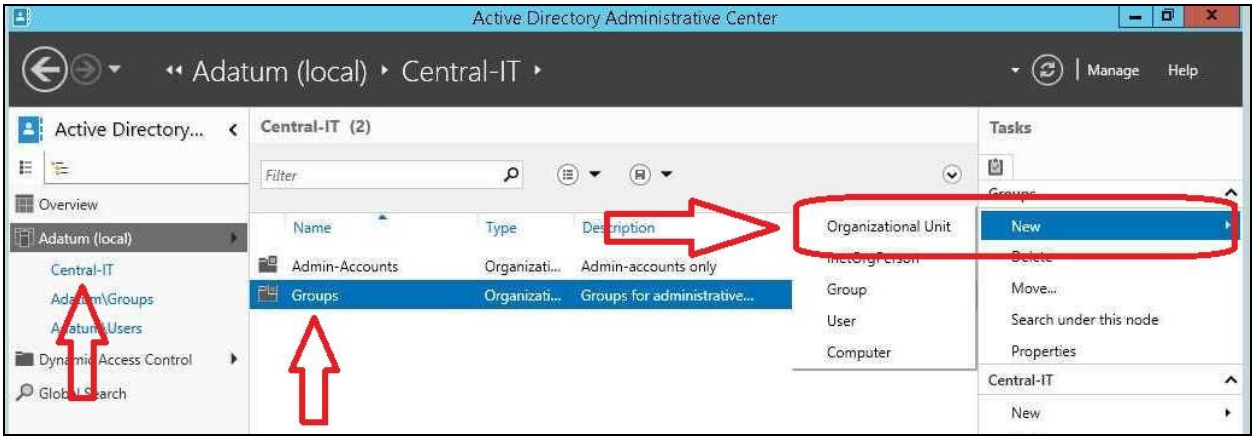
d. Vào OU **Groups**.

Chú ý: Trong OU Groups có các group như hình bên dưới.

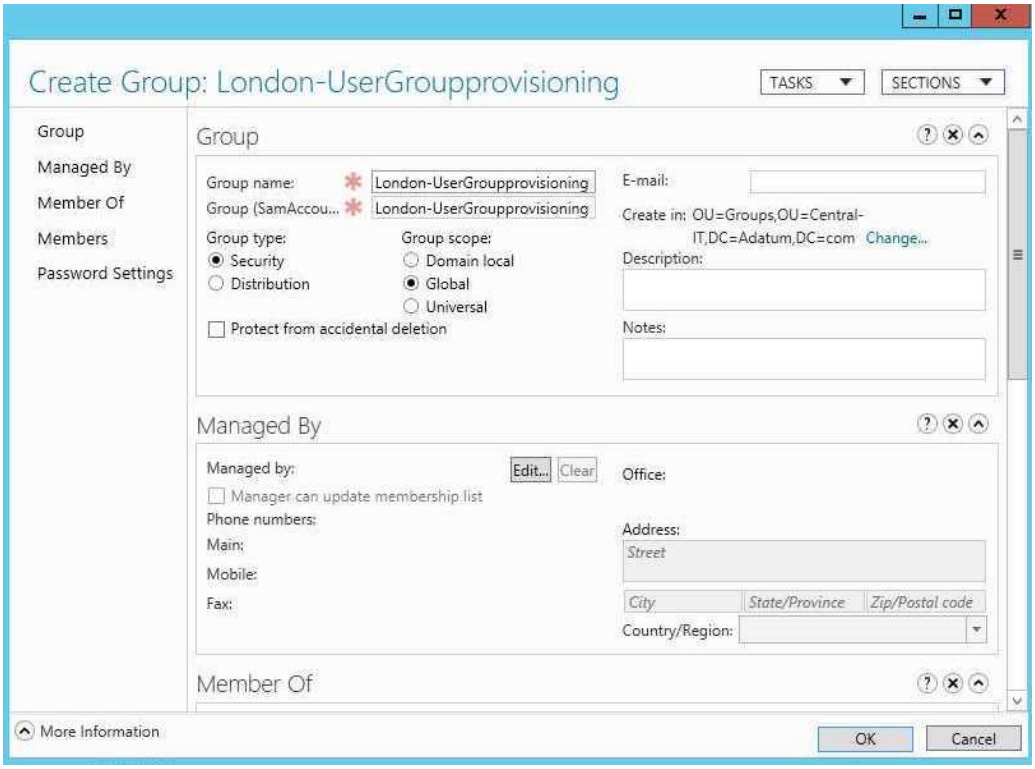


Bước 3. Tạo các Group theo yêu cầu.

1. Mở công cụ **Active Directory Administrative Center**, bung **Adatum (local)**, bung OU **Central-IT**, OU **Groups**, chọn **New**, và chọn **Group**.



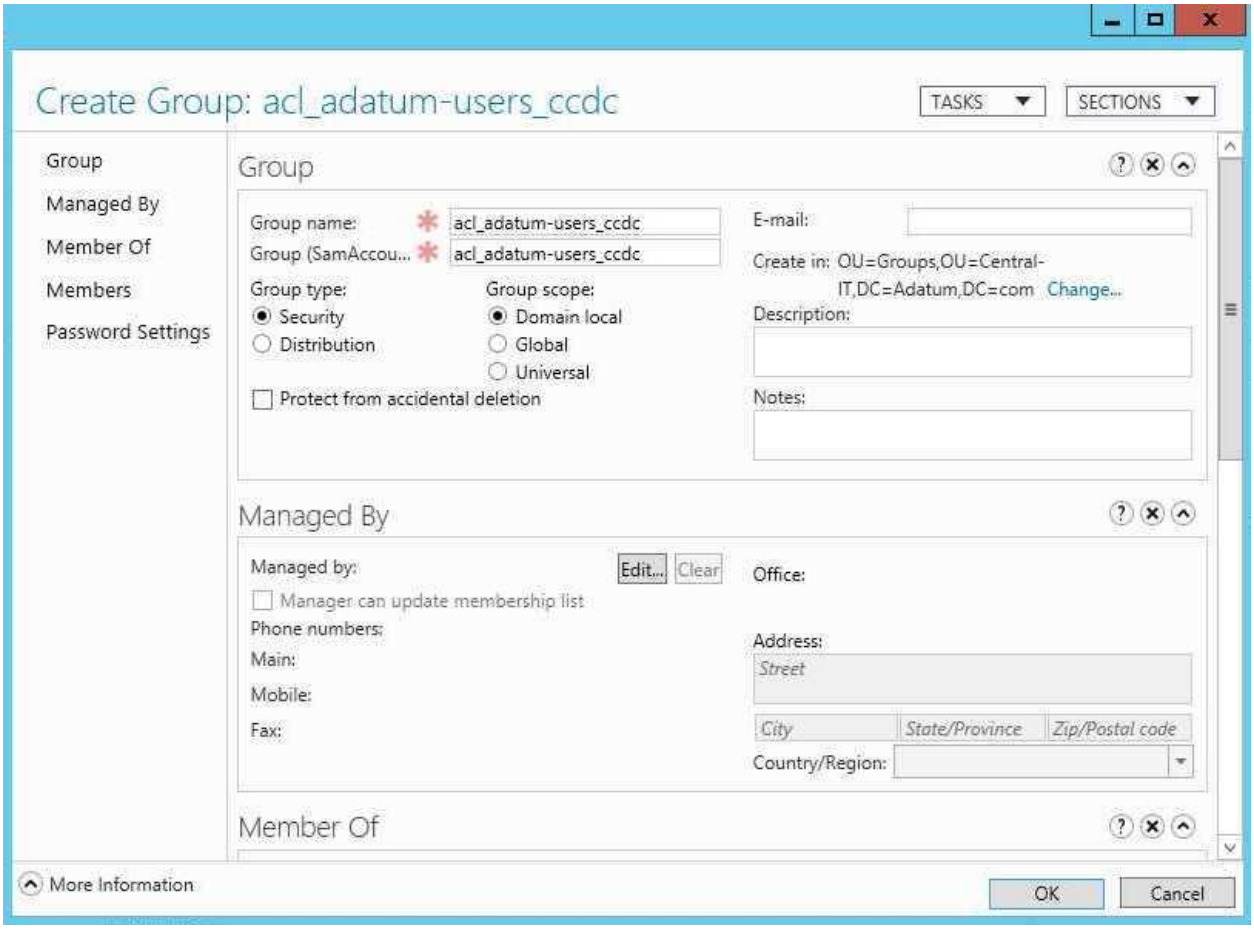
2. Trong hộp thoại **Create Group**, nhập tên **London- UserGroupprovisioning** vào ô **Group name**, và chọn **OK**.



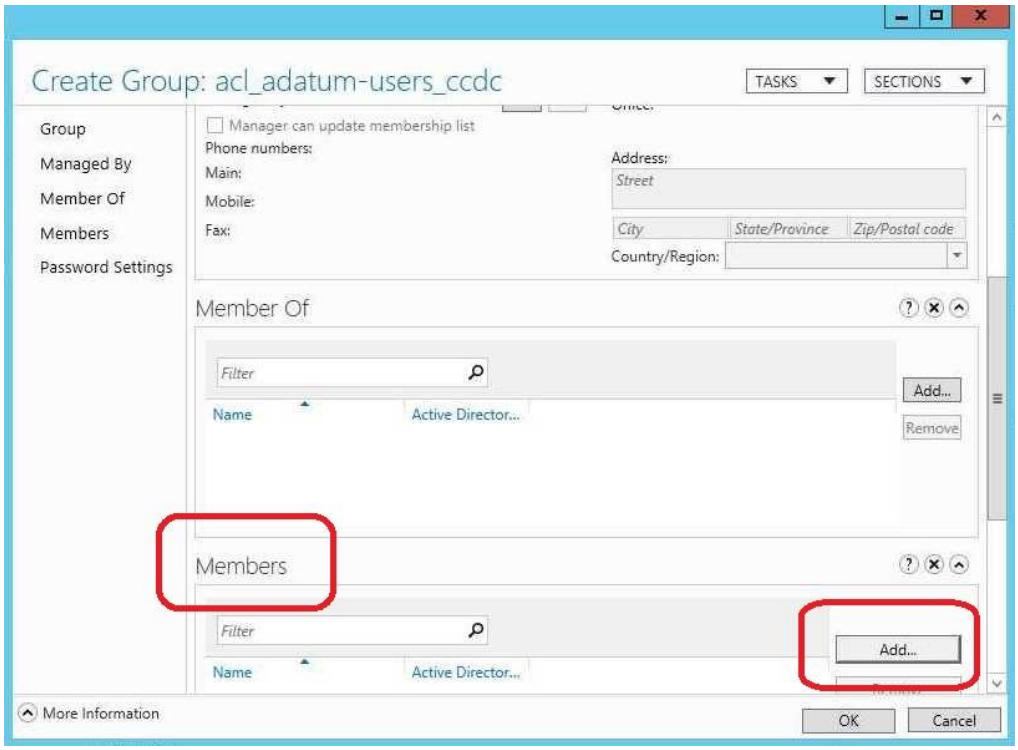
3. Lập lại bước 2 để tạo thêm các group sau:

- Name: **Enterprise-ServerOps**
  - Type: **Global/Security**
- Name: **Marketing-Admins**
  - Type: **Global/Security**
- Name: **London-Admins**
  - Type: **Global/Security**

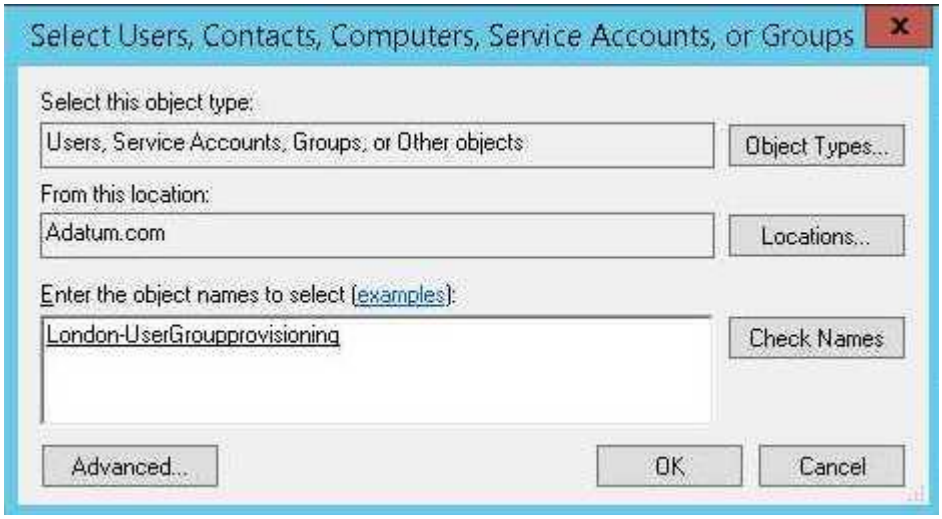
4. Tương tự bước 2, trong hộp thoại **Create Group**, nhập **acl_adatum-users_ccdc** vào ô **Group name,** trong phần **Group scope**, chọn **Domain Local**.



5. Kéo thanh trượt xuống dưới, trong phần **Members**, chọn **Add**.



6. Hộp thoại **Select Users, Contacts, Computers, Service accounts, or Groups**, nhập **London-UserGroupProvisioning** vào ô **Enter the object name to select (examples)**, chọn **Check Names**, và chọn **OK**.



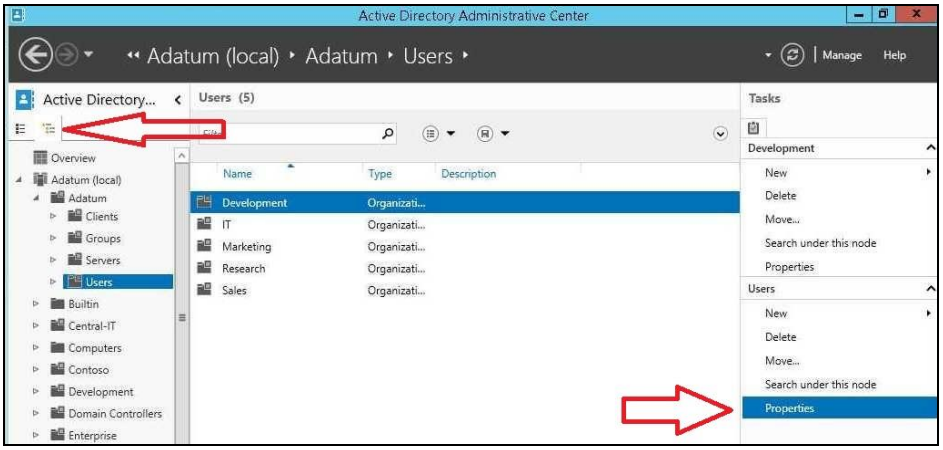
7. Hộp thoại **Create Group: acl_adatum-users_ccdc**, chọn **OK**.

8. Lập lại từ bước 4 đến 7 để tạo các group sau:

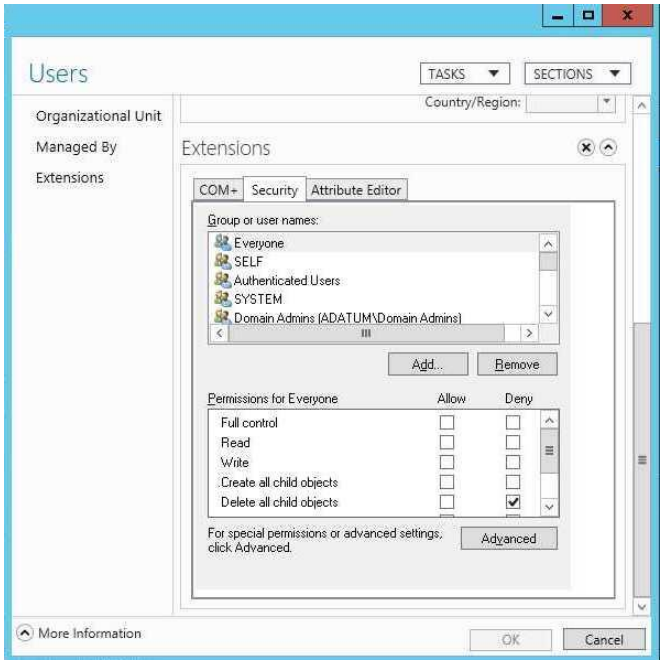
- Name: **acl_adatum-groups_ccdc**
  - Type: **Domain Local/Security**
  - Member: **London-UserGroupProvisioning**
- Name: **acl_enterprise-serveroperator**
  - Type: **Domain Local/Security**
  - Member: **Enterprise-ServerOps**
- Name: **acl_Users-Marketing_resetpwd**
  - Type: **Domain Local/Security**
  - Member: **Marketing-Admins**
- Name: **acl_clients-London_computer_ccdc**
  - Type: **Domain Local/Security**
  - Member: **London-Admins**
- Name: **acl_servers-London_computer_ccdc**
  - Type: **Domain Local/Security**
  - Member: **London-Admins**

Bước 4. Ủy quyền quản lý cho các group.

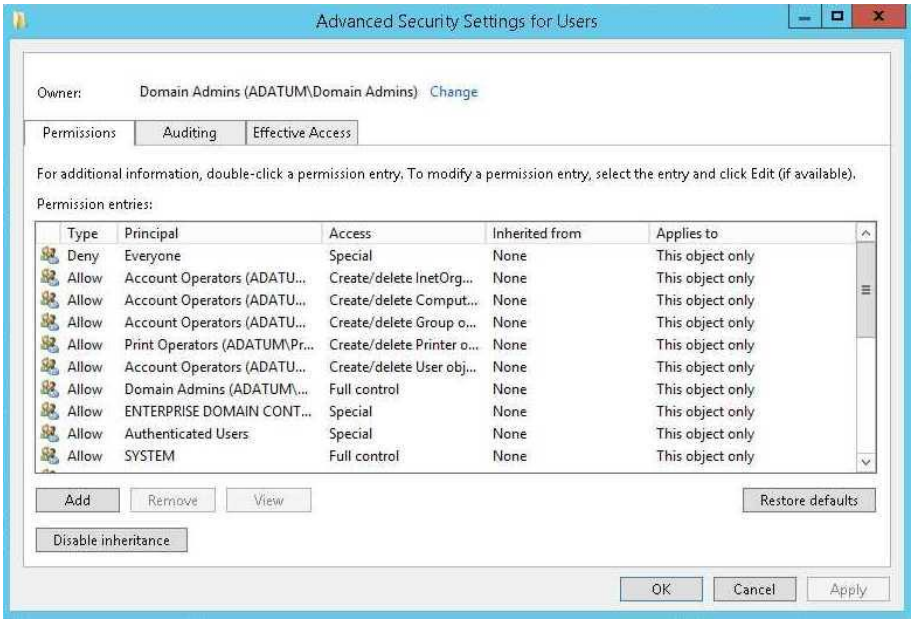
1. Mở công cụ **Active Directory Administrative Center**, chuyển qua chế độ **Tree View**. Bung **Adatum (local)**, bung OU **Adatum**, chọn OU **Users**. Trong mục Users bên phải, chọn **Properties**.



2. Trong hộp thoại **Users**, kéo thanh trượt xuống mục **Extensions**, qua tab **Security**, chọn **Advanced**.



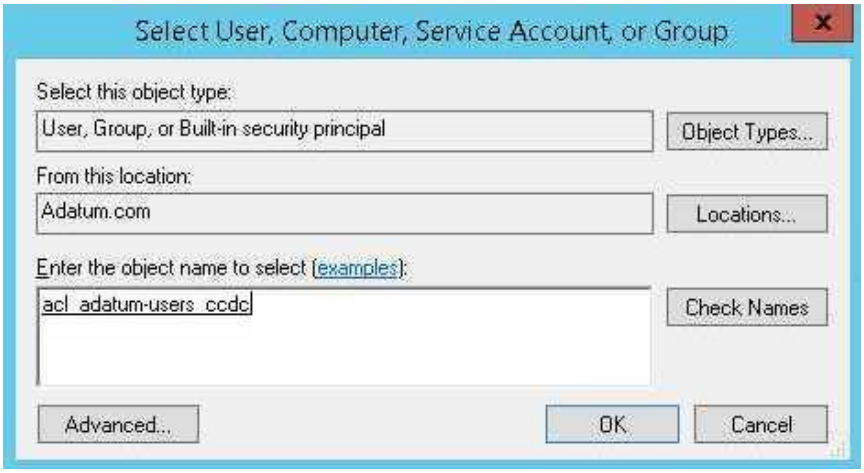
3. Hộp thoại **Advanced Security Settings for Users**, qua tab **Permissions,** chọn **Add**.



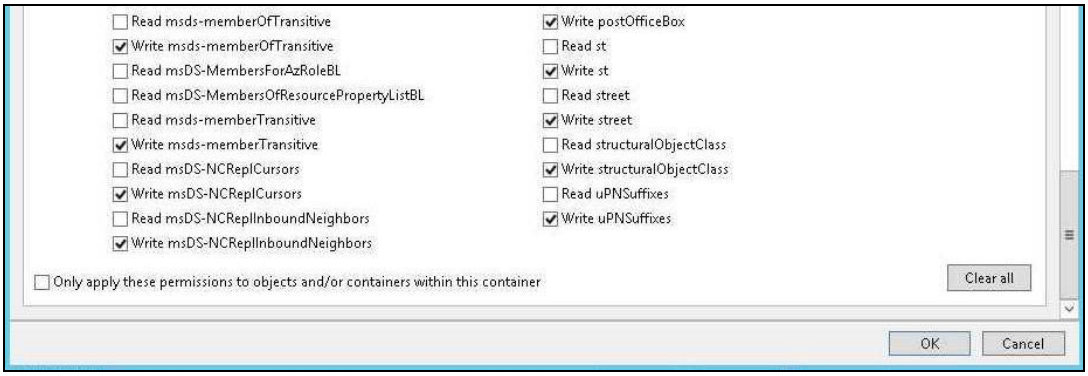
4. Hộp thoại **Permission Entry for Users**, chọn **Select a principal**.



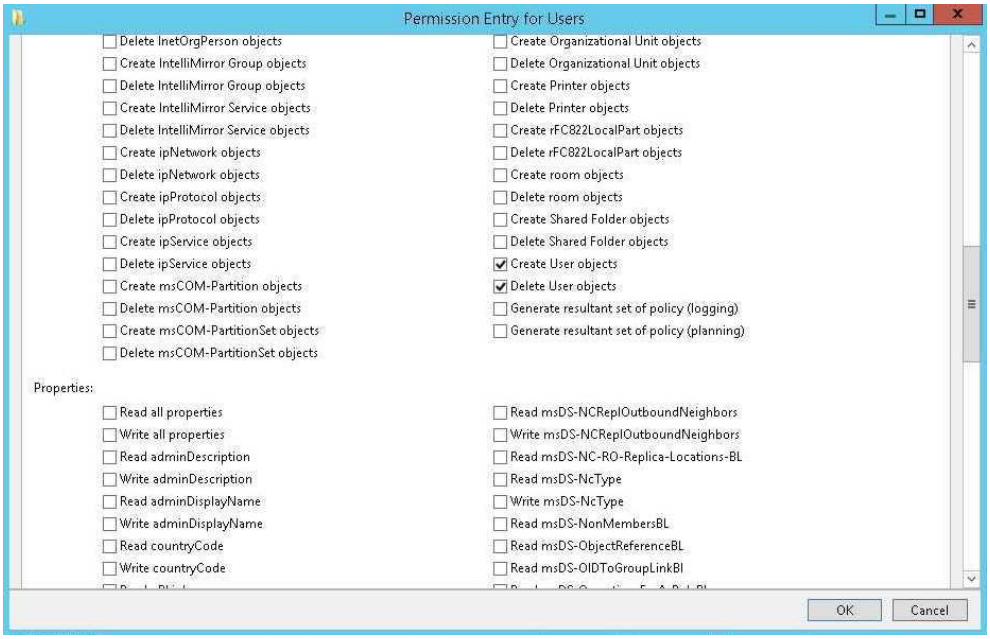
5. Hộp thoại **Select User, Computer, Service Account or Group**, trong ô **Enter the object name to select (examples)**, nhập **acl_adatum-users_ccdc**, chọn **Check Names**, và chọn **OK**.



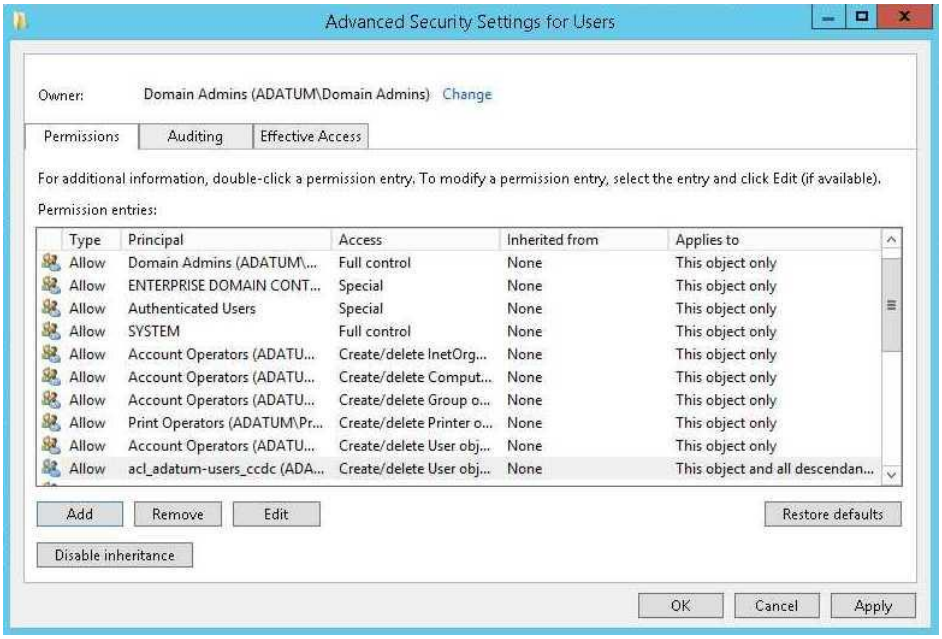
6. Hộp thoại **Permission Entry for Users**, kéo thanh trượt xuống dưới cùng, chọn **Clear All**.



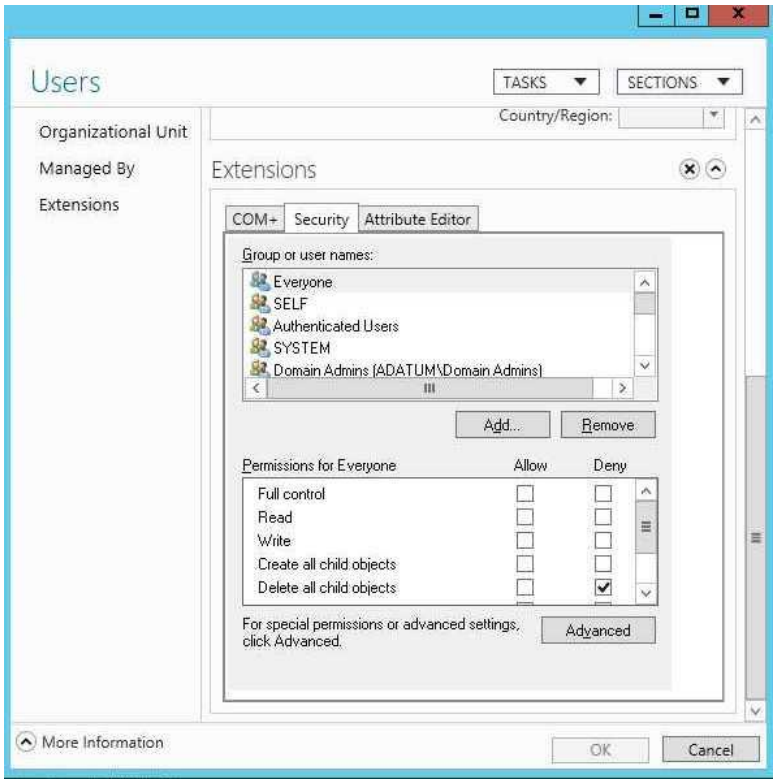
7. Trong hộp thoại **Permission Entry for Users**, đánh dấu chọn 2 ô **Create User objects** và **Delete User objects**, chọn **OK**.



8. Hộp thoại **Advanced Security for Users**, chọn **OK**.



9. Hộp thoại **Users**, chọn **Cancel**.



10. Lập lại từ bước 1 đến 9 để ủy quyền cho các group theo yêu cầu sau:

- OU: **Adatum\Groups**

  Group: **acl_adatum-groups_ccdc**

  Permissions: **Create Group objects, Delete Group objects**

- OU: **Adatum\Users\Marketing**

  Group: **acl_users-Marketing_resetPwd**

  Applies to: **Descendant User objects**

  Permissions: **Reset password**

- OU: **Adatum\Clients\London**

  Group: **acl_clients-London_computer_ccdc**

  Permissions: **Create Computer objects, Delete Computer objects**

- OU: **Adatum\Servers\London**
  Group: **acl_servers-London_computer_ccdc**
  Permissions: **Create Computer objects, Delete Computer Objects**

Kết quả: Sau khi hoàn thành bài tập này, bạn đã thiết kế và triển khai thành công cấu trúc OU và mô hình ủy quyền quản trị hệ thống.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.

Bài 8: Thiết kế và triển khai Group Policy Object (GPO)

I. Mục tiêu:

- Thiết kế chiến lược GPO.
- Triển khai và cấu hình GPO.

II. Kịch bản:

Sau khi hoàn thành việc thiết kế cấu trúc OU, bước tiếp theo trong dự án thiết kế AD cho công ty A. Datum là thiết kế chiến lược GPO để quản lý các máy tính để bàn và bảo mật máy chủ. Thiết kế GPO mới sẽ là một nền tảng cho phép các quản trị viên quản lý tập trung các thiết lập của máy tính và người dùng. Thiết kế GPO cũng phải đáp ứng yêu cầu bảo mật của A. Datum.

A. Datum muốn sử dụng GPO để thiết lập cấu hình chức năng Windows Update, và hạn chế sử dụng các công cụ quản trị đối với người dùng thông thường. Ngoài ra, yêu cầu bảo mật của A. Datum là người dùng phải nhận được cảnh báo an ninh trước khi đăng nhập vào máy tính của công ty.

Là quản trị viên của A.Datum, bạn có nhiệm vụ xem xét các yêu cầu thiết lập GPO. Sau đó, bạn phải thiết kế và triển khai các GPO sao cho phù hợp với các yêu cầu đặt ra.

III. Yêu cầu tổng quan:

Thiết kế một chiến lược GPO đáp ứng các yêu cầu sau:

- Tất cả các máy tính của công ty phải chịu ảnh hưởng của các thiết lập GPO sau đây:
  - Thiết lập các tài khoản Local Administrators
  - Cấu hình chức năng Windows Update.
  - Cấm sử dụng công cụ Registry.

  Các thiết lập trên không ảnh hưởng lên các tài khoản quản trị.
- Mỗi văn phòng nên thiết lập GPO để áp dụng cho các máy clients của họ. Hiện tại, bạn cần phải thực hiện yêu cầu sau đây:

- Hiển thị một cảnh báo an ninh trước khi đăng nhập máy tính có nội dung: "**Only A. Datum employees can use the computers** ". Thiết lập này cần phải được áp dụng cho từng vị trí, và hiển thị tự động bằng các ngôn ngữ khác cho những địa điểm ở nước ngoài.

- Tất cả người dùng phải được ánh xạ một ổ đĩa mạng (Map Network Drive).
- Nhóm IT ở London phải có khả năng quản lý tất cả các GPO. Các nhóm IT của mỗi văn phòng khác chỉ có thể quản lý GPO áp dụng cho văn phòng đó.

Danh sách các GPO cần tạo:

Tên GPO	**Chức năng**	**Đường dẫn Policy**	**Áp dụng cho**
All_Clients	Cấu hình tài khoản local admin	Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Restricted Groups	OU=Clients
All_Clients	Cấu hình Windows Update	Computer Configuration \ Policies \ Administrative Templates \ Windows Components \ Windows Update \ Configure Automatic Updates	OU=Clients
All_Users_but_Admins	Ngăn chặn chỉnh sửa Registry	User Configuration \ Policies \ Administrative Templates \ System \ Prevent access to registry editing tools	DC=adatum
London_ Clients	Hiển thị cảnh báo an ninh cần tuân thủ	Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options \ Interactive Logon: Message text for users attempting to log on Interactive Logon:	OU=London, OU=Clients

		Message title for users attempting to log on	
Marketing_Share	Map Network Drive	User Configuration \ Preferences \ Windows Settings \ Drive Maps	OU=Marketing

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-CL1**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.

2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.

3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.

4. Logon vào máy ảo với thông tin sau:

- User name: **Adatum\Administrator**
- Password: **Pa$$w0rd**

5. Thực hiên từ bước 2 đến 4 cho máy ảo **20413C-LON-CL1.**

VI. Thực hành:

Thời gian thực hành: 60 phút

Bài thực hành bao gồm các bước:

1. Tạo OU và Share Folder.

2. Tạo các GPO cần thiết và liên kết chúng vào các OU theo yêu cầu.

3 Cấu hình chức năng Filter.

4 Kiểm tra kết quả.

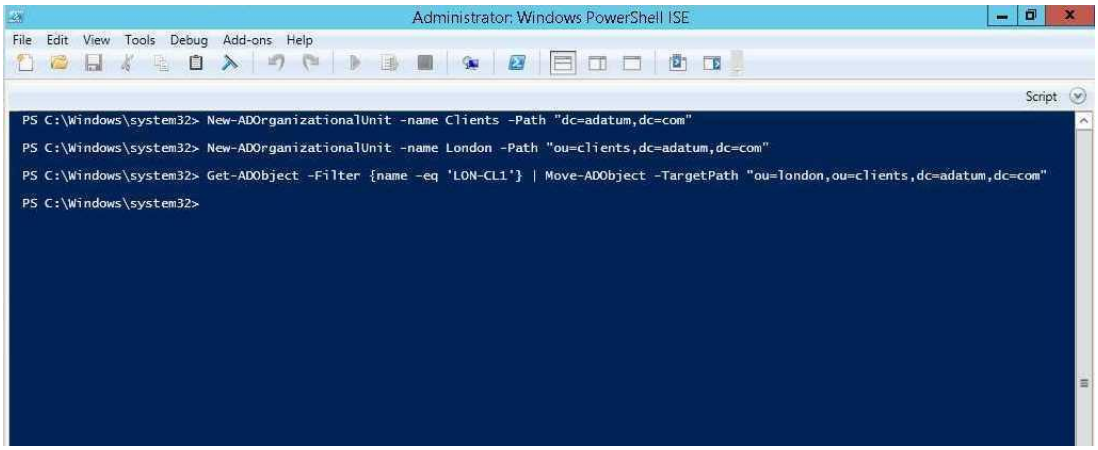
Bước 1. Tạo OU và Share Folder.

1. Logon vào máy **LON-DC1**. Trên thanh taskbar, nhấn chuột phải lên biểu tượng **Windows PowerShell®**, chọn **Run ISE as Administrator**.

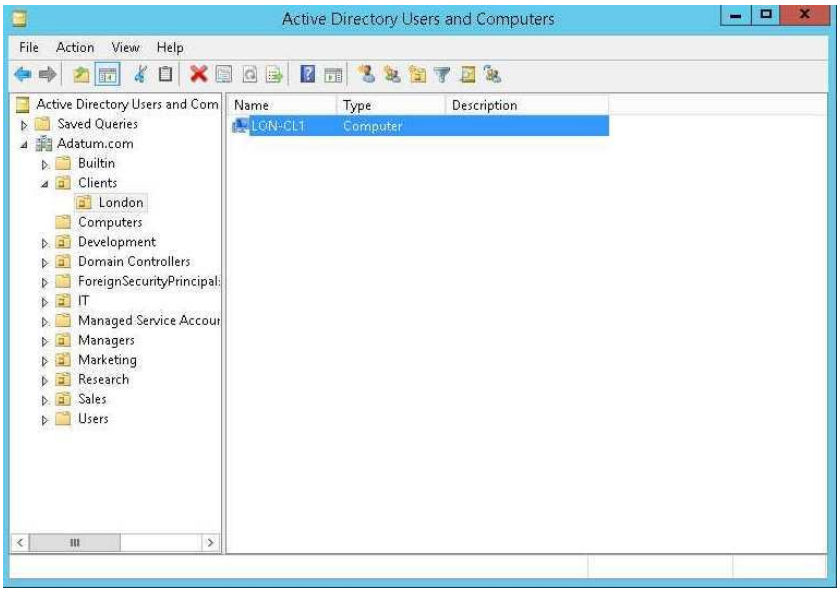


2. Trong cửa sổ **Administrator: Windows PowerShell ISE**, gõ các lệnh sau: (nhấn Enter sau mỗi dòng lệnh)

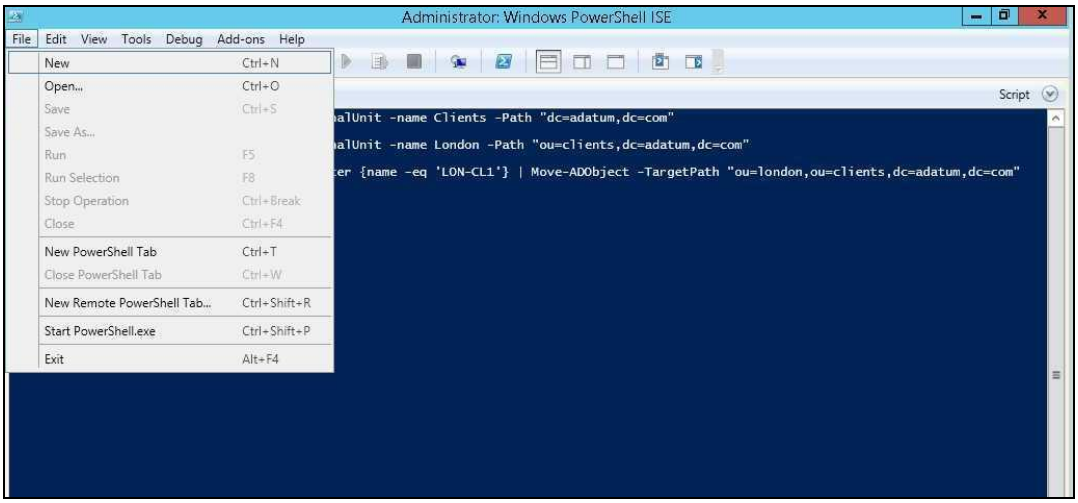
- New-ADOrganizationalUnit –name Clients –path “dc=adatum,dc=com”
- New-ADOrganizationalUnit –name London –path “ou=clients,dc=adatum,dc=com”
- Get-ADObject -Filter {name –eq ‘LON-CL1’} | Move-ADObject -TargetPath “ou=London,ou=Clients,dc=adatum,dc=com”



3. Mở công cụ **Active Directory Users and Computer**, bung OU **Clients**, bung OU **London**, kiểm tra có chứa computer account **LON-CL1.**

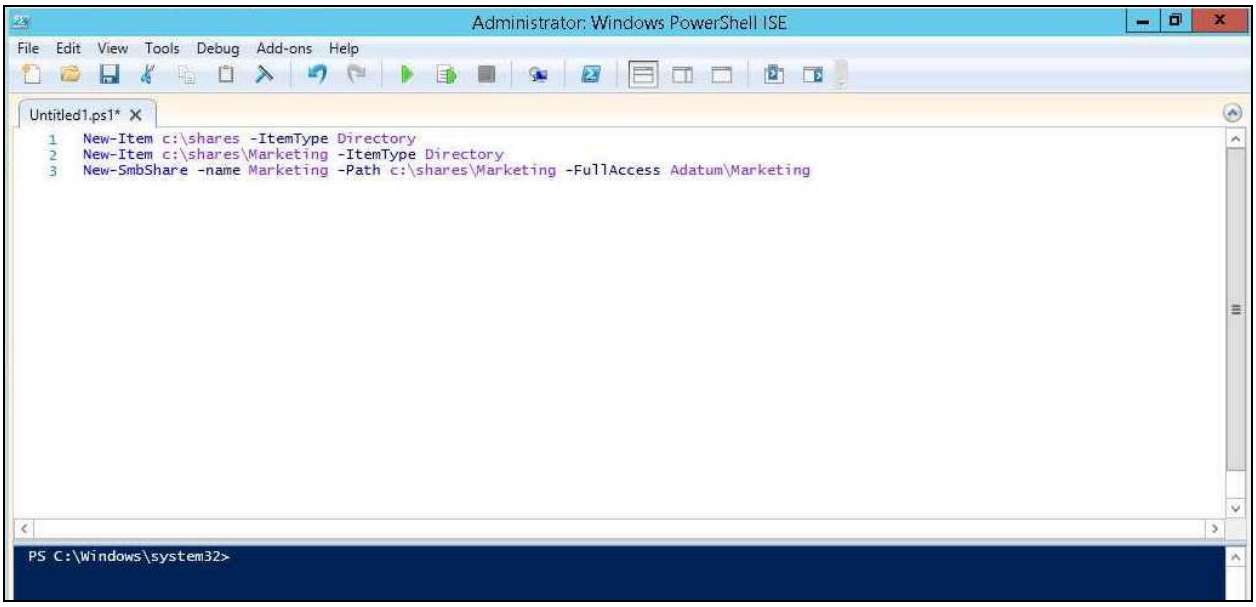


4. Quay lại cửa sổ **Administrator: Windows PowerShell ISE**, bung **File**, chọn **New**.

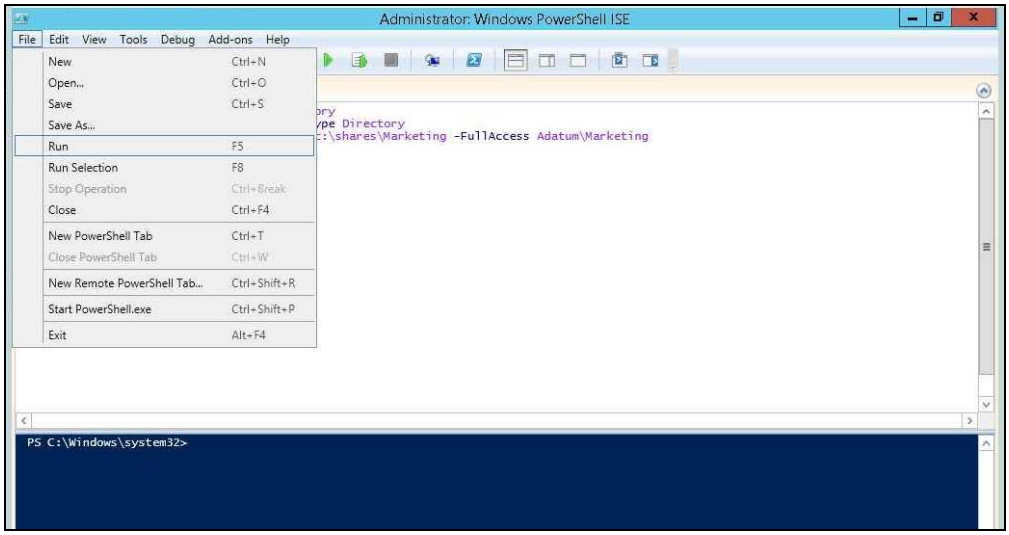


5. Trong tab **Untitled1.ps1**, gõ các lệnh sau: (nhấn Enter sau mỗi dòng lệnh)

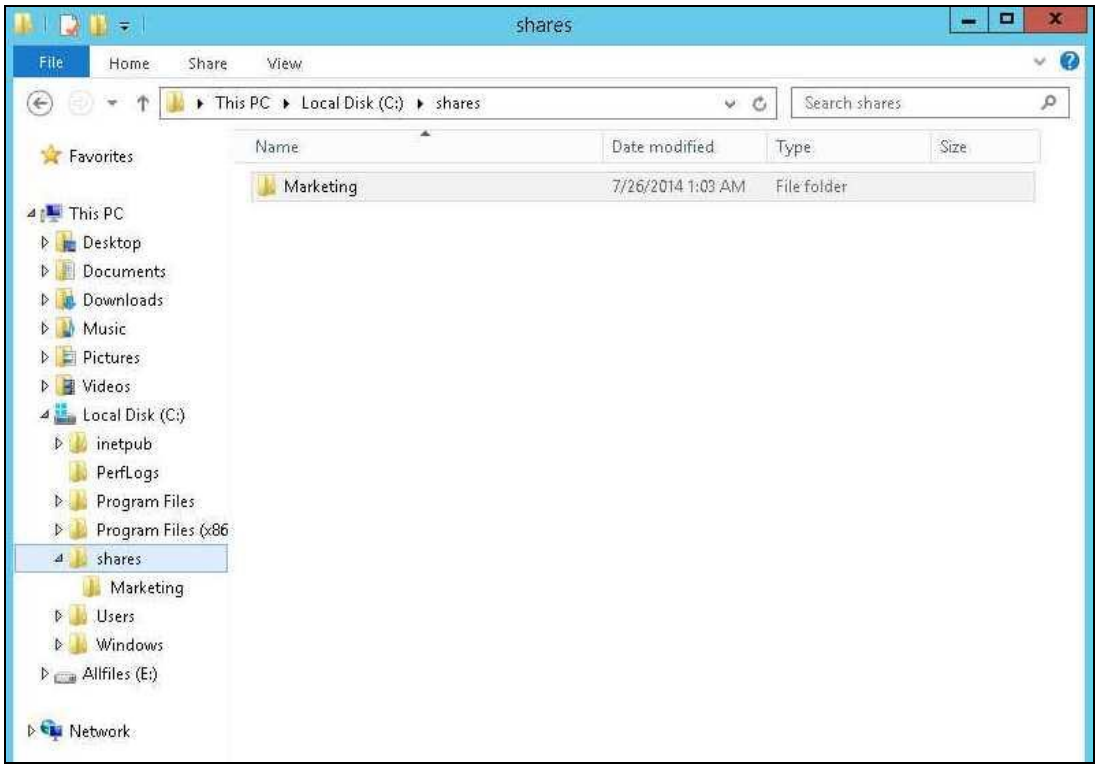
- New-Item c:\shares –ItemType Directory
- New-Item c:\shares\Marketing –ItemType Directory
- New-SmbShare –Name Marketing –Path c:\shares\Marketing –FullAccess ADatum\Marketing



6. Bung **File**, chọn **Run**.



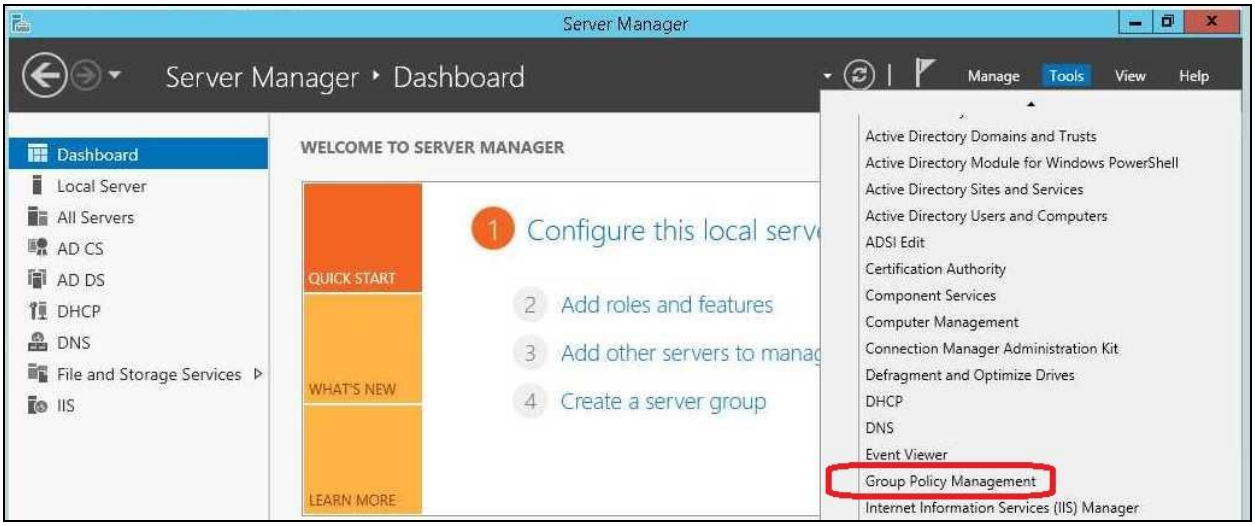
7. Mở **File Explorer**, vào đường dẫn **C:\shares**, kiểm tra có share folder **Marketing**



Bước 2. Tạo các GPO cần thiết và liên kết chúng vào các OU theo yêu cầu.

1. Qua máy **LON-DC1**

2. Mở **Server Manager**, bung menu **Tools**, chọn **Group Policy Management**.



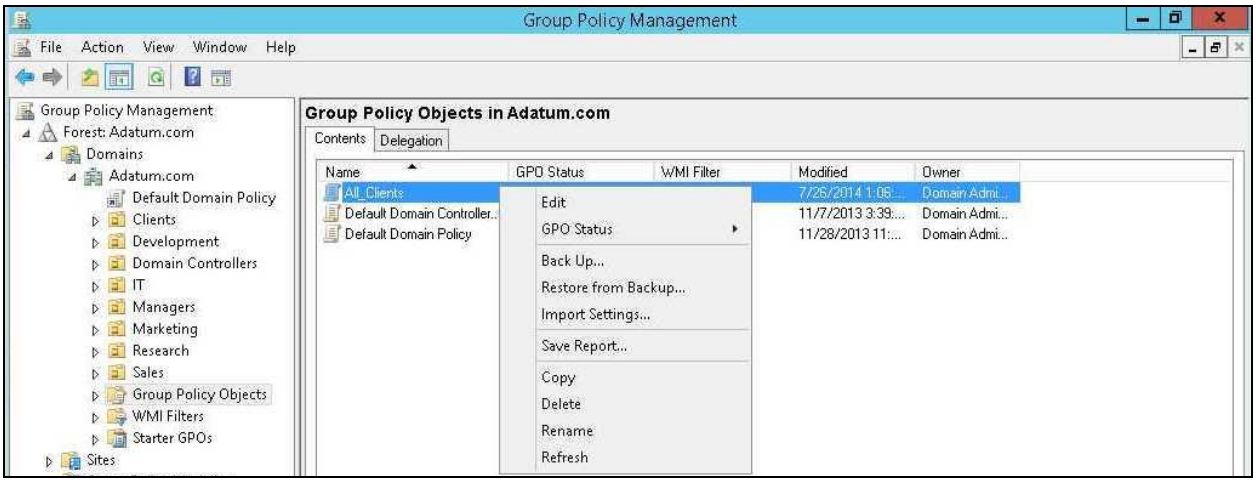
3. Trong cửa sổ **Group Policy Management Console**, bung **Forest Adatum.com**, bung **Domains**, bung **Adatum.com**, nhấn chuột phải **Group Policy Objects**, chọn **New**.



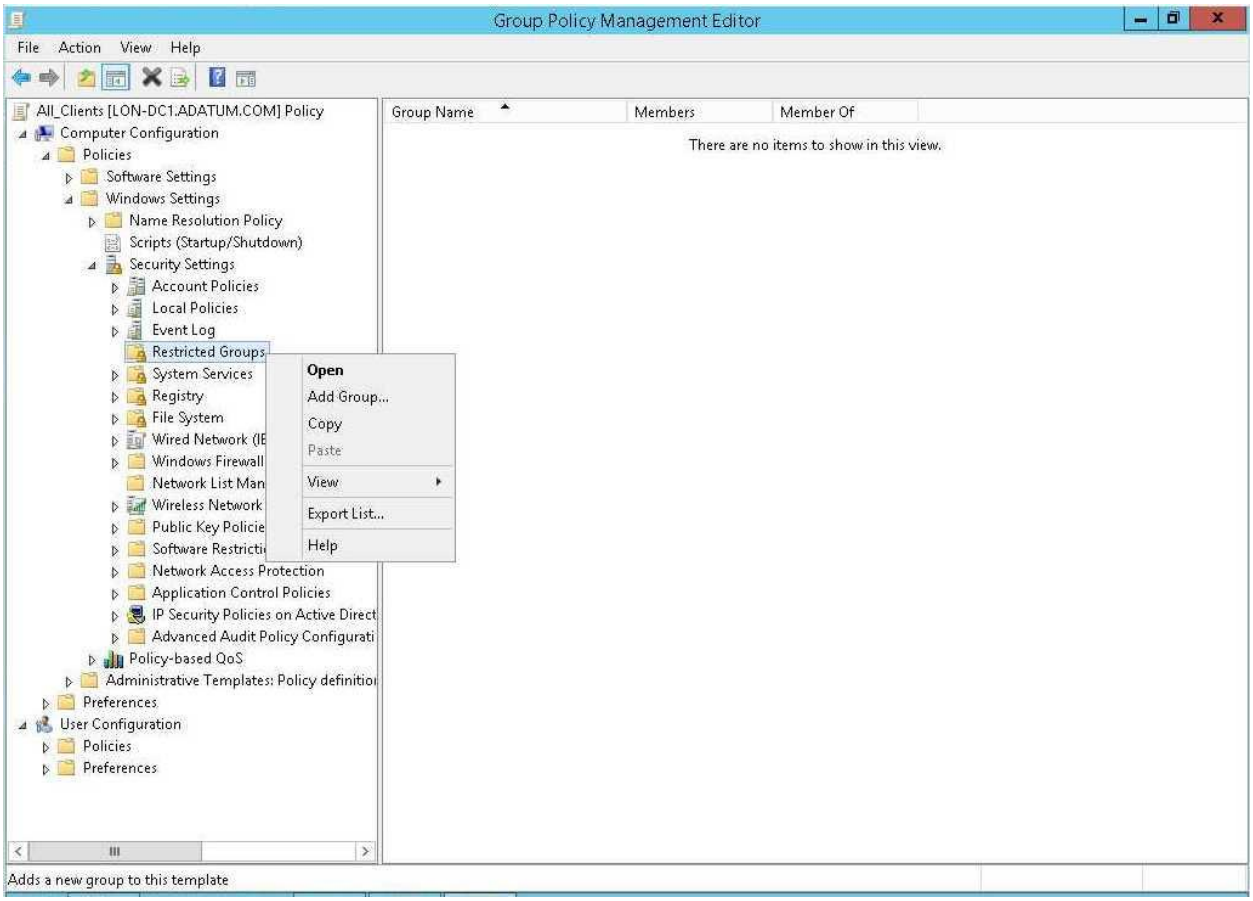
4. Hộp thoại **New GPO**, nhập tên **All_Clients** vào ô **Name**, chọn **OK**.



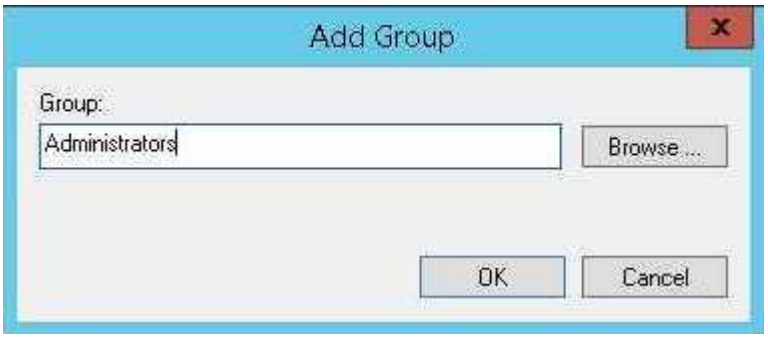
5. Nhấn chuột phải lên GPO **All_Clients**, chọn **Edit**.



6. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, nhấn chuột phải **Restricted Groups**, chọn **Add Group**.



7. Hộp thoại **Add Group**, nhập tên **Administrators** vào ô **Group**, chọn **OK**.



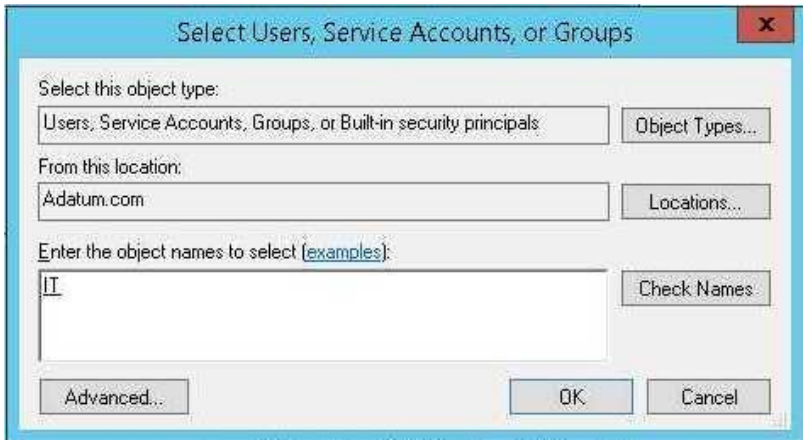
8. Hộp thoại **Administrators Properties**, trong ô **Members of this group**, chọn **Add**.



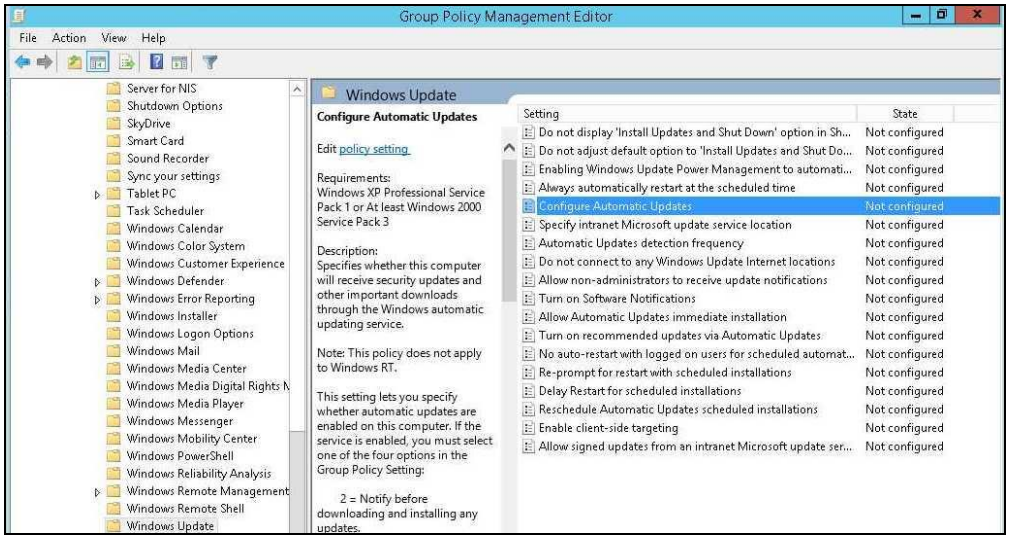
9. Hộp thoại **Add Member**, chọn **Browse**.



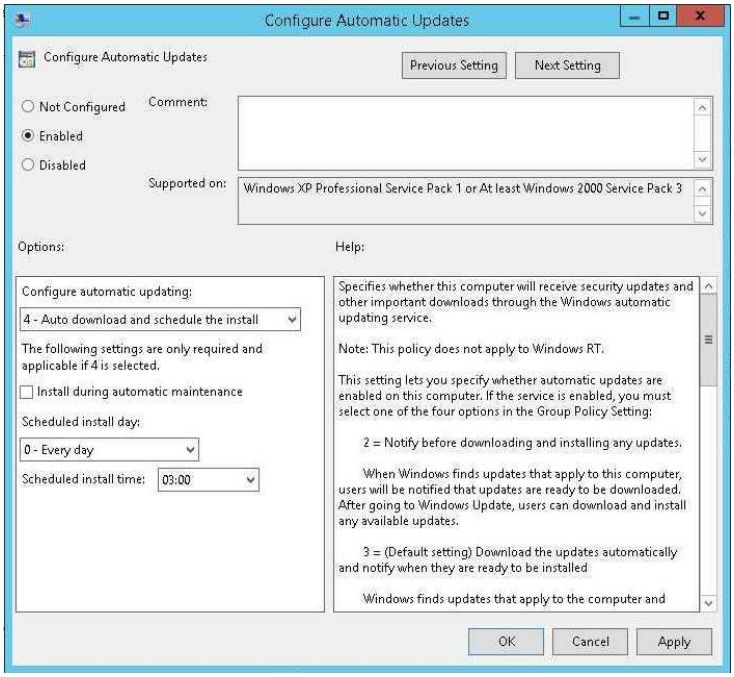
10. Hộp thoại **Select Users, Service Accounts, or Groups**, nhập tên **IT** vào ô **Enter the object names to select**, chọn **Check Names**, Chọn **OK** 3 lần để tắt các hộp thoại.



11. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Administrative Templates**, bung **Windows Components**, bung **Windows Update**, mở policy **Configure Automatic Updates**.

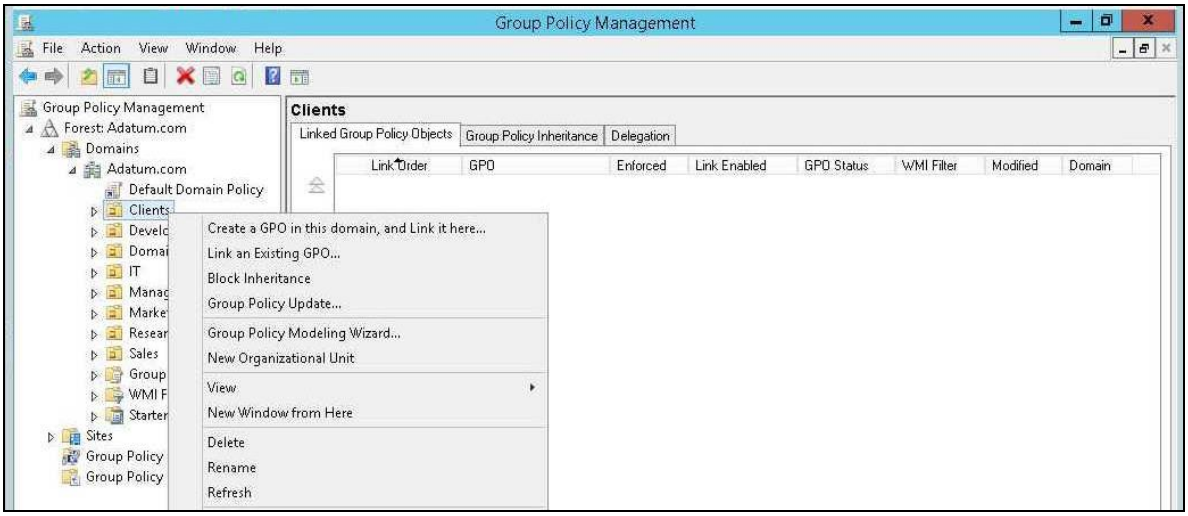


12. Trong hộp thoại Configure Automatic Updates, chọn **Enable,** bung ô **Configure automatic updating**, chọn **4 – Auto download and schedule the install**, chọn **OK**.

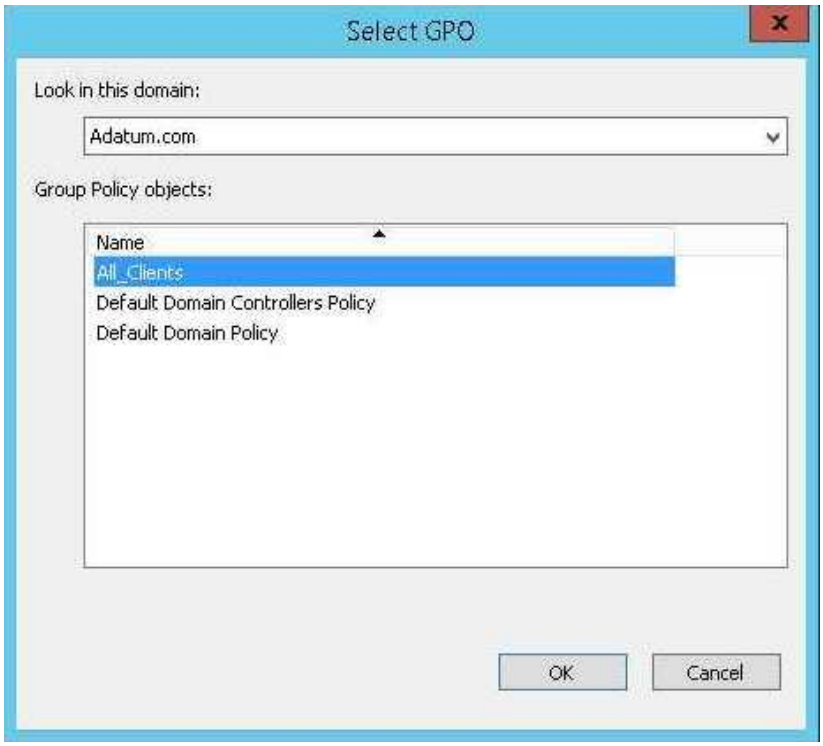


13. Tắt cửa sổ **Group Policy Management Editor**.

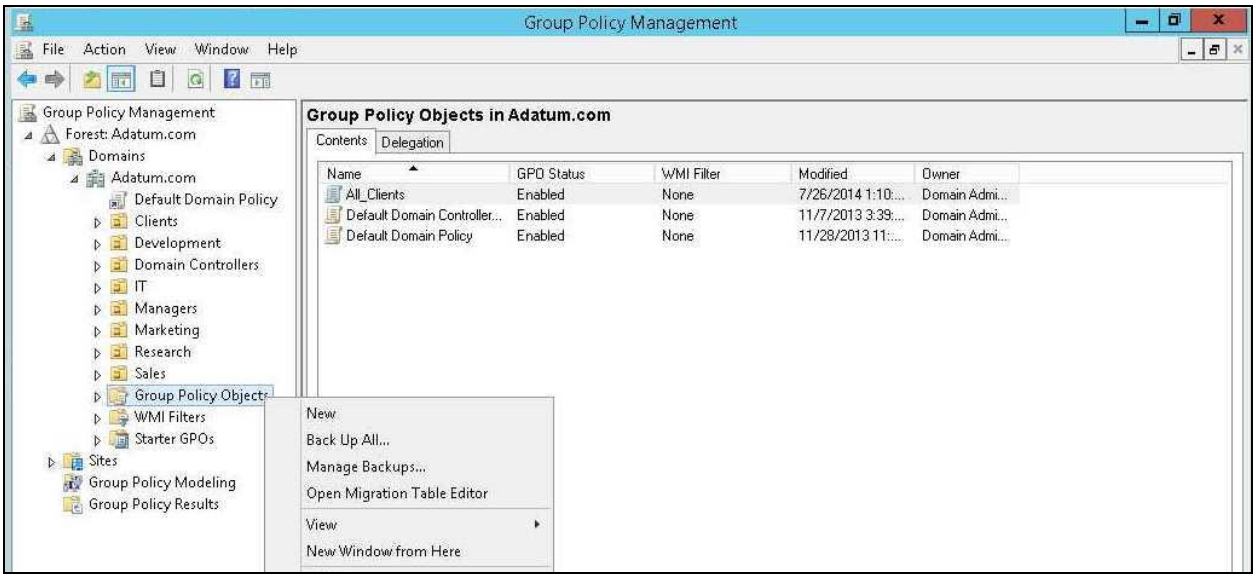
14. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải lên OU **Clients**, chọn **Link an Existing GPO**.



15. Hộp thoại **Select GPO**, chọn GPO **All_Clients**, và chọn **OK**.



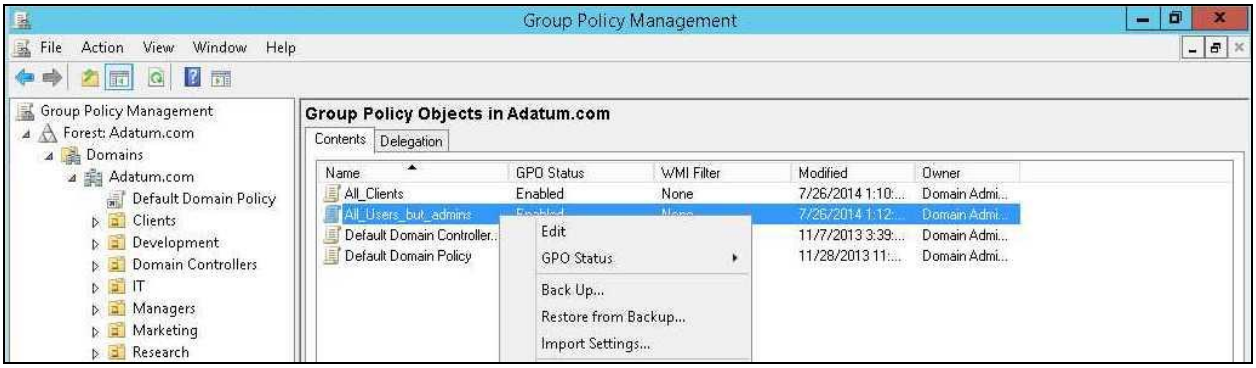
16. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải **Group Policy Objects**, chọn **New**.



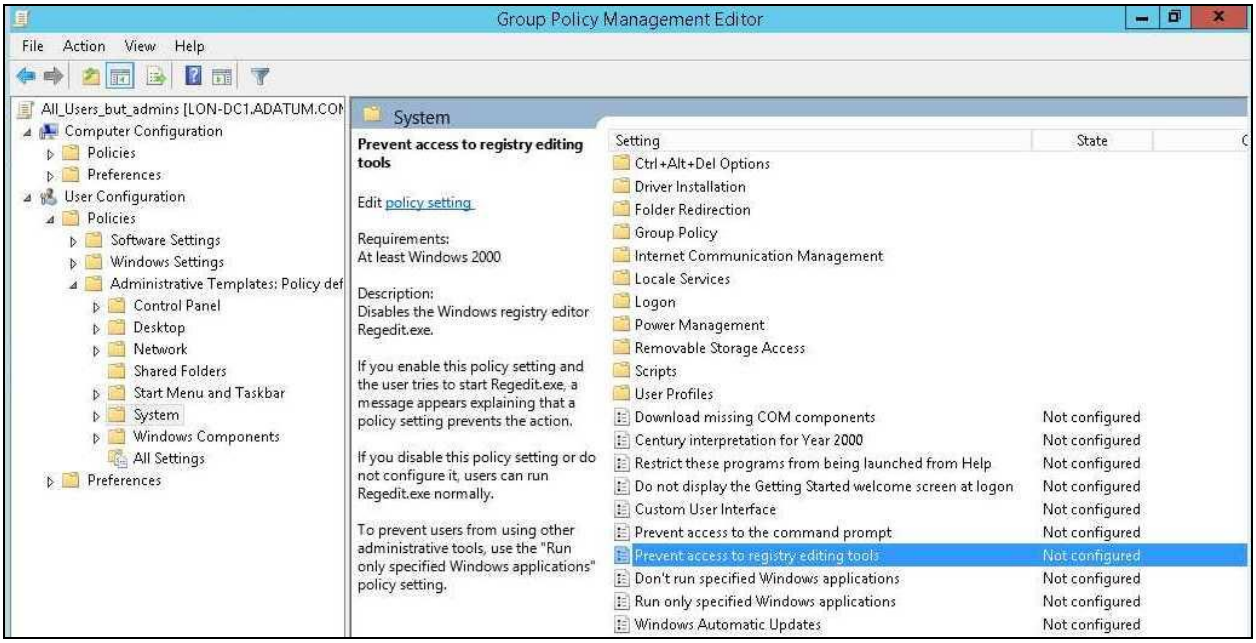
17. Hộp thoại **New GPO**, nhập tên **All_Users_but_Admins** vào ô **Name**, và chọn **OK**.



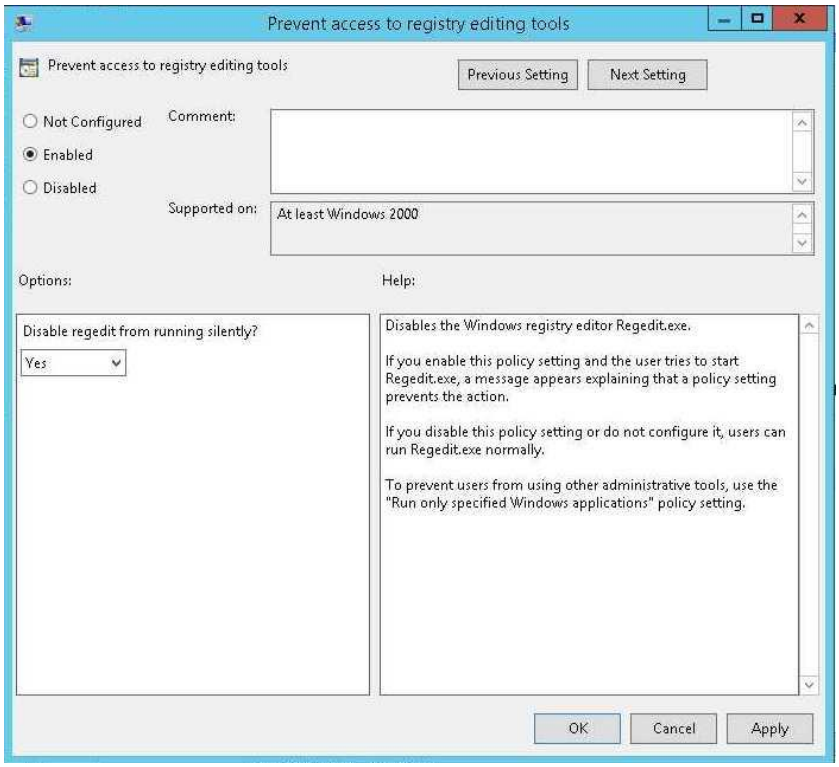
18. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải lên GPO **All_Users_but_Admins**, chọn **Edit**.



19. Cửa sổ **Group Policy Management Editor**, bung **User Configuration**, bung **Policies**, bung **Administrative Templates**, chọn mục **System**, mở policy **Prevent access to registry editing tools**.

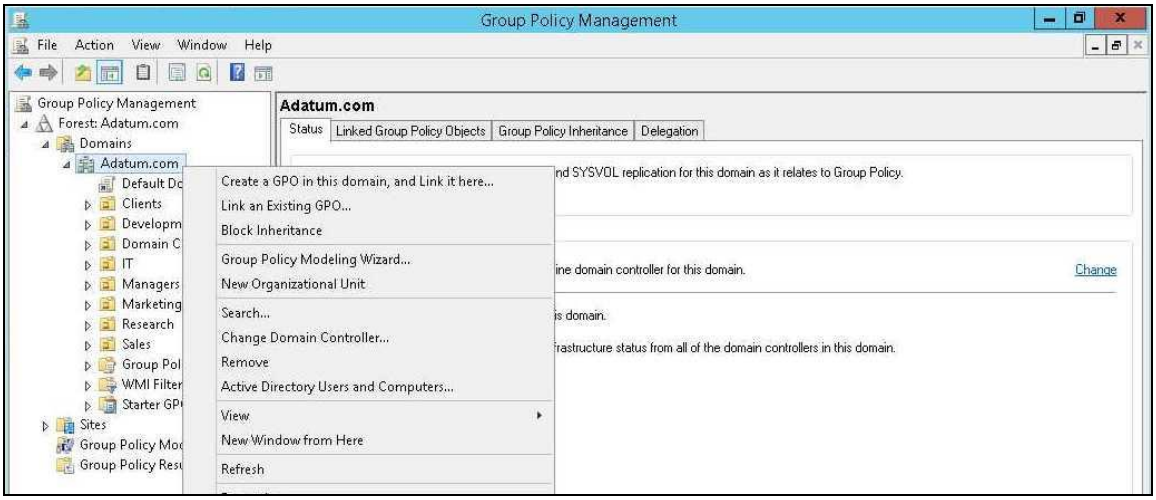


20. Hộp thoại **Prevent access to registry editing tools**, chọn **Enable**, chọn **OK**.

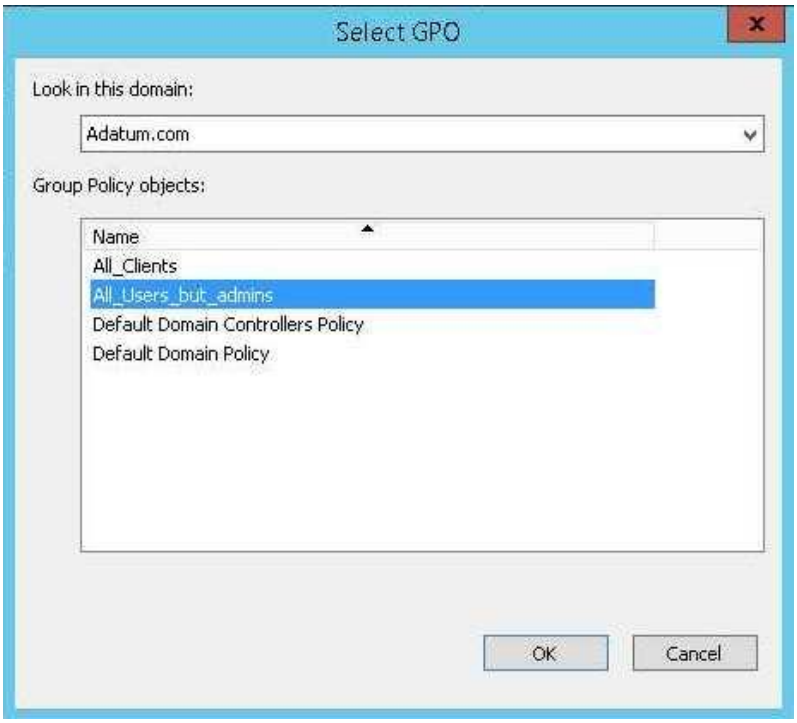


21. Tắt **Group Policy Management Editor**.

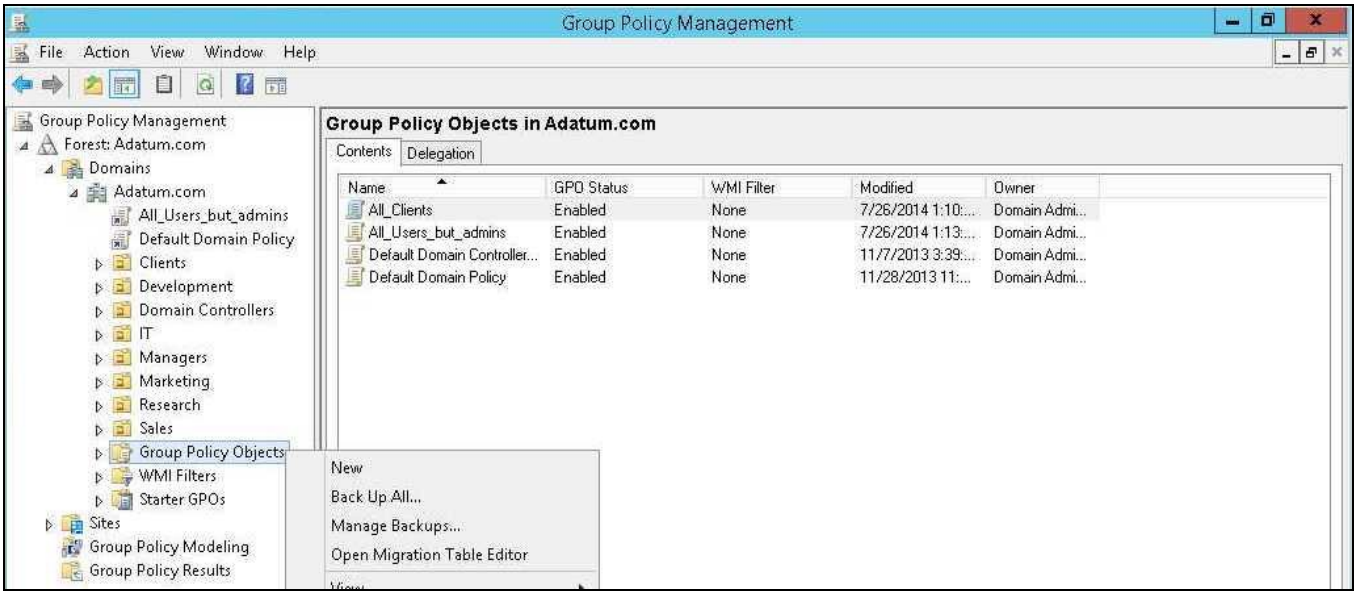
22. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải lên domain **Adatum**, chọn **Link an Existing GPO**.



23. Trong hộp thoại **Select GPO**, chọn **All_Users_but_Admins**, và chọn **OK**.



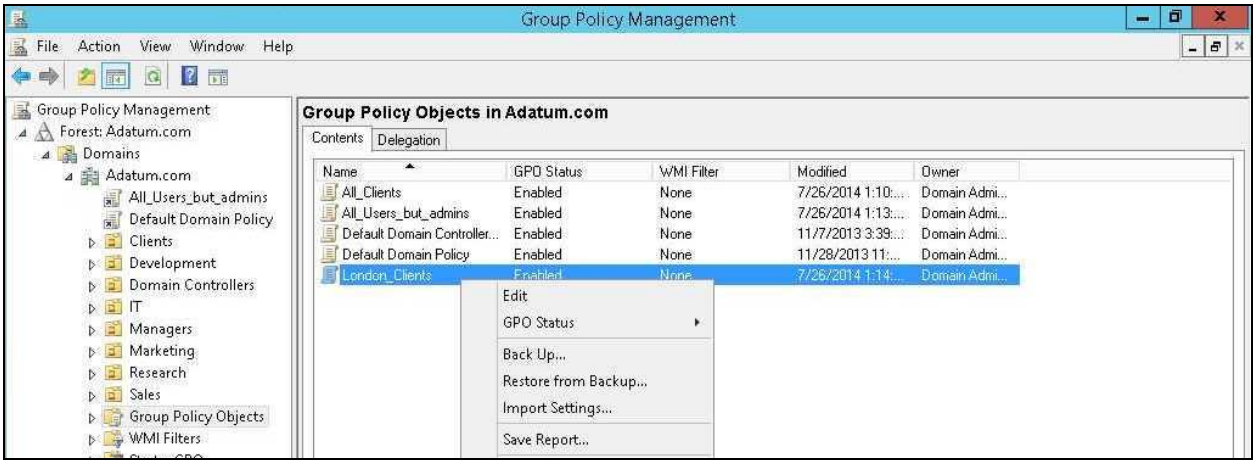
24. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải **Group Policy Objects**, chọn **New**.



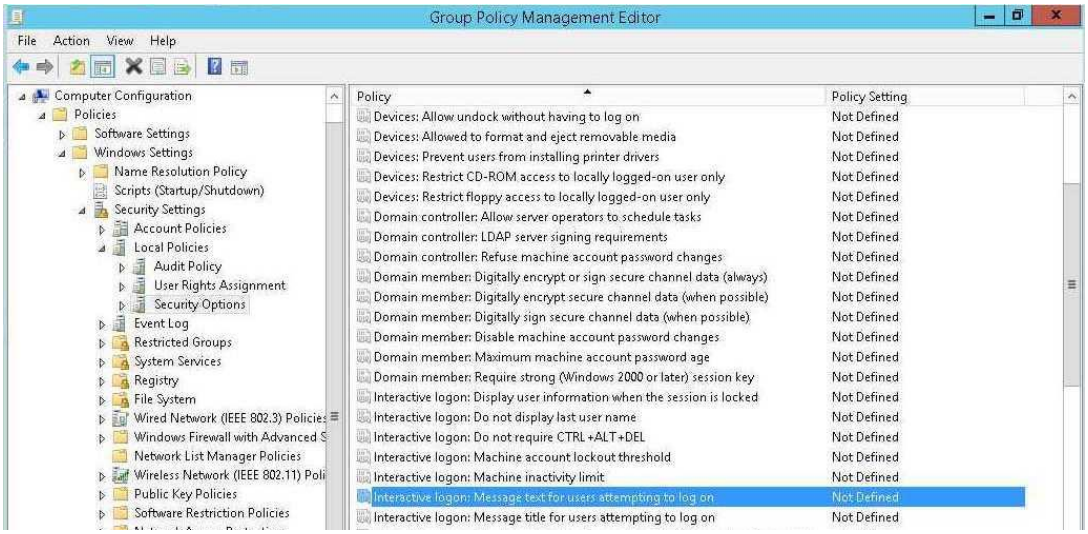
25. Hộp thoại **New GPO**, nhập tên **London_Clients** vào ô **Name**, và chọn **OK**.



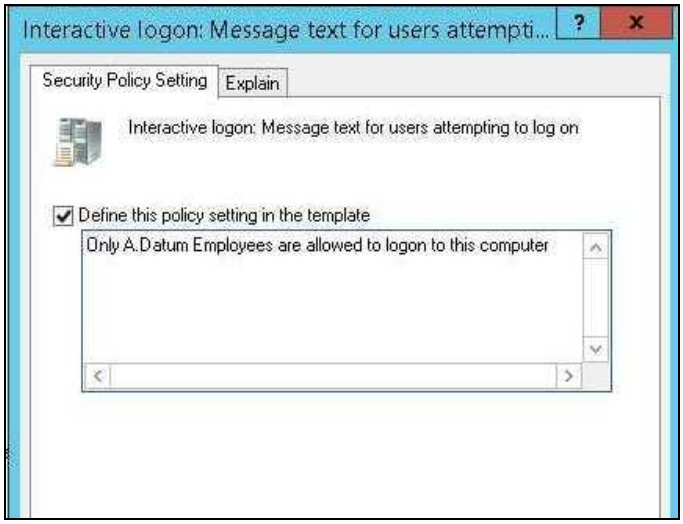
26. Nhấn chuột phải lên GPO **London_Clients**, chọn **Edit**.



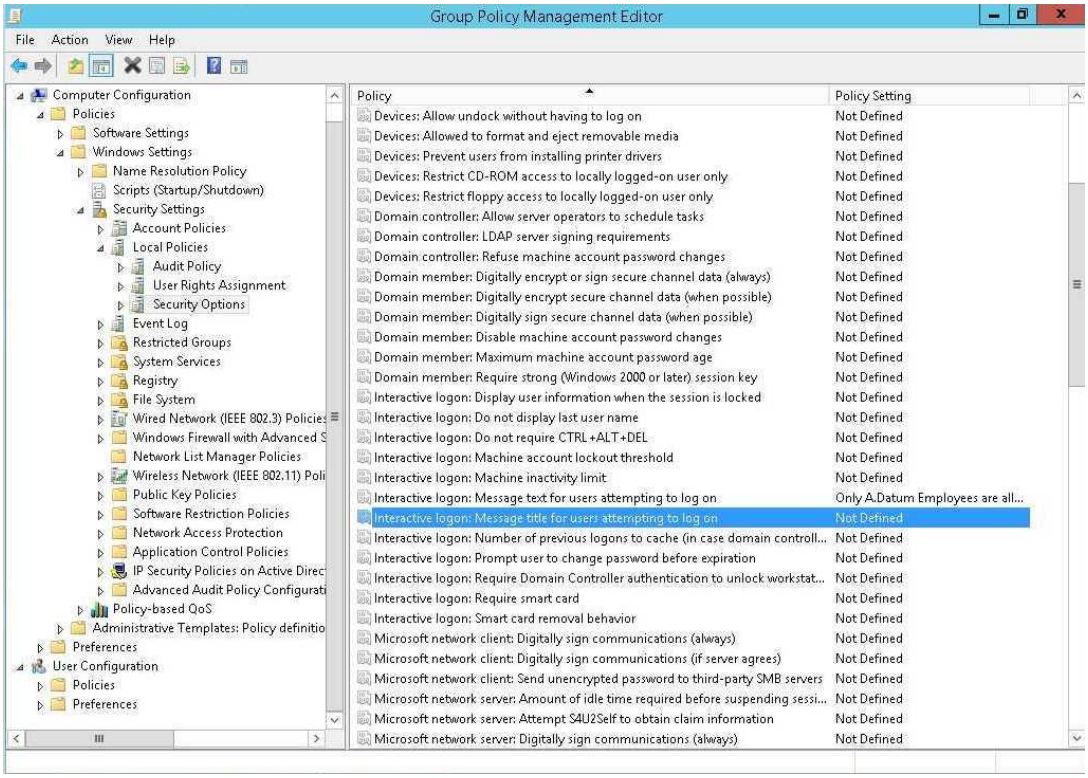
27. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Local Policies**, chọn **Security Options**, mở policy **Interactive Logon: Message text for users attempting to log on.**



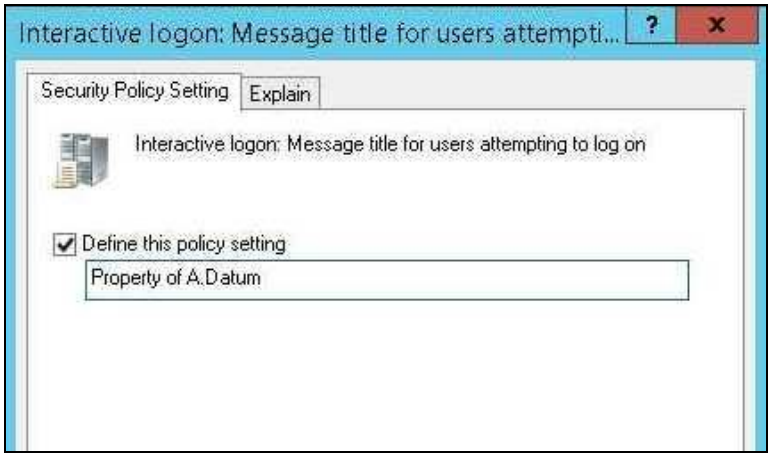
28. Đánh dấu chọn **Define this policy setting in the template**, nhập nội dung **Only A. Datum Employees are allowed to log on to this computer**, và chọn **OK**.



29. Trong cửa sổ **Group Policy Management Editor**, mở policy **Interactive Logon: Message title for users attempting to log on**.

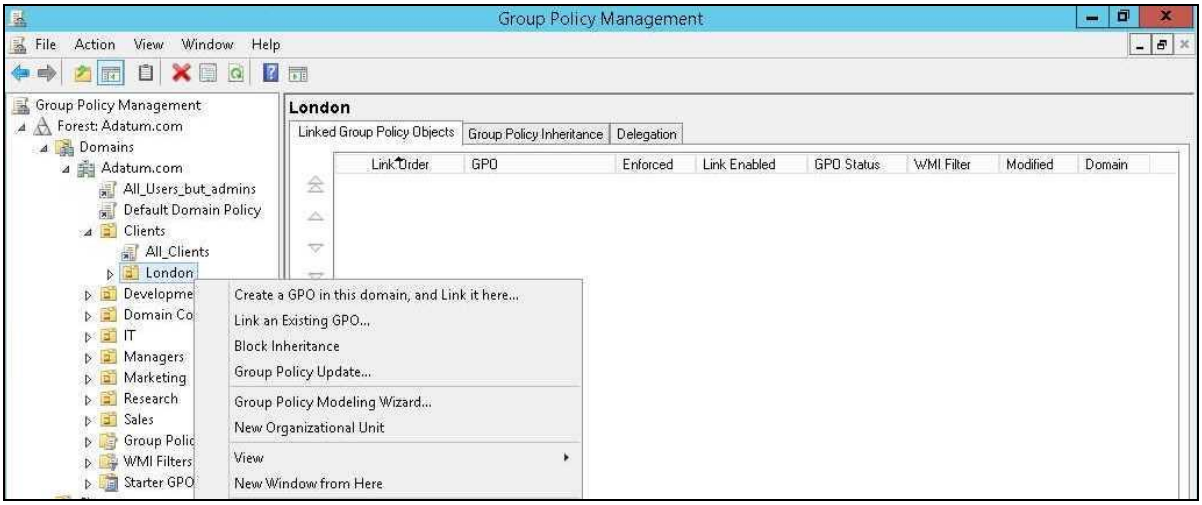


30. Đánh dấu chọn **Define this policy setting**, nhập nội dung **Property of A. Datum**, và chọn **OK**.

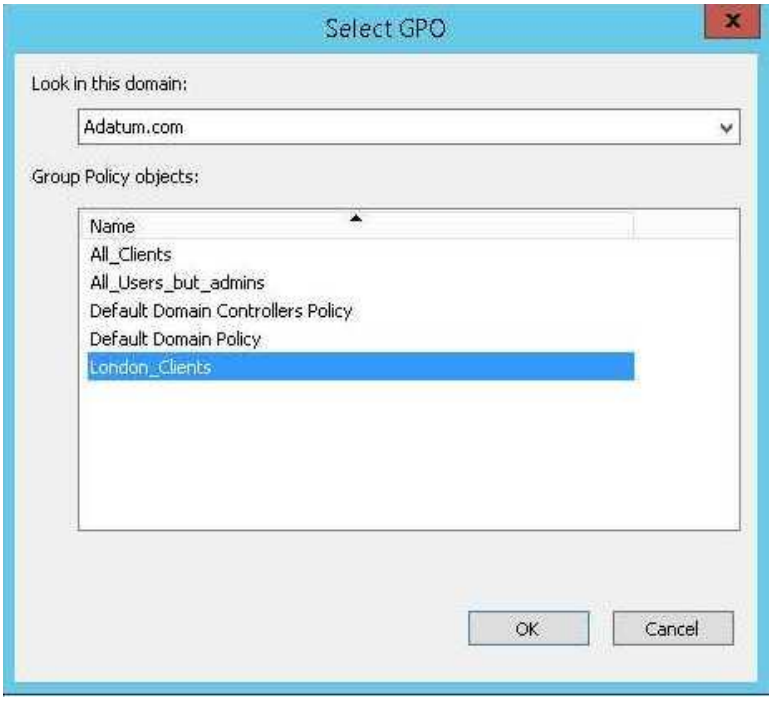


31. Tắt **Group Policy Management Editor.**

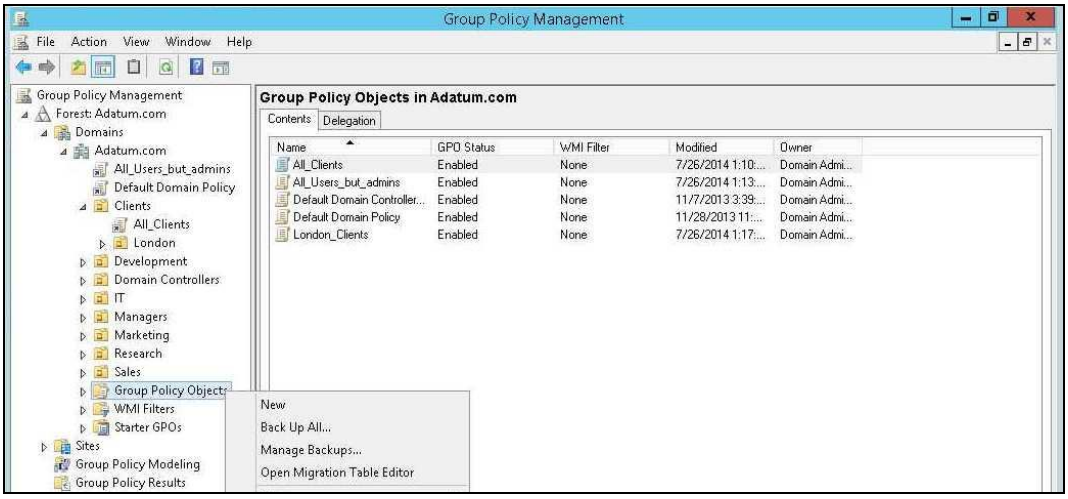
32. Trong cửa sổ **Group Policy Management Console**, bung OU **Clients**, nhấn chuột phải OU **London**, chọn **Link an Existing GPO**.



33. Hộp thoại **Select GPO** dialog box, chọn GPO **London_Clients**, chọn **OK**.



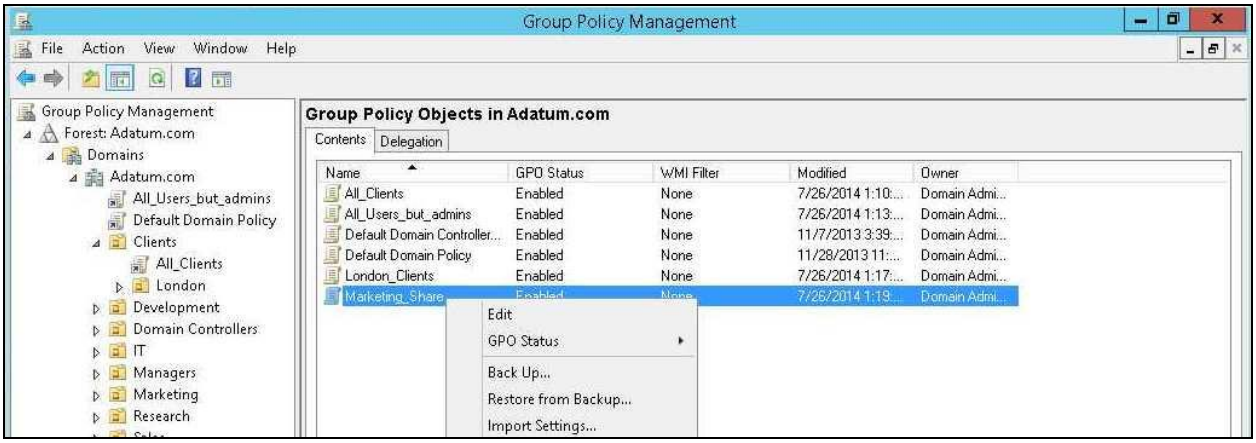
34. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải **Group Policy Objects**, chọn **New**.



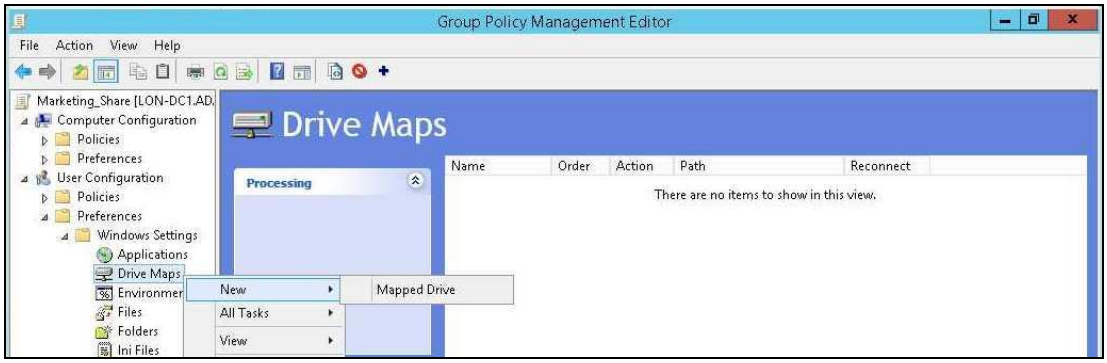
35. Trong hộp thoại **New GPO**, nhập tên **Marketing_Share** vào ô **Name**, và chọn **OK**.



36. Nhấn chuột phải lên policy **Marketing_Share**, chọn **Edit**.

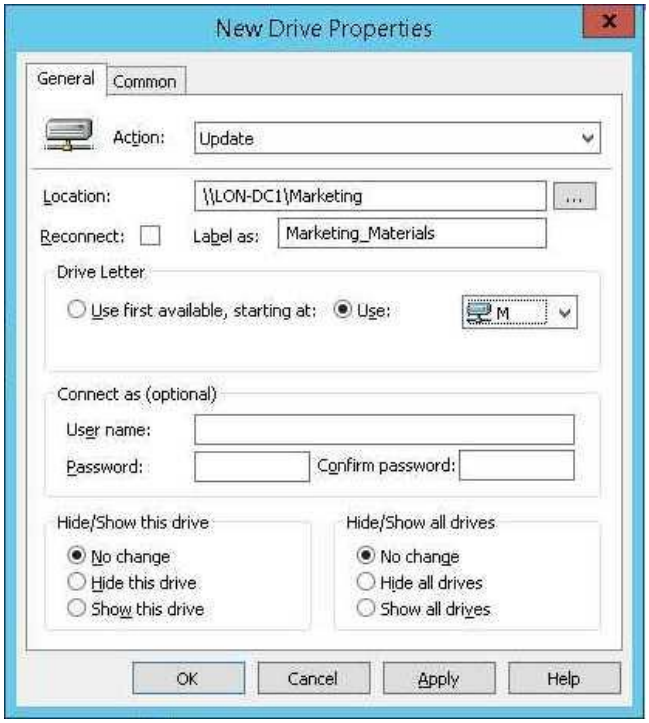


37. Trong cửa sổ **Group Policy Management Editor**, bung **User Configuration**, bung **Preferences**, bung **Windows Settings**, nhấn chuột phải **Drive Maps**, chọn **New**, và chọn **Mapped Drive**.



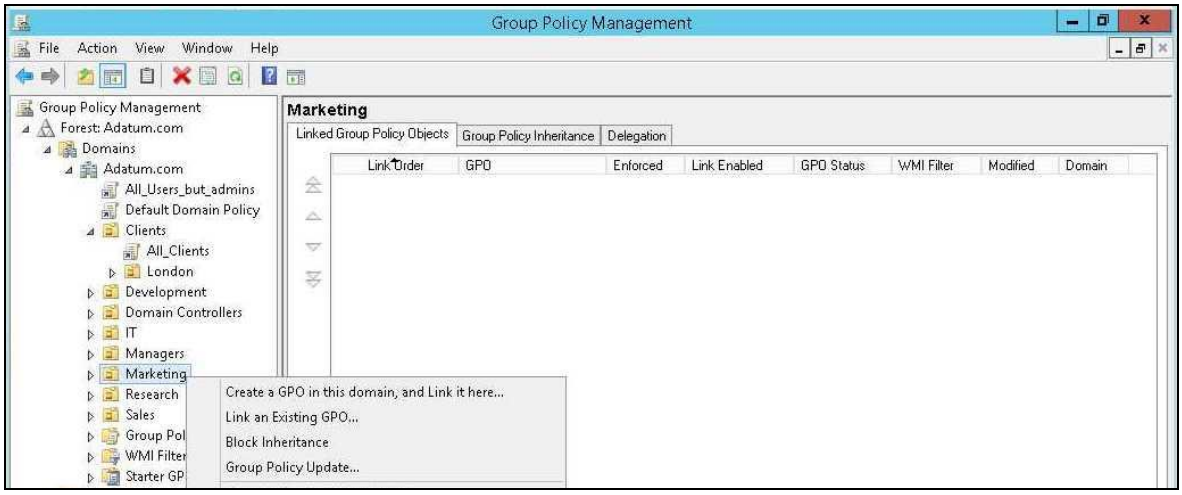
38. Hộp thoại **New Drive Properties**, cấu hình thông tin như bên dưới và chọn OK**:**

- Location: **\\LON-DC1\Marketing**.
- Label as: **Marketing-Materials**.
- Drive Letter: **M**.

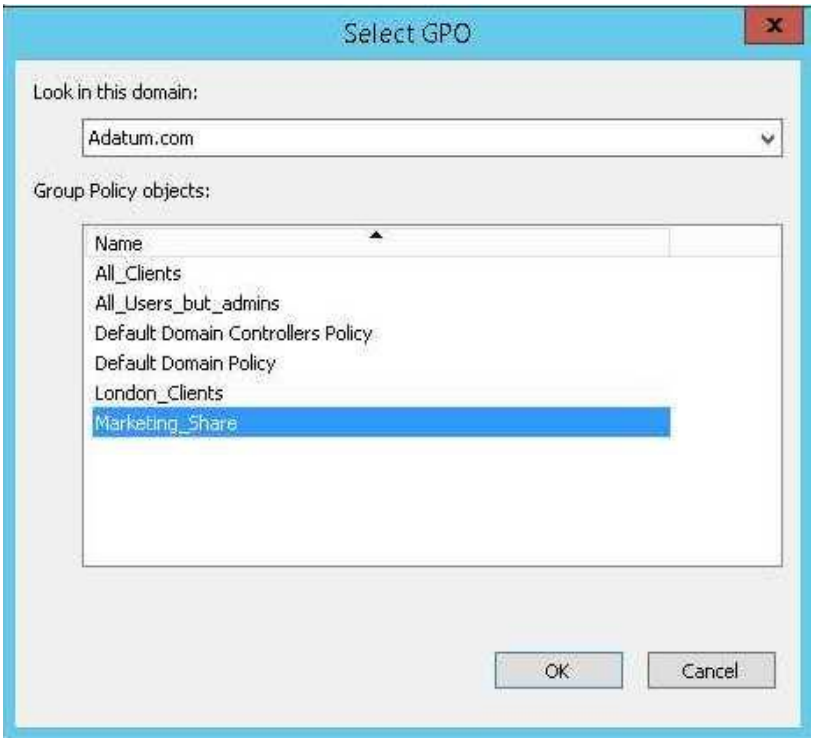


39. Tắt **Group Policy Management Editor**.

40. Trong cửa sổ **Group Policy Management Console**, nhấn chuột phải lên OU **Marketing**, chọn **Link an Existing GPO**.

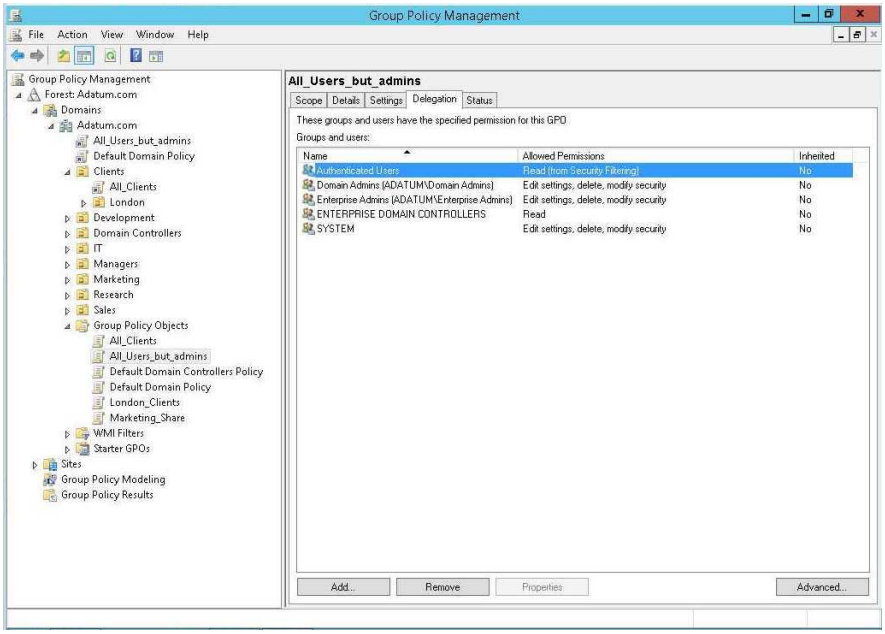


41. Hộp thoại **Select GPO**, chọn **Marketing_Share**, và chọn **OK**.

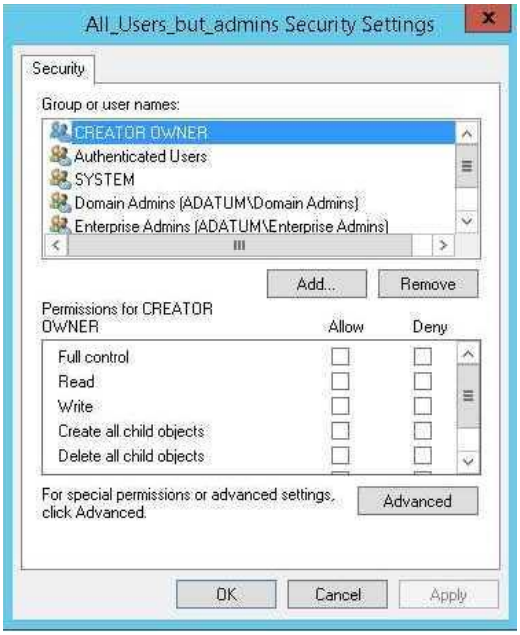


Bước 3 Cấu hình chức năng Filter.

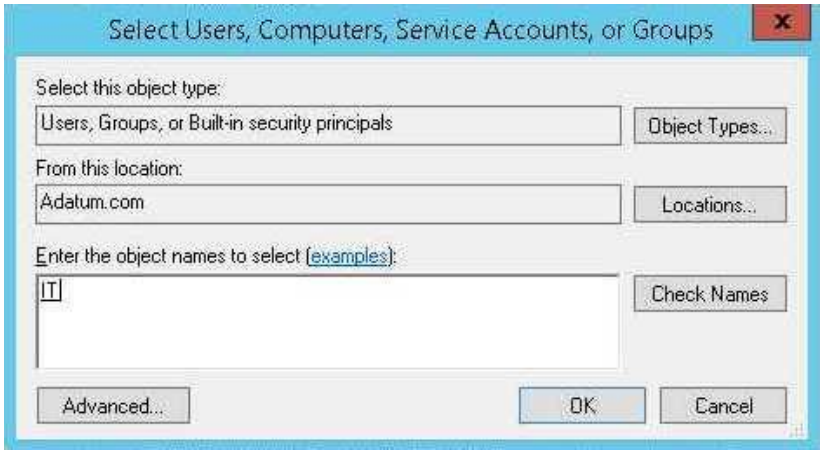
1. Trong cửa sổ **Group Policy Management**, bung **Group Policy Objects**, chọn GPO **All_Users_but_Admins**. Cửa sổ bên phải, qua tab **Delegation**, chọn **Advanced**.



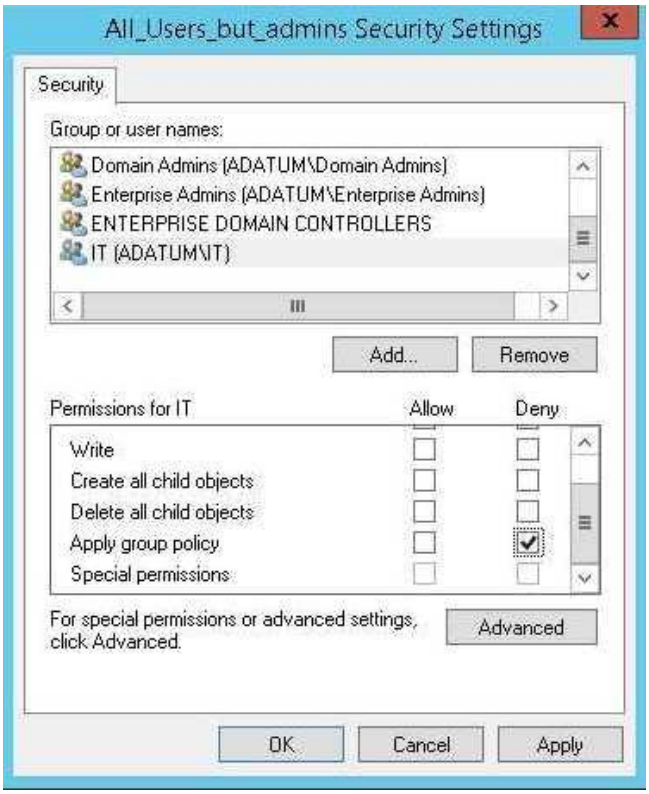
2. Trong hộp thoại **All_Users_but_Admins Security Settings**, chọn **Add**.



3. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, nhập tên **IT** vào ô **Enter the object names to select**, chọn **Check Names**, và chọn **OK**



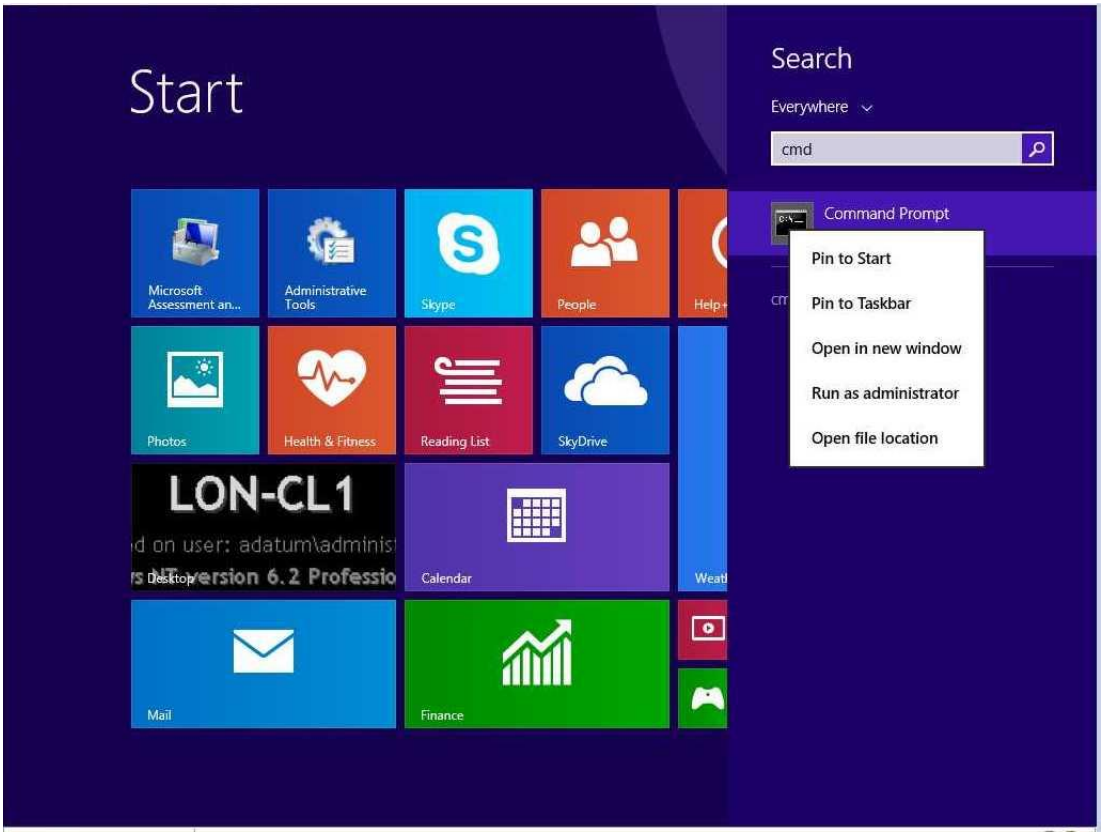
4. Trong hộp thoại **All_Users_but_Admins**, chọn group **IT**, đánh dấu chọn vào ô **Deny** của quyền **Apply group policy ,** chọn **OK**, và chọn **Yes**.



Bước 4: Kiểm tra kết quả.

1. Qua máy **LON-CL1**, logon **Adatum\Administrator** với password **Pa$$w0rd**.

2. Bung **Start** menu, gõ **cmd**, nhấn chuột phải **Command Prompt**, chọn **Run as Administrator**.

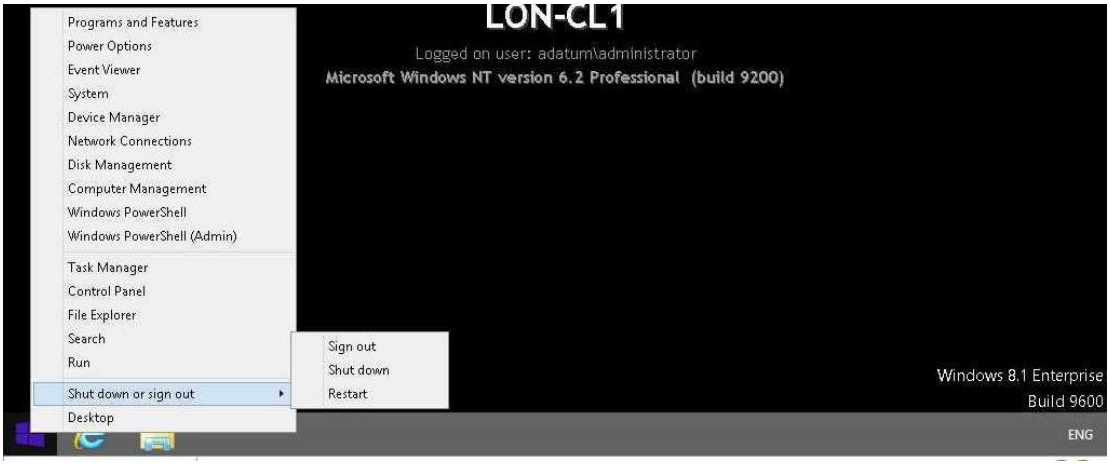


3. Trong cửa sổ **Administrator: Command Prompt**, gõ lệnh: **gpupdate /force.**



4. Tắt **Command Prompt.**

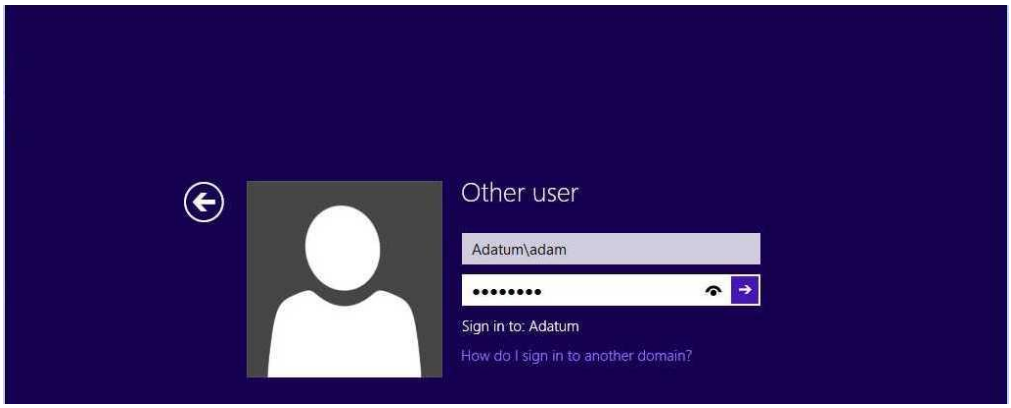
5. Nhấn chuột phải **Start** menu, bung **Shut down or sign out**, và chọn **Restart**.



6. Sau khi máy **LON-CL1** khởi động thành công, kiểm tra nhận được thông báo sau:



7. Logon bằng tài khoản **Adatum\Adam** với password **Pa$$w0rd**.



Chú ý: Adam Barr là thành viên của group Marketing.

8. Sau khi logon thành công, mở công cụ **Control Panel**. Trong **Control Panel**, chọn **System and Security**.



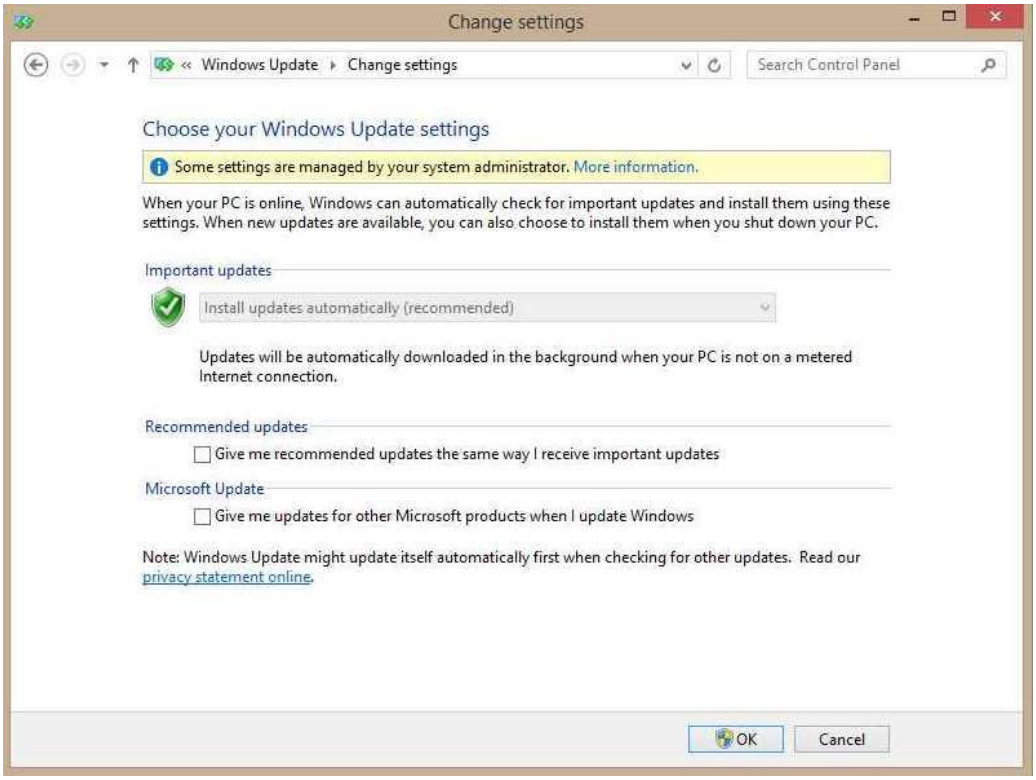
9. Trong System and Security, chọn **Windows Update**.



10. Chọn **Change settings**.

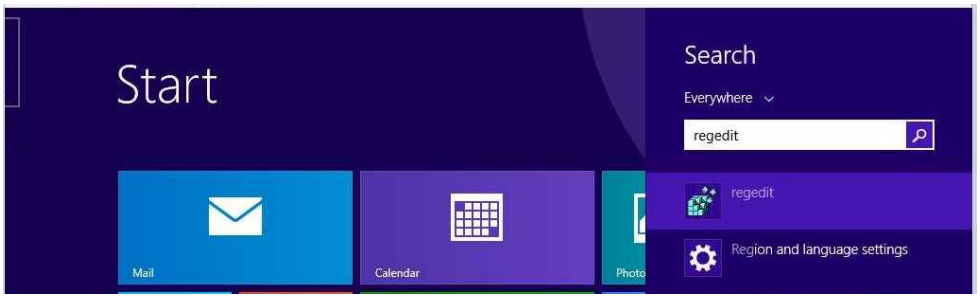


11. Trong cửa sổ **Change Settings**, chú ý thông báo: **Some settings are managed by your system administrator**. Trong ô **Important Updates**, đang chọn chế độ **Install updates automatically (recommended)**, và không chophép thay đổi chế độ **Important Updates**.



12. Chọn **OK**, và tắt **Control Panel.**

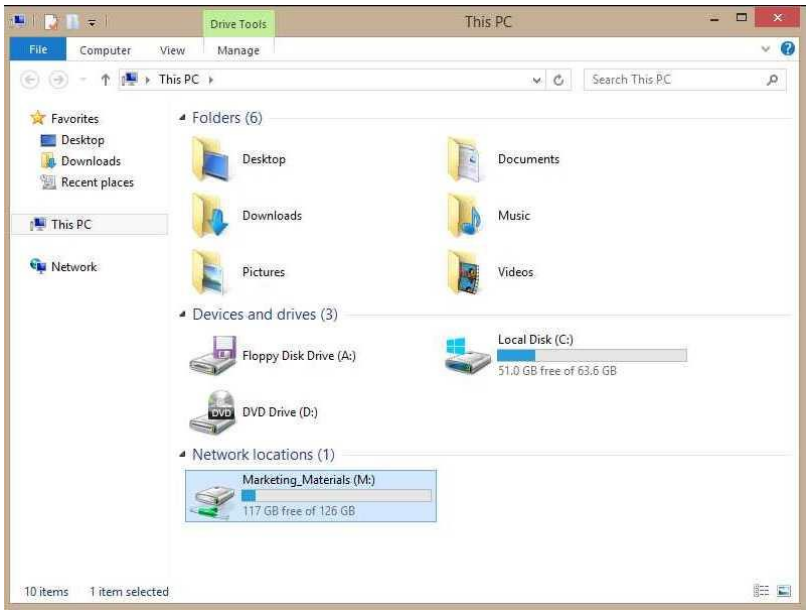
13. Bung **Start** meny, gõ **Regedit**, và mở **Regedit**.



14. Chú ý nhận được thông báo: **Registry editing has been disabled by your administrator**.



15. Mở **File Explorer**, chọn **This PC**, trong phần **Network Locations**, chú ý có ổ đĩa **Marketing-Materials (M:).**



16. Nhấn chuột phải **Start** menu, bung **Shut down or sign out,** chọn **Sign out**.



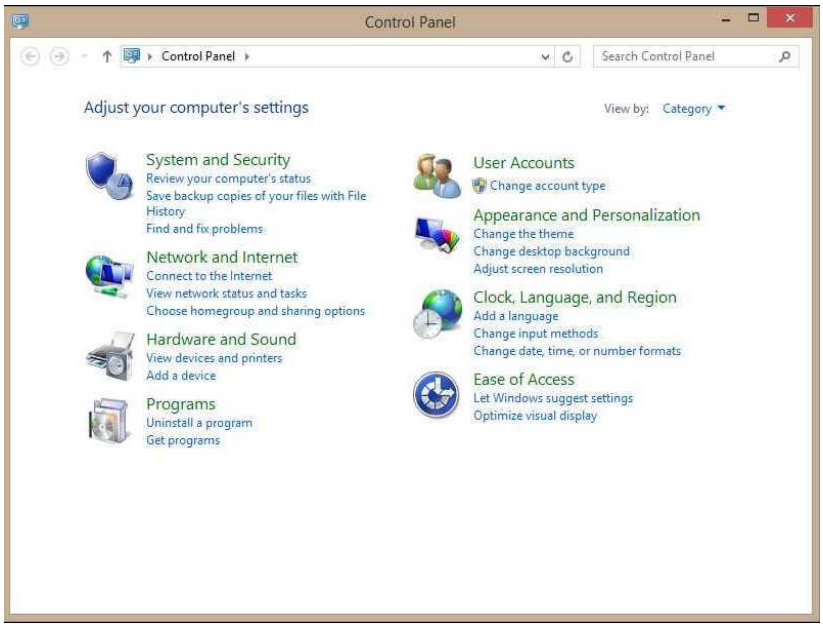
17. Logon bằng tài khoản **Adatum\Brad** với password **Pa$$w0rd**.



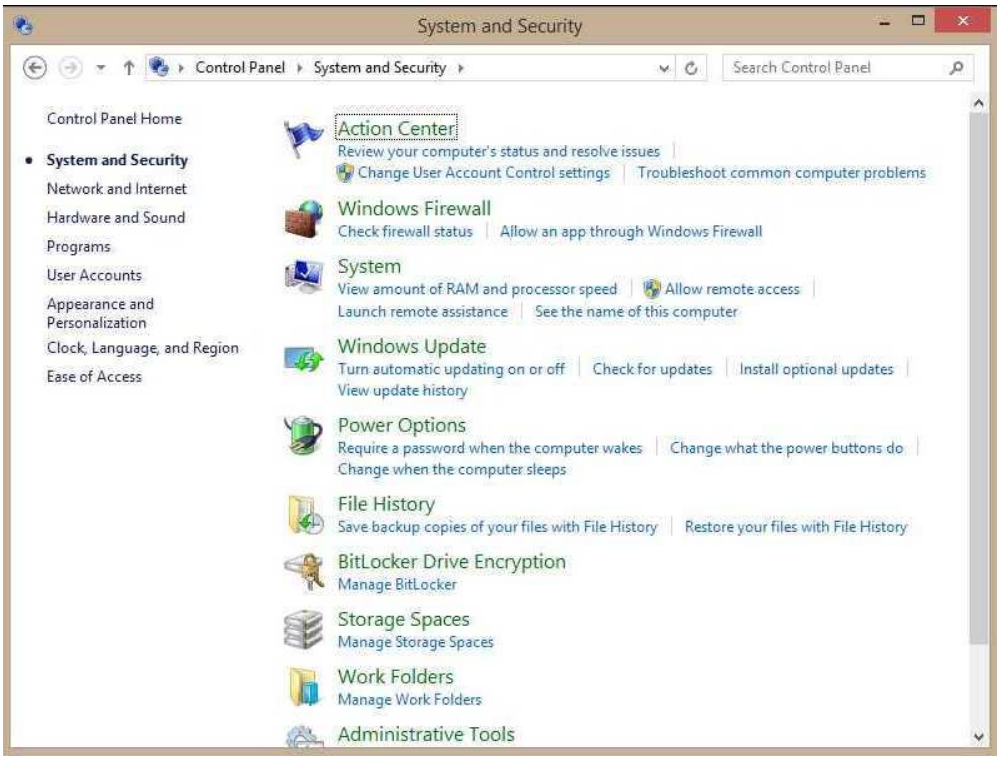
Chú ý: Trước khi đăng nhập, Brad đang nhận được một thông báo sau:



18. Sau khi logon thành công, mở công cụ **Control Panel**, chọn **System and Security**.



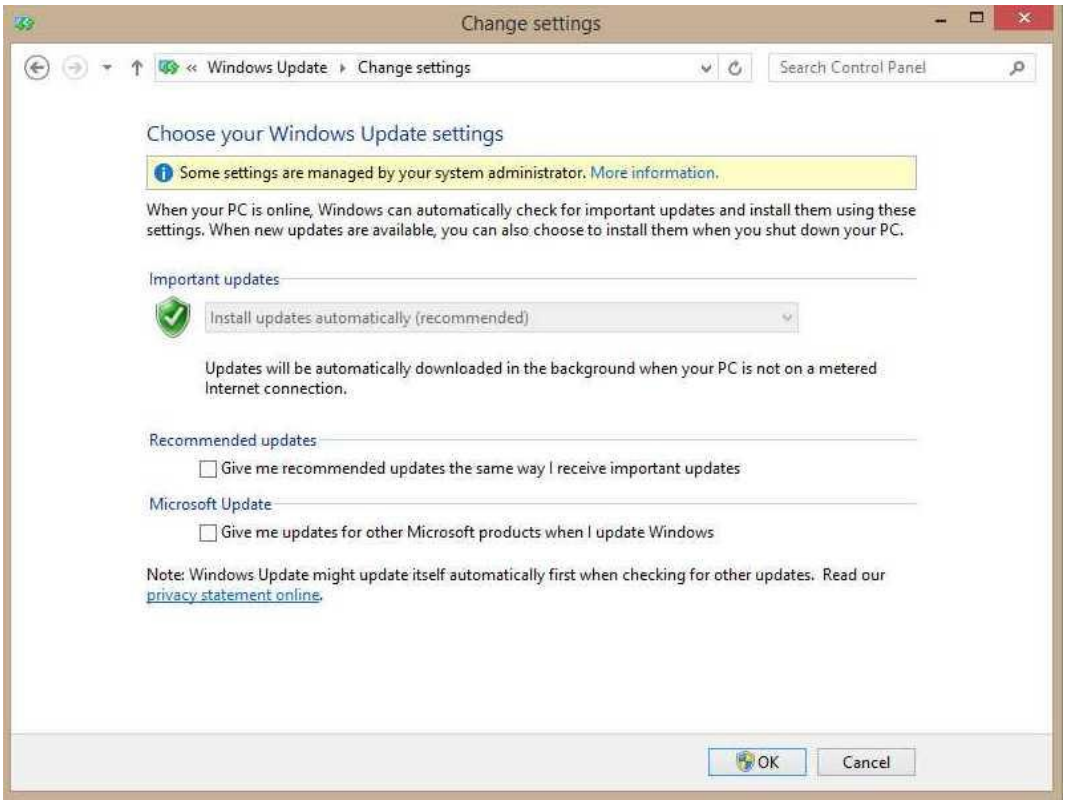
19. Trong System and Security, chọn **Windows Update**.



20. Chọn **Change settings**.



21. Trong cửa sổ **Change Settings**, chú ý thông báo: **Some settings are managed by your system administrator**. Trong ô **Important Updates**, đang chọn chế độ **Install updates automatically (recommended)**, và không cho phép thay đổi chế độ **Important Updates**.



22. Chọn **OK**, và tắt **Control Panel.**

23. Bung **Start** menu, gõ **regedit**, mở công cụ r**egedit**.



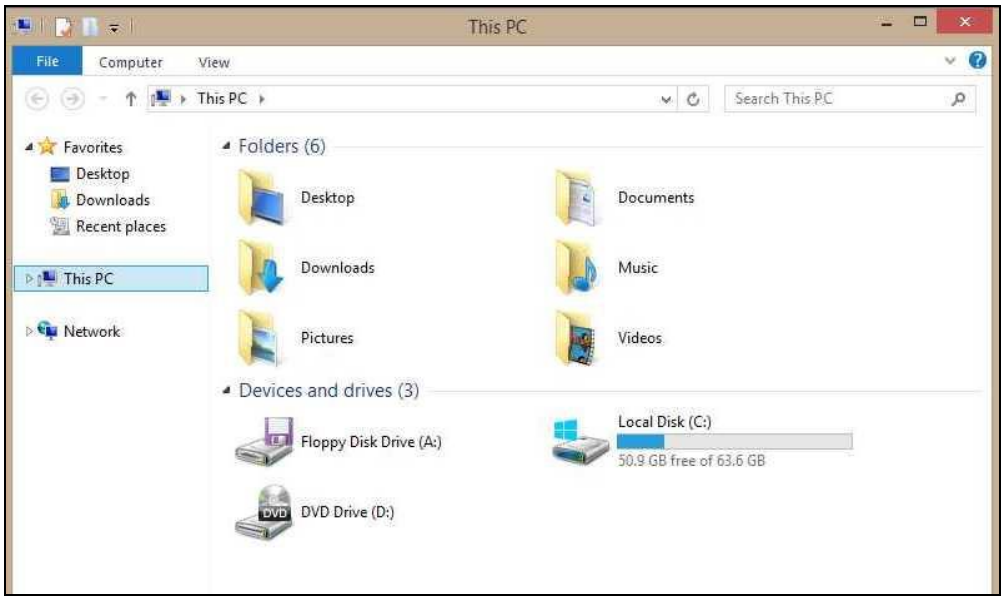
24. Hộp thoại **User Account Control**, chọn **Yes**



Chú ý: Mở công cụ Registry thành công.



25. Trên thanh taskbar, mở **File Explorer**. Kiểm tra không có ổ đĩa **Marketing-Materials (M:).**

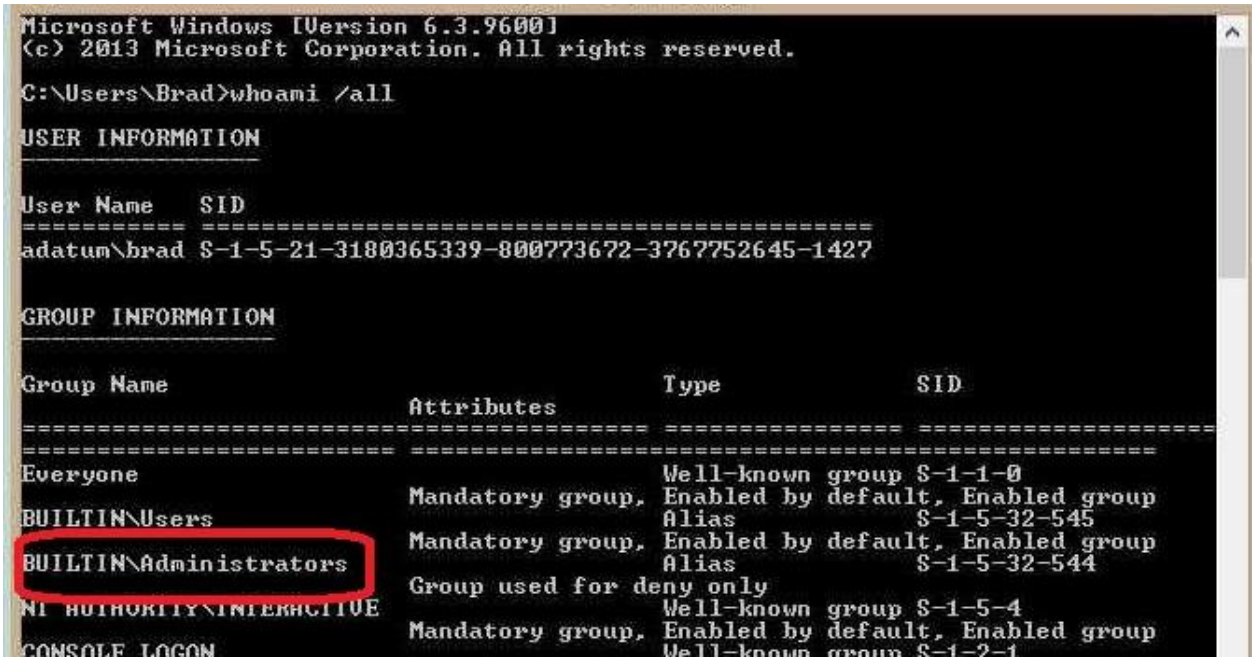


26. Bung **Start** menu, gõ **cmd**, mở **Command Prompt**.



27. Trong cửa sổ command prompt, gõ lệnh: **whoami /all**

28. Kiểm tra **Brad** là thành viên của group local Administrator.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã thực hiện thành công việc thiết kế và triển khai GPO theo yêu cầu của công ty A. Datum.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-LON-CL1**.

Bài 9: Thiết kế và triển khai mô hình Active Directory Sites

I. Mục tiêu:

- Thiết kế mô hình AD có nhiều Site.
- Lập kế hoạch triển khai Domain Controller trong mỗi Site.
- Thực hiện chia Site và di chuyển Domain Controller vào Site tương ứng.

II. Kịch bản:

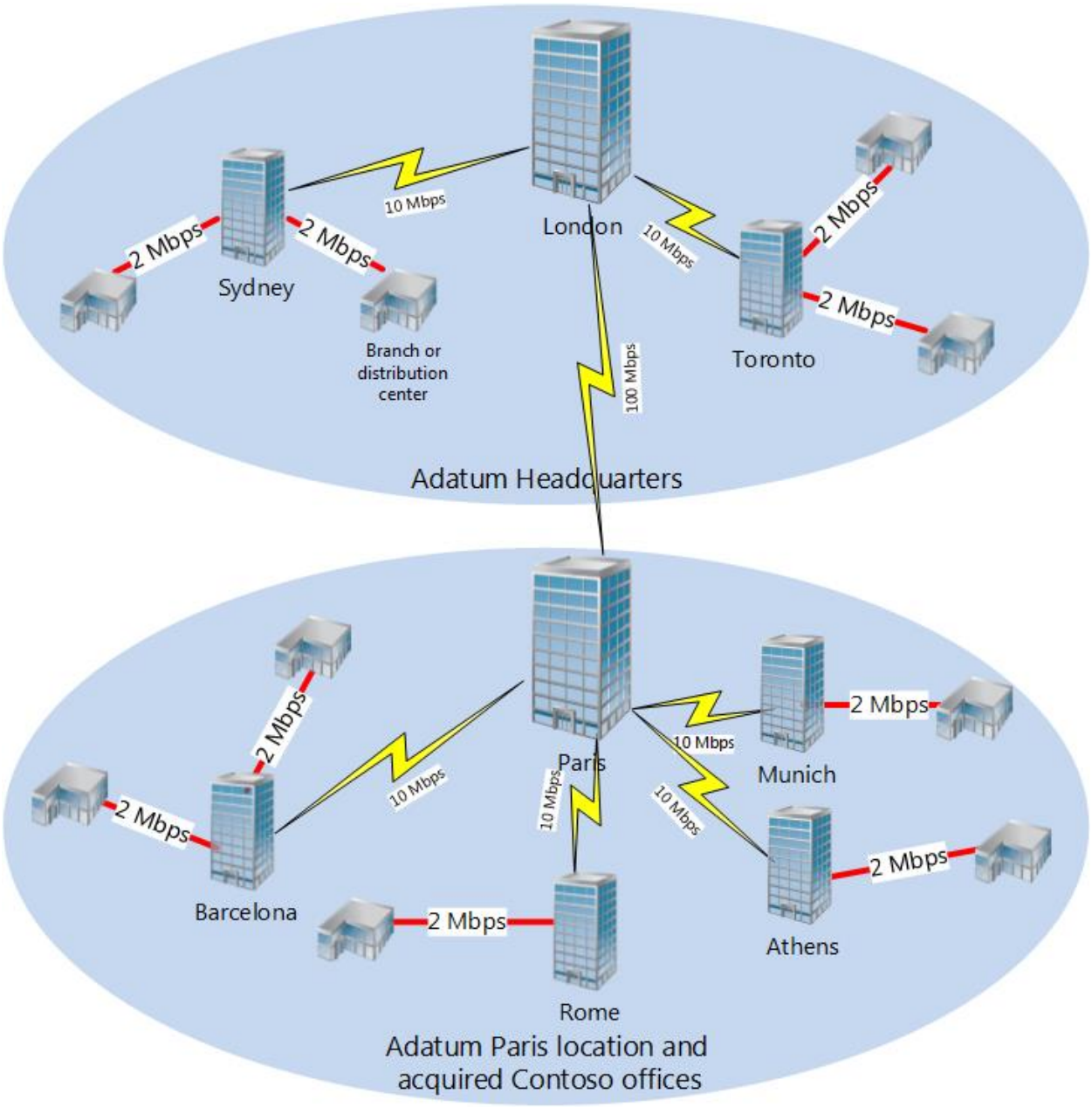
Công ty A. Datum đã trải qua một số vấn đề với việc triển khai hệ thống AD. Bởi vì những vấn đề này, nhóm thiết kế AD phải xem xét các vị trí và cấu trúc đồng bộ trong hệ thống AD hiện tại, và sau đó cung cấp các khuyến nghị cho việc thực hiện những thay đổi. Bạn được giao nhiệm vụ điều tra nguyên nhân của các vấn đề này, và sau đó thiết kế một giải pháp phù hợp cho A. Datum.

Các vấn đề hiện hữu của A. Datum:

- Thỉnh thoảng, người sử dụng ở London và Paris đăng nhập vào hệ thống rất chậm.
- E-mail được gửi thông qua Exchange Server có thể mất vài phút để đến nơi. Nhóm quản trị hê thống Exchange cung cấp thông tin cho biết nguyên nhân của việc này là do sự phản ứng chậm từ Domain Controller. Hiện nay, A. Datum triển khai các Exchange Server ở Paris và London.
- Đội ngũ thiết kế AD phải cung cấp một thiết kế cho nhiều văn phòng chi nhánh mới. Những văn phòng này được kết nối với văn phòng ở Paris bằng các đường truyền tốc độ cao. Bởi vì các văn phòng này tương đối nhỏ (nhưng đang phát triển), họ không có nhân viên IT chuyên dụng. Các nhân viên IT ở Paris không triển khai Domain Controller mới ở các địa điểm này, nhưng họ đang xem xét lựa chọn thay thế trong trường hợp tốc độ đường truyền giữa Paris và các văn phòng chi nhánh giảm bất ngờ.
- Một cơ sở sản xuất sẽ được đặt tại Rome. Người dùng tại Rome sẽ kết nối đến Paris rất nhiều trong giờ làm việc để truy cập cơ sở dữ liệu và chia sẻ file. Hiện nay, trong

hệ thống AD đã có một Site tồn tại cho vị trí London. Tại mỗi địa điểm, ngoại trừ cho các vị trí mới, ít nhất có một Domain Controller.

Mô hình các địa điểm hiện tại của A. Datum:



Tóm tắt thông tin:

- Hiện nay Exchange Server đặt tại London và Paris.
- Các Domain Controller đặt ở trụ sở chính London.
- London và Paris được kết nối bởi một đường truyền có tốc độ 100 Mbps.
- Cả hai thành phố Sydney và Toronto được kết nối với London bằng đường truyền có tốc độ 10-Mbps.
- Tất cả các trung tâm khu vực ở châu Âu được kết nối với Paris bằng đường truyền có tốc độ 10-Mbps.
- Tất cả các văn phòng chi nhánh và các trung tâm phân phối tại A. Datum được kết nối với văn phòng trung tâm khu vực gần nhất bởi đường truyền có tốc độ 2 Mbps.
- Tất cả các chi nhánh đều có File Server riêng.
- Hệ thống AD hiện tại của A. Datum gồm một forest duy nhất, Forest root domain được triển khai tại London với 4 Domain Controller chạy Windows Server 2012, và 5 Operation Master Roles được đặt trên cùng một Server.

III. Yêu cầu tổng quan:

Thiết kế một mô hình AD có nhiều Site hỗ trợ các mục tiêu sau đây:

- Tối ưu thời gian đăng nhập ở tất cả các địa điểm.
- Tối ưu lưu lượng email trong toàn bộ tổ chức.
- Hệ thống AD phải có khả năng sẵn sàng cao trong việc chứng thực ở tất cả các địa điểm. (Người dùng phải đăng nhập thành công dù Domain Controler hoặc đường truyền gặp sự cố).

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-RTR** **20413C-LON-SVR4**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
    - User name: **Adatum\Administrator**
    - Password: **Pa$$w0rd**
5. Thực hiên bước 2 tới 4 cho máy ảo **20413C-LON-RTR** và **20413C-LON-SVR4.**

VI. Thực hành:

Thời gian thực hành: 75 phút

Bài thực hành bao gồm các bước:

1. Cài đặt Additional Domain Controller ở Paris.
2. Chia Site
3. Cấu hình Site Links
4. Chuyển Domain Controller mới qua site Paris

Bước 1. Cài đặt Additional Domain Controller ở Paris.

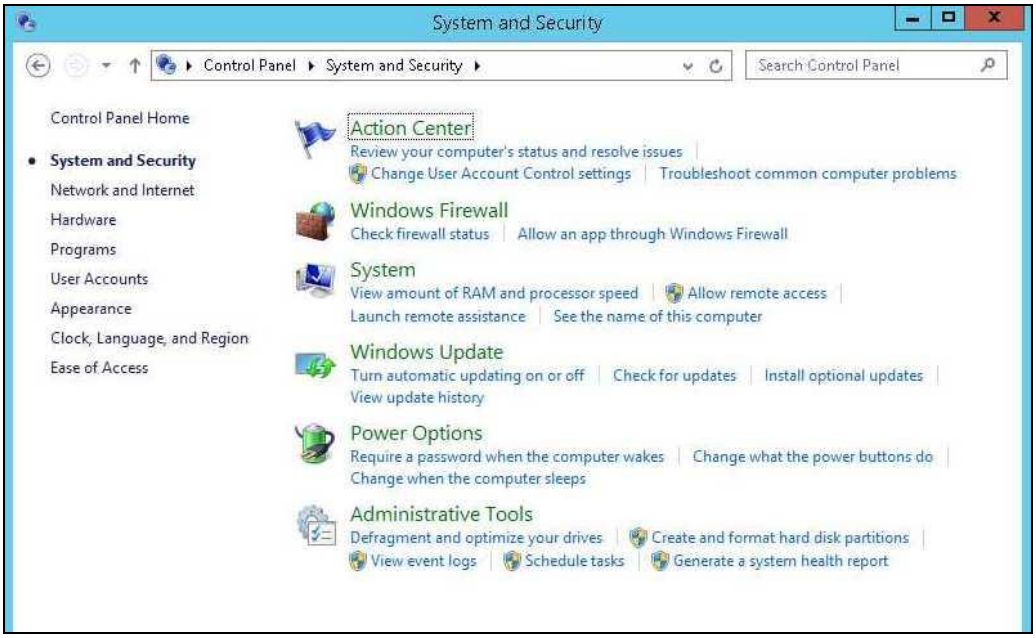
1. Logon vào máy **LON-SVR4**, nhấn chuột phải **Start** menu, mở **Control Panel**.



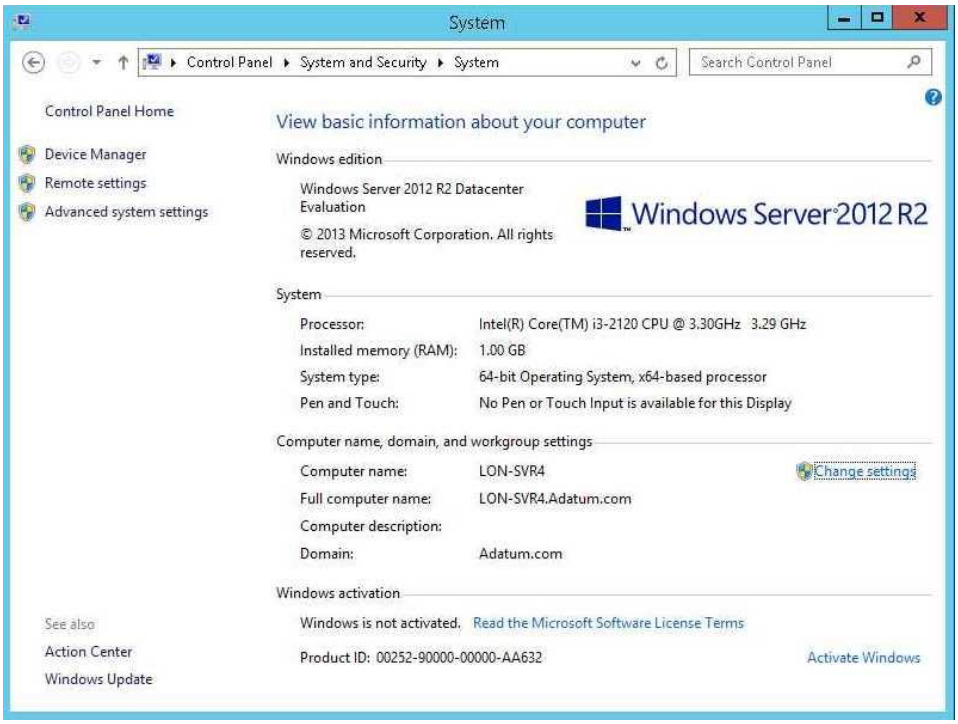
2. Trong cửa sổ **Control Panel**, chọn **System and Security**.



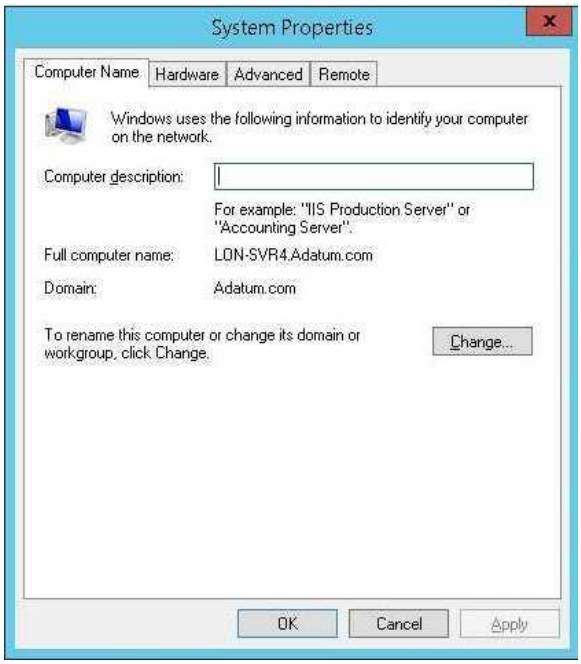
3. Cửa sổ **System and Security**, chọn **System**



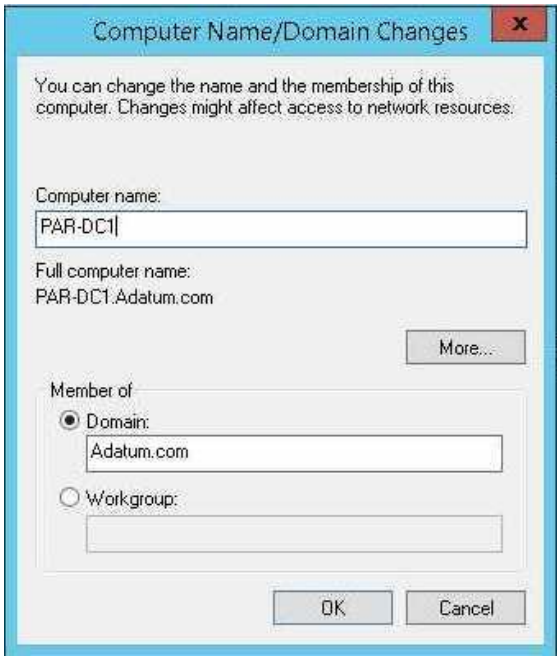
4. Cửa sổ **System**, chọn **Change settings**.



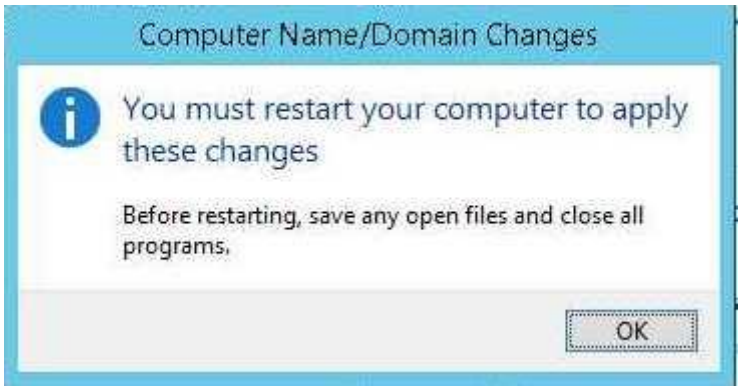
5. Trong hộp thoại **System Properties**, chọn **Change**.



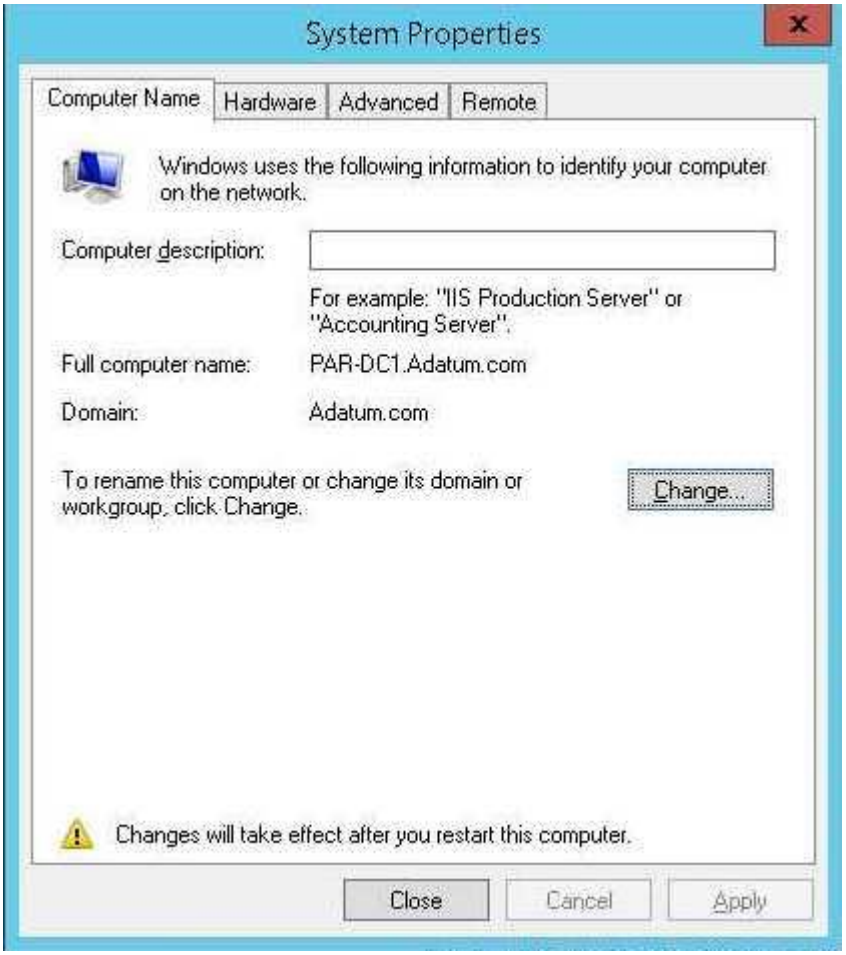
6. Hộp thoại **Computer Name/Domain Changes**, đổi **Computer name** thành **PAR-DC1**, và chọn **OK**.



7. Hộp thoại **Computer Name/Domain Changes**, chọn **OK**.



8. Hộp thoại **System Properties**, chọn **Close**.



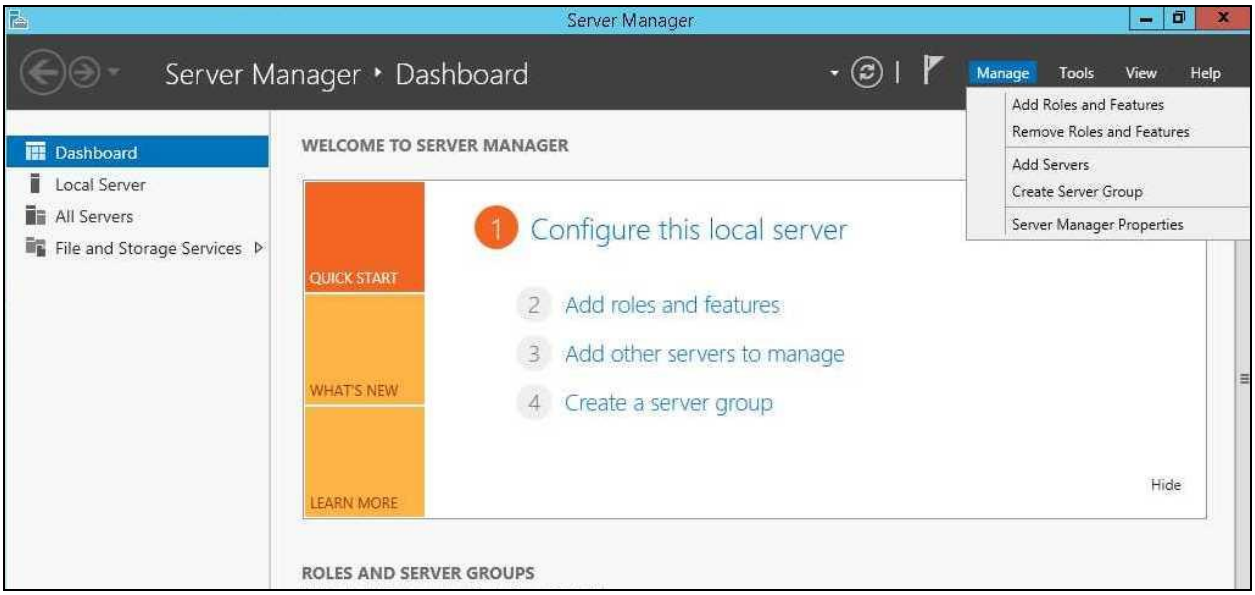
9. Chọn **Restart Now**.



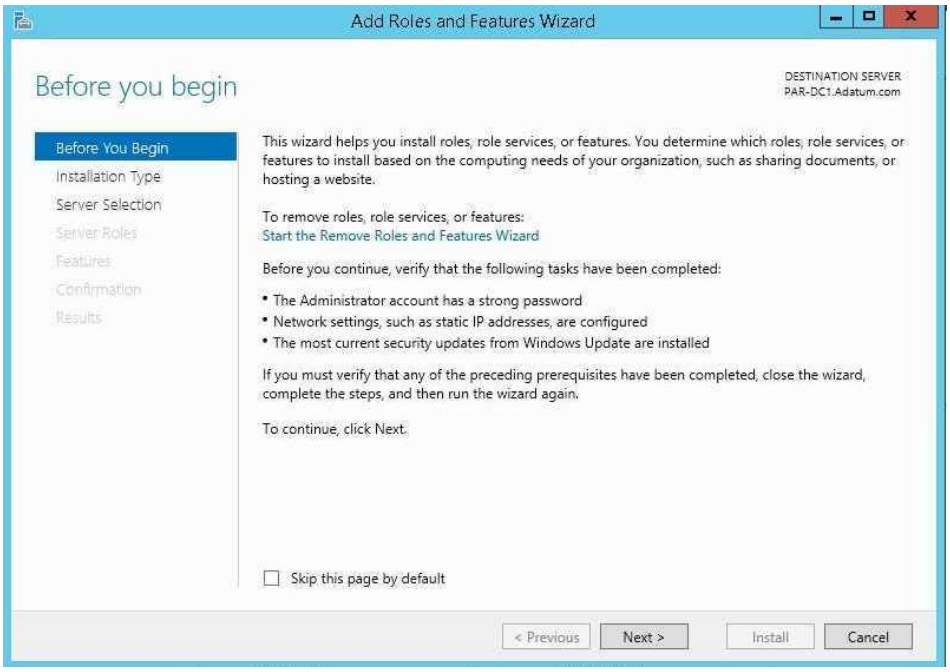
Chú ý: Trong các bước tiếp theo máy LON-SVR4 được đổi tên thành PAR-DC1.

10. Sau khi khởi động thành công, trên máy **PAR-DC1** (20413C-LON-SVR4), logon **Adatum\Administrator** với password **Pa$$w0rd**.

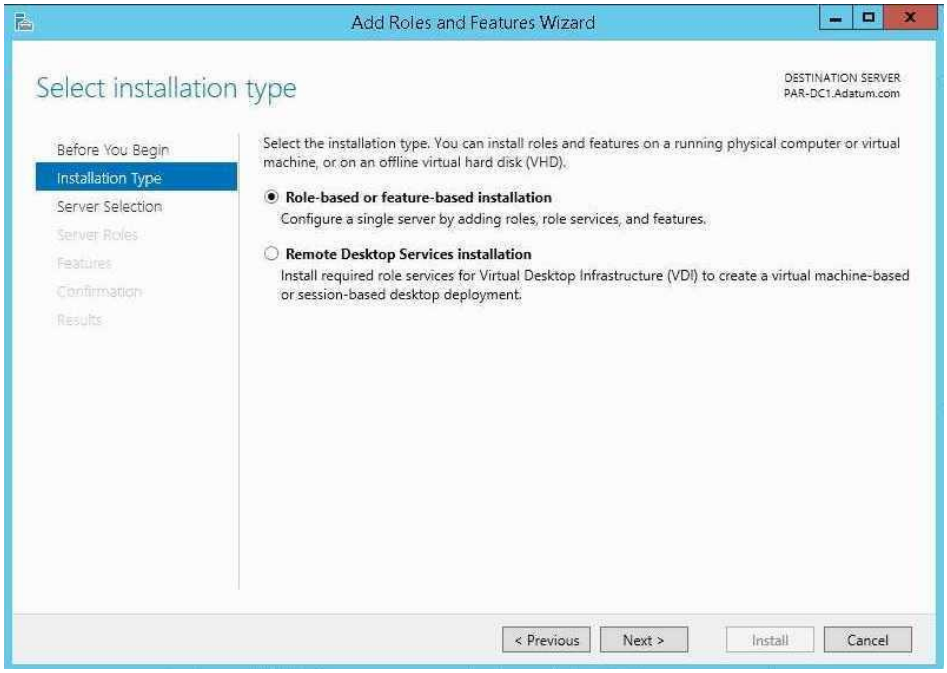
11. Mở **Server Manager**, bung menu **Manage**, chọn **Add Roles and Features**.



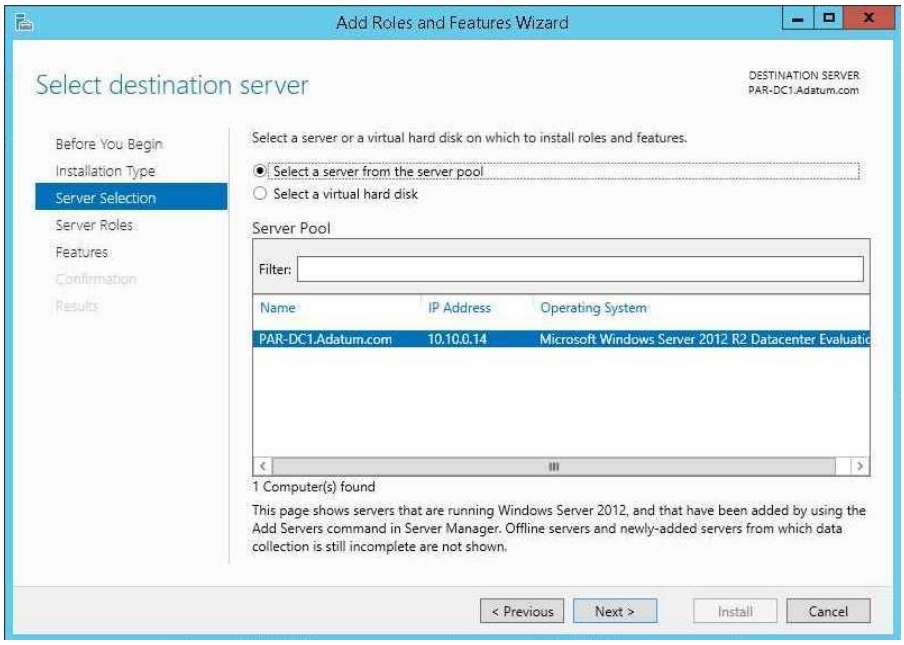
12. Cửa sổ **Before you begin**, chọn **Next**.



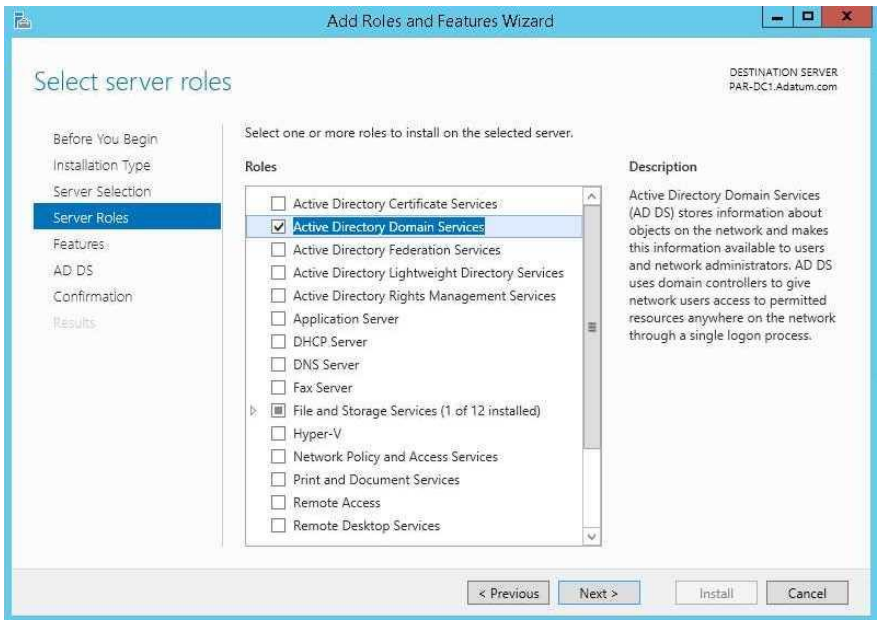
13. Cửa sổ **Select installation type**, chọn **Next**.



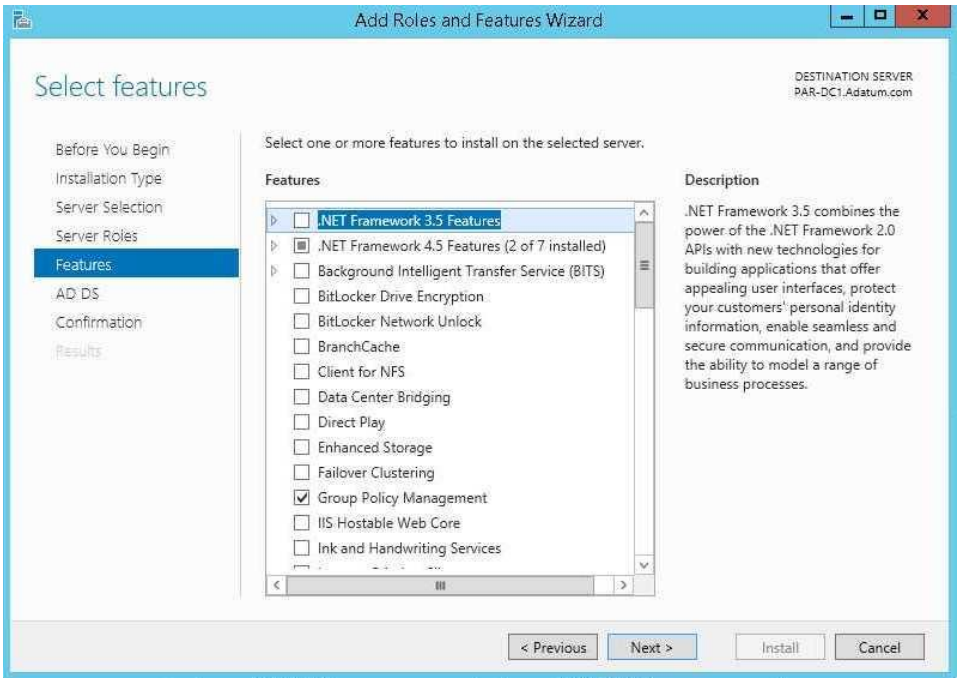
14. Cửa sổ **Select destination server**, chọn **Next**.



15. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Domain Services**, hộp thoại **Add features that are required for Active Directory Domain Services**, chọn **Add Features**, và chọn **Next**.



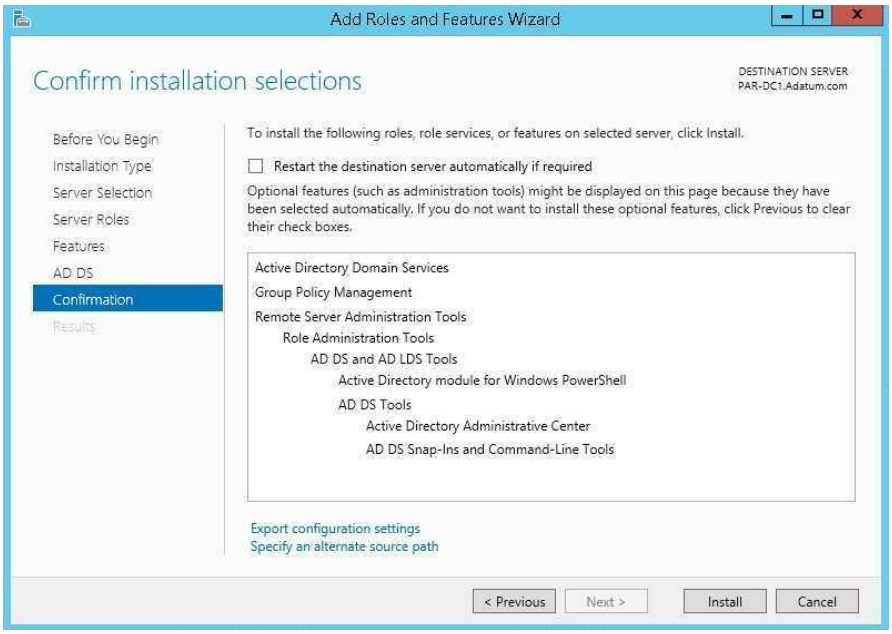
16. Cửa sổ **Select features**, chọn **Next**.



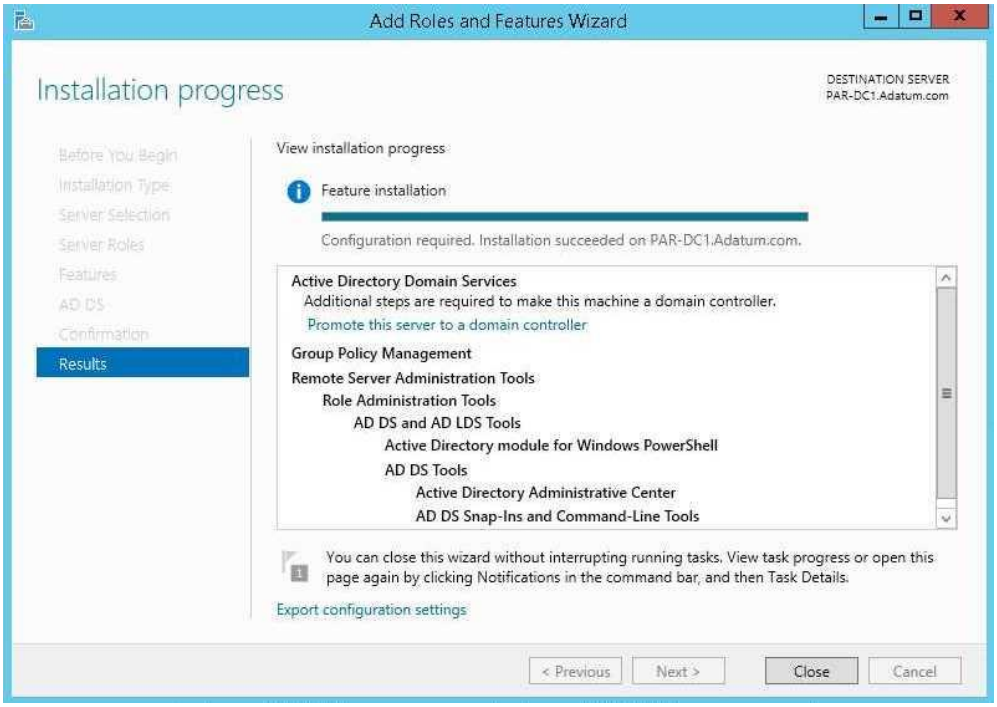
17. Cửa sổ **Active Directory Domain Services**, chọn **Next**.



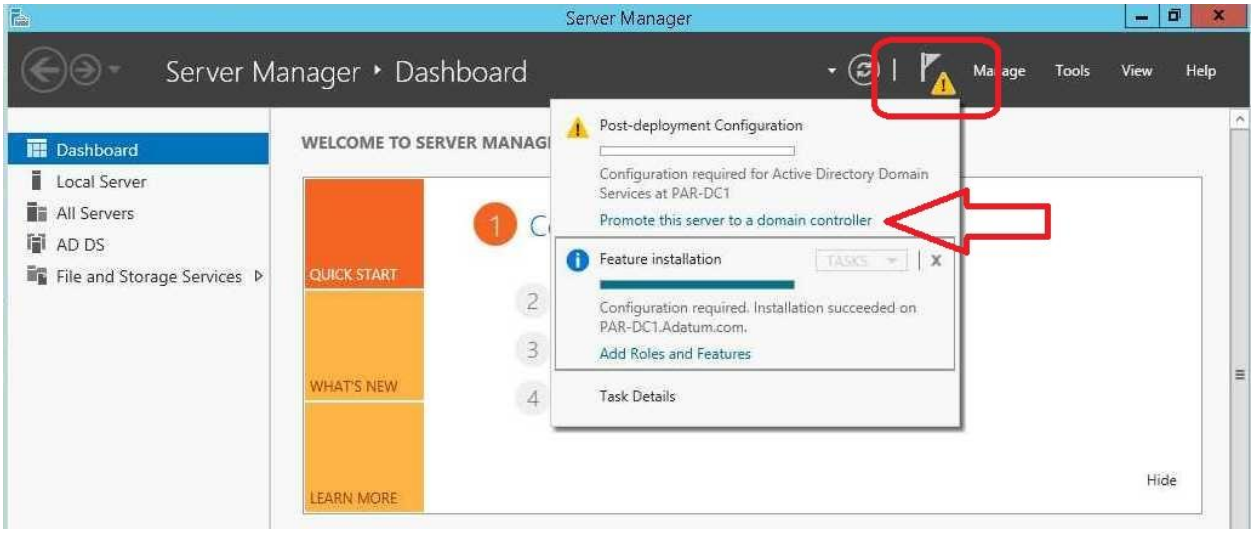
18. Cửa sổ **Confirm installation selections**, chọn **Install**.



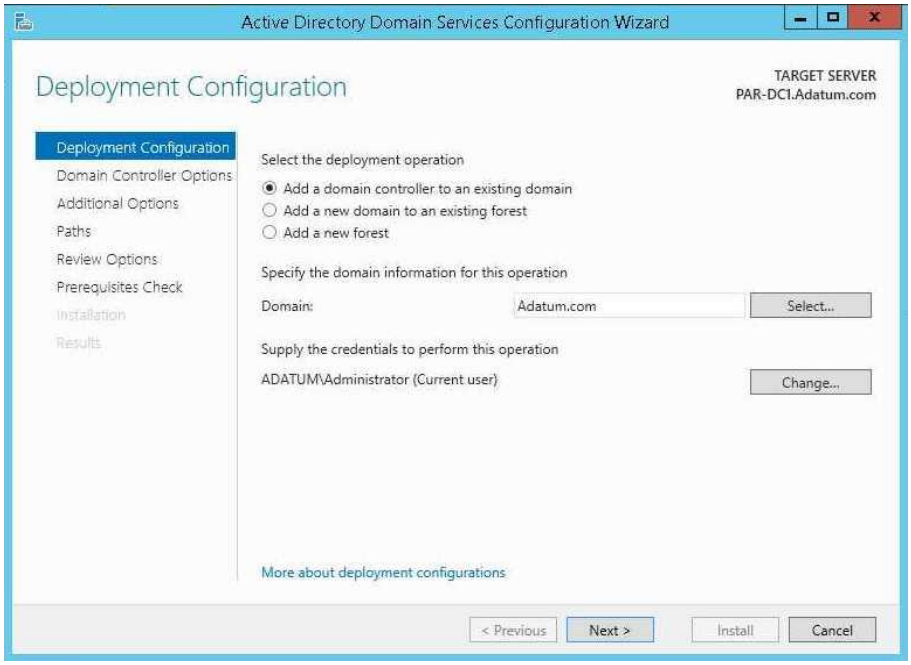
19. Sau khi cài đặt thành công, chọn **Close**.



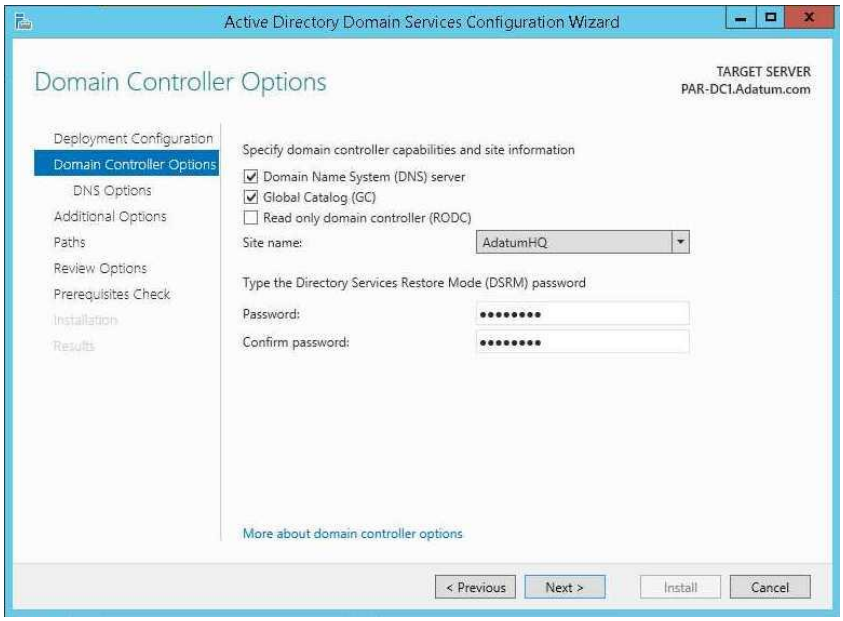
20. Trong cửa sổ **Server Manager**, bung biểu tượng thông báo màu vàng, chọn **Promote this server to a domain controller**.



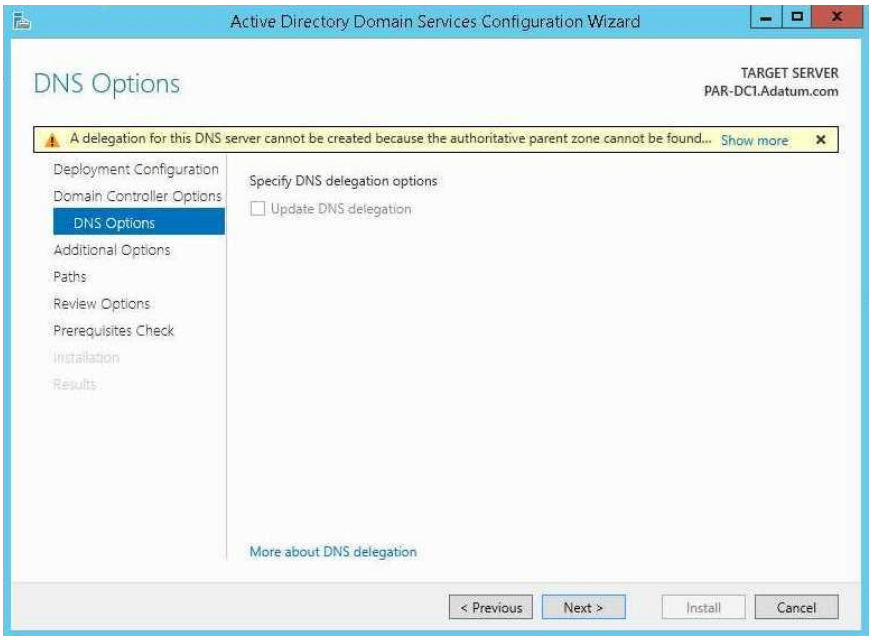
21. Cửa sổ **Deployment Configuration**, chọn **Add a domain controller to an existing domain**, và chọn **Next**.



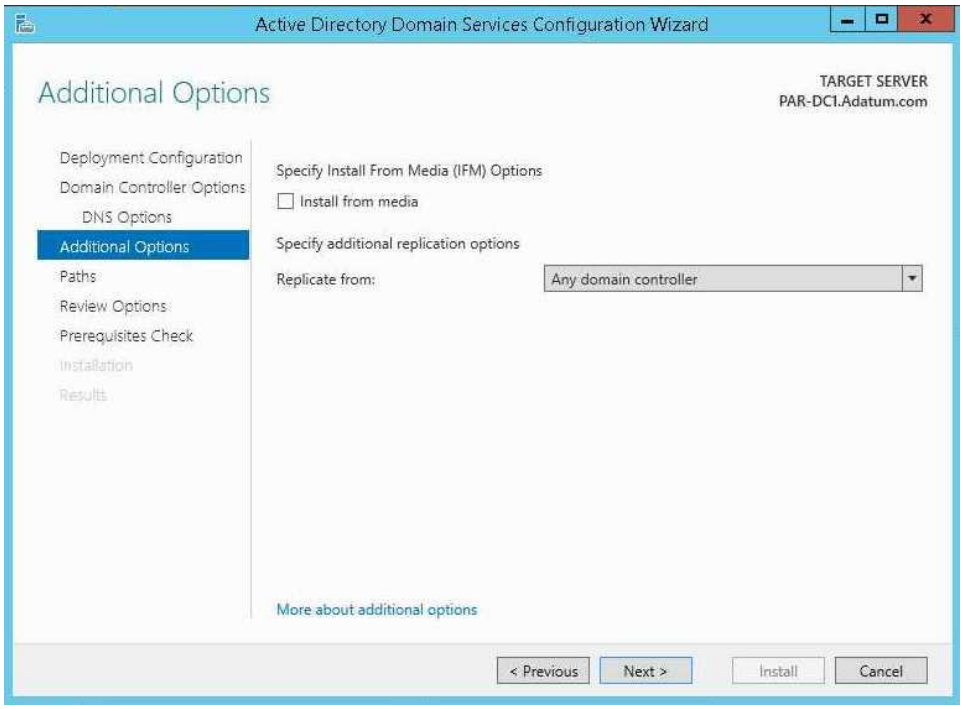
22. Cửa sổ **Domain Controller Options**, đảm bảo cáo đánh dấu chọn 2 ô **Domain Name System (DNS) server** và **Global Catalog (GC).** Trong ô **Site name** chọn **AdatumHQ.** Nhập **Pa$$w0rd** vào 2 ô **Password** và **Confirm password**, và chọn **Next**.



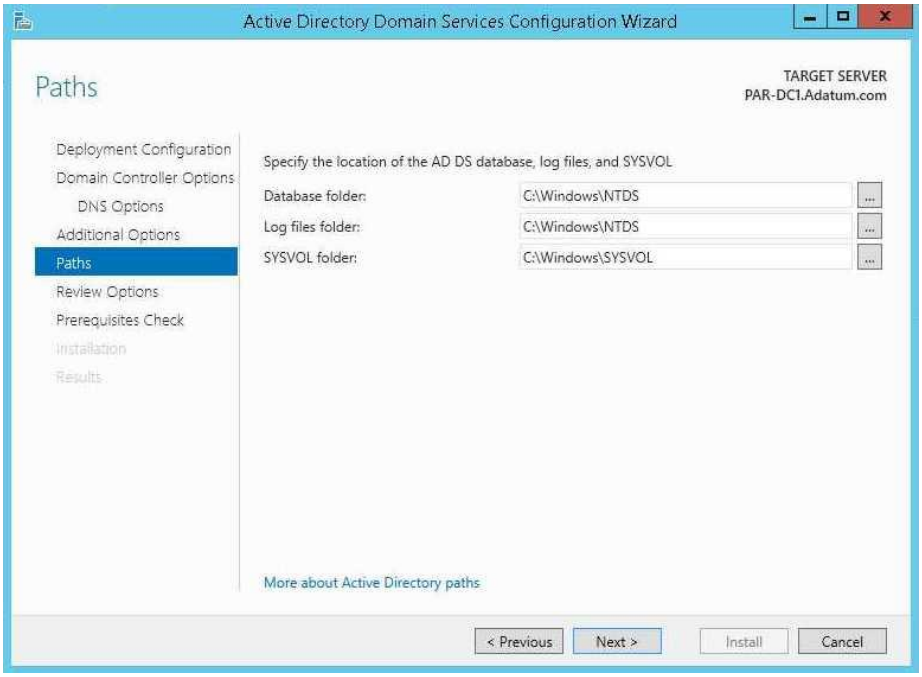
23. Cửa sổ **DNS Options**, chọn **Next**.



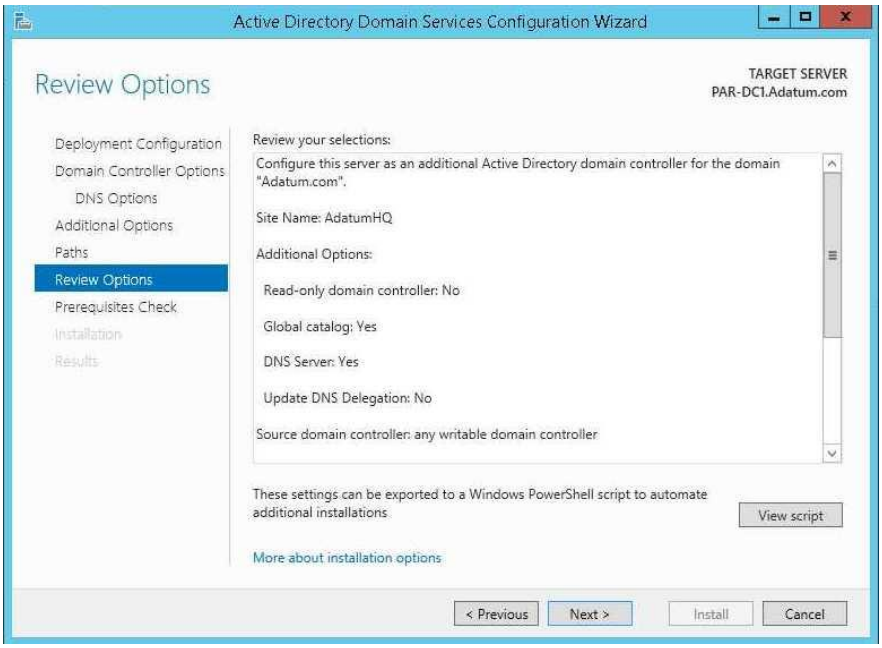
24. Cửa sổ **Additional Options**, chọn **Next**.



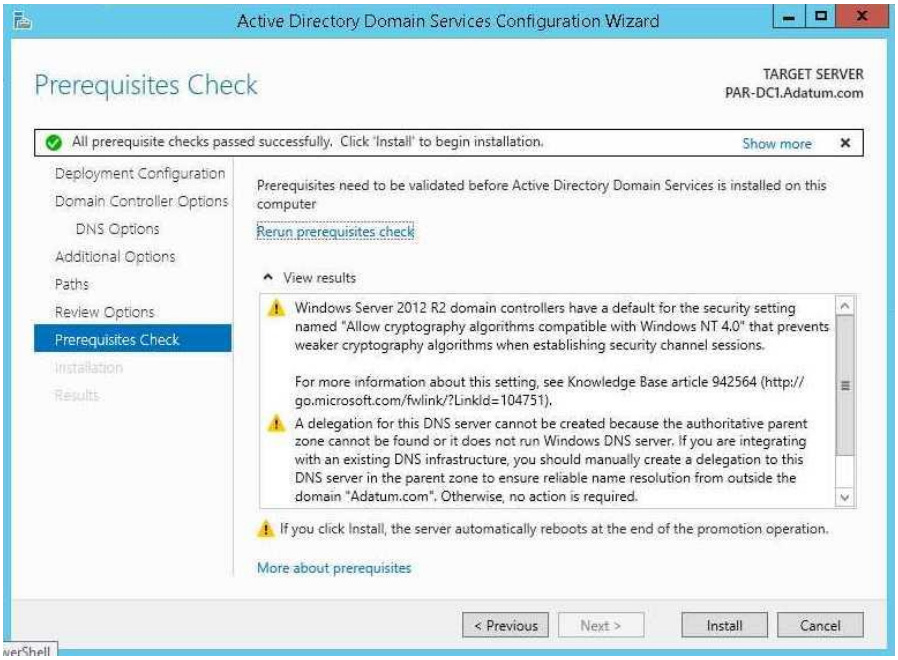
25. Cửa sổ **Paths**, chọn **Next**.



26. Cửa sổ **Review Options**, chọn **Next**.



27. Cửa sổ **Prerequisites Check**, chọn **Install**. Hệ thống sẽ tự động khởi động lại sau khi cài đặt thành công.



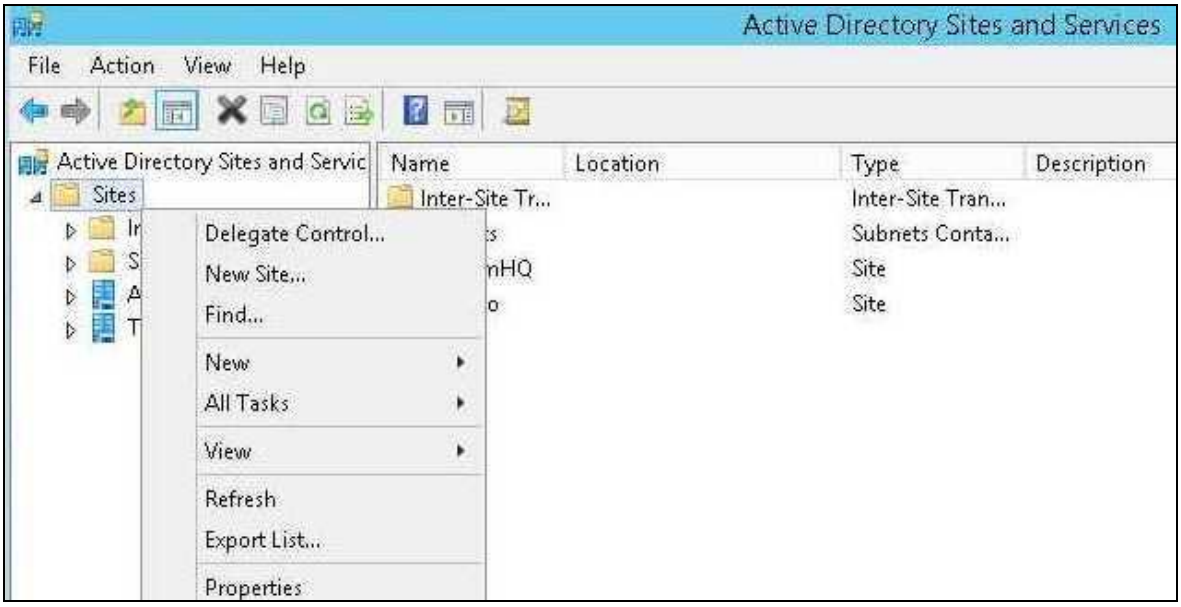
28. Sau khi khởi động thành công, logon **Adatum\Administrator** với password **Pa$$w0rd**.

Bước 2. Chia Site

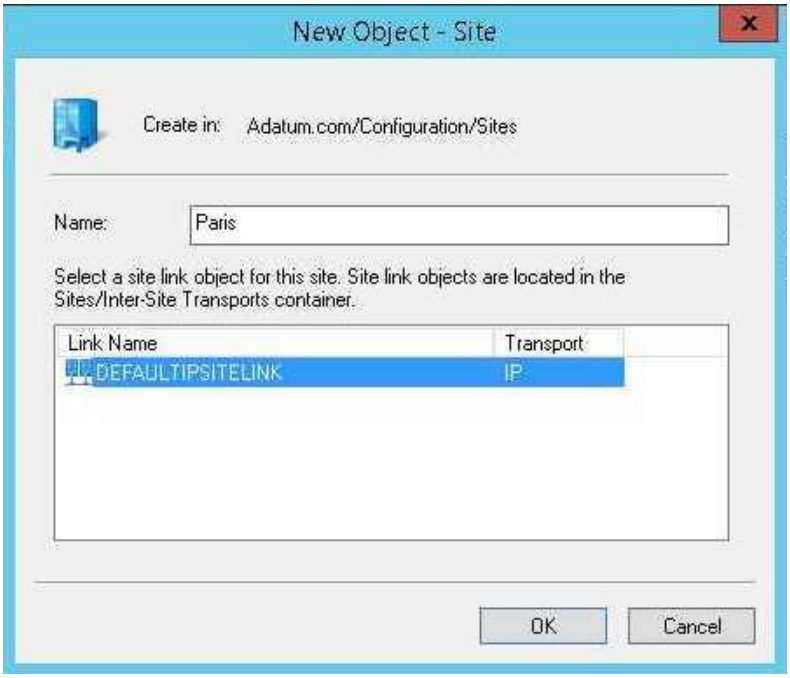
1. Trên máy **PAR-DC1**, mở **Server Manager**, bung menu **Tools**, mở **Active Directory Sites and Services**.



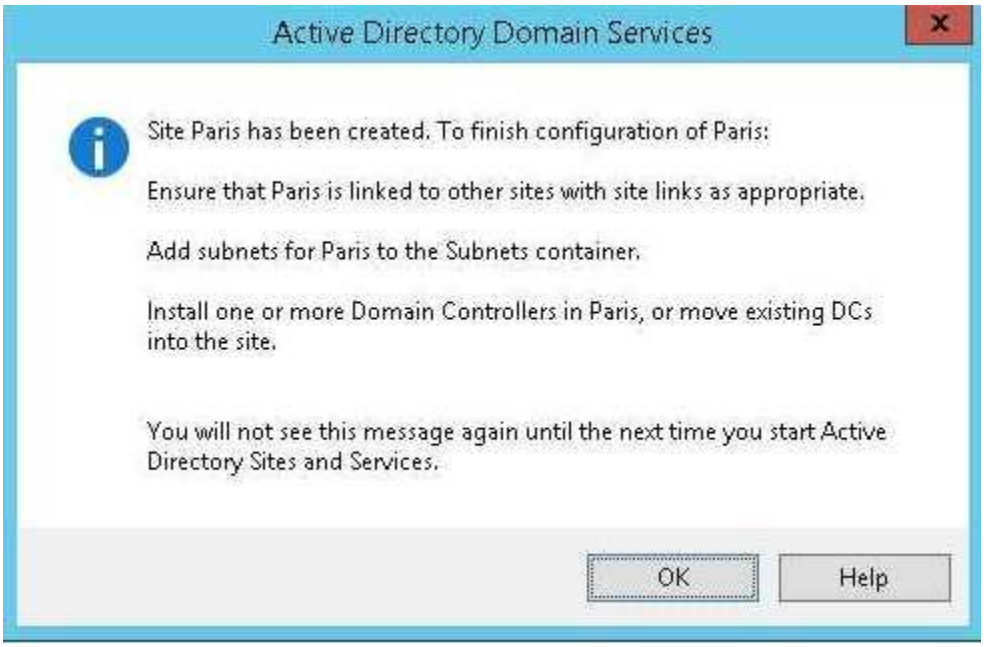
2. Trong cửa sổ **Active Directory Sites and Services**, nhấn chuột phải **Sites**, chọn **New Site**.



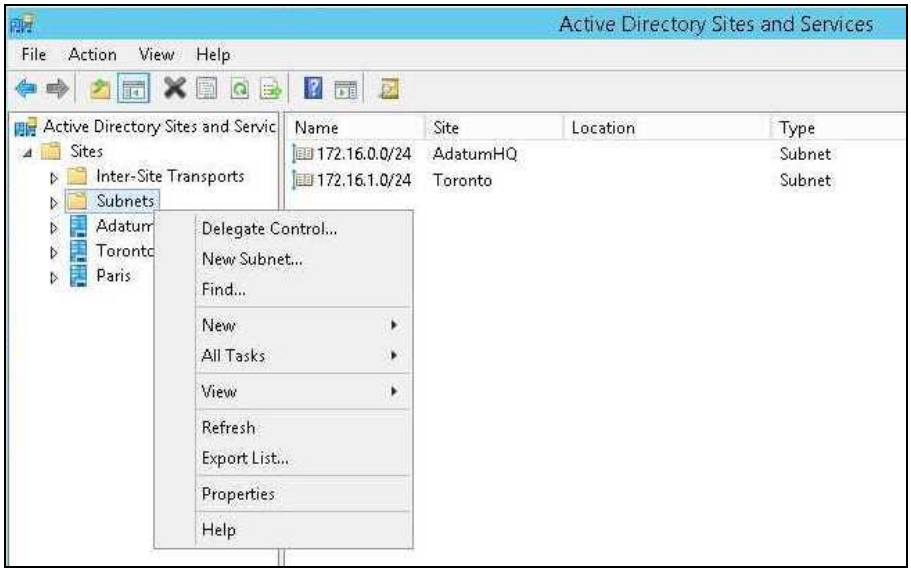
3. Hộp thoại **New Object – Site**, nhập **Paris** vào ô **Name**. Trong phần **Select a site link object for this site**, chọn **DEFAULTIPSITELINK**, và chọn **OK**.



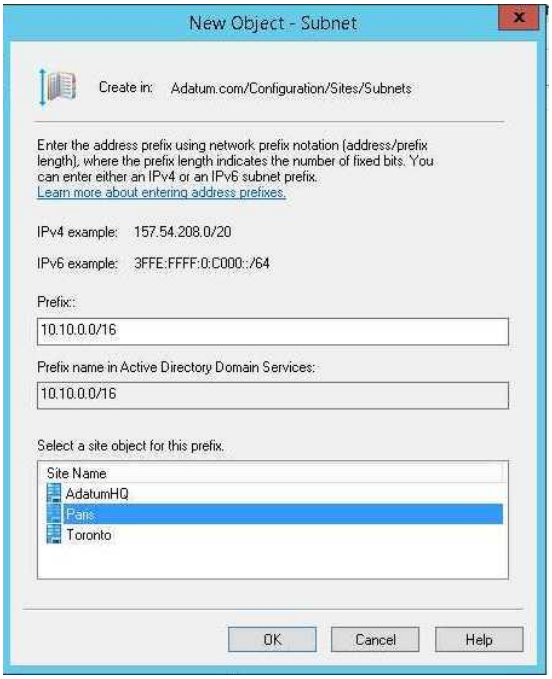
4. Hộp thoại **Active Directory Domain Services**, chọn **OK**.



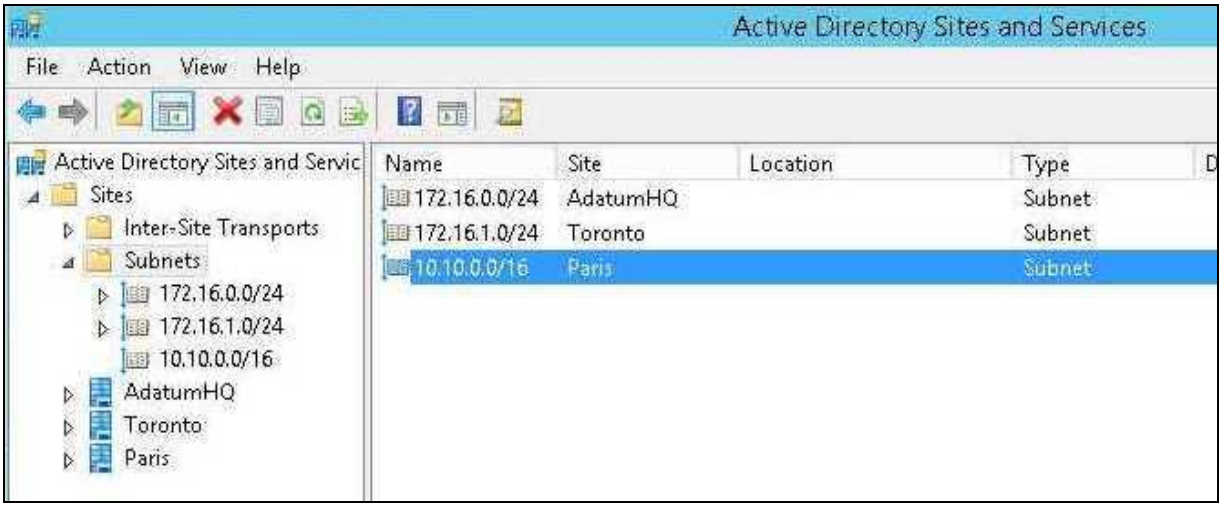
5. Trong cửa sổ **Active Directory Sites and Services**, bung **Sites**, nhấn chuột phải **Subnets**, chọn **New Subnet**.



6. Hộp thoại **New Object – Subnet**, nhập **10.10.0.0/16** vào ô **Prefix**. Trong ô **Select a site object for this prefix**, chọn **Paris**, và chọn **OK**.

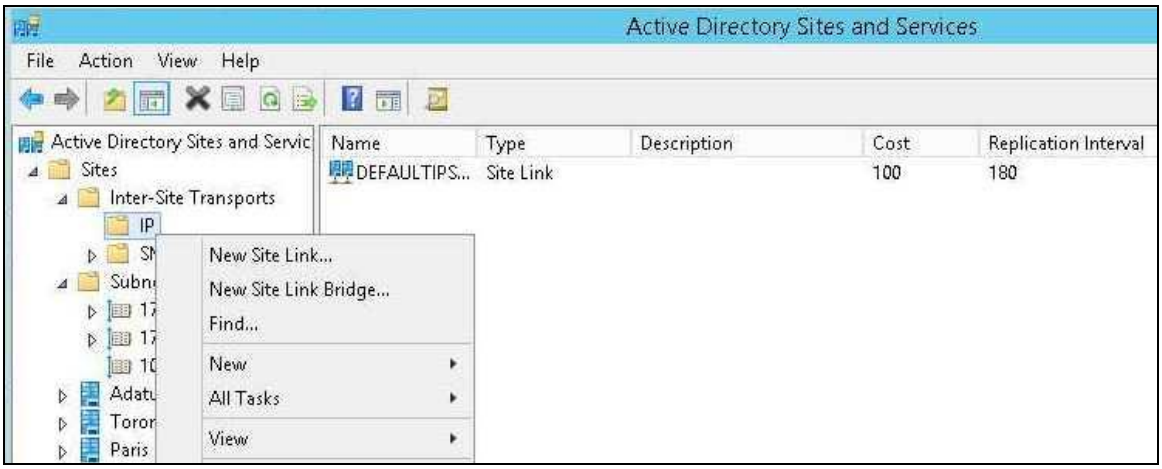


7. Trong cửa sổ **Active Directory Sites and Services**, bung **Sites**, chọn **Subnets**, kiểm tra subnet hiển thị đúng với site Paris.

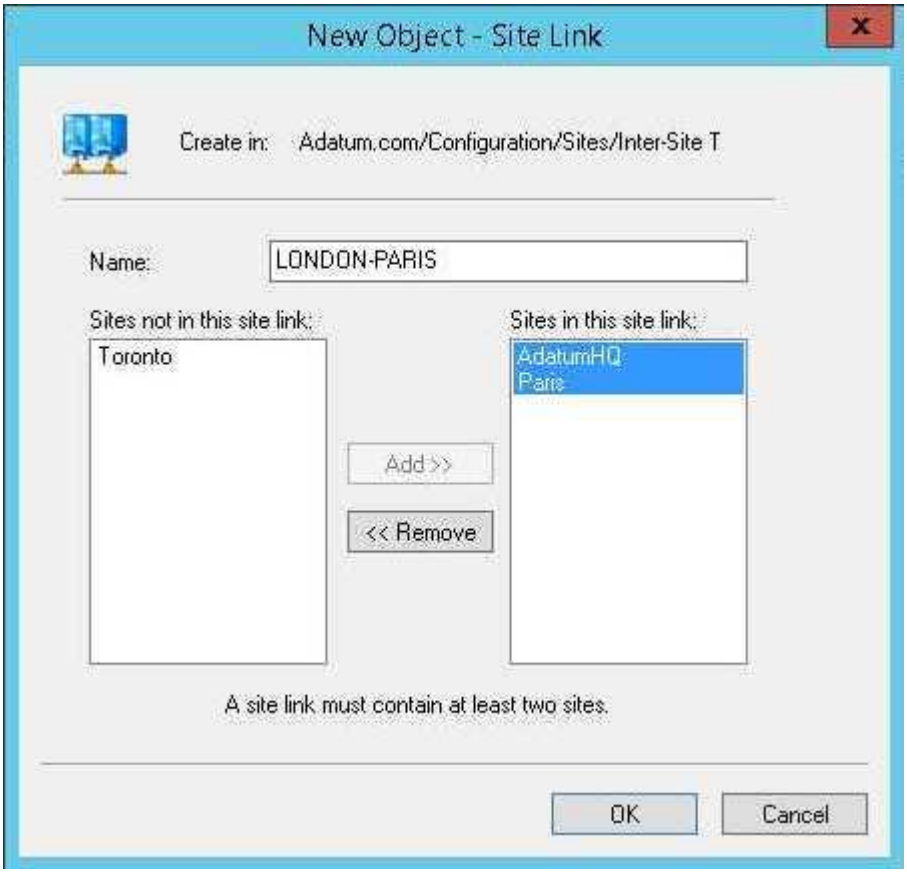


Bước 3. Cấu hình Site Links

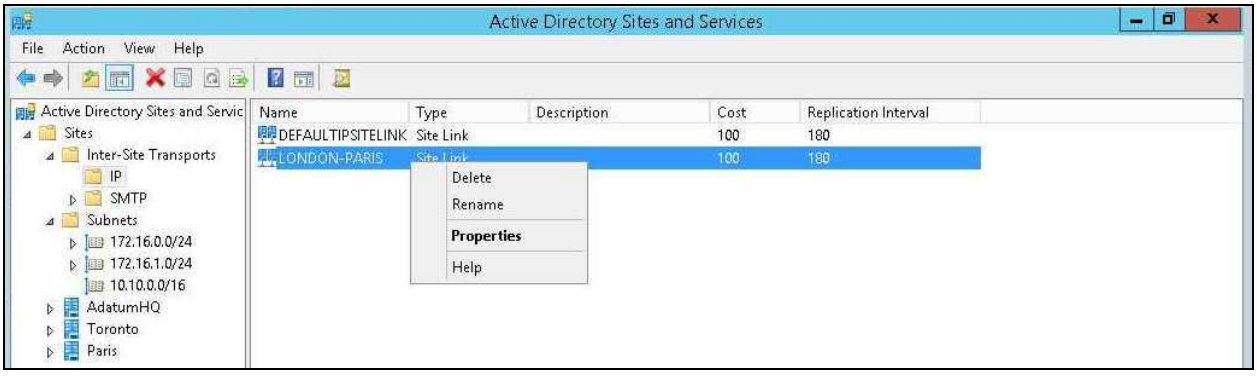
1. Trên máy **PAR-DC1**, trong cửa sổ **Active Directory Sites and Services**, bung **Sites**, bung **Inter-Site Transports**, nhấn chuột phải lên mục **IP**, chọn **New Site Link**.



2. Trong ô **Name**, đặt tên **LONDON-PARIS**. Trong ô **Sites not in this site link**, nhấn giữ phím **Ctrl,** chọn **AdatumHQ** và **PARIS**, chọn **Add**, và chọn **OK**.

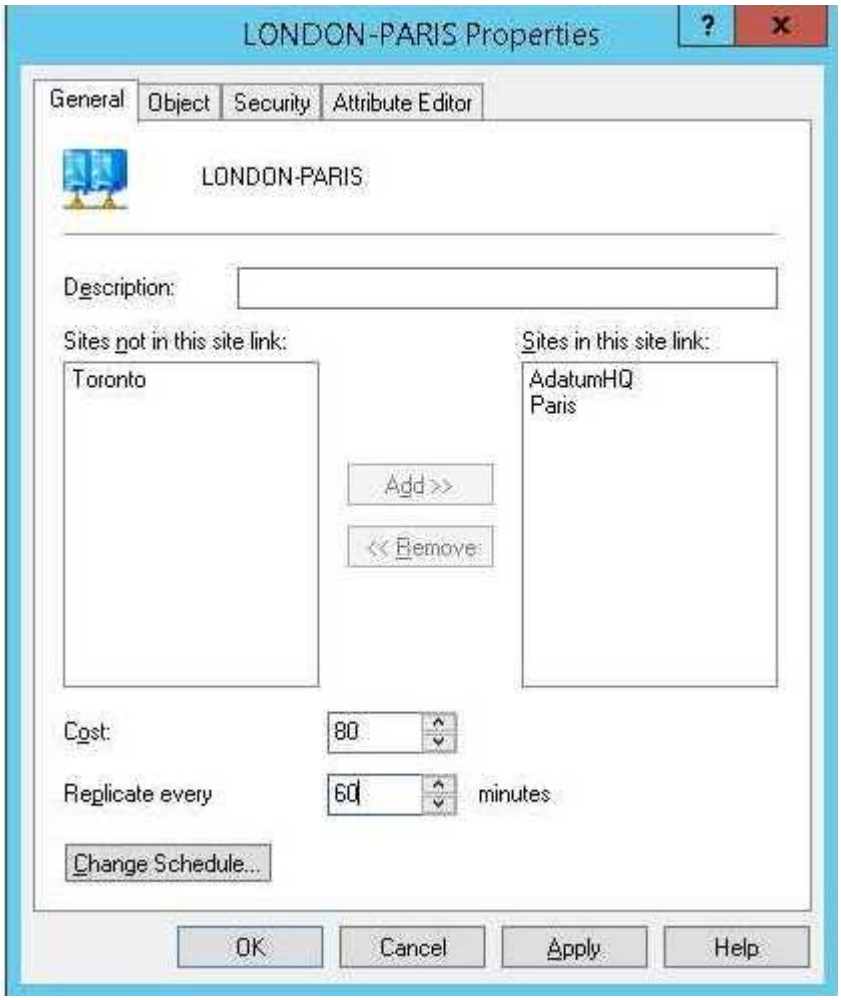


3. Nhấn chuột phải **LONDON-PARIS**, chọn **Properties**.



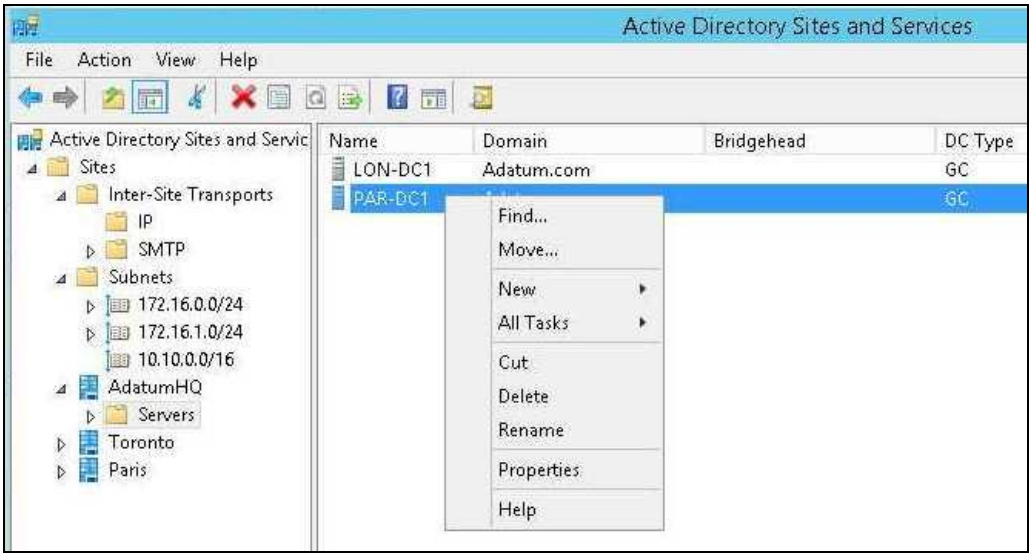
4. Hộp thoại **LONDON-PARIS Properties**, nhập thông tin như bên dưới, và chọn **OK**:

- Cost: **80**
- Replicate Every: **60 minutes**.

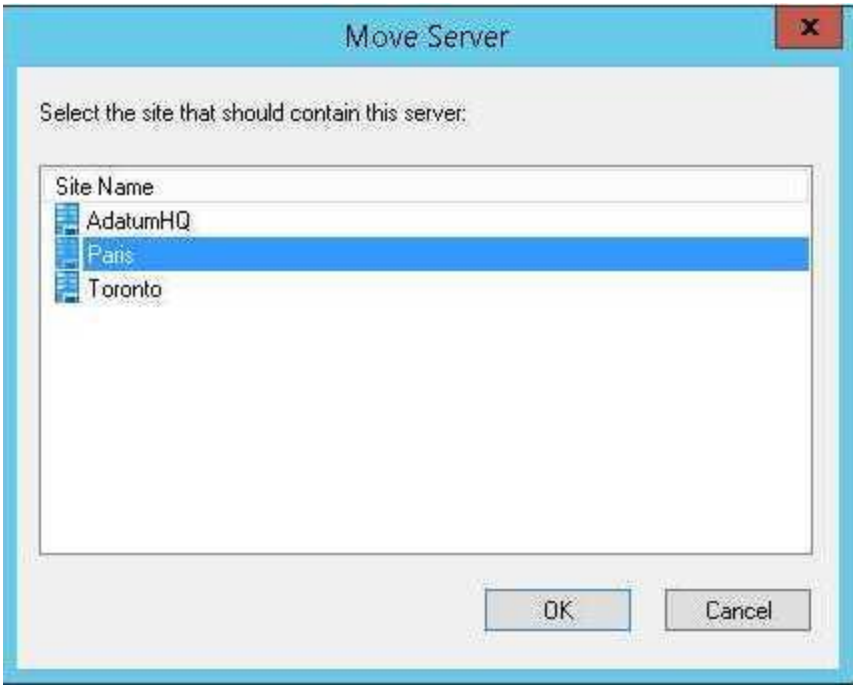


Bước 4. Chuyển Domain Controller mới qua site Paris

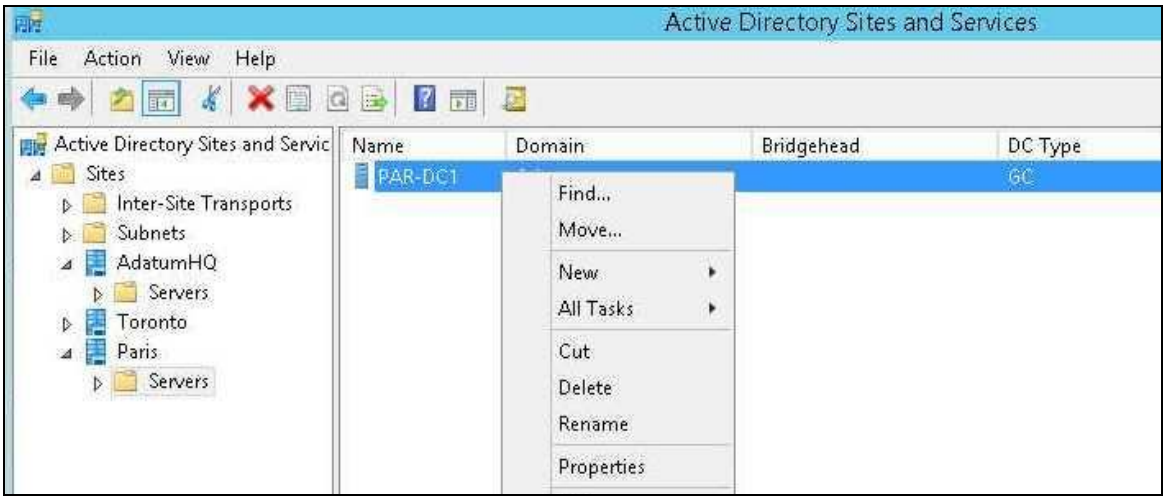
1. Trên máy **PAR-DC1**, trong cửa sổ **Active Directory Sites and Services**, bung **Sites**, bung **AdatumHQ**, bung **Servers**, nhấn chuột phải **PAR-DC1**, chọn **Move**.



2. Hộp thoại **Move Server**, chọn **Paris**, và chọn **OK**.



3. Bung **Paris**, bung **Servers**, nhấn chuột phải **PAR-DC1**, chọn **Properties**.



4. Hộp thoại **PAR-DC1 Properties**, trong ô **Transports available for inter-site data transfer**, chọn **IP**, chọn **Add**, và chọn **OK**.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công mô hình AD có nhiều site, cài đặt Domain Controller cho mỗi site và cấu hình cơ chế đồng bộ dữ liệu AD giữa các site.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20413C-LON-RTR** và **20413C-LON-SVR4.**

Bài 10: Lập kế hoạch và triển khai giải pháp lưu trữ dữ liệu

I. Mục tiêu:

- Lập kế hoạch cho giải pháp lưu trữ.
- Triển khai giải pháp lưu trữ iSCSI SAN.
- Cấu hình khả năng chịu lỗi cho hệ thống lưu trữ.

II. Kịch bản:

Trước đây, công ty A. Datum sử dụng công nghệ lưu trữ gắn trực tiếp DAS (Direct-Attached Storage). Khi chuyển đổi hệ thống sang Windows Server 2012 R2, chúng ta phải xem xét lựa chọn giải pháp để thay thế cho công nghệ lưu trữ này. Công nghệ lưu trữ mới phải giúp cải thiện hiệu suất của các ứng dụng, và cải thiện cơ chế quản lý lưu trữ.

Trong hệ thống của A. Datum có một số ứng dụng rất quan trọng, vì vậy công nghệ lưu trữ mới phải cung cấp cơ chế chịu lỗi phù hợp để các ứng dụng này có khả năng sẵn sàng cao. Các ứng dụng này hoạt động dựa trên SQL Server.

SQL Server là nền tảng của ứng dụng quản lý bán hàng và quản lý khách hàng. Các nhân viên bán hàng của A. Datum hiện đang được đào tạo về cách sử dụng ứng dụng này.

Các nền tảng hỗ trợ ứng dụng này đã được ảo hóa và có khả năng sẵn sàng cao. Điều quan trọng là giải pháp lưu trữ dữ liệu cho ứng dụng này phải có khả năng chịu lỗi.

III. Yêu cầu tổng quan:

Lập kế hoạch cho một chiến lược lưu trữ hỗ trợ các mục tiêu sau đây:

- Giải pháp lưu trữ phải có khả năng sẵn sàng cao.
- Tối ưu hiệu suất hoạt động để nhiều người dùng được kết nối vào các ứng dụng.
- Chi phí cho các giải pháp lưu trữ không được quá tốn kém.

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.

2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Start**.

3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.

4. Logon vào máy **20413C-LON-DC1** với thông tin sau:

   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**

5. Thực hiên từ bước 2 đến 4 cho máy ảo **20413C-LON-SVR1.**

VI. Thực hành:

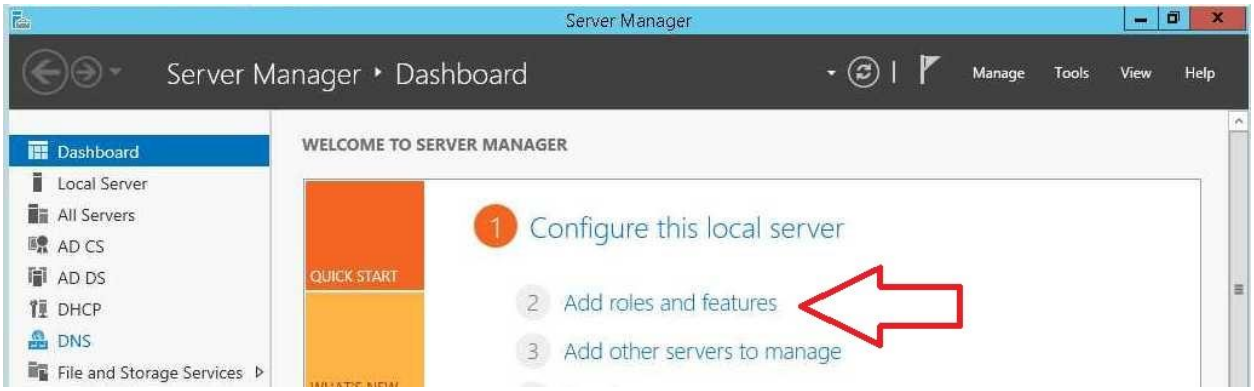
Thời gian thực hành: 50 phút

Bài thực hành bao gồm các bước:

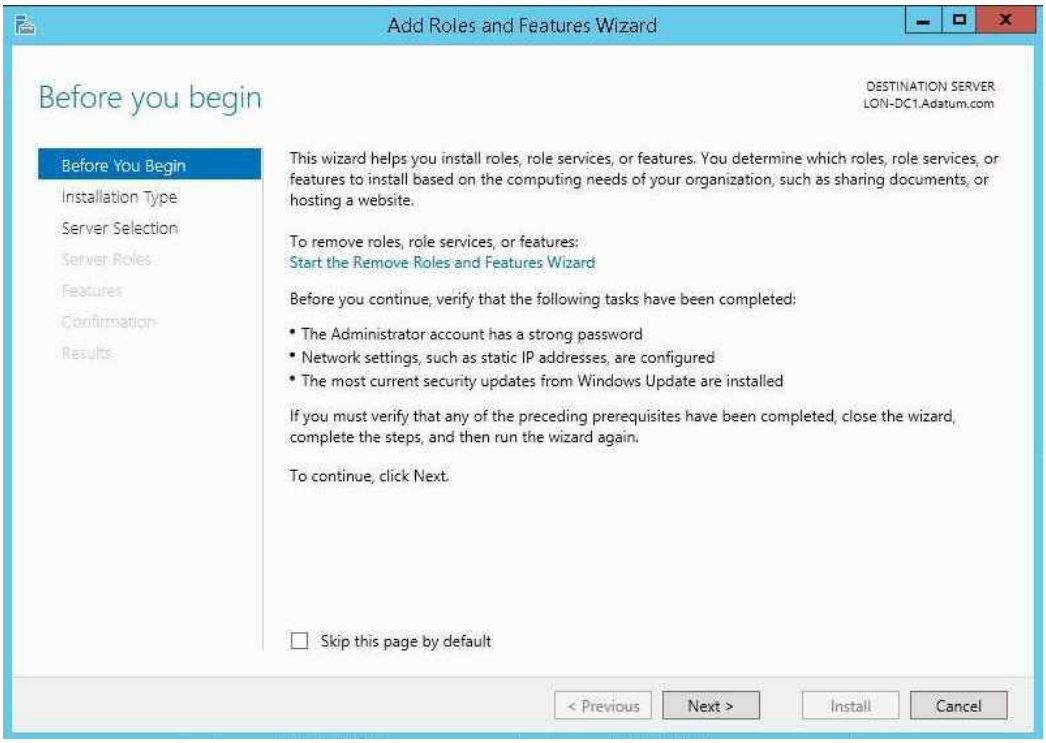
1. Cài đặt iSCSI target.
2. Cấu hình iSCSI targets.
3. Kết nối tới iSCSI targets.
4. Tạo Storage pool sử dụng iSCSI Disk.
5. Tạo Mirrored Disk.
6. Chép dữ liệu vào Mirror Disk.
7. Ngắt kết nối một đĩa iSCSI và kiểm tra vẫn truy cập ứng dụng thành công.

Bước 1. Cài đặt iSCSI target.

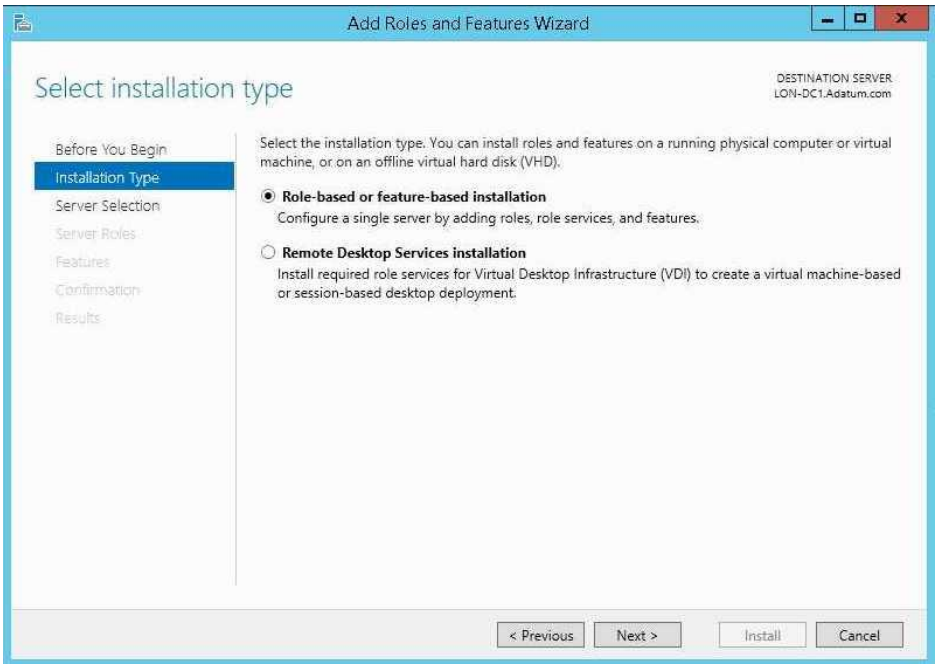
1. Trên máy **LON-DC1**, mở **Server Manager**, chọn **Add roles and features**.



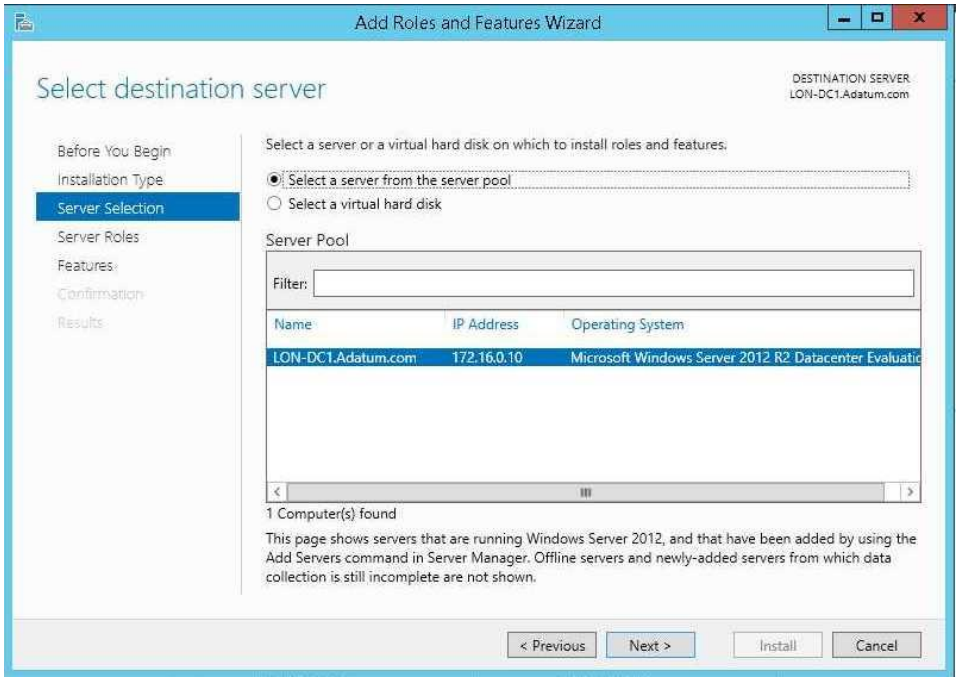
2. Cửa sổ **Before you begin**, chọn **Next**.



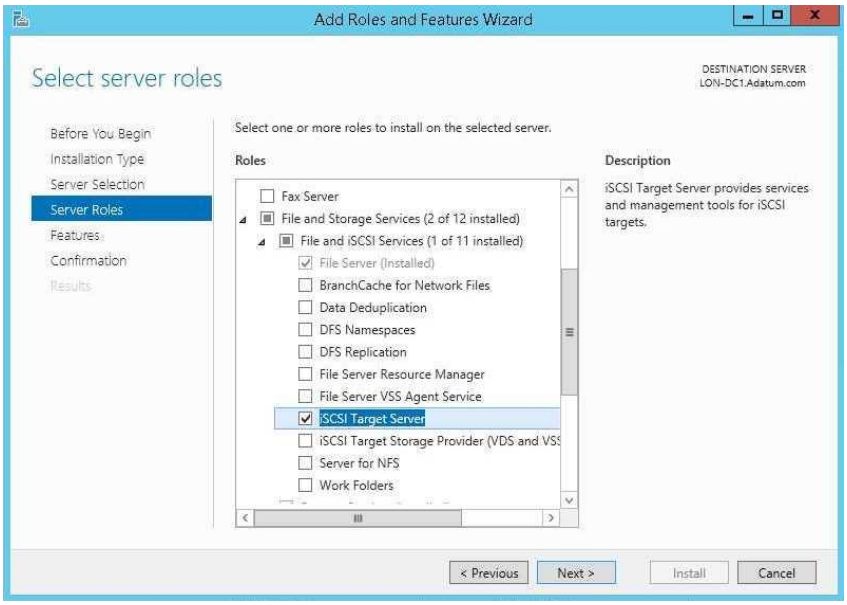
3. Cửa sổ **Select installation type**, chọn **Next**.



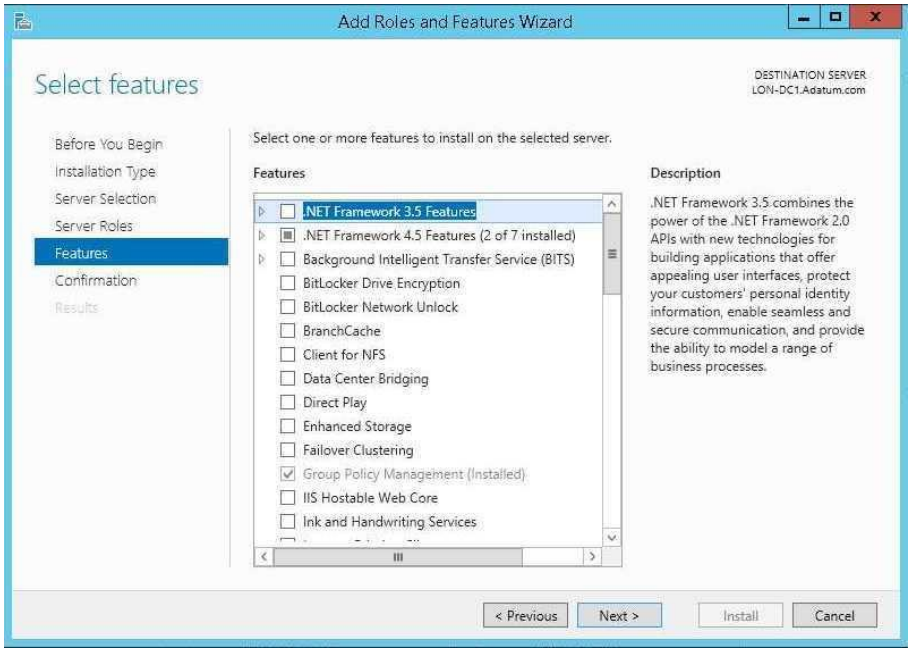
4. Cửa sổ **Select destination server**, chọn **Next**.



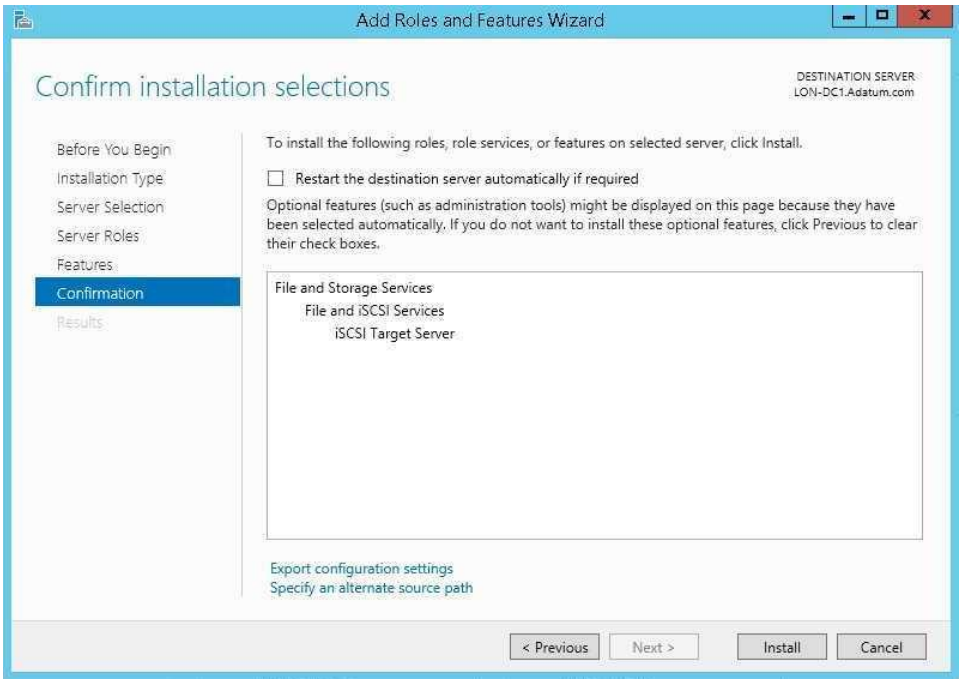
5. Cửa sổ **Select server roles**, bung **File And Storage Services (2 of 12 Installed)**, bung **File and iSCSI Services (1 of 11 installed)**, đánh dấu chọn **iSCSI Target Server**, và chọn **Next**.



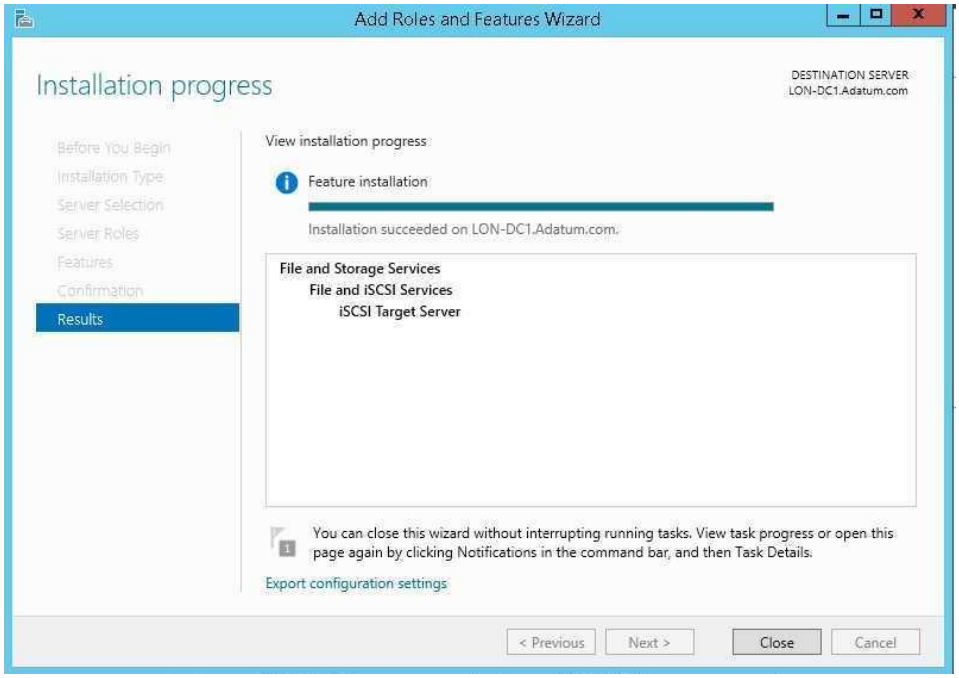
6. Cửa sổ **Select features**, chọn **Next**.



7. Cửa sổ **Confirm installation selections**, chọn **Install**.



8. Sau khi cài đặt thành công, chọn **Close**.

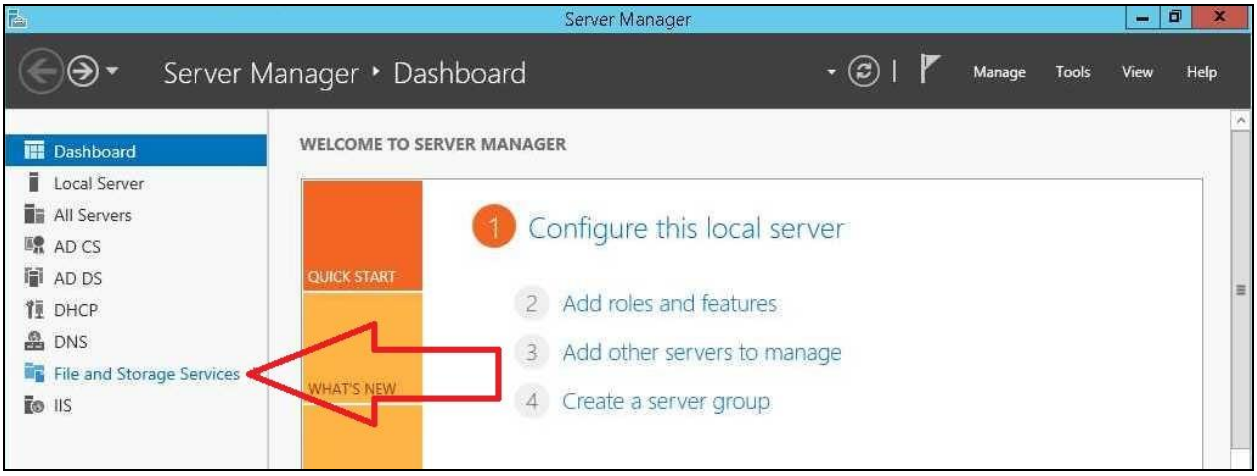


9. Nếu có yêu cầu khởi động lại hệ thống thì chọn **Restart Now**.

10. Sau khi khởi động thành công, logon **LON-DC1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

Bước 2. Cấu hình iSCSI targets.

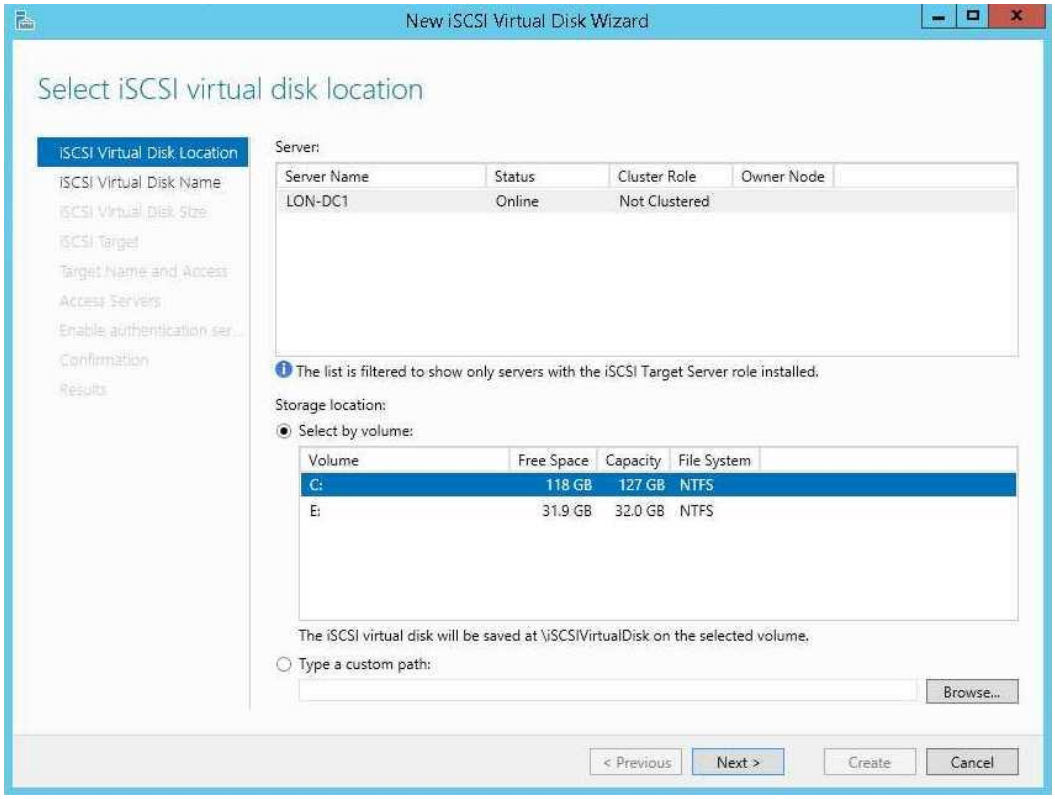
1. Trên máy **LON-DC1**, mở **Server Manager**, chọn **File and Storage Services**.



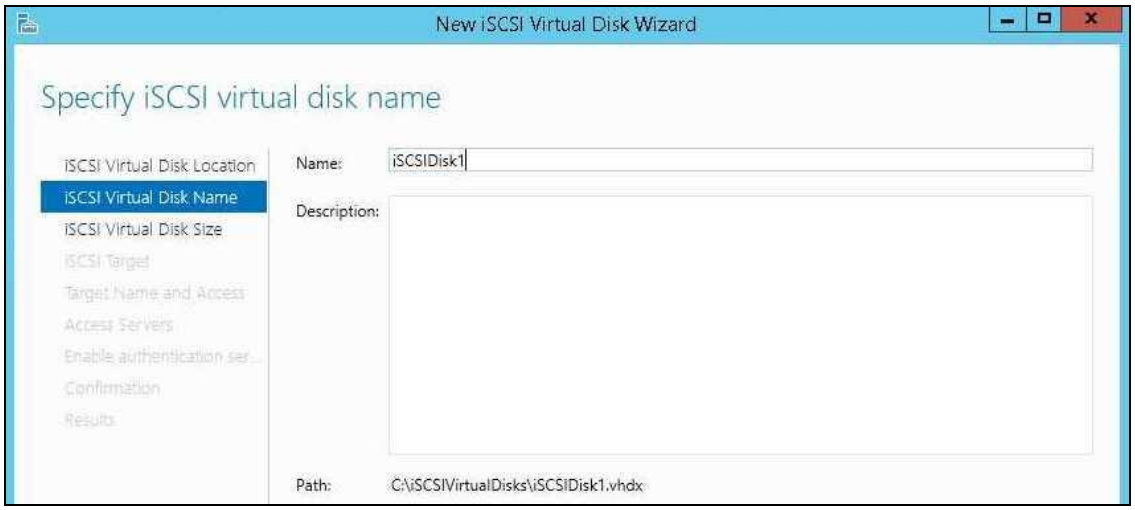
2. Trong cửa sổ **File and Storage Services**, chọn **iSCSI**, bung **TASKS**, chọn **New iSCSI Virtual Disk**.



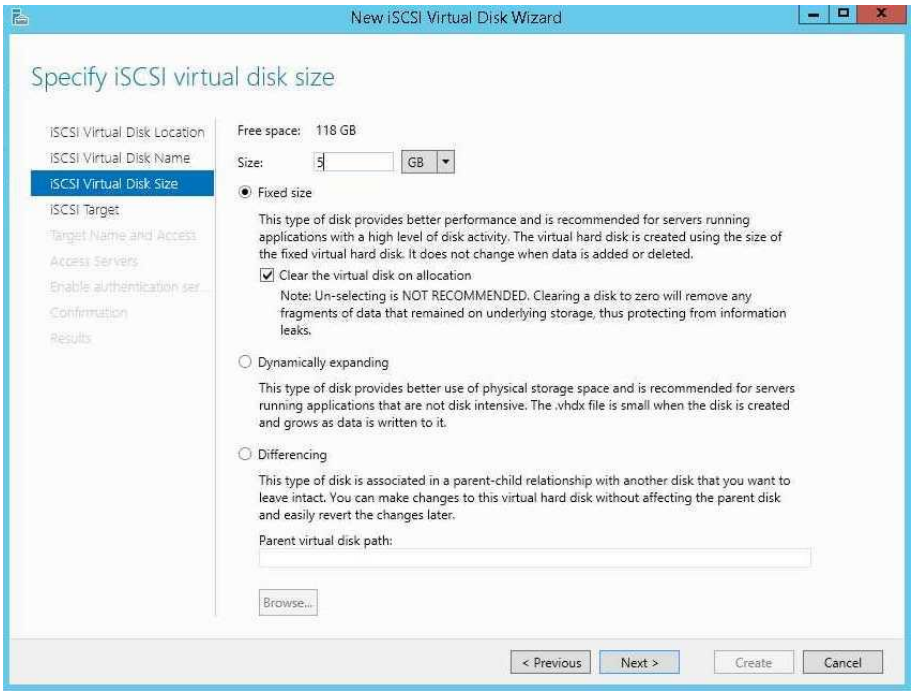
3. Cửa sổ **Select iSCSI virtual disk location**, trong ô **Storage location**, chọn **C:**, và chọn **Next**.



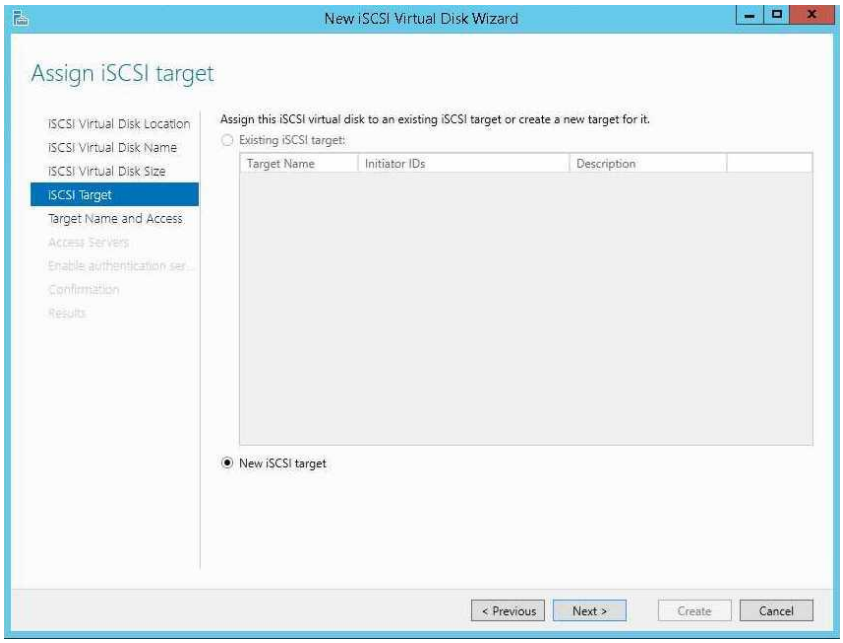
4. Cửa sổ **Specify iSCSI virtual disk name**, nhập **iSCSIDisk1** vào ô **Name**, chọn **Next**.



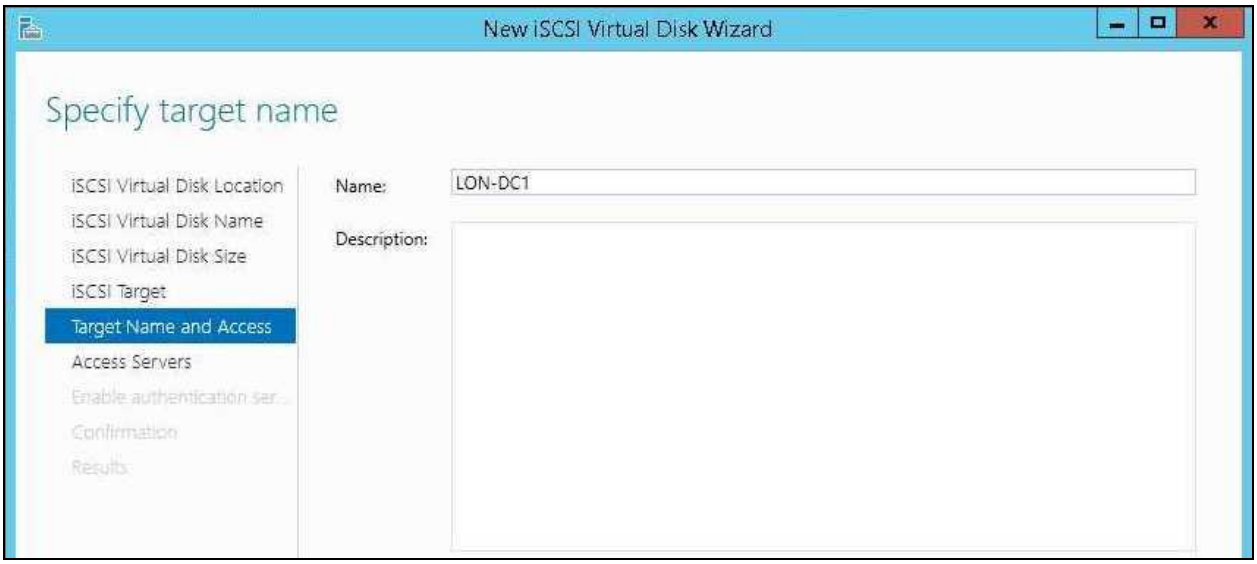
5. Cửa sổ **Specify iSCSI virtual disk size**, trong ô **Size**, nhập số **5**, chọn **GB**, và chọn **Next**.



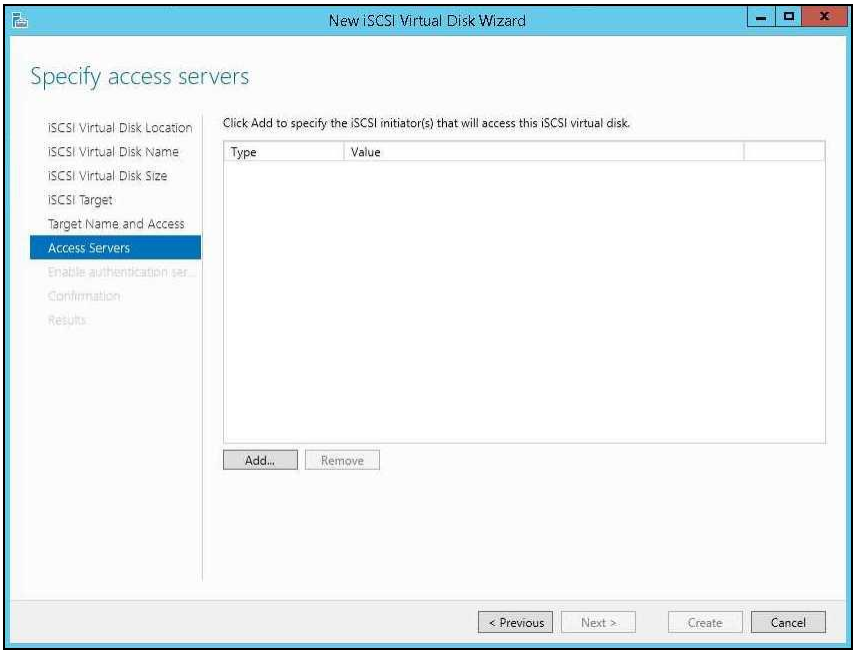
6. Cửa sổ **Assign iSCSI target**, chọn **New iSCSI target**, chọn **Next**.



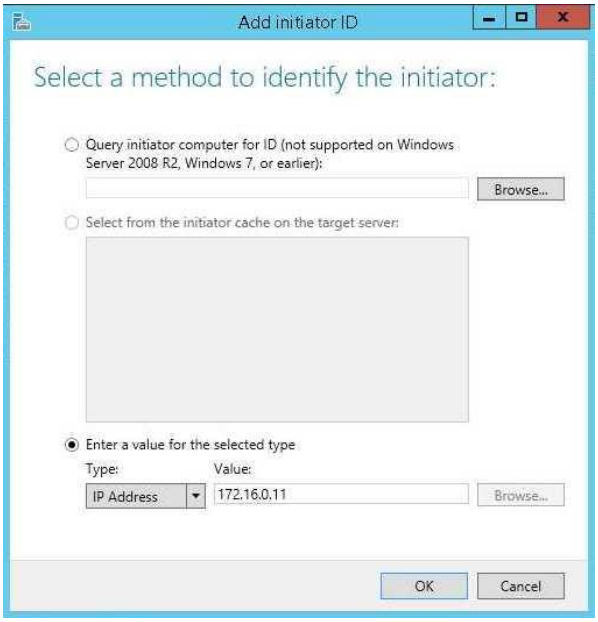
7. Cửa sổ **Specify target name**, nhập **LON-DC1** vào ô **Name**, chọn **Next**.



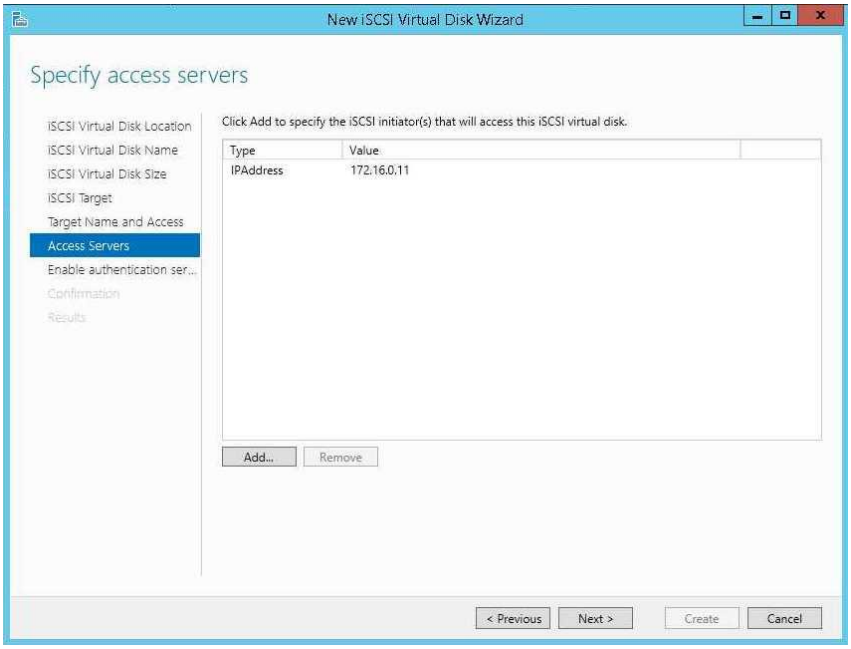
8. Cửa sổ **Specify access servers**, chọn **Add**.



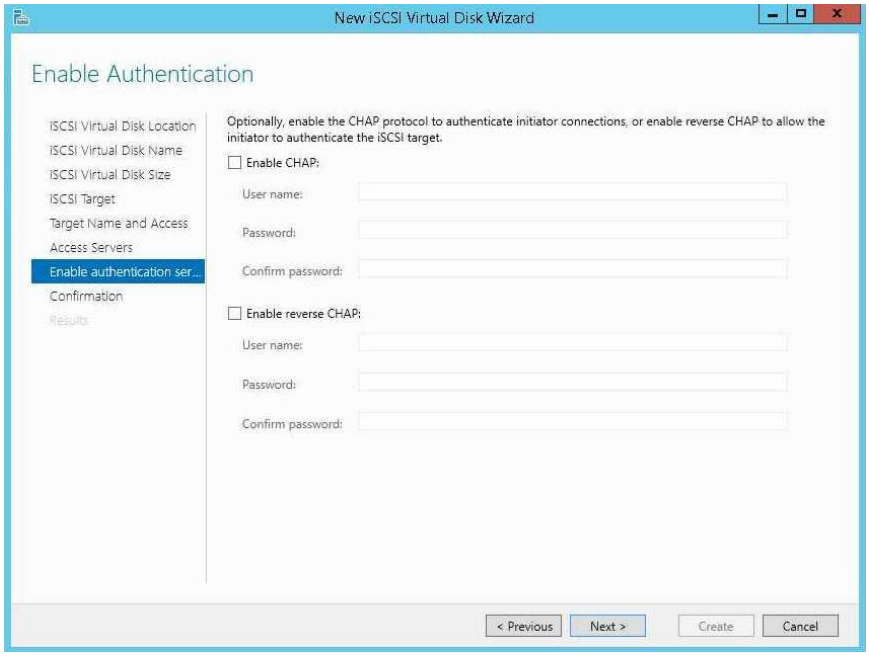
9. Trong hộp thoại **Select a method to identify the initiator**, chọn **Enter a value for the selected type**, bung ô **Type**, chọn **IP Address**, nhập **172.16.0.11** vào ô **Value**, và chọn **OK**.



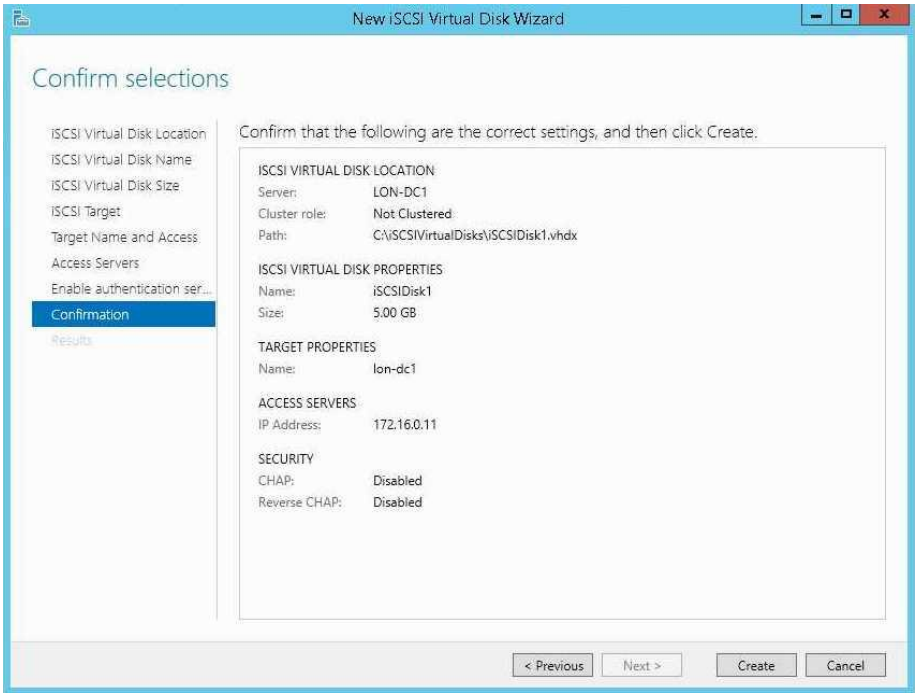
10. Cửa sổ **Specify access servers**, chọn **Next**.



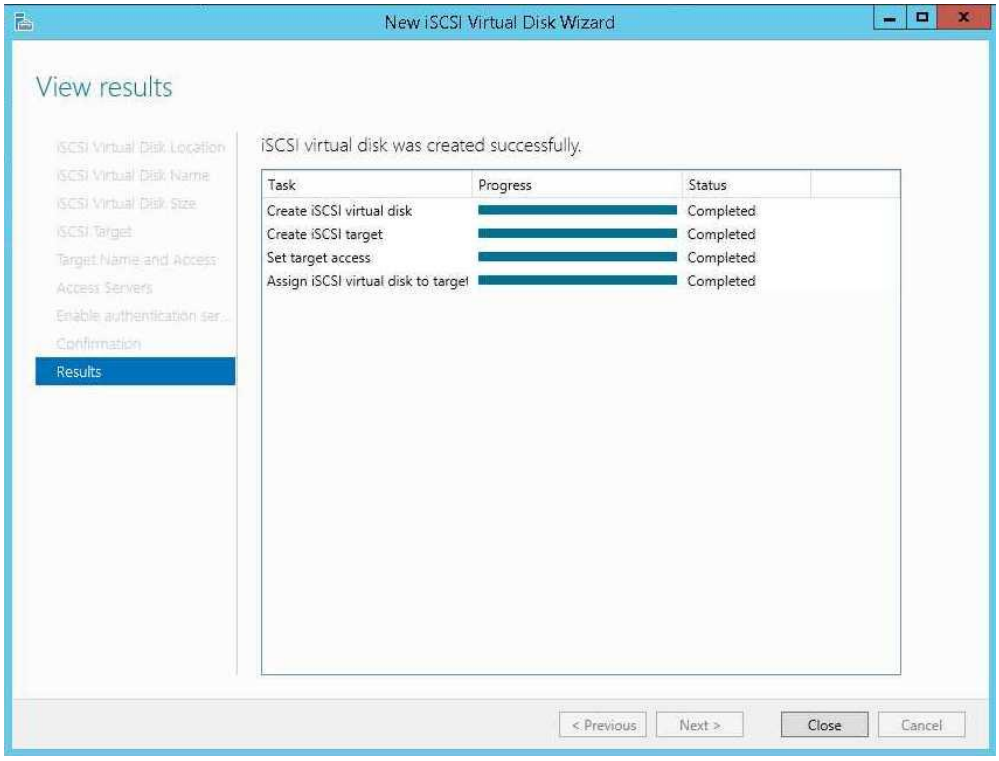
11. Cửa sổ **Enable Authentication**, chọn **Next**.



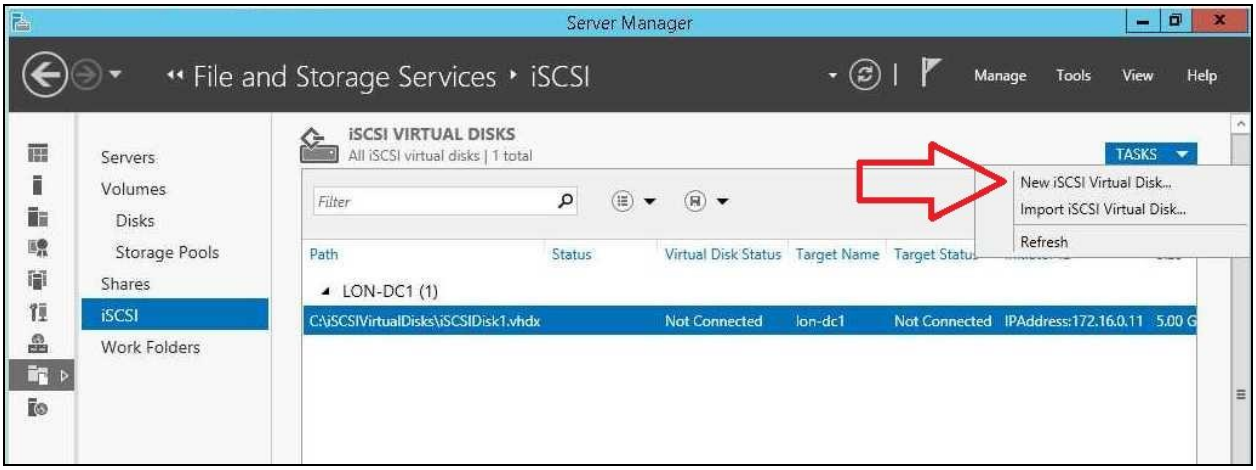
12. Cửa sổ **Confirm selections**, chọn **Create**.



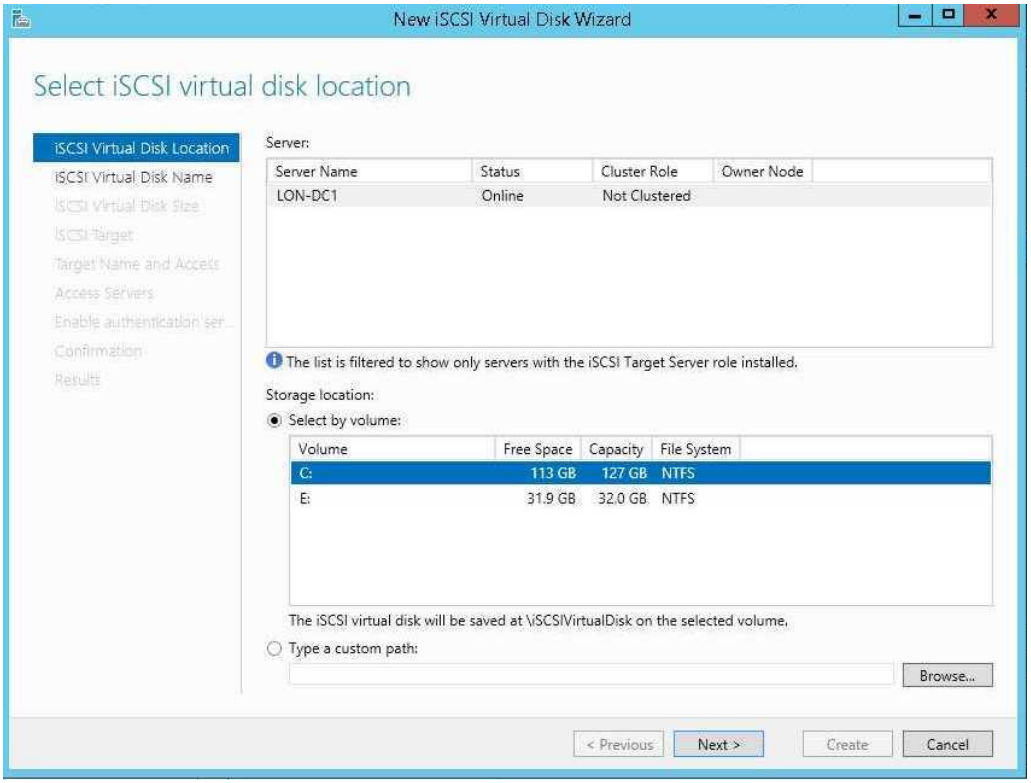
13. Cửa sổ **View results**, chọn **Close**.



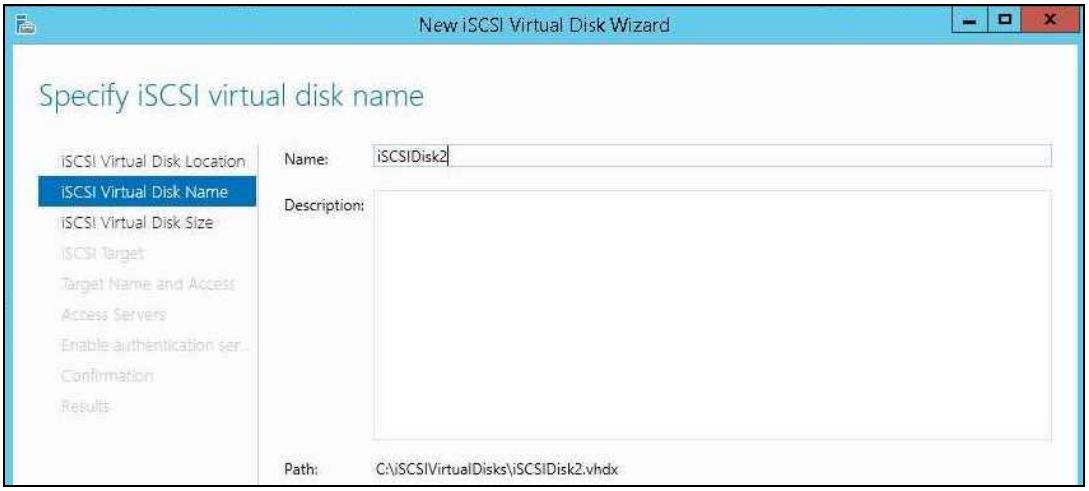
14. Trong cửa sổ **iSCSI VIRTUAL DISKS**, bung **TASKS**, chọn **New iSCSI Virtual Disk**.



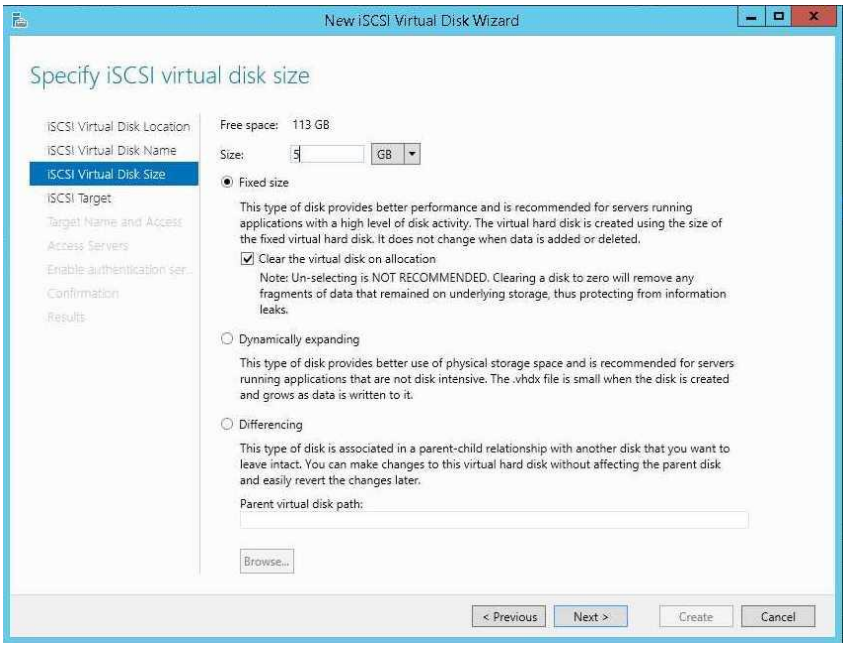
15. Cửa sổ **Select iSCSI virtual disk location**, trong ô **Storage location**, chọn **C:**, và chọn **Next**.



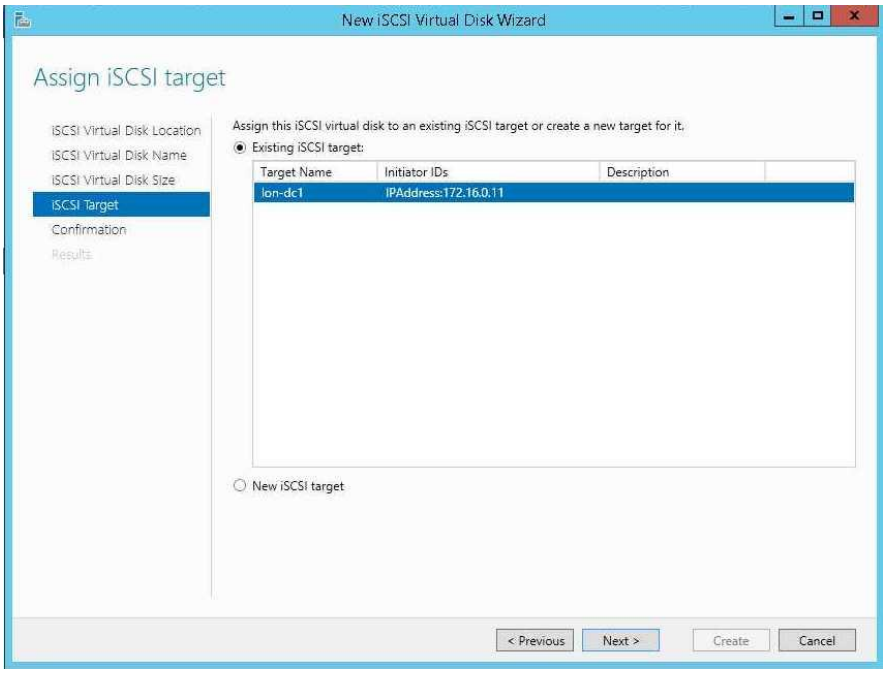
16. Cửa sổ **Specify iSCSI virtual disk name**, nhập **iSCSIDisk2** vào ô **Name**, chọn **Next**.



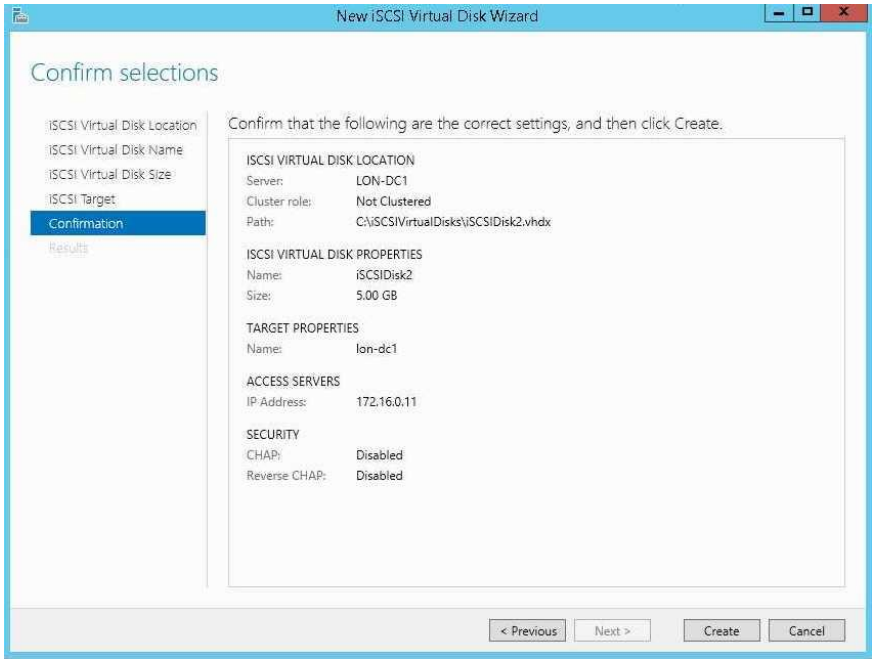
17. Cửa sổ **Specify iSCSI virtual disk size**, trong ô **Size**, nhập số **5**, chọn **GB**, và chọn **Next**.



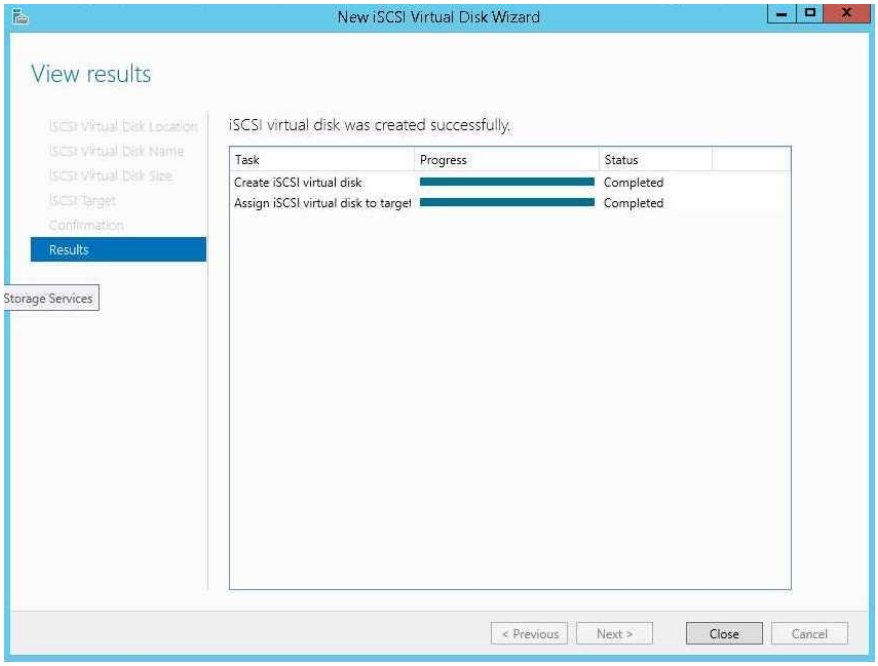
18. Cửa sổ **Assign iSCSI target**, chọn **lon-dc1**, và chọn **Next**.



19. Cửa sổ **Confirm selection**, chọn **Create**.



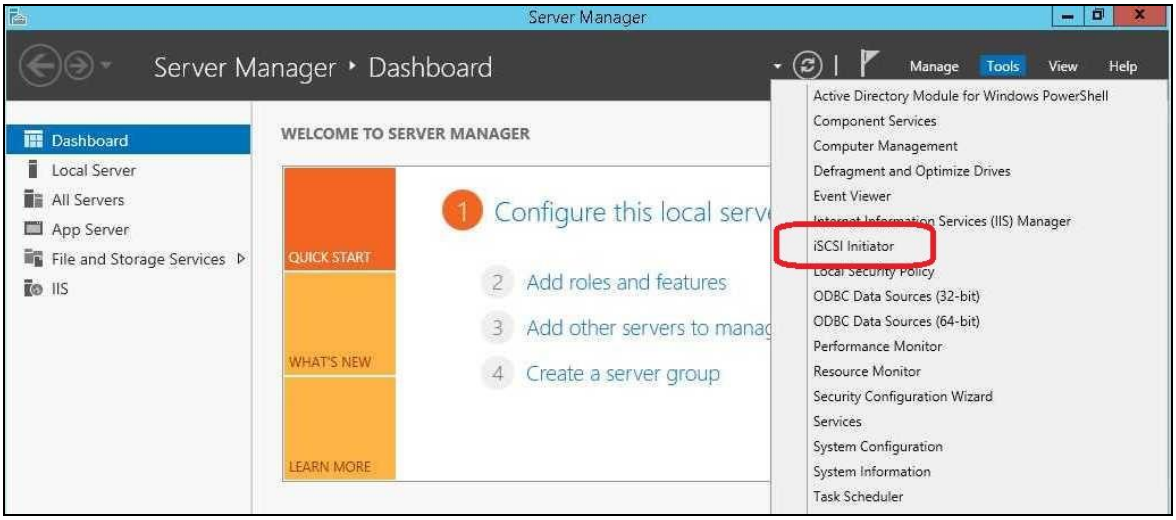
20. Cửa sổ **View results**, sau khi tạo thành công, chọn **Close**.



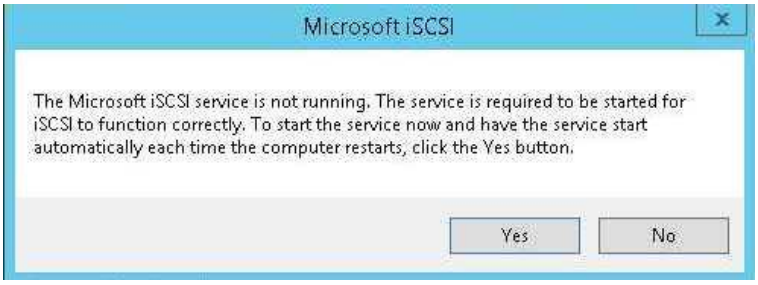
Bước 3. Kết nối tới iSCSI targets.

1. Qua máy **LON-SVR1**.

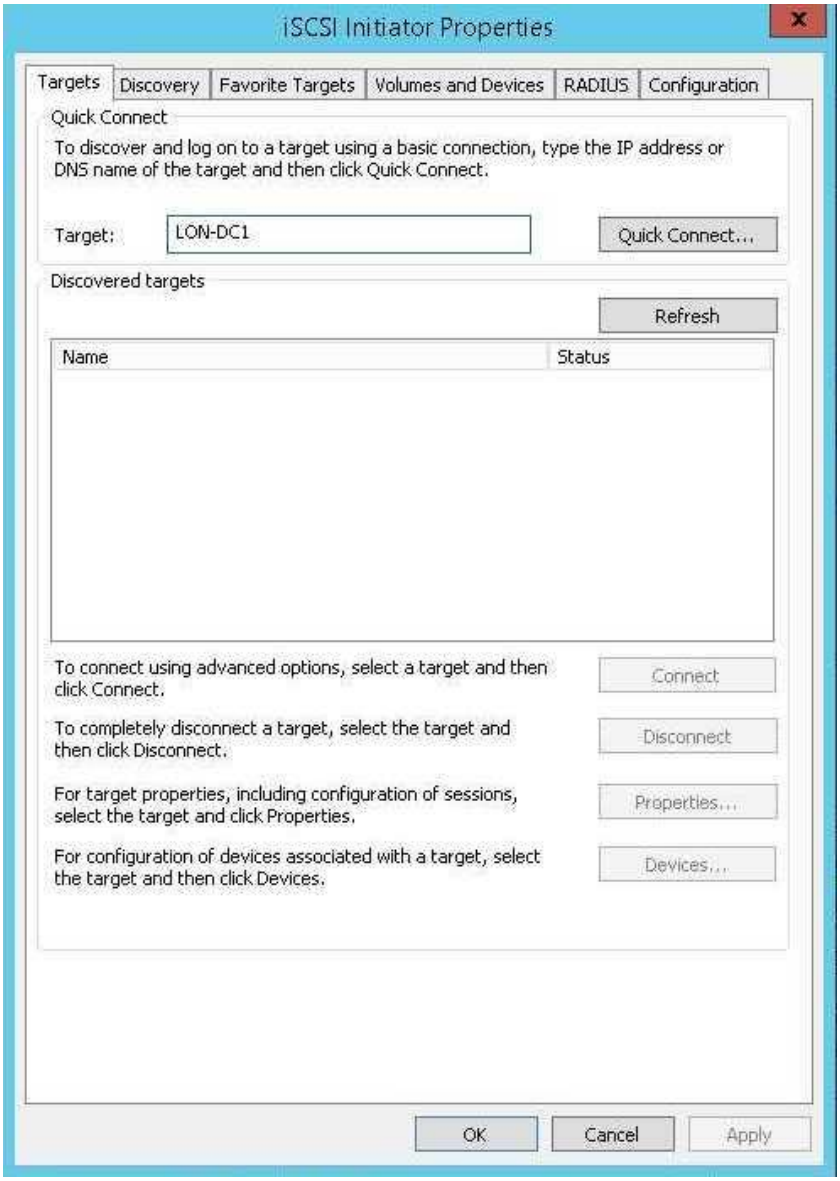
2. Mở **Server Manager**, bung menu **Tools**, mở **iSCSI Initiator**.



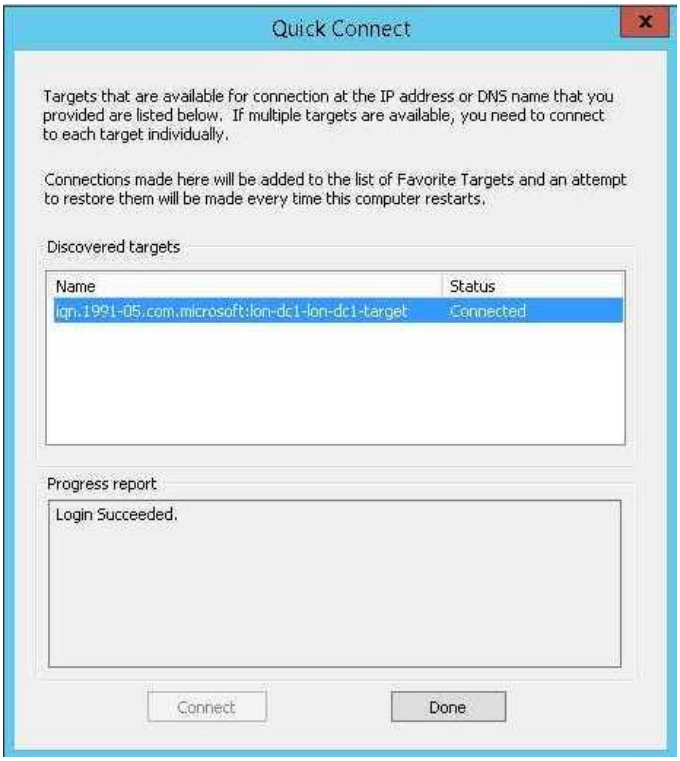
3. Hộp thoại **Microsoft iSCSI**, chọn **Yes**.



4. Trong hộp thoại **iSCSI Initiator Properties**, nhập **LON-DC1** vào ô **Targets**, chọn **Quick Connect**.



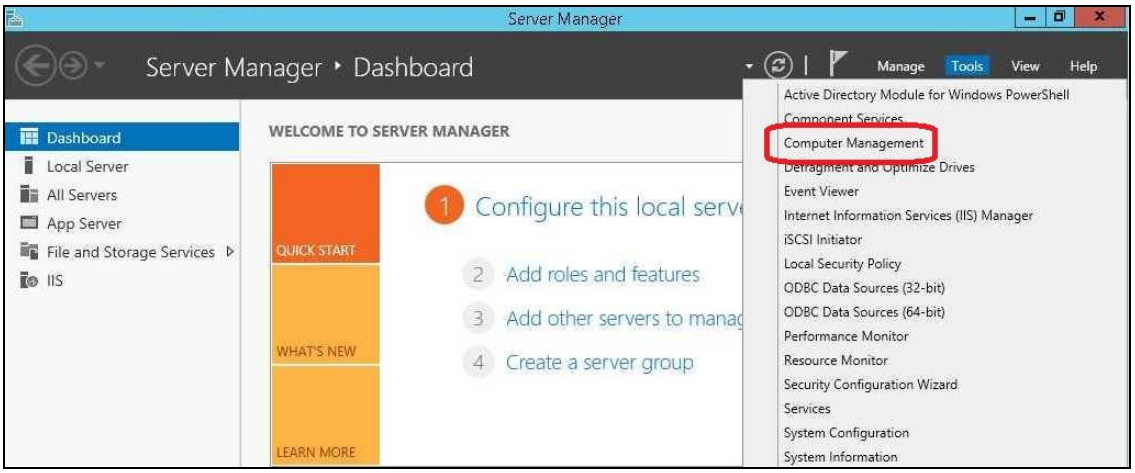
5. Trong hộp thoại **Quick Connect**, chọn **iqn.1991- 05.com.microsoft:lon-dc1-lon-dc1-target**, và chọn **Done**.



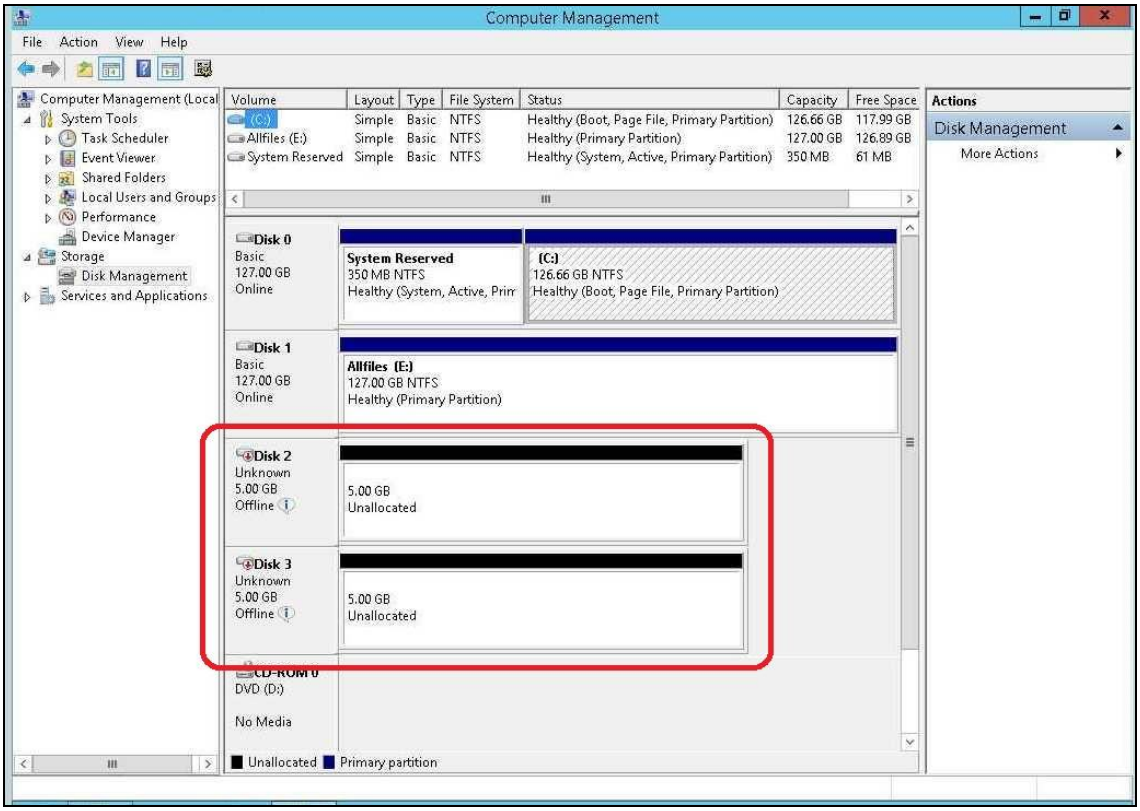
6. Hộp thoại **iSCSI Initiator Properties**, chọn **OK**.



7. Trong cửa sổ **Server Manager**, bung menu **Tools**, chọn **Computer Management**.



8. Trong cửa sổ **Computer Management**, bung **Storage**, chọn **Disk Management**. Kiểm tra có thêm 2 ổ cứng mới. Tuy nhiên, chúng đang ở trạng thái offline và chưa được định dạng.



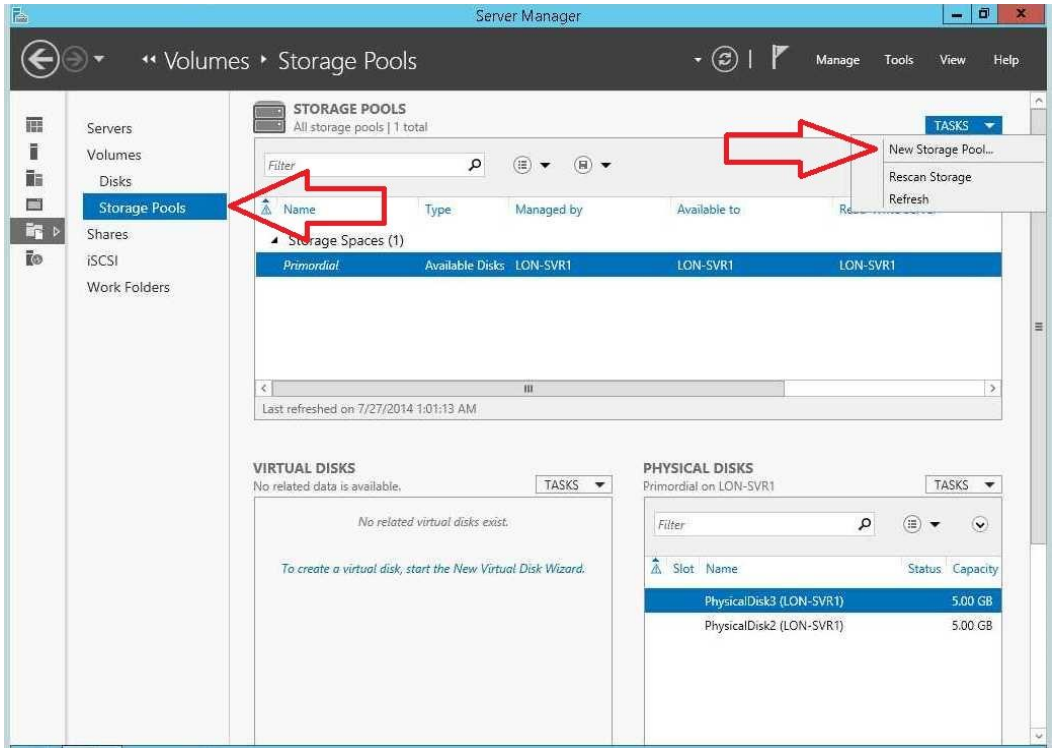
9. Tắt **Computer Management**.

Bước 4. Tạo Storage pool sử dụng iSCSI Disk.

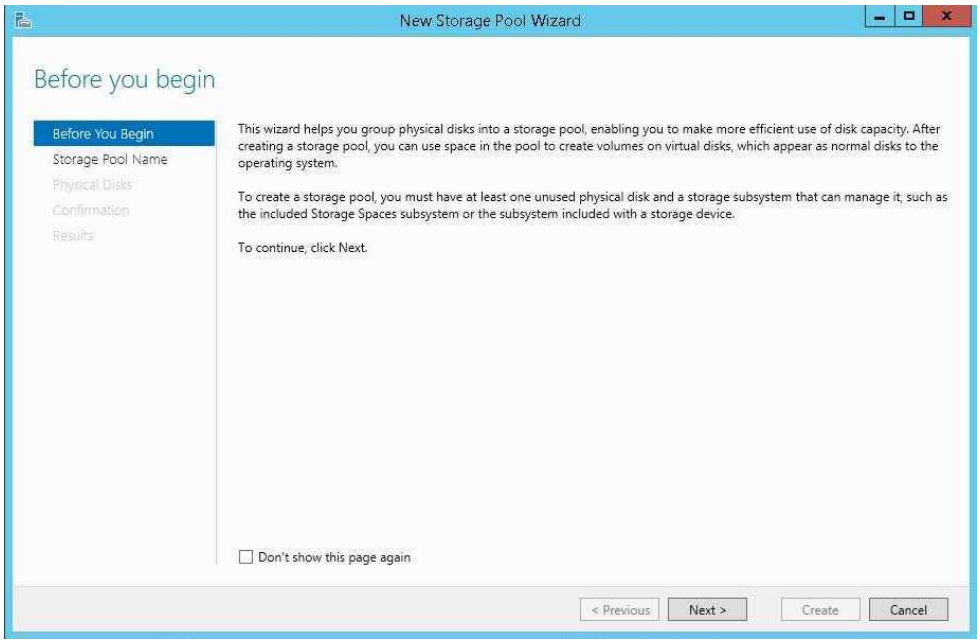
1. Trên máy **LON-SVR1**, mở **Server Manager**, chọn **File and Storage Services**.



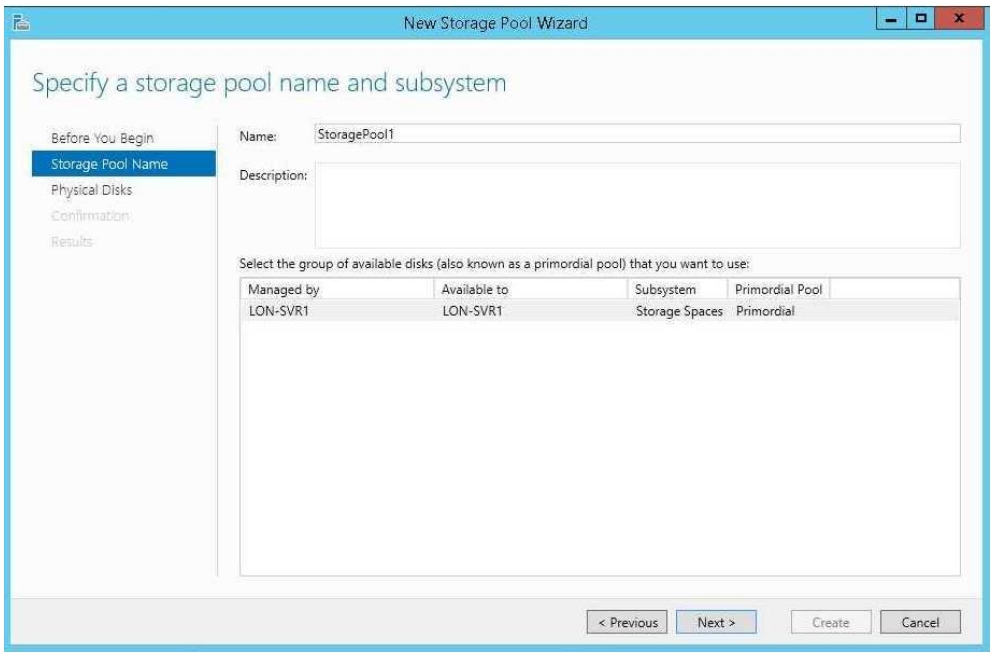
2. Chọn **Storage Pools**, bung **TASKS**, chọn **New Storage Pool**.



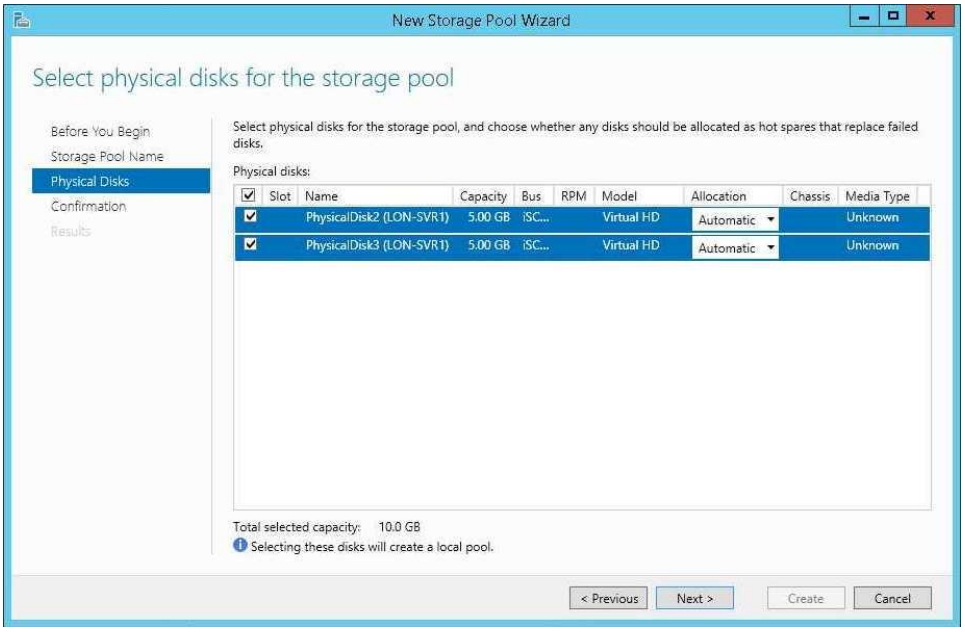
3. Trong cửa sổ **Before you begin**, chọn **Next**.



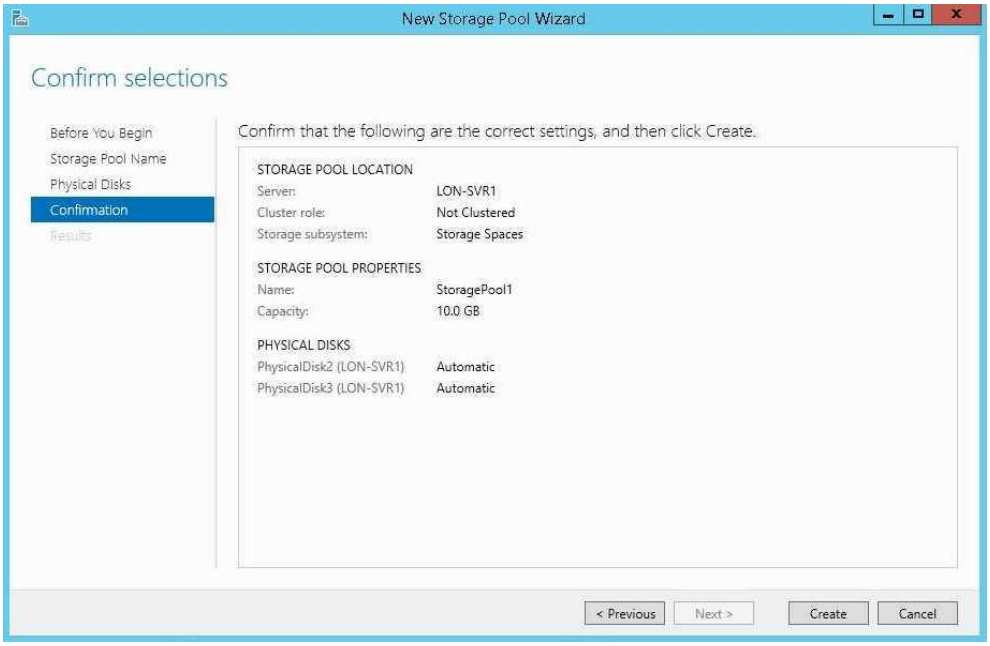
4. Cửa sổ **Specify a storage pool name and subsystem**, nhập **StoragePool1**vào ô **Name,** chọn **Next**.



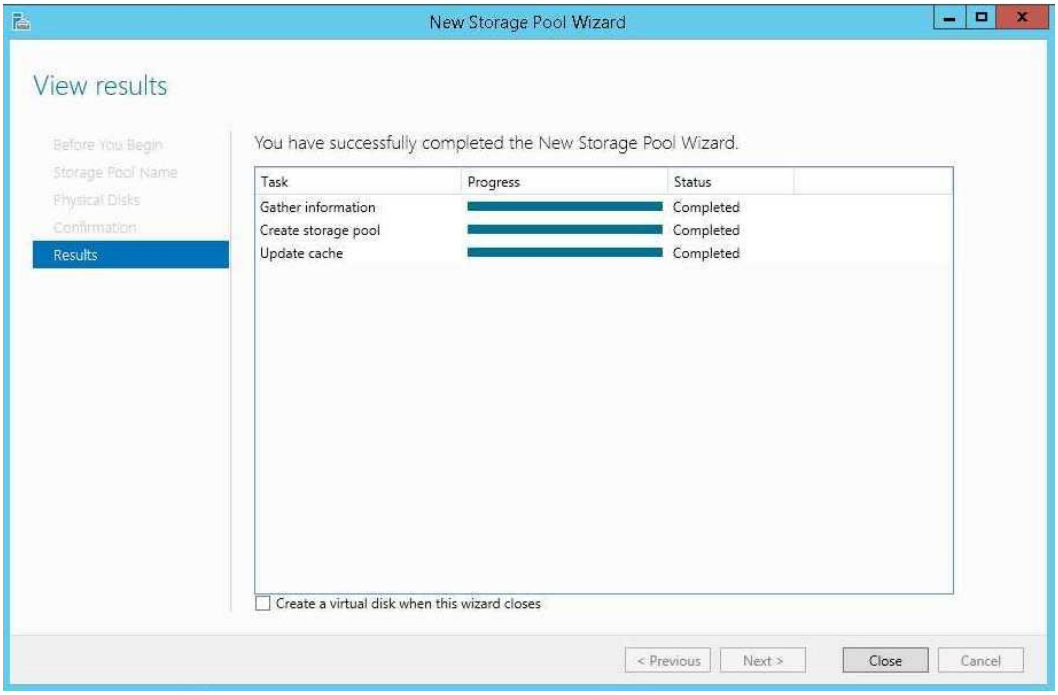
5. Cửa sổ **Select physical disks for the storage pool**, đánh dấu chọn cả 2 ổ cứng đang có, và chọn **Next**.



6. Cửa sổ **Confirm selections**, chọn **Create**.

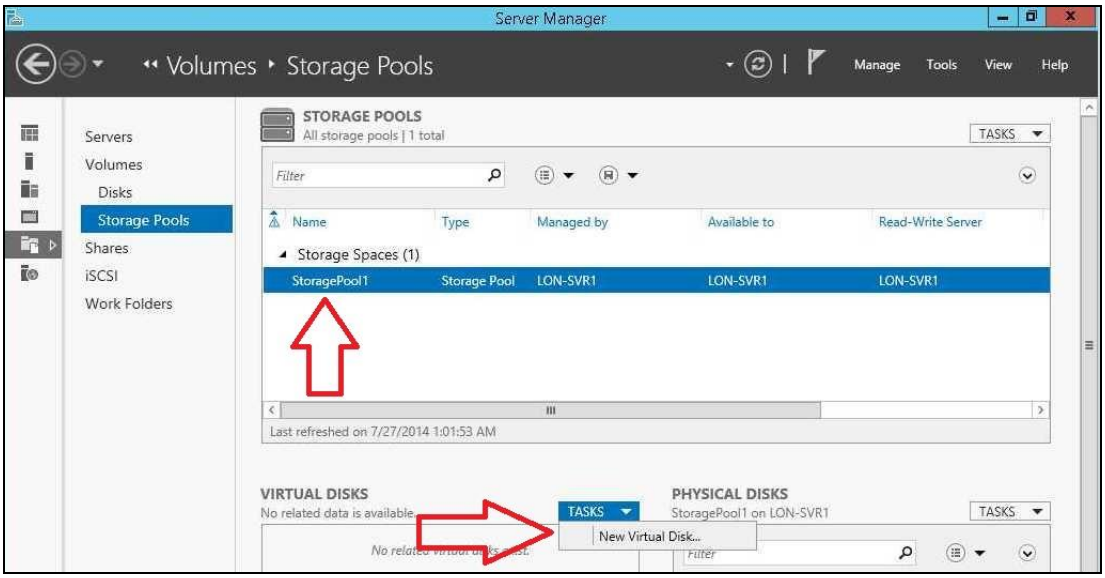


7. Cửa sổ **View results**, sau khi tạo thành công, và chọn **Close**.

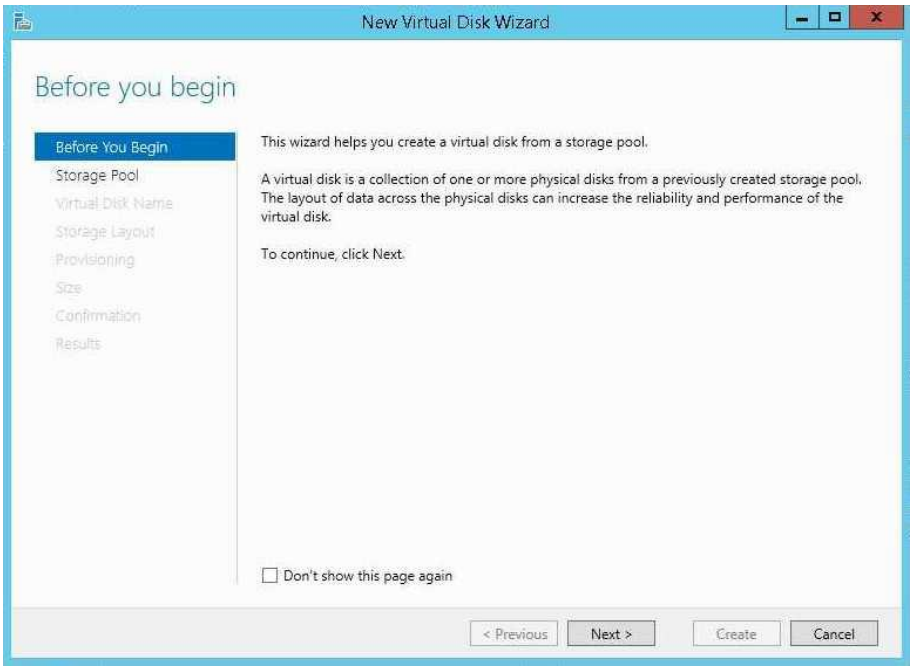


Bước 5. Tạo Mirrored Disk.

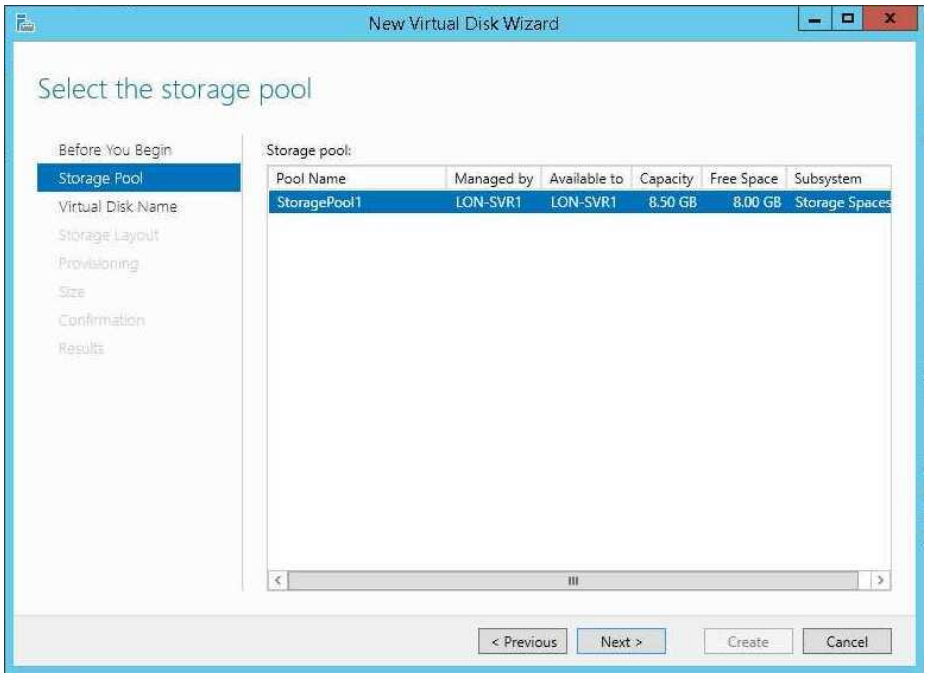
1. Trên máy **LON-SVR1**, quay lại cửa sổ **STORAGE POOLS**, chọn **StoragePool1**, trong phần **VIRTUAL DISKS**, bung **TASKS**, chọn **New Virtual Disk**.



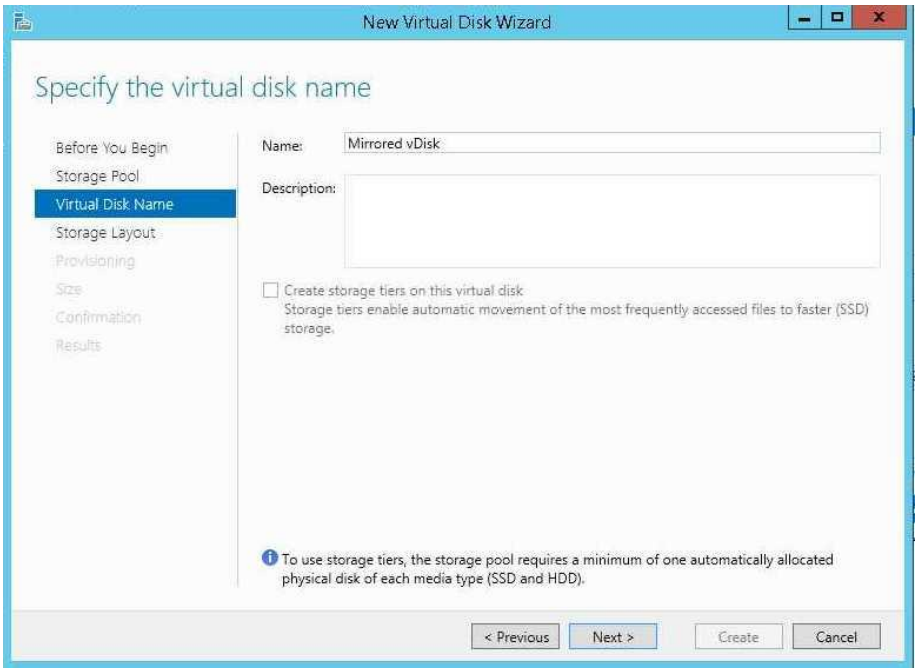
2. Cửa sổ **Before you begin**, chọn **Next**.



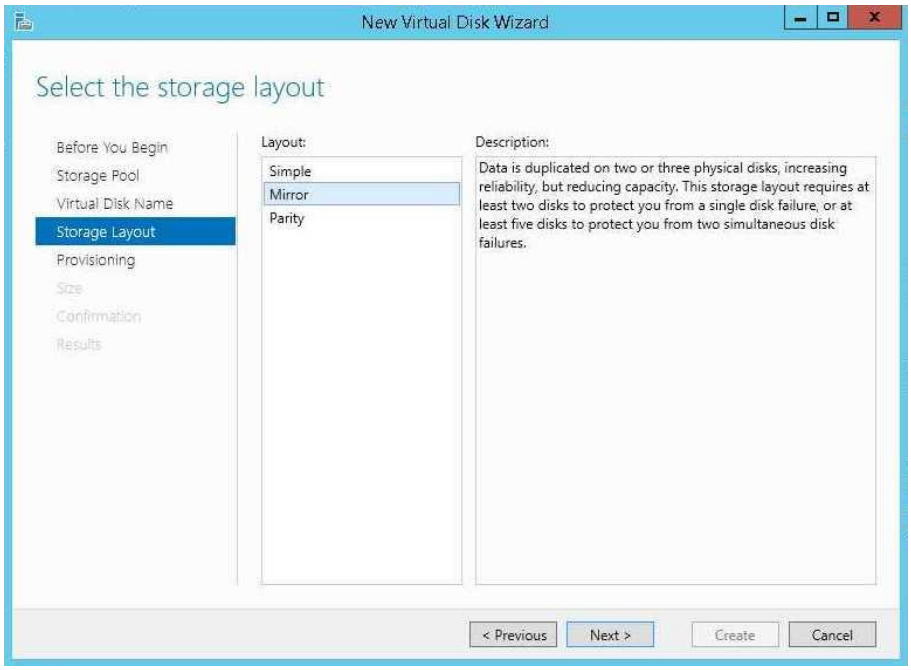
3. Cửa sổ **Select the storage pool**, chọn **StoragePool1**, và chọn **Next**.



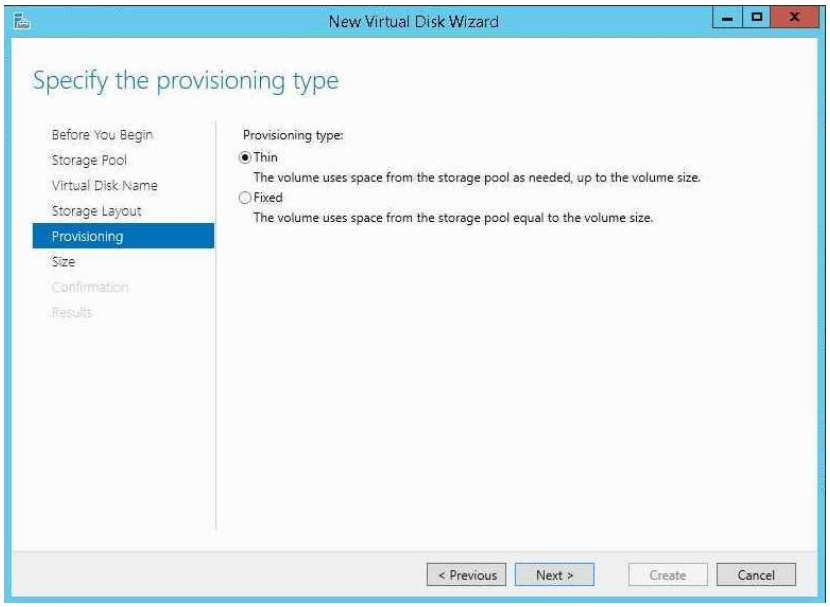
4. Cửa sổ **Specify the virtual disk name**, nhập **Mirrored vDisk** vào ô **Name**, và chọn **Next**.



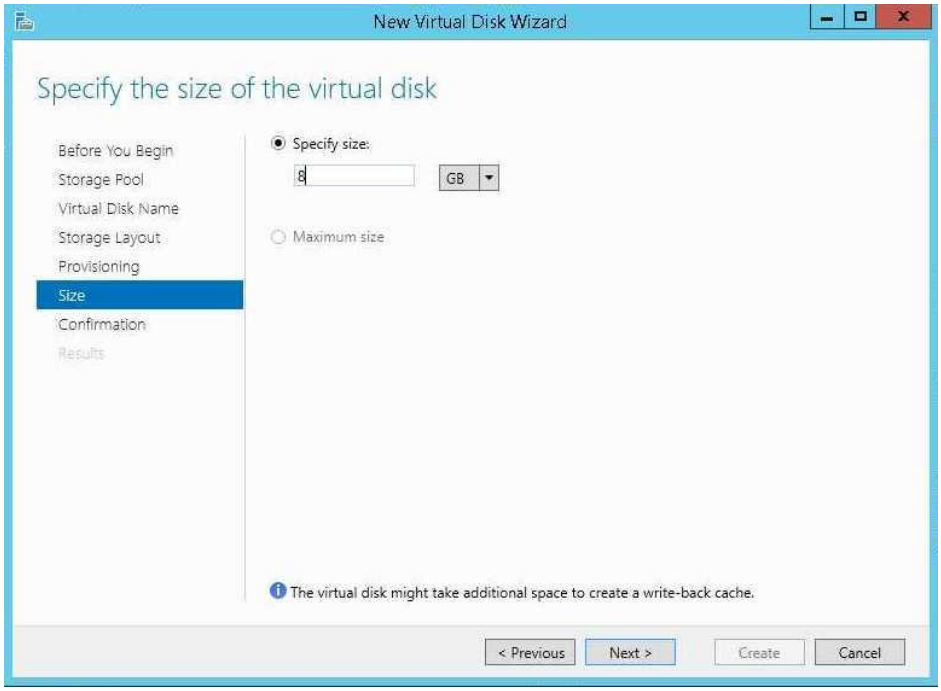
5. Cửa sổ **Select the storage layout**, chọn **Mirror**, chọn **Next**.



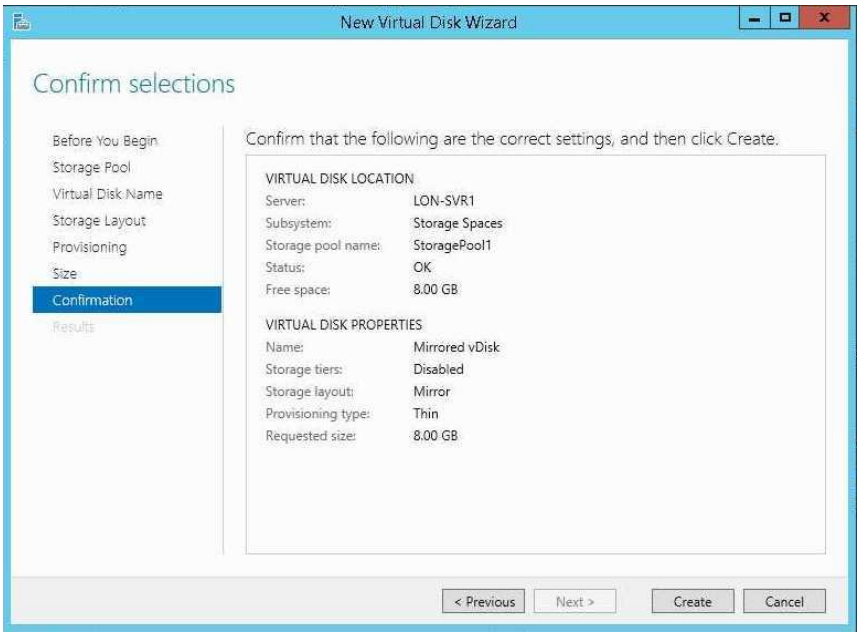
6. Cửa sổ **Specify the provisioning type**, chọn **Thin**, chọn **Next**.



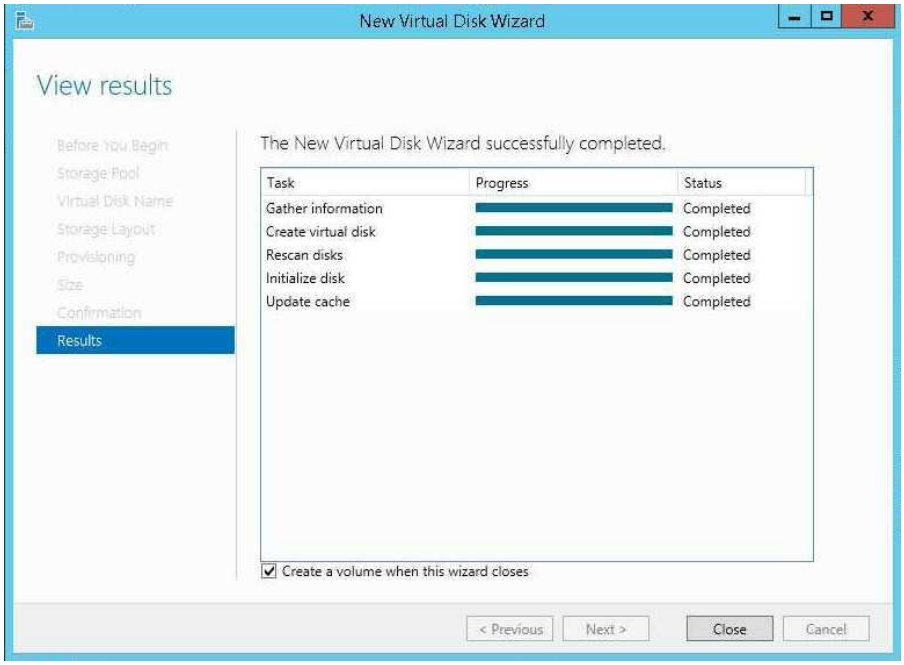
7. Cửa sổ **Specify the size of the virtual disk**, trong ô **Virtual disk size**, nhập **8 GB**, chọn **Next**.



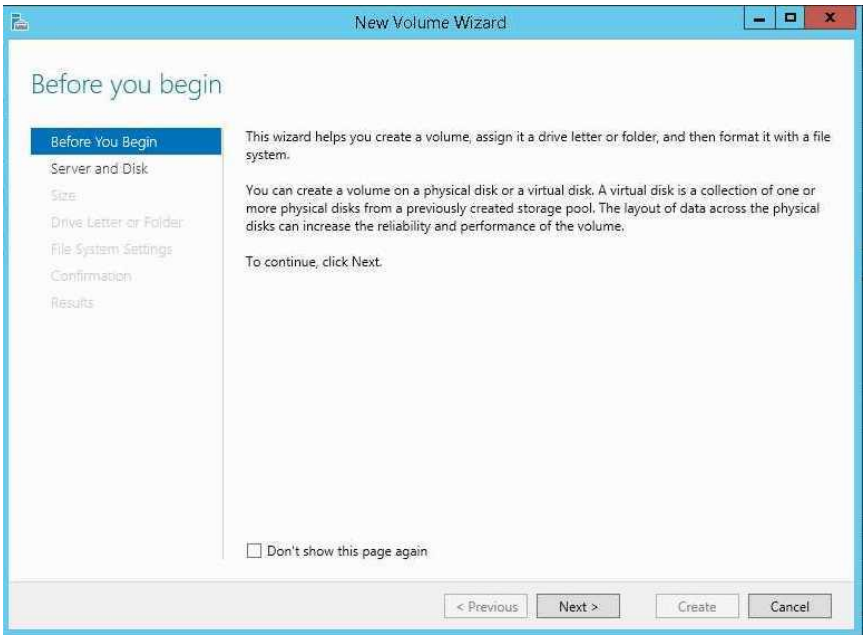
8. Cửa sổ **Confirm selections**, chọn **Create**.



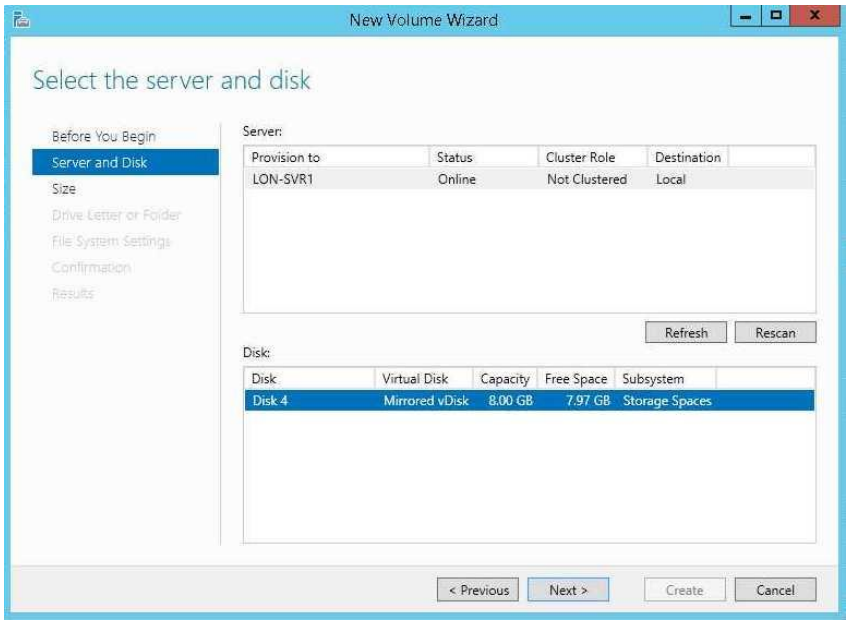
9. Cửa sổ **View results**, đợi sau khi tạo thành công, đảm bảo có đánh dấu chọn ô **Create a volume when this wizard closes**, chọn **Close**.



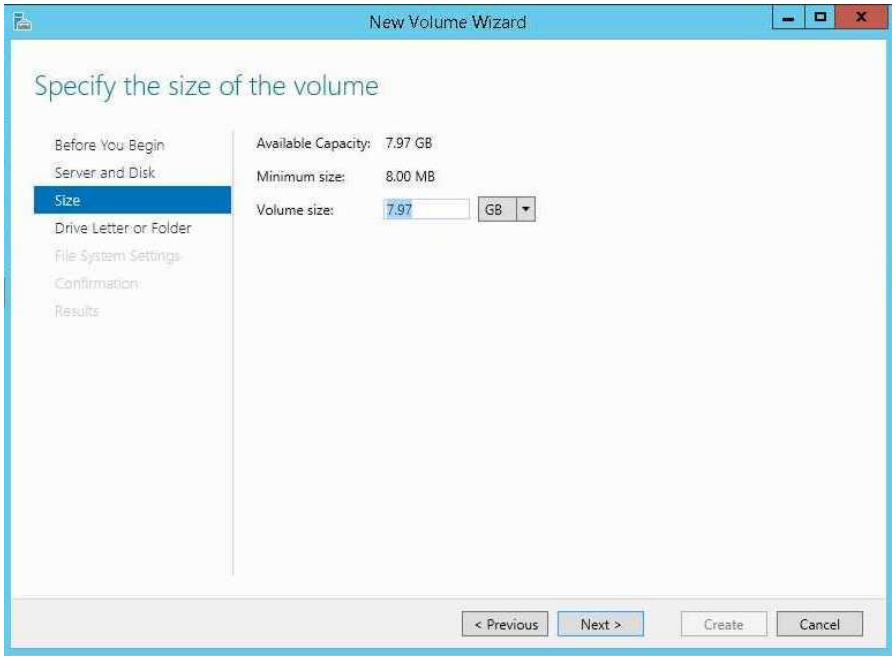
10. Cửa sổ **Before you begin**, chọn **Next**.



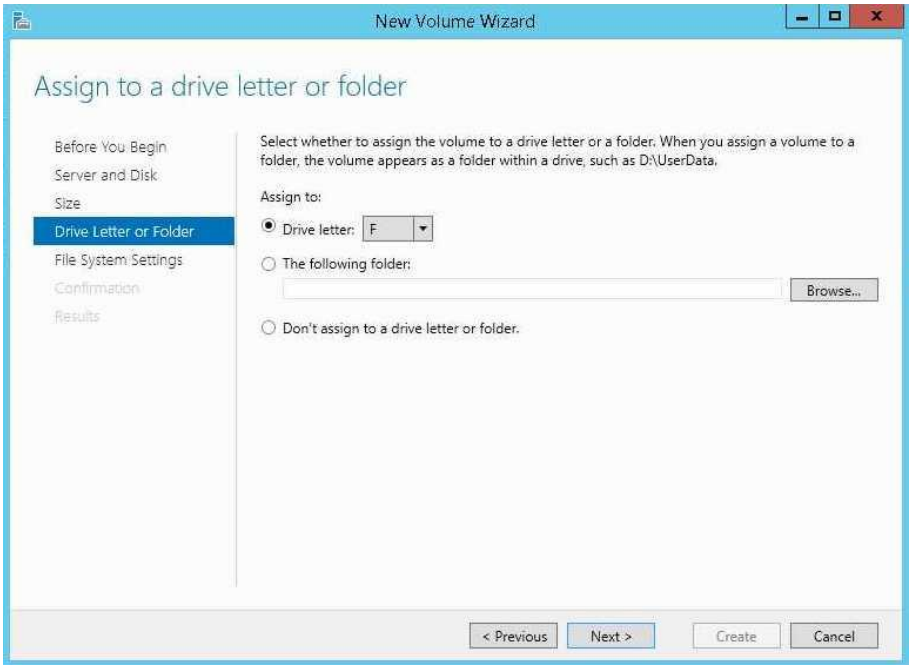
11. Cửa sổ **Select the server and disk**, trong ô **Disk**, chọn ổ đĩa **Mirrored vDisk**, và chọn **Next**.



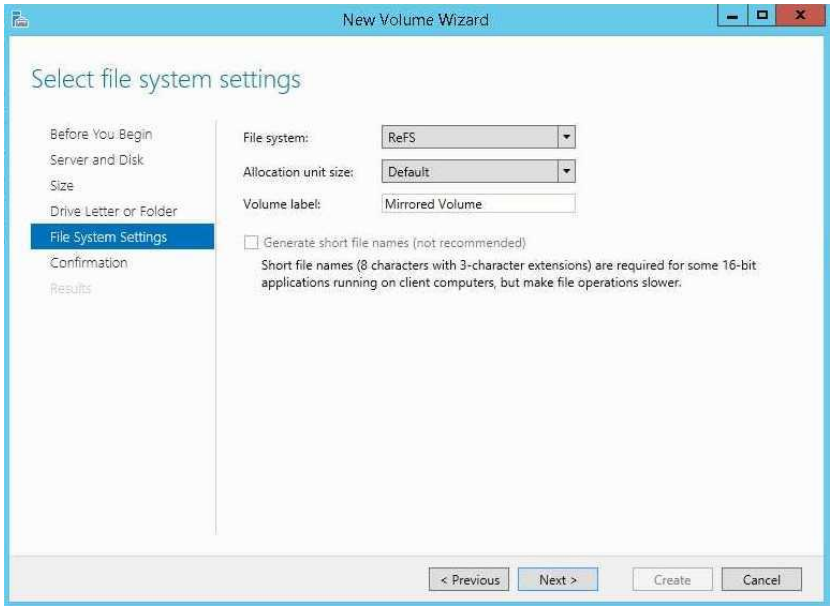
12. Cửa sổ **Specify the size of the volume**, để dung lượng mặc định, chọn **Next**.



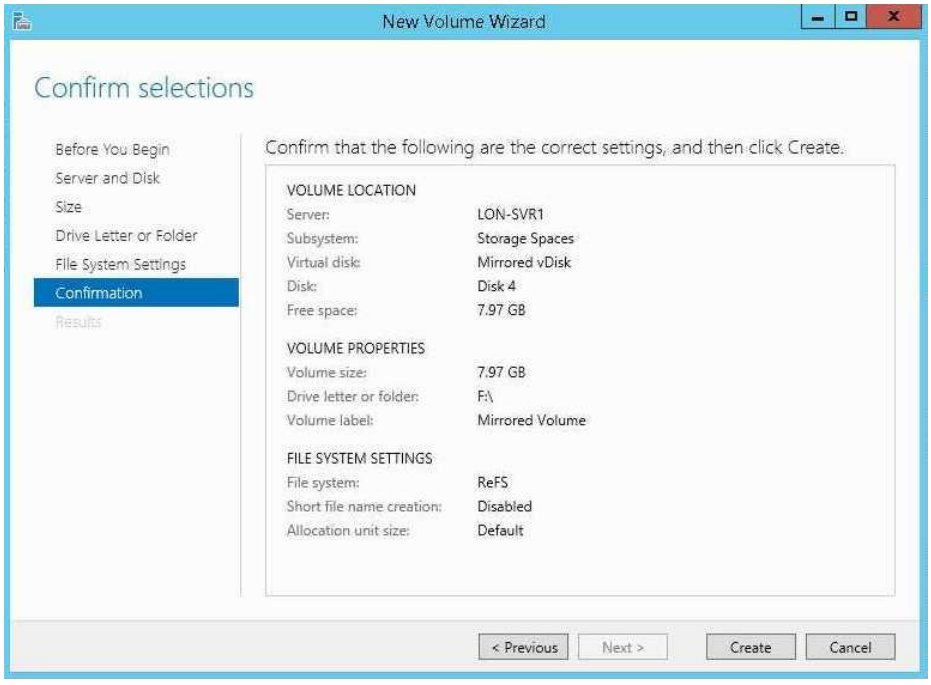
13. Cửa sổ **Assign to a drive letter or folder**, bung **Drive letter**, chọn **F**, chọn **Next**.



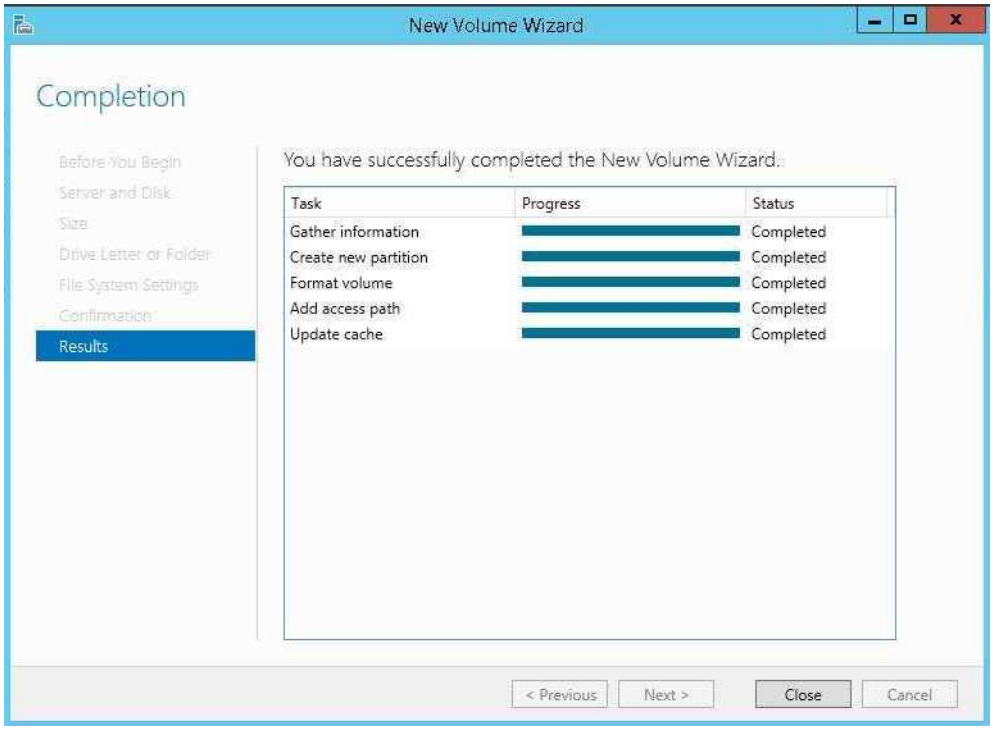
14. Cửa sổ **Select file system settings** page, bung **File system**, chọn **ReFS**. Nhập **Mirrored Volume** vào ô **Volume label**, và chọn **Next**.



15. Cửa sổ **Confirm selections**, chọn **Create**.

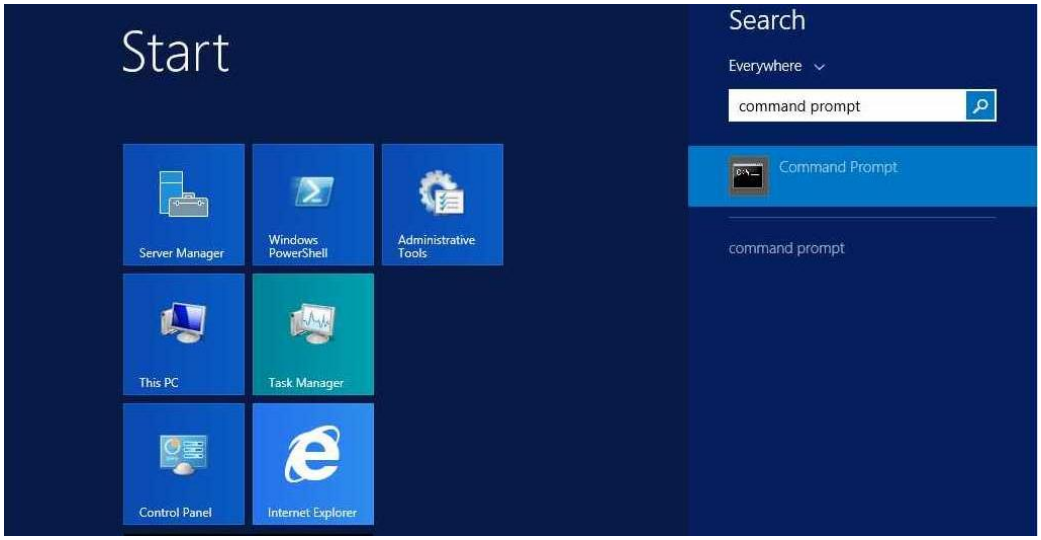


16. Cửa sổ **Completion**, sau khi tạo thành công, chọn **Close**.



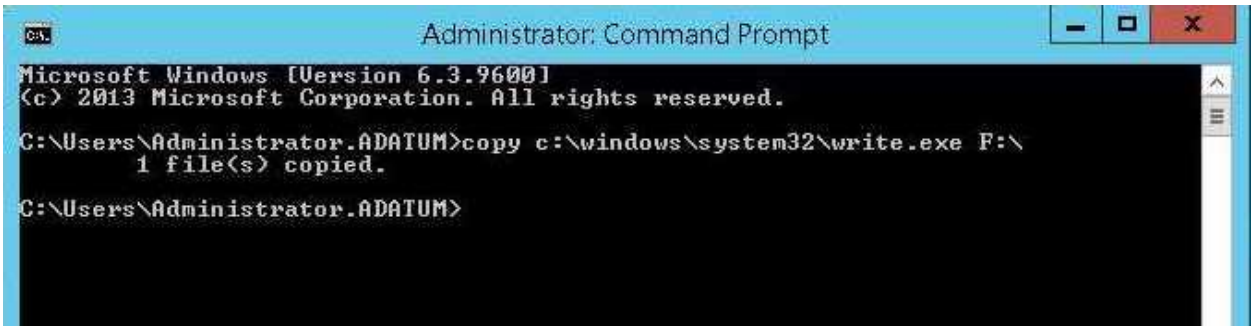
Bước 6. Chép dữ liệu vào Mirror Disk.

1. Trên máy **LON-SVR1**, bung menu **Start**, gõ **command prompt**, nhấn **Enter**.



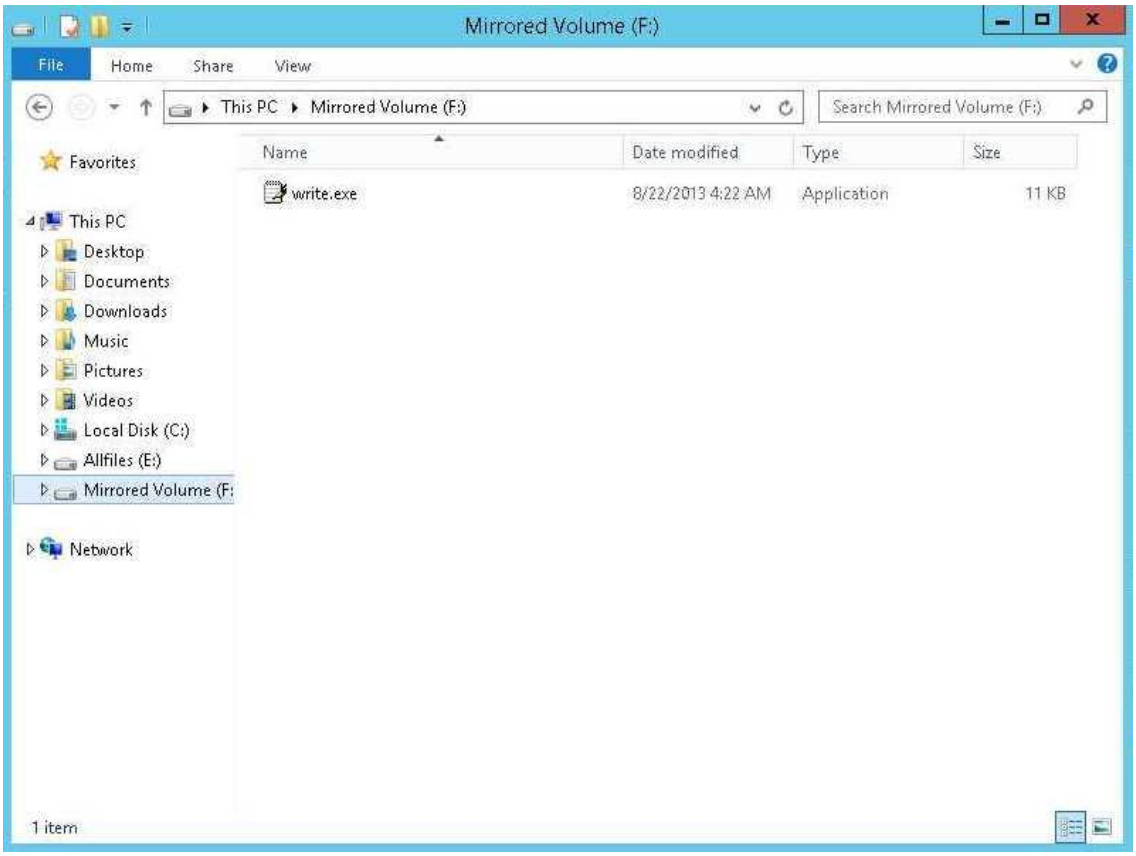
2. Trong cửa sổ **Command prompt**, gõ lệnh:

Copy C:\windows\system32\write.exe F:



3. Tắt Command prompt.

4. Trên thanh **Taskbar**, mở **File Explorer**. Vào ổ đĩa **Mirrored Volume (F:)**, kiểm tra có file **write.exe**.



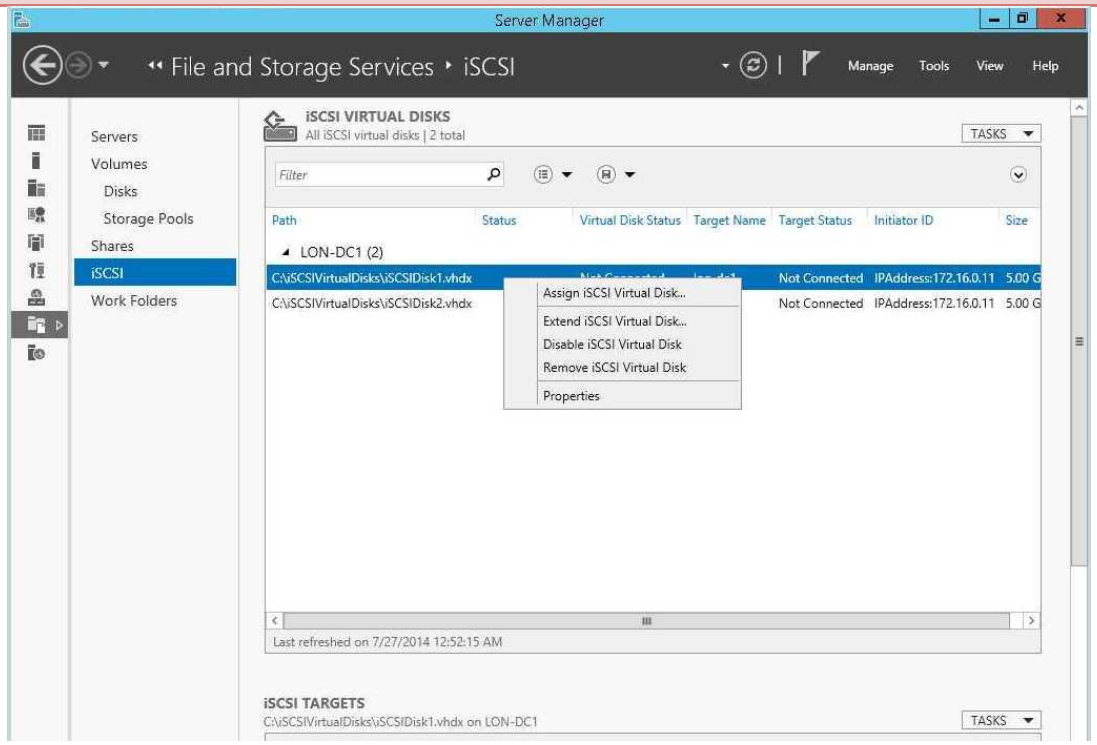
5. Tắt **File Explorer**.

Bước 7. Ngắt kết nối một đĩa iSCSI và kiểm tra vẫn truy cập ứng dụng thành công.

1. Qua máy **LON-DC1.**

2. Mở **Server Manager**, chọn **File and Storage Services**, chọn **iSCSI**, nhấn chuột phải **C:\iSCSIVirtualDisks\iSCSIDisk1.vhdx**, chọn **Disable iSCSI Virtual Disk**.

Chú ý: Bước này để giả lập Disk1 bị lỗi.

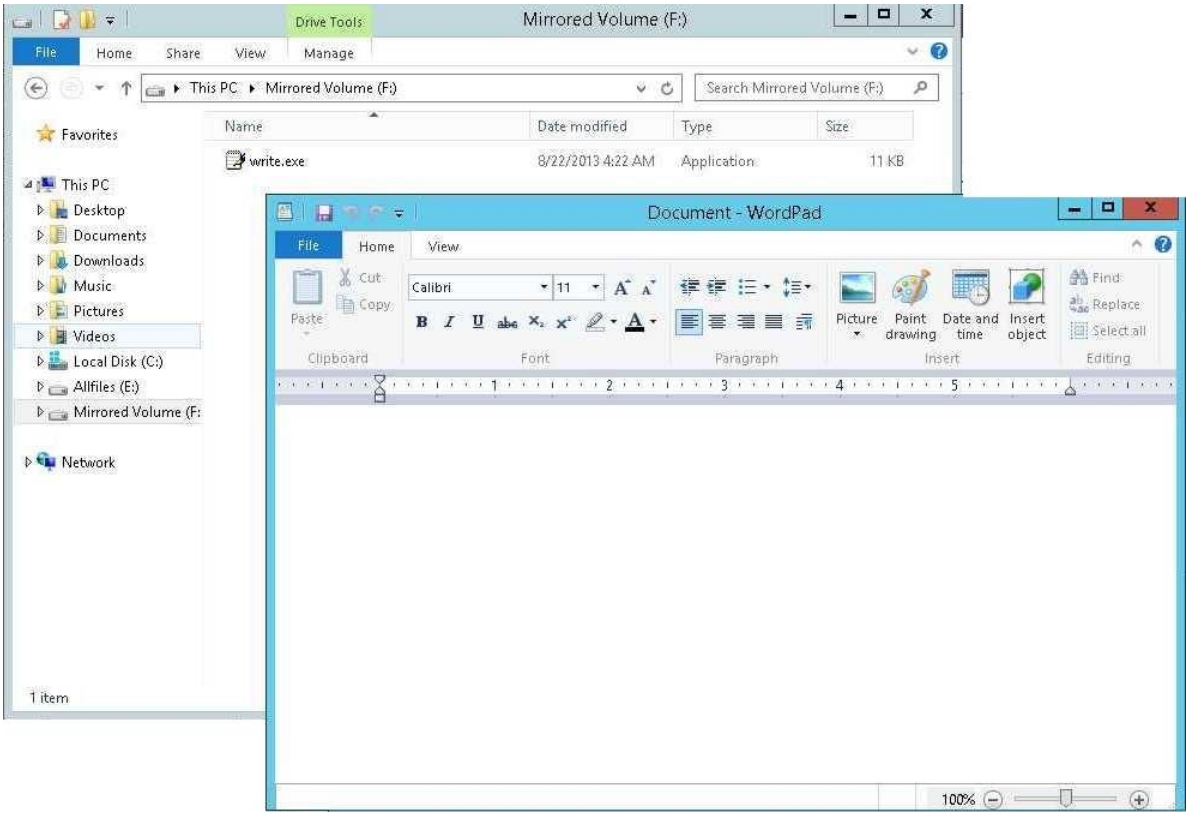


3. Hộp thoại **Disable iSCSI Virtual Disk**, chọn **Yes**.



4. Qua máy **LON-SVR1**.

5. Trên thanh **Taskbar**, mở **File Explorer**, vào ổ đĩa **Mirrored Volume (F:)**, chạy file **write.exe,** kiểm tra vẫn truy cập ứng dụng thành công.



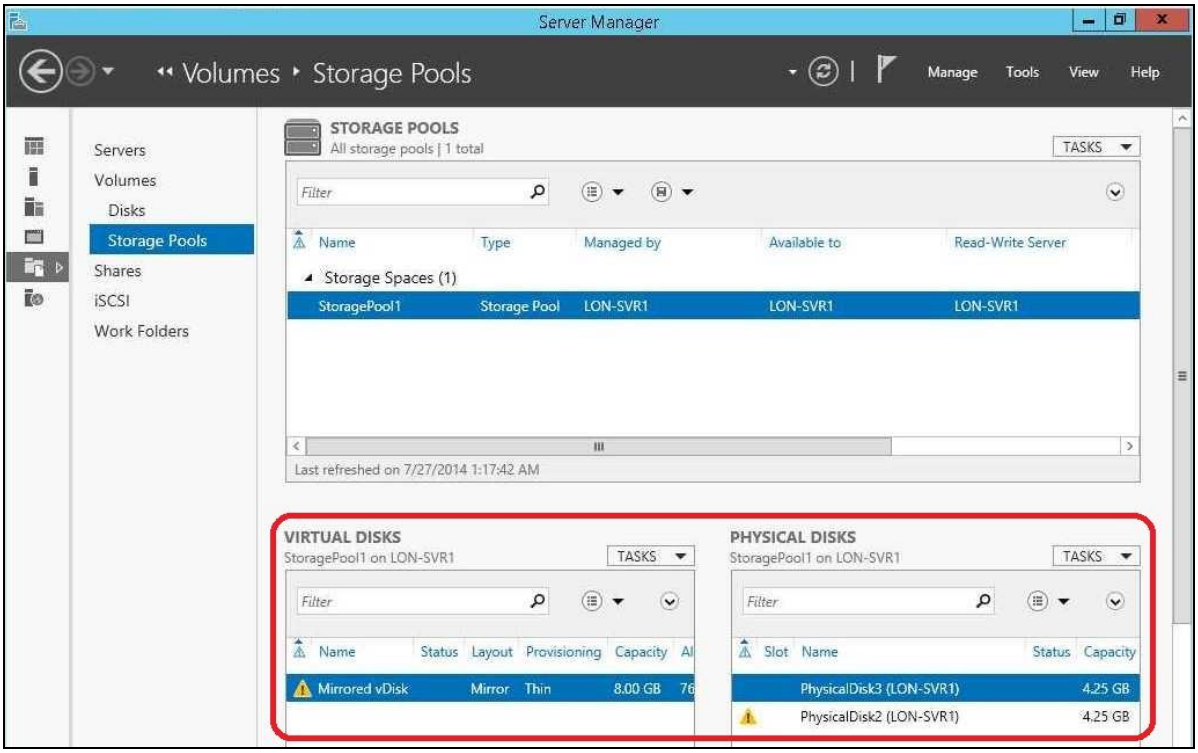
6. Tắt cửa sổ **Document - WordPad**.

7. Tắt **File Explorer**.

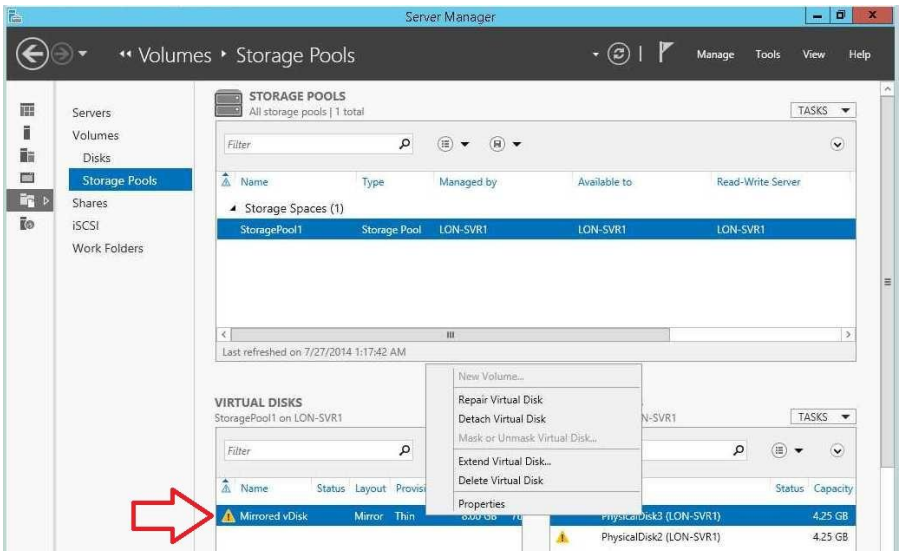
8. Mở **Server Manager**, trong cửa sổ **STORAGE POOLS**, chọn **StoragePool1**, chọn biểu tượng **Refresh.**



Chú ý: Cảnh báo được hiển thị trong ô **VIRTUAL DISK** và **PHYSICAL DISKS**.

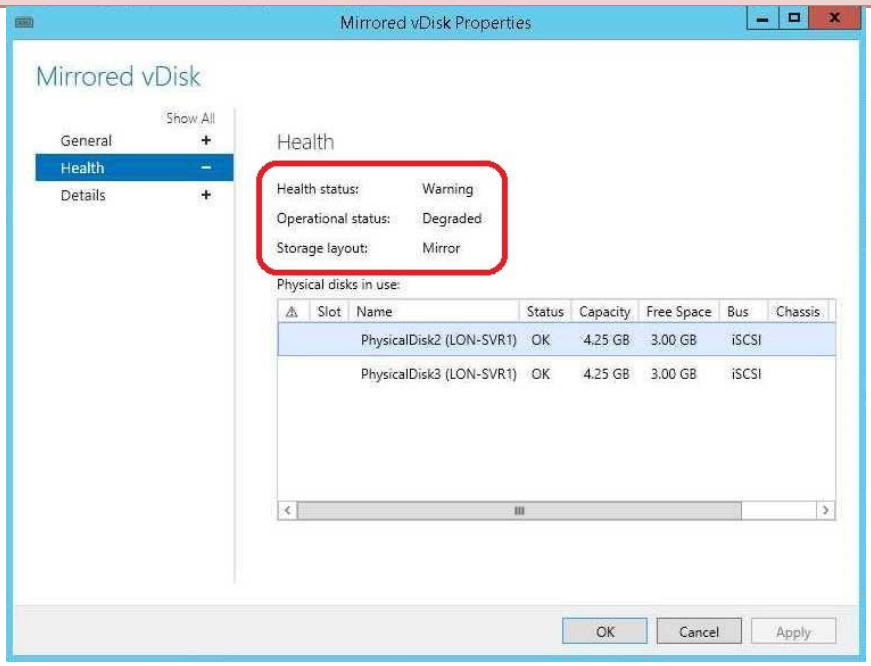


9. Trong ô **VIRTUAL DISK**, nhấn chuột phải **Mirrored vDisk**, chọn **Properties**.



10. Hộp thoại **Mirrored vDisk Properties**, chọn **Health**.

Chú ý: Nhận được cảnh báo về tình trạng sức khỏe và tình trạng hoạt động đang bị sụt giảm của Mirrored vDisk.



11. Chọn **OK** để tắt hộp thoại **Mirrored vDisk Properties**.

Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công giải pháp lưu trữ iSCSI SAN và khả năng chịu lỗi cho hệ thống lưu trữ.

VII. Chuẩn bị cho bài tiếp theo:

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-LON-SVR1.**

Bài 11: Thiết kế và triển khai giải pháp bảo vệ hệ thống mạng

I. Mục tiêu:

- Thiết kế giải pháp Windows Firewall.
- Cấu hình Windows Firewall.
- Thiết kế giải pháp Network Access Protection (NAP).
- Triển khai giải pháp NAP thực thi IPsec (NAP with IPsec enforcement)..

II. Kịch bản:

Gần đây, công ty A. Datum gặp vấn đề với phần mềm độc hại (malware) và ngăn chặn lưu lượng của đường truyền. Các phần mềm độc hại được phát tán từ các máy tính không phù hợp với chính sách bảo mật của công ty. Nguyên nhân gây ra việc bị ngăn chặn lưu lượng đường truyền là do các gói tin đánh hơi (packet-sniffing) được phát tán vào đường truyền.

A. Datum muốn cải thiện an ninh cho hệ thống bằng cách đảm bảo rằng các máy Server nhạy cảm phải được bảo vệ bởi những quy tắc tường lửa thích hợp, và các máy Server này chỉ chấp nhận các truy cập được chứng thực và mã hóa. Bất kỳ máy client khi tương tác với các máy Server này cần phải đáp ứng được tiêu chuẩn an toàn mà hệ thống đề ra.

A. Datum đang lo ngại rằng cấu trúc an ninh hiện tại không hiệu quả cho việc phân bổ nguồn lực. Gần đây, một nhóm các chuyên gia tư vấn bảo mật đã hoàn thành phân tích về rủi ro và nhu cầu bảo mật, và bây giờ bạn phải thực hiện một số thay đổi được đề xuất trong cơ sở hạ tầng mạng. Sau khi phân tích an ninh mạng, đội ngũ chuyên gia tư vấn bảo mật khuyên rằng bạn có thể cải thiện an ninh nội bộ bằng cách cấu hình Windows Firewall. Để tối đa hóa an ninh, họ đề xuất việc cấu hình các quy tắc truy cập ra ngoài đối với các máy clients và servers.

Để bảo mật thông tin liên lạc giữa các thành viên trong nhóm nghiên cứu của A. Datum, bạn phải ngăn cản người dùng không thuộc nhóm nghiên cứu truy cập dữ liệu hoặc các ứng dụng của nhóm này.

Để hỗ trợ việc thực hiện các quy tắc tường lửa, các nhân viên IT đã tạo ra một danh sách đầy đủ các ứng dụng đang được sử dụng tại A. Datum. Các ứng dụng và các cổng (port) được liệt kê trong bảng dưới đây.

Client application	**Destination port**	**Executable**
File and printer sharing server message block (SMB)	445	n/a
Research custom application	10101	Research.exe
Internet Explorer	80, 443, 8080	Iexplore.exe
Email client	Random RPC	Outook.exe

Server application	**Incoming port**	**Executable**
File and printer sharing (SMB)	445	n/a
Research custom application	10101	ResearchSrv.exe
Customer service web application	8080	n/a
Email server	Random RPC	Store.exe

Ngoài ra, bạn còn được yêu cầu thiết kế và triển khai giải pháp NAP để bổ sung tính năng bảo vệ cho hệ thống của A.Datum.

Các thông tin khác:

- Tất cả các máy client đã được nâng cấp lên Windows 8.1.
- Tất cả các máy client sử dụng địa chỉ IP động.

- Một WSUS Server nằm trong mạng nội bộ.
- Tất cả các máy clients và servers của bộ phận nghiên cứu là thành viên của domain Adatum.com.

III. Yêu cầu tổng quan:

1. Cấu hình Windows Firewall để giải quyết các vấn đề sau:
   - Cho phép truy cập các ứng dụng được liệt kê.
   - Ngoài các ứng dụng được liệt kê, bạn cũng phải cho phép truy cập các dịch vụ cần thiết, chẳng hạn như chứng thực và truy vấn DNS.
2. Cấu hình NAP để hỗ trợ các mục tiêu sau đây:
   - Giúp ngăn chặn sự lây lan của phần mềm độc hại.
   - Đảm bảo rằng chỉ có các máy tính có bật Windows Firewall, Windows Update, và có cài đặt phần mềm chống malware mới có thể kết nối với các máy tính của bộ phận nghiên cứu.
   - Tự động bật Windows Firewall, Windows Update đối với các máy tính không có bật Windows Firewall, Windows Update.

IV. Thực hành:

Thời gian thực hành: 75 phút

Bài tập 1: Cấu hình Windows Firewall

❖ **Mô hình thực hành gồm các máy:**

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1** **20413C-LON-CL1**
User Name	Adatum\Administrator
Password	Pa$$w0rd

❖ **Chuẩn bị:**

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiên lại từ bước 2 đến 4 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-CL1.**

❖ **Bài thực hành bao gồm các bước:**

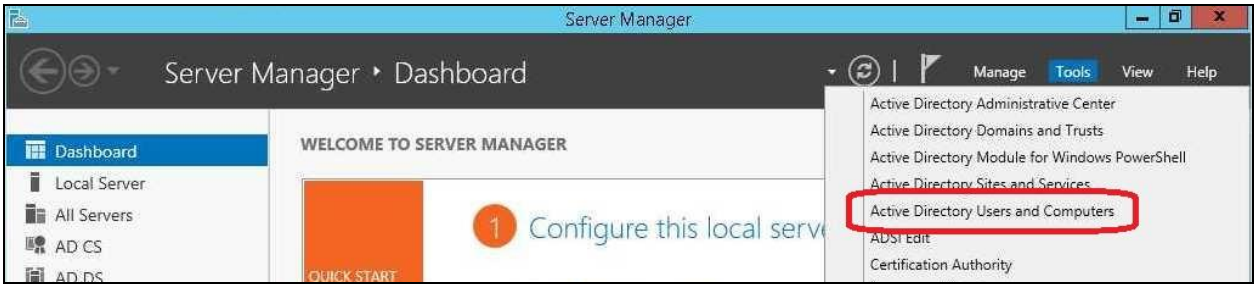
1. Chuyển Computer Account vào OU Research.
2. Tạo GPO và liên kết vào OU Research.
3. Tạo Connection Security Rule.
4. Tạo Firewall Rules.
5. Cập nhật cấu hình Group Policy.
6. Truy cập vào Web Server
7. Kiểm tra

❖ **Thực hiện:**

Bước 1. Chuyển Computer Account vào OU Research.

1. Logon vào máy **LON-DC1**.

2. Mở **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**.



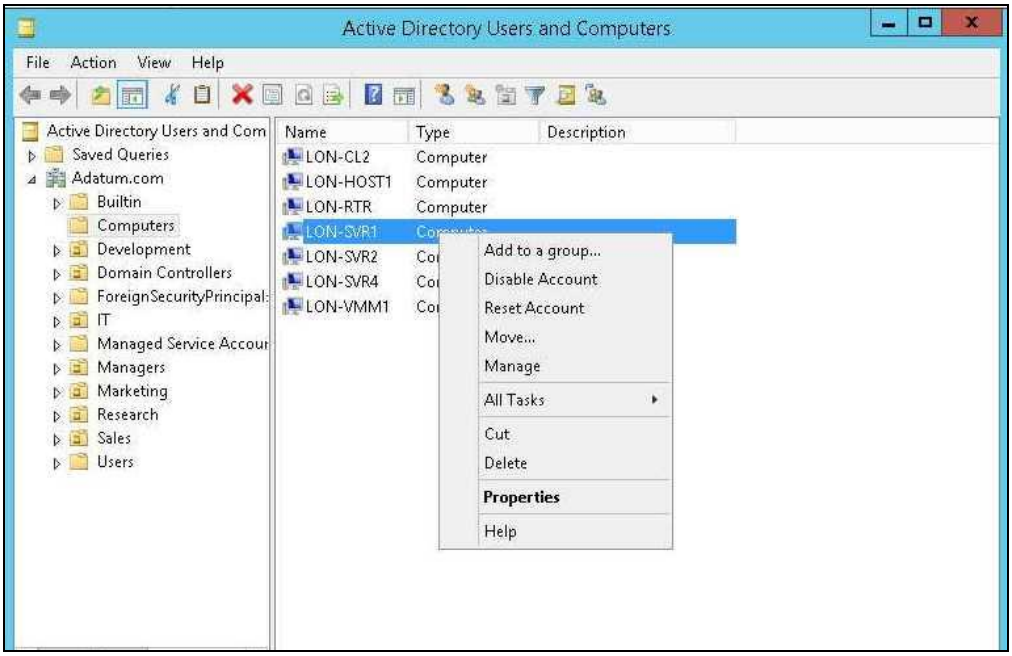
3. Trong cửa sổ **Active Directory Users and Computers**, bung **Adatum.com**, chọn **Computers**. Nhấn chuột phải **LON-CL1**, chọn **Move**.



4. Hộp thoại **Move**, chọn OU **Research**, và chọn **OK**.



5. Nhấn chuột phải **LON-SVR1**, chọn **Move**.

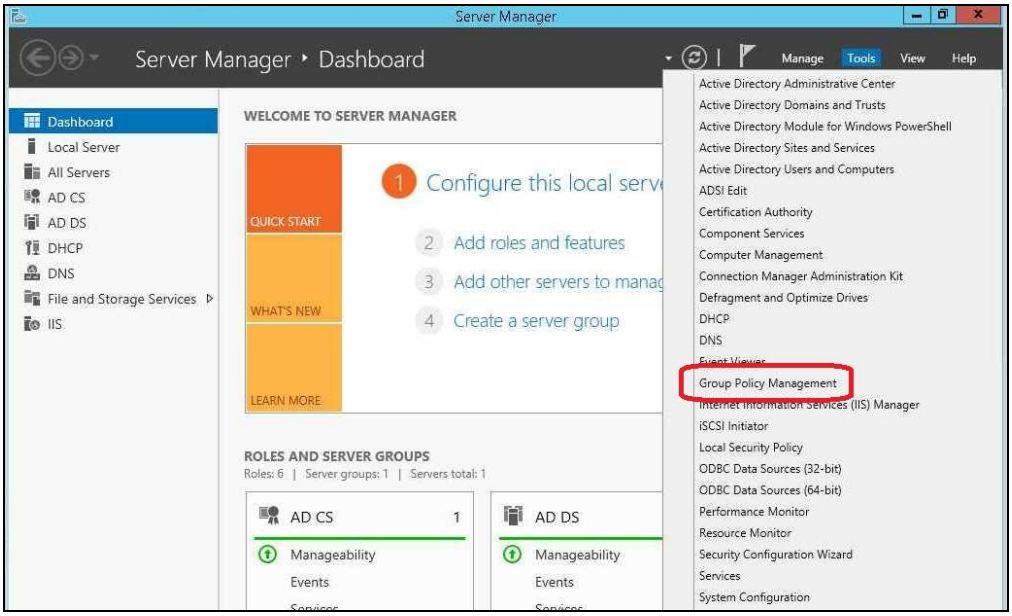


6. Hộp thoại **Move**, chọn OU **Research**, và chọn **OK**.

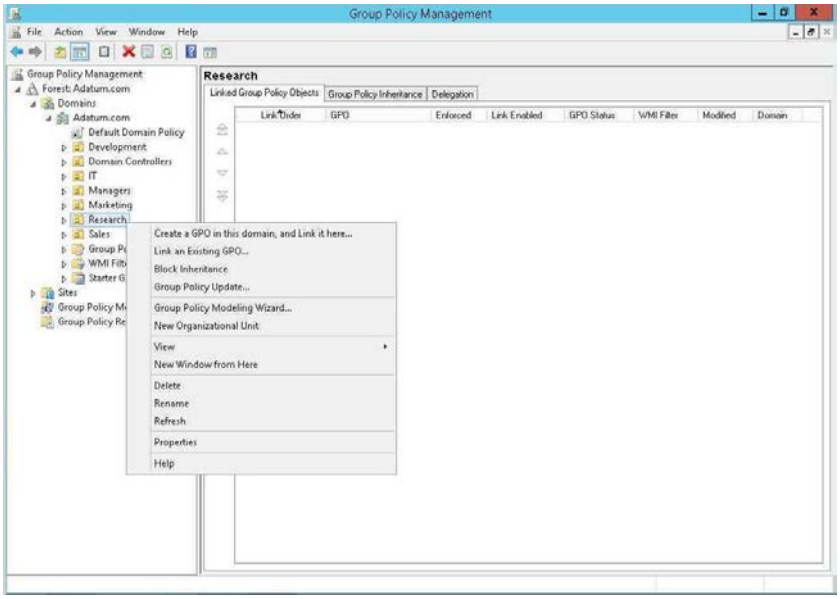


Bước 2. Tạo GPO và liên kết vào OU Research.

1. Quay lại cửa sổ **Server Manager**, bung menu **Tools**, mở **Group Policy Management**.



2. Trong cửa sổ **Group Policy Management**, bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, nhấn chuột phải OU **Research**, chọn **Create a GPO in this domain, and link it here**.

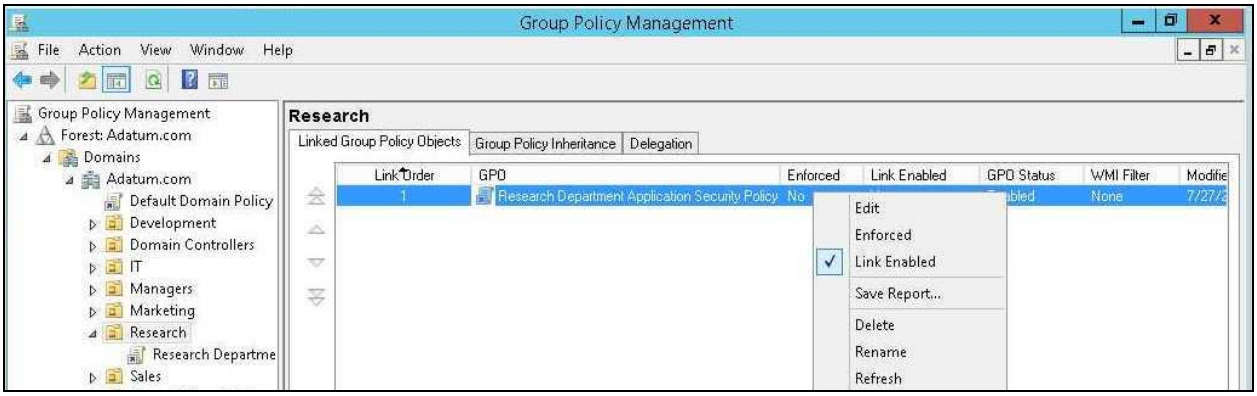


3. Hộp thoại **New GPO**, nhập **Research Department Application Security Policy** vào ô **Name**, và chọn **OK**.

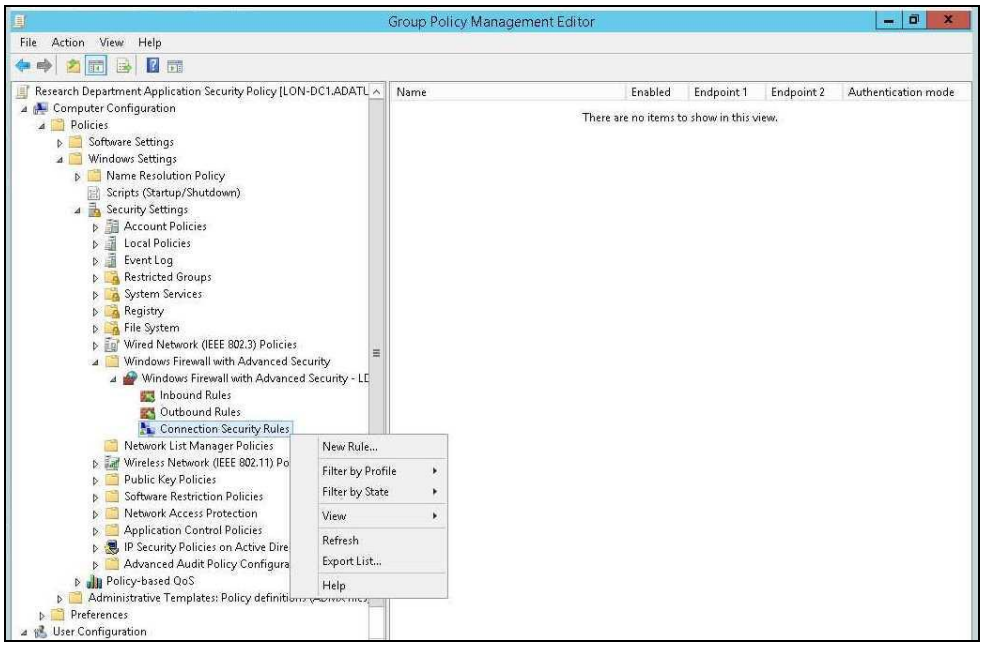


Bước 3. Tạo Connection Security Rule.

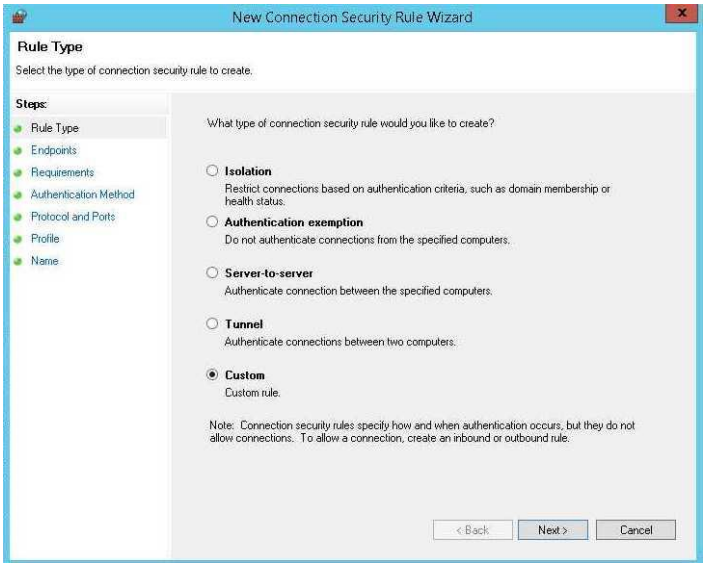
1. Trong cửa sổ **Group Policy Management**, bung OU **Research**. Nhấn chuột phải lên GPO **Research Department Application Security Policy**, chọn **Edit**.



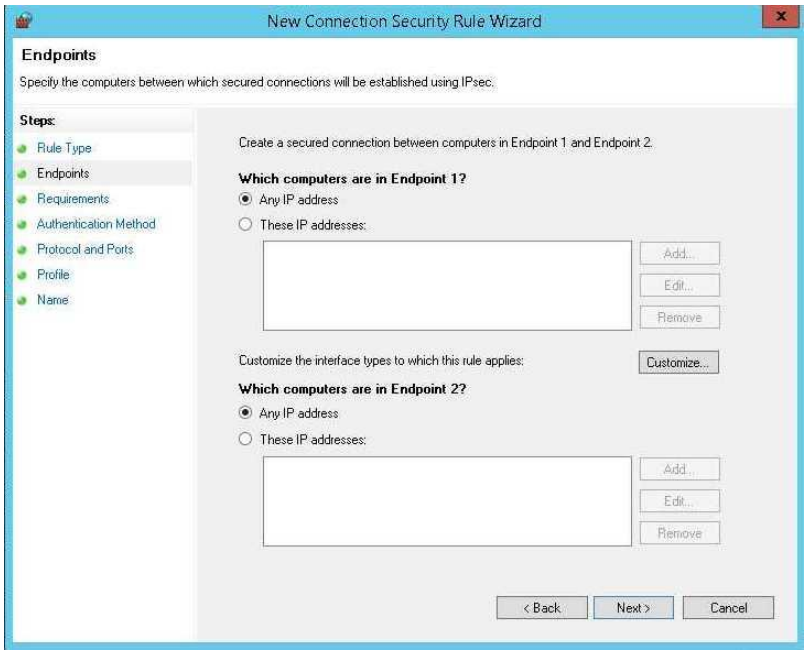
2. Cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Windows Firewall with Advanced Security**, bung **Windows Firewall with Advanced Security – LDAP://CN={GUID}**, nhấn chuột phải **Connection Security Rules**, chọn **New Rule**.



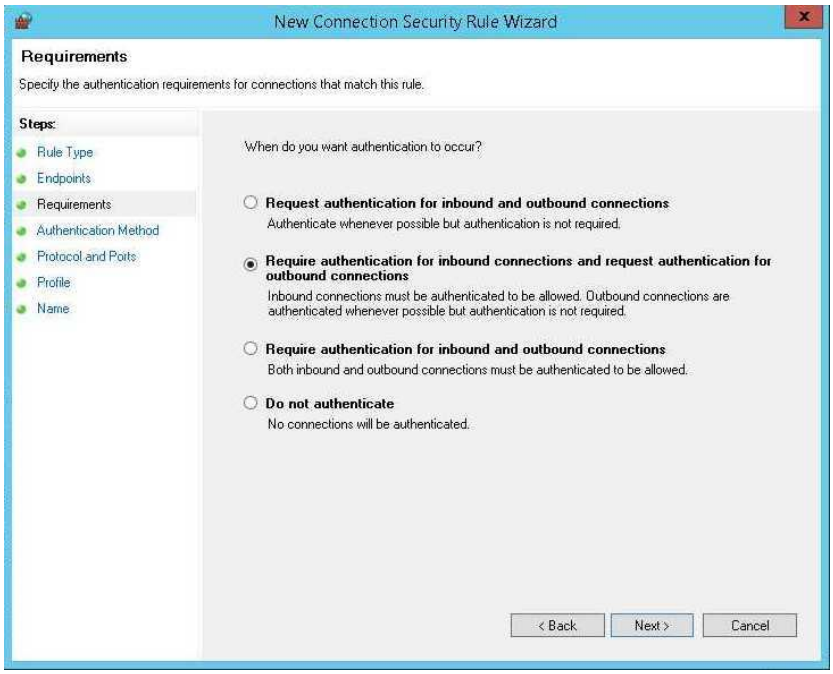
3. Cửa sổ **Rule Type**, chọn **Custom**, và chọn **Next**.



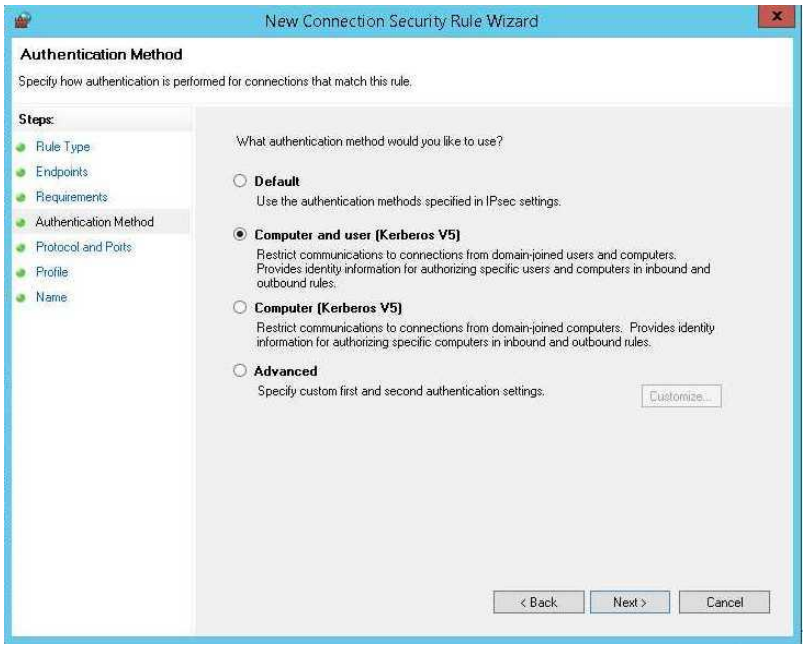
4. Cửa sổ **Endpoints**, chọn **Next**.



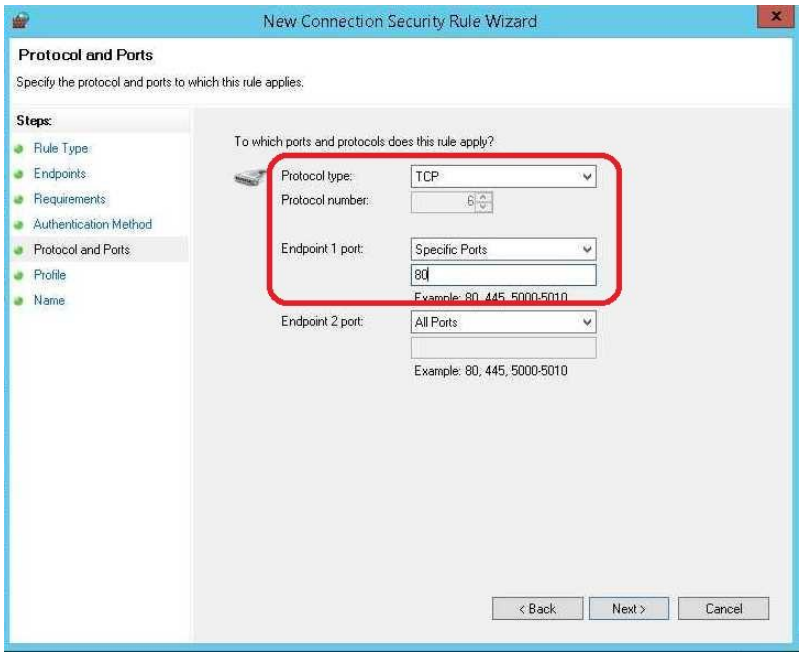
5. Cửa sổ **Requirements**, chọn **Require authentication for inbound connections and request authentication for outbound connections**, và chọn **Next**.



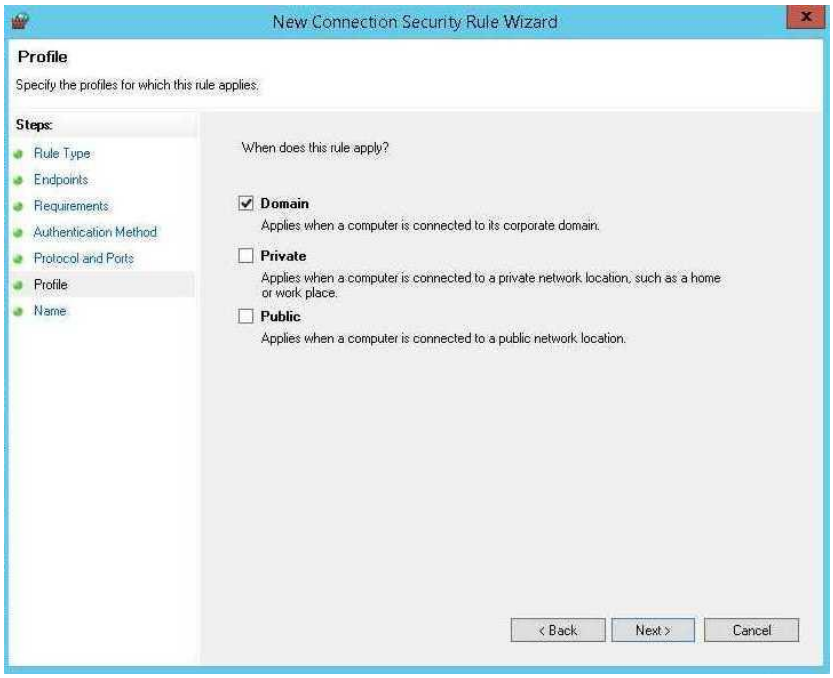
6. Cửa sổ **Authentication Method**, chọn **Computer and user (Kerberos V5)**, chọn **Next**.



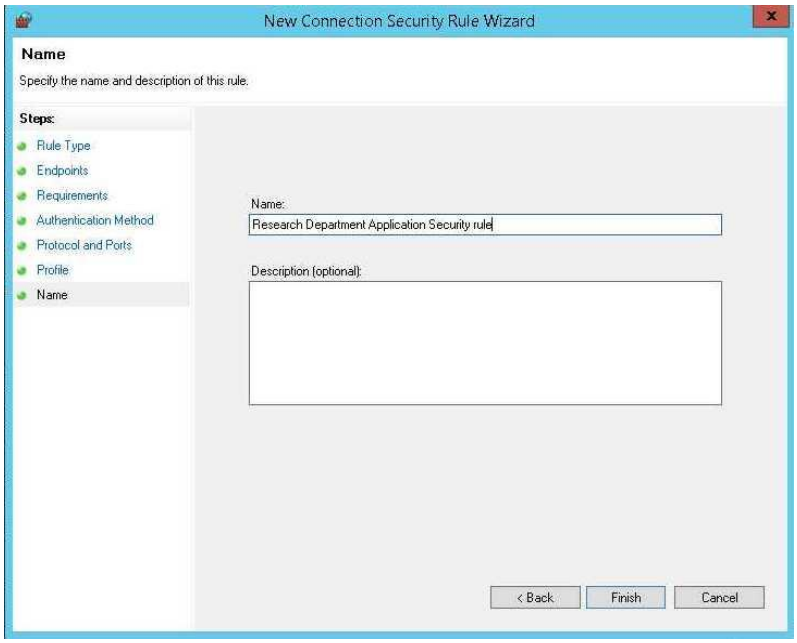
7. Cửa sổ **Protocol and Ports**, bung ô **Protocol type**, chọn **TCP**. Bung ô **Endpoint 1 port**, chọn **Specific Ports**, nhập **80**, chọn **Next**.



8. Cửa sổ **Profile**, bỏ dấu chọn ô **Private** và **Public**, chọn **Next**.

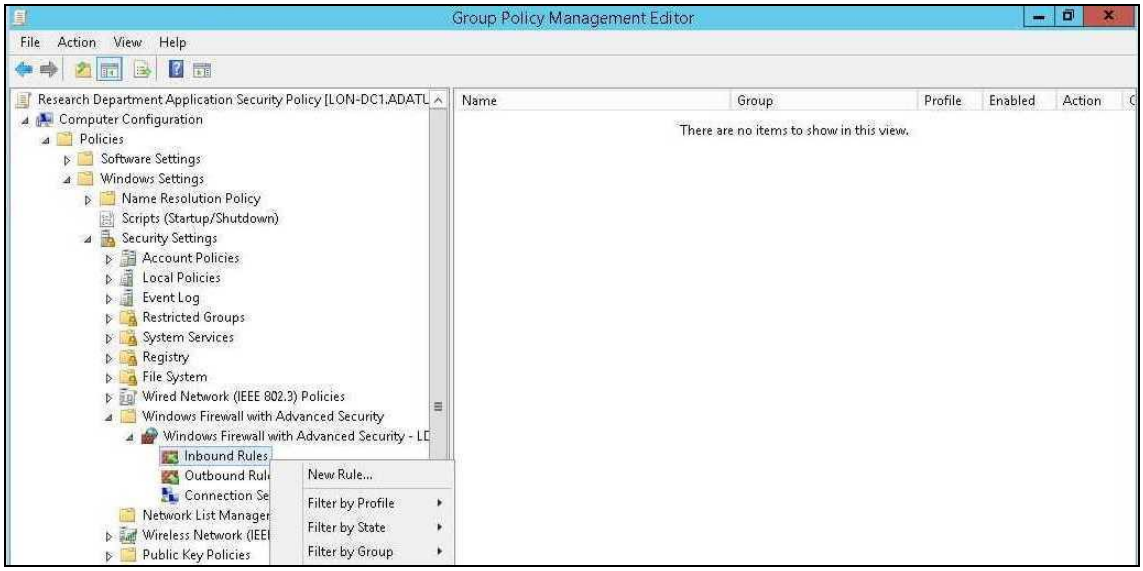


9. Cửa sổ **Name**, nhập **Research Department Application Security rule** vào ô **Name**, và chọn **Finish**.

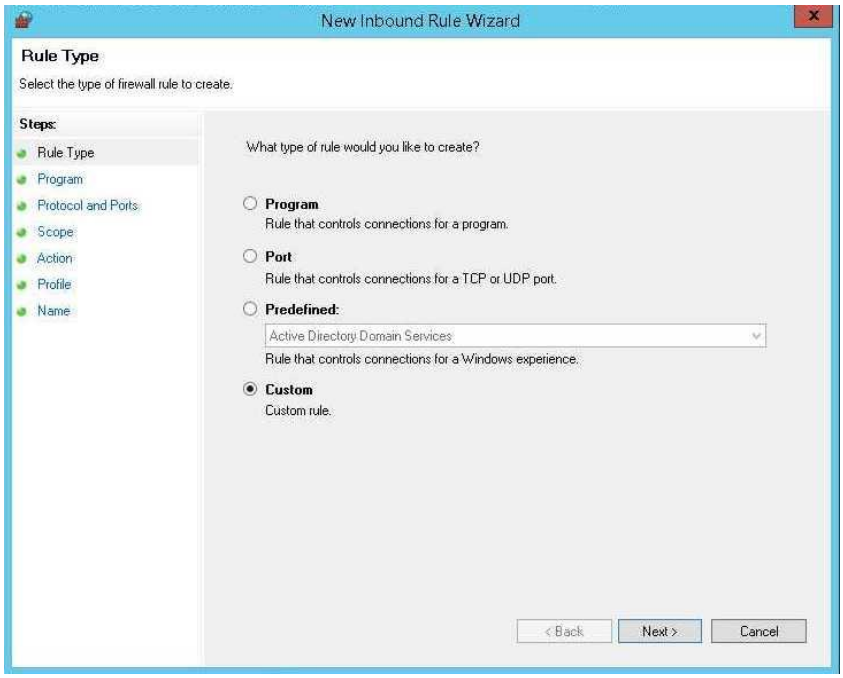


Bước 4. Tạo Firewall Rules.

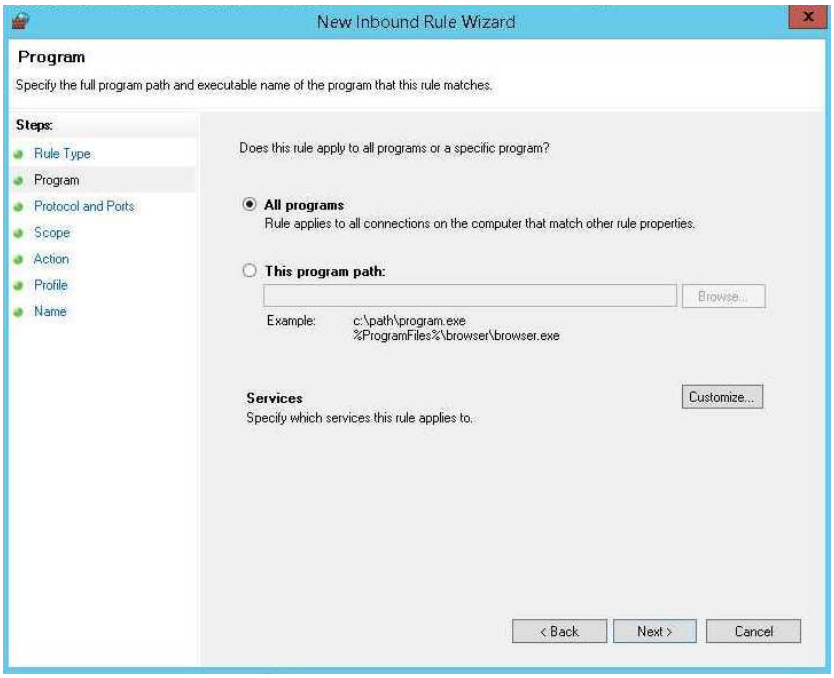
1. Trong cửa sổ **Group Policy Management Editor**, nhấn chuột phải **Inbound Rules**, chọn **New Rule**.



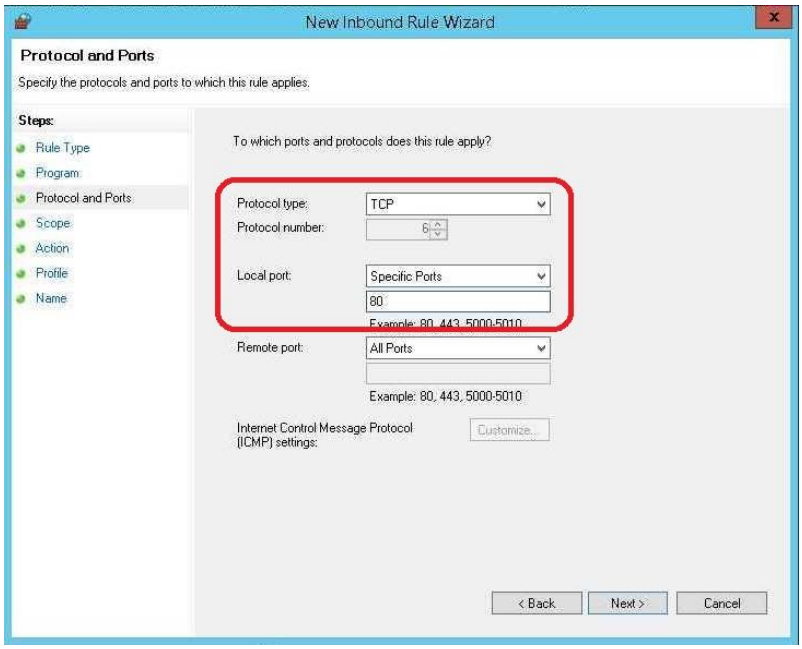
2. Cửa sổ **Rule Type**, chọn **Custom**, và chọn **Next**.



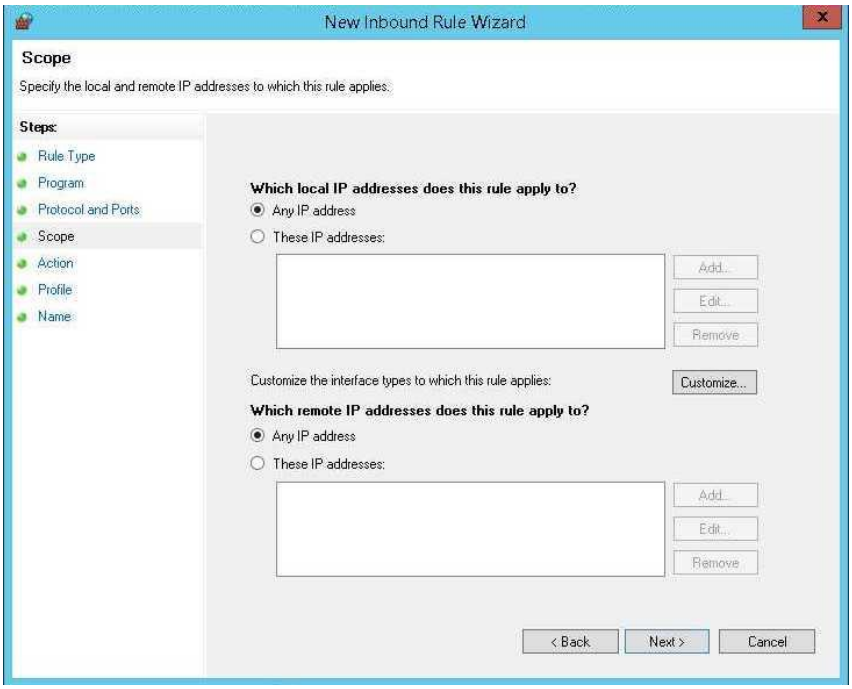
3. Cửa sổ **Program**, chọn **Next**.



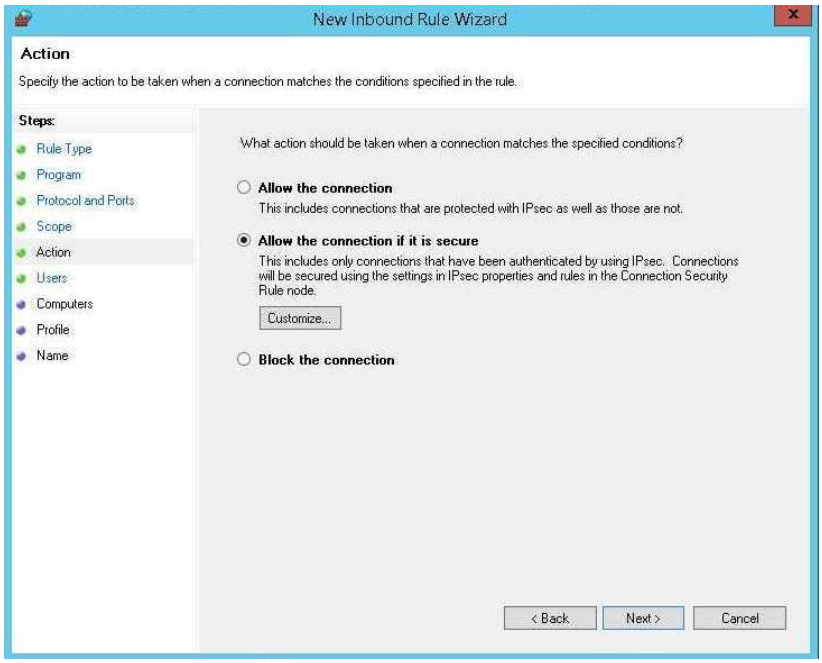
4. Cửa sổ **Protocol and Ports**, bung ô **Protocol type**, chọn **TCP**, bung ô **Local port**, chọn **Specific Ports**, nhập **80**, chọn **Next**.



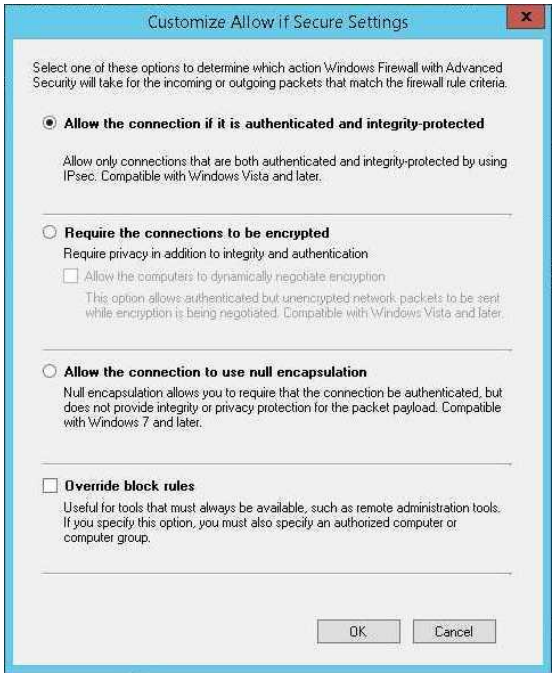
5. Cửa sổ **Scope**, chọn **Next**.



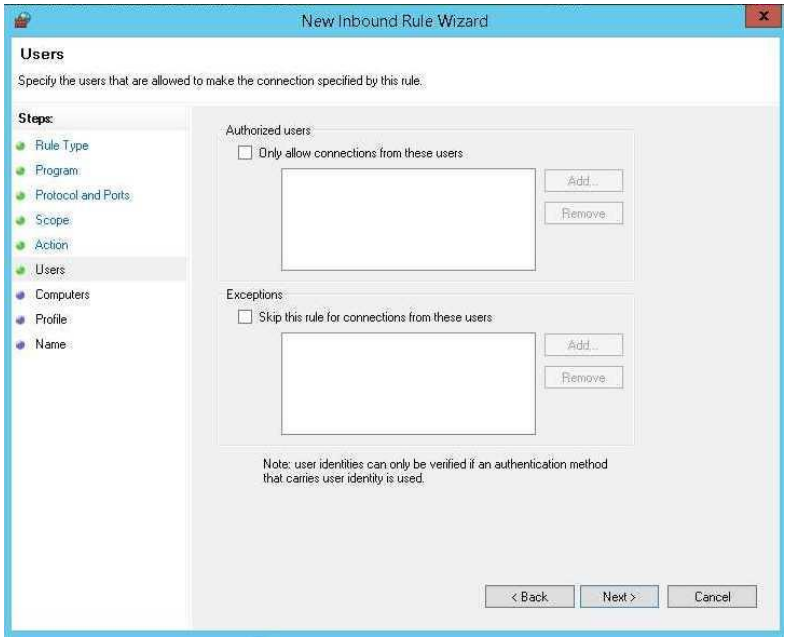
6. Cửa sổ **Action**, chọn **Allow the connection if it is secure**, chọn **Customize**.



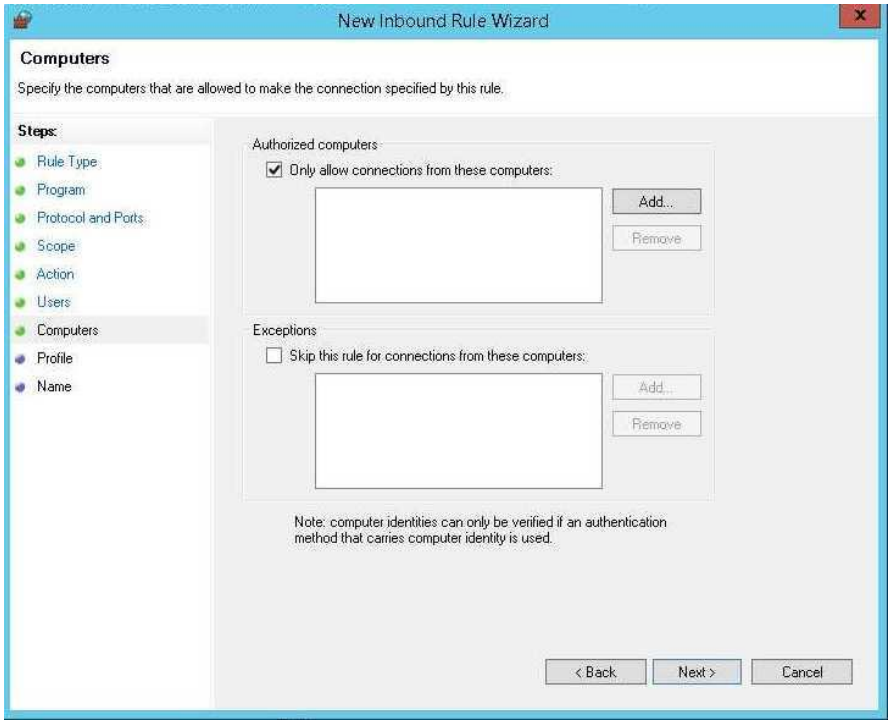
7. Trong hộp thoại Customize, chọn **Allow the connection if it is authenticated and integrity-protected**, chọn **OK**, và chọn **Next**.



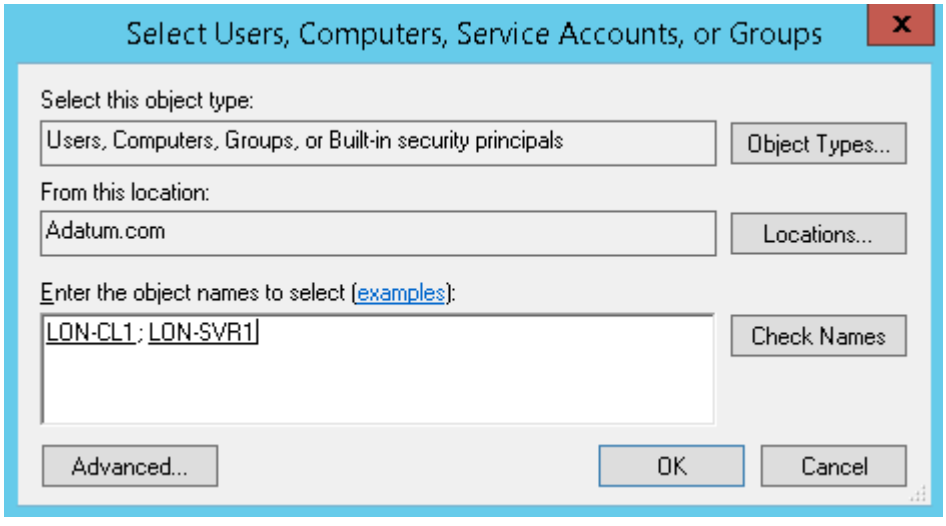
8. Cửa sổ **Users**, chọn **Next**.



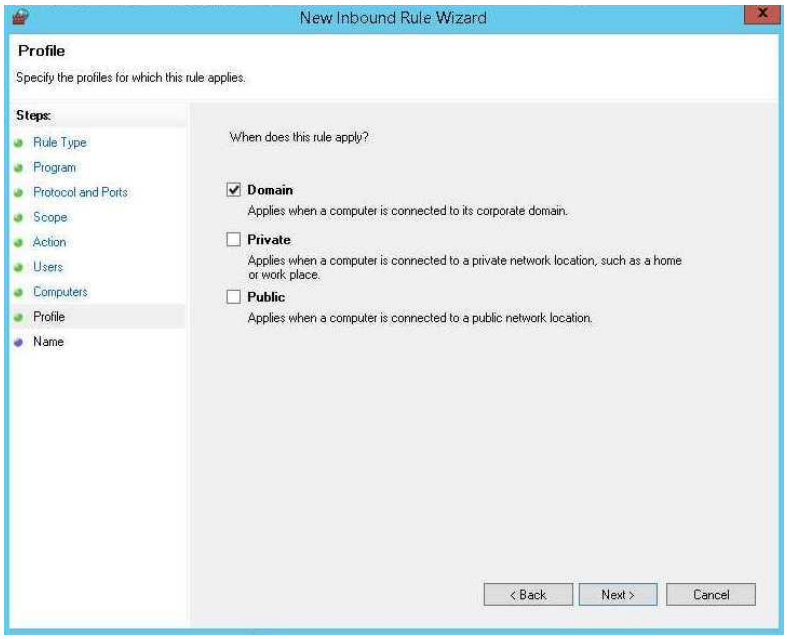
9. Cửa sổ **Computers**, đánh dấu chọn **Only allow connections from these computers**, và chọn **Add**.



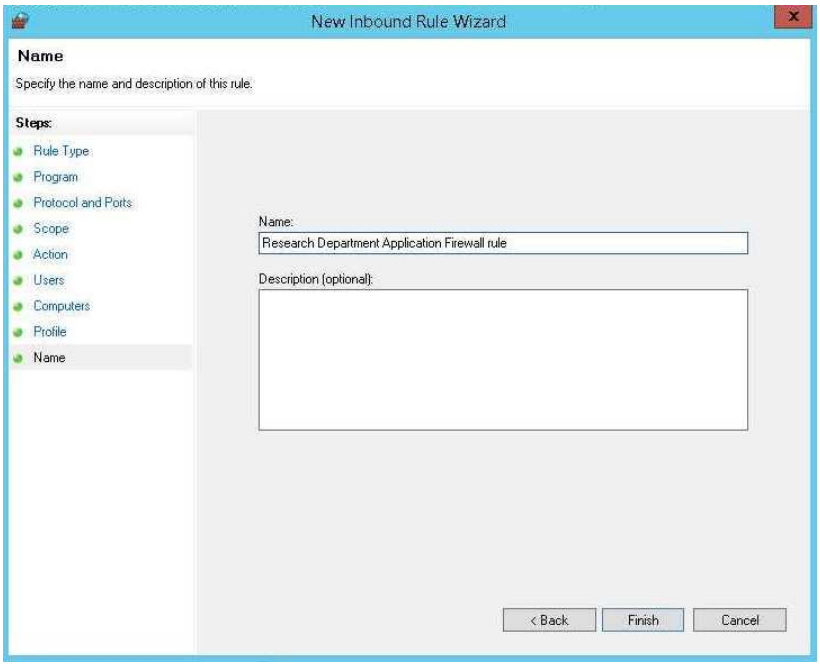
10. Hộp thoại **Select Computers, or Groups**, trong **Enter the object names to select (examples)**, nhập **LON-CL1; LON-SVR1**, chọn **Check Names**, chọn **OK**, và chọn **Next**.



11. Cửa sổ **Profile**, bỏ dấu chọn ô **Private** và **Public**, và chọn **Next**.



12. Cửa sổ **Name**, nhập **Research Department Application Firewall rule** vào ô **Name**, và chọn **Finish**.



Bước 5. Cập nhật cấu hình Group Policy.

1. Qua máy **LON-CL1**.

2. Bung **Start** menu, gõ **cmd.exe**, nhấn **Enter**.



3. Trong cửa sổ **Command Prompt**, gõ lệnh: **Gpupdate /force**

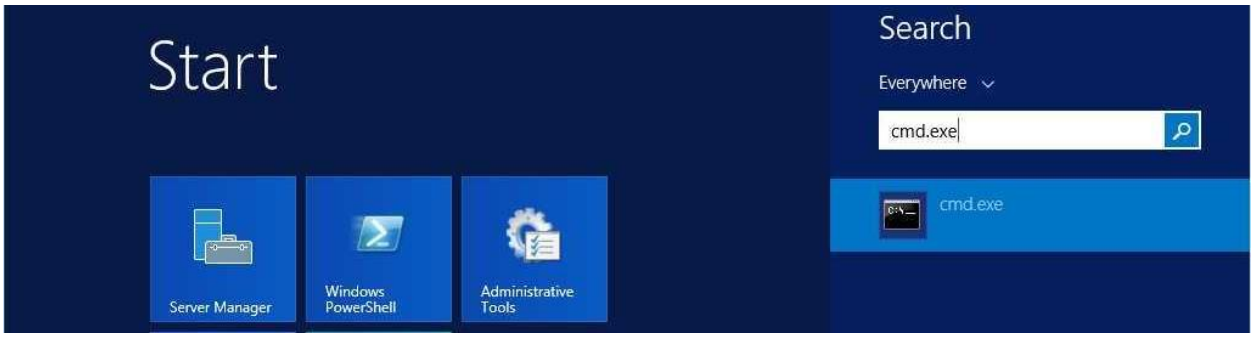


4. Trong cửa sổ **Command Prompt**, gõ lệnh: **Shutdown /r /t 0**



5. Qua máy **LON-SVR1**.

6. Bung **Start** menu, gõ **cmd.exe**, nhấn **Enter**.



7. Trong cửa sổ **Command Prompt**, gõ lệnh: **Gpupdate /force**



8. Trong cửa sổ **Command Prompt**, gõ lệnh: **Shutdown /r /t 0**

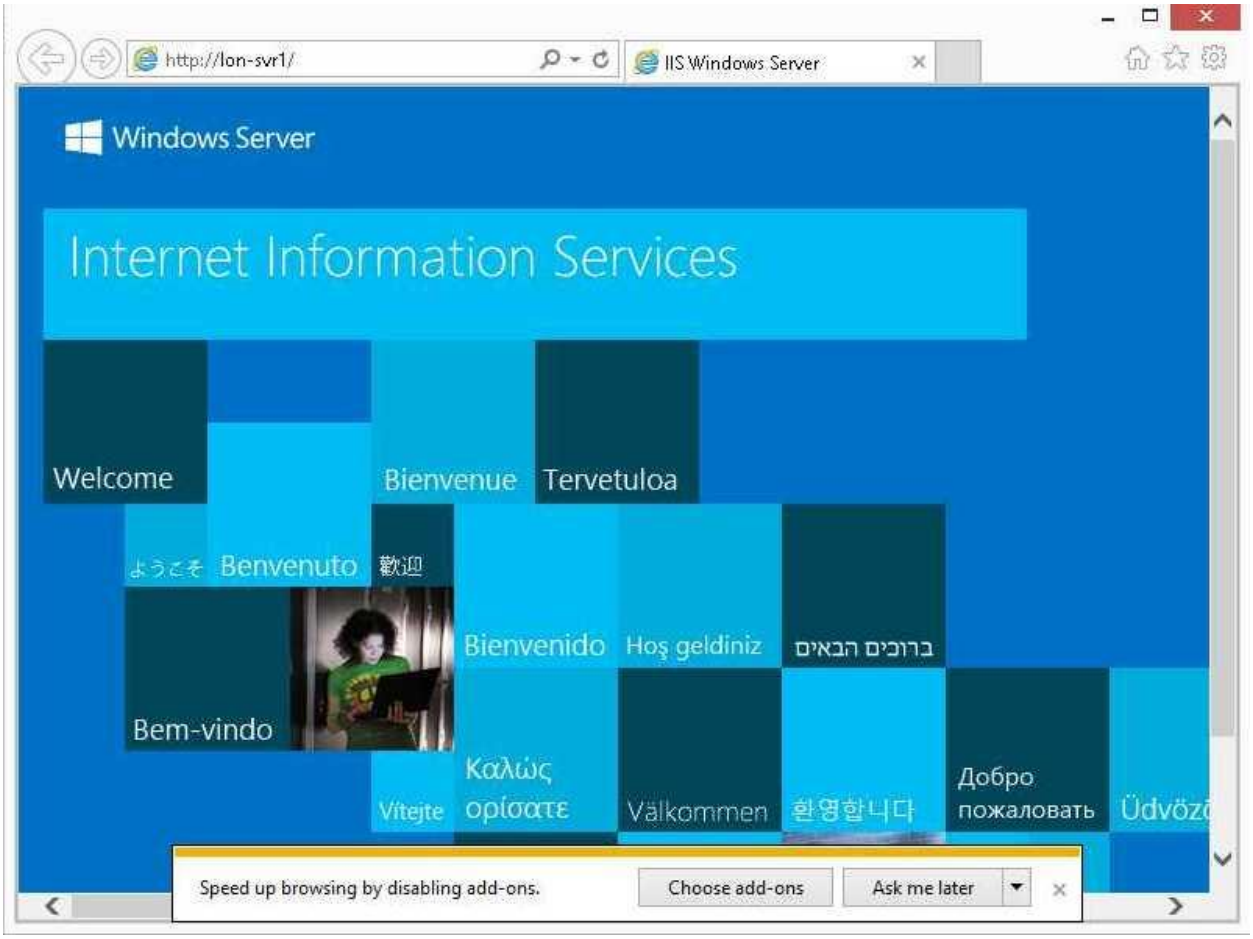


9. Sau khi khởi động thành công, logon **Adatum\Administrator** với password **Pa$$w0rd**.

Bước 6. Truy cập vào Web Server

1. Qua máy **LON-CL1**. logon **Adatum\Administrator** với password **Pa$$w0rd**.

2. Mở **Internet Explorer**, truy cập địa chỉ **http://LON-svr1**. Kiểm tra truy cập thành công vào giao diện web IIS 8.



Bước 7. Kiểm tra

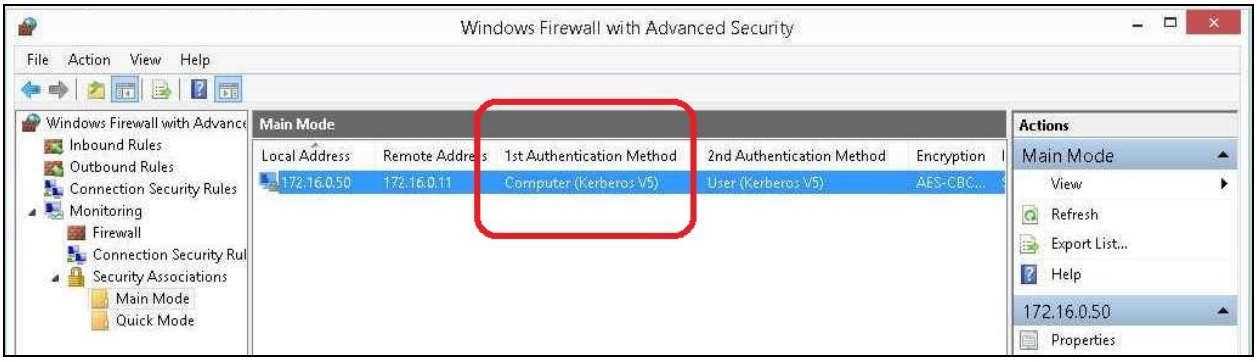
1. Trên **LON-CL1,** bung **Start** menu, gõ **Windows Firewall**, mở **Windows Firewall**.



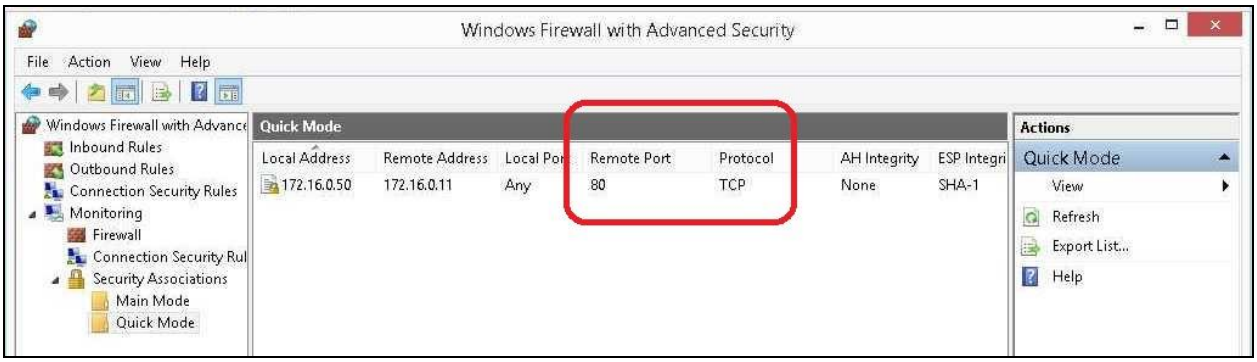
2. Trong cửa sổ **Windows Firewall**, chọn **Advanced settings**.



3. Cửa sổ **Windows Firewall with Advanced Security**, bung **Monitoring**, bung **Security Associations**, chọn **Main Mode**. Trong cửa sổ bên phải, kiểm tra **1st Authentication Method** là **Computer (Kerberos V5)**



4. Chọn **Quick Mode**. Trong cửa sổ bên phải, kiểm tra **Remote port** là 80



Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình các quy tắc tường lửa theo yêu cầu của A. Datum.

❖ **Chuẩn bị cho bài tiếp theo:**

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-LON-SVR1** và **20413C-LON-CL1.**

Bài tập 2: Cấu hình NAP-IPsec

❖ **Mô hình thực hành gồm các máy:**

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR2** **20413C-LON-CL1**
User Name	Adatum\Administrator
Password	Pa$$w0rd

❖ **Chuẩn bị:**

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiên từ bước 2 đến 4 cho máy ảo **20413C-LON-SVR2** và **20413C-LON-CL1.**

❖ **Bài thực hành bao gồm các bước:**

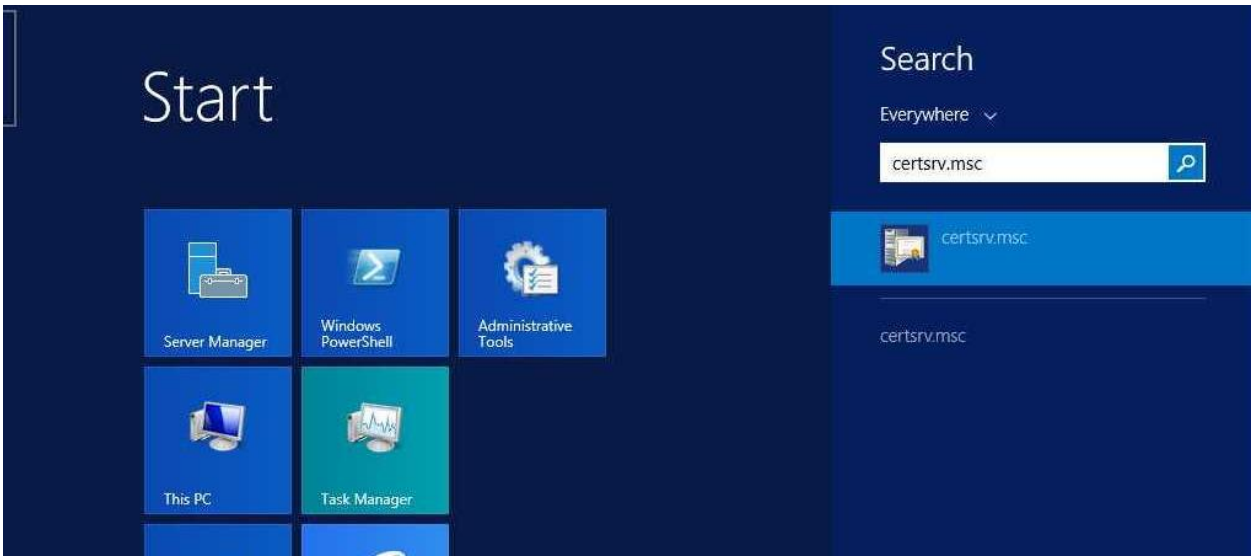
1. Tạo NAP Health Compliance certificate.
2. Cài đặt Network Policy and Access Services role trên LON-SVR2.
3. Cấu hình Health Registration Authority (HRA).
4. Cấu hình Health Policy.
5. Cấu hình Health Validator.
6. Tạo GPO để thiết lập cấu hình NAP client.
7. Kiểm tra Client đã ảnh hưởng GPO.
8. Kiểm tra Client tuân thủ chính sách an toàn.

Thực hiện:

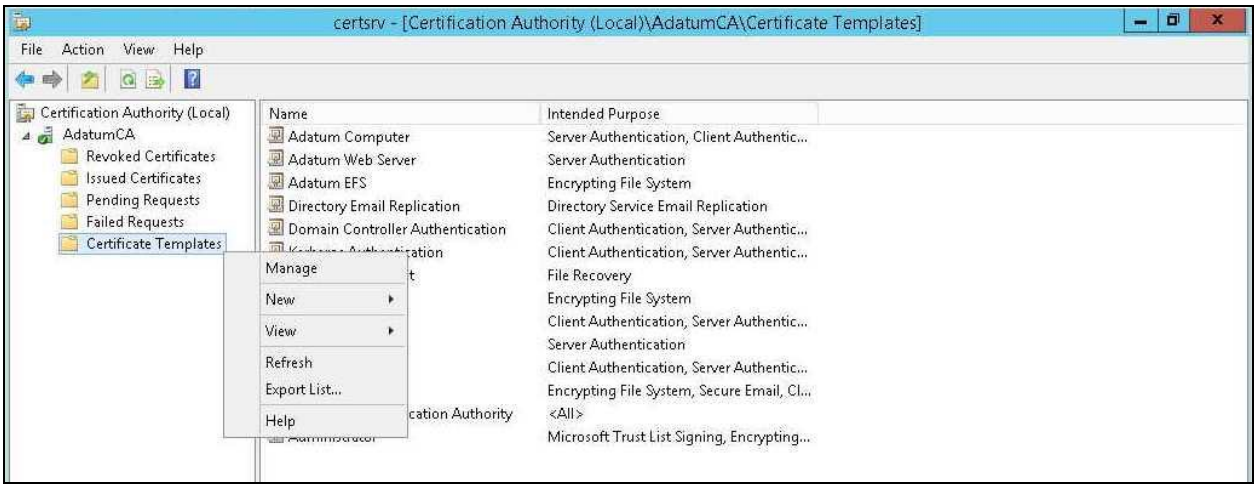
Bước 1. Tạo NAP Health Compliance certificate.

1. Logon máy **LON-DC1**.

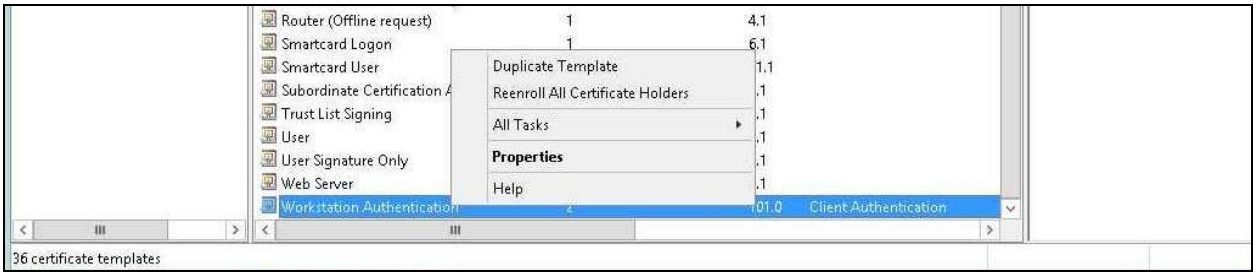
2. Bung Start, gõ **certsrv.msc**, nhấn **Enter**.



3. Trong cửa sổ **Certification Authority**, bung **AdatumCA,** nhấn chuột phải **Certificate Templates**, chọn **Manage**.



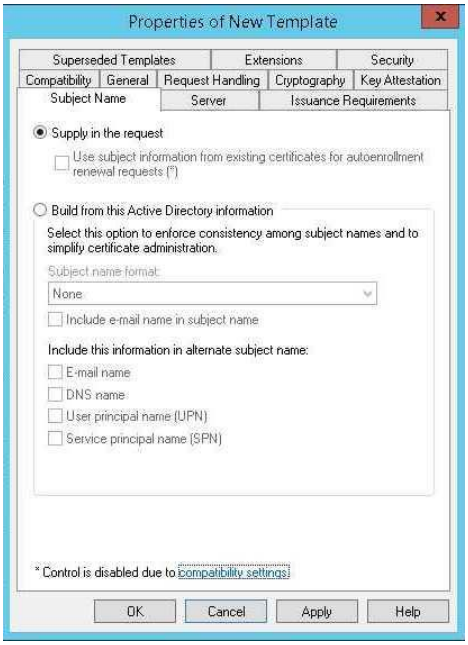
4. Trong cửa sổ **Certificate Templates**, nhấn chuột phải **Workstation Authentication**, chọn **Duplicate Template**.



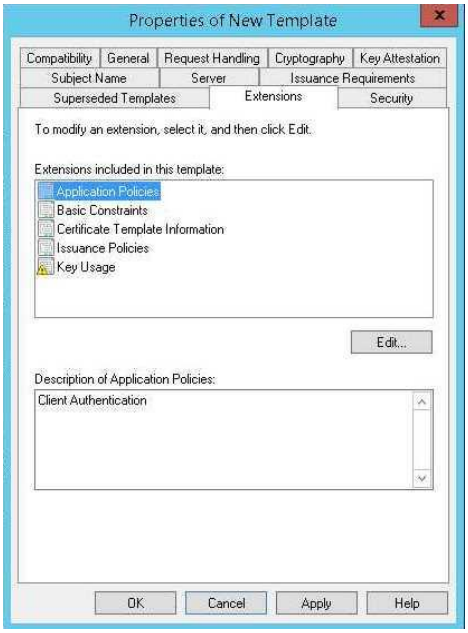
5. Trong hộp thoại **Properties of New Template,** qua tab **General**, trong ô **Template display name**, nhập **NAP Health Certificate**.



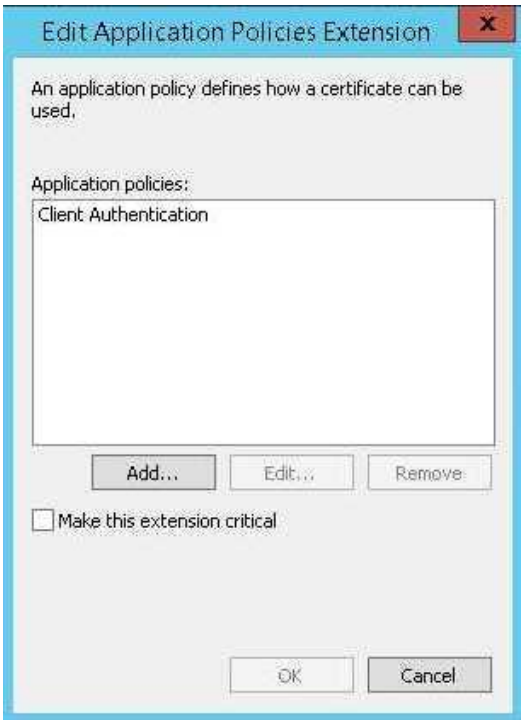
6. Qua tab **Subject Name**, chọn **Supply in the request**, hộp thoại **Certificate Templates warning**, chọn **OK**.



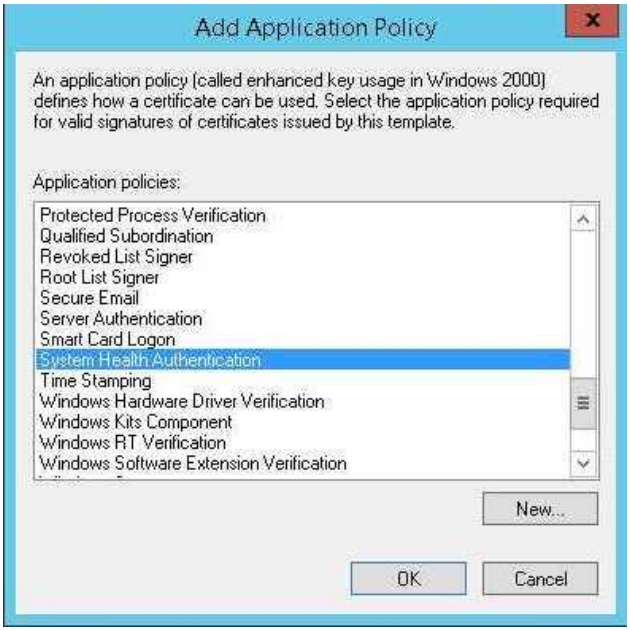
7. Qua tab**Extensions**, chọn **Application Policies**, và chọn **Edit**.



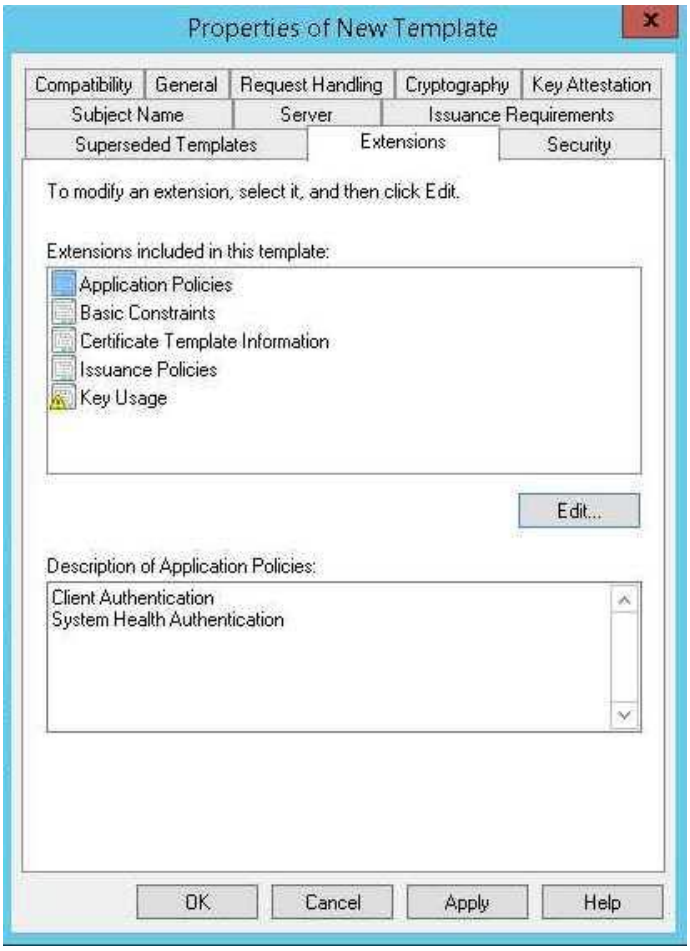
8. Trong hộp thoại **Edit Application Policies Extension**, chọn **Add**.



9. Hộp thoại **Add Application Policy**, chọn **System Health Authentication**, chọn **OK** 2 lần.

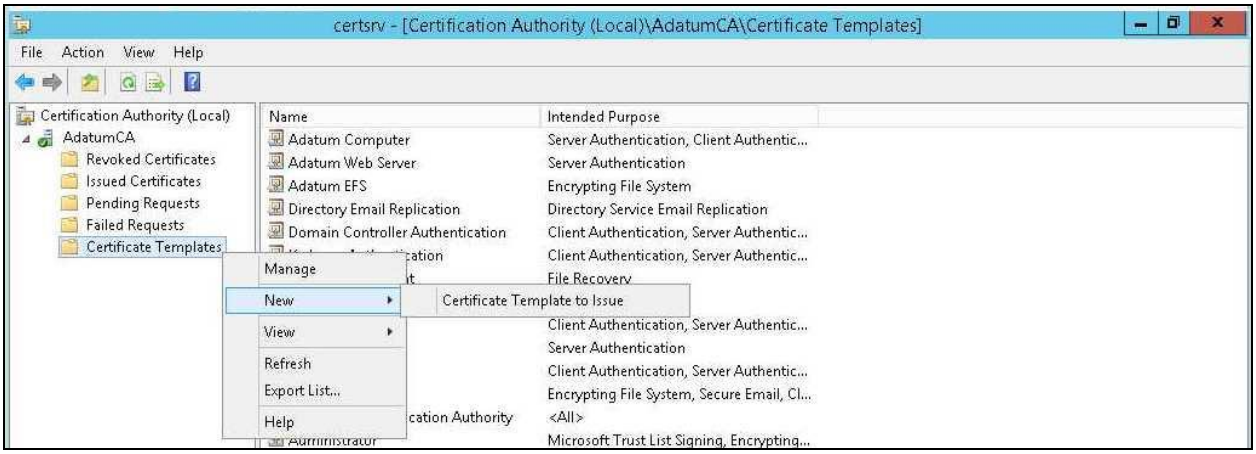


10. Hộp thoại **Properties of New Template**, chọn **OK**.

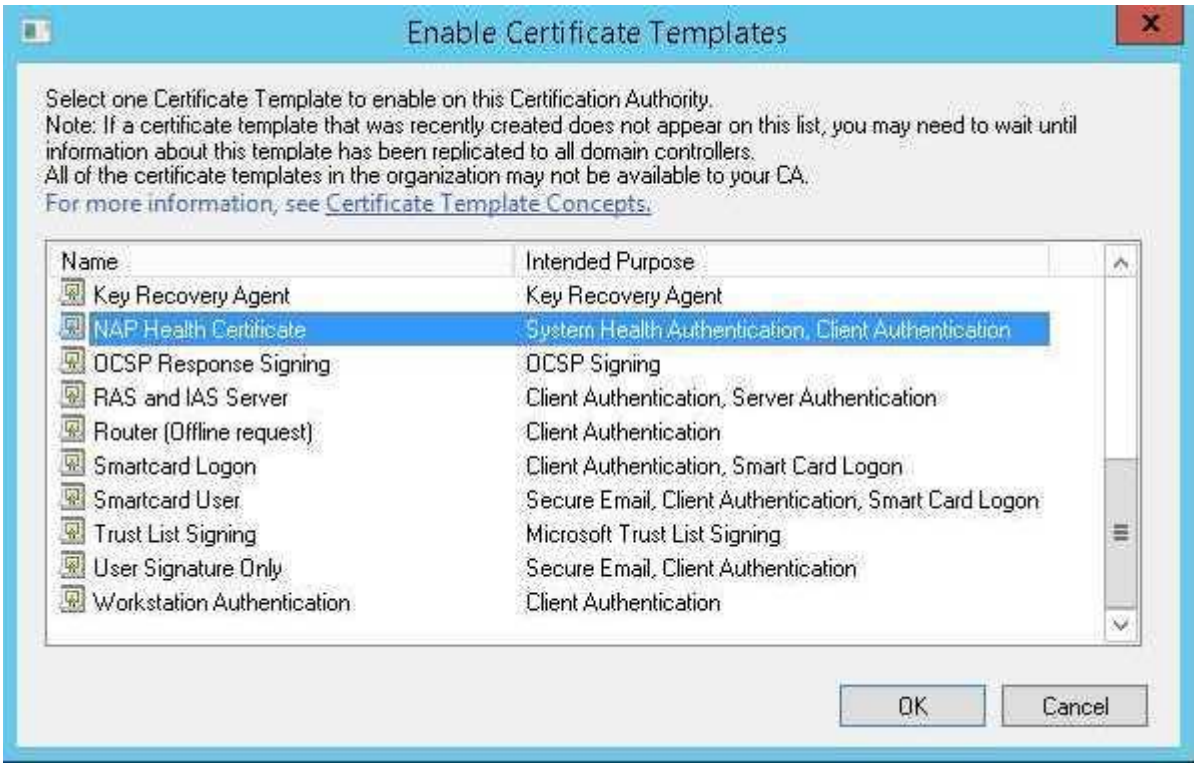


11. Tắt cửa sổ **Certificate Templates**.

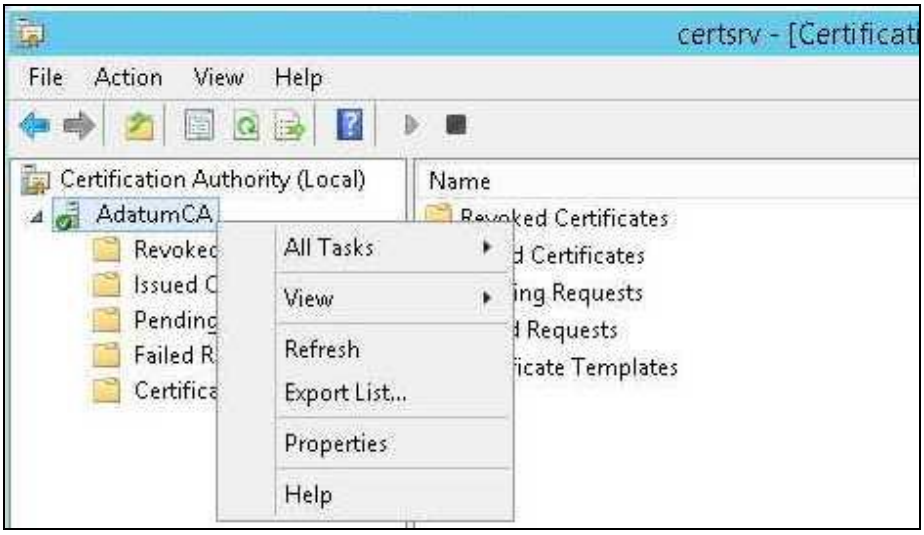
12. Trong cửa sổ **Certification Authority**, nhấn chuột phải **Certificate Templates**, chọn **New**, và chọn **Certificate Template to Issue**.



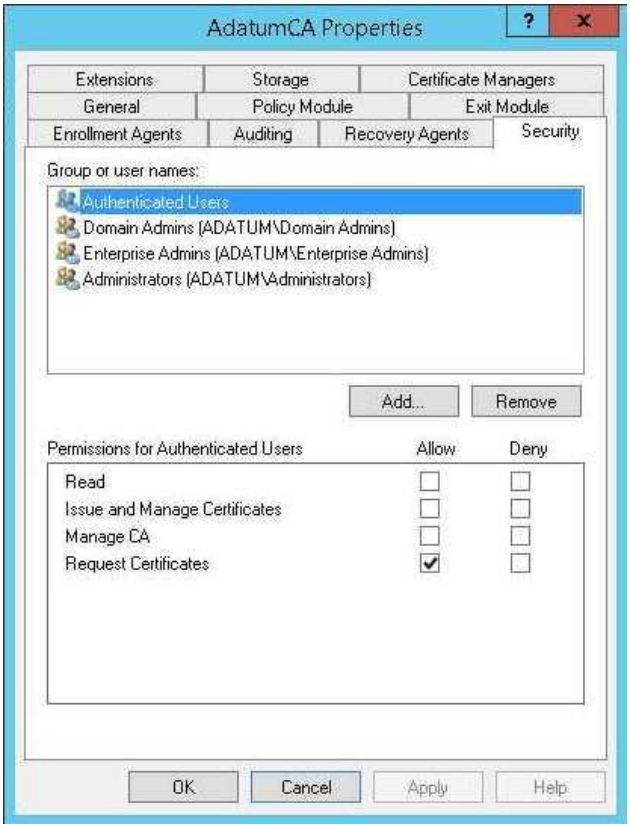
13. Chọn **NAP Health Certificate**, chọn **OK**.



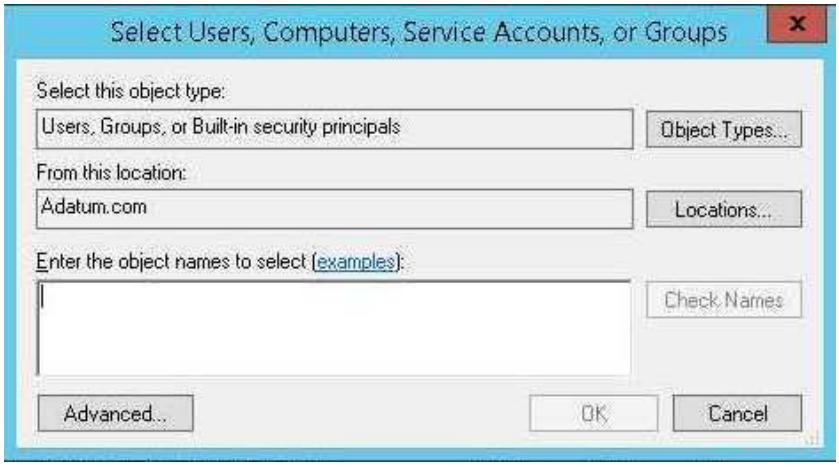
14. Cửa sổ **Certification Authority**, nhấn chuột phải **AdatumCA**, chọn **Properties**.



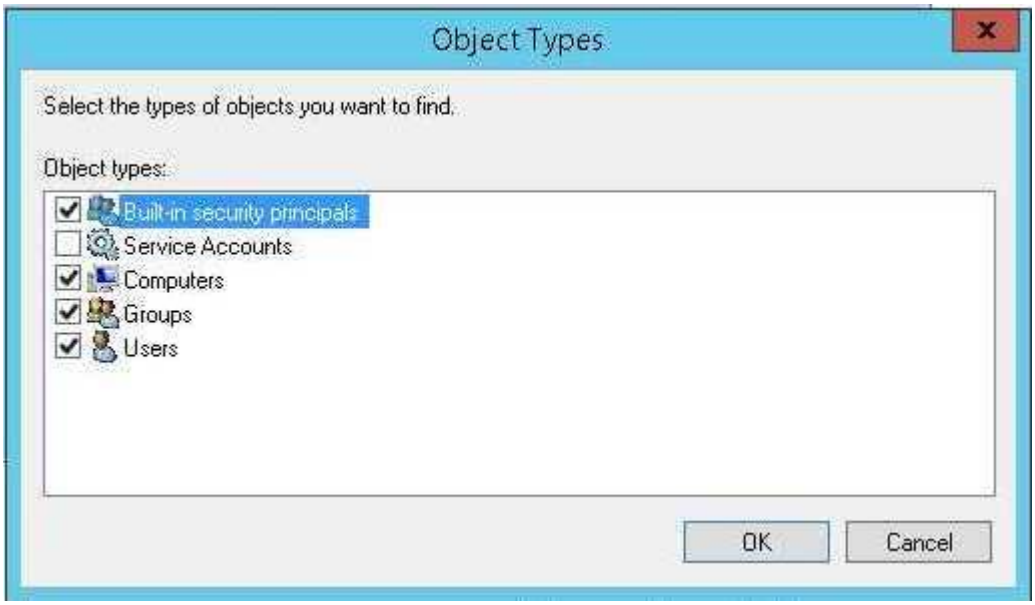
15. Trong hộp thoại **AdatumCA Properties**, qua tab **Security**, chọn **Add**.



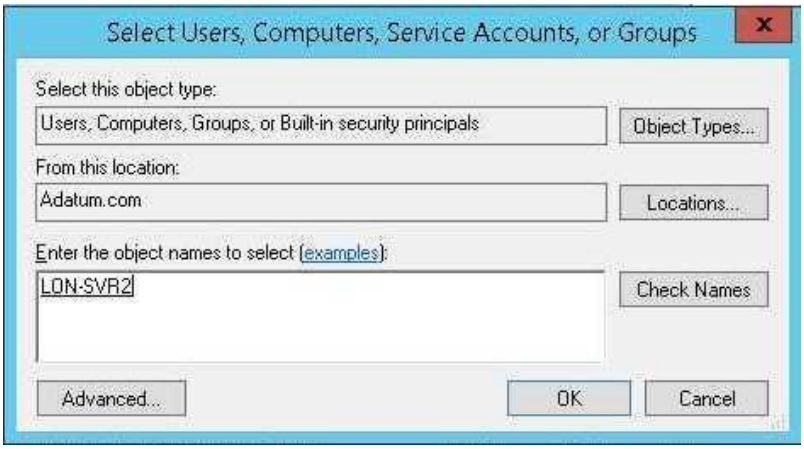
16. Hộp thoại **Select Users, Computers, Service Accounts, or Groups,** chọn **Object Types**.



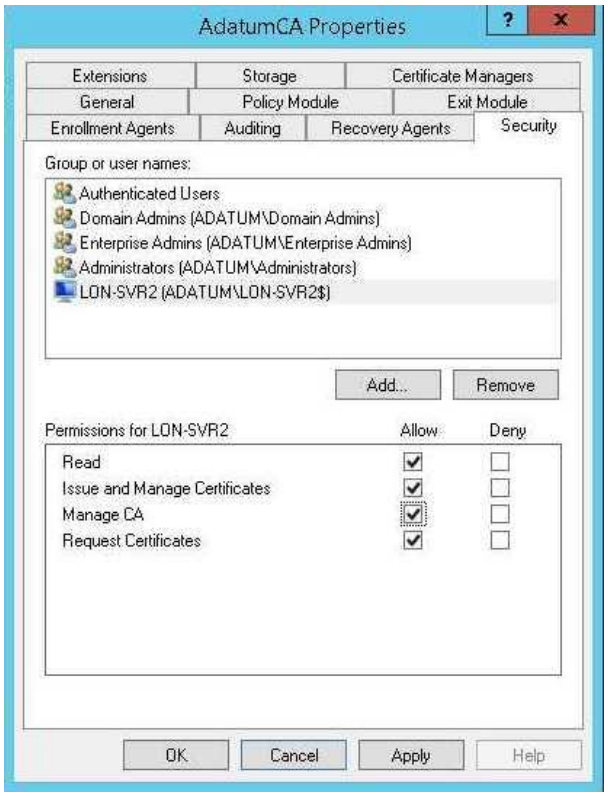
17. Hộp thoại Object Types, đánh dấu chọn **Computers**, và chọn **OK**.



18. Trong ô **Enter the object names to select**, nhập **LON-SVR2**, chọn Check Name, chọn **OK**.



19. Trong tab **Security**, chọn **LON-SVR2**, đánh dấu chọn **Read**, **Issue and Manage Certificates**, **Manage CA**, và **Request Certificates** ở cột **Allow**, và chọn **OK**.



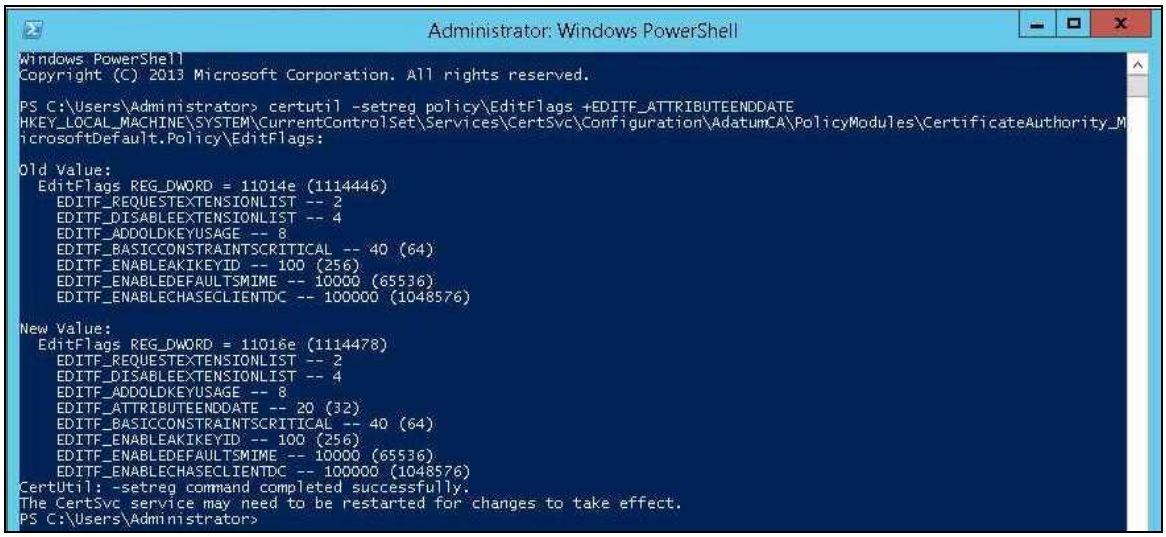
20. Tắt **Certification Authority**.

21. Trên Taskbar, nhấn chuột phải **Windows PowerShell**, chọn **Run as Administrator**.



22. Trong **Windows PowerShell**, gõ lệnh:

Certutil -setreg policy\EditFlags +EDITF_ATTRIBUTEENDDATE



23. Mở Command Prompt, gõ lệnh: **net stop certsvc**



24. Sau đó, gõ tiếp lệnh: **net start certsvc**



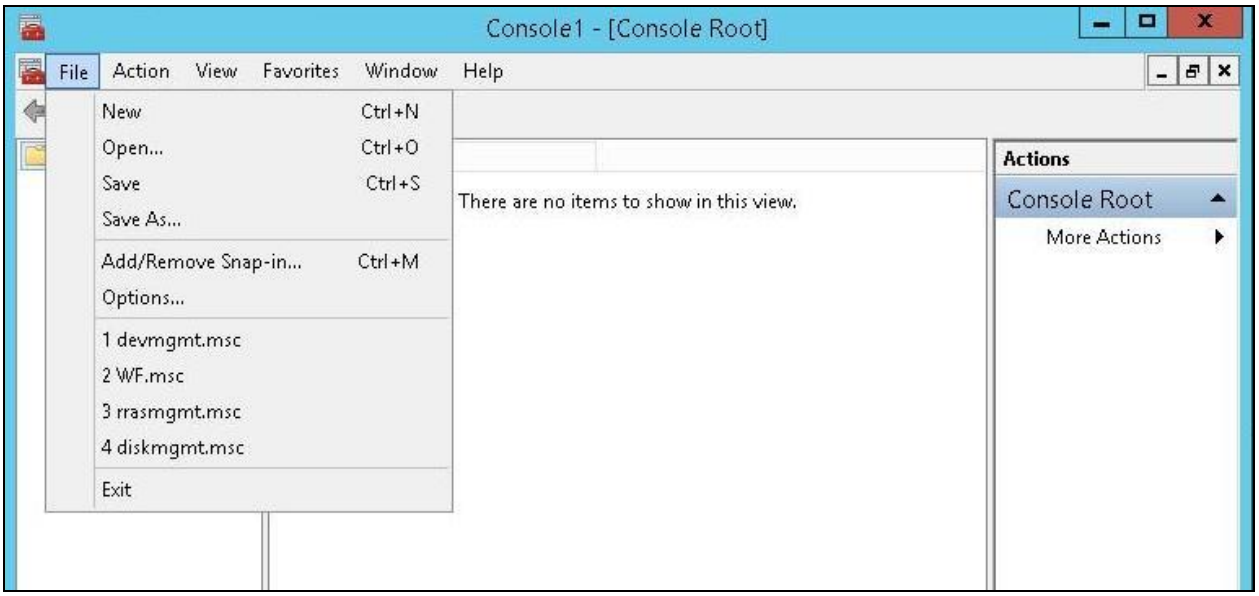
Bước 2. Cài đặt Network Policy and Access Services role trên LON-SVR2.

1. Qua máy **LON-SVR2**.

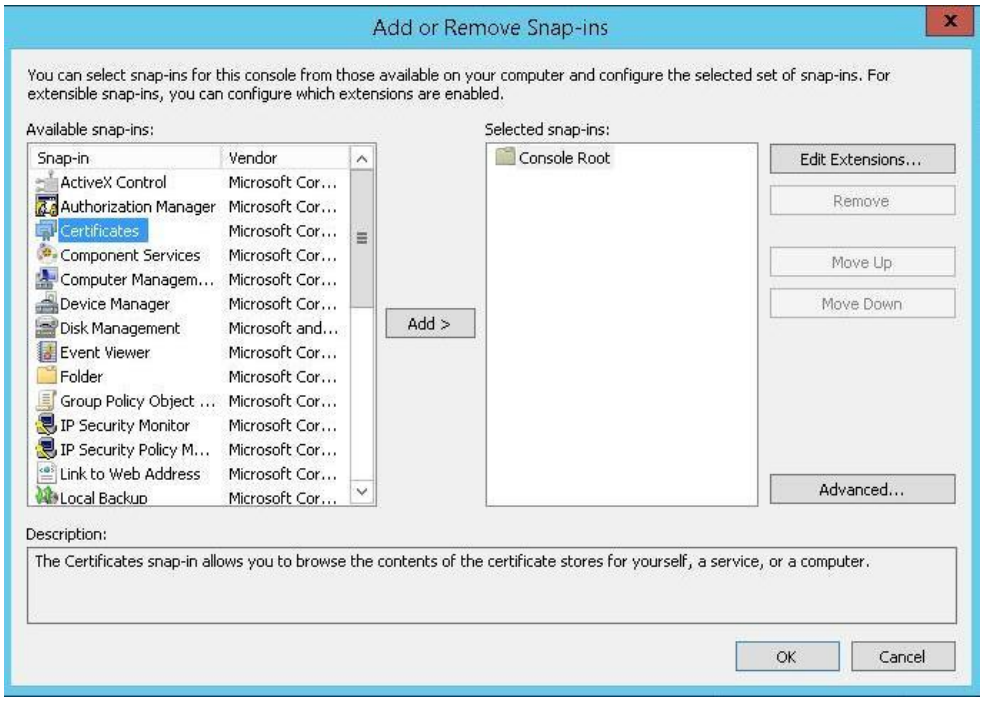
2. Bung **Start** menu, gõ **mmc.exe**, nhấn **Enter**.



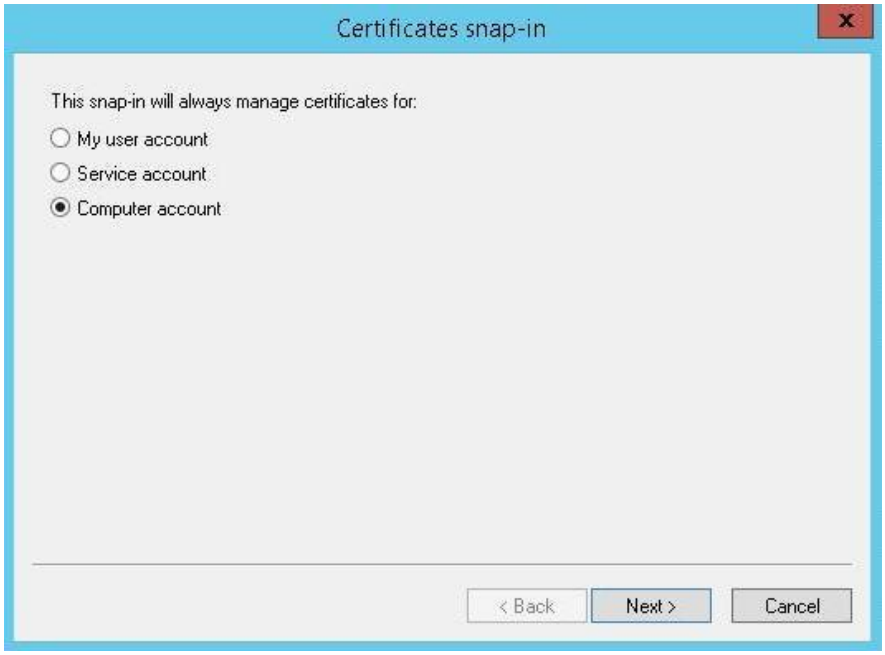
3. Bung menu **File**, chọn **Add/Remove Snap-in**.



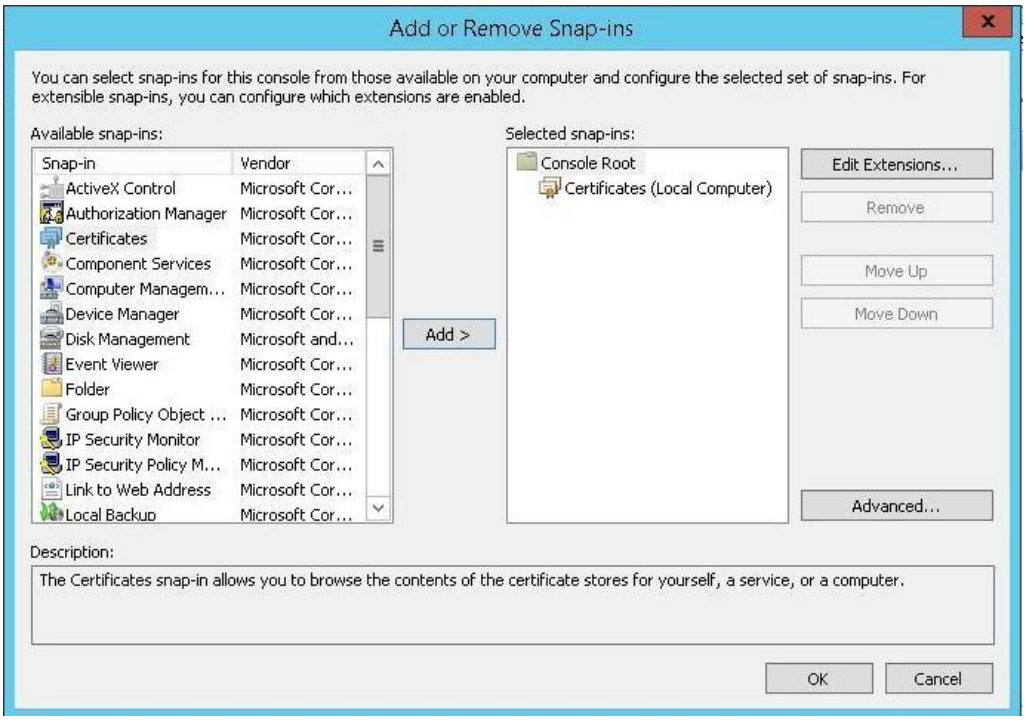
4. Trong hộp thoại **Add or Remove Snap-ins**, chọn **Certificates**, chọn A**dd**.



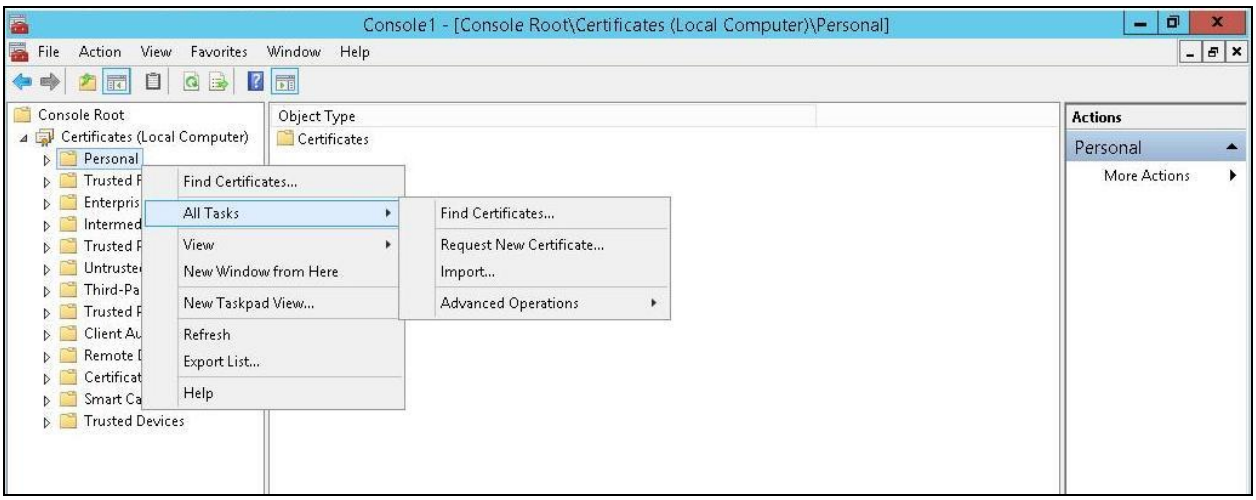
5. Chọn **Computer account**, chọn **Next**, và chọn **Finish**.



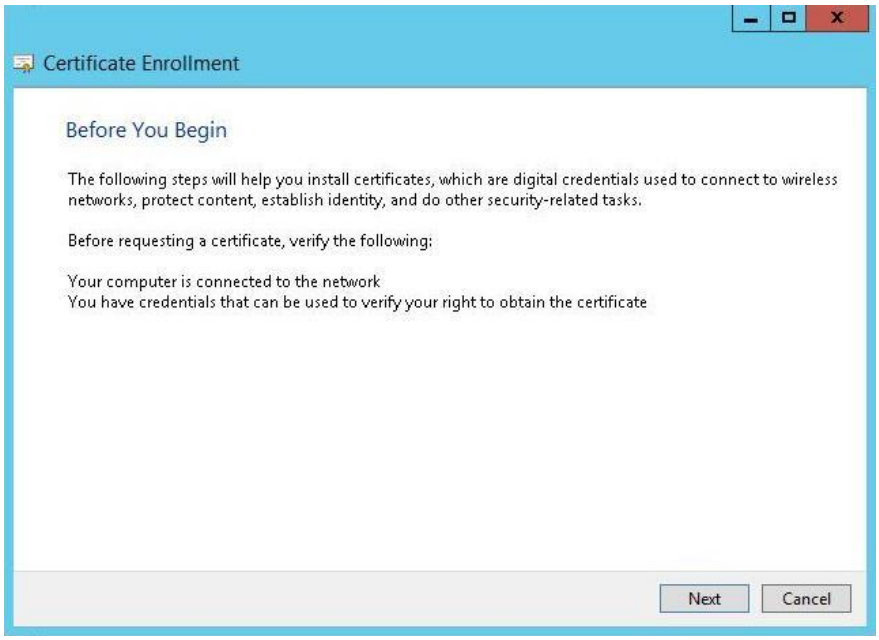
6. Hộp thoại **Add or Remove Snap-ins**, chọn **OK**.



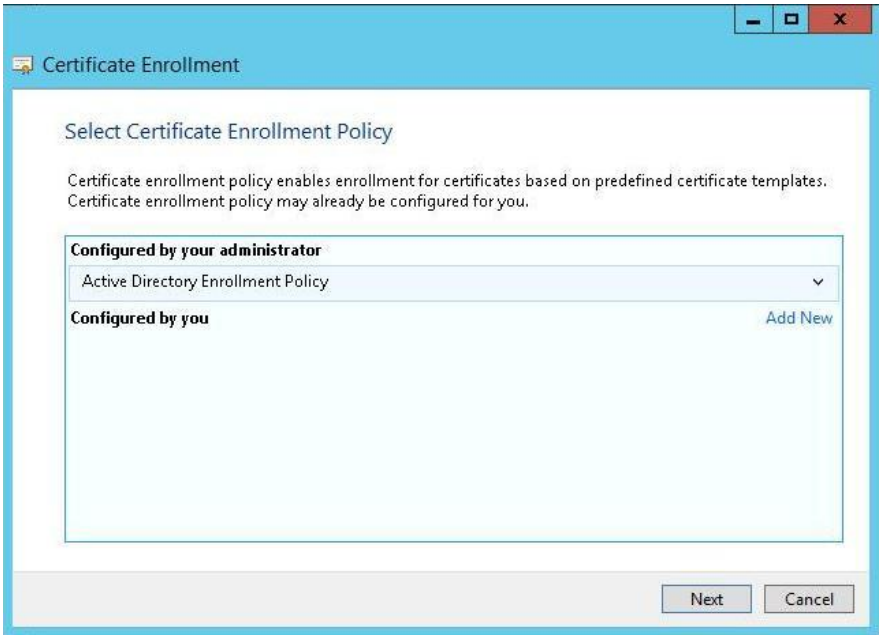
7. Trong cửa sổ console, bung **Certificates**, nhấn chuột phải **Personal**, chọn **All Tasks**, và chọn **Request New Certificate**.



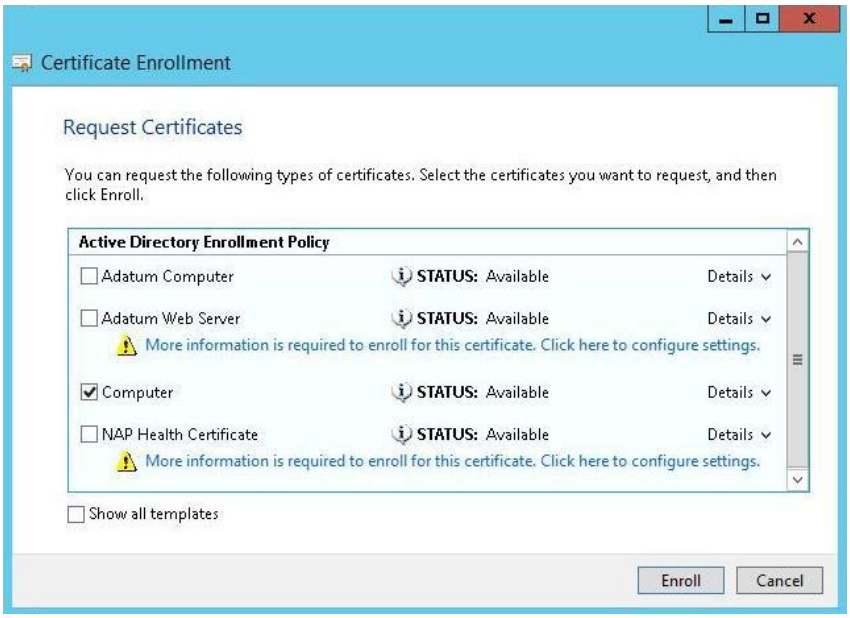
8. Cửa sổ **Before You Begin** , chọn **Next**.



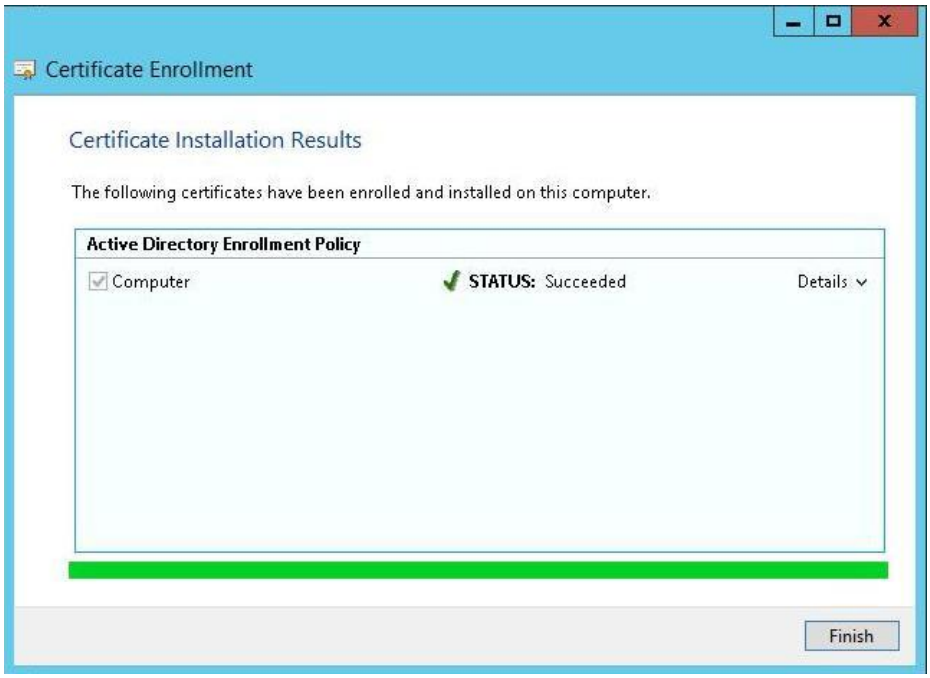
9. Cửa sổ **Select Certificate Enrollment Policy**, chọn **Active Directory Enrollment Policy**, chọn **Next**.



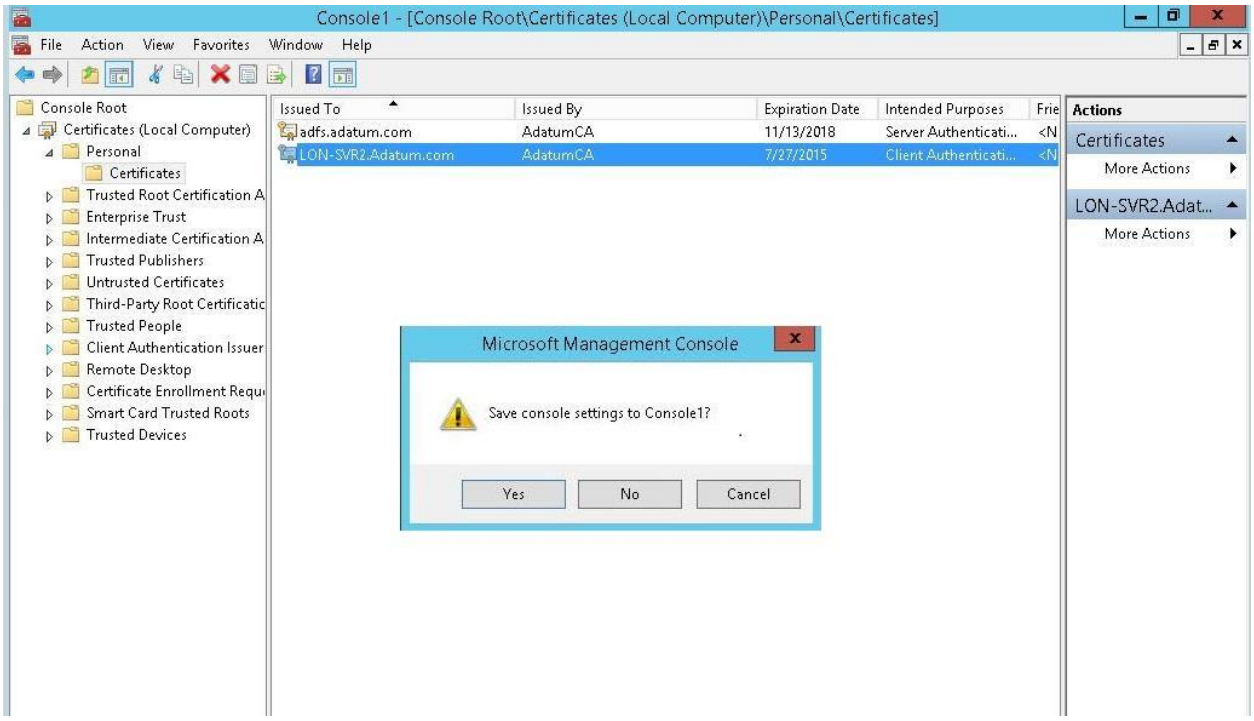
10. Cửa sổ **Request Certificate**s, đánh dấu chọn **Computer**, chọn **Enroll**.



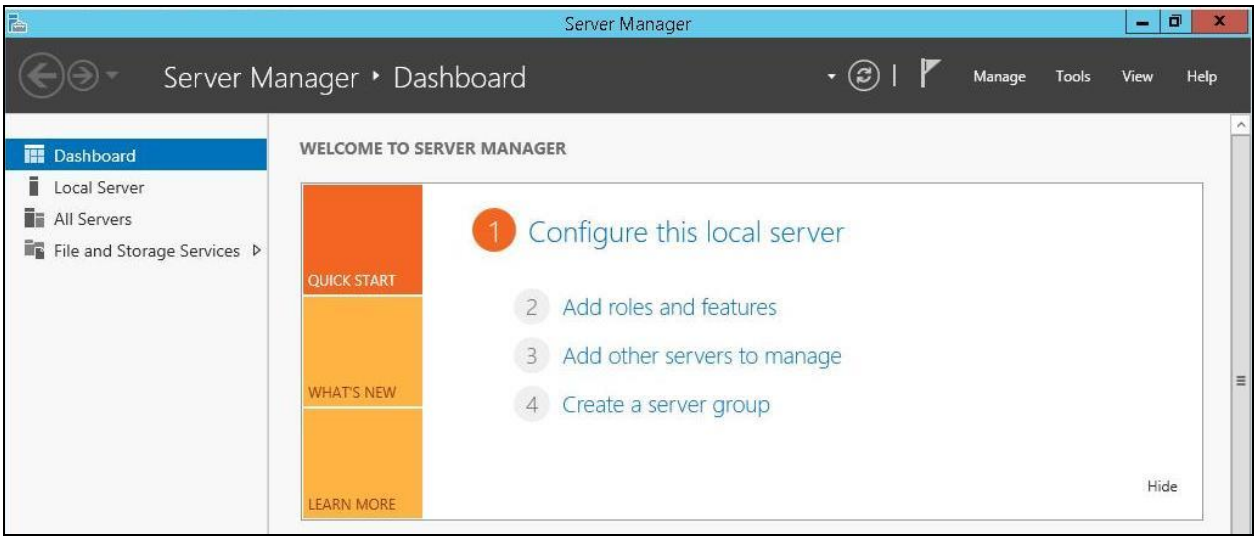
11. Cửa sổ **Certificate Installation Results**, kiểm tra Status thông báo **Succeeded**, và chọn **Finish**.



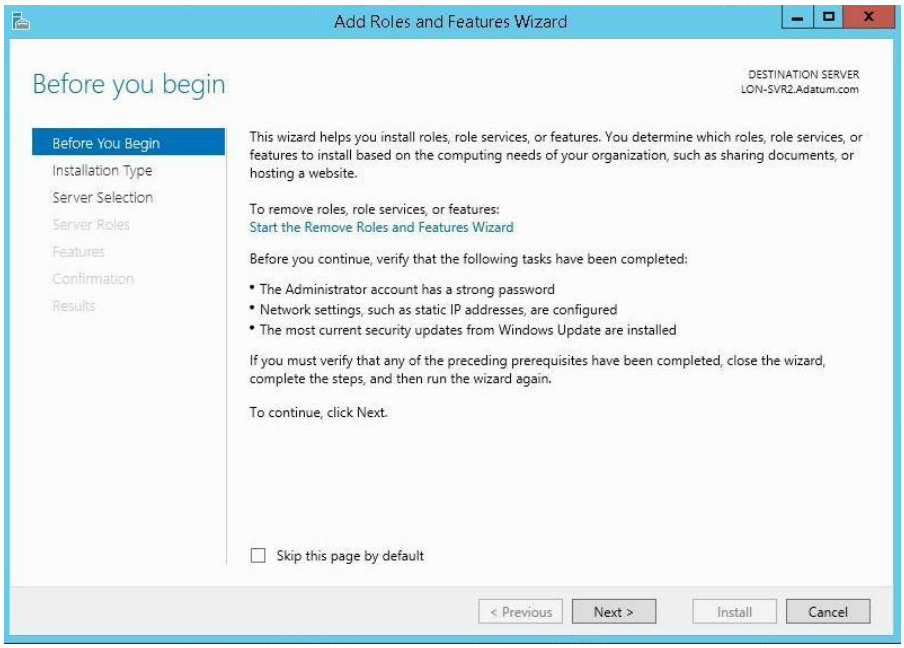
12. Tắt cửa sổ Console1, trong hộp thoại thông báo, chọn **No**.



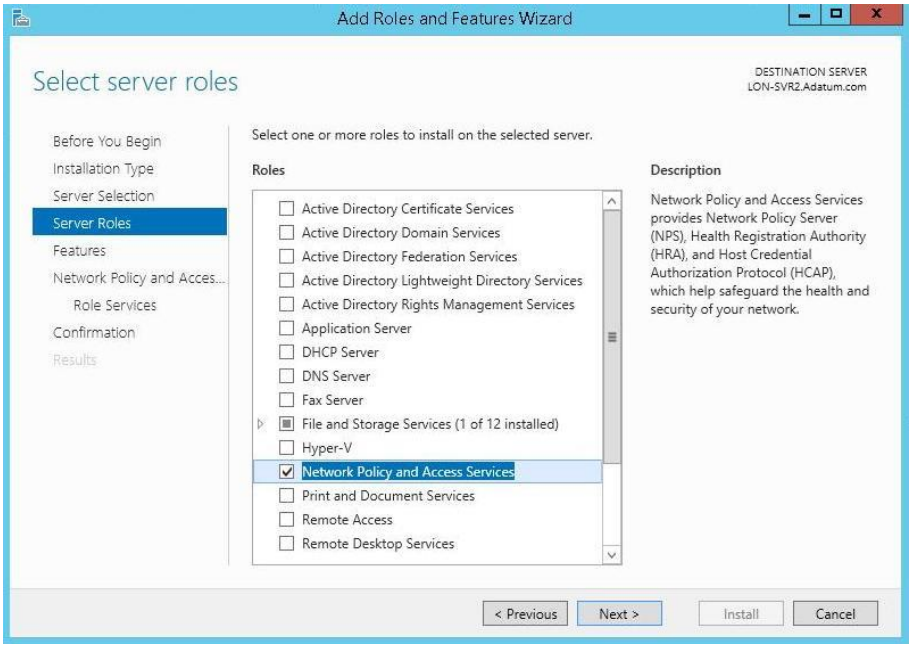
13. Mở **Server Manager**, chọn **Add roles and features**.



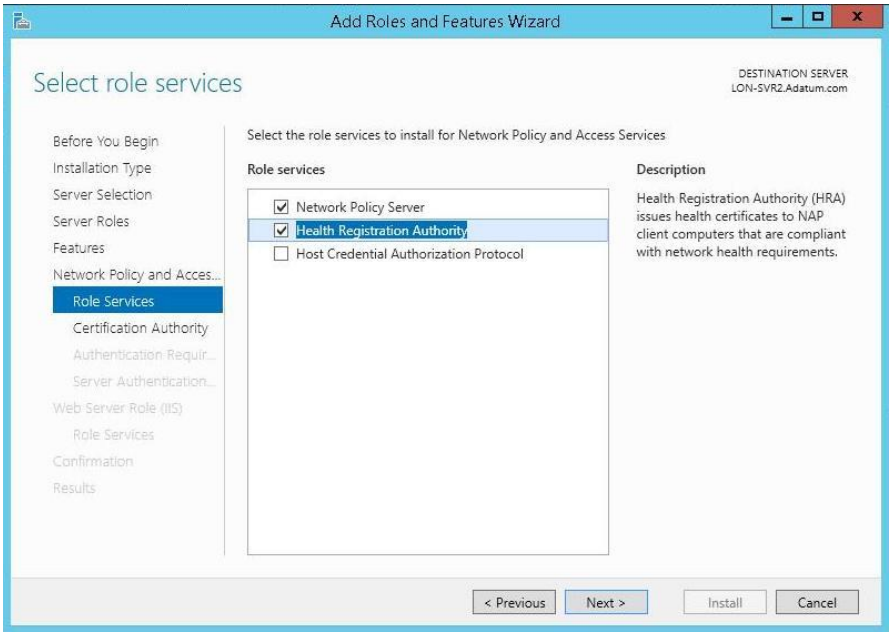
14. Cửa sổ **Before you begin** , chọn **Next** 3 lần.



15. Cửa sổ **Select server roles**, đánh dấu chọn **Network Policy and Access Services**, chọn **Add Features**, và chọn **Next** 3 lần.



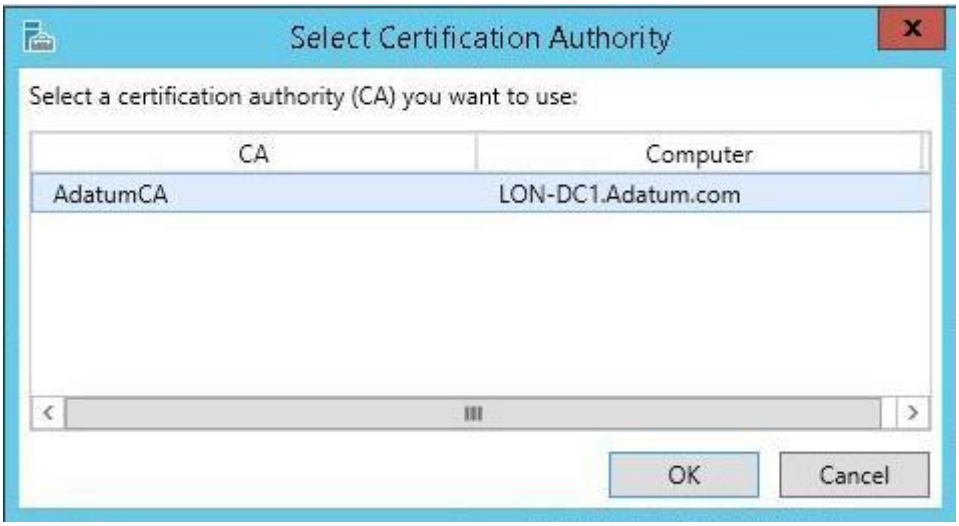
16. Cửa sổ **Select role services**, đánh dấu chọn **Network Policy Server** và **Health Registration Authority**, chọn **Add Features**, và chọn **Next**.



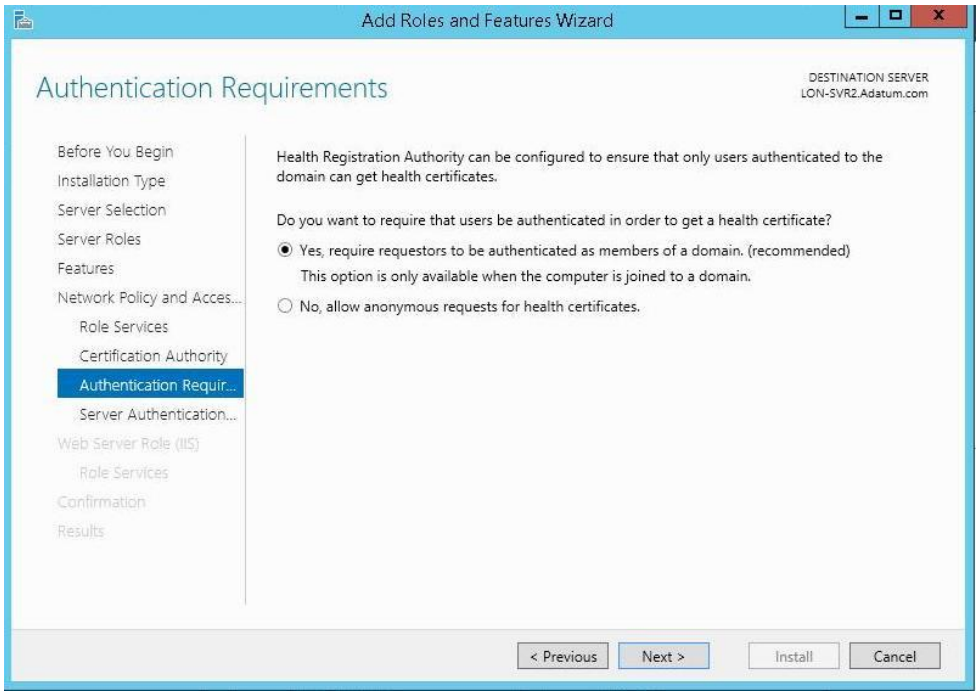
17. Cửa sổ **Certification Authority**, chọn **Use an existing remote CA**, và chọn **Select**.



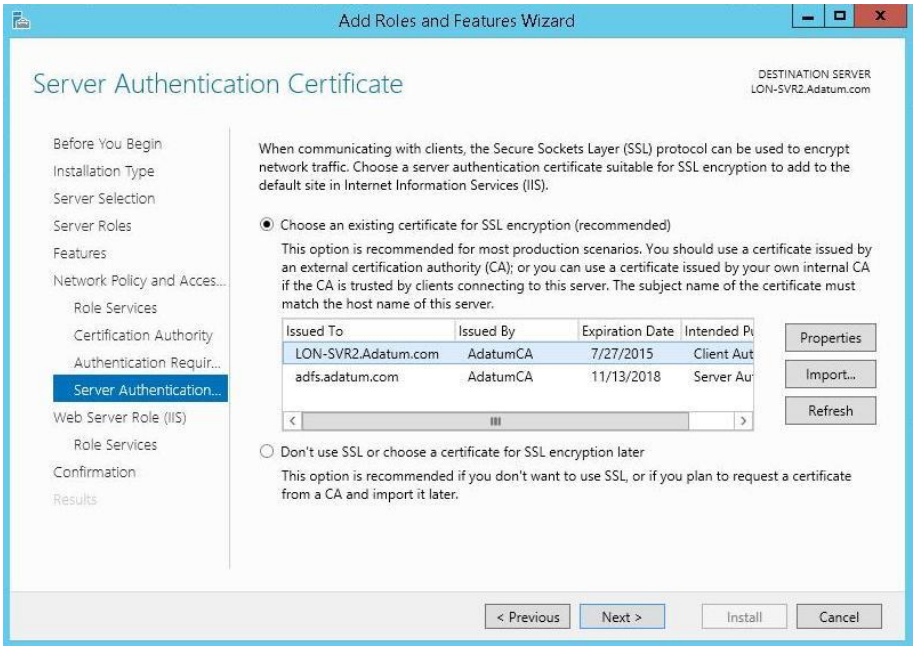
18. Cửa sổ **Select Certification Authority**, chọn **AdatumCA**, chọn **OK**, và chọn **Next**.



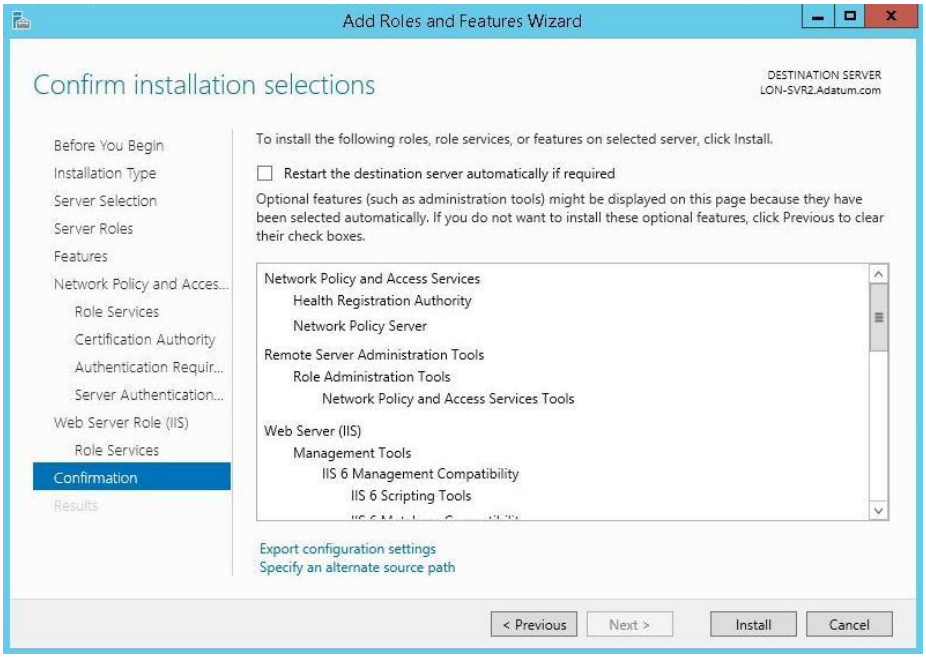
19. Cửa sổ **Authentication requirements**, chọn **Yes, require requestors to be authenticated as members of a domain**, và chọn **Next**.



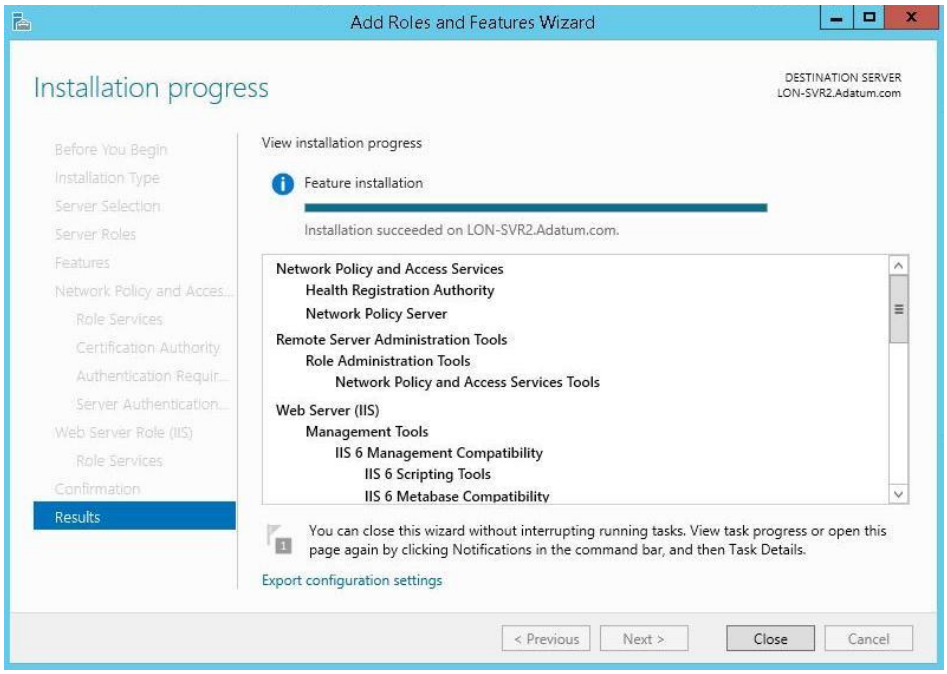
20. Cửa sổ **Server Authentication Certificate**, chọn **LON-SVR2.Adatum.com**, và chọn **Next** 3 lần.



21. Cửa sổ **Confirm installation selections**, chọn **Install**.

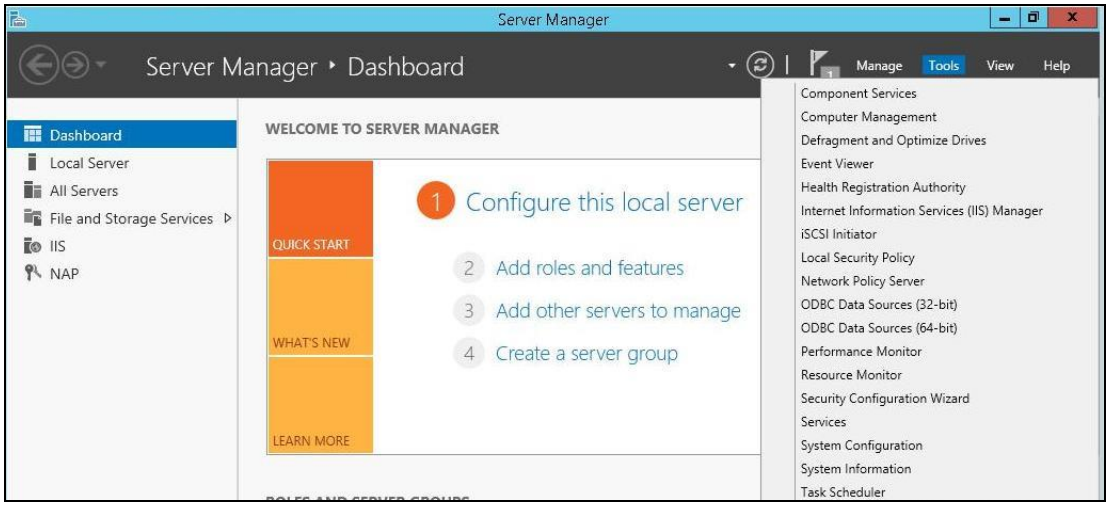


22. Cửa sổ **Installation progress**, kiểm tra cài đặt thành công, và chọn **Close**.

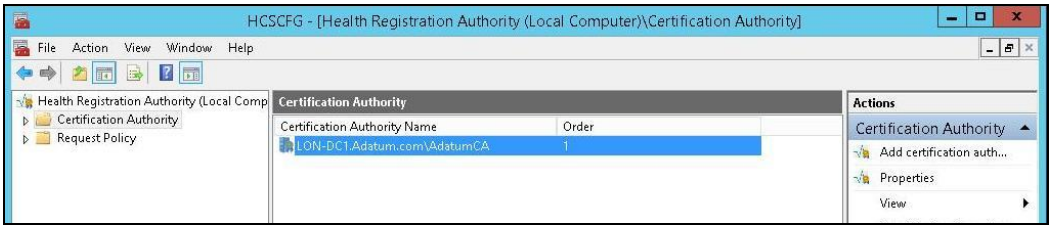


Bước 3. Cấu hình Health Registration Authority (HRA).

1. Trên máy **LON-SVR2**, mở **Server Manager**, bung menu **Tools**, mở **Health Registration Authority**.



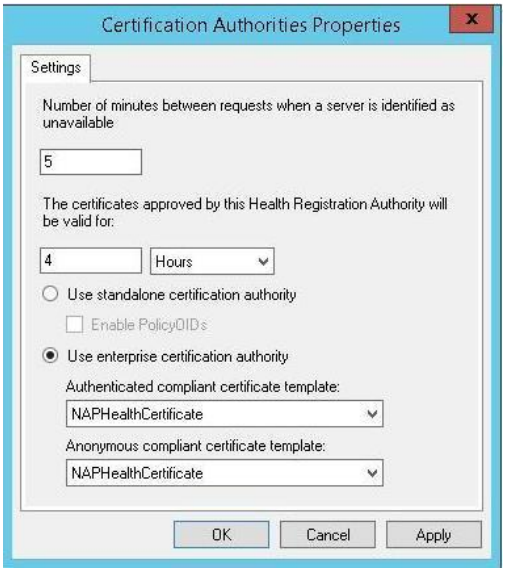
2. Trong cửa sổ **Health Registration Authority**, chọn **Certification Authority**, kiểm tra có **LON-DC1.Adatum.com\AdatumCA**.



3. Nhấn chuột phải **Certification Authority**, chọn **Properties**.



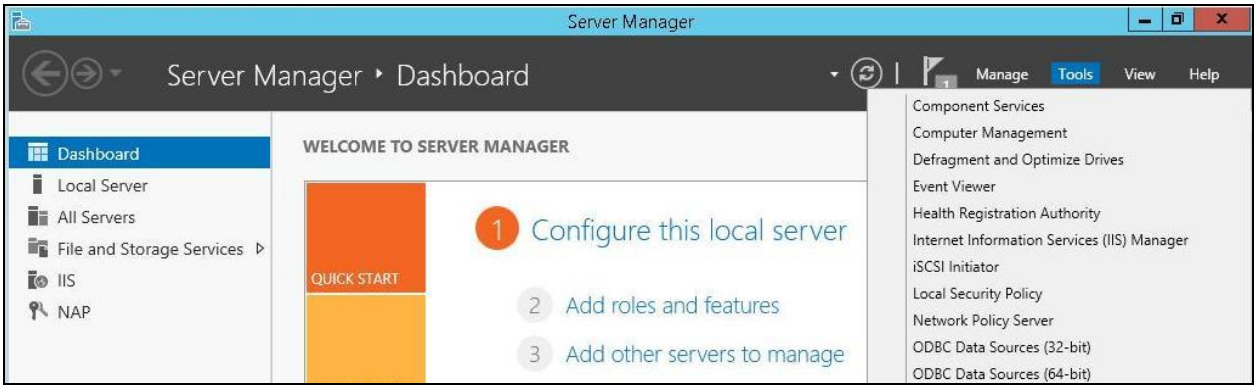
4. Trong hộp thoại **Certificate Authorities Properties**, chọn **Use enterprise certification authority**, bung 2 ô **Authenticated compliant certificate template** và **Anonymous compliant certificate template**, chọn **NAP Health Certificate**, và chọn **OK**.



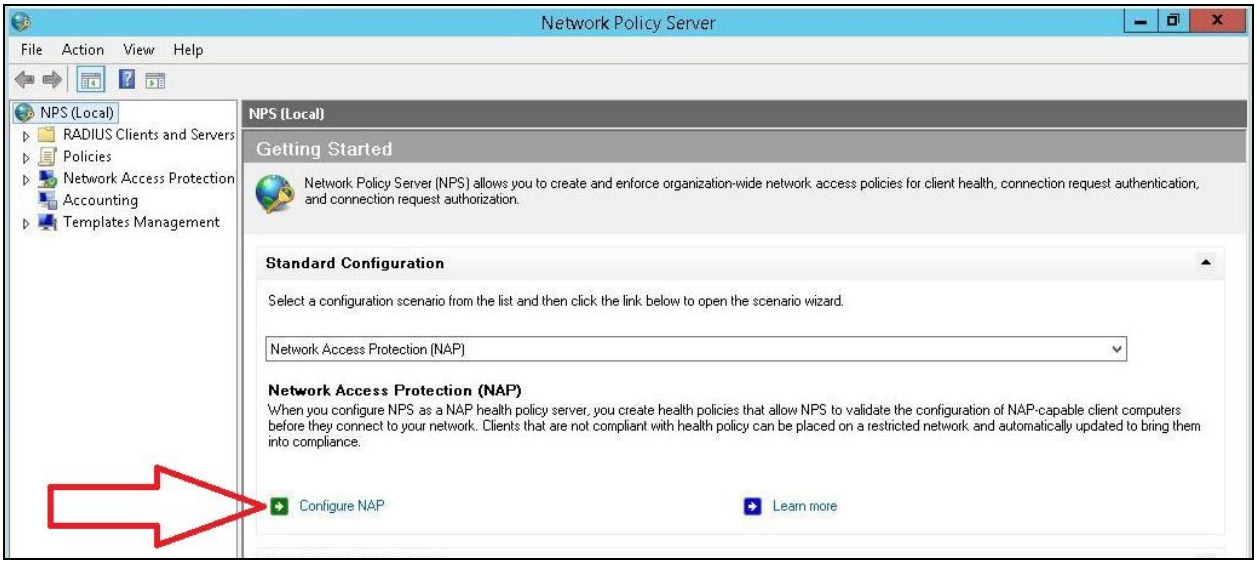
5. Tắt cửa sổ **Health Registration Authority**.

Bước 4. Cấu hình Health Policy.

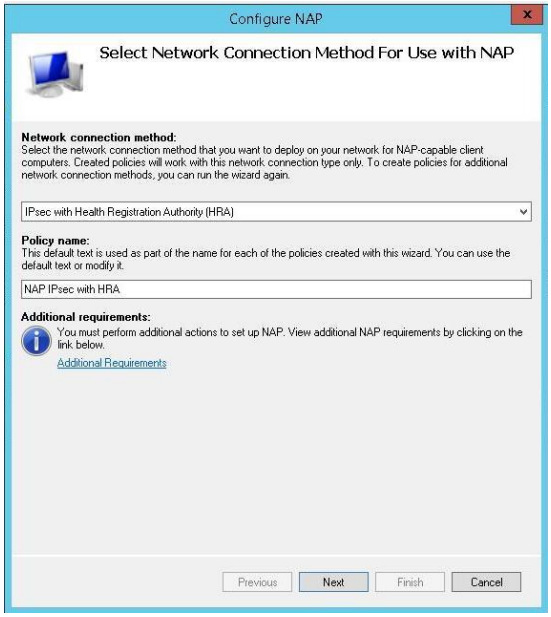
1. Trên máy **LON-SVR2**, mở **Server Manager**, bung menu **Tools**, mở **Network Policy Server**.



2. Trong cửa sổ **Network Policy Server**, chọn **Configure NAP**.



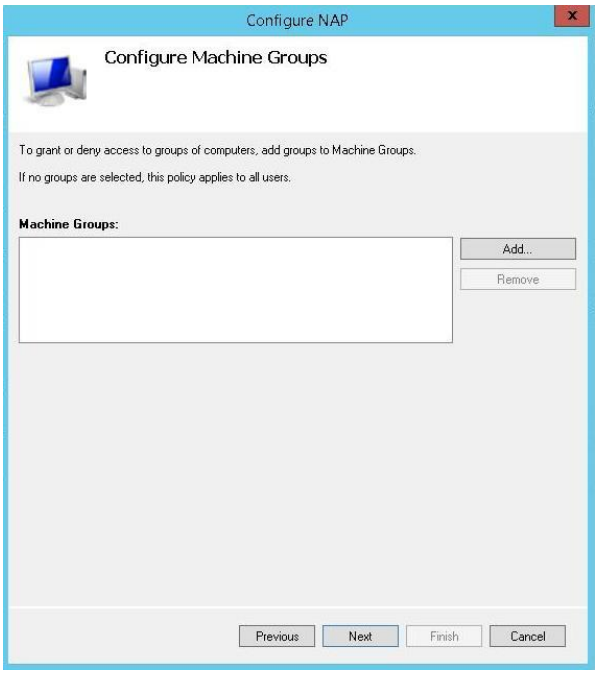
3. Cửa sổ **Select Network Connection Method For Use with NAP**, bung **Network connection method**, chọn **IPsec with Health Registration Authority (HRA)**, và chọn **Next**.



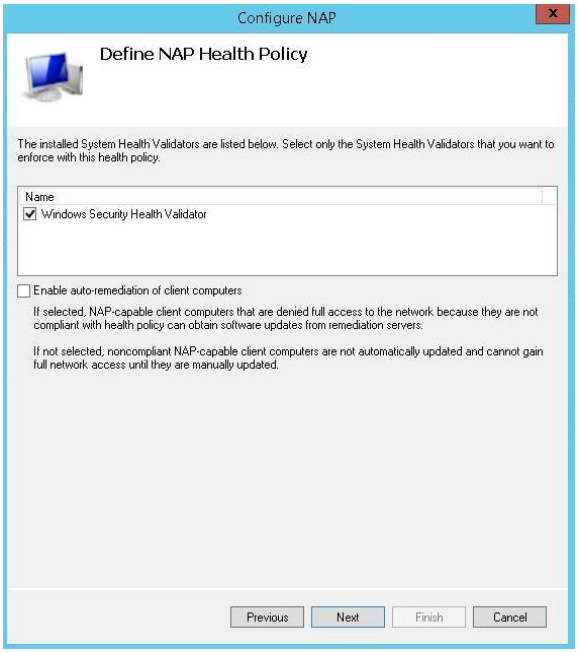
4. Cửa sổ **Specify NAP Enforcement Servers Running HRA**, chọn **Next**.



5. Cửa sổ **Configure Machine Groups**, chọn **Next**.

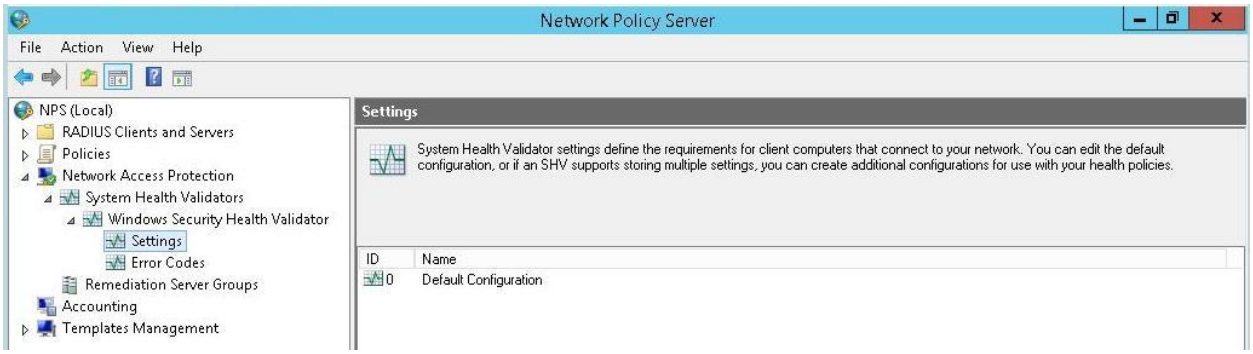


6. Cửa sổ **Define NAP Health Policy**, đánh dấu chọn Windows Security Health Validator, và bỏ dấu chọn **Enable auto-remediation of client computers**, chọn **Next** và chọn **Finish**.



Bước 5. Cấu hình Health Validator.

1. Trên máy **LON-SVR2**, trong cửa sổ **Network Policy Server**, bung **Network Access Protection**, bung **System Health Validators**, bung **Windows Security Health Validators**, chọn **Settings**, mở **Default configuration**.



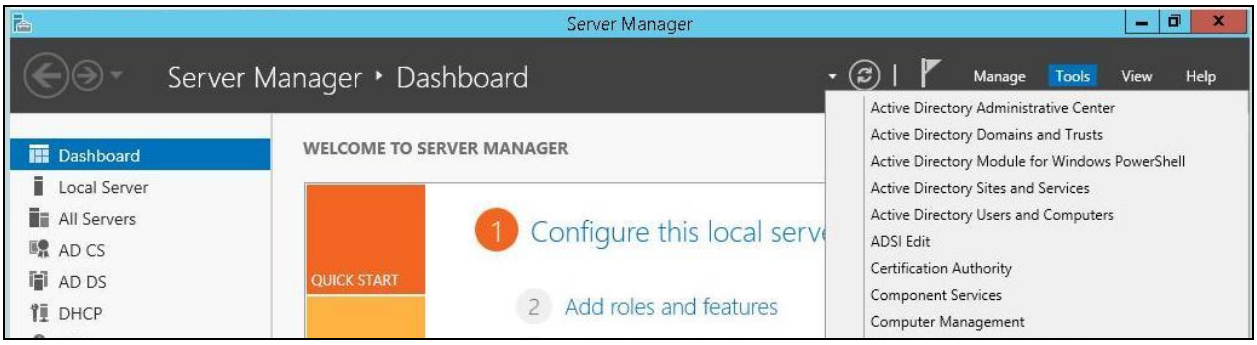
2. Trong cửa sổ **Windows Security Health Validators,** chọn mục **Windows 8/Windows 7/Windows Vista**, bỏ trắng tất cả các lựa chọn, và đánh dấu chọn **A firewall is enabled for all network connections**, chọn **OK**.



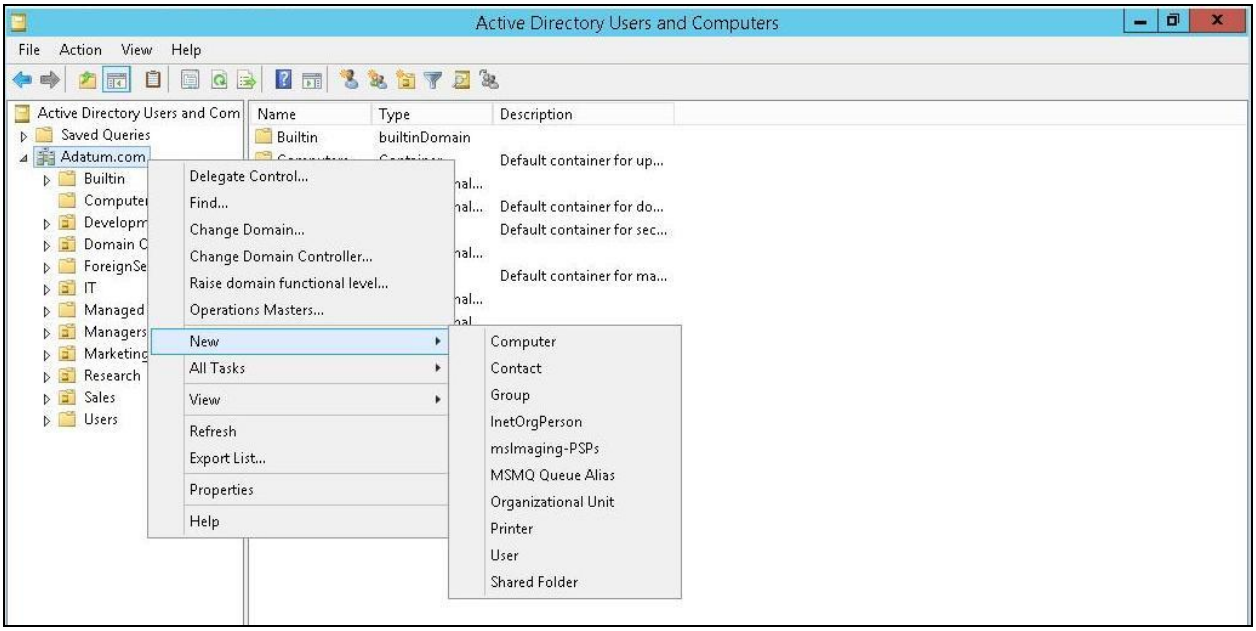
Bước 6. Tạo GPO để thiết lập cấu hình NAP Client.

1. Qua máy **LON-DC1**.

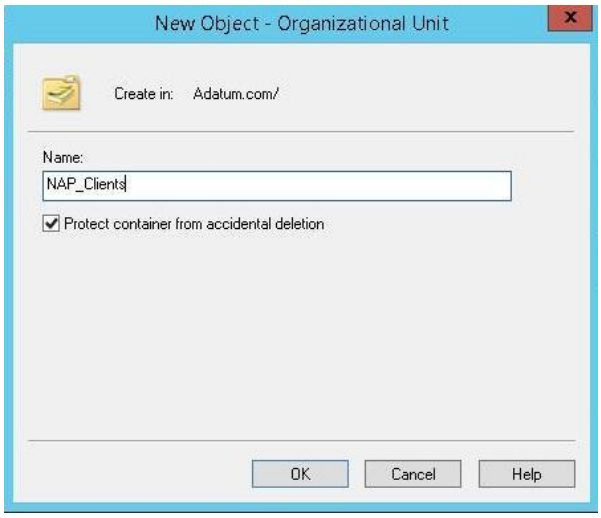
2. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**.



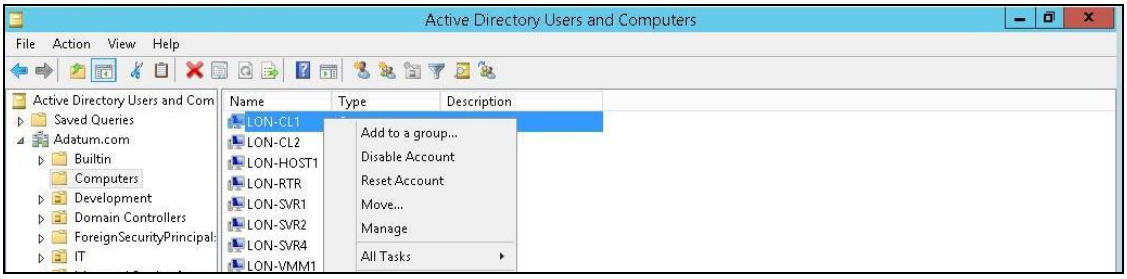
3. Cửa sổ **Active Directory Users and Computers**, nhấn chuột phải **Adatum.com**, chọn **New**, chọn **Organizational Unit**.



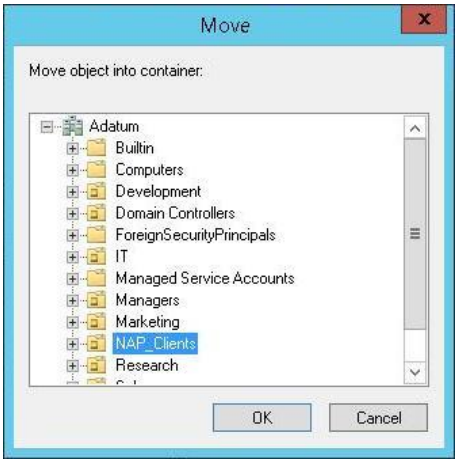
4. Hộp thoại **New Object – Organizational Unit**, nhập **NAP_Clients**, chọn **OK**.



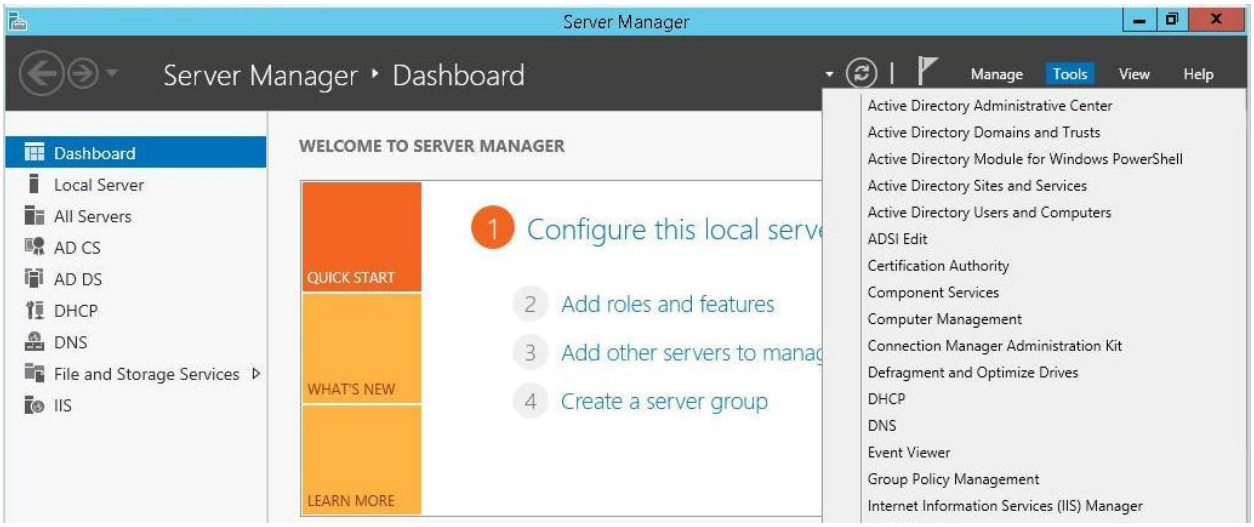
5. Cửa sổ **Active Directory Users and Computers,** chọn **Computers**, nhấn chuột phải **LON-CL1**, chọn **Move**.



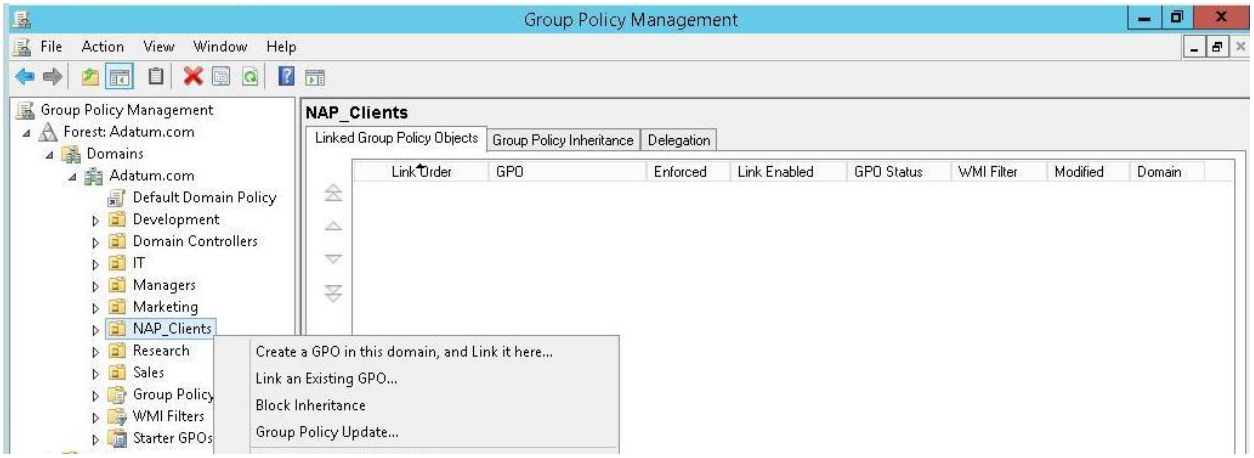
6. Hộp thoại **Move**, chọn OU **NAP_Clients**, và chọn **OK**.



7. Quay lại cửa sổ **Server Manager**, bung **Tools**, mở **Group Policy Management**.



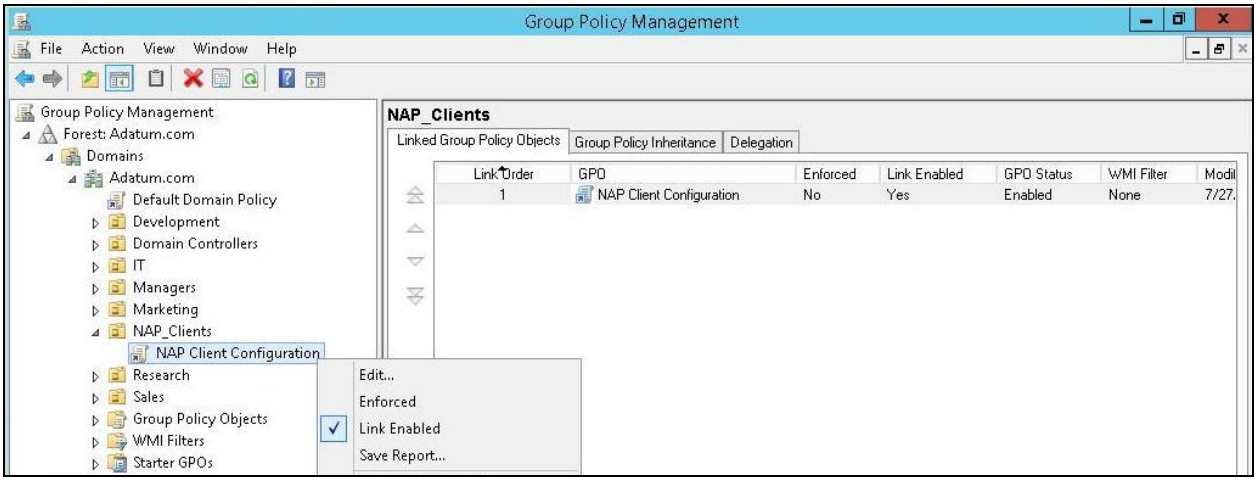
8. Trong cửa sổ **Group Policy Management**, bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, nhấn chuột phải OU **NAP_Clients**, chọn **Create a GPO in this domain, and Link it here**.



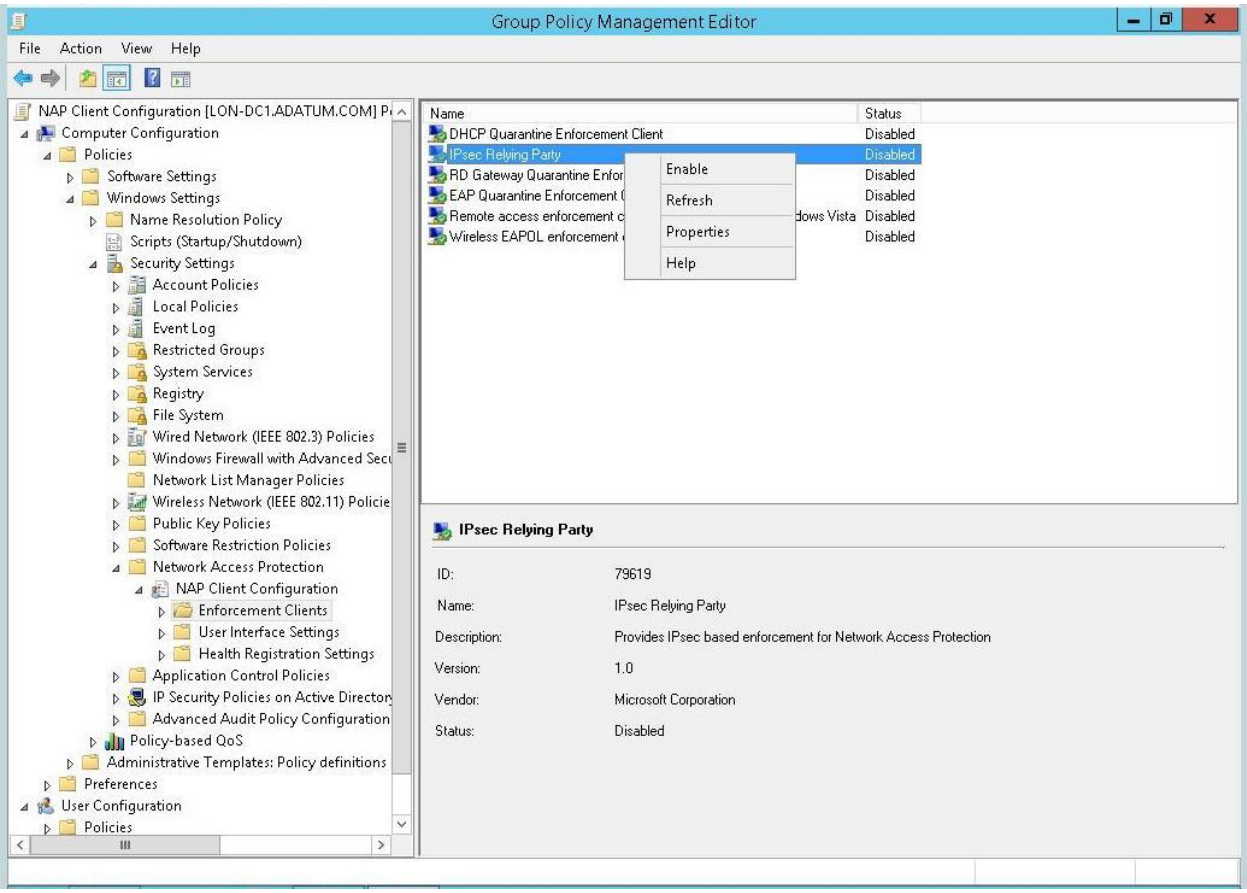
9. Hộp thoại **New GPO**, trong ô **Name**, nhập **NAP Client Configuration**, chọn **OK**.



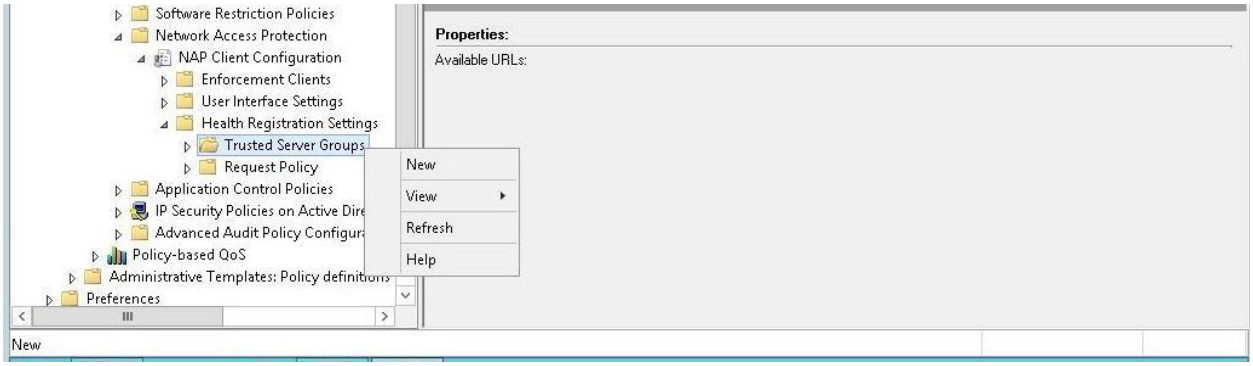
10. Bung OU **NAP_Clients**, nhấn chuột phải **NAP Client Configuration**, chọn **Edit**.



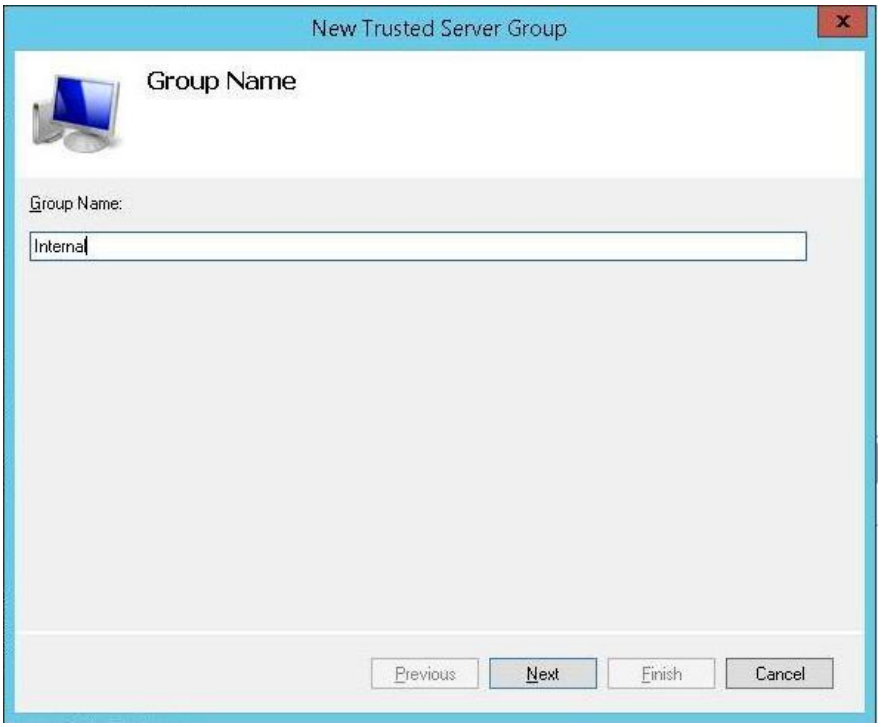
11. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Network Access Protection**, bung **NAP Client Configuration**, chọn **Enforcement Clients**. Nhấn chuột phải **IPsec Relying Party**, chọn **Enable**.



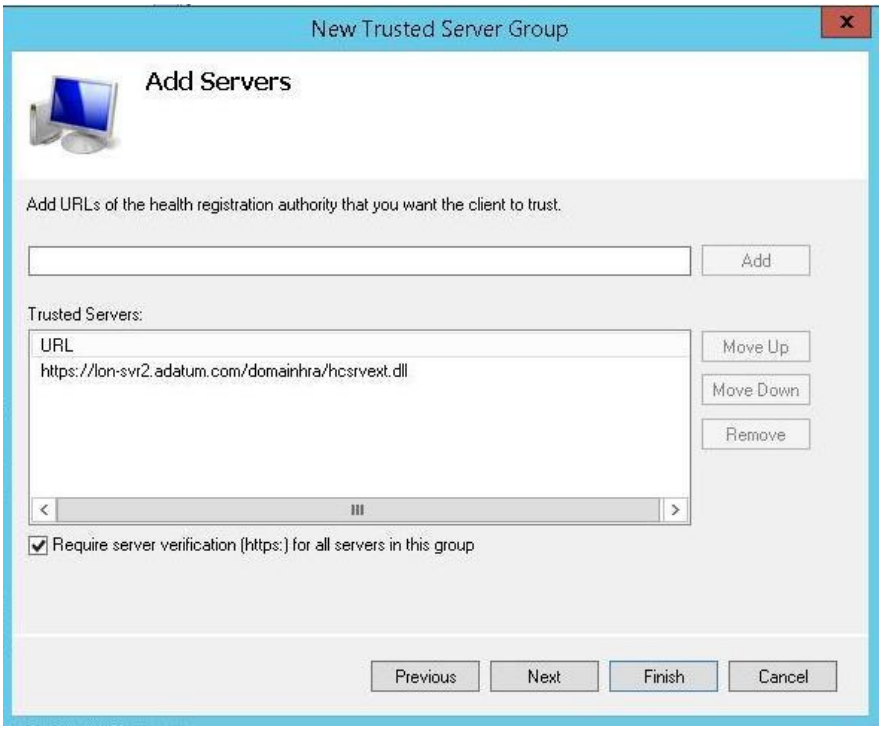
12. Bung **Health Registration Settings**, nhấn chuột phải **Trusted Server Groups**, chọn **New**.



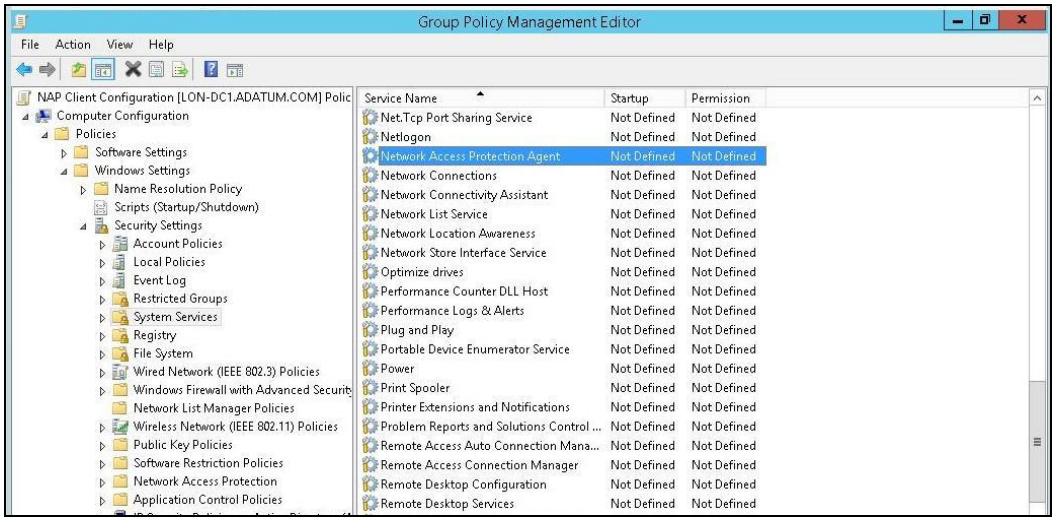
13. Cửa sổ **Group Name**, nhập **Internal**, và chọn **Next**.



14. Cửa sổ **Add Servers**, nhập **https://lon-svr2.adatum.com/domainhra/hcsrvext.dll**, chọn **Add**, và chọn **Finish**.



15. Trong cửa sổ **Group Policy Management Editor**, bung **Security Settings**, chọn **System Services**, mở **Network Access Protection Agent**.



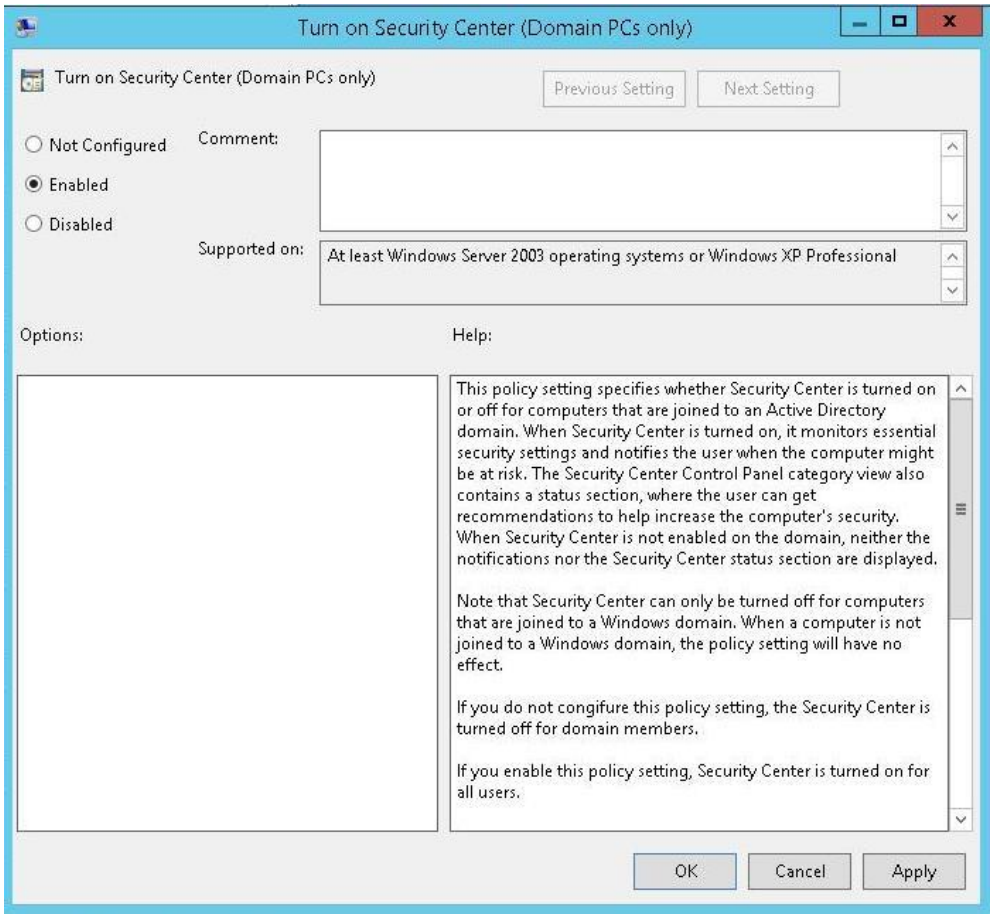
16. Hộp thoại **Network Access Protection Agent Properties**, đánh dấu chọn **Define this policy setting**, trong **Select services startup mode**, chọn **Automatic**, chọn **OK**.



17. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration,** bung **Administrative Templates**, bung **Windows Components**, chọn **Security Center**, mở **Turn on Security Center**.



18. Hộp thoại **Turn on Security Center**, chọn **Enabled**, và chọn **OK**.



19. Tắt **Group Policy Management Editor**.

Bước 7. Kiểm tra Client đã ảnh hưởng GPO.

1. Khởi động lại máy **LON-CL1**, logon **Adatum\Administrator** với password **Pa$$w0rd**.

2. Bung **Start** menu, gõ **Windows PowerShell**, nhấn **Enter**.



3. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

gpupdate /force



4. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

get-service napagent

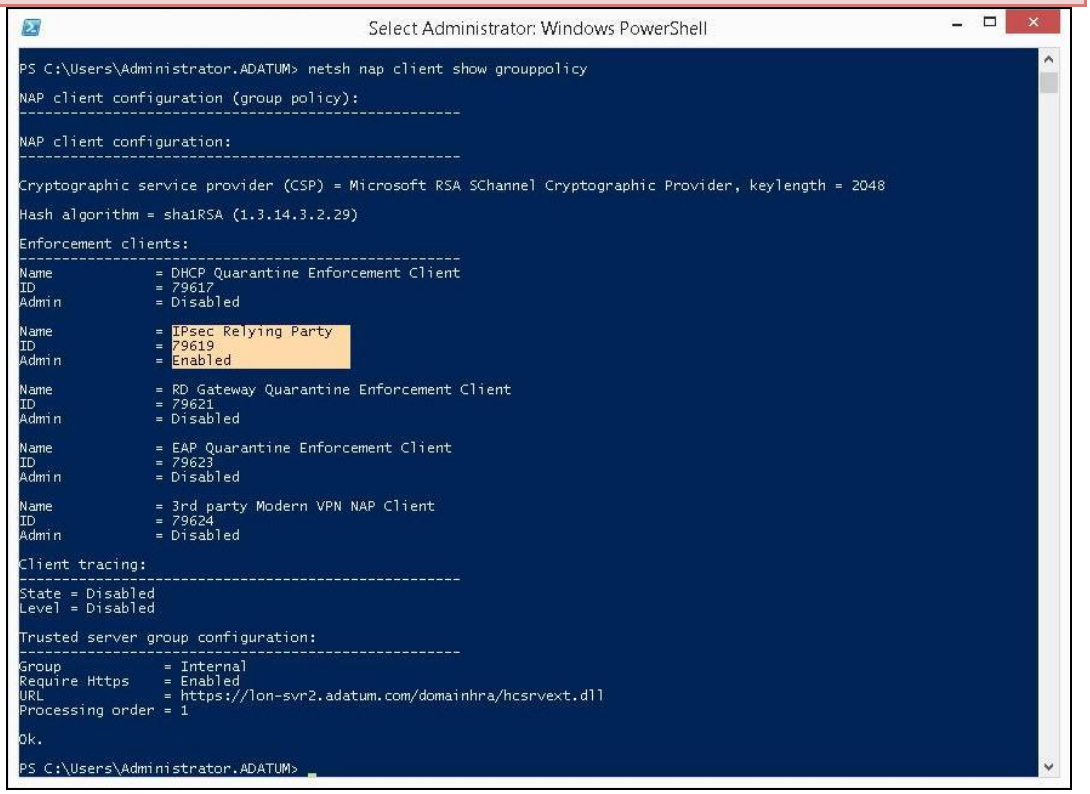
Chú ý:Dịch vụ napagent đang có trạng thái Running.



5. Trong cửa sổ **Windows PowerShell**, gõ lệnh:

netsh nap client show grouppolicy

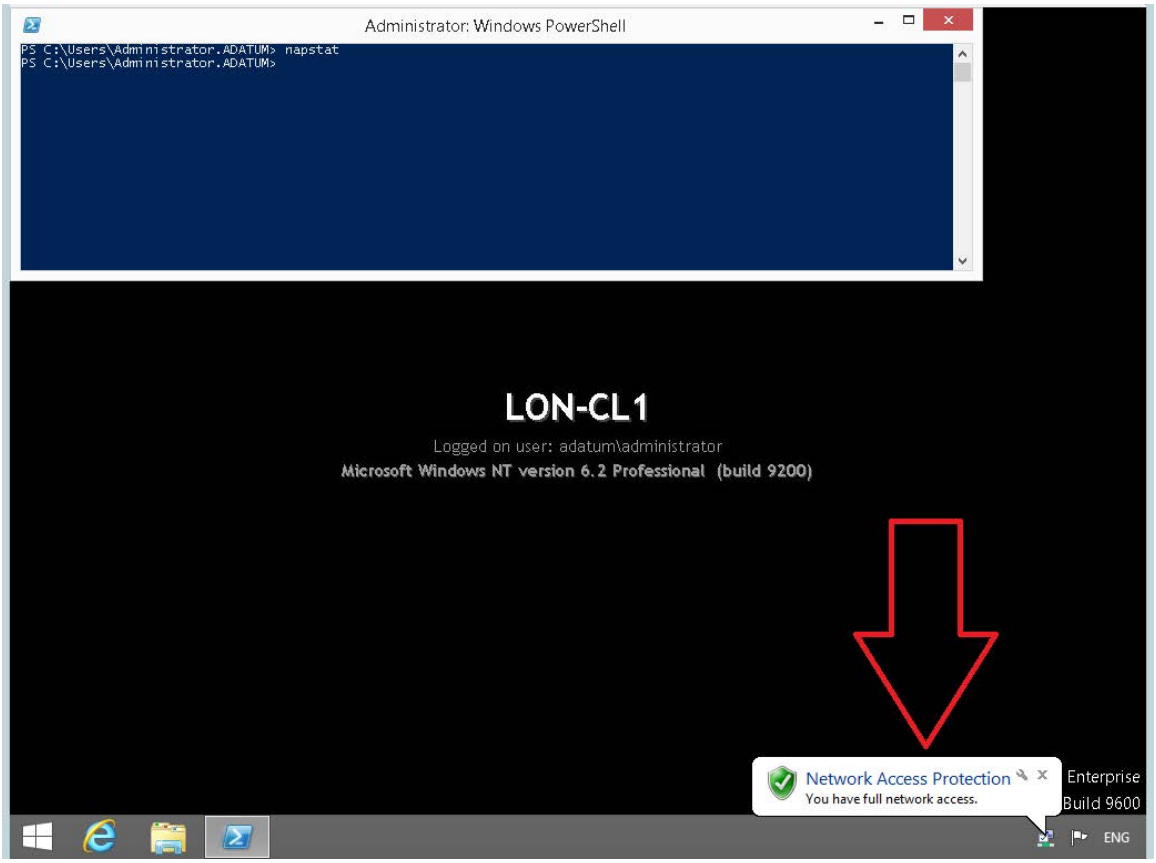
Chú ý: Lệnh này có chức năng kiểm tra GPO đã được áp dụng. Kiểm tra IPsec Relying Party đã được Enable.



Bước 8. Kiểm tra Client tuân thủ chính sách an toàn.

1. Trên **LON-CL1**, mở Windows PowerShell, gõ lệnh: **napstat**

Kiểm tra: Client nhận được thông báo tuân thủ của NAP.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công chức năng NAP thực thi IPsec. (NAP with IPSec Enforcement)

❖ **Chuẩn bị cho bài tiếp theo:**

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho máy ảo **20413C-LON-SVR2** và **20413C-LON-CL1.**

Bài 12: Thiết kế và triển khai giải pháp truy cập từ xa (DirectAccess & VPN)

I. Mục tiêu:

- Thiết kế giải pháp truy cập từ xa.
- Lập kế hoạch và triển khai giải pháp DirectAccess.
- Lập kế hoạch và triển khai giải pháp VPN.
- Lập kế hoạch và triển khai giải pháp Web Application Proxy.

II. Kịch bản:

Công ty A. Datum đang đánh giá các yêu cầu truy cập từ xa của những người dùng thường xuyên làm việc từ khách sạn hoặc tại nhà. Nhiều nhân viên quản lý ở trụ sở London thường di du lịch và phải truy cập dữ liệu từ xa. Giám đốc điều hành cũng muốn làm việc từ nhà, hoặc trong khi đi du lịch. Ngoài ra, nhiều nhân viên của công ty Trey Research và Contoso làm việc tại nhà. Đôi khi họ lại mang máy tính vào văn phòng công ty, và thường bị thất bại trong việc truy cập tài nguyên trong hệ thống mạng bởi vì máy tính của họ vi phạm các chính sách an toàn của hệ thống đề ra.

Hiện nay việc triển khai mạng riêng ảo (VPN) tại công ty A. Datum bao gồm một VPN Server duy nhất. Các VPN Clients sử dụng kết nối PPTP, và được phép liên lạc với toàn bộ hệ thống khi kết nối thành công. VPN Server hiện đang được đặt ở London, bạn phải thiết kế một giải pháp truy cập từ xa dựa trên yêu cầu của người dùng và doanh nghiệp.

Bây giờ bạn phải xác định các thành phần cần thiết để hỗ trợ việc triển khai chức năng DirectAccess. Bạn cũng cần phải xác định các vai trò máy chủ cần thiết mà bạn phải cài đặt trước khi triển khai DirectAccess. Còn đối với những máy tính không đáp ứng tiêu chí của DirectAccess, bạn sẽ hỗ trợ truy cập bằng giải pháp VPN. Ngoài ra, bạn cần phải cấu hình

chức năng Web Application Proxy để cho phép người dùng bên ngoài truy cập các ứng dụng tại A.Datum.

Các thông tin khác:

- Các máy clients của A. Datum chạy Windows 8.1, Windows 8 và Windows 7.
- Một số người dùng sử dụng các máy tính không phải là thành viên của domain Adatum.com truy cập vào mạng nội bộ. Vấn đề bảo mật cho các thiết bị này là rất quan trọng.
- Một số người dùng của Contoso chỉ cần truy cập vào một trang web an toàn trong mạng nội bộ tại A.Datum.
- Chức năng tự động kết nối của máy client là rất quan trọng.
- Hệ thống VPN hiện tại bao gồm một VPN Server duy nhất.
- Các máy VPN Clients sử dụng kết nối PPTP, và được phép liên lạc với toàn bộ hệ thống khi kết nối thành công.
- A.Datum đã có cơ sở hạ tầng cho việc triển khai Certificate và Smart Card.
- Một số giám đốc điều hành không kết nối VPN được từ khách sạn vì bị tường lửa của khách sạn chặn truy cập.
- Người sử dụng từ các địa điểm không thuộc châu Âu phàn nàn tốc độ truy cập vào dữ liệu thông qua VPN bị chậm.
- Chỉ có một đường truyền kết nối Internet duy nhất cho Contoso, hiện đang được đặt tại Paris.

III. Yêu cầu tổng quan:

Thiết kế một chiến lược truy cập từ xa để hỗ trợ các mục tiêu sau đây:

- Bảo mật dữ liệu là rất quan trọng.
- Hỗ trợ người dùng truy cập từ xa dù bị tường lửa chặn kết nối PPTP và L2TP.
- Cải thiện tốc độ truy cập từ xa.

- Kết nối phải được thiết lập lại tự động nếu bị ngắt kết nối.
- Giám đốc điều hành được phép truy cập từ xa, và không bị giới hạn.
- Nhân viên quản lý chi nhánh chỉ được phép truy cập từ xa vào các tài nguyên trong văn phòng chính của họ. (Ví dụ, giám đốc chi nhánh ở châu Âu chỉ được phép truy cập vào các tài nguyên ở Paris.)
- Nhân viên dịch vụ khách hàng không được phép truy cập từ xa.
- Nhân viên tiếp thị được phép truy cập từ xa, nhưng chỉ cho truy cập hệ thống email.
- Cấu hình Web Application Proxy để cho phép người dùng của Contoso truy cập vào trang web trong mạng nội bộ tại A.Datum.

IV. Mô hình thực hành gồm các máy:

Máy ảo (VM)	**20413C-LON-DC1** **20413C-LON-SVR1** **20413C-LON-RTR** **20413C-LON-CL1** **20413C-LON-CL2**
User name	Adatum\Administrator
Password	Pa$$w0rd

V. Chuẩn bị:

1. Trên máy thật, bung **Start** menu, mở công cụ **Hyper-V Manager**.
2. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải **20413C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20413C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiên từ bước 2 đến 4 cho máy ảo **20413C-LON-RTR.**

6. Chú ý: Không khởi động máy **20413C-LON-SVR1, 20413C-LON-CL1** và **20413C-LON-CL2**cho tới khi có yêu cầu

VI. Thực hành:

Bài tập 1: Triển khai giải pháp DirectAccess

❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình AD DS và DNS.
2. Cấu hình Certificates.
3. Cấu hình Internal Resources.
4. Cấu hình DirectAccess Server.
5. Triển khai GPO để thiết lập cấu hình DirectAccess.
6. Kiểm tra Certificate distribution.
7. Kiểm tra cấu hình IP.
8. Di chuyển **LON-CL1**, và kiểm tra kết nối vào nội bộ.

❖ **Thực hiện:**

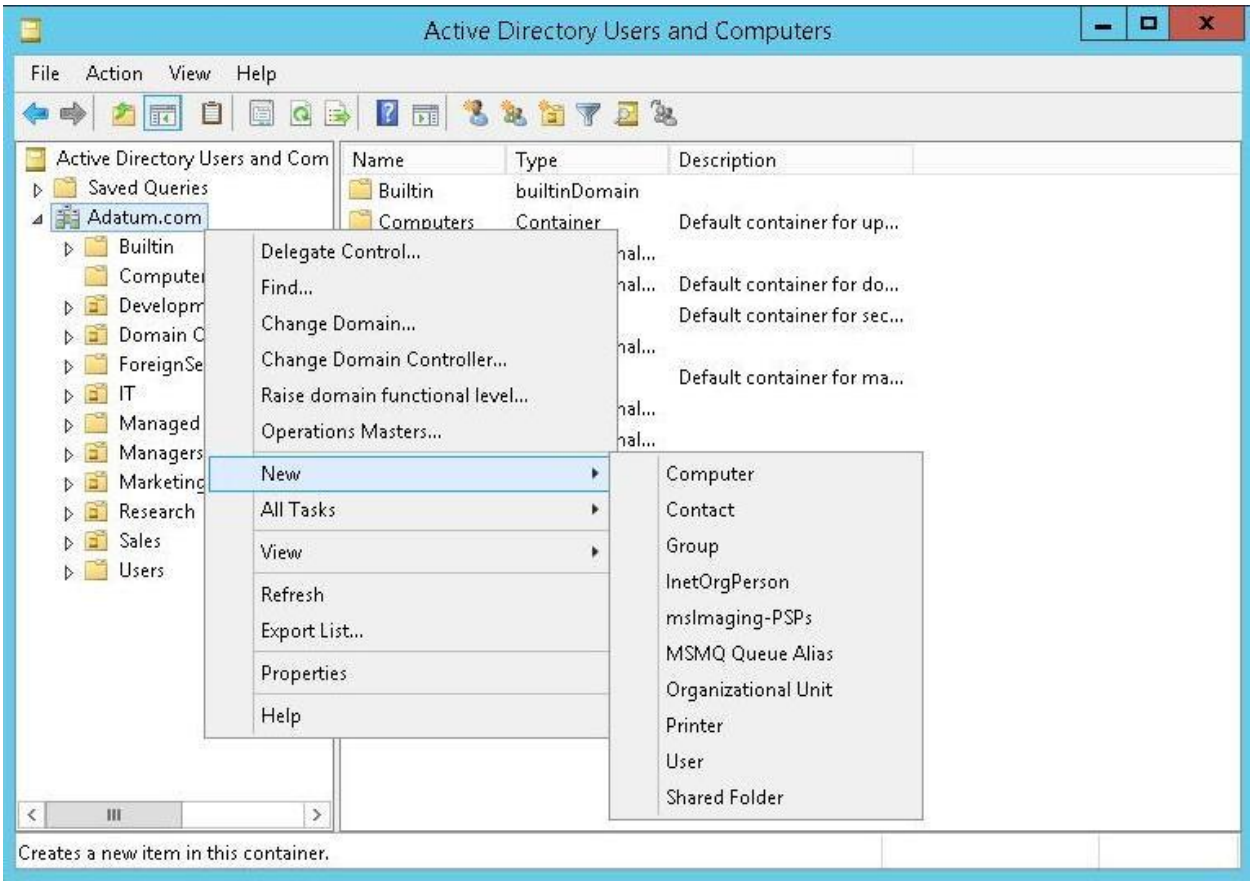
Bước 1. Cấu hình AD DS và DNS.

1. Tạo một Security Group cho các máy Clients truy cập DirectAccess:

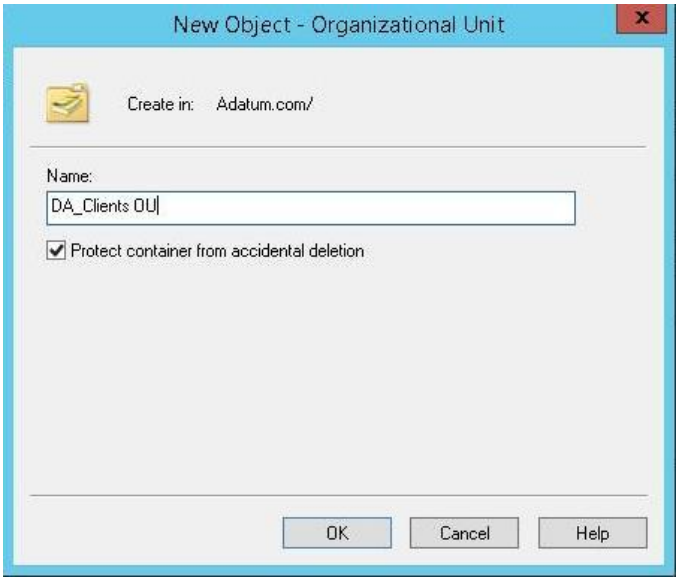
a. Logon máy **LON-DC1**.

b. Mở **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**.

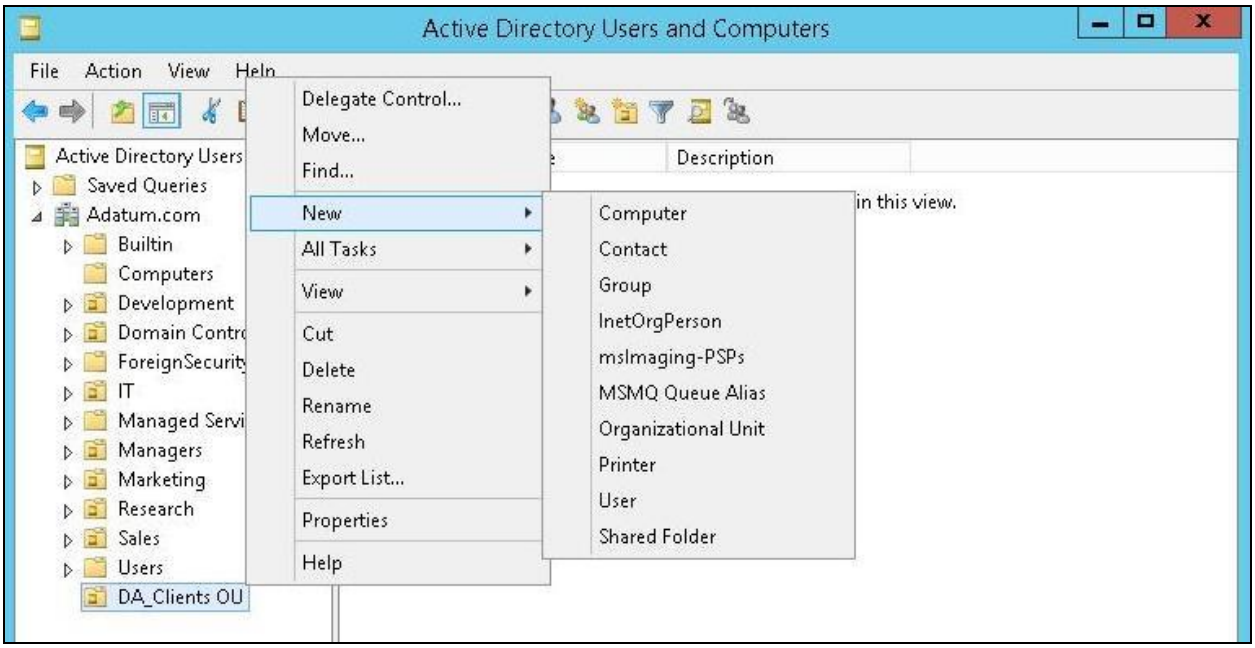
c. Trong **Active Directory Users and Computers**, nhấn chuột phải **Adatum.com**, bung **New**, và chọn **Organizational Unit**



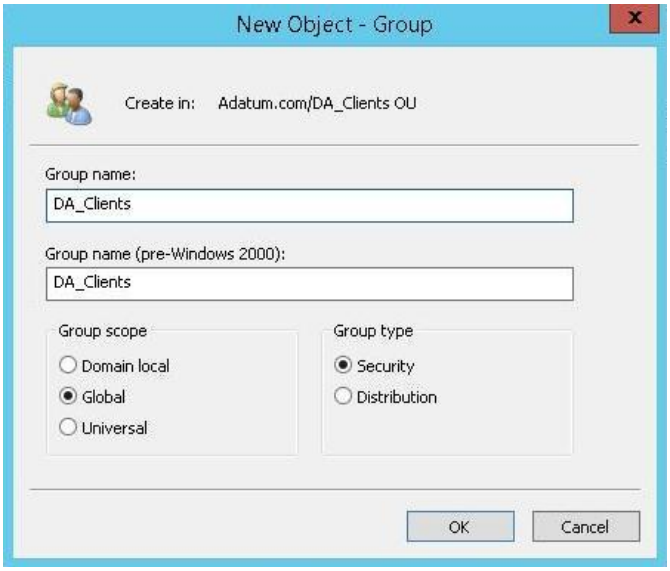
d. Hộp thoại **New Object – Organizational Unit**, trong ô **Name**, nhập **DA_Clients OU**, chọn **OK**.



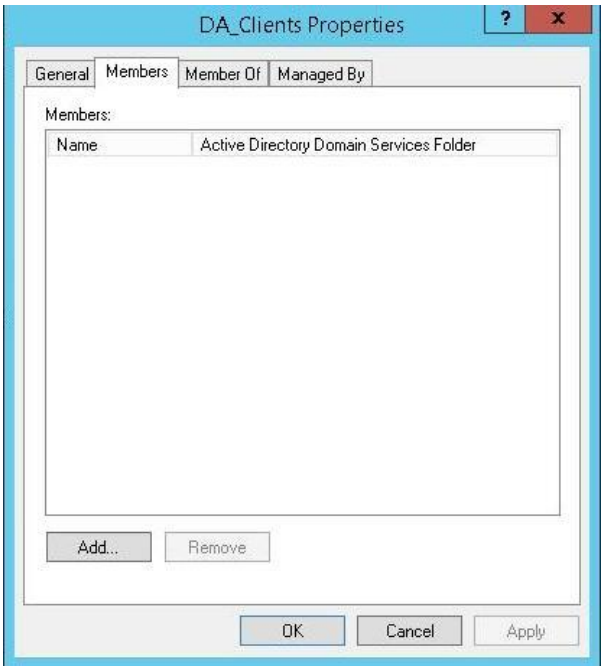
e. Trong cửa sổ **Active Directory Users and Computers,** bung **Adatum.com**, nhấn chuột phải **DA_Clients OU**, bung **New**, và chọn **Group**.



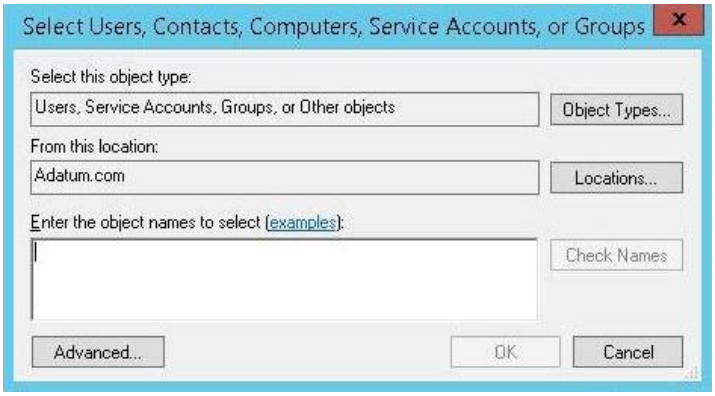
f. Hộp thoại **New Object - Group**, trong ô **Group name**, nhập **DA_Clients**. Trong **Group scope**, chọn **Global**, trong **Group type**, chọn **Security**, và chọn **OK**.



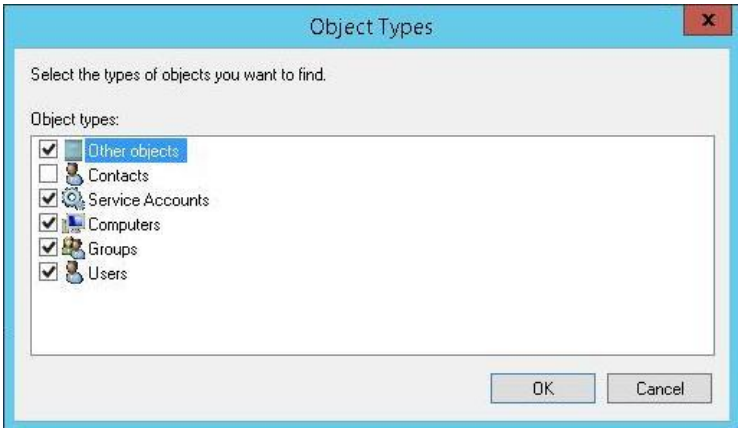
g. Nhấp đôi chuột mở group **DA_Clients**, trong hộp thoại **DA_Clients Properties**, qua tab **Members**, chọn **Add**.



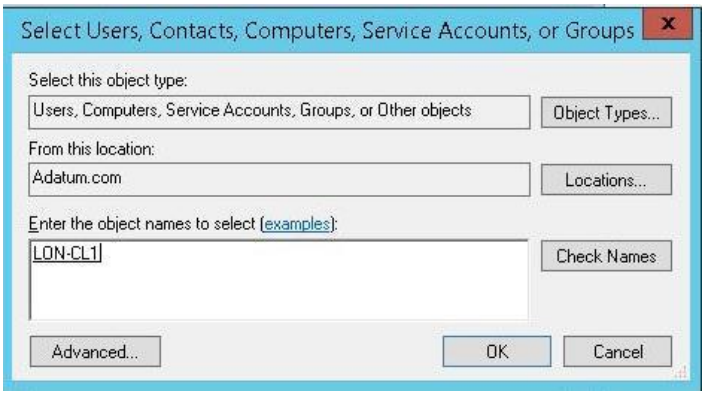
h. Hộp thoại **Select Users, Contacts, Computers, Service Accounts, or Groups**, chọn **Object Types.**



i. Hộp thoại Object Types, đánh dấu chọn **Computers**, và chọn **OK**.



j. Hộp thoại **DA_Clients Properties**, trong ô **Enter the object names to select (examples)**, nhập **LON-CL1**, chọn **OK**.



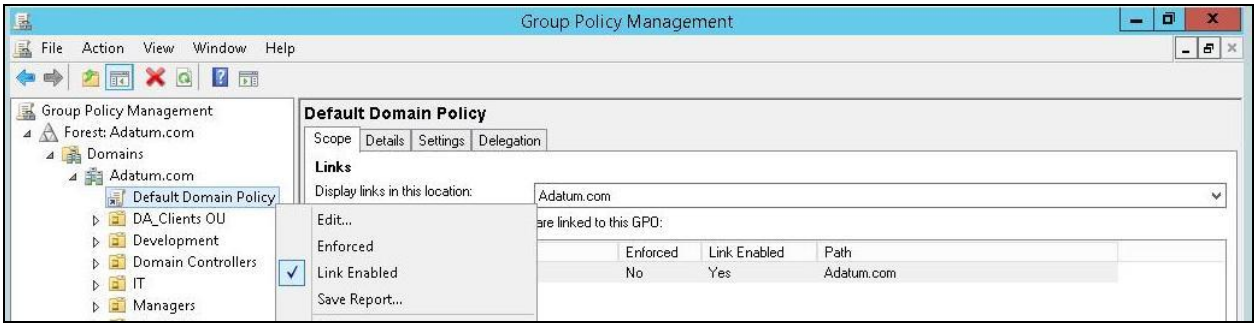
k. Trong hộp thoại **DA_Clients Properties,** kiểm tra **LON-CL1** hiển thị trong danh sách **Members**, chọn **OK**.

2. Cấu hình Firewall Rules chấp nhận gói tin ICMPv6:

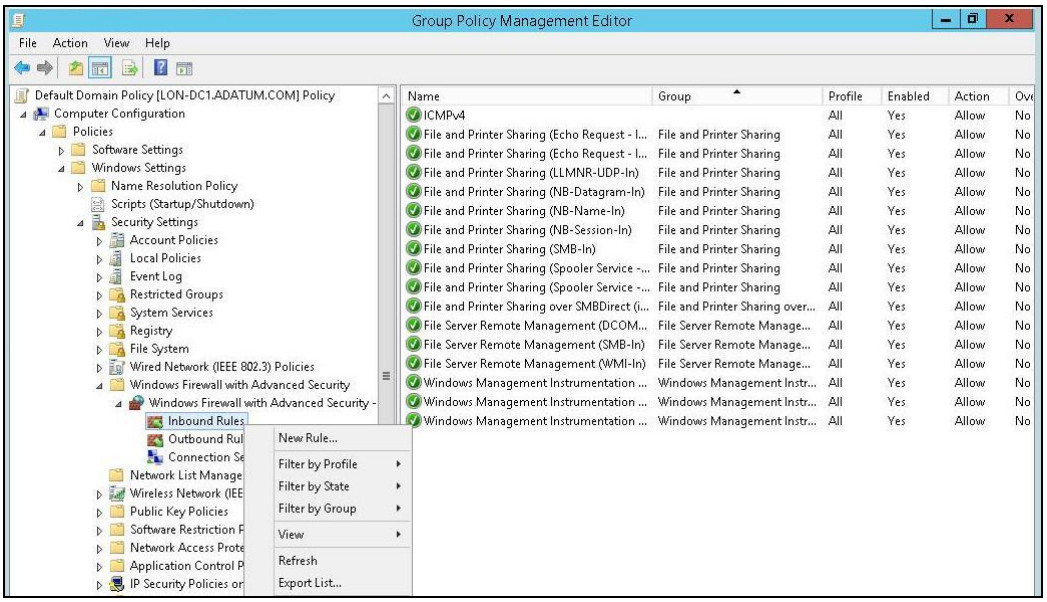
Chú ý: Bạn cấu hình Firewall Rules chấp nhận gói tin ICMPv6 để kiểm tra truy cập DirectAccess trong môi trường lab.

a. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Group Policy Management**.

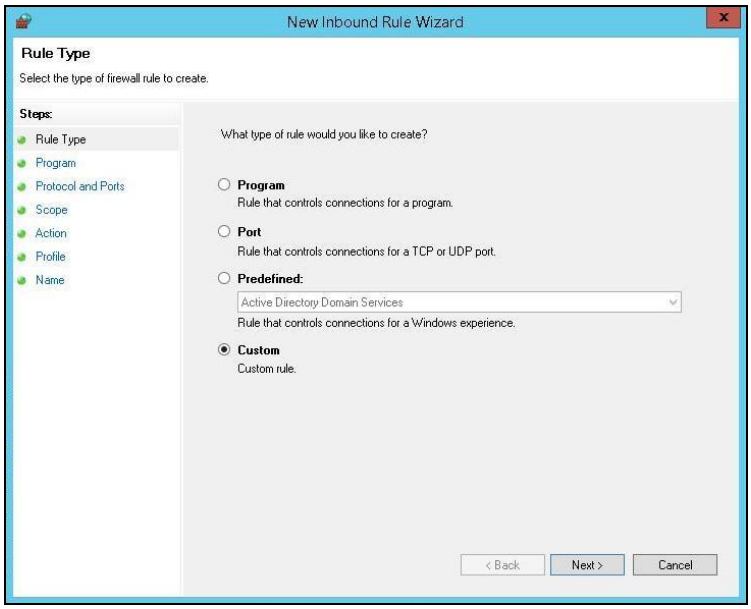
b. Cửa sổ **Group Policy Management Console**, bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, nhấn chuột phải **Default Domain Policy**, chọn **Edit**.



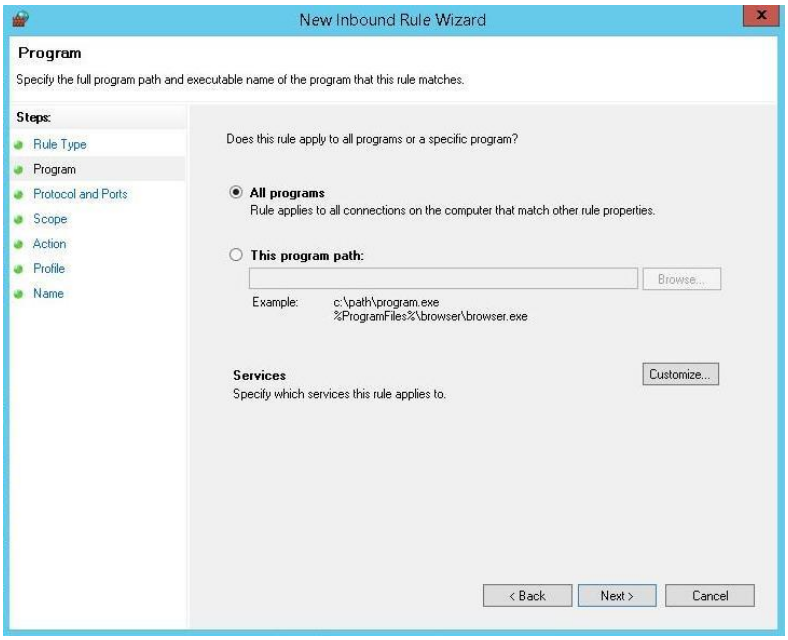
c. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Windows Firewall with Advanced Security**, bung **Windows Firewall with Advanced Security**, nhấn chuột phải **Inbound Rules**, chọn **New Rule**.



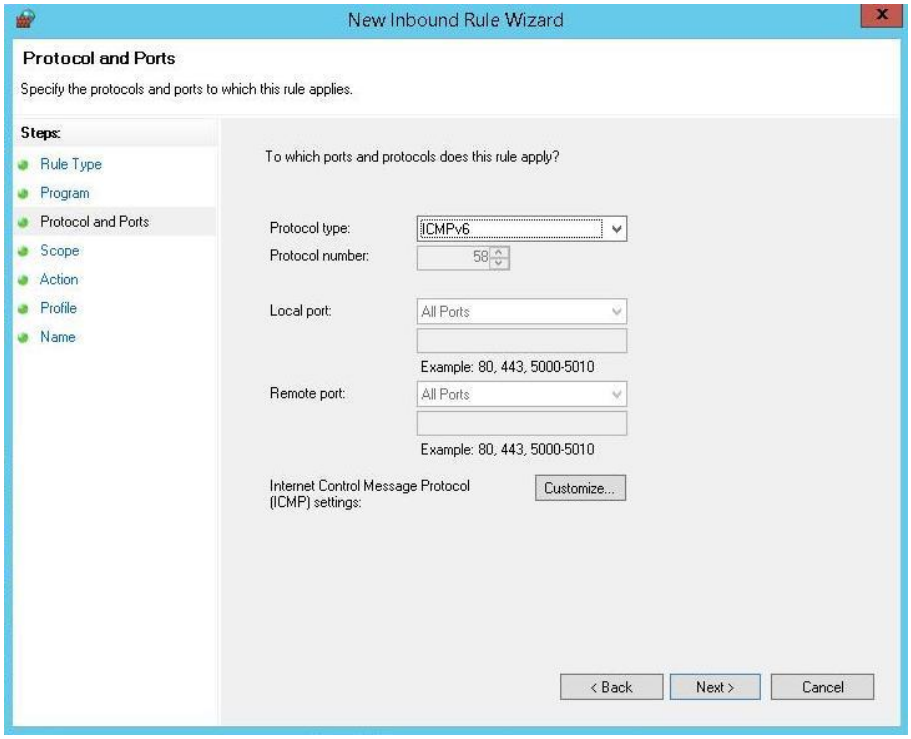
d. Cửa sổ **Rule Type**, chọn **Custom**, chọn **Next**.



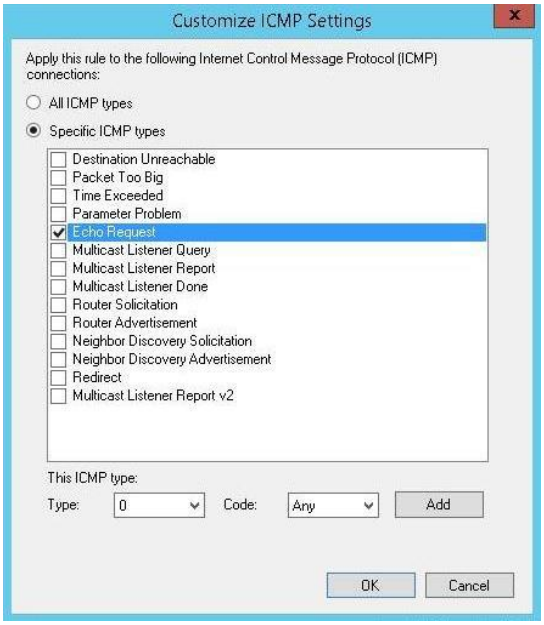
e. Cửa sổ **Program**, chọn **Next**.



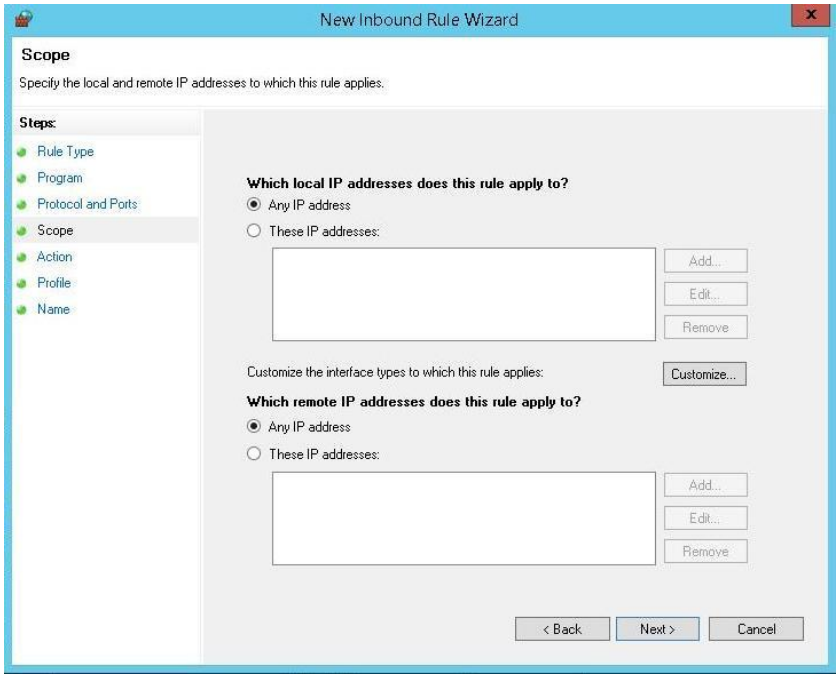
f. Cửa sổ **Protocols and Ports**, bung **Protocol type**, chọn **ICMPv6**, và chọn **Customize**.



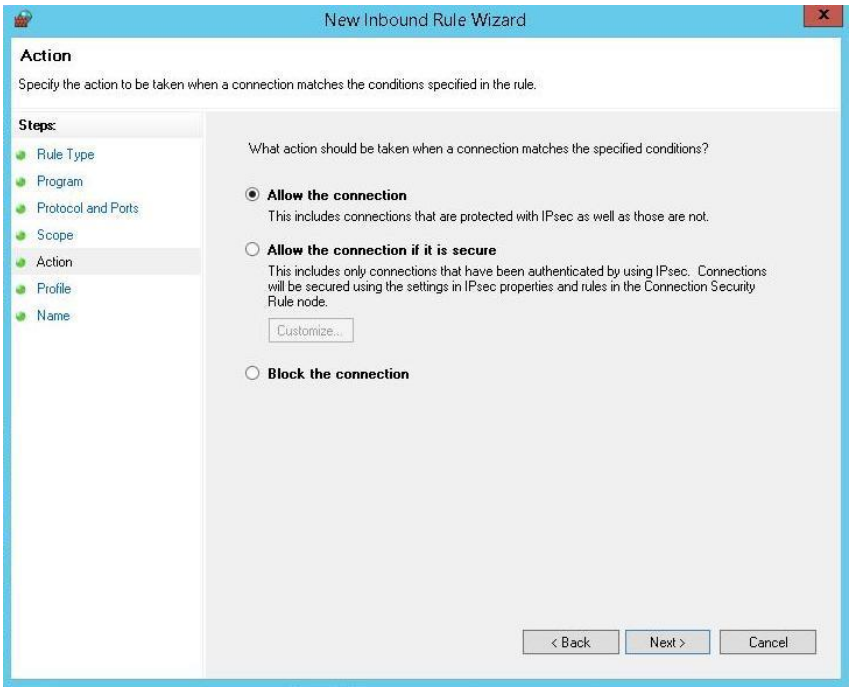
g. Hộp thoại **Customize ICMP Settings**, chọn **Specific ICMP types**, đánh dấu chọn **Echo Request**, chọn **OK**, và chọn **Next**.



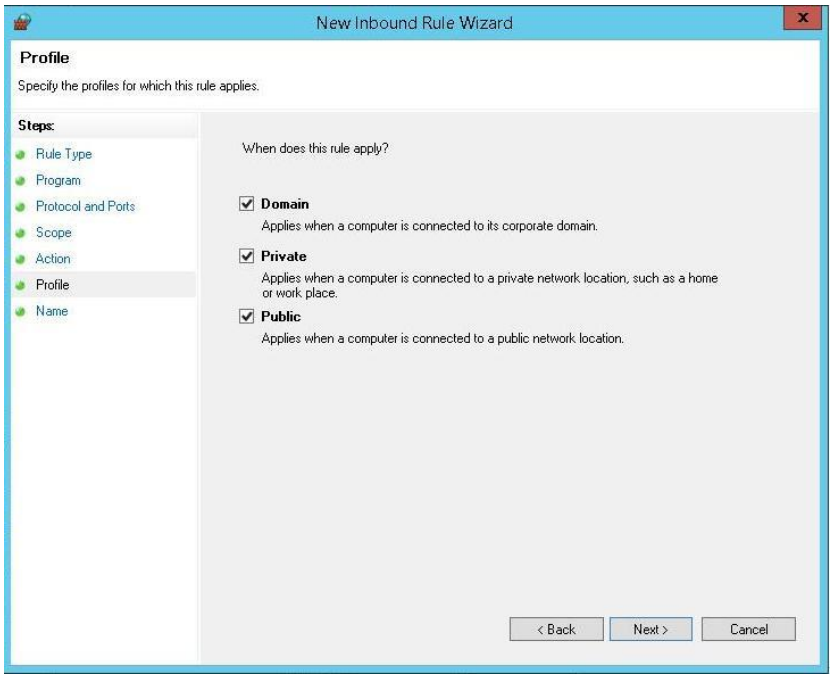
h. Cửa sổ **Scope**, chọn **Next**.



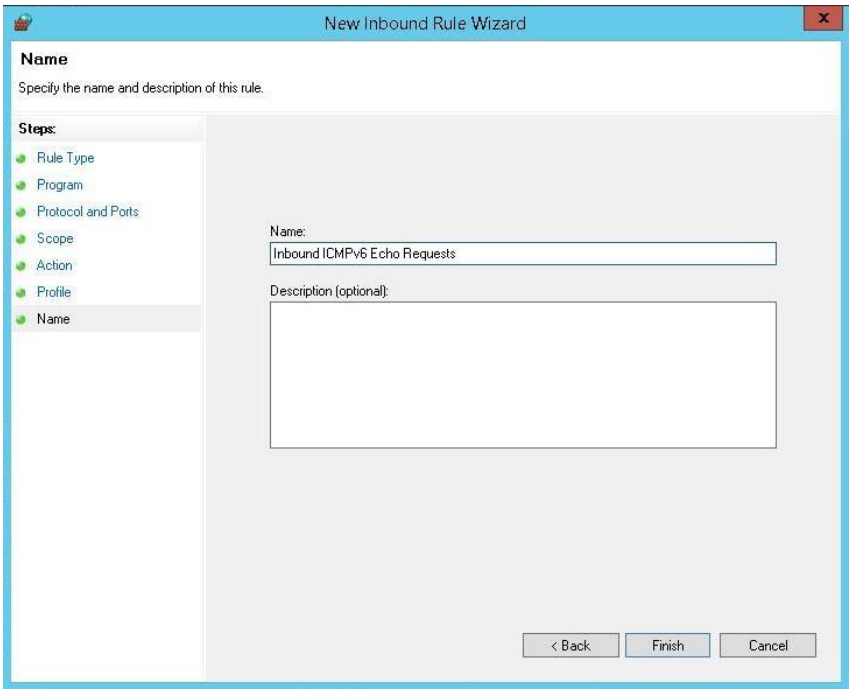
i. Cửa sổ **Action**, chọn **Next**.



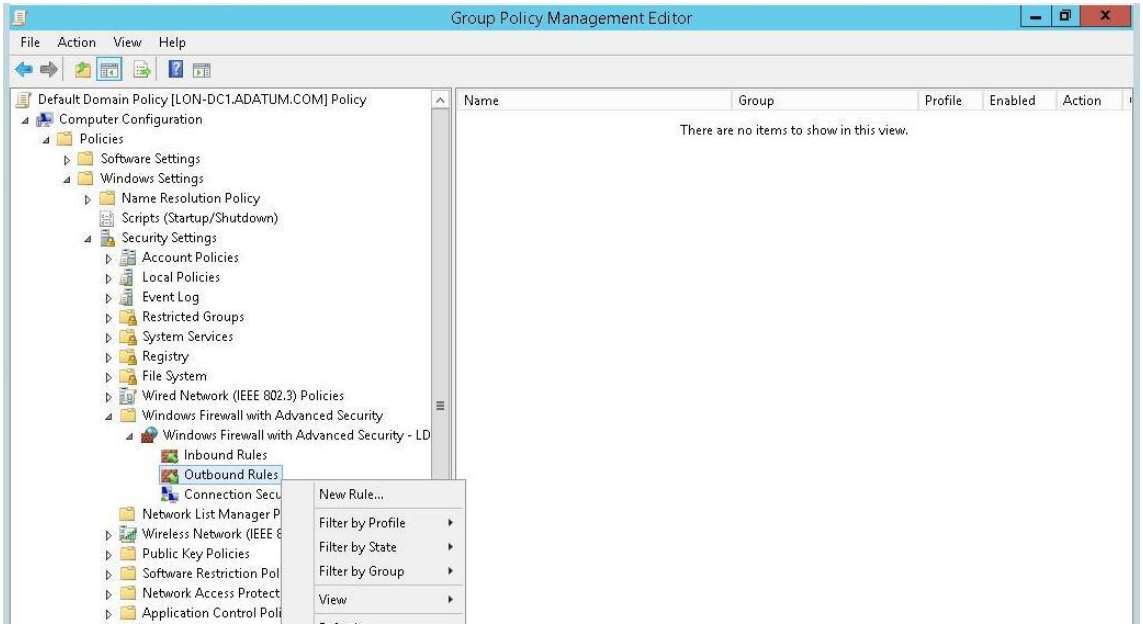
j. Cửa sổ **Profile**, chọn **Next**.



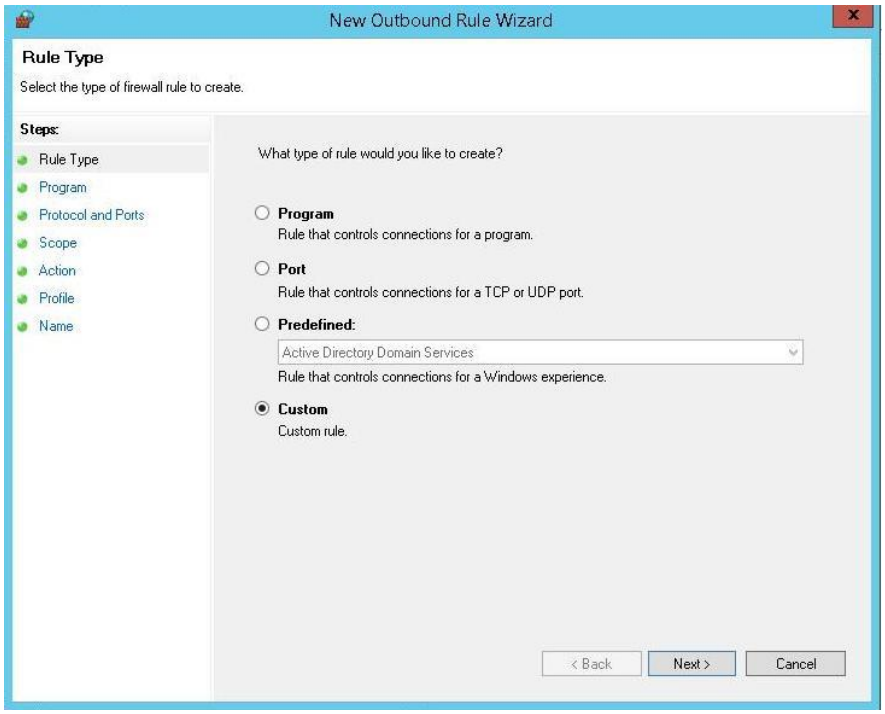
k. Cửa sổ **Name**, trong ô **Name**, nhập **Inbound ICMPv6 Echo Requests**, và chọn **Finish**.



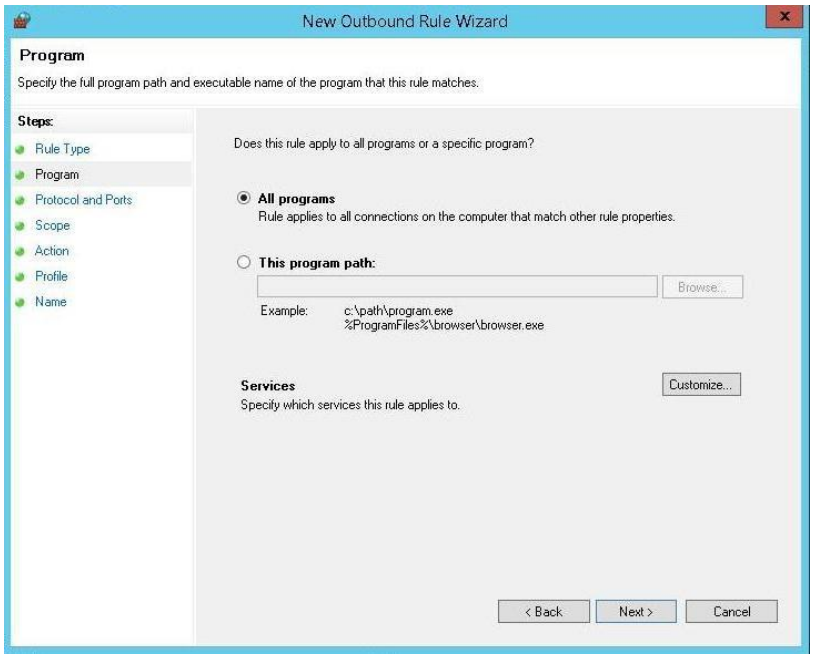
l. Trong cửa sổ **Group Policy Management Editor**, nhấn chuột phải **Outbound Rules**, chọn **New Rule**.



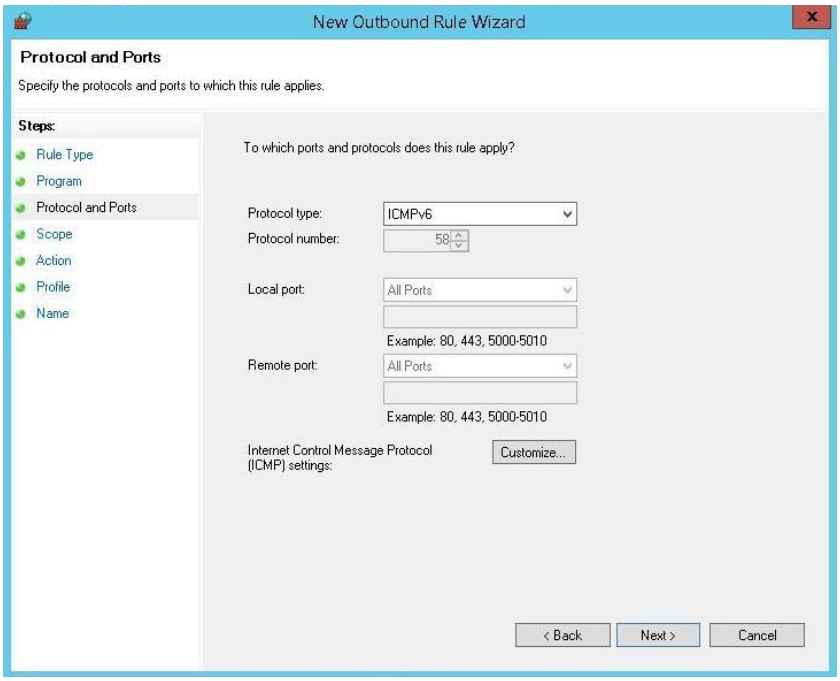
m. Cửa sổ **Rule Type**, chọn **Custom**, và chọn **Next**.



n. Cửa sổ **Program**, chọn **Next**.



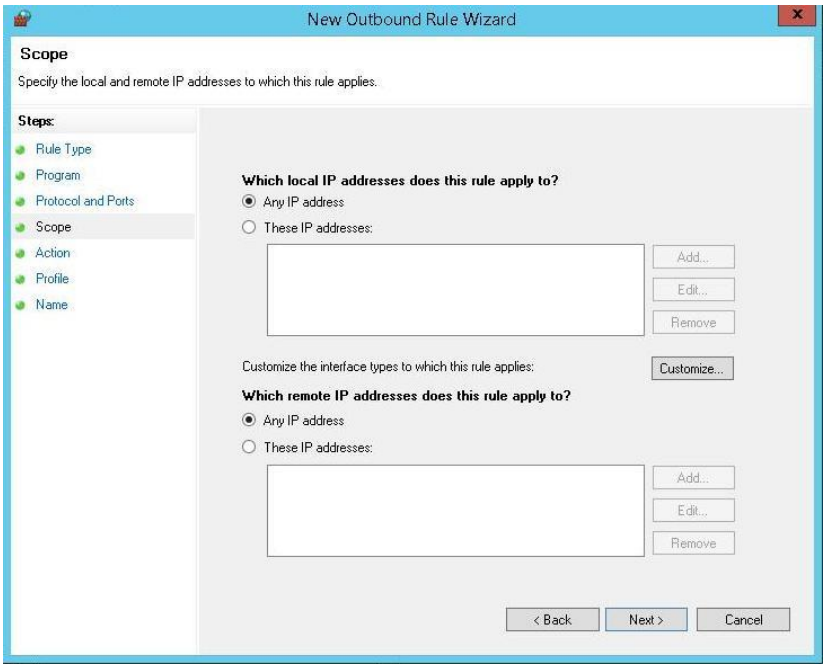
o. Cửa sổ **Protocols and Ports**, bung **Protocol type**, chọn **ICMPv6**, chọn **Customize**.



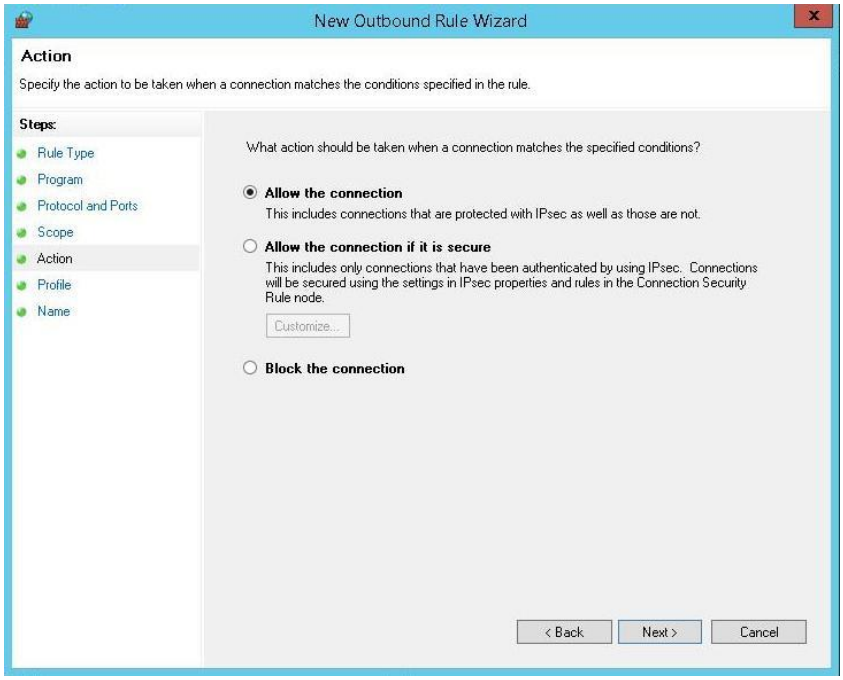
p. Hộp thoại **Customize ICMP Settings**, chọn **Specific ICMP types**, đánh dấu chọn **Echo Request**, chọn **OK**, và chọn **Next**.



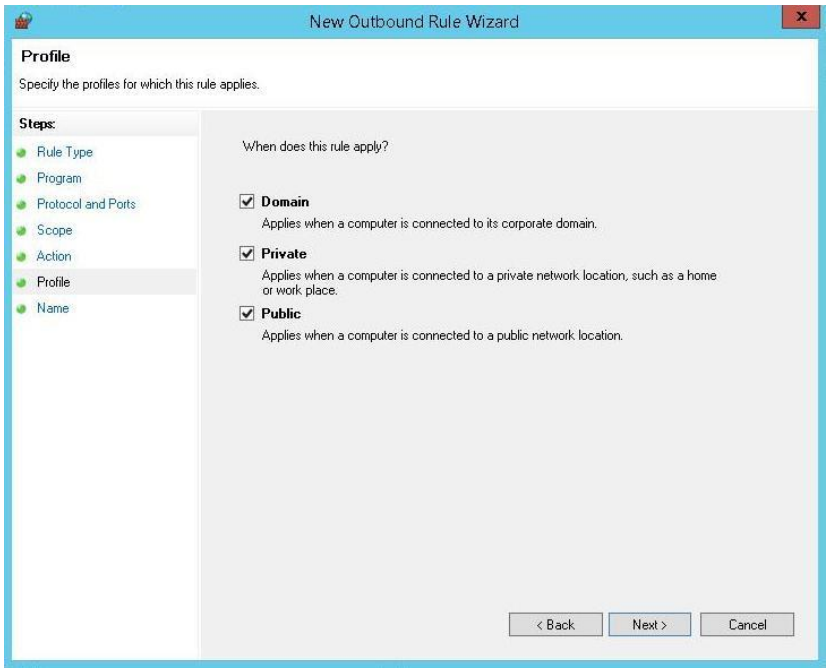
q. Cửa sổ **Scope**, chọn **Next**.



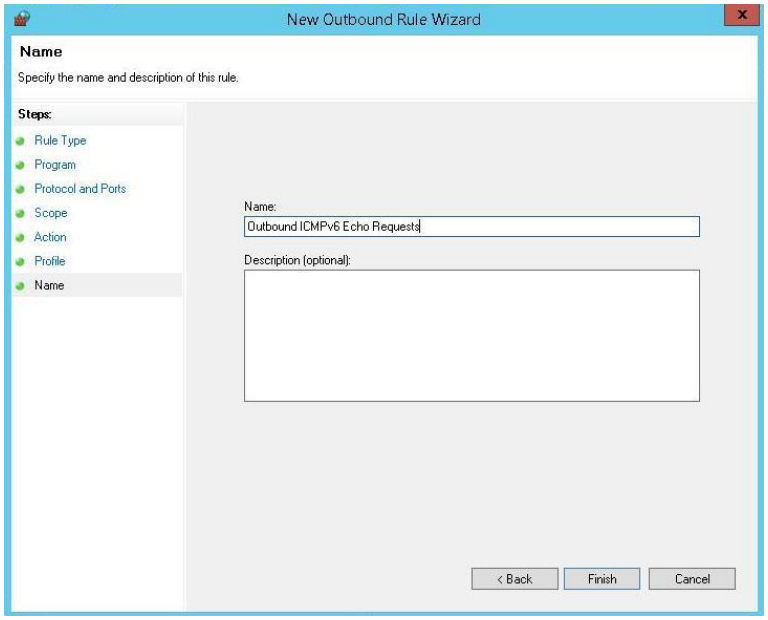
r. Cửa sổ **Action**, chọn **Allow the connection**, và chọn **Next**.



s. Cửa sổ **Profile**, chọn **Next**.



t. Cửa sổ **Name**, trong ô **Name**, nhập **Outbound ICMPv6 Echo Requests**, và chọn **Finish**.

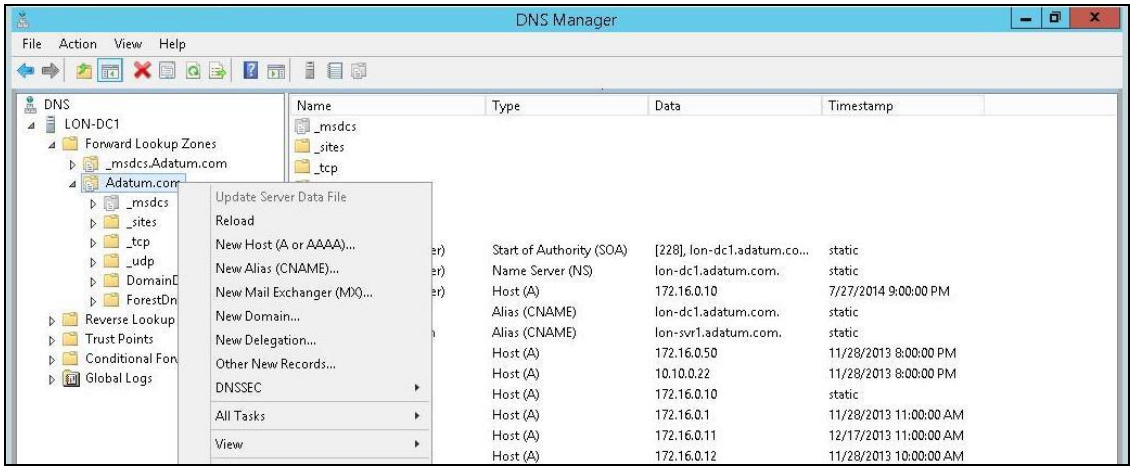


u. Tắt **Group Policy Management Editor** và **Group Policy Management Console.**

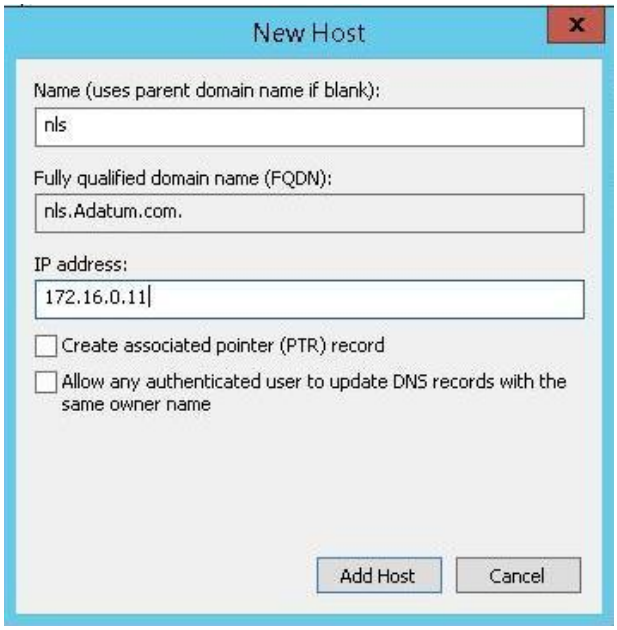
3. Tạo DNS records:

a. Trong **Server Manager**, bung menu **Tools**, mở **DNS**.

b. Trong cửa sổ **DNS Manager**, bung **LON-DC1**, bung **Forward Lookup Zones**, nhấn chuột phải **Adatum.com**, chọn **New Host (A or AAAA)**.



c. Trong ô **Name**, nhập **nls**. Trong ô **IP address**, nhập **172.16.0.11**, chọn **Add Host**, chọn **OK** 2 lần, và chọn **Done**



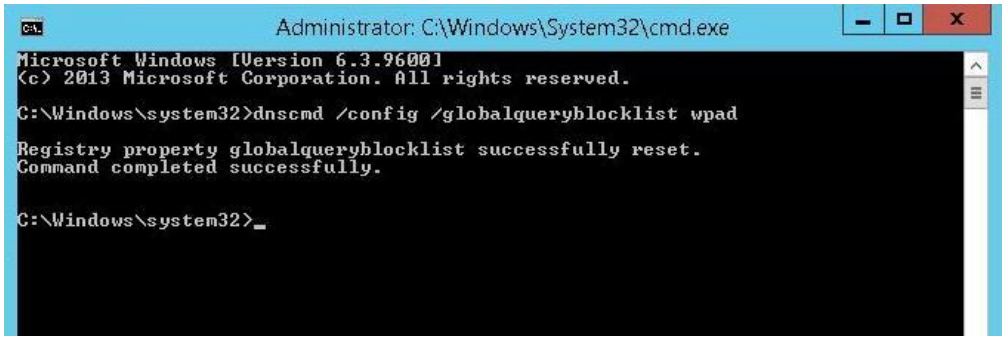
d. Tắt **DNS Manager**.

4. Gở bỏ **ISATAP** trong danh sách **DNS global query block list**:

a. Bung Start menu, gõ **cmd.exe**, nhấn Enter.

b. Trong Command Prompt, gõ lệnh:

dnscmd /config /globalqueryblocklist wpad

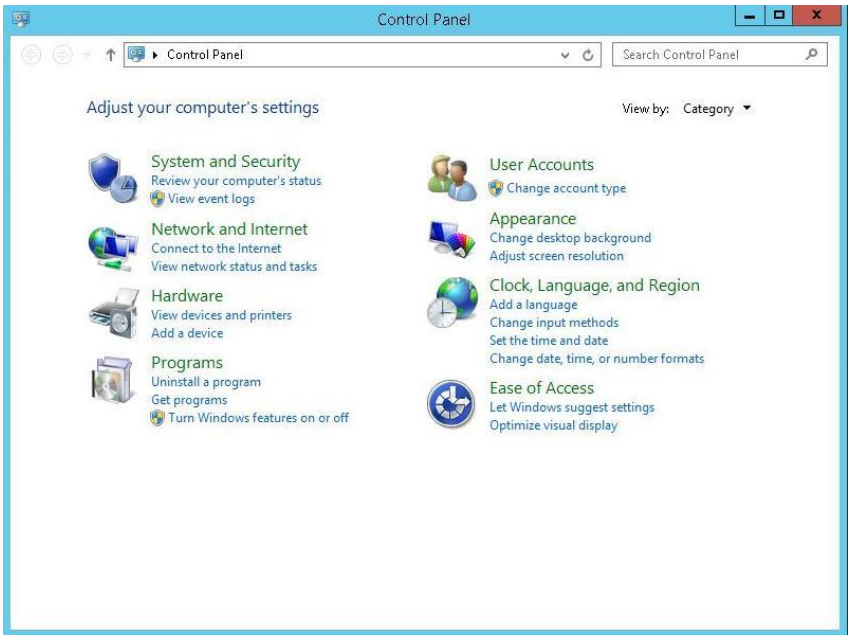


c. Tắt Command Prompt.

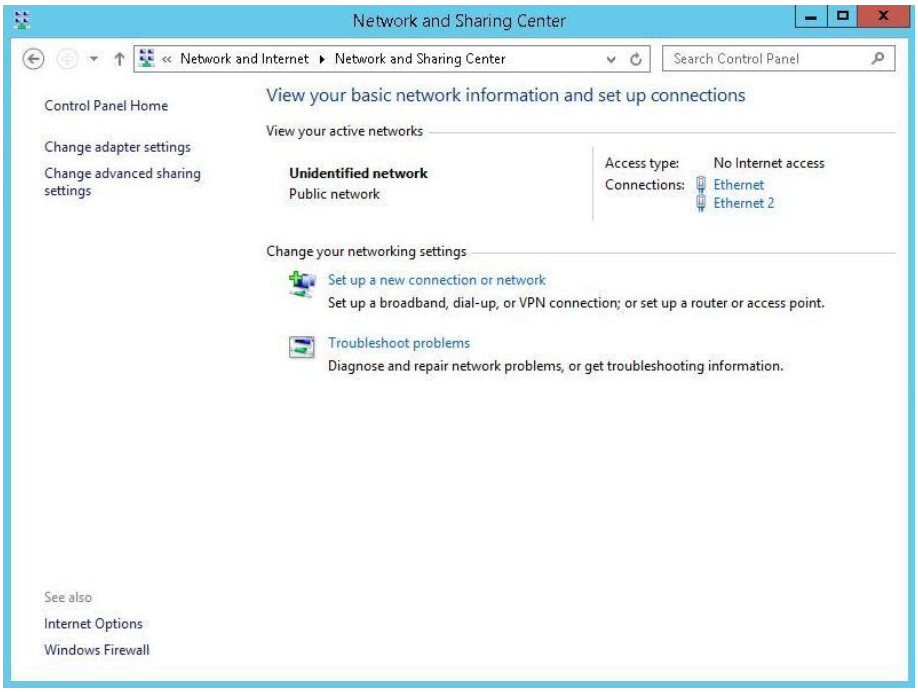
5. Cấu hình DNS suffix trên máy LON-RTR:

a. Qua máy **LON-RTR.**

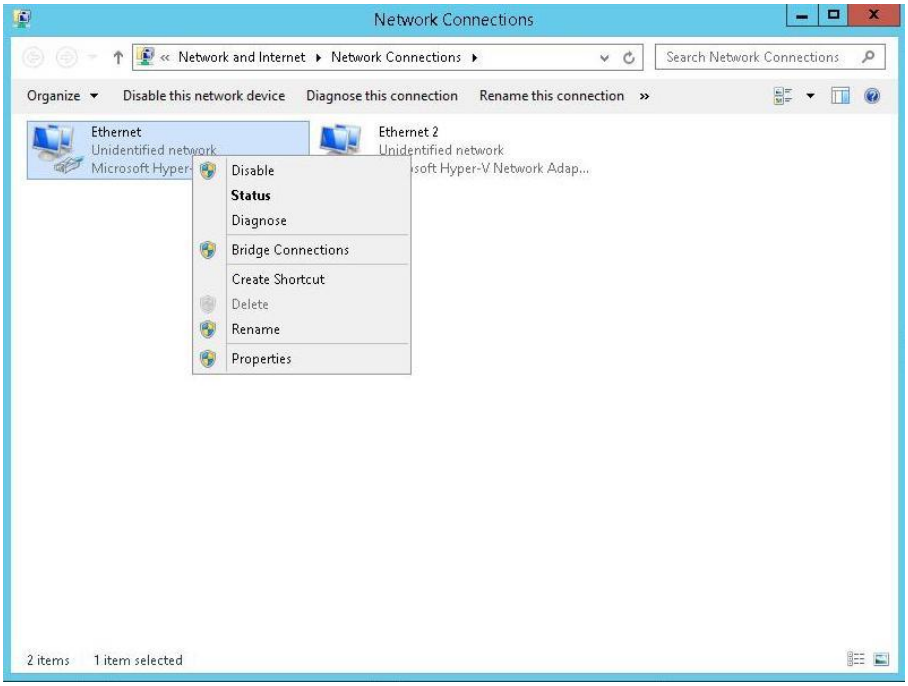
b. Mở **Control Panel**, chọn **View network status and tasks**.



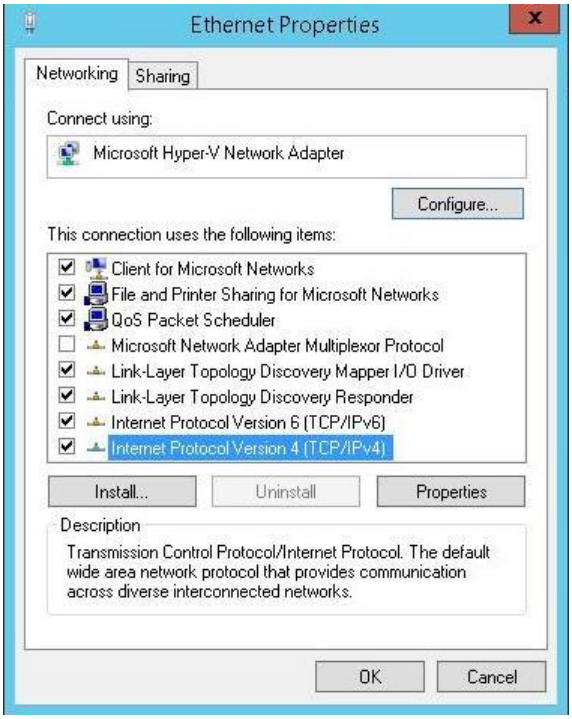
c. Trong cửa sổ **Network and Sharing Center**, chọn **Change adapter settings**.



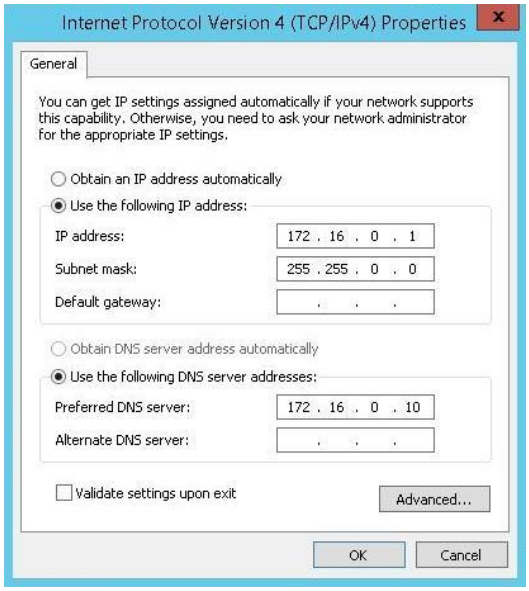
d. Cửa sổ **Network Connection**, nhấn chuột phải **Ethernet**, chọn **Properties**.



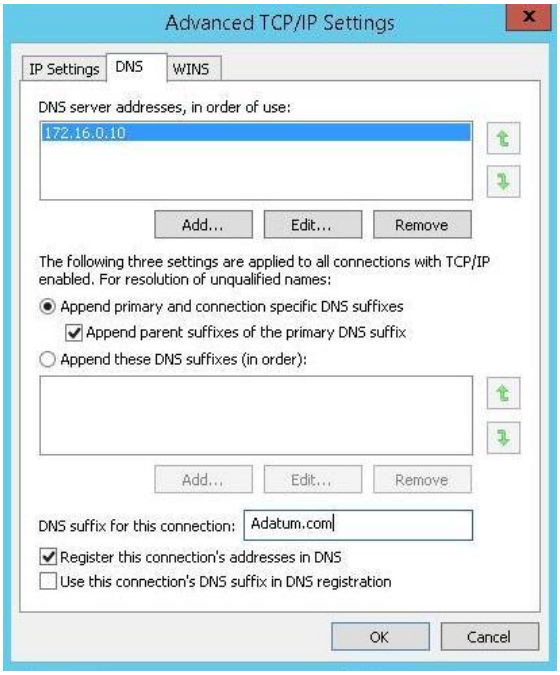
e. Hộp thoại **Ethernet Properties**, nhấp đôi chuột **Internet Protocol Version 4 (TCP/IPv4)**.



f. Hộp thoại **Internet Protocol Version 4 (TCP/IPv4)**, chọn **Advanced**.

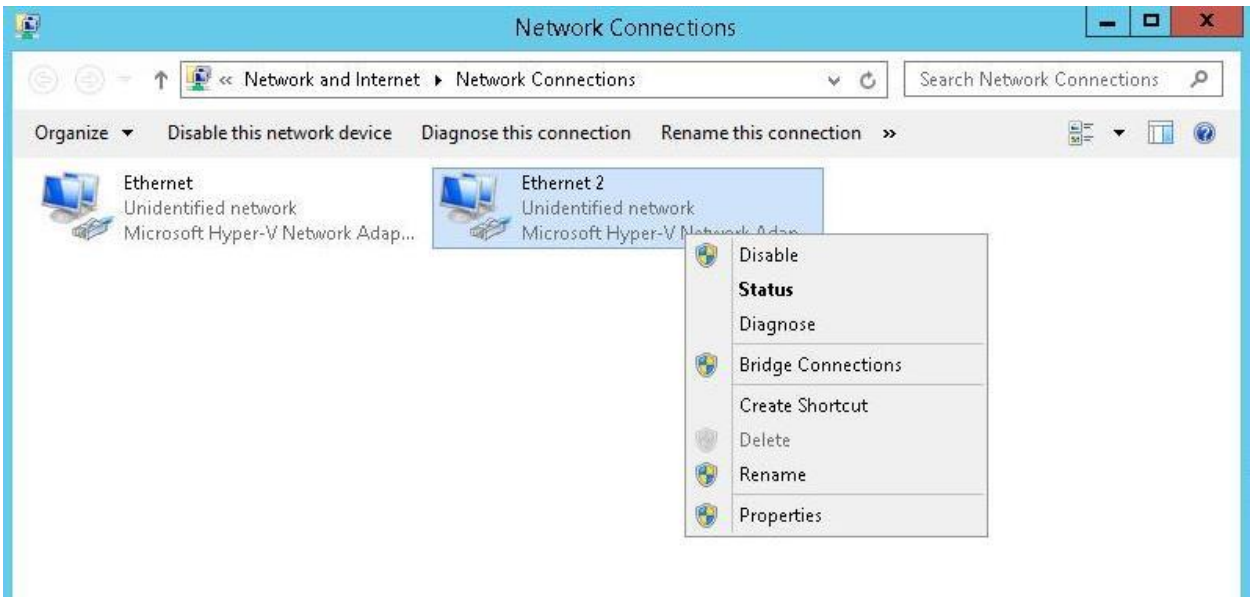


g. Qua tab **DNS**, trong ô **DNS suffix for this connection**, nhập **Adatum.com**, và chọn **OK** 3 lần.

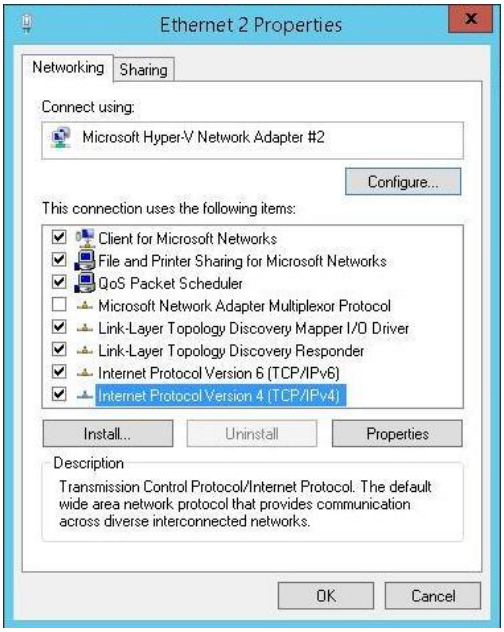


6. Cấu hình lại thông số TCP/IP của card mạng **Ethernet 2** trên máy **LON-RTR**:

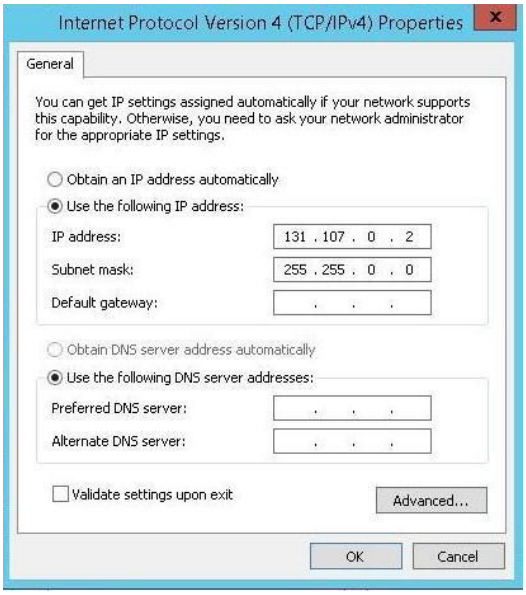
a. Trong cửa sổ **Network Connection**, nhấn chuột phải **Ethernet 2**, chọn **Properties**.



b. Hộp thoại **Ethernet 2 Properties**, nhấp đôi chuột **Internet Protocol Version 4 (TCP/IPv4)**.



c. Hộp thoại **Internet Protocol Version 4 (TCP/IPv4)**, trong ô **IP address**, nhập **131.107.0.2**, trong ô **Subnet mask**, nhập **255.255.0.0**, chọn **OK** 3 lần.



d. Tắt cửa sổ **Network Connections**.

Bước 2. Cấu hình Certificates.

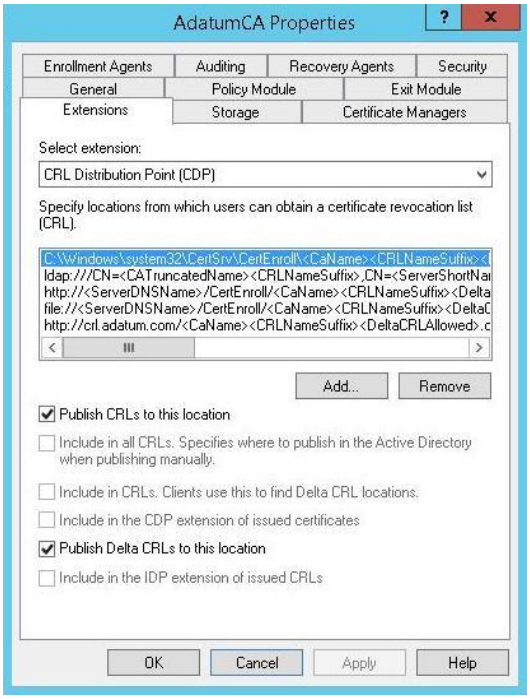
1. Cấu hình chức năng phân phối danh sách **CRL**:

a. Trên máy **LON-DC1**, mở **Server Manager**, bung menu **Tools**, mở **Certification Authority**.

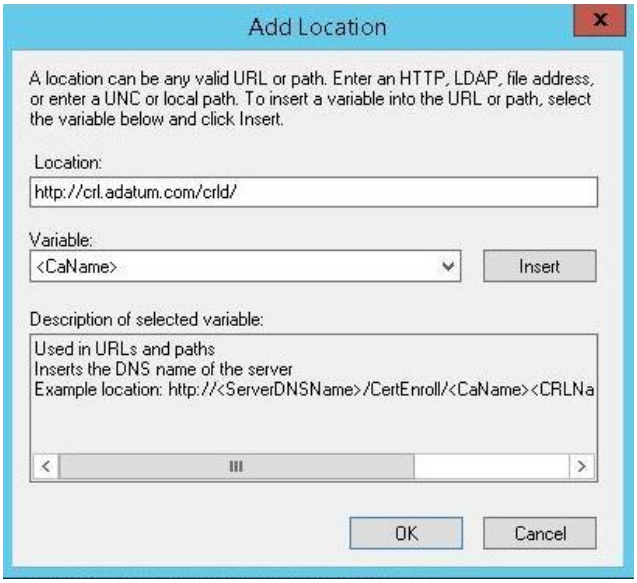
b. Trong cửa sổ **Certification Authority**, nhấn chuột phải **AdatumCA**, chọn **Properties**.



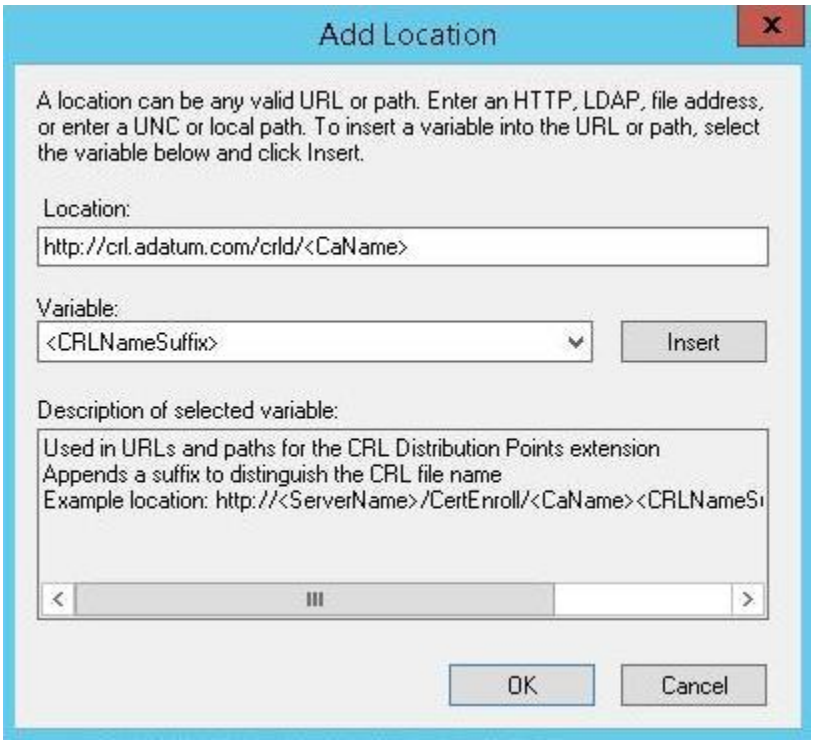
c. Trong hộp thoại **AdatumCA Properties**, qua tab **Extensions**, chọn **Add**



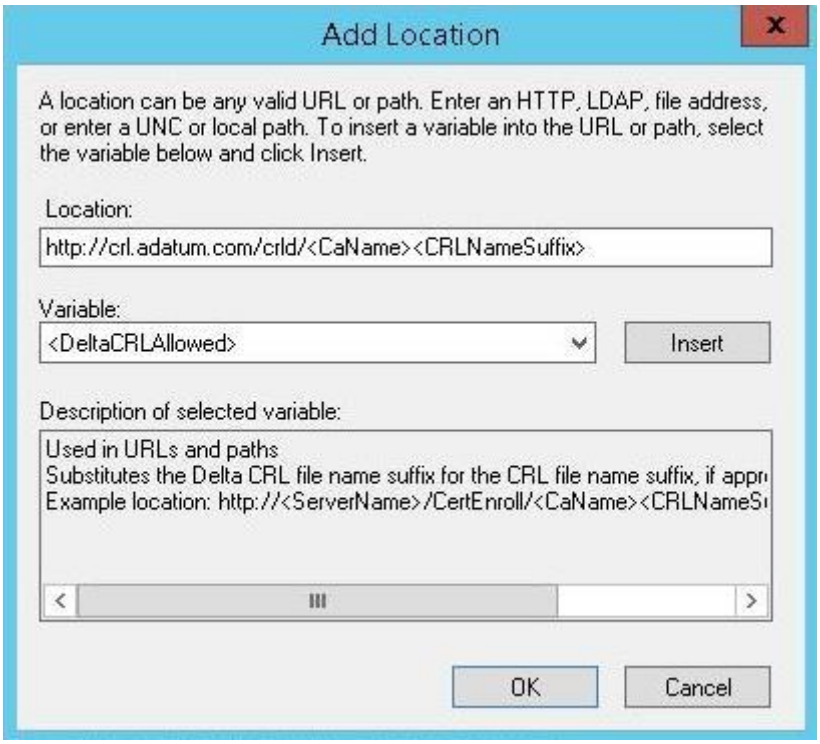
d.Hộp thoại **Add Location**, trong ô **Location**, nhập **http://crl.adatum.com/crld/**, bung ô **Variable**, chọn **<CaName>**, và chọn **Insert**.



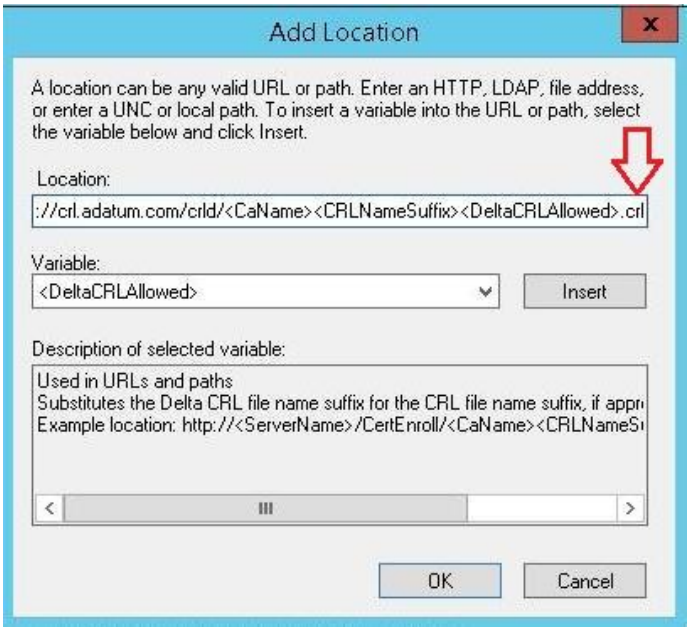
e. Bung ô **Variable**, chọn **<CRLNameSuffix>**, và chọn **Insert**.



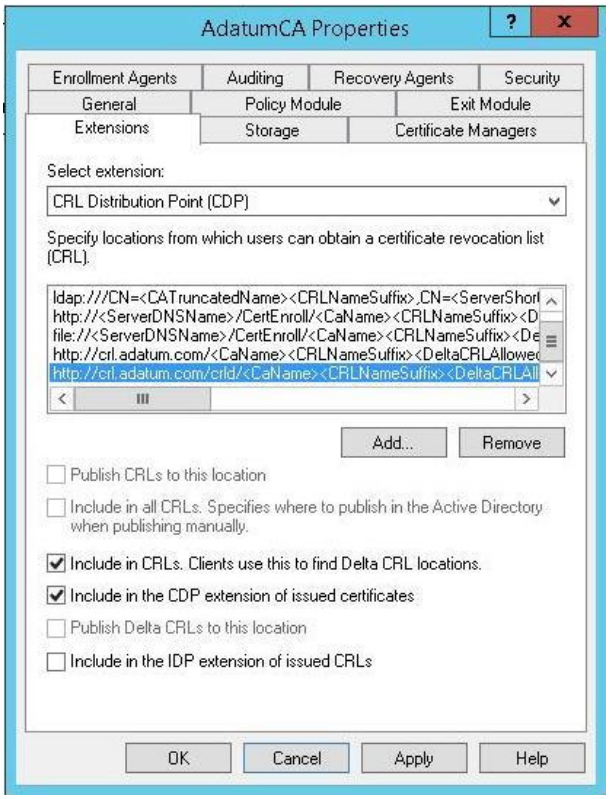
f. Bung ô **Variable**, chọn **<DeltaCRLAllowed>**, và chọn **Insert**.



g. Trong ô **Location**, đưa con trỏ về cuối đường dẫn, nhập **.crl**, chọn **OK**.



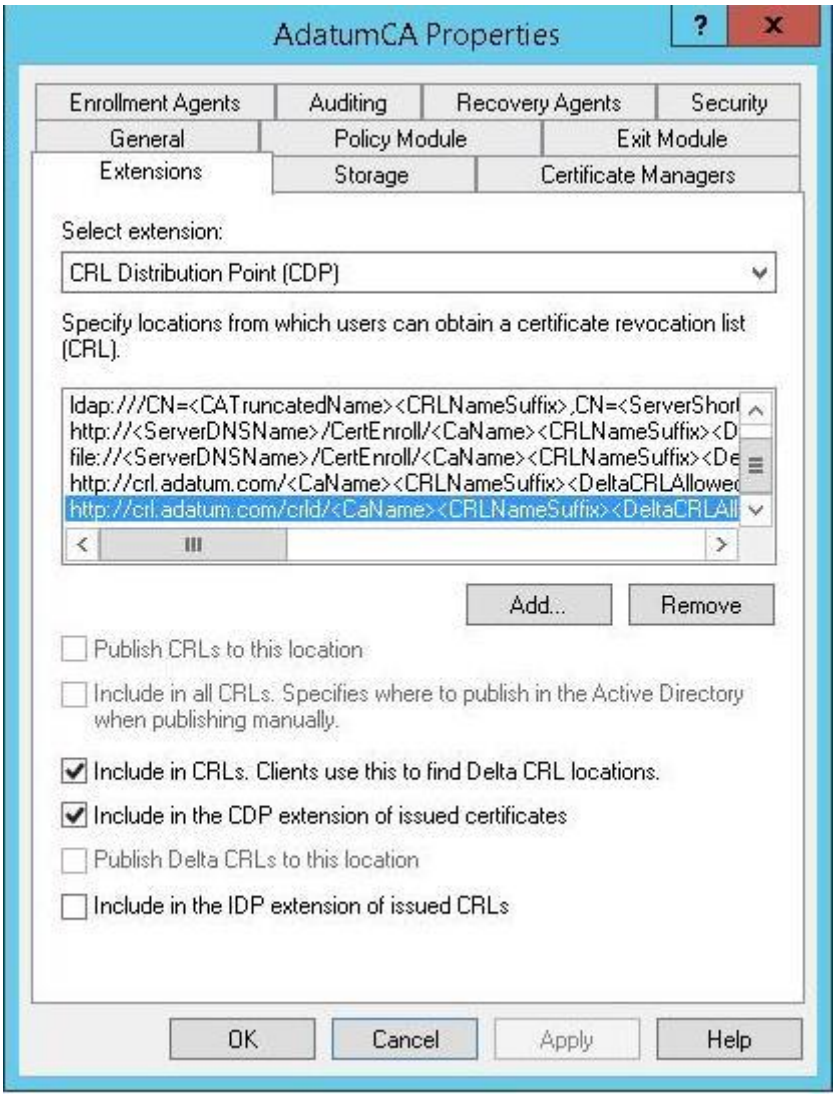
h. Trong tab **Extensions**, đánh dấu chọn cả 2 ô **Include in CRLs. Clients use this to find Delta CRL locations** và **Include in the CDP extension of issued certificates**, chọn **Apply**.



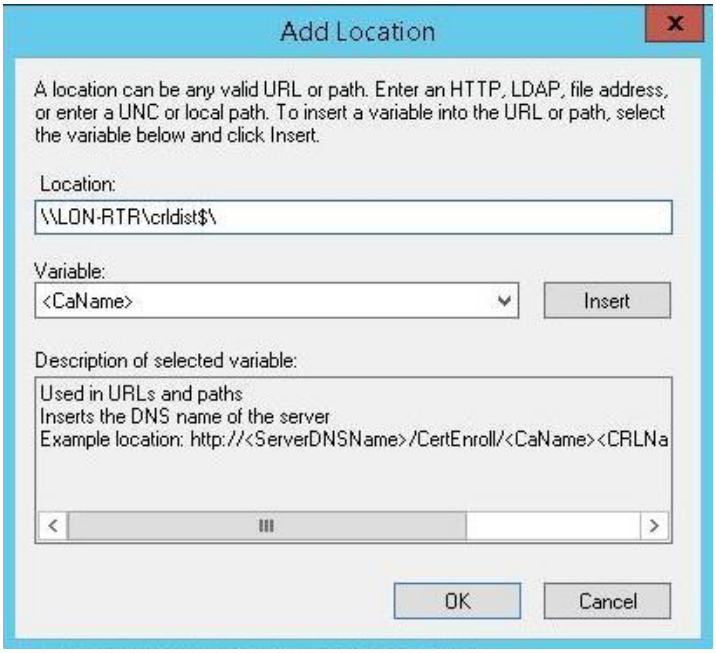
i. Hộp thoại yêu cầu khởi động lại dịch vụ **Active Directory Certificate Services**, chọn **No**.



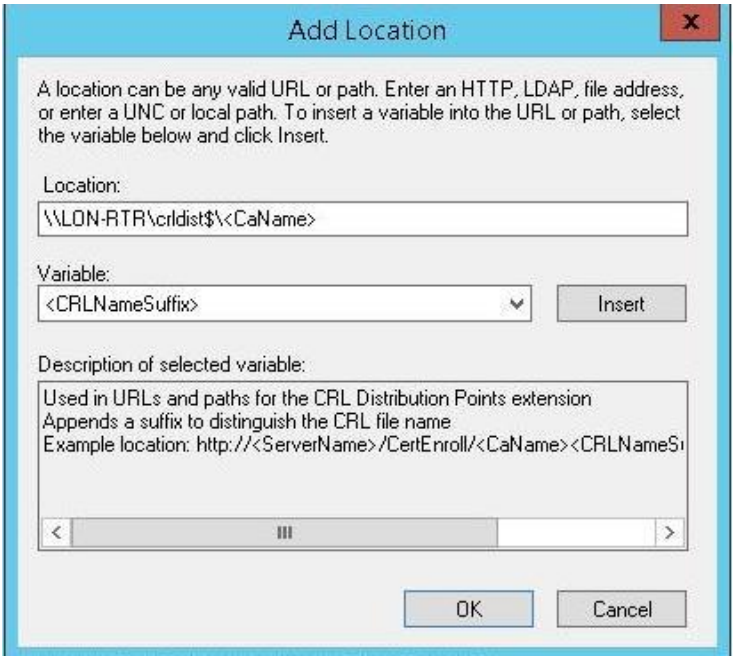
j. Trong tab **Extensions,** chọn **Add**.



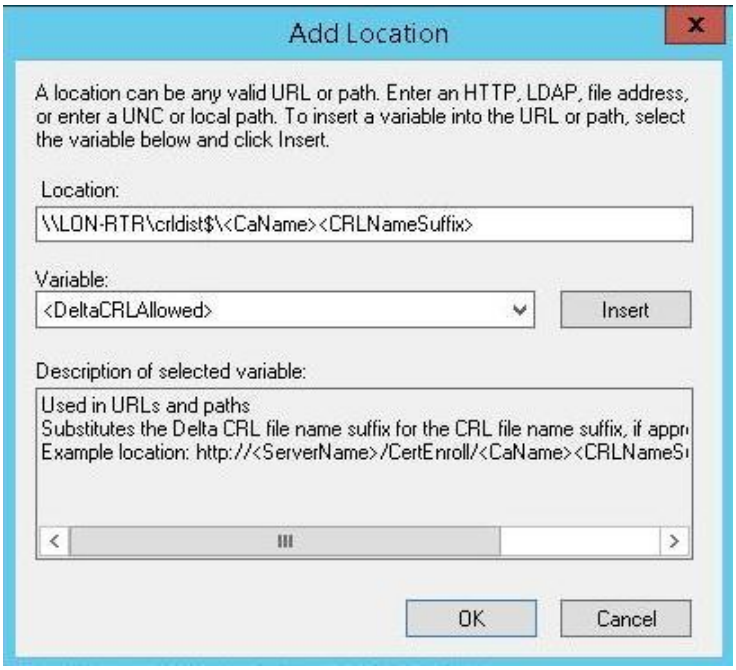
k. Hộp thoại **Add Location**, trong ô **Location**, nhập **\\LON-RTR\crldist$**, bung ô **Variable**, chọn **<CaName>**, và chọn **Insert**.



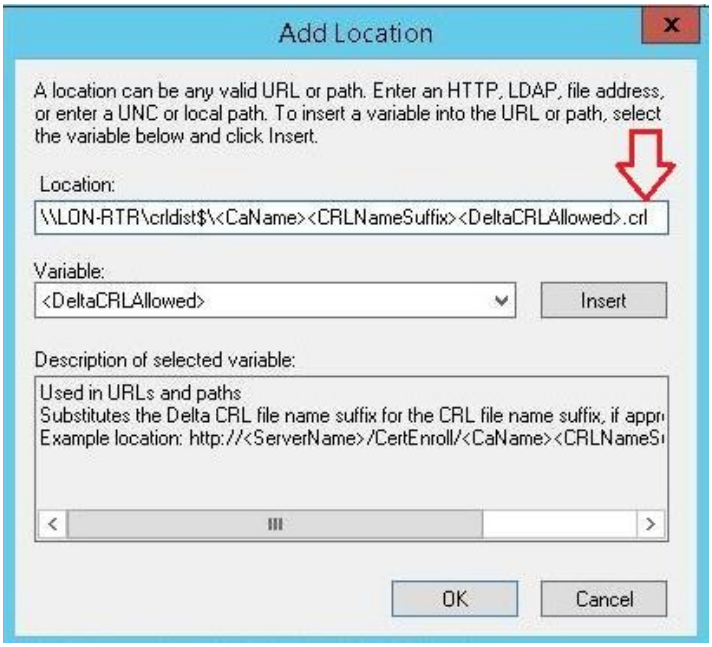
l. Bung ô **Variable**, chọn **<CRLNameSuffix>**, và chọn **Insert**.



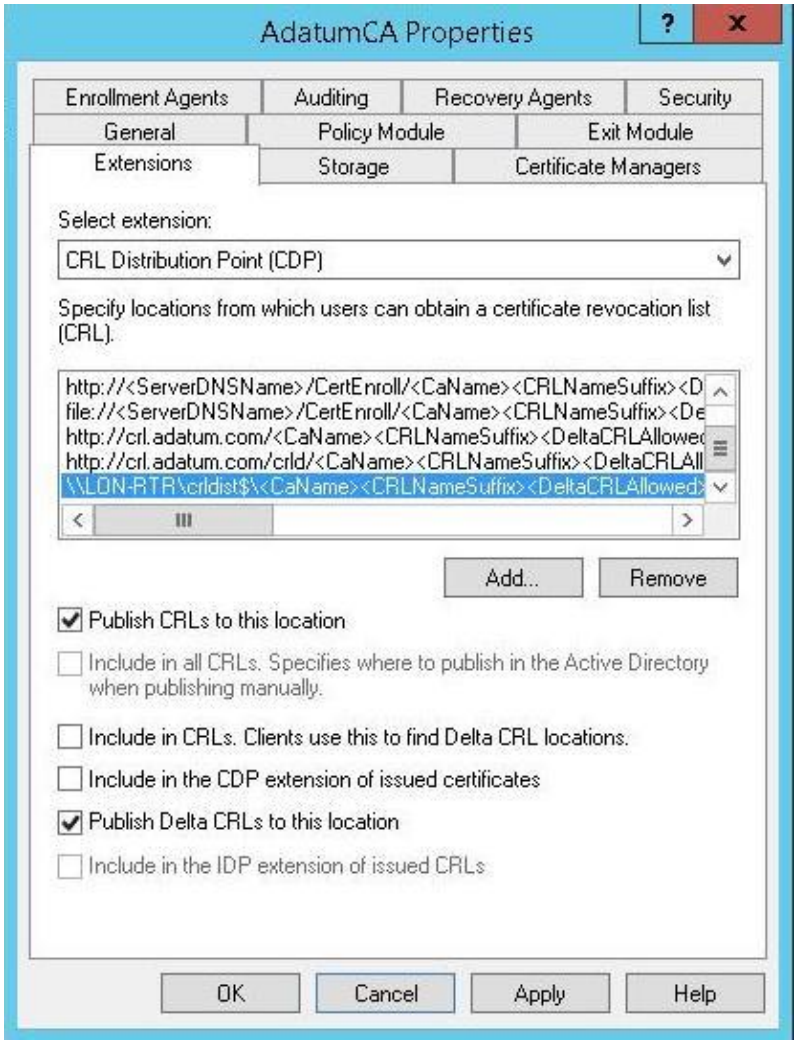
m. Bung ô **Variable**, chọn **<DeltaCRLAllowed>**, và chọn **Insert**.



n. Trong ô **Location**, đưa con trỏ về cuối đường dẫn, nhập **.crl**, chọn **OK**.



o. Trong tab **Extentions**, dánh dấu chọn cả 2 ô **Publish CRLs to this location** và **Publish Delta CRLs to this location**, và chọn **OK**.

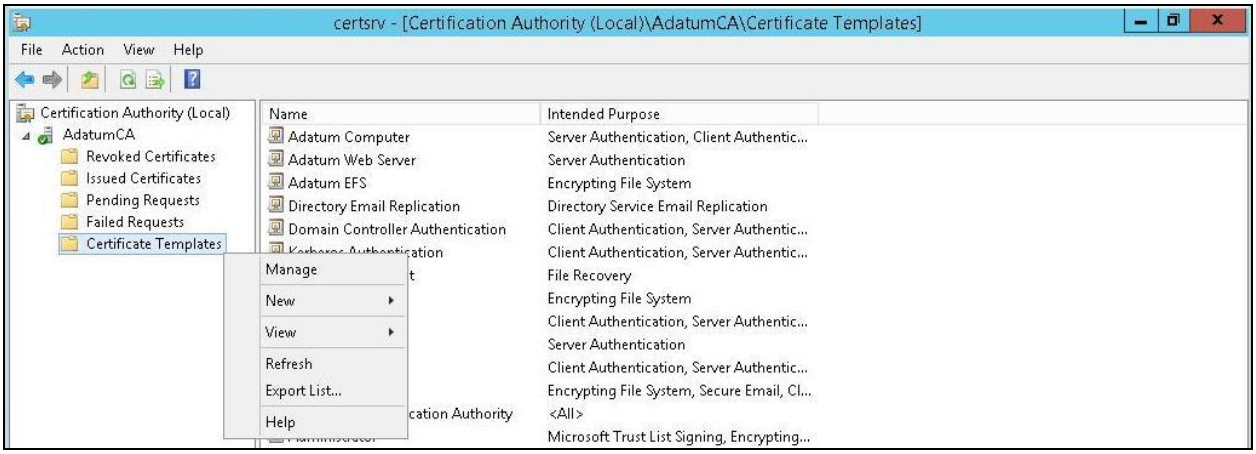


p. Hộp thoại yêu cầu khởi động lại dịch vụ **Active Directory Certificate Services** ,chọn **Yes.**

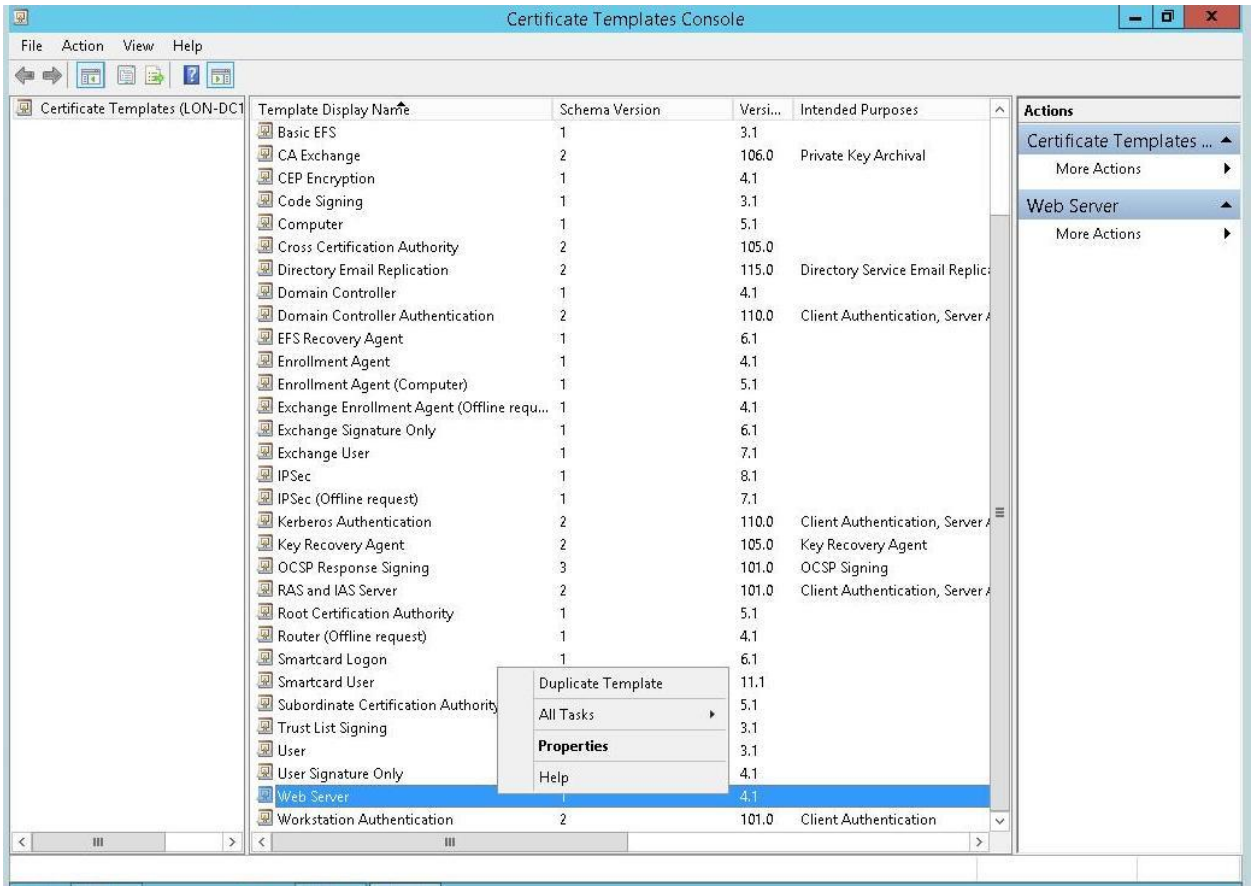


2. Tạo Web Server Certificate:

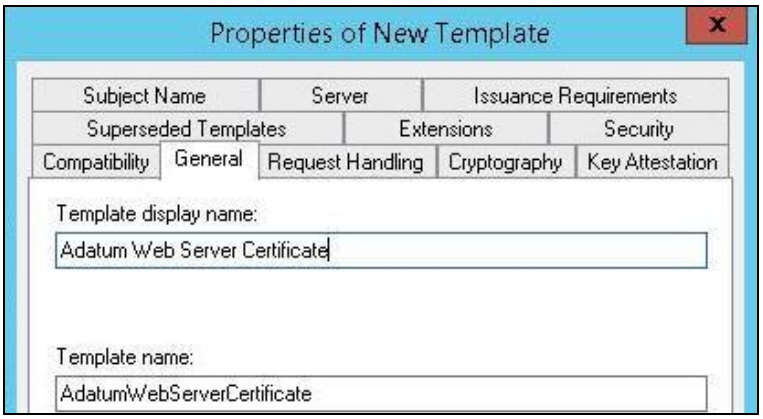
a. Trong cửa sổ **Certification Authority**, bung **AdatumCA**, nhấn chuột phải **Certificate Templates**, chọn **Manage**.



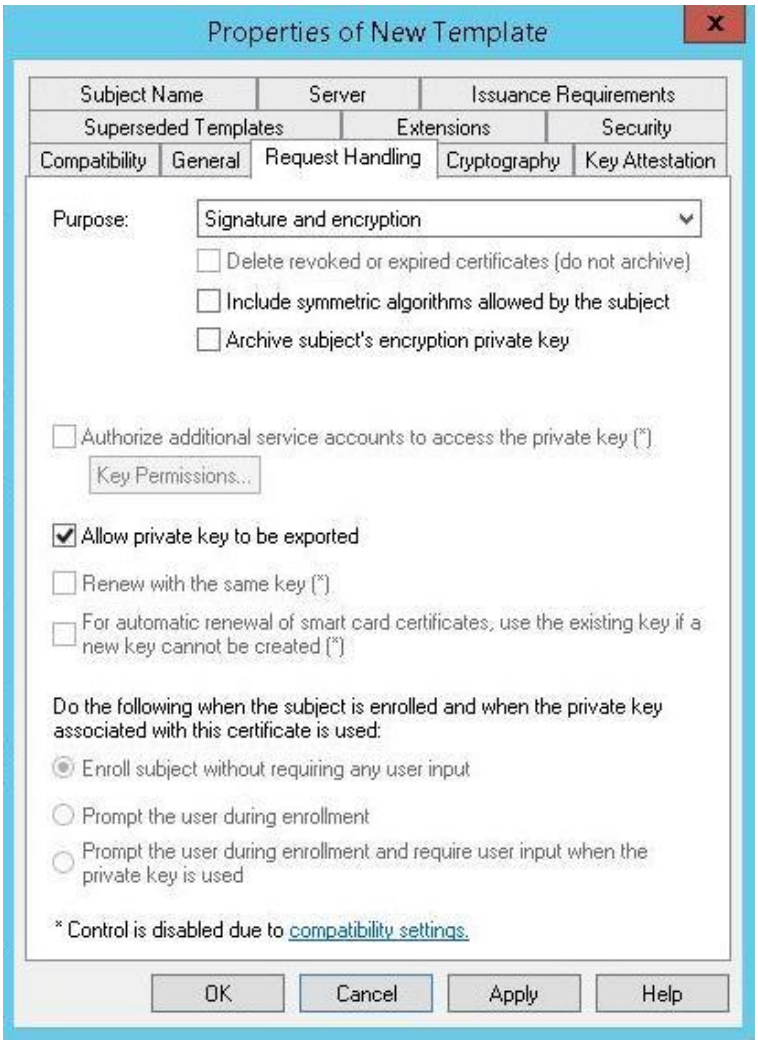
b. Cửa sổ **Certificate Templates**, nhấn chuột phải **Web Server**, chọn **Duplicate Template**.



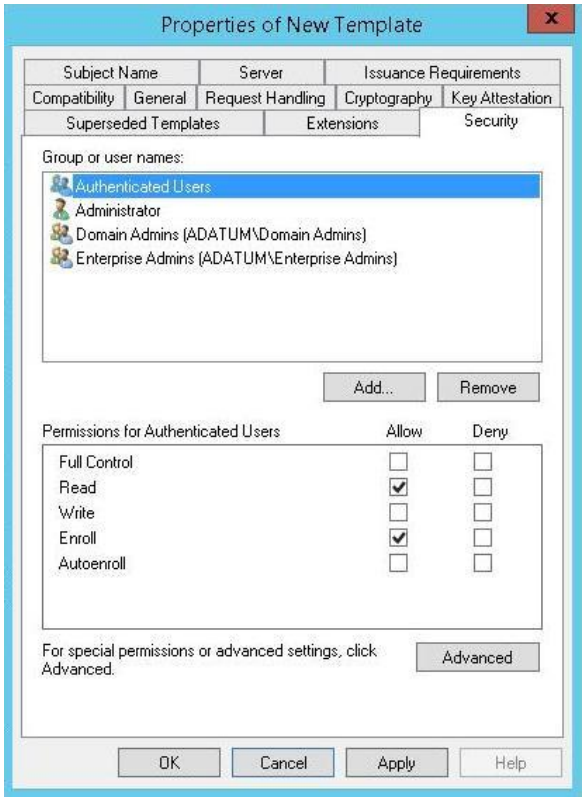
c. Qua tab **General**, trong ô **Template display name**, nhập **Adatum Web Server Certificate**.



d. Qua tab **Request Handling**, chọn **Allow private key to be exported**.

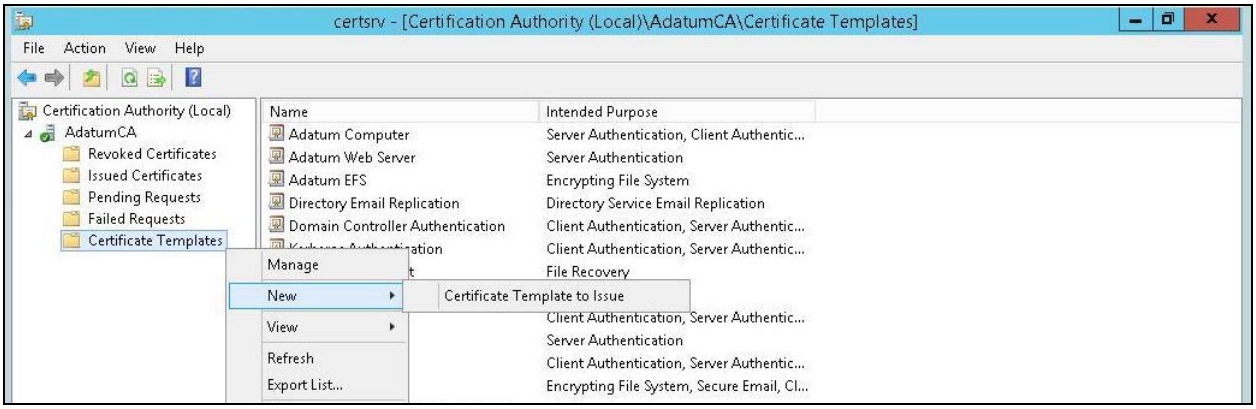


e. Qua tab **Security**, chọn **Authenticated Users**, đánh dấu chọn thêm ô **Enroll** ở cột **Allow**, chọn **OK**.

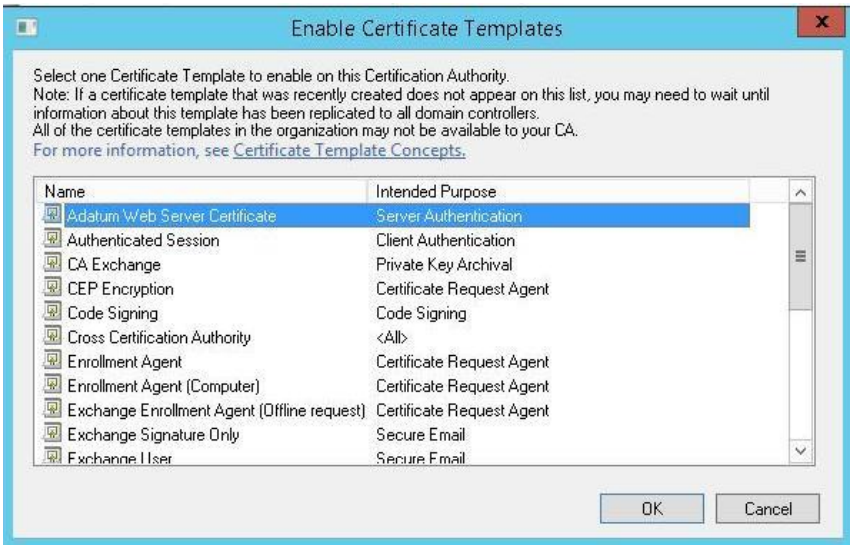


f. Tắt cửa sổ **Certificate Templates**.

g. Trong cửa sổ **Certification Authority**, nhấn chuột phải **Certificate Templates**, chọn **New**, và chọn **Certificate Template to Issue**.



h. Chọn **Adatum Web Server Certificate**, và chọn **OK**.



i. Trong cửa sổ **Certification Authority**, nhấn chuột phải **AdatumCA**, bung **All Tasks**, chọn **Stop Service**. Sau đó, nhấn chuột phải **AdatumCA**, bung **All Tasks**, và chọn **Start Service**.

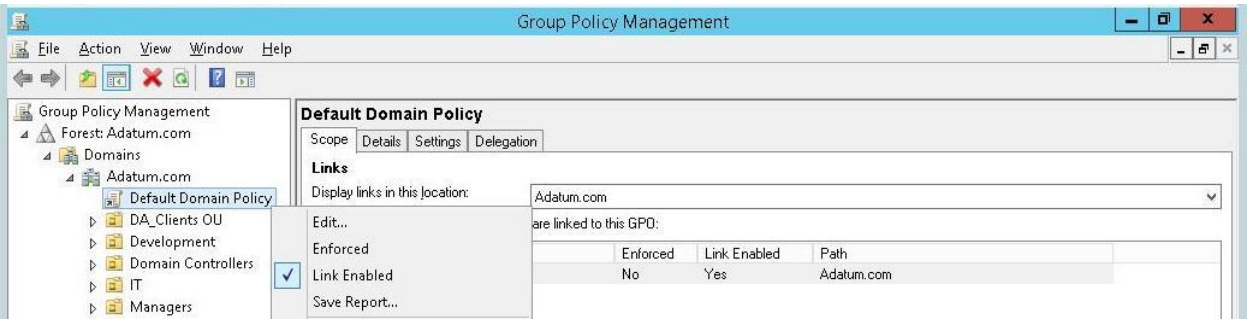


j. Tắt cửa sổ **Certification Authority**.

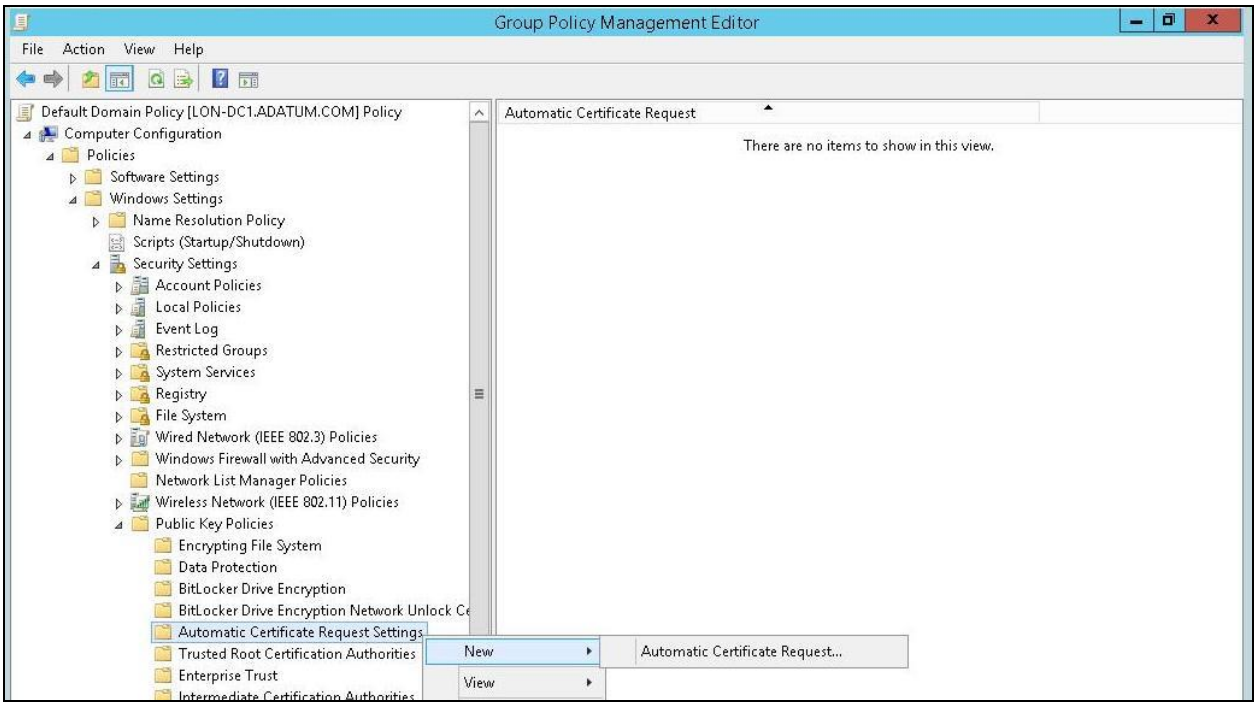
3. Cấu hình GPO để tự động đăng ký Certificate:

a. Trên máy **LON-DC1**, mở **Server Manager,** bung menu **Tools**, mở **Group Policy Management**.

b. Trong cửa sổ **Group Policy Management Console**, bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, nhấn chuột phải **Default Domain Policy**, chọn **Edit**.



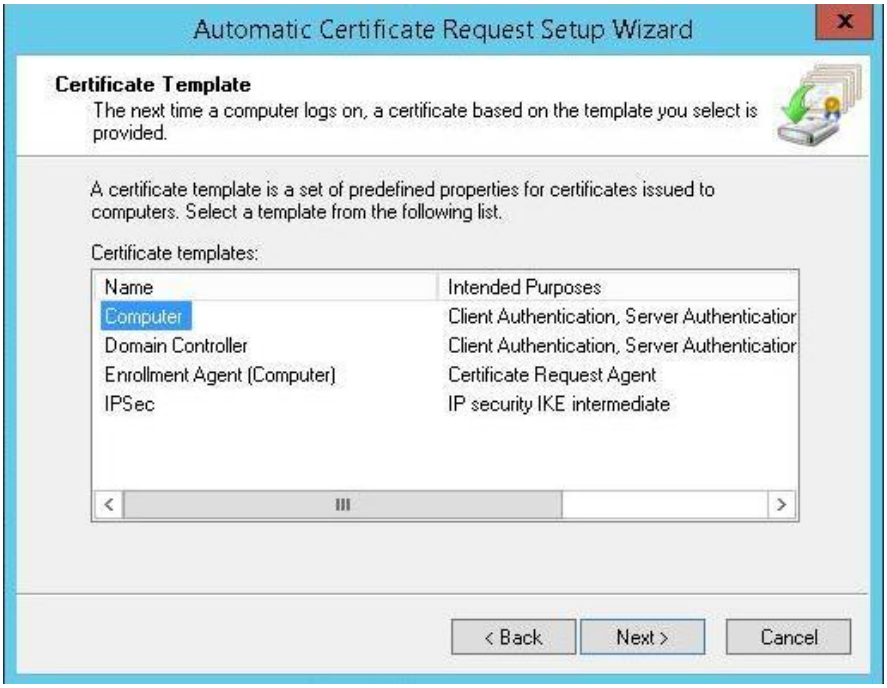
c. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, và bung **Public Key Policies**, nhấn chuột phải **Automatic Certificate Request Settings**, chọn **New**, và chọn **Automatic Certificate Request**.



d. Cửa sổ **Automatic Certificate Request Setup Wizard**, chọn **Next**.



e. Cửa sổ **Certificate Template**, chọn **Computer**, chọn **Next**, và chọn **Finish**.



f. Tắt cửa sổ **Group Policy Management Editor** và **Group Policy Management Console**.

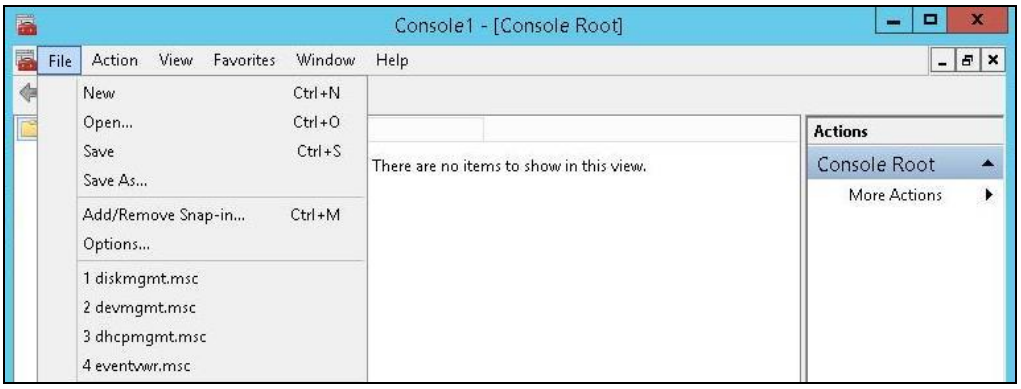
Bước 3. Cấu hình Internal Resources.

1.Xin certificate cho máy **LON-SVR1**:

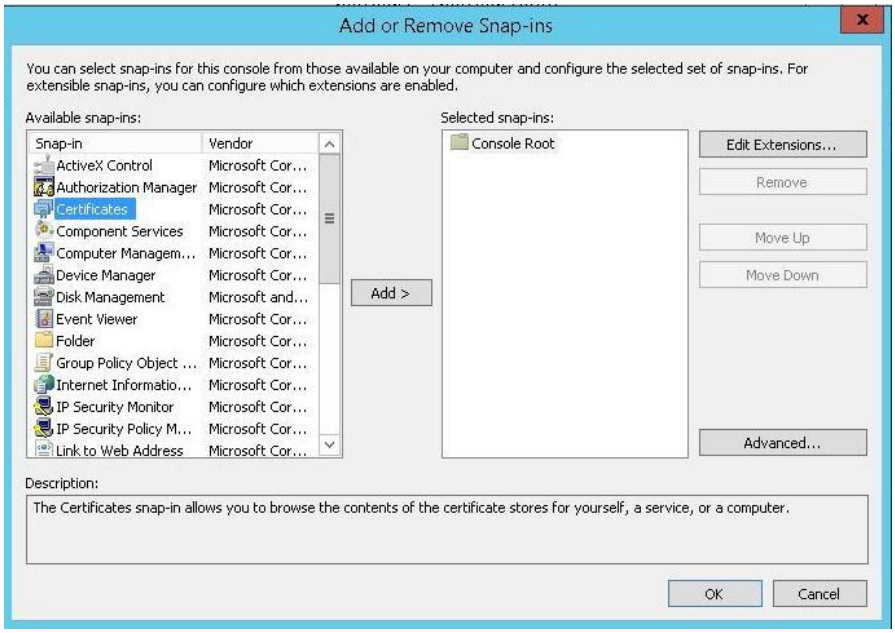
a. Khởi động máy **LON-SVR1**, logon **Adatum\Administrator** với password **Pa$$w0rd.**

b. Bung **Start** menu, gõ **mmc**, nhấn Enter:

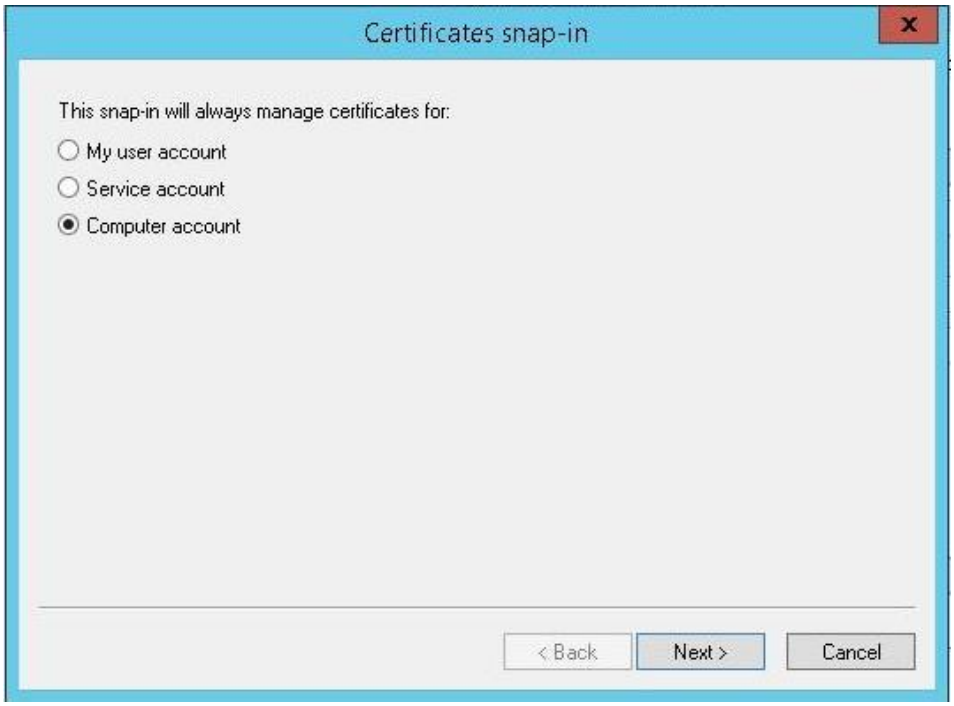
c. Trong cửa sổ **Microsoft Management Console (MMC)**, bung menu **File**, chọn **Add/Remove Snap-in**.



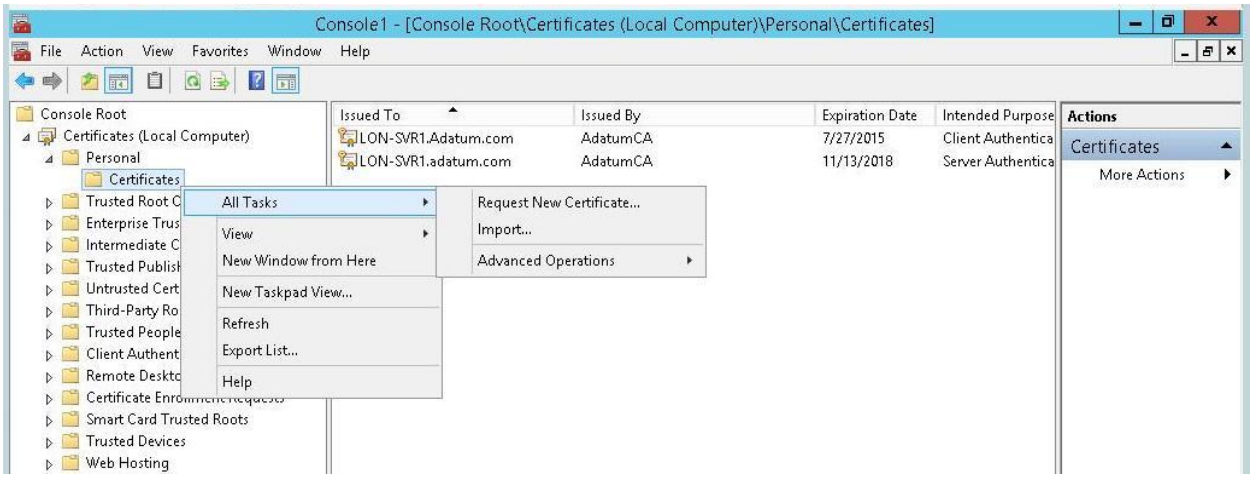
d. Trong cửa sổ **Add/Remove Snap-in**, chọn **Certificates**, chọn **Add**,



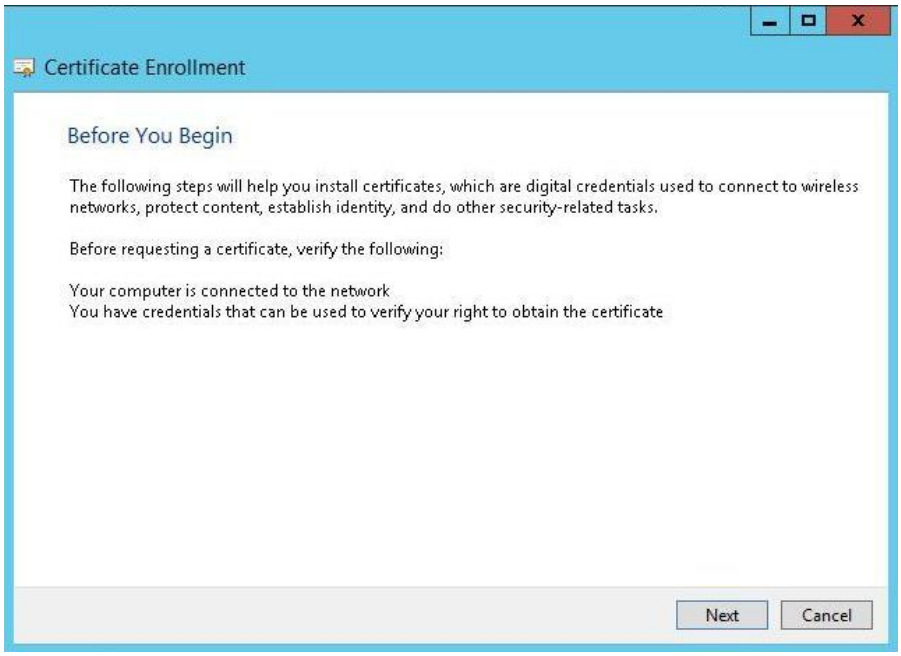
e. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**, chọn **Finish**, chọn **OK**.



f. Trong cửa sổ **Console1**, bung **Certificates (Local Computer)**, bung **Personal**, nhấn chuột phải **Certificates**, chọn **All Tasks**, chọn **Request New Certificate**.



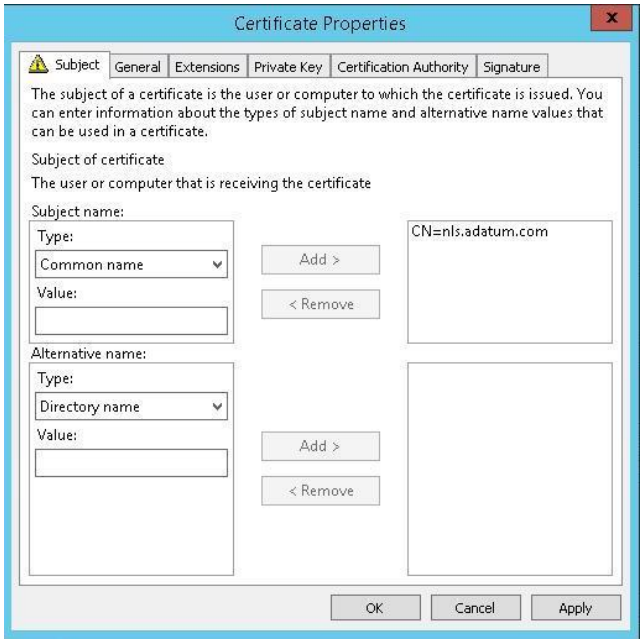
g. Cửa sổ **Before You Begin**, chọn **Next** 2 lần.



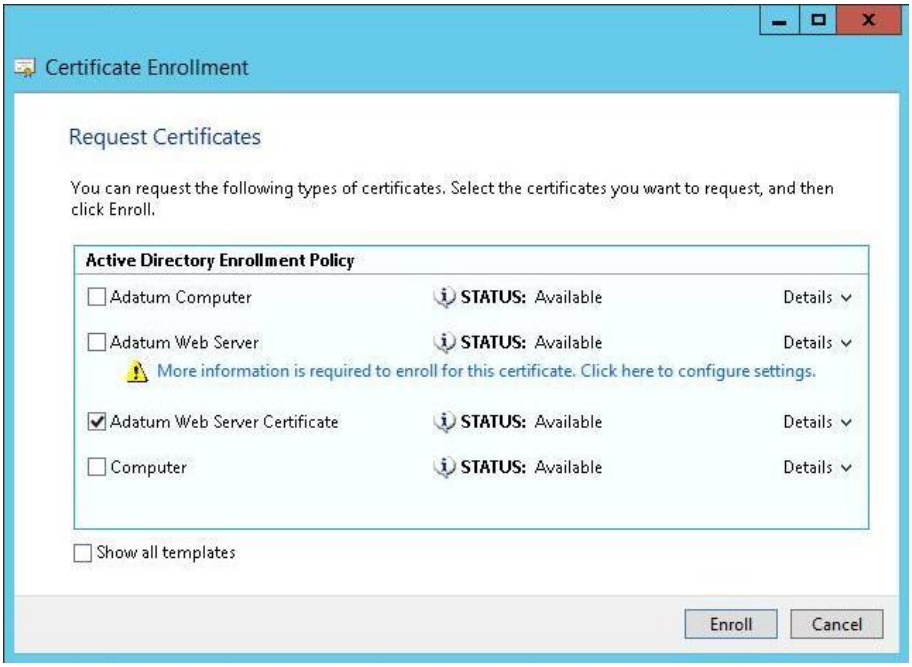
h. Cửa sổ **Request Certificates**, chọn **Adatum Web Server Certificate**, và chọn **More information is required to enroll for this certificate**.



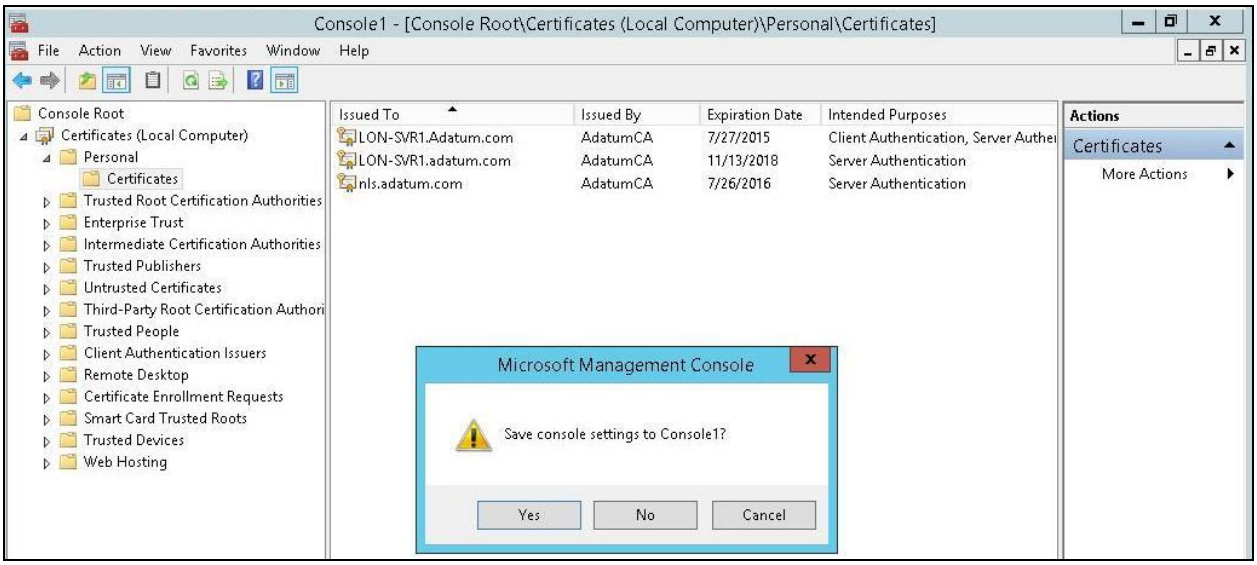
i. Hộp thoại **Certificate Properties**, qua tab **Subject**, trong ô **Subject name**, bung **Type**, chọn **Common name**, trong ô **Value**, nhập **nls.adatum.com**, và chọn **Add**, và chọn **OK.**



j. Cửa sổ **Request Certificates**, chọn **Enroll**, và chọn **Finish**.



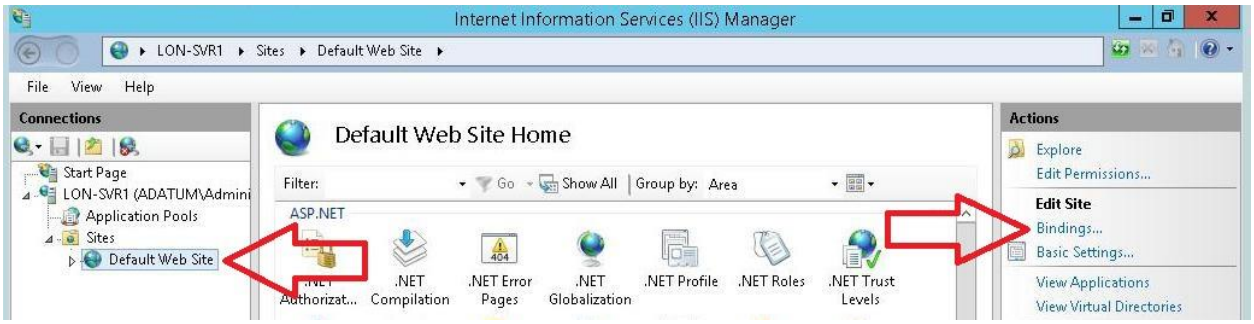
k. Trong cửa sổ **Certificates**, kiểm tra có certificate mới tên **nls.adatum.com** với chức năng **Server Authentication**. Sau đó, tắt cửa sổ **Console1**, và chọn **No**.



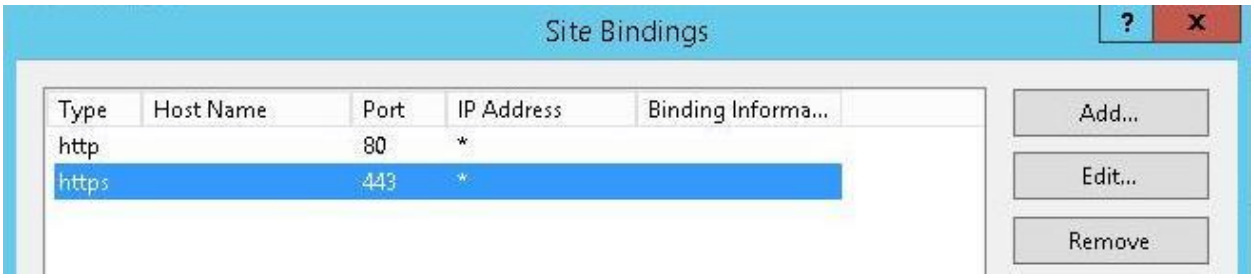
2. Cấu hình Website hỗ trợ HTTPS:

a. Mở **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**.

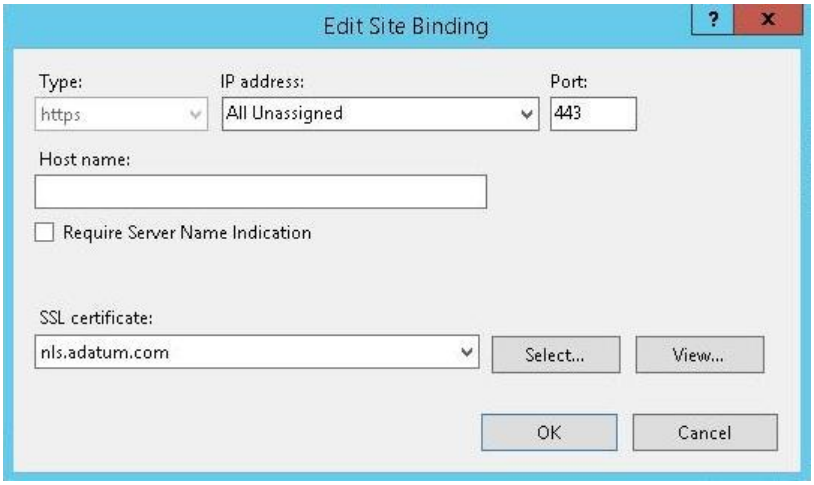
b. Trong cửa **sổ Internet Information Services (IIS) Manager**, bung **LON-SVR1**, bung **Sites**, chọn **Default Web Site**. Trong cửa sổ **Actions**, chọn **Bindings**,



c. Hộp thoại **Site Bindings**, chọn **https**, chọn **Edit**.



d. Hộp thoại **Edit Site Bindings**, bung ô **SSL Certificate**, chọn **nls.adatum.com**, chọn **OK**, và chọn **Close**.



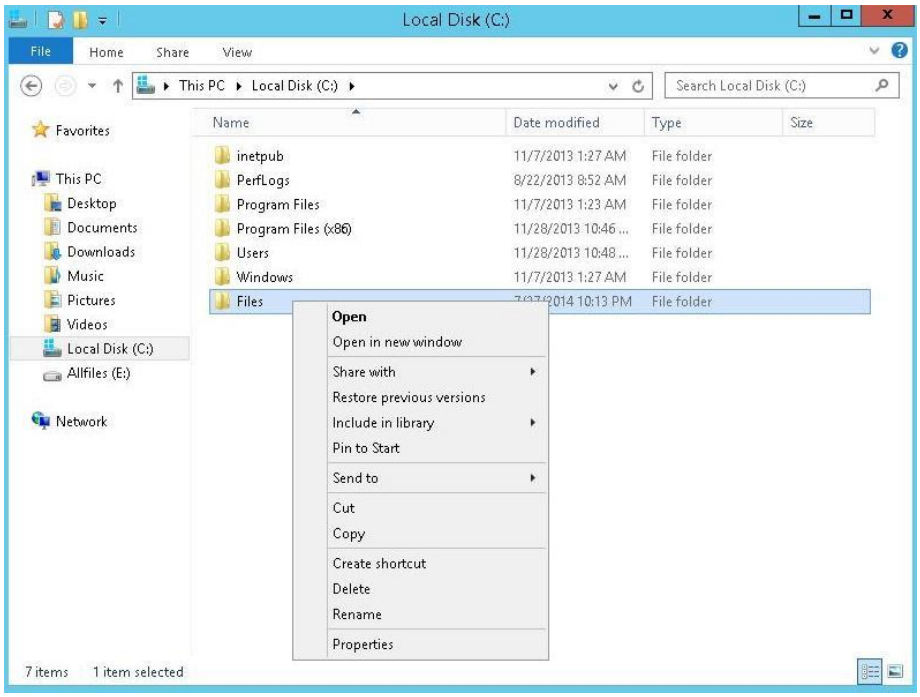
e. Tắt cửa sổ **Internet Information Services (IIS) Manager**.

3. Tạo Shared Folder trên máy **LON-SVR1**:

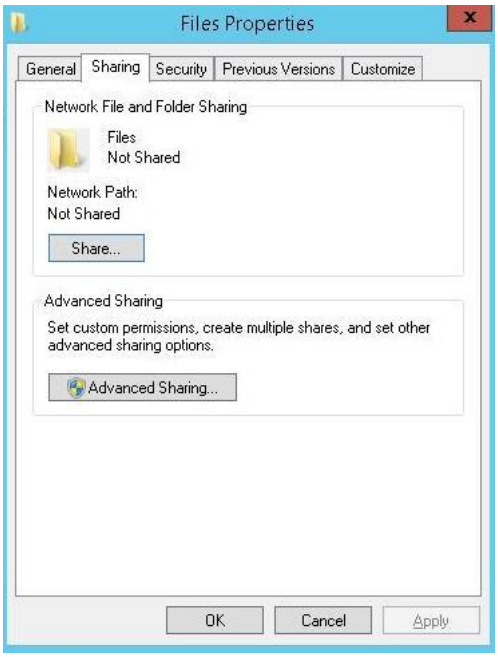
a. Trên máy **LON-SVR1**.

b. Trên thanh Taskbar, mở **File Explorer,** vào ổ đĩa **Local Disk (C:)**.

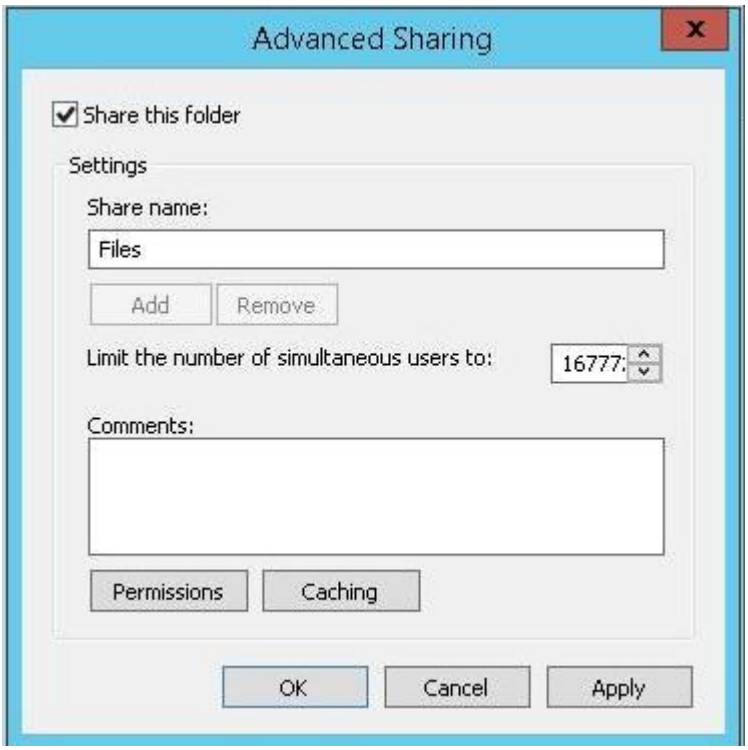
c. Tạo một folder mới đặt tên là **Files**. Nhấn chuột phải folder **Files**, chọn **Properties**.



d. Hộp thoại **Files Properties**, qua tab **Sharing**, chọn **Advanced Sharing**.

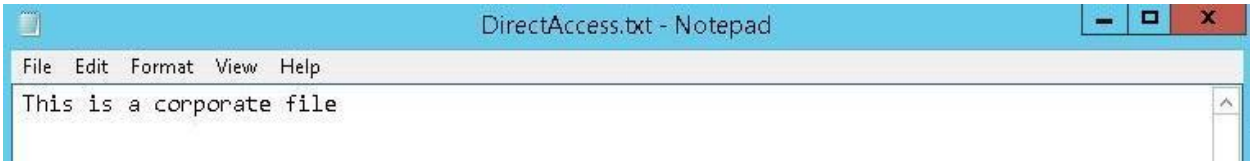


e. Hộp thoại **Advanced Sharing**, đánh dấu chọn **Share this folder**, chọn **OK**, và chọn **Close**.



f. Mở folder **Files**, tạo một file **Text Document,** đặt tên là **DirectAccess.txt**

g. Mở file **DirectAccess**.txt, nhập nội dung **This is a corporate file**.



m. Tắt Notepad, chọn **Save**. Tắt File Explorer.

Bước 4. Cấu hình DirectAccess Server.

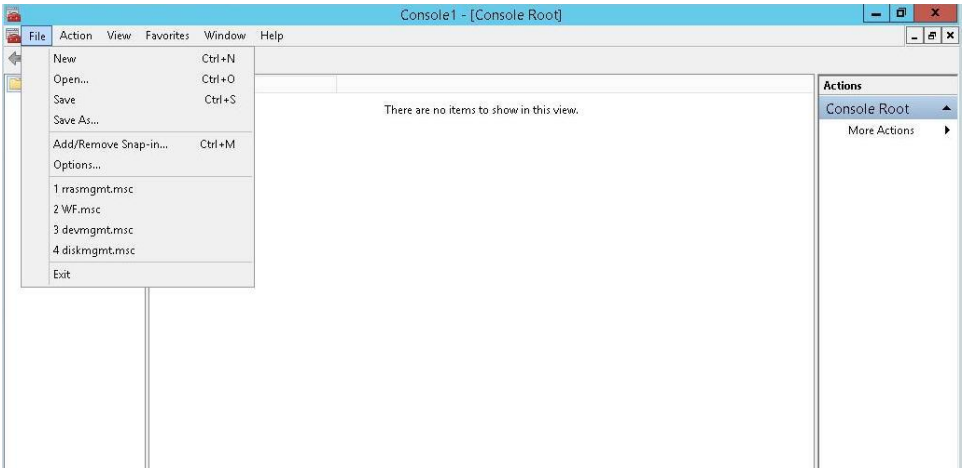
1. Xin certificate cho máy **LON-RTR**:

a. Qua máy **LON-RTR**. Mở **cmd**

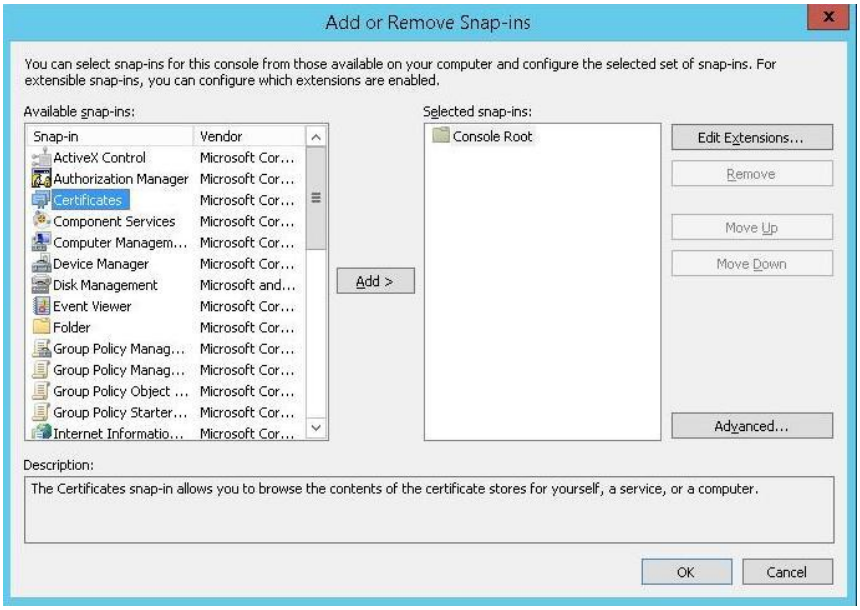
b. Trong cửa sổ Command prompt, gõ lệnh: **gpupdate /force**



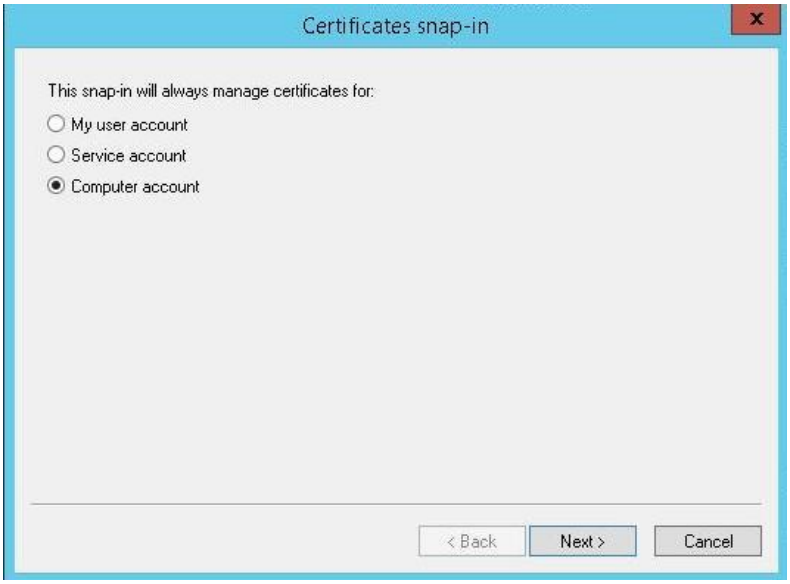
c. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.



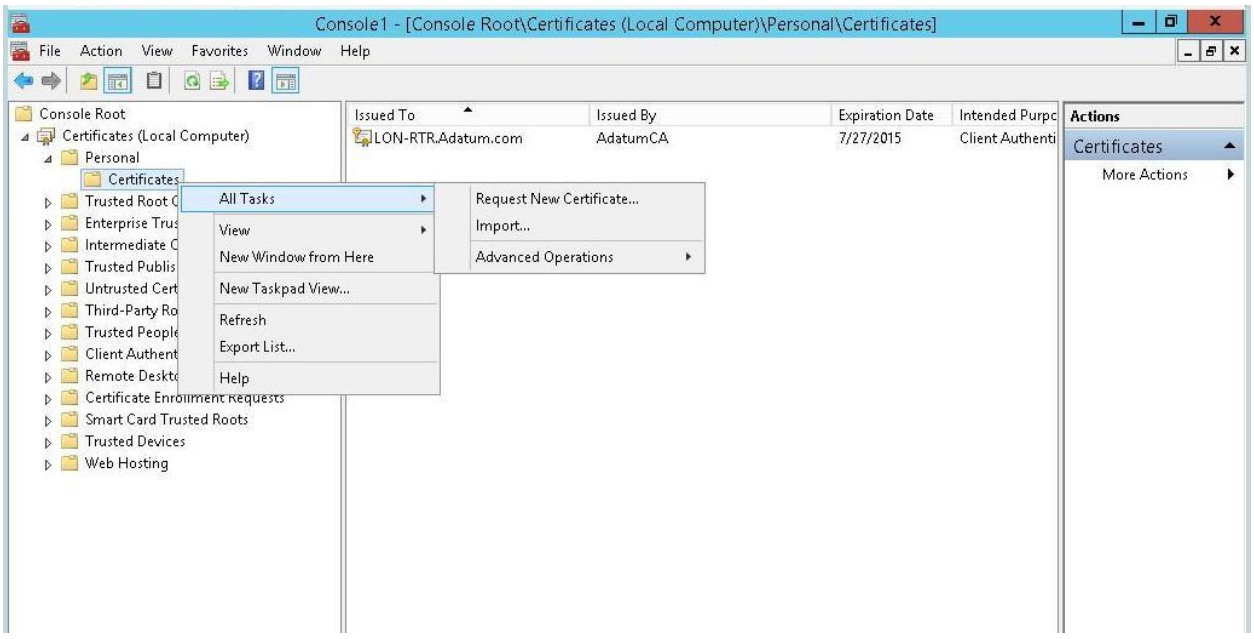
d. Trong hộp thoại **Add/Remove Snap-in**, chọn **Certificates**, chọn **Add**.



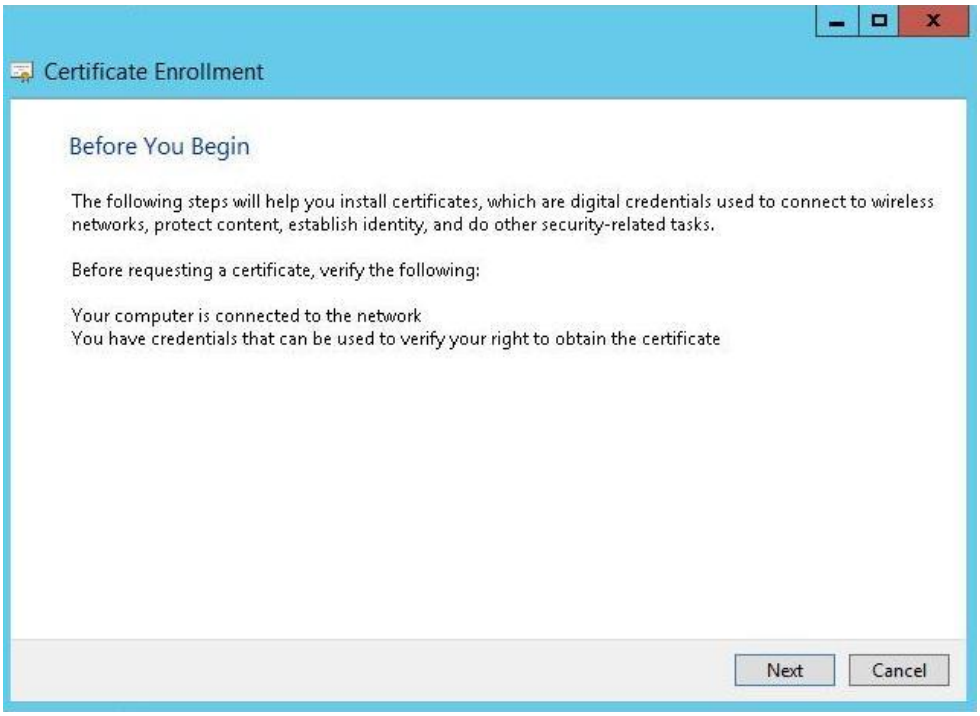
e. Cửa sổ **Certificates snap-in**, chọn **Computer account**, và chọn **Next**, chọn **Finish**, và chọn **OK**.



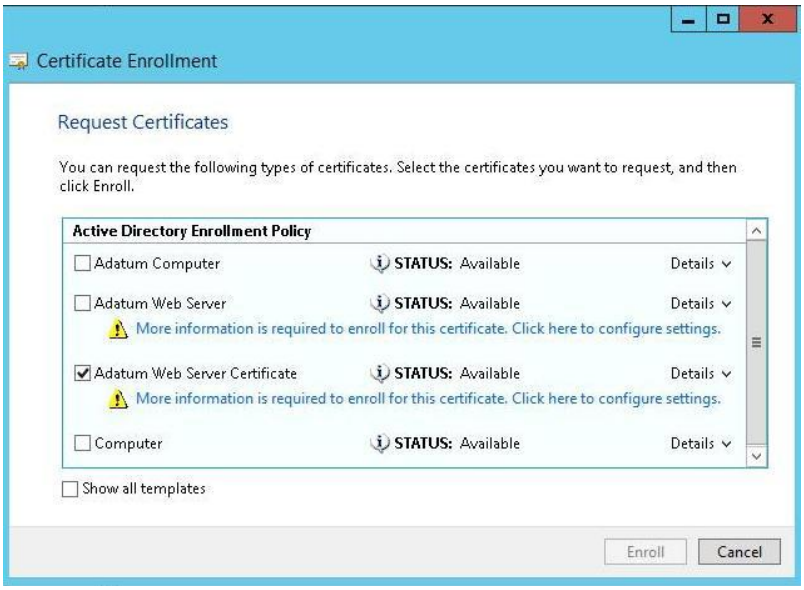
f. Trong cửa sổ **Console1**, bung **Certificates (Local Computer)**, bung **Personal**, nhấn chuột phải **Certificates**, bung **All Tasks**, chọn **Request New Certificate**.



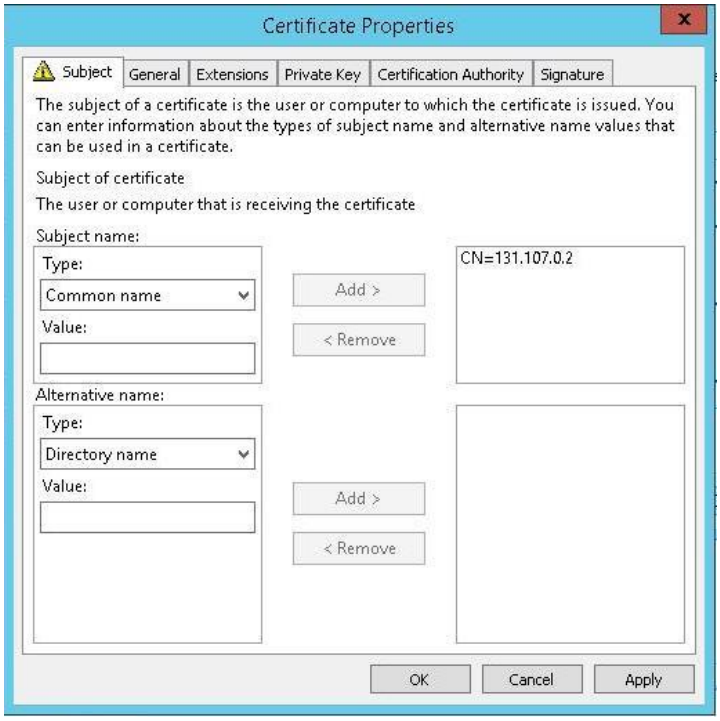
g. Cửa sổ Before You Begin, chọn **Next** 2 lần.



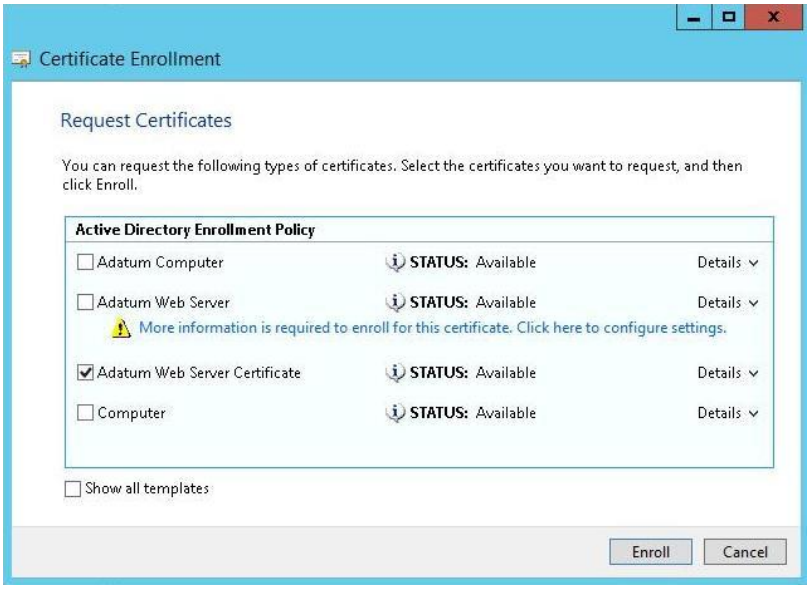
h. Cửa sổ **Request Certificates**, chọn **Adatum Web Server Certificate**, và chọn **More information is required to enroll for this certificate**.



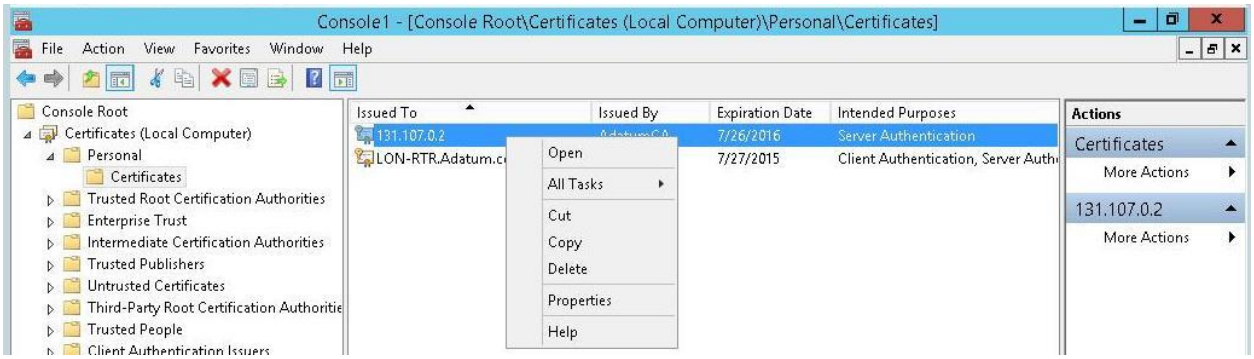
i. Hộp thoại **Certificate Properties**, qua tab **Subject**, trong **Subject name**, bung **Type**, chọn **Common name**, trong ô **Value**, nhập **131.107.0.2**, chọn **Add**, và chọn **OK**



j. Cửa sổ **Request Certificates**, chọn **Enroll**, chọn **Finish**.



k. Trong Certificates, kiểm tra hiển thị certificate mới **131.107.0.2** có chức năng **Server Authentication**. Nhấn chuột phải certificate **131.107.0.2**, chọn **Properties**.



l. Hộp thoại **Properties**, trong ô **Friendly Name**, nhập **IP-HTTPS Certificate**, chọn **OK**.

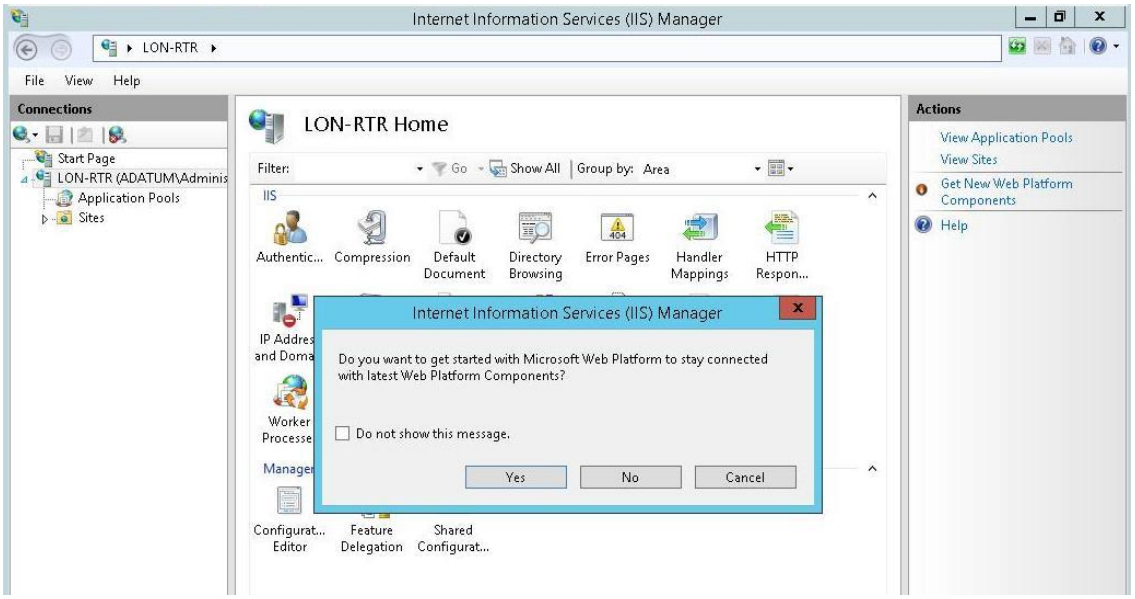


m. Tắt cửa sổ **Console1**, chọn **No**.

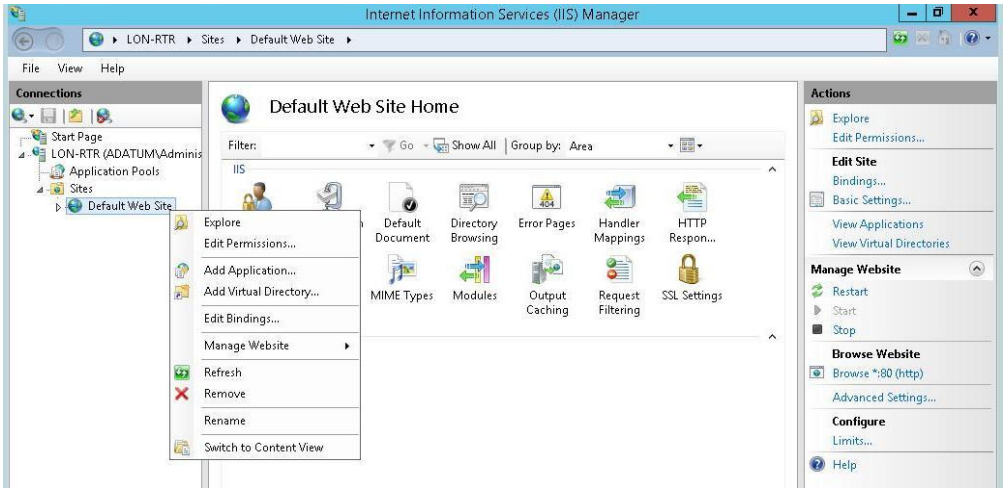
2. Tạo Certificate Revocation List (CRL) Distribution Point trên máy LON-RTR:

a. Trên máy **LON-RTR**.

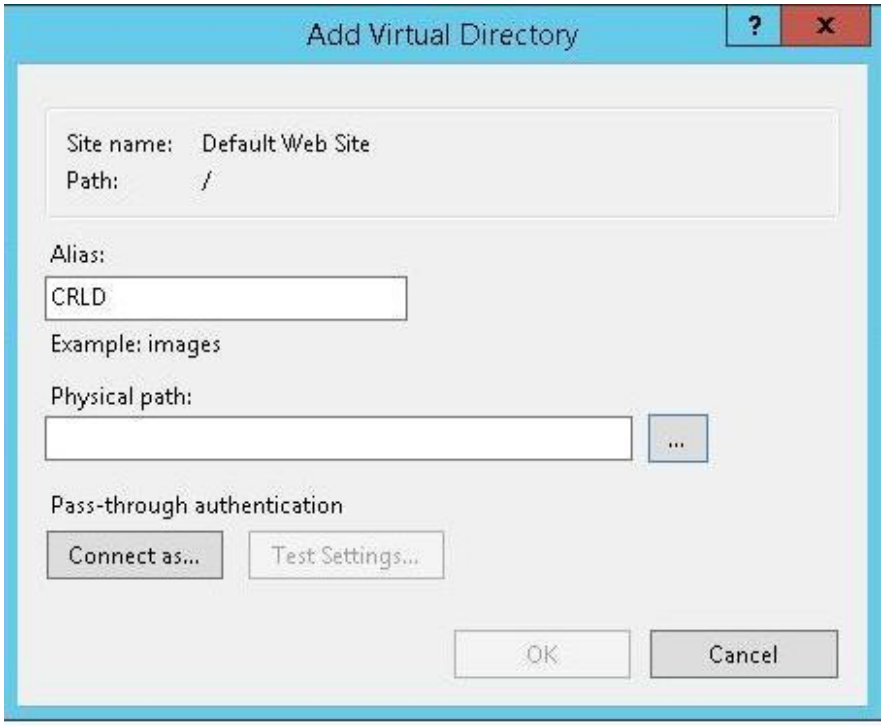
b. Trong Server Manager, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**. Nếu xuất hiện hộp thoại **Internet Information Service Manager**, chọn **No**.



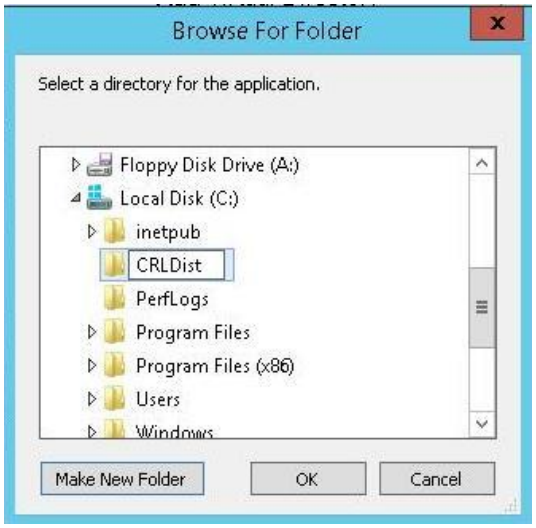
c. Trong cửa sổ **Internet Information Service Manager,** bung **LON-RTR**, bung **Sites**, nhấn chuột phải **Default Web Site**, chọn **Add Virtual Directory**.



d. Hộp thoại **Add Virtual Directory**, trong ô **Alias**, nhập **CRLD**. Trong ô **Physical path**, chọn (**...**).



e. Hộp thoại **Browse for Folder**, chọn **Local Disk (C:)**, và chọn **Make New Folder**. Nhập **CRLDist**, nhấn Enter, chọn **OK.**



f. Hộp thoại **Browse for Folder**, chọn **OK** 2 lần.



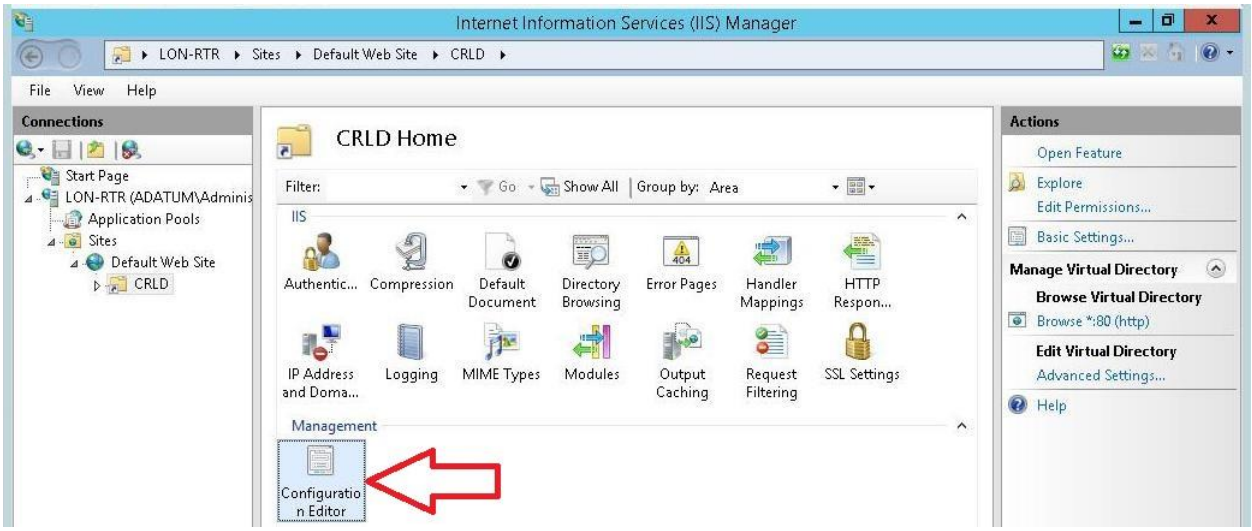
g. Cửa sổ **IIS Manager**, chọn folder **CRLD**. Trong cửa sổ giữa, nhấp đôi chuột **Directory Browsing**,



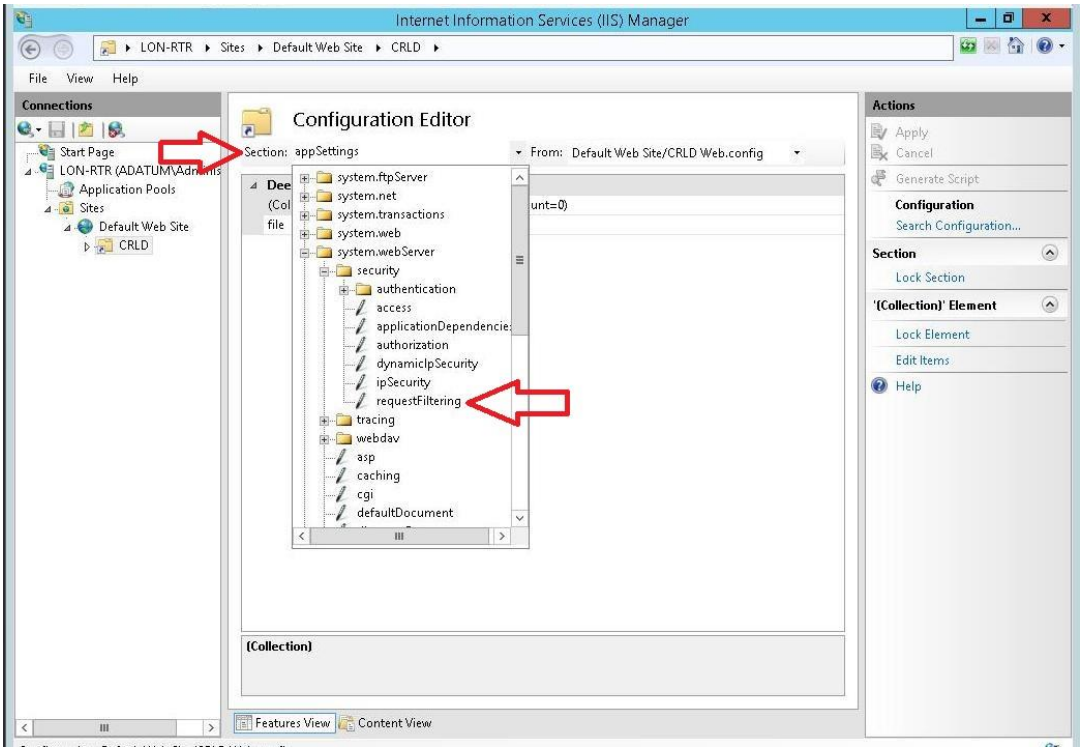
h. Trong cửa sổ **Actions**, chọn **Enable**.



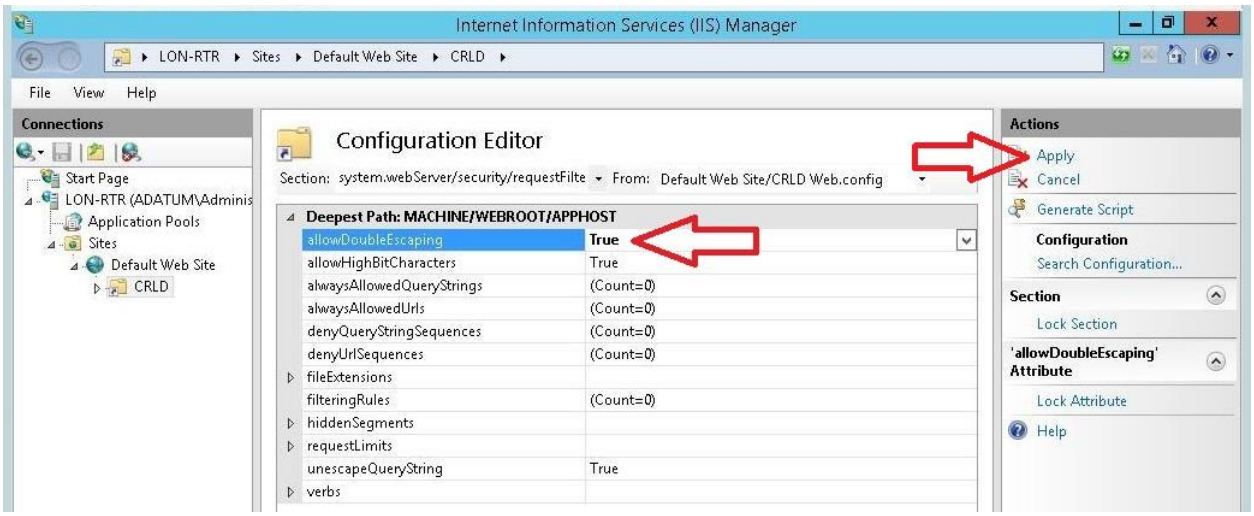
i. Cửa sổ **IIS Manager**, chọn folder **CRLD**. trong cửa sổ giữa, nhấp đôi chuột **Configuration Editor**.



j. Trong Configuration Editor, trong ô **Section**, bung **system.webServer**, bung **security**, và chọn **requestFiltering**.



k. Trong cửa sổ giữa, nhấp đôi chuột **allowDoubleEscaping** để thay đổi giá trị False thành **True**, trong cửa sổ **Actions**, chọn **Apply**.



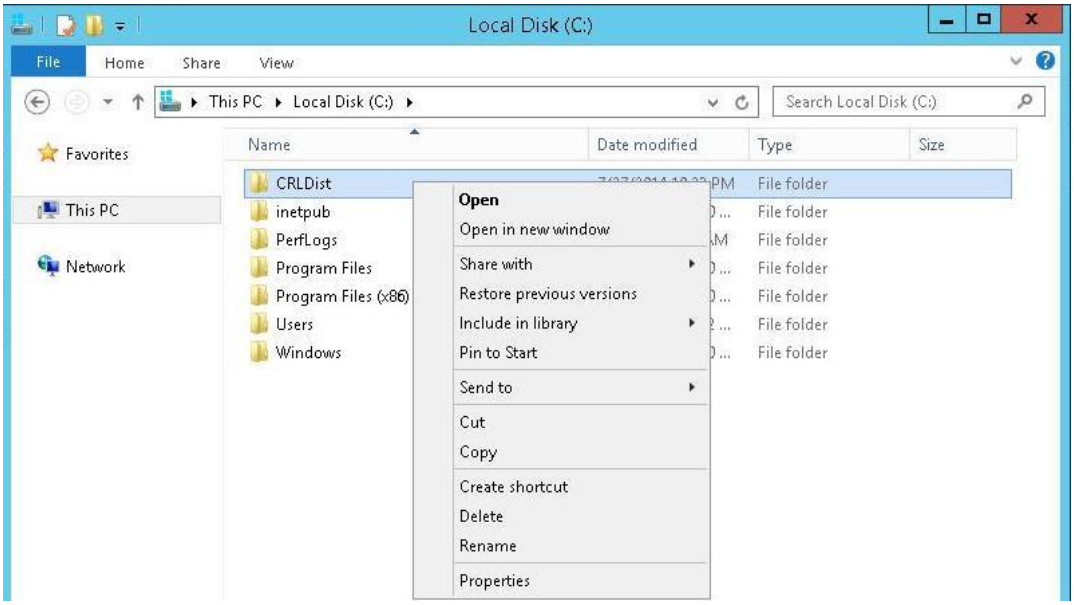
l. Tắt **Internet Information Services (IIS) Manager**.

3. Share và cấp quyền trên CRL Distribution Point:

a. Trên máy **LON-RTR.**

b. Trên Taskbar, mở **File Explorer**. chọn **This PC**, mở **Local Disk (C:)**.

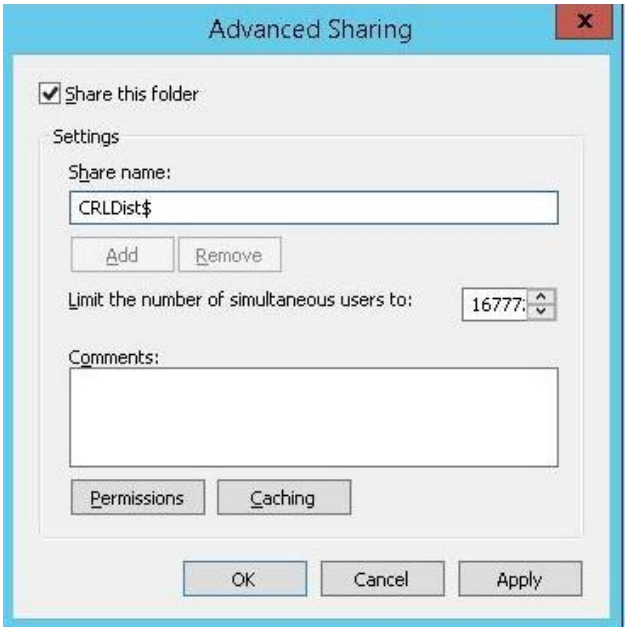
c. Nhấn chuột phải folder **CRLDist**, chọn **Properties**.



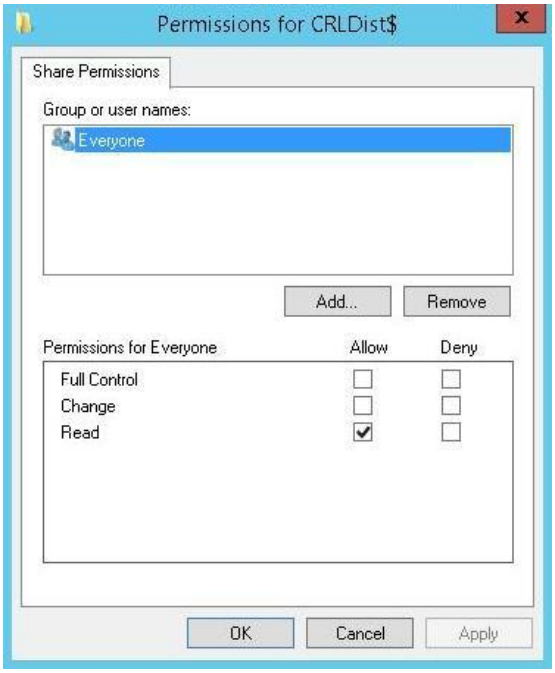
d. Trong hộp thoại **CRLDist Properties**, qua tab **Sharing**, chọn **Advanced Sharing**.



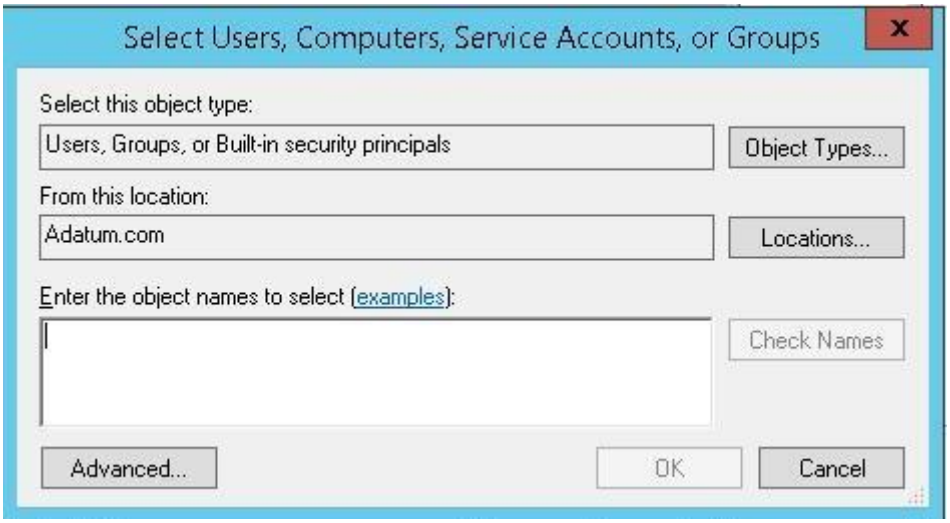
e. Hộp thoại **Advanced Sharing**, đánh dấu chọn **Share this folder**, trong ô **Share name**, nhập **CRLDist$**, và chọn **Permissions**



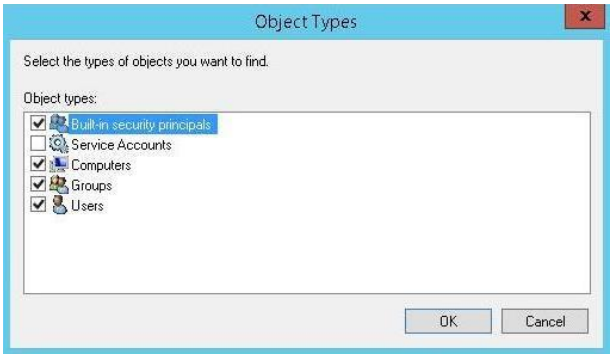
f. Hộp thoại **Permissions for CRLDist$**, chọn **Add**.



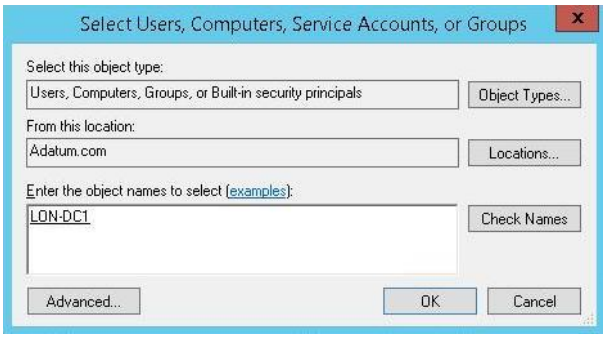
g. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, chọn **Object Types**.



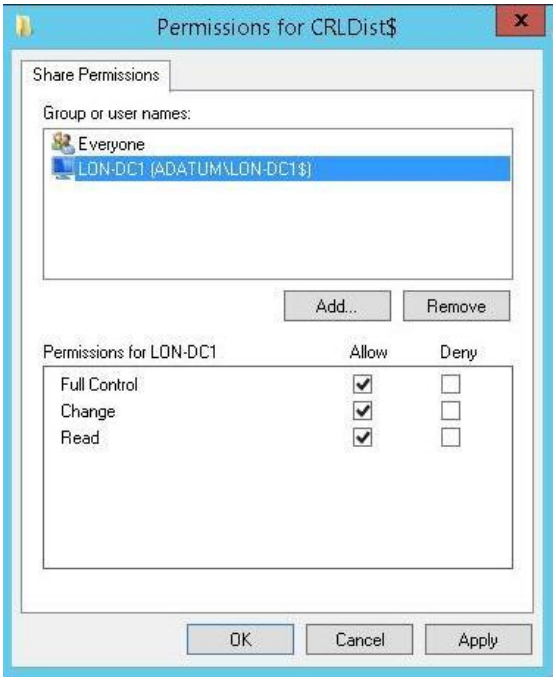
h. Hộp thoại **Object Types**, đánh dấu chọn **Computers**, và chọn **OK**.



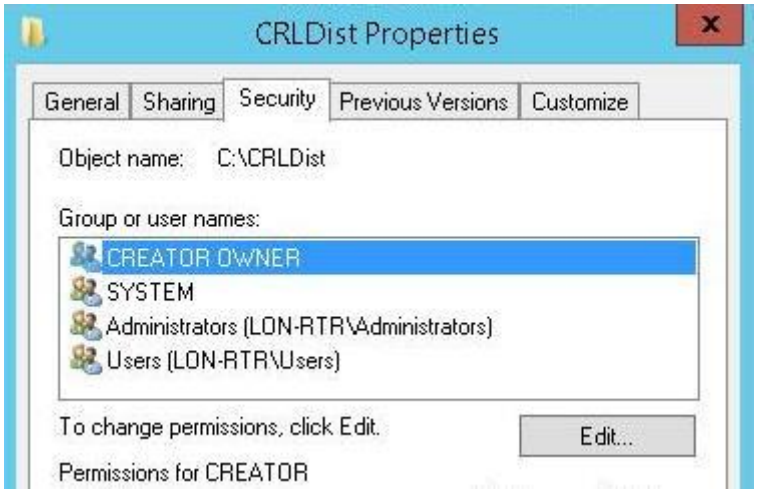
i. Trong ô **Enter the object names to select**, nhập **LON-DC1**, chọn **Check Names**, chọn **OK**.



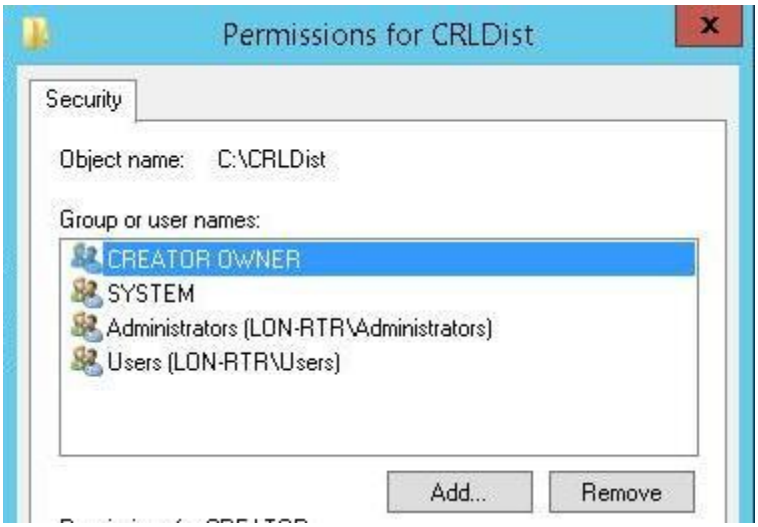
j. Hộp thoại **Permissions for CRLDist$**, chọn **LON-DC1 (ADATUM\NYC-DC1$),** đánh dấu chọn **Full control** ở cột **Allow**, và chọn **OK** 2 lần.



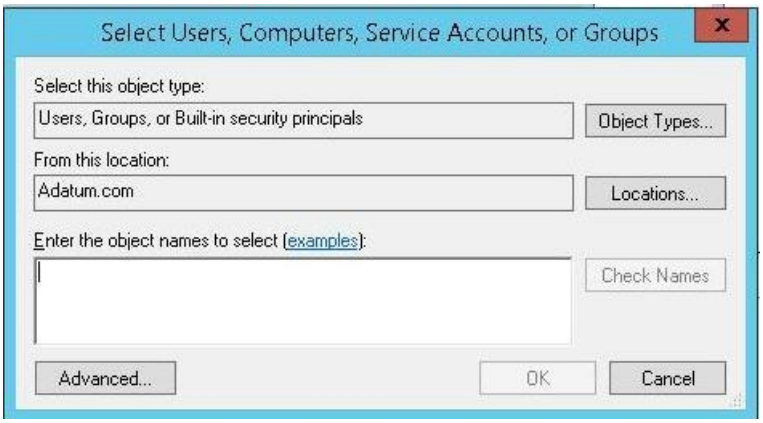
k. Hộp thoại **CRLDist Properties**, qua tab **Security**, chọn **Edit**.



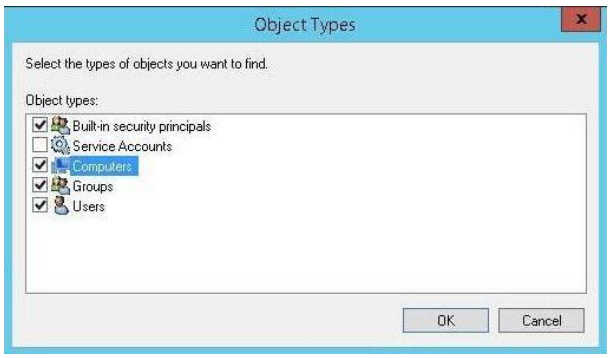
l. Trong hộp thoại **Permissions for CRLDist**, chọn **Add**.



m. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, chọn **Object Types**.



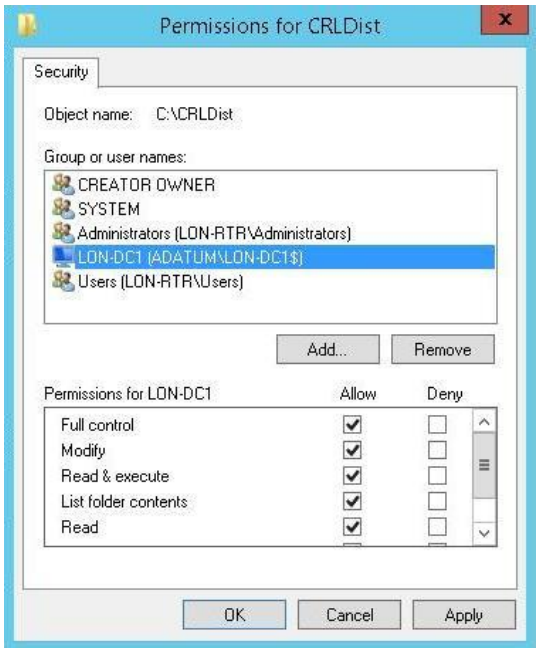
n. Hộp thoại **Object Types**, đánh dấu chọn **Computers**, và chọn **OK**.



o. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, trong ô **Enter the object names to select**, nhập **LON-DC1**, chọn **Check Names**, và chọn **OK**.



p. Hộp thoại **Permissions for CRLDist**, chọn **LON-DC1 (ADATUM\LON-DC1$)**, đánh dấu chọn **Full control** ở cột **Allow**, chọn **OK**, và chọn **Close**. Tắt File Explorer.

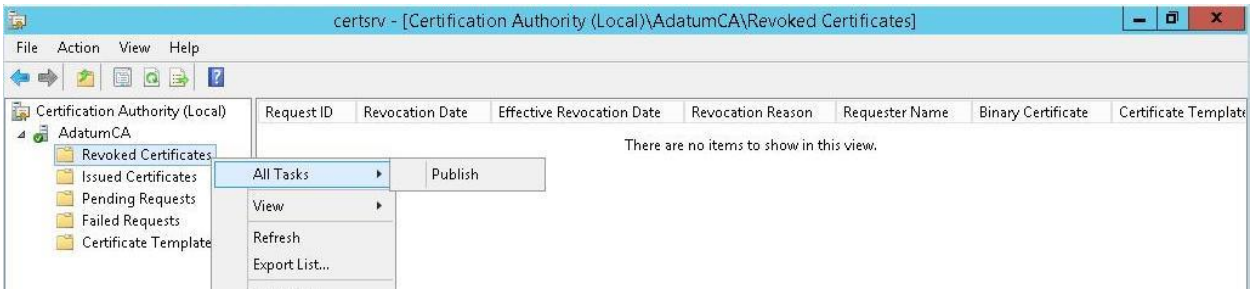


4. Publish danh sách CRL để các máy Client từ Internet có thể truy cập:

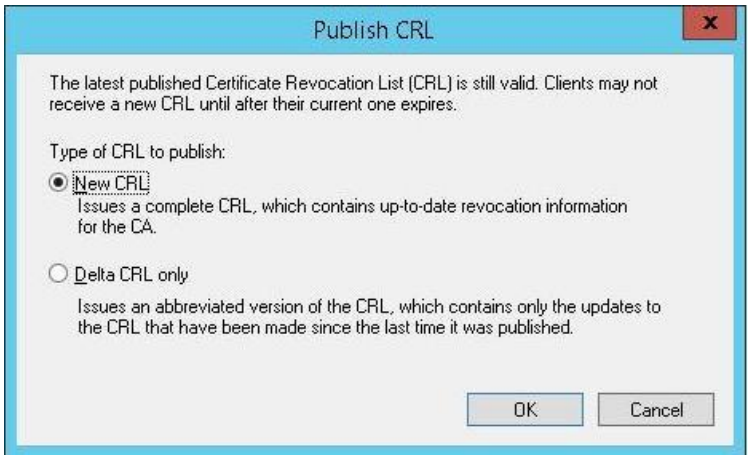
a. Qua máy **LON-DC1**.

b. Mở **Server Manager**, bung **Tools**, mở **Certification Authority**.

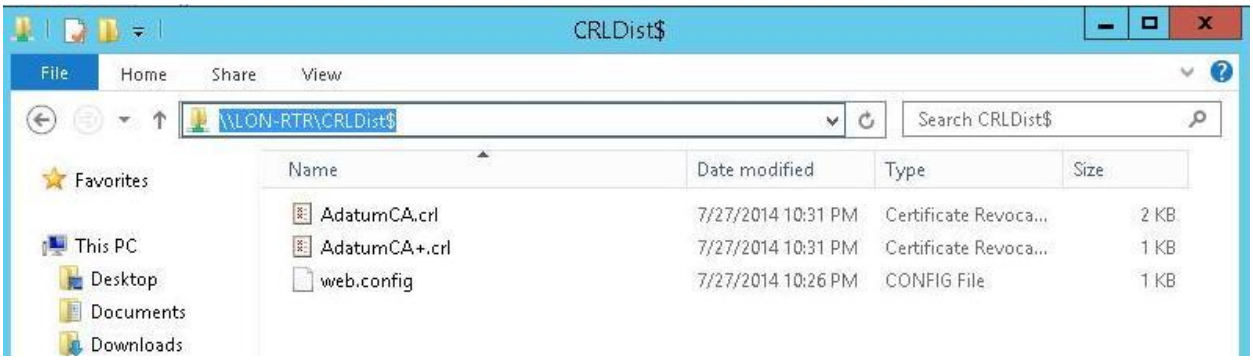
c. Trong cửa sổ **Certification Authority**, bung **AdatumCA**, nhấn chuột phải **Revoked Certificates**, bung **All Tasks**, và chọn **Publish**.



d. Hộp thoại **Publish CRL**, chọn **New CRL**, và chọn **OK**.



e. Trên thanh Taskbar, mở **File Explorer**, tuy cập **\\LON-RTR\CRLDist$** . Kiểm tra hiển thị file **AdatumCA**



f. Tắt File Explorer.

5. Cấu hình máy LON-RTR làm DirectAccess Server:

a. Khởi động lại máy **LON-RTR,** logon **Adatum\Administrator** với password **Pa$$w0rd**.

b. Mở **Server Manager**, bung menu **Tools**, mở **Routing and Remote Access**.

c. Trong cửa sổ **Routing and Remote Access**, nhấn chuột phải **LON-RTR (local)**, chọn **Disable Routing and Remote Access**.



d. Hộp thoại **Routing and Remote Access**, chọn **Yes**.



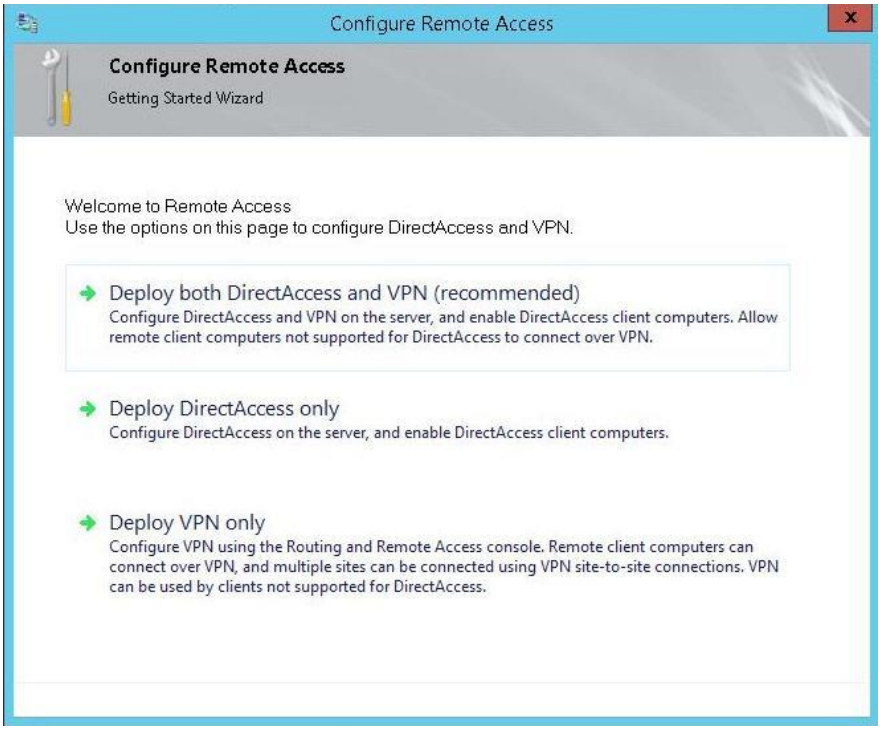
e. Tắt **Routing and Remote Access**.

f. Trong **Server Manager**, bung menu **Tools**, chọn **Remote Access Management**.

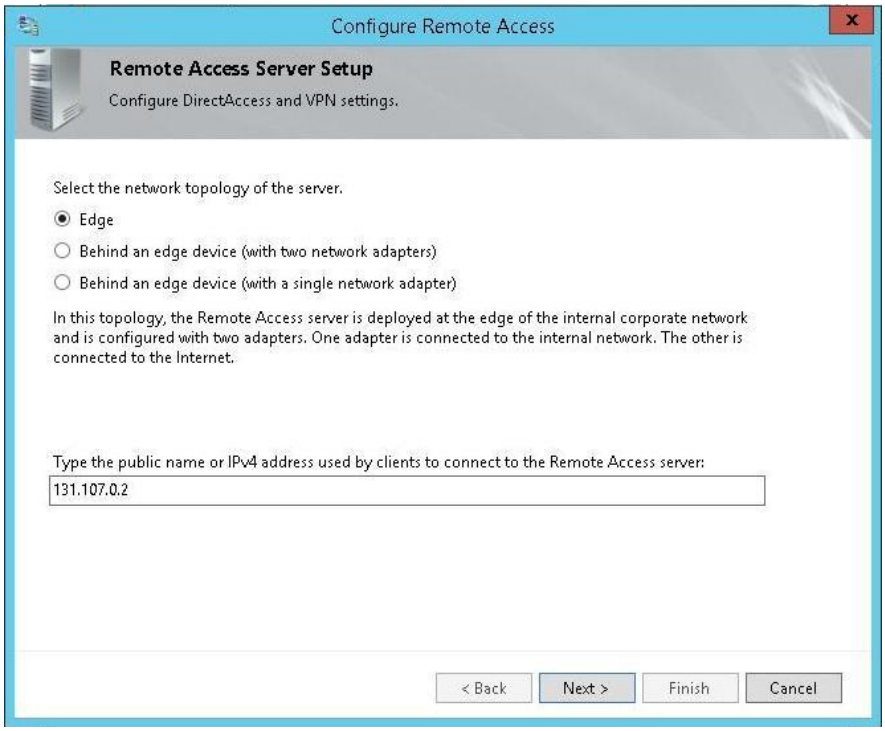
g. Trong cửa sổ **Remote Access Management**, chọn **DirectAccess and VPN**, chọn **Run the Getting Started Wizard**.



h. Cửa sổ **Configure Remote Access Wizard**, chọn **Deploy DirectAccess only**.



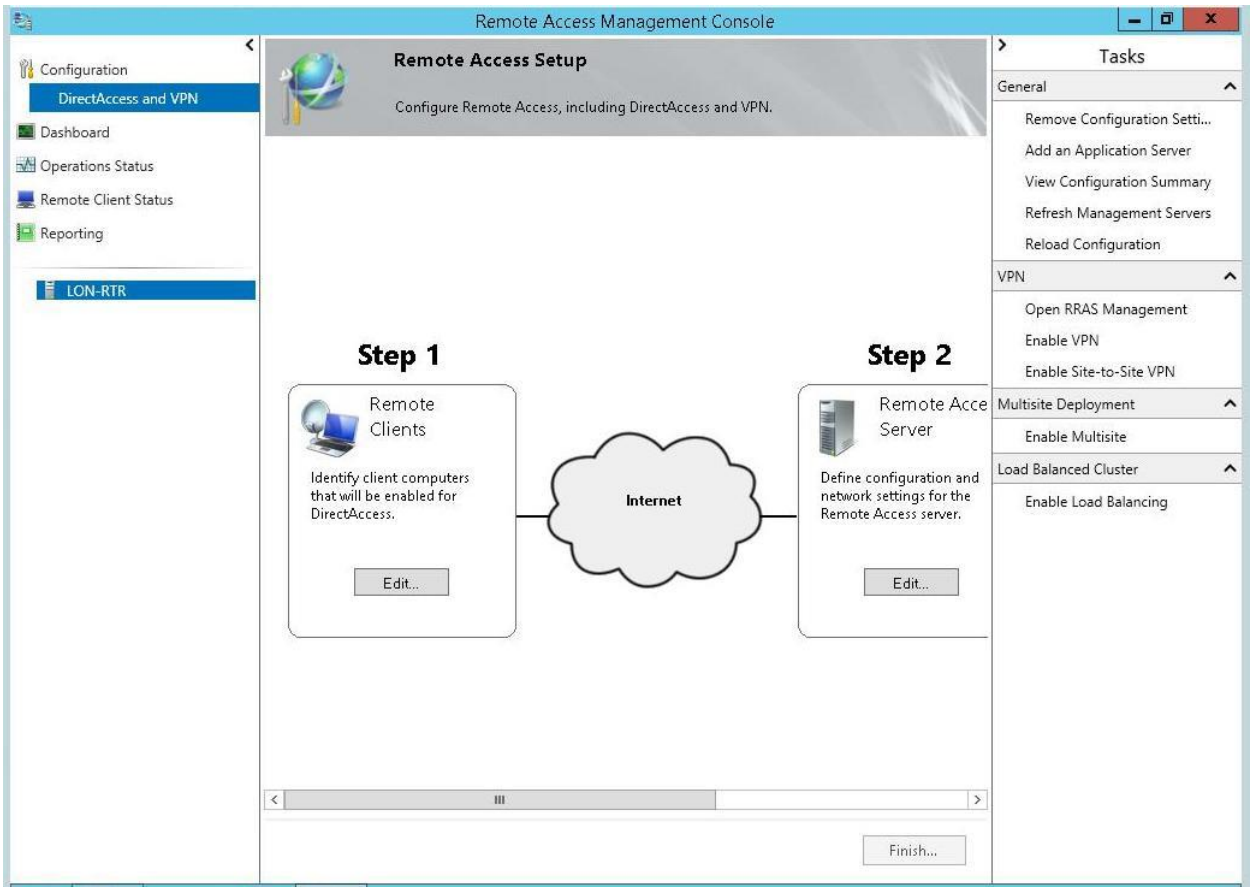
i. Trong **Network Topology**, chọn **Edge**, nhập **131.107.0.2** vào ô **Type the public name**, chọn **Next**, và chọn **Finish**



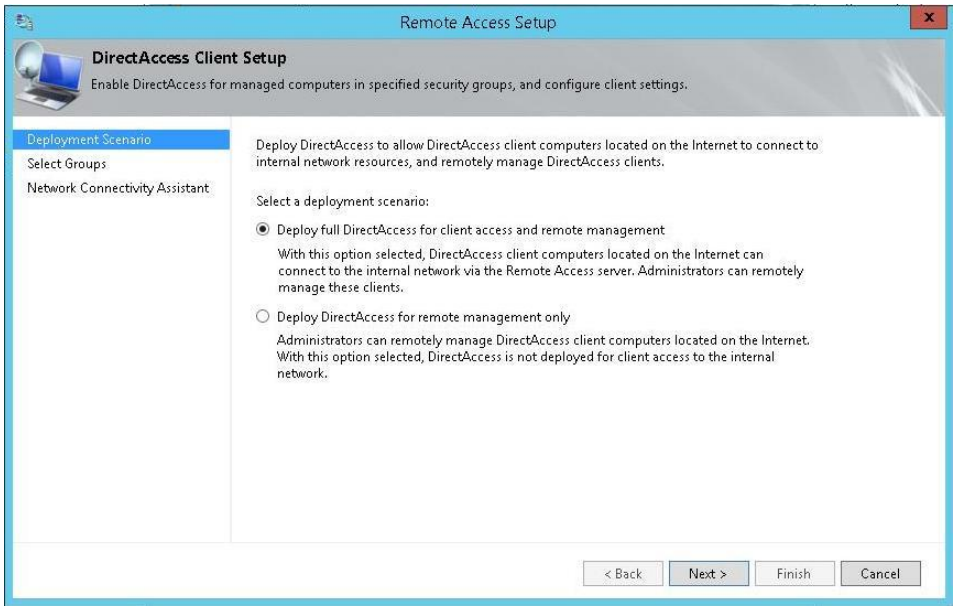
j. Hộp thoại Applying Getting Started Wizard Setting, chọn **Close**.



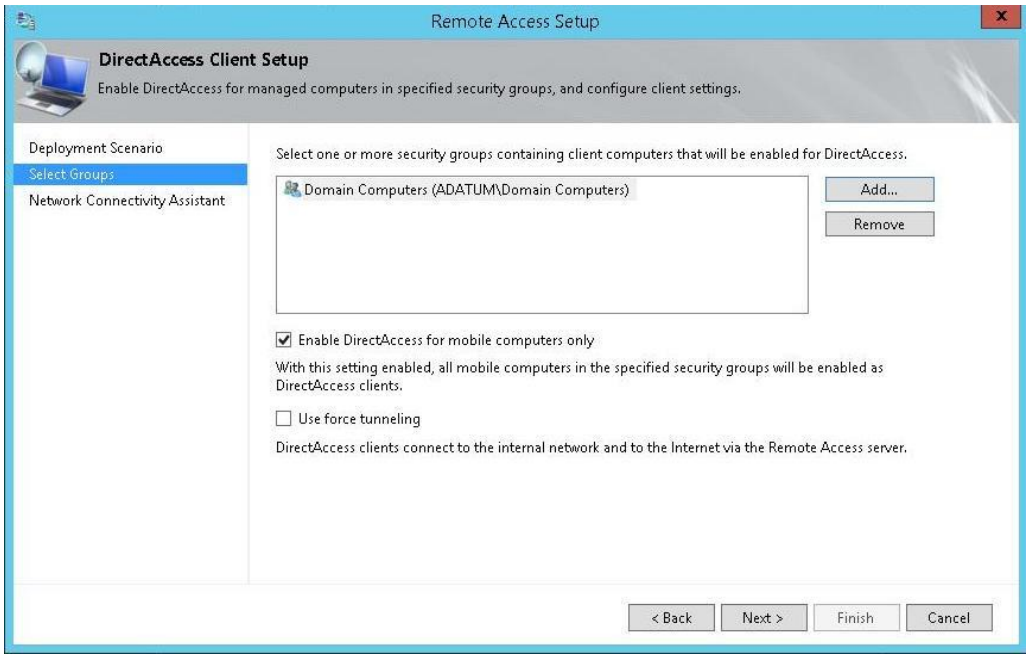
k. Cửa sổ **Remote Access Management**, trong ô **Step 1**, chọn **Edit.**



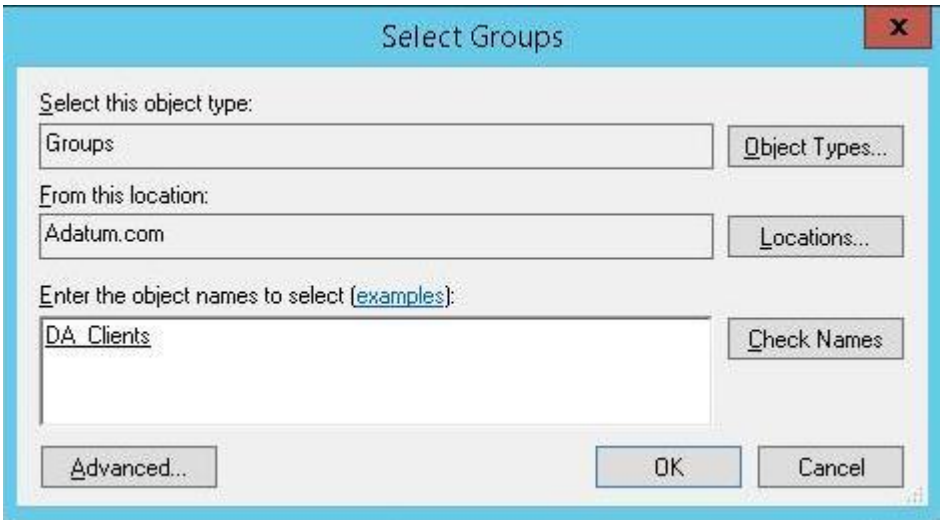
l. Cửa sổ **Select a deployment scenario**, chọn **Next**.



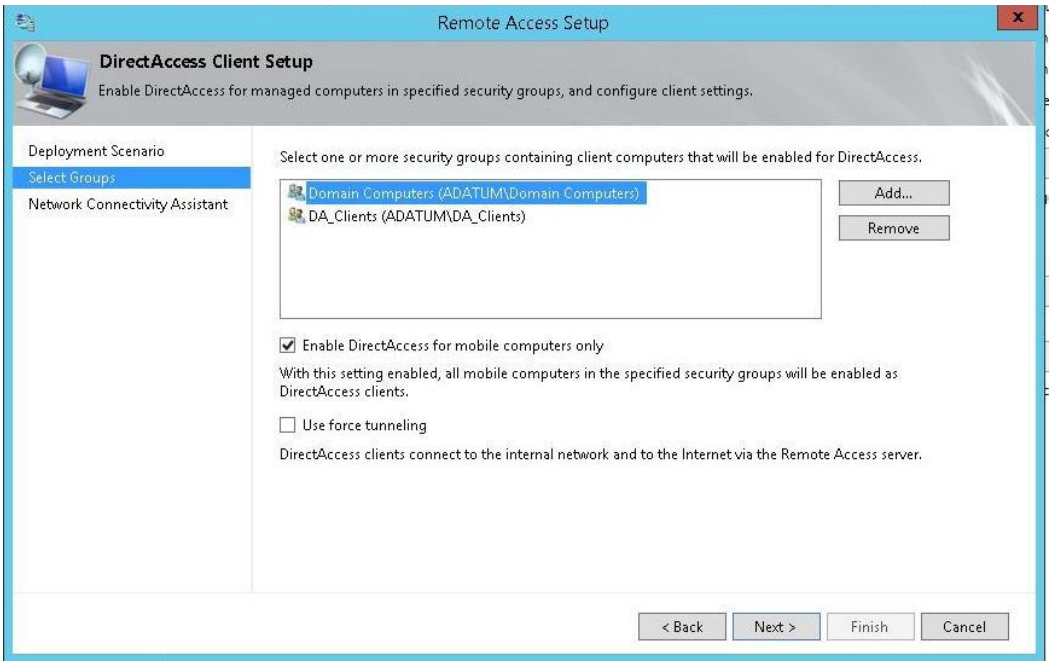
m. Trong **Select one or more security groups**, chọn **Add**.



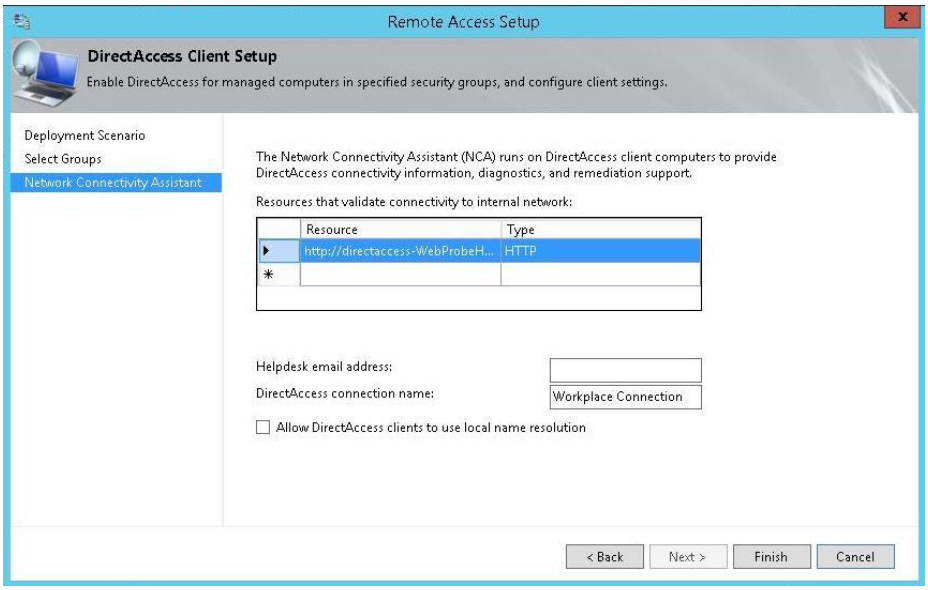
n. Hộp thoại **Select Groups**, nhập **DA_Clients**, chọn **Check Name**, và chọn **OK**.



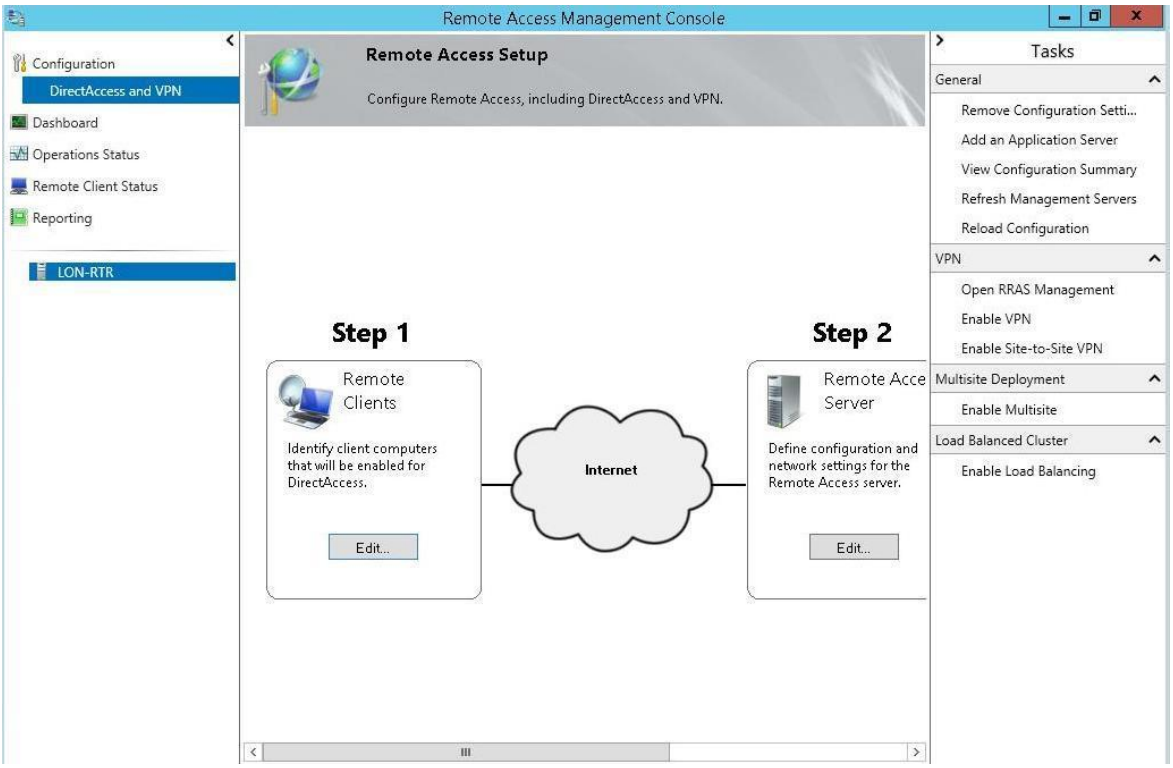
o. Trong danh sách groups, chọn **Domain Computers**, và chọn **Remove**, và chọn **Next.**



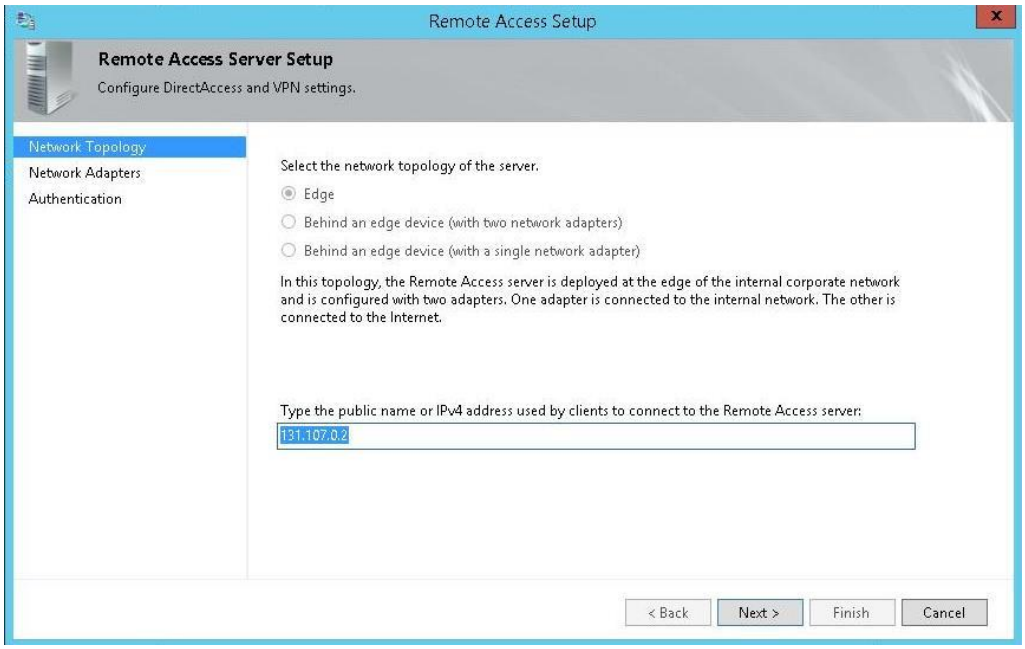
q. Cửa sổ **Network Connectivity Assistant,** chọn **Finish**.



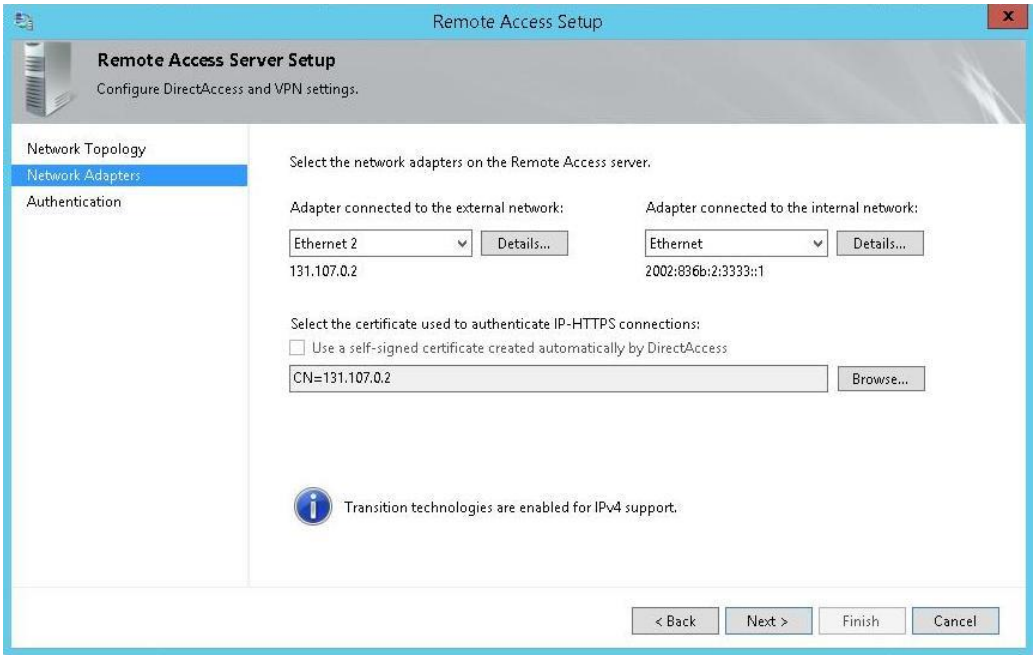
r. Cửa sổ **Remote Access Management**, trong ô **Step 2**, chọn **Edit**.



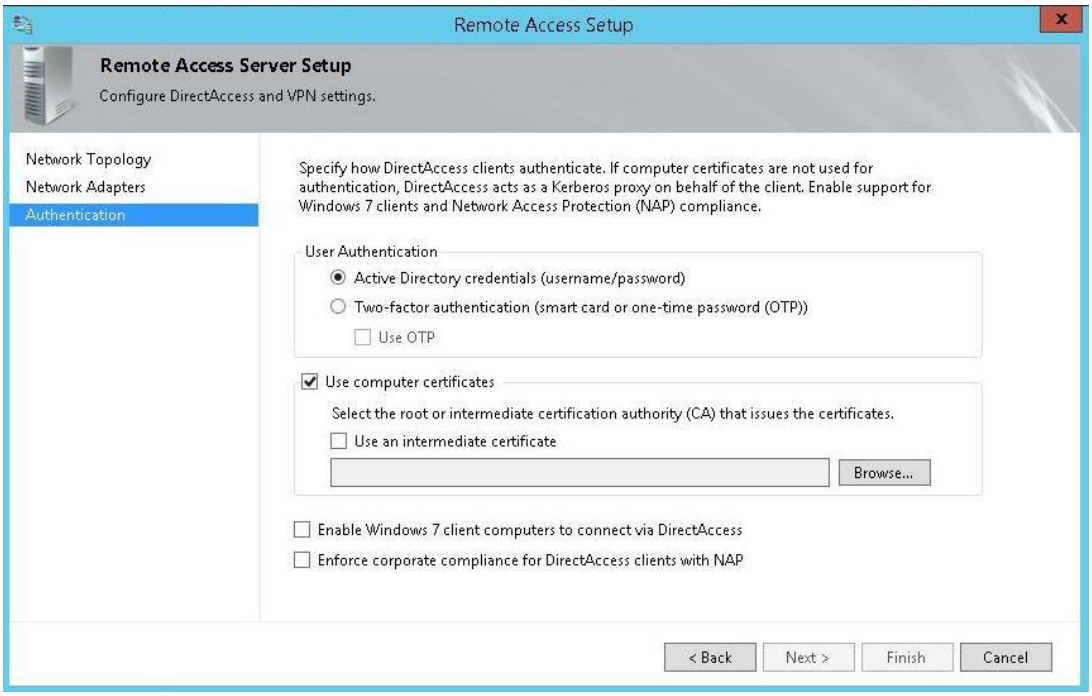
s. Cửa sổ **Network Topology**, kiểm tra chon **Edge**, nhập **131.107.0.2**, và chọn **Next**.



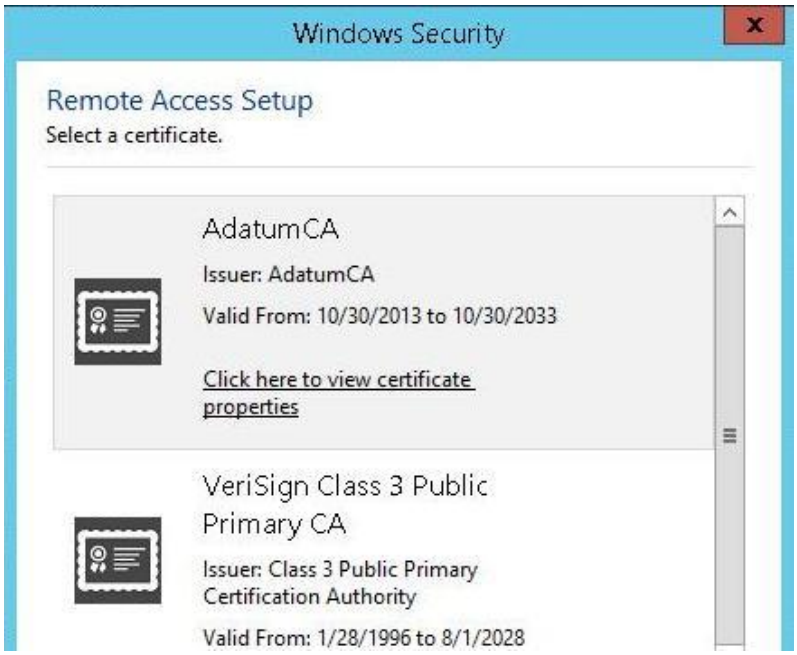
t. Cửa sổ **Network Adapters**, kiểm tra ô **Select the certificate used to authenticate IP-HTTPS connections** đang chọn **CN=131.107.0.2**, và chọn **Next**.



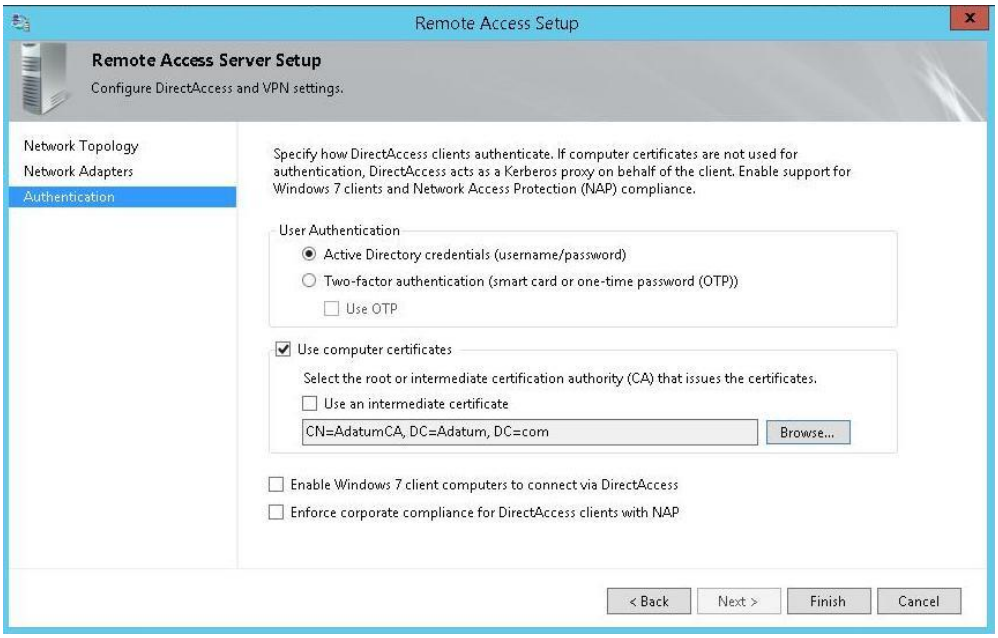
u. Cửa sổ **Authentication**, chọn **Use computer certificates**, chọn **Browse**.



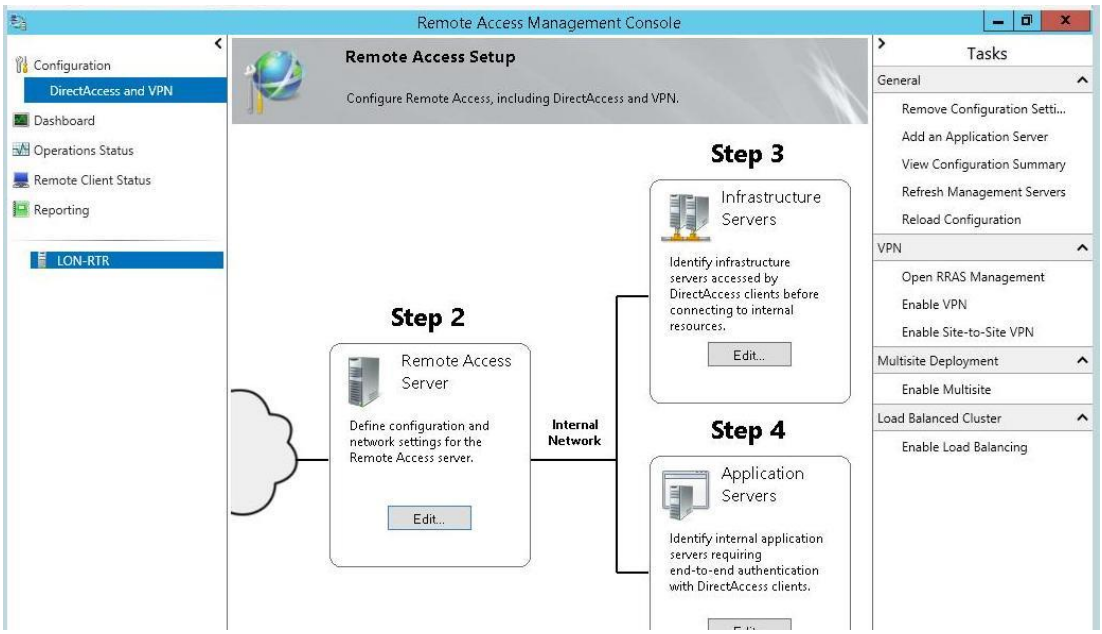
v. Hộp thoại **Windows Security**, chọn **AdatumCA**, chọn **OK**.



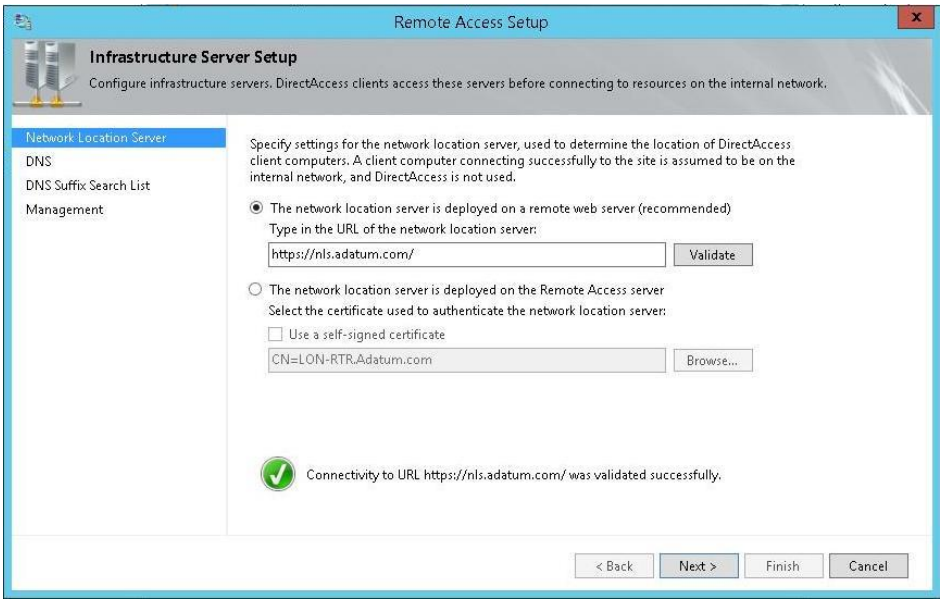
w. Cửa sổ **Authentication**, chọn **Finish**



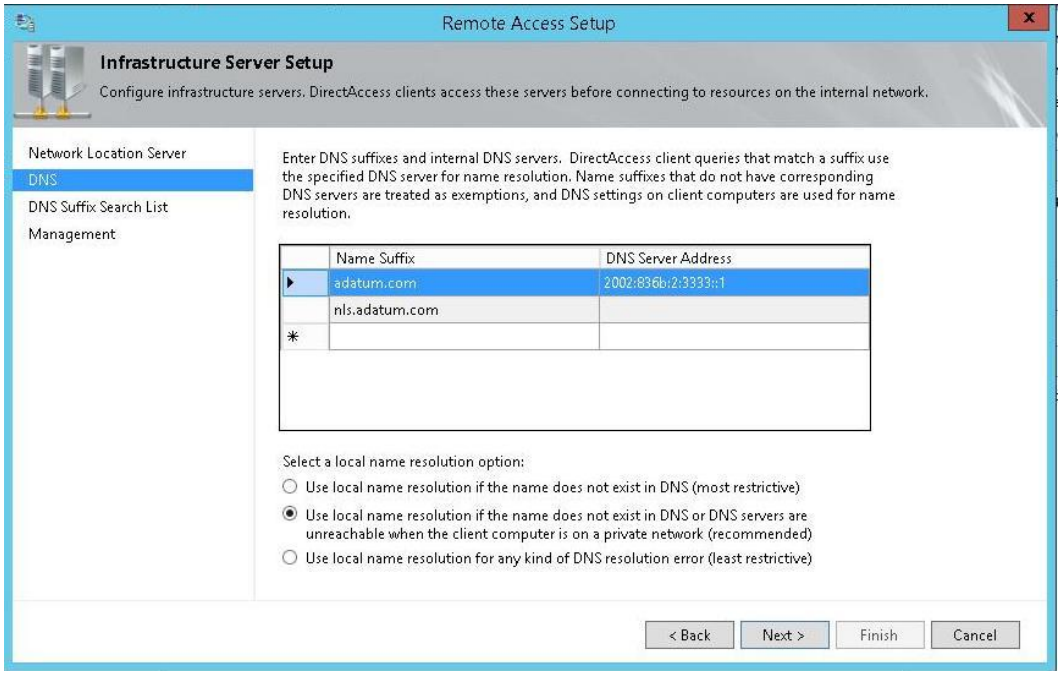
x. Cửa sổ **Remote Access Setup**, trong ô **Step 3**, chọn **Edit**.



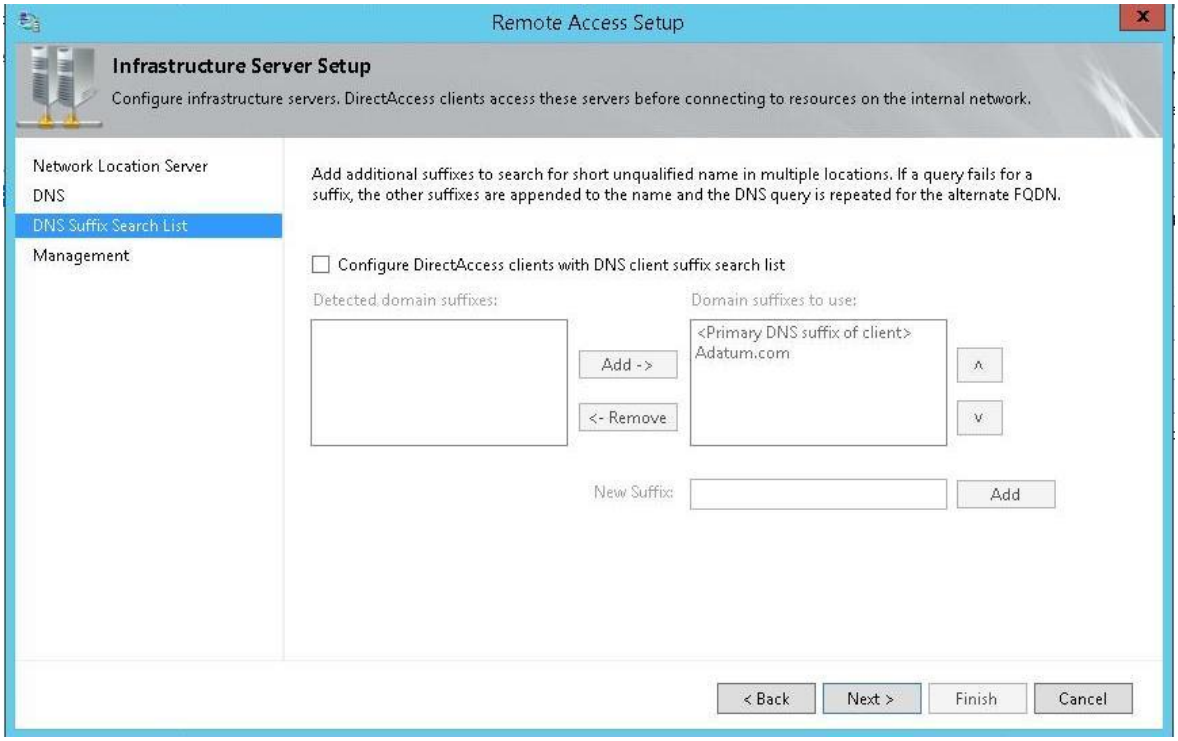
y. Cửa sổ **Network Location Server**, chọn **The network location server is deployed on a remote web server (recommended)**. Trong ô **Type in the URL of the network location server**, nhập **https://nls.adatum.com**, và chọn **Validate,** và chọn **Next**.



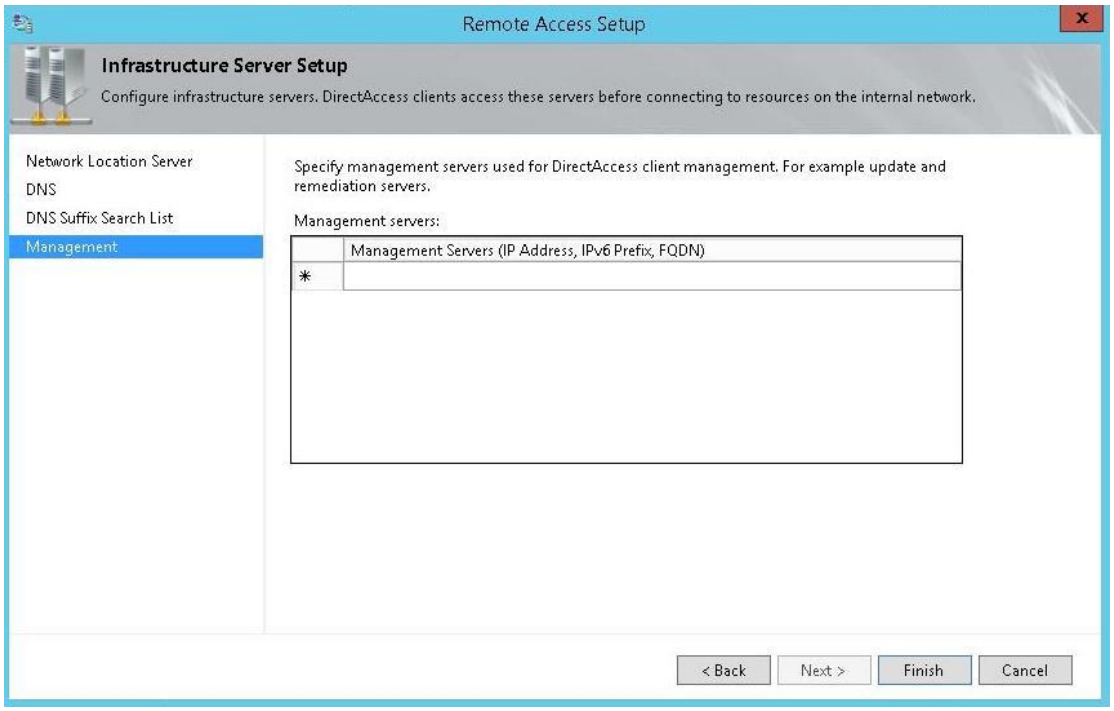
z. Cửa sổ **DNS**, chọn **Next**.



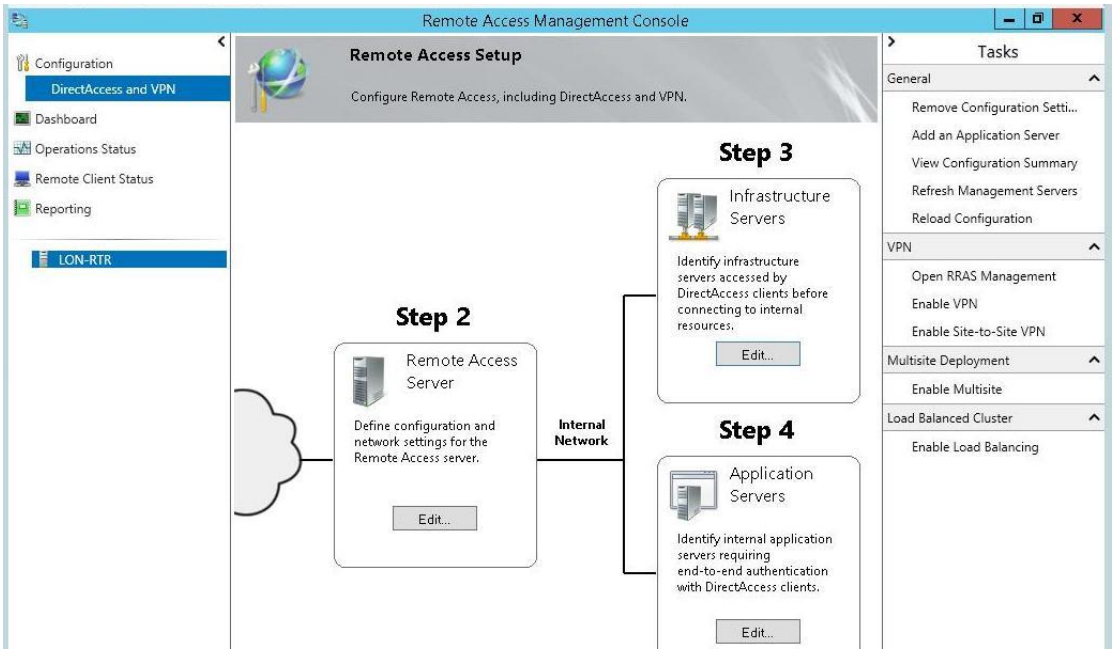
aa. Trong **DNS Suffix Search List**, chọn **Next**.



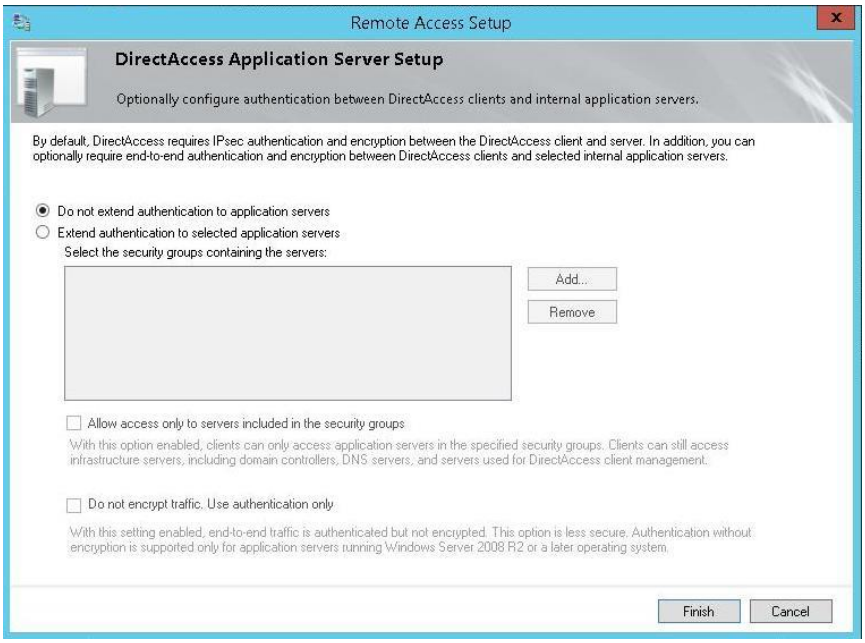
bb. Cửa sổ **Management**, chọn **Finish**.



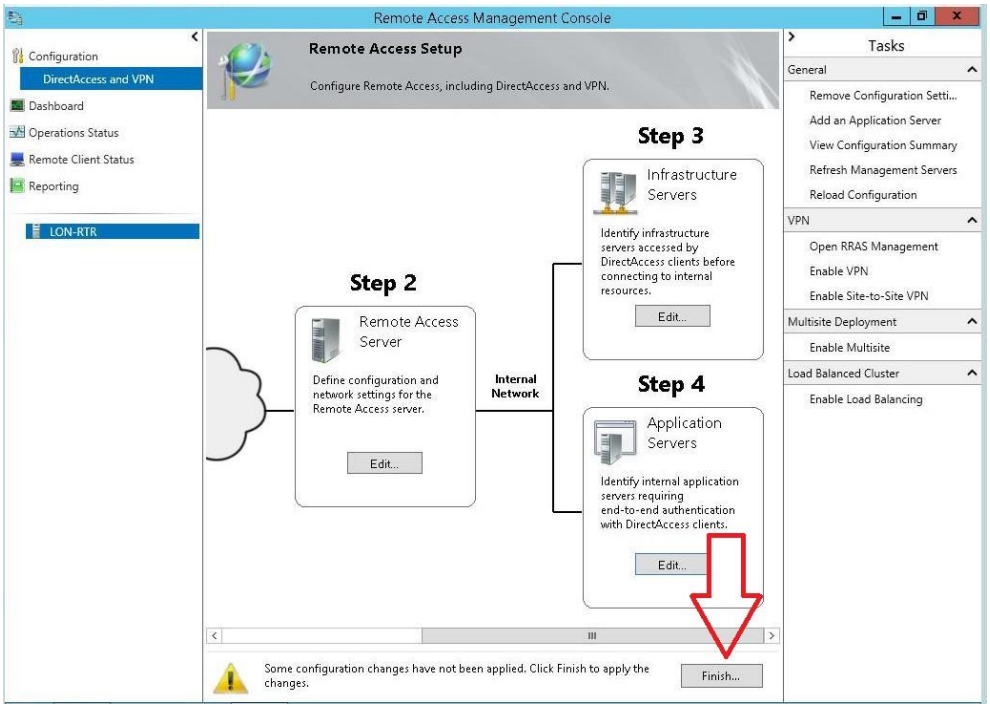
bb. Cửa sổ **Remote Access Management**, trong ô **Step 4**, chọn **Edit**.



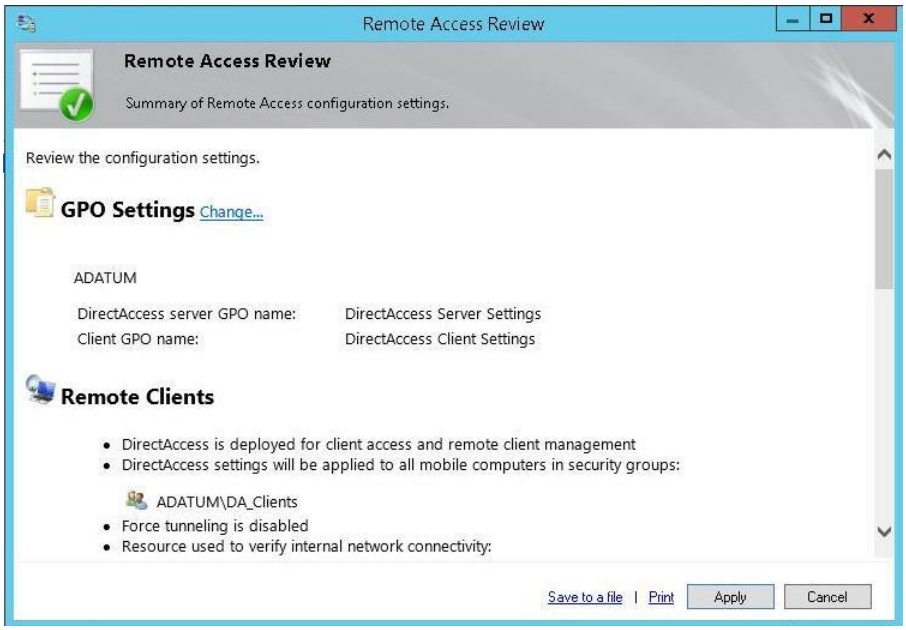
cc. Cửa sổ **DirectAccess Application Server Setup**, chọn **Finish**.



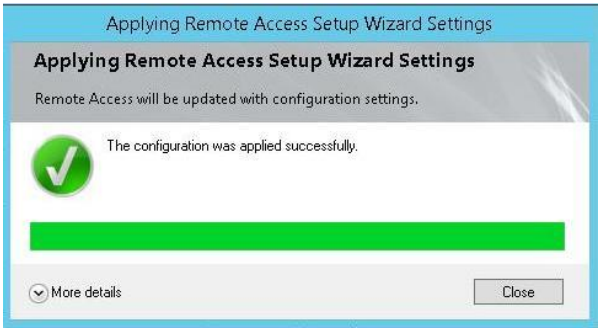
dd. Trong cửa sổ **Remote Access Management,** chọn **Finish**.



ee. Hộp thoại **Remote Access Review**, chọn **Apply**.



ff. Hộp thoại **Applying Remote Access Setup Wizard Settings**, chọn **Close**.



6. Cập nhật Group Policy:

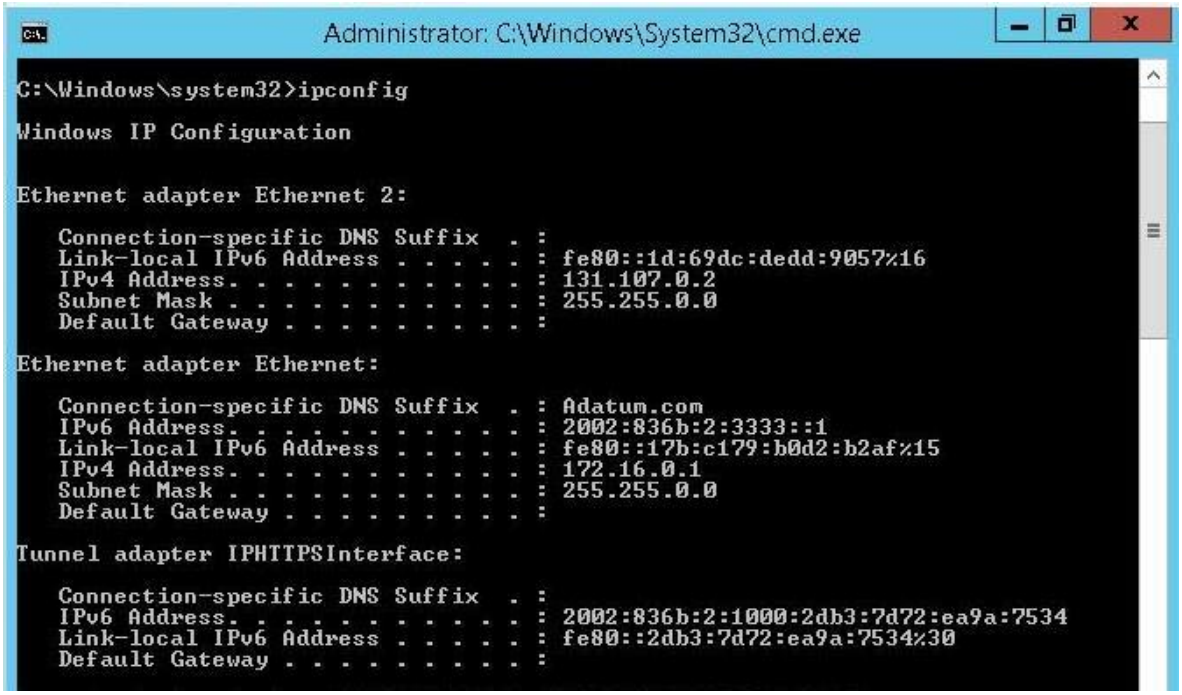
a. Trên LON-RTR, Di chuyển con trỏ chuột đến góc dưới bên phải màn hình, chọn **Search**.

b. Mở **cmd**, gõ lệnh: **gpupdate /force**



c. Trong cửa sổ **Command prompt**, gõ lệnh: i**pconfig**

Kiểm tra địa chỉ IPv6 của **Tunnel adapter IPHTTPSInterface** bắt đầu với **2002**.



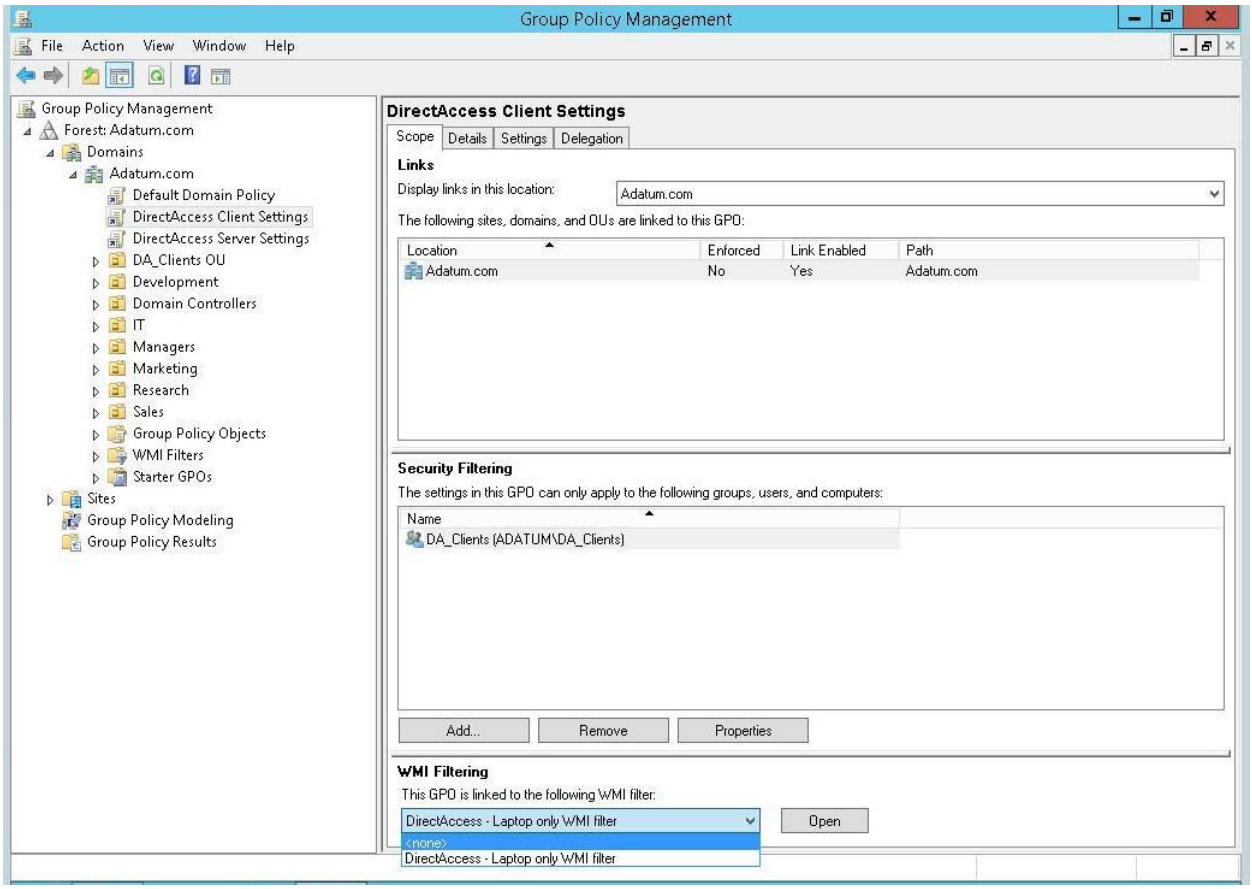
Bước 5. Triển khai GPO để thiết lập cấu hình DirectAccess.

1. Qua máy LON-DC1.

2. Trong **Server Manager**, bung menu **Tools**, mở **Group Policy Management**.

3. Trong cửa sổ **Group Policy Management Console**, bung **Adatum.com**, chọn **DirectAccess Client Settings**.

4. Bung **WMI Filtering**, chọn **DirectAccess – Laptop only WMI filter**, và chọn **<none>**.



5. Hộp thoại **Group Policy Management**, chọn **Yes**.



6. Tắt **Group Policy Management Editor** và **Group Policy Management Console**.

7. Khởi động máy **LON-CL1**, logon **Adatum\Administrator** với password **Pa$$w0rd**.

8. Mở **cmd**, gõ lệnh: **gpupdate /force**



9. Trong Command prompt, gõ lệnh: **gpresult /R**

Kiểm tra: Trong phần Applied Group Policy Objects, có GPO DirectAccess Client Settings.

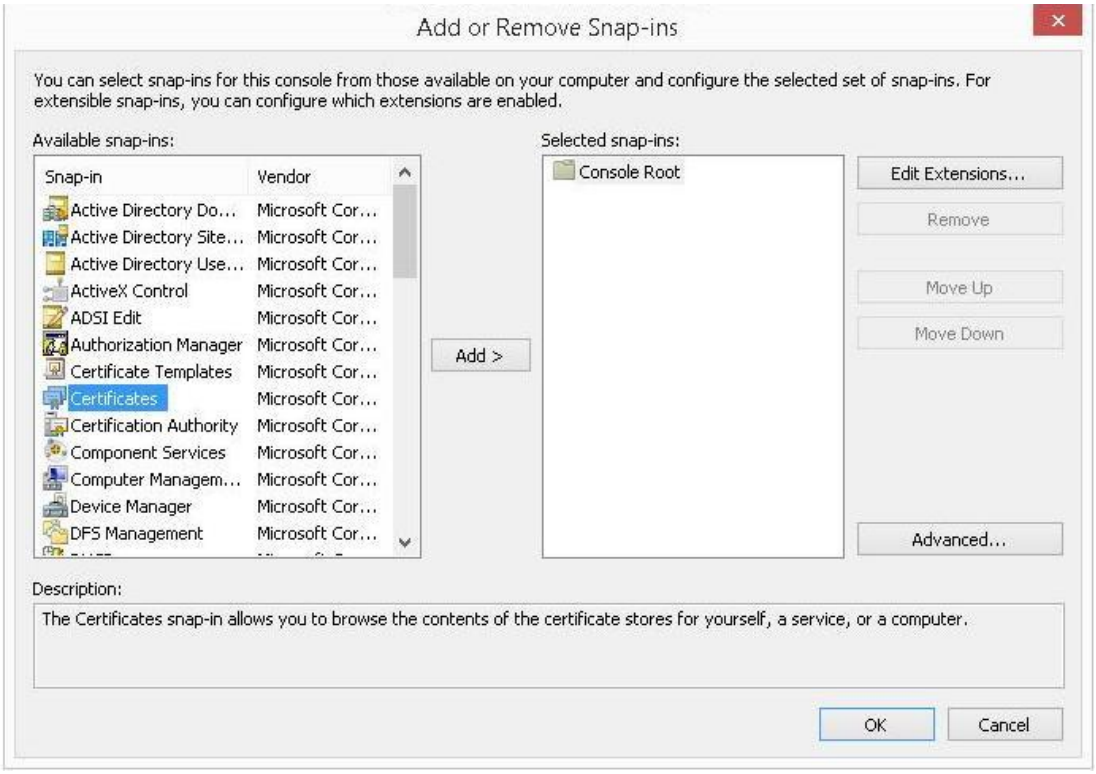


Bước 6. Kiểm tra certificate distribution.

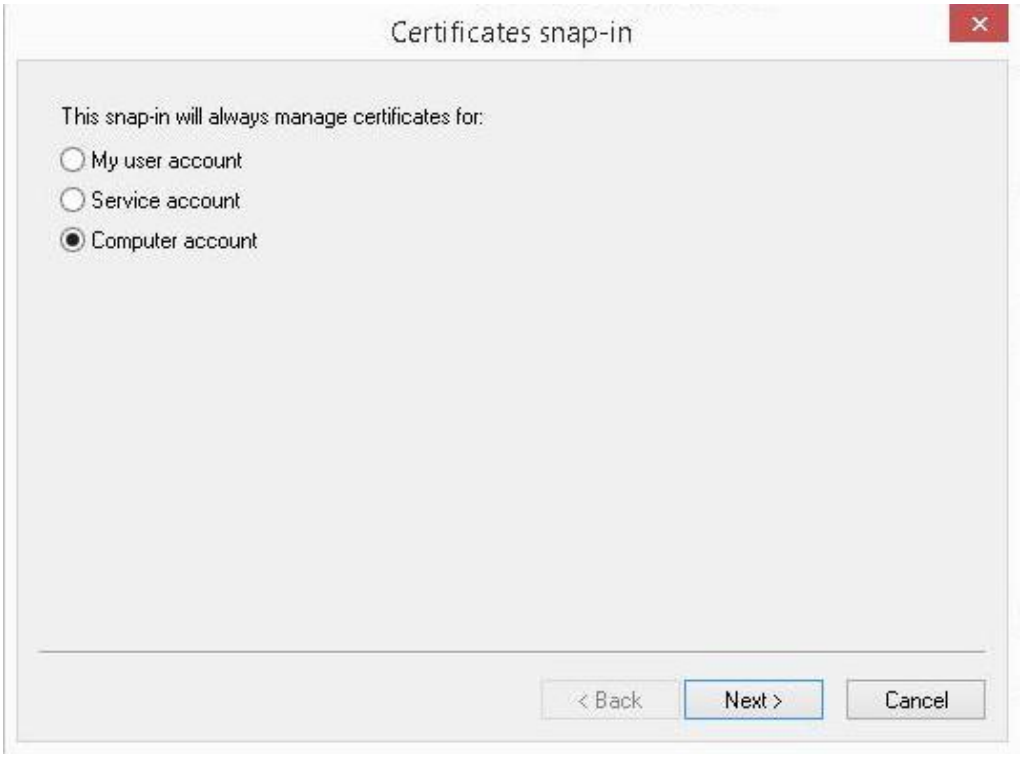
1. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.



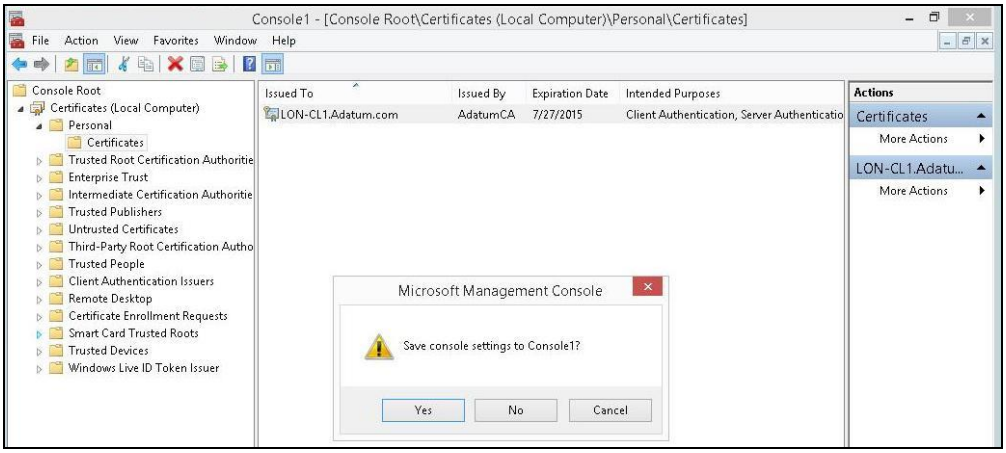
2. Hộp thoại **Add/Remove Snap-in**, chọn **Certificates**, chọn **Add**.



3. Cửa sổ **Certificates snap-in,** Chọn **Computer account**, và chọn **Next**, chọn **Finish**, và chọn **OK**.



4. Trong cửa sổ **Console1**, bung **Certificates (Local Computer)**, bung **Personal**, achọn **Certificates**. Kiểm tra có certificate **LON-CL1.adatum.com** có chức năng **Client Authentication** và **Server Authentication**. Tắt cửa sổ **Console1**, chọn **No**.

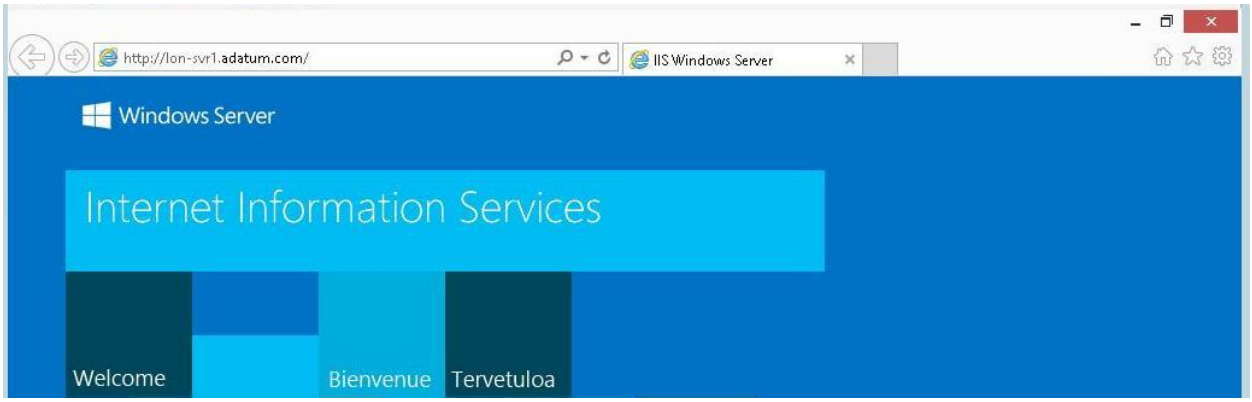


Bước 7. Kiểm tra cấu hình IP.

1. Trên máy **LON-CL1**.

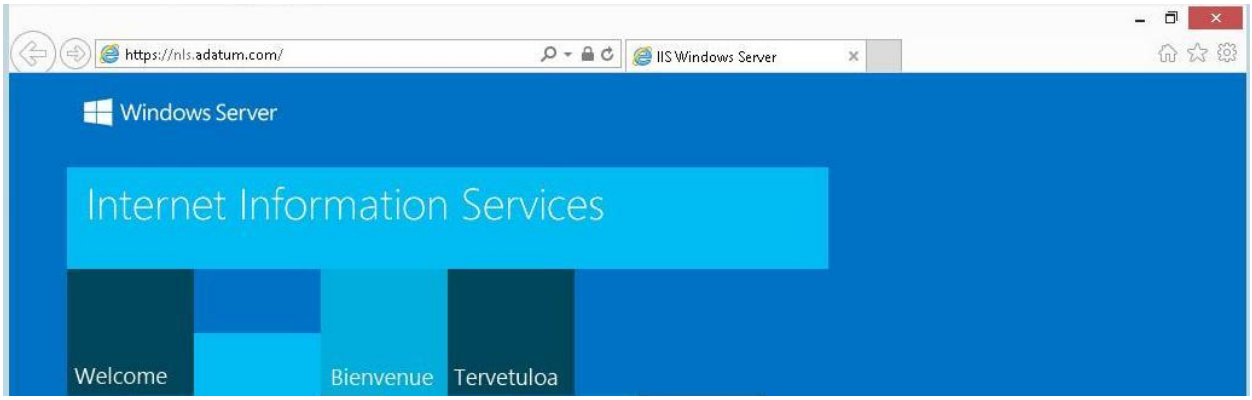
2. Mở **Internet Explorer,** truy cập **http://lon-svr1.adatum.com**

Kiểm tra truy cập thành công Website IIS 8 của **LON-SVR1**.



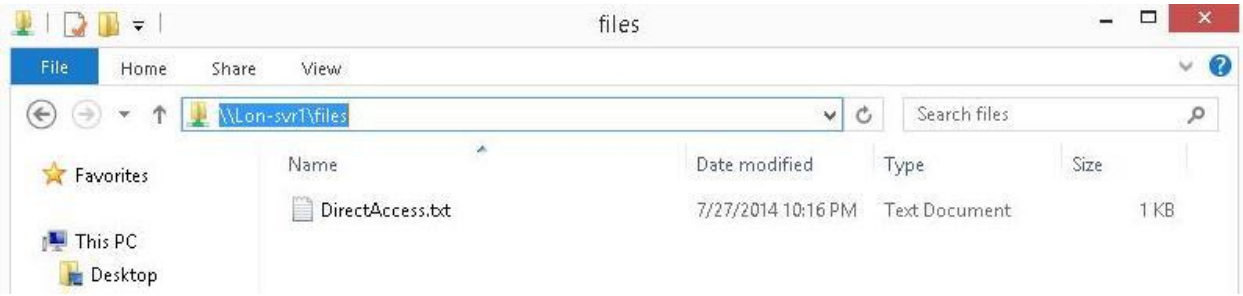
3. Truy cập **https://nls.adatum.com/**

Kiểm tra truy cập thành công Website IIS 8 của **LON-SVR1**.



4. Mở **File Explorer**, truy cập **\\Lon-SVR1\Files**, và nhấn Enter.

Kiểm tra truy cập thành công folder **Files**.



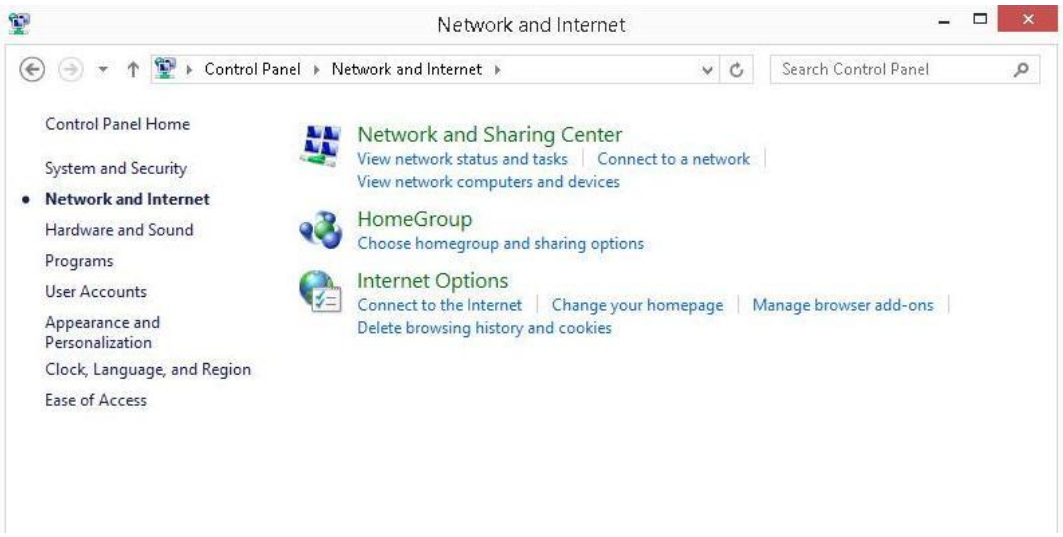
Bước 8. Di chuyển LON-CL1 ra ngoài, và kiểm tra kết nối vào nội bộ.

1. Trên máy **LON-CL1**.

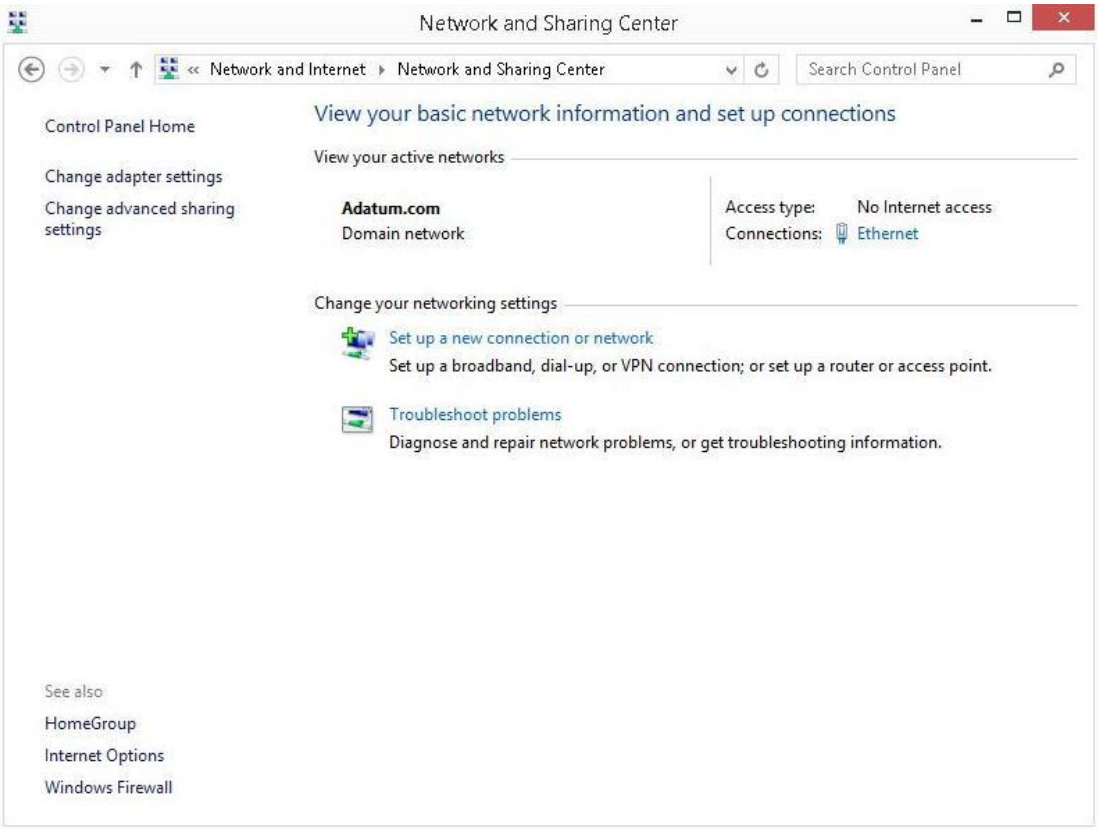
2. Mở **Control Panel**, chọn **Network and Internet**.



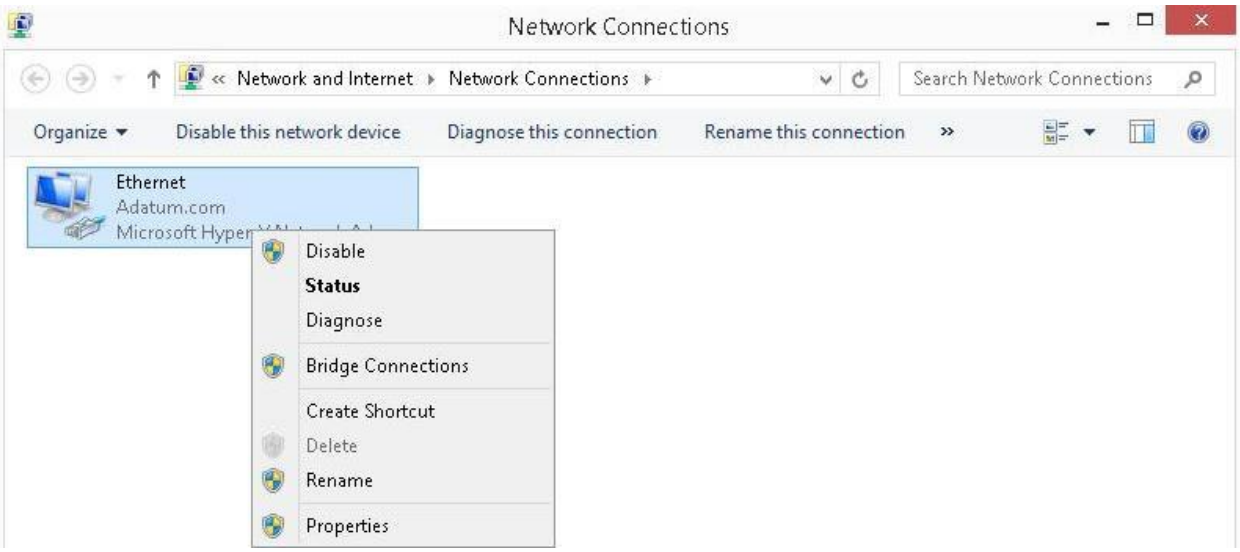
3. Cửa sổ **Network and Internet**, chọn **Network and Sharing Center**.



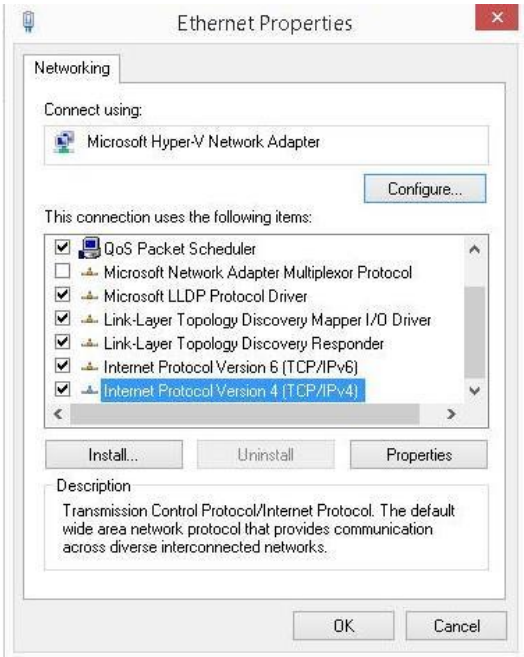
4. Cửa sổ **Network and Sharing Center**, chọn **Change adapter settings**.



5. Nhấn chuột phải **Ethernet**, chọn **Properties**.

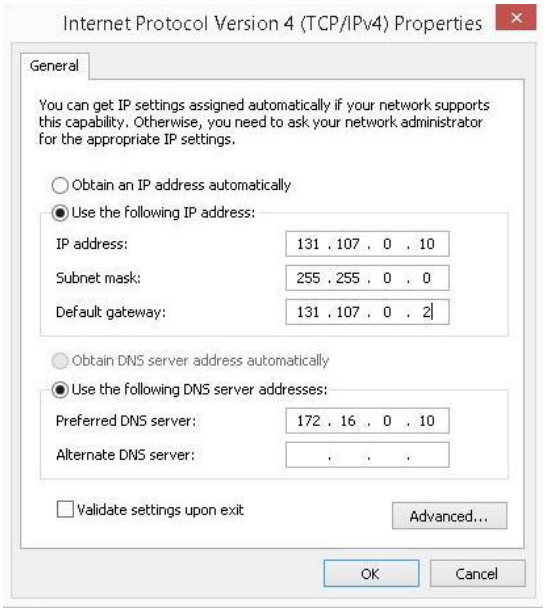


6. Hộp thoại **Ethernet Properties**, nhấp đôi chuột **Internet Protocol Version 4**

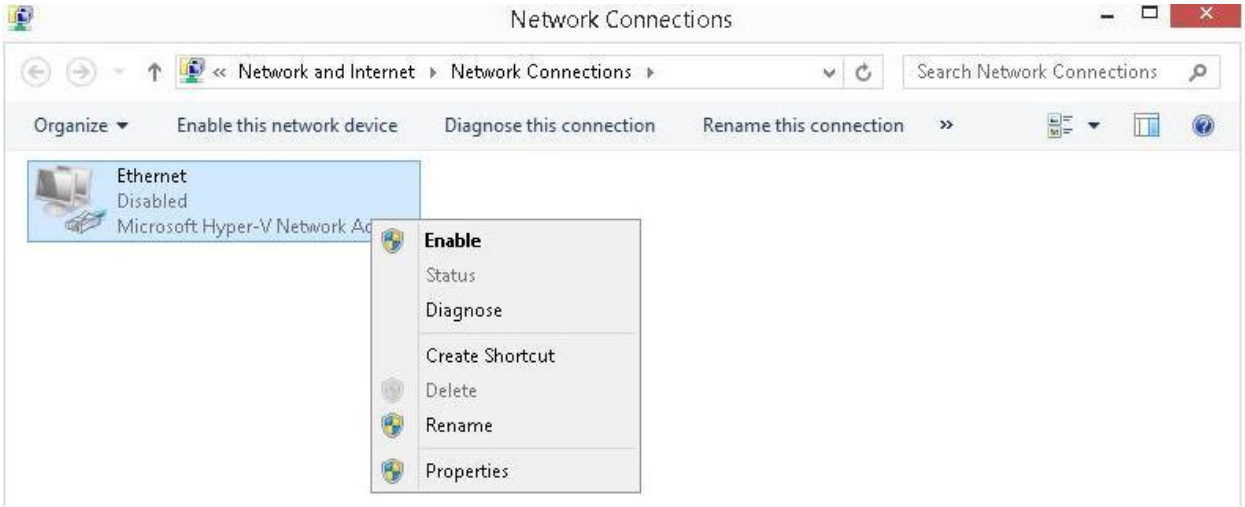


7. Hộp thoại **Internet Protocol Version 4 (TCP/IPv4) Properties**, cấu hình thông số TCP/IP như sau và chọn **OK** 2 lần:

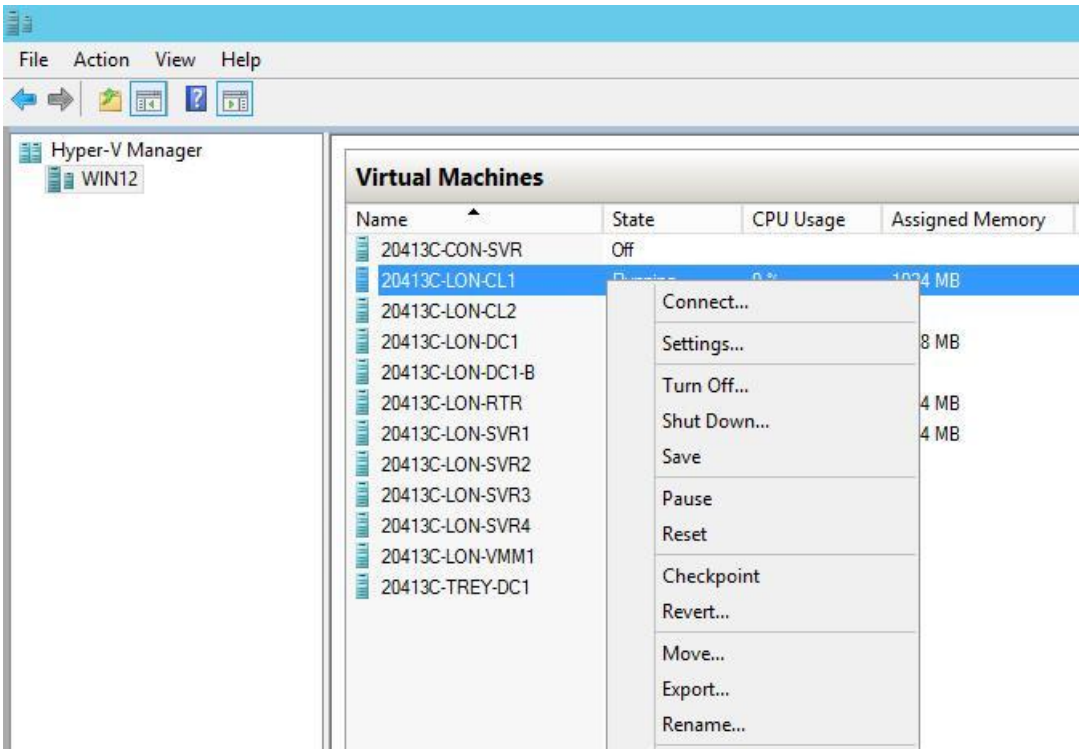
- IP address: **131.107.0.10**
- Subnet mask: **255.255.0.0**
- Default gateway: **131.107.0.2**



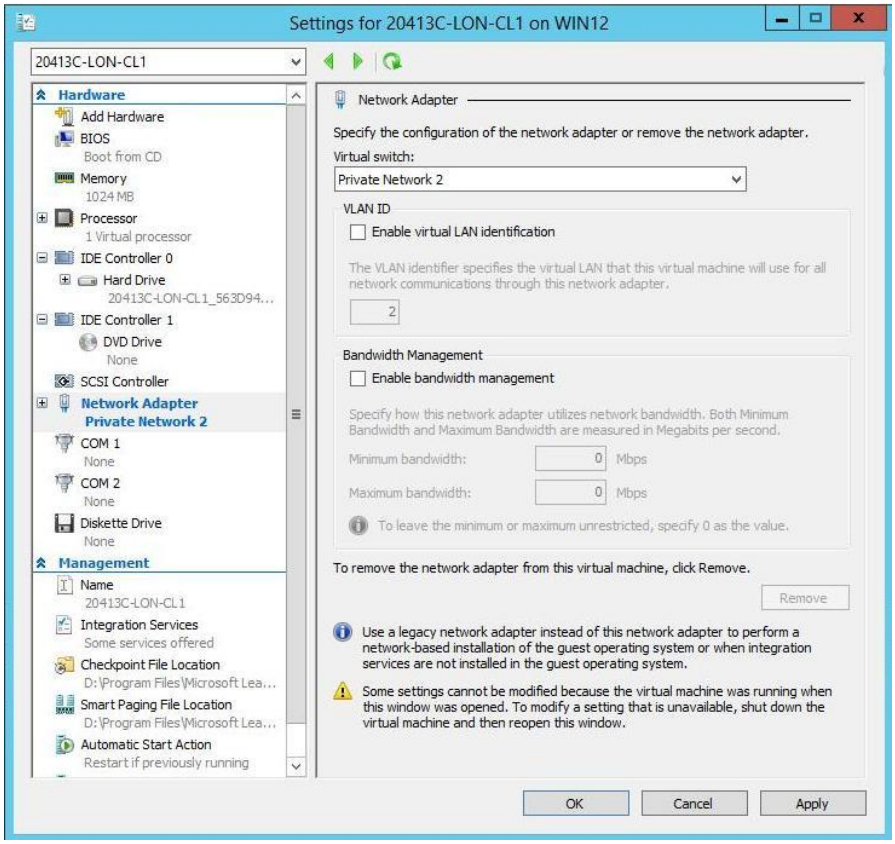
8. Cửa sổ **Network Connections**, nhấn chuột phải **Ethernet**, chọn **Disable**. Sau đó nhấn chuột phải **Ethernet**, chọn **Enable**.



9. Trên máy thật, mở **Hyper-V Manager**, nhấn chuột phải máy ảo **20413C-LON-CL1**, chọn **Settings**.



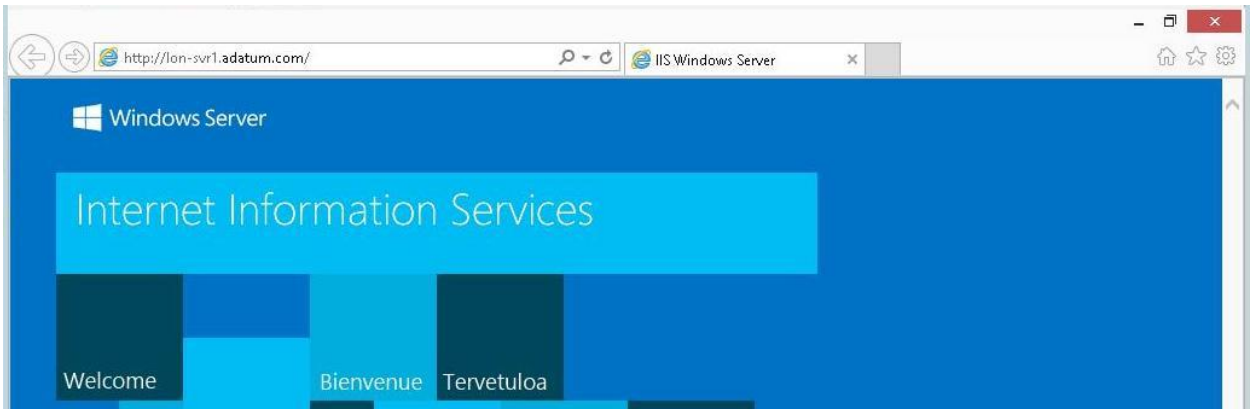
10. Chọn **Network Adapter**, bung **Virtual Switch**, chọn **Private Network 2**, chọn **OK**.



11. Qua máy **LON-CL1**.

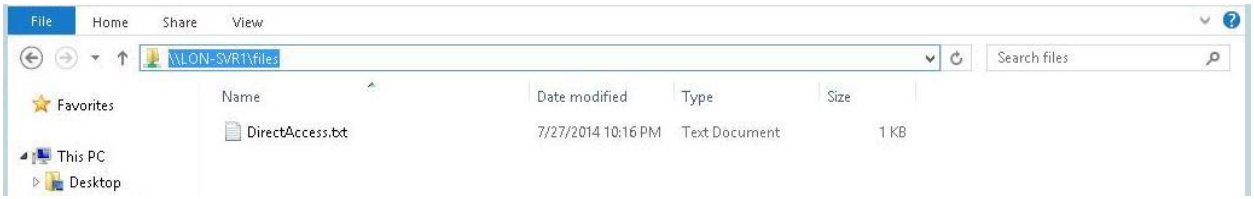
12. Mở **Internet Explorer,** truy cập **http://lon-svr1.adatum.com**

Kiểm tra truy cập thành công Website IIS 8 của **LON-SVR1**.



13. Mở **File Explorer**, truy cập **\\LON-SVR1\Files**

Kiểm tra truy cập thành công folder **Files**.



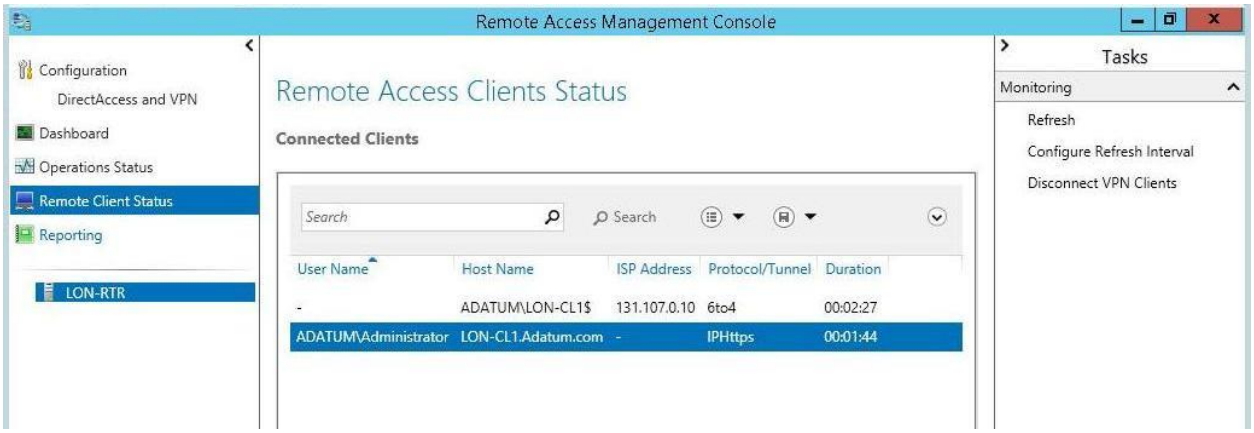
14. Mở **cmd**, gõ lệnh: **ping lon-dc1.adatum.com**

Kiểm tra ping máy lon-dc1.adatum.com thành công.



15. Qua máy **LON-RTR**.

16. Mở **Remote Access Management**, chọn **Remote Client Status**. Kiểm tra **LON-CL1** đang kết nối bằng **IP-HTTPS.**



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công giải pháp DirectAccess.

❖ **Chuẩn bị cho bài tiếp theo:**

Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20413C-LON-RTR, 20413C-LON-SVR1 và 20413C-LON-CL1.**
5. Trong cửa sổ **Hyper-V® Manager**, nhấn chuột phải **20413C-LON-DC1**, chọn **Start**.
6. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
7. Logon vào máy **20413C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
8. Thực hiên từ bước 5 đến 7 cho máy ảo **20413C-LON-SVR1, 20413C-LON-RTR, 20413C-LON-CL1,** và **20413C-LON-CL2.**

Bài tập 2: Triển khai giải pháp VPN

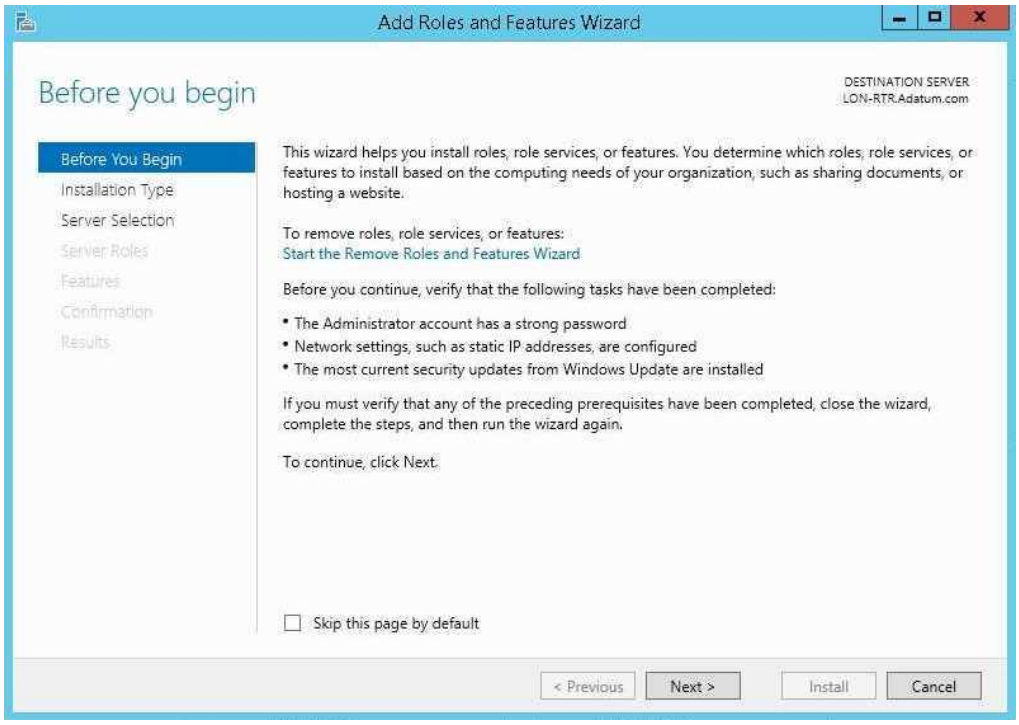
❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt và cấu hình Remote Access Server.
2. Tạo Network Policies.
3. TạoVPN Connection.
4. Kiểm tra kết nối VPN.

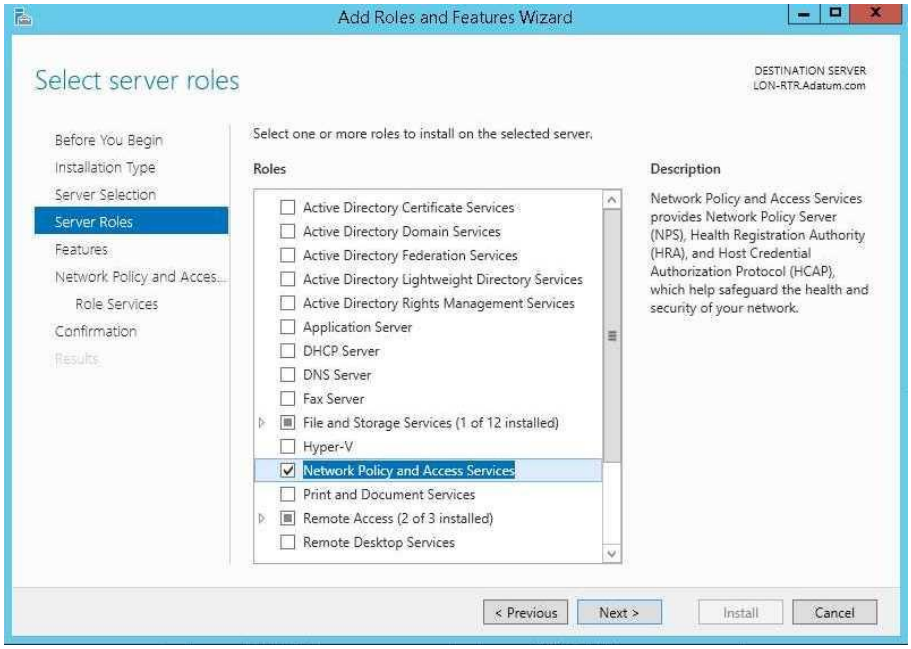
❖ **Thực hiện:**

Bước 1. Cài đặt và cấu hình Remote Access Server.

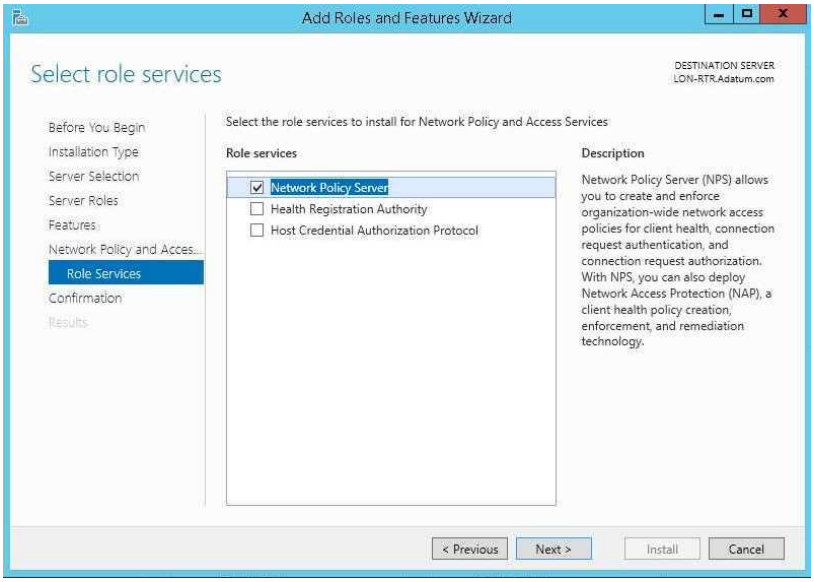
1. Qua máy **LON-RTR,** logon **Adatum\Administrator** với password **Pa$$w0rd**.
2. Mở **Server Manager**, chọn **Add roles and features**.
3. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



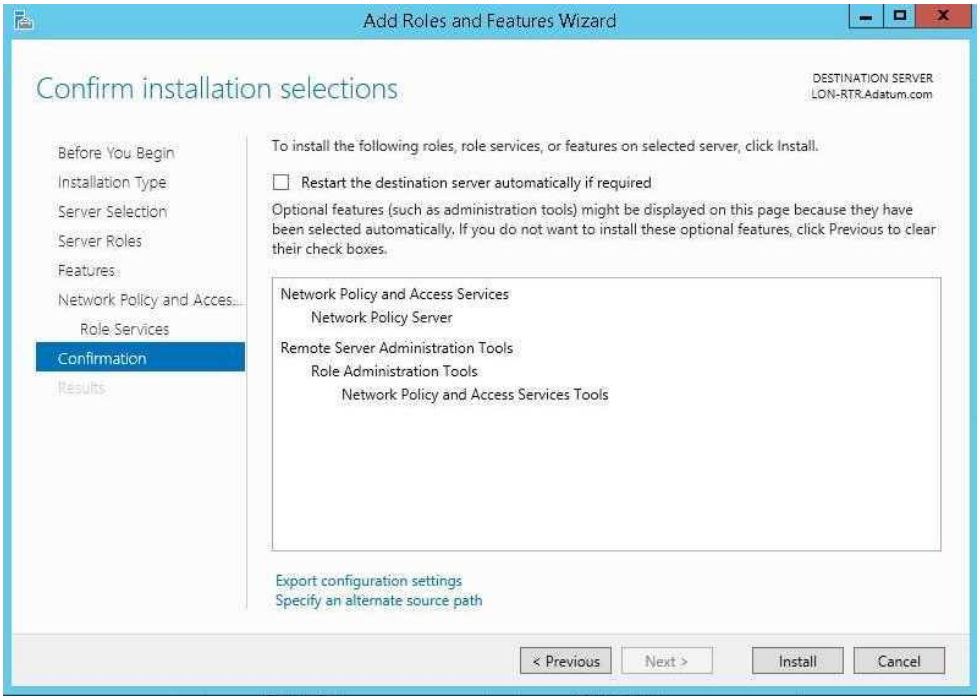
4. Cửa sổ **Select server roles**, đánh dấu chọn **Network Policy and Access Services**, chọn **Add Features**, và chọn **Next** 3 lần.



5. Cửa sổ **Select role services**, kiểm tra có đánh dấu chọn **Network Policy Server**, chọn **Next**.

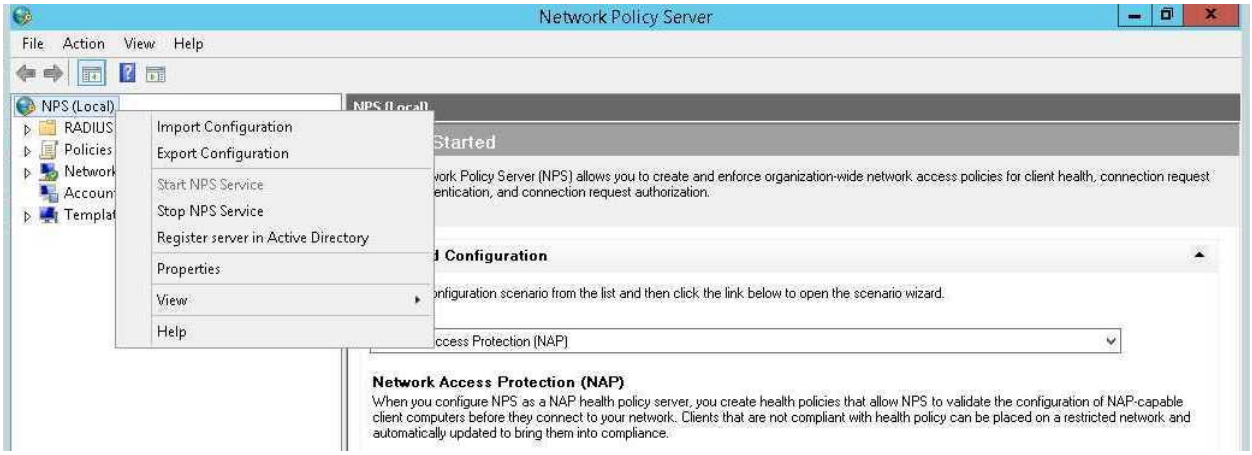


6. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.

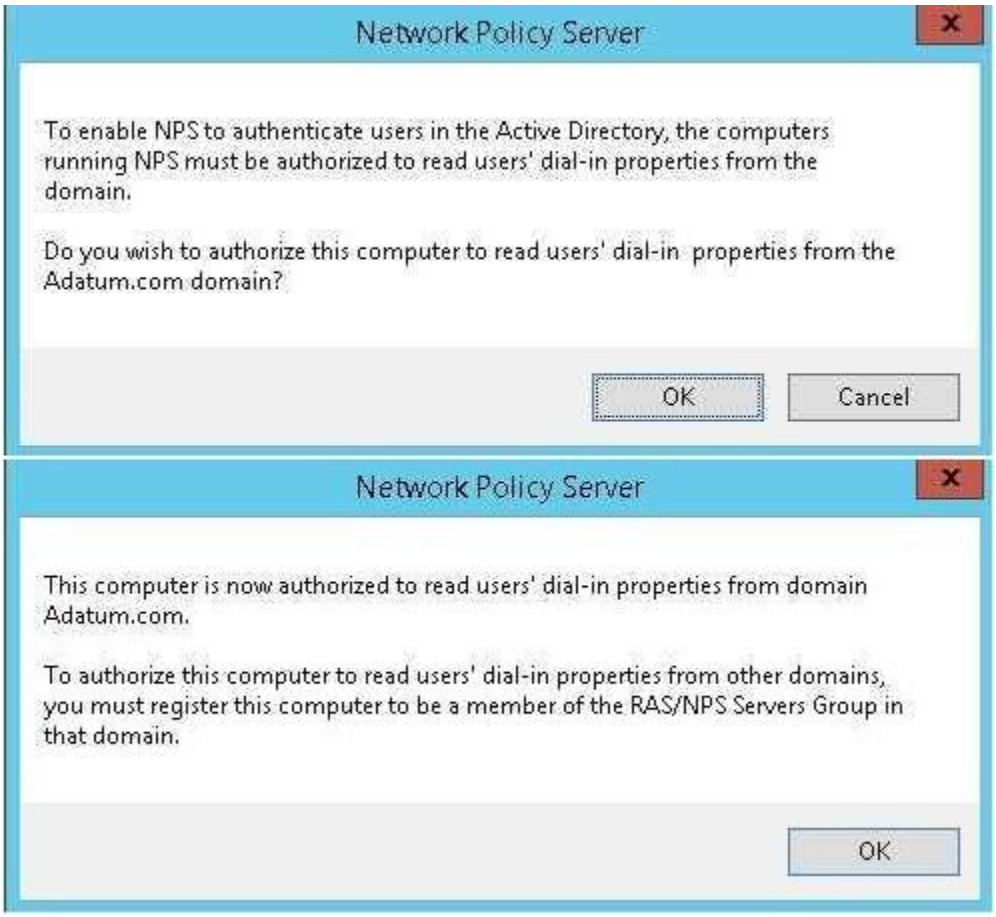


7. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Network Policy Server**.

8. Trong cửa sổ **Network Policy Manager**, nhấn chuột phải **NPS (Local)**,chọn **Register server in Active Directory**.



9. Trong 2 hộp thoại **Network Policy Server**, chọn **OK**.

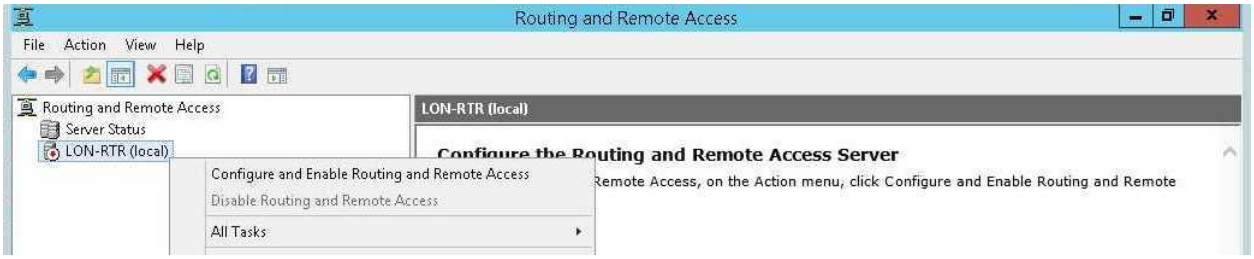


10. Qua cửa sổ **Server Manager**, bung menu **Tools**, mở **Routing and Remote Access.**

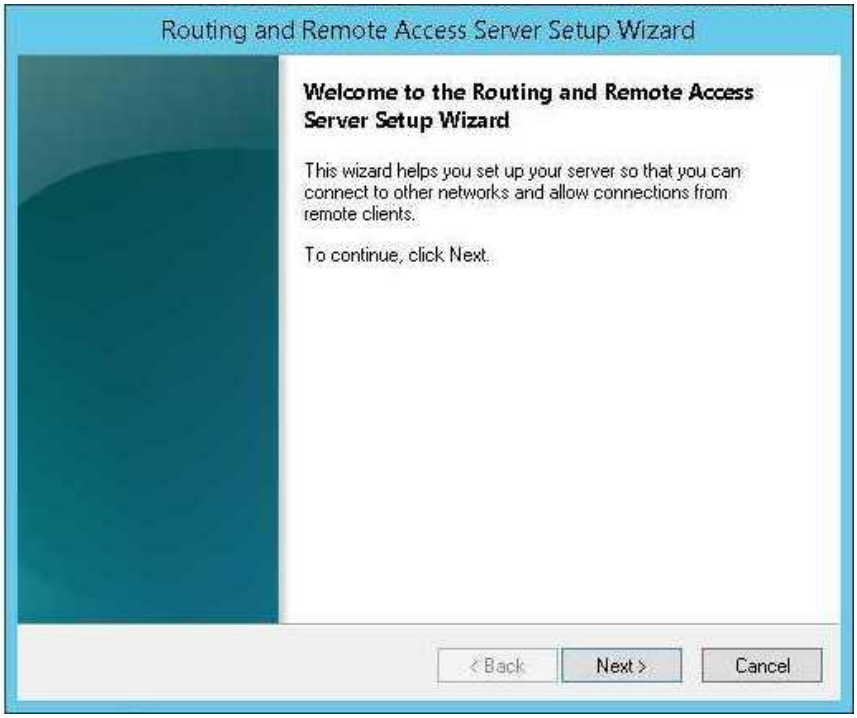
11. Trong cửa sổ **Routing and Remote Access**, nhấn chuột phải **LON-RTR**, chọn **Disable Routing And Remote Access**. chọn **Yes**.



12. Cửa sổ **Routing and Remote Access**, nhấn chuột phải **LON-RTR**, chọn **Configure and Enable routing and remote access**.



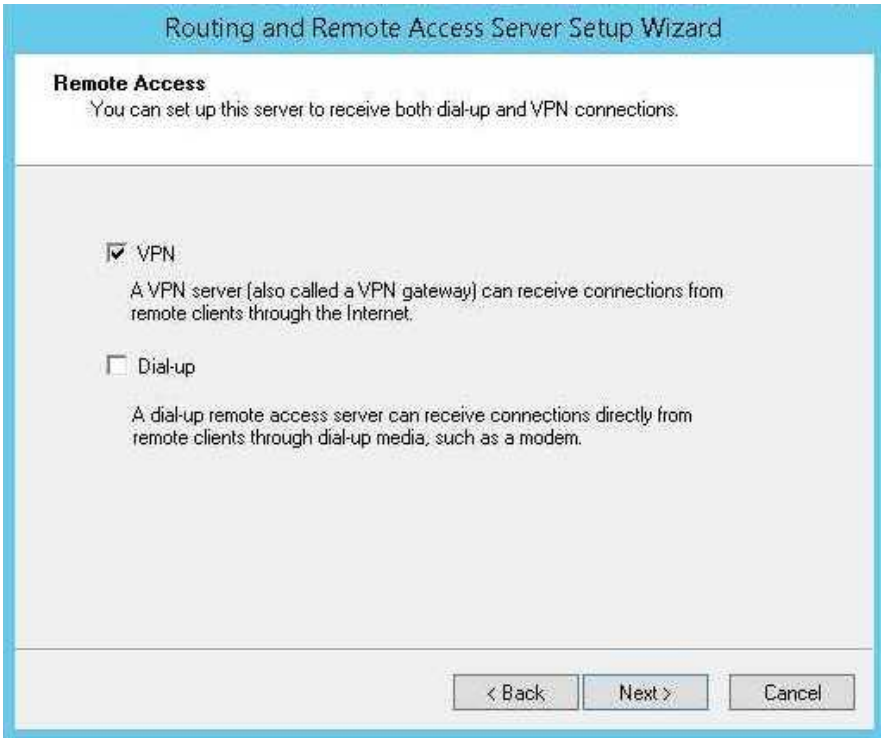
13. Cửa sổ **Welcome to the Routing and Remote Access Server Setup Wizard**, chọn **Next**.



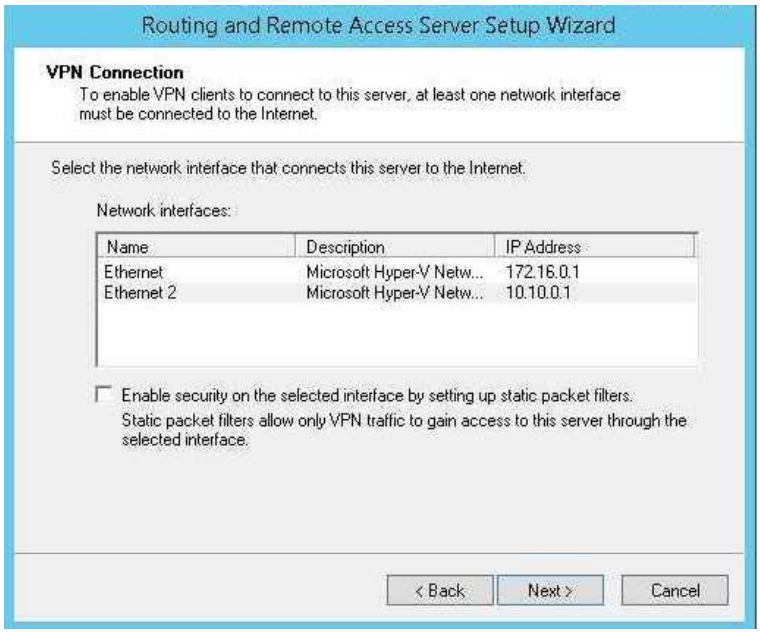
14. Cửa sổ **Configuration**, chọn **Remote access (dial-up or VPN),** và chọn **Next**.



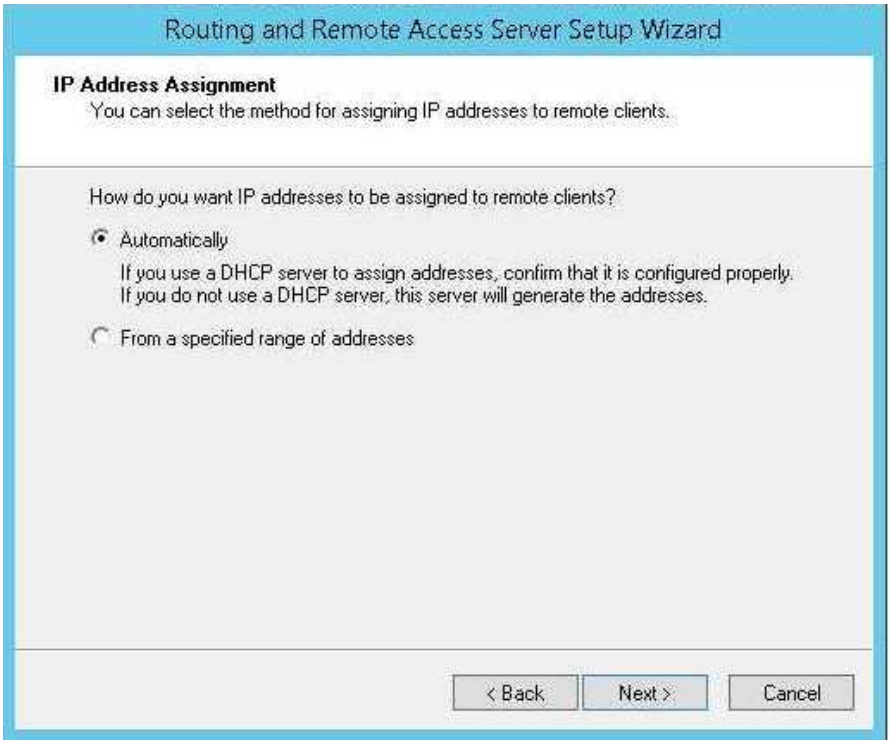
15. Cửa sổ **Remote Access**, đánh dấu chọn **VPN**, và chọn **Next**.



16. Cửa sổ **VPN Connection**, chọn **Ethernet 2**, bỏ dấu chọn **Enable security**, và chọn **Next**.



17. Cửa sổ **IP Address Assignment**, chọn **Next**.



18. Cửa sổ **Managing Multiple Remote Access Servers**, chọn **Next**, và chọn **Finish**



19. Hộp thoại **Routing and Remote Access ,** chọn **OK** 2 lần.

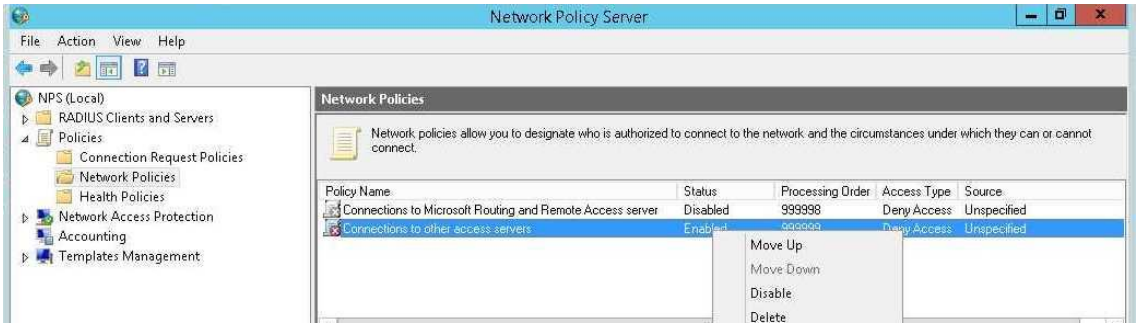


Bước 2. Tạo Network Policies.

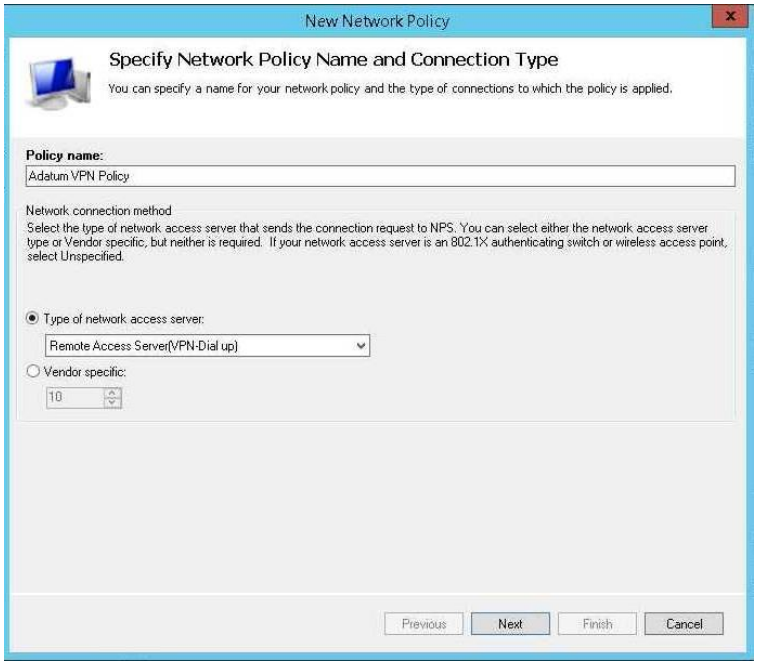
1. Trên máy **LON-RTR**.

2. Mở **Server Manager**, bung menu **Tools**, mở **Network Policy Server**.

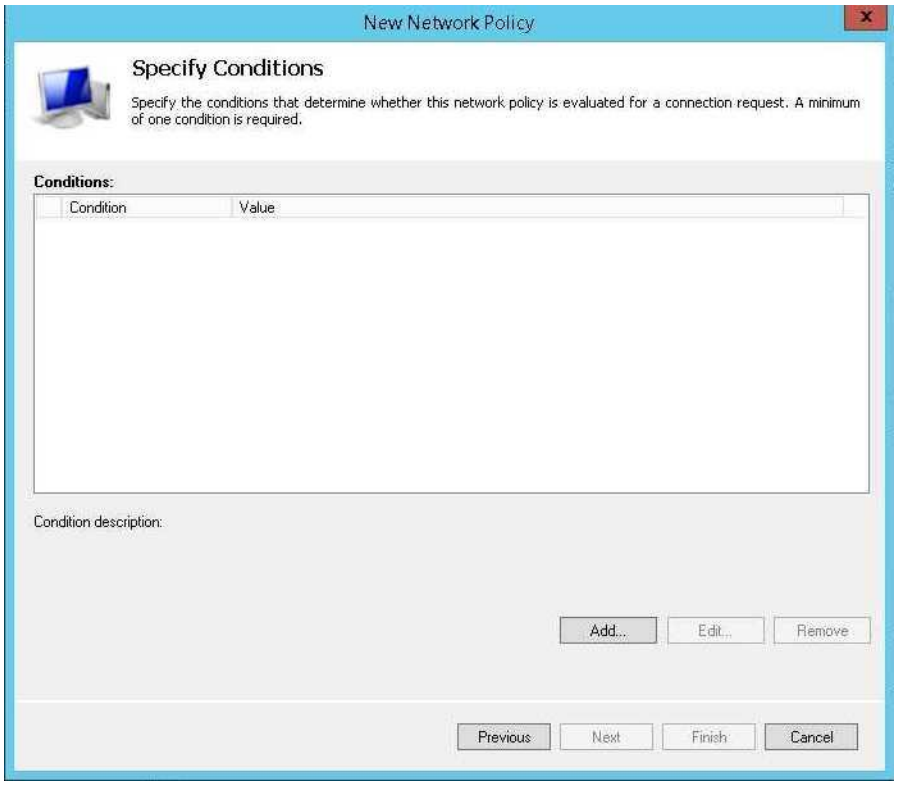
3. Trong cửa sổ **Network Policy Server**, bung **Policies**, chọn **Network Policies**, lần lượt **Disable** 2 policy mặc định.



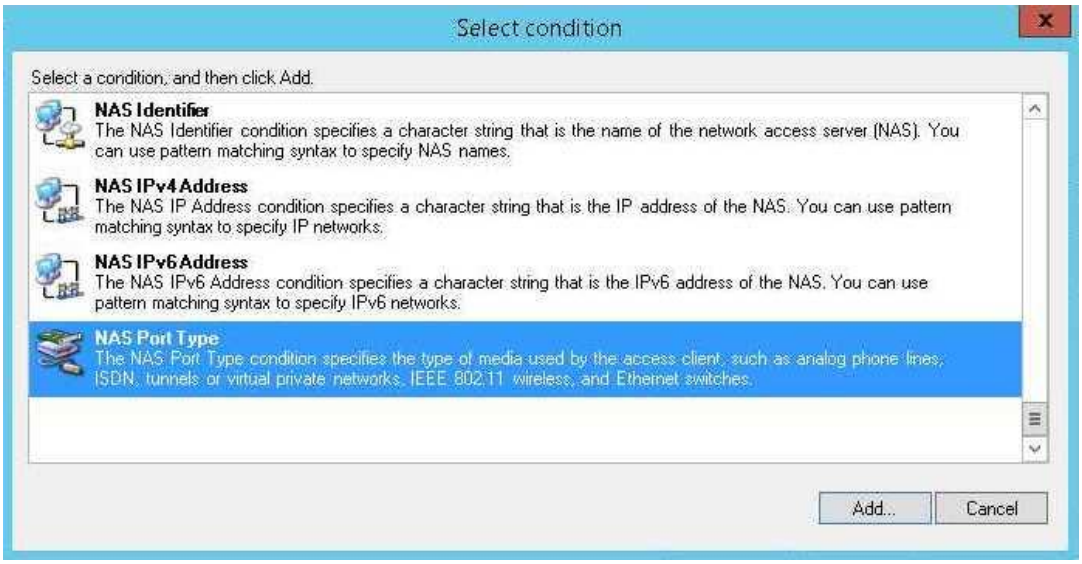
4. Trong cửa sổ **Network Policy Server**, nhấn chuột phải **Network Policies**, chọn **New**. Cửa sổ **Specify Network Policy Name and Connection Type**, trong ô **Policy name**, nhập **Adatum VPN Policy**. Bung ô **Type of network access server**, chọn **Remote Access Server (VPN-Dial up)**, và chọn **Next**.



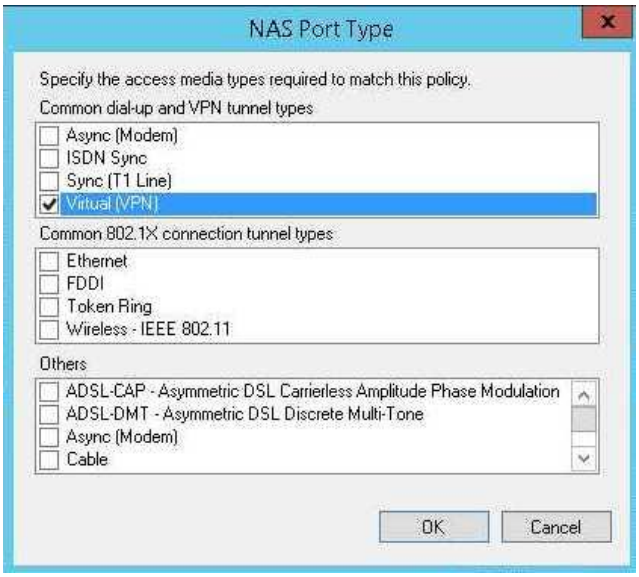
5. Cửa sổ **Specify Conditions**, chọn **Add**.



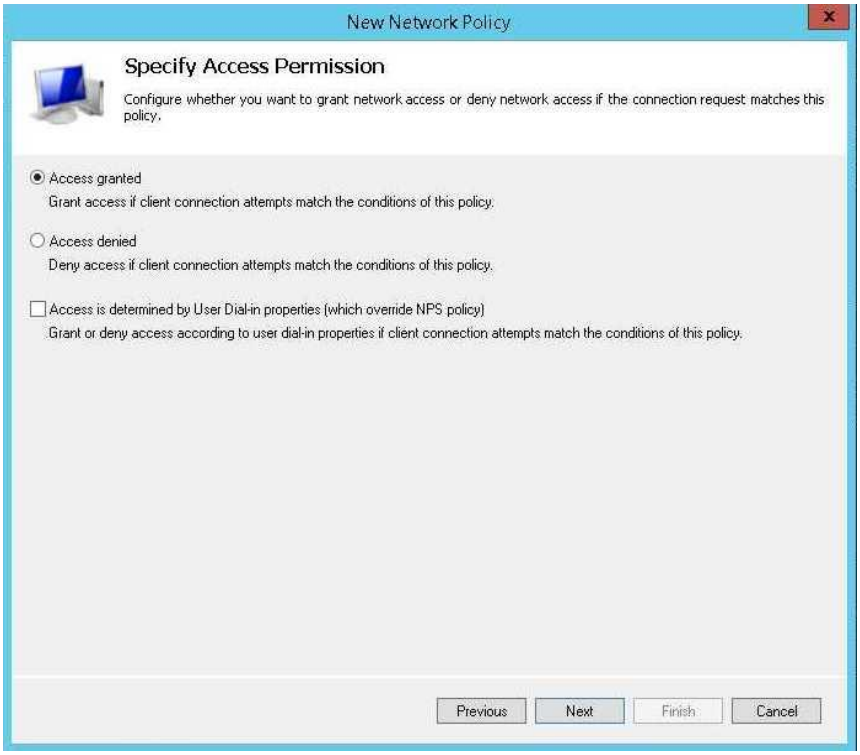
6. Cửa sổ **Select condition**, chọn **NAS Port Type**, và chọn **Add**.



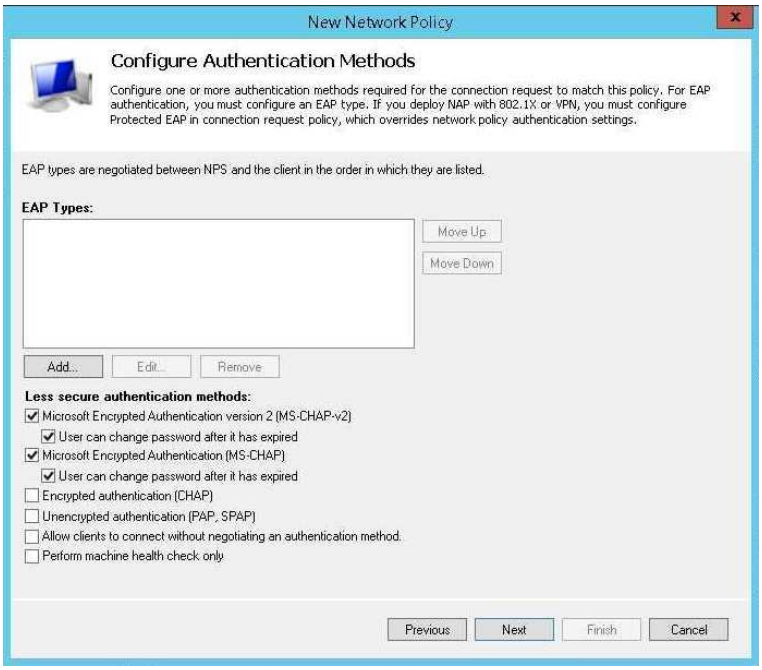
7. Cửa sổ **NAS Port Type**, đánh dấu chọn **Virtual (VPN)**, chọn **OK**, và chọn **Next**.



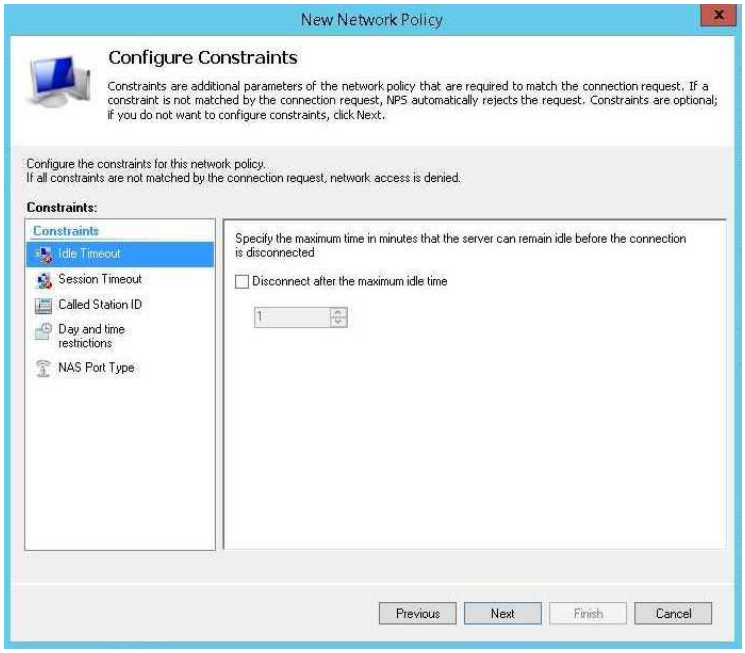
8. Cửa sổ **Specify Access Permission**, chọn **Access granted**, và chọn **Next**.



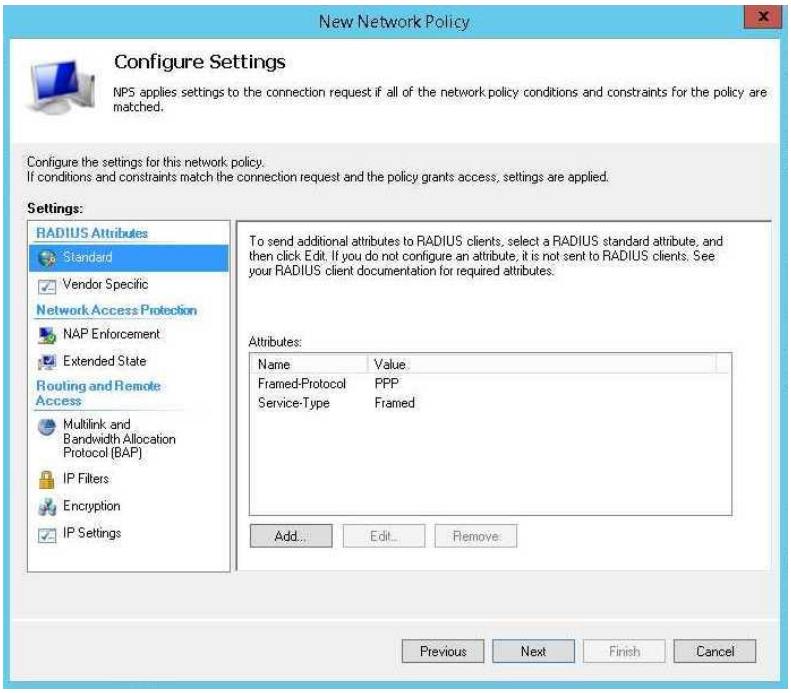
9. Cửa sổ **Configure Authentication Methods**, chọn **Next**.



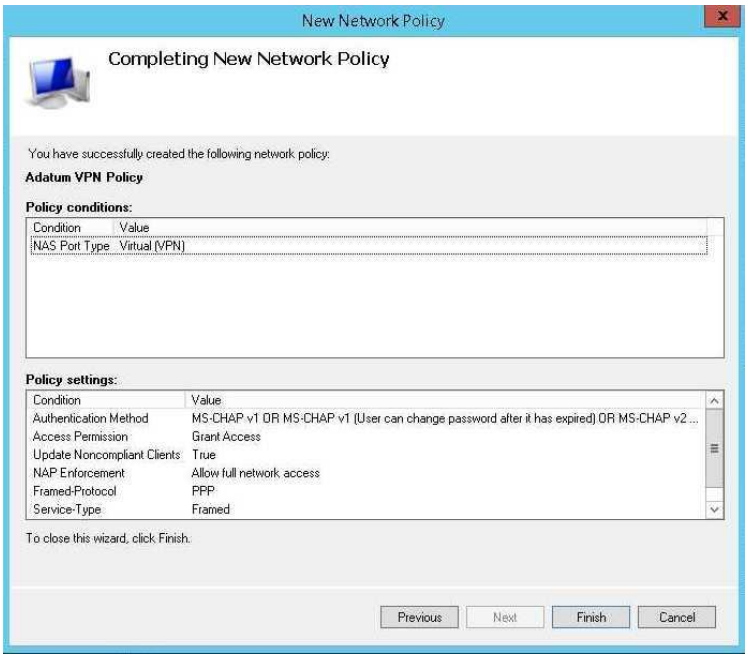
10. Cửa sổ **Configure Constraints**, chọn **Next**.



11. Cửa sổ **Configure Settings**, chọn **Next**.



12. Cửa sổ **Completing New Network Policy**, chọn **Finish**.



Bước 3. TạoVPN Connection.

1. Qua máy **LON-CL2.**

2. Logon **Adatum\Administrator** với password **Pa$$w0rd**.

3. Mở **Control Panel**, chọn **Network and Internet**.



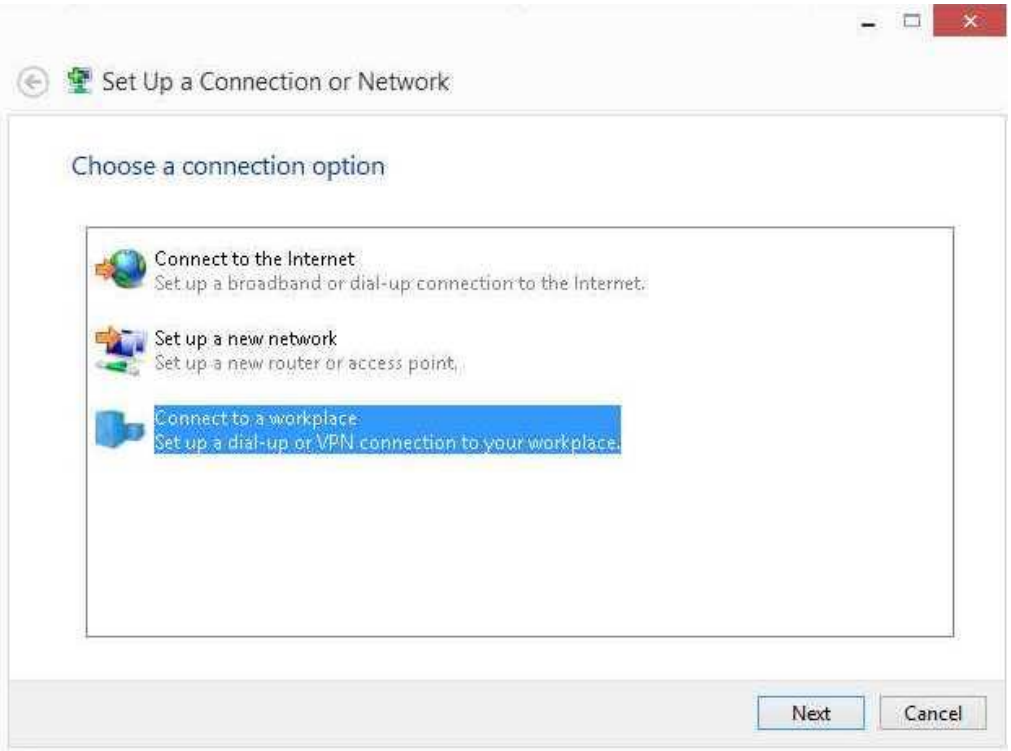
4. Trong cửa sổ **Network and Internet**, chọn **Network and Sharing Center**.



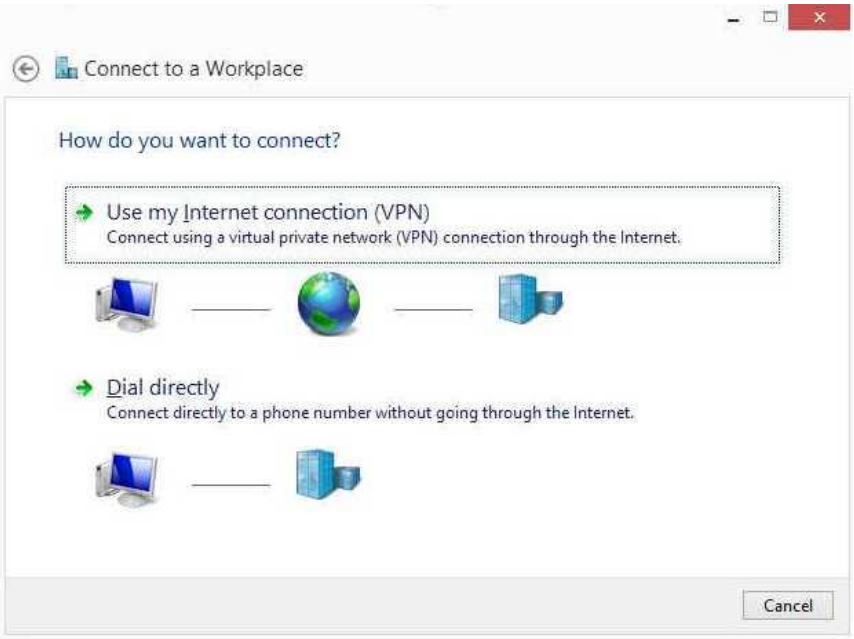
5. Cửa sổ **Network and Sharing Center**, chọn **Set up a new connection or network**.



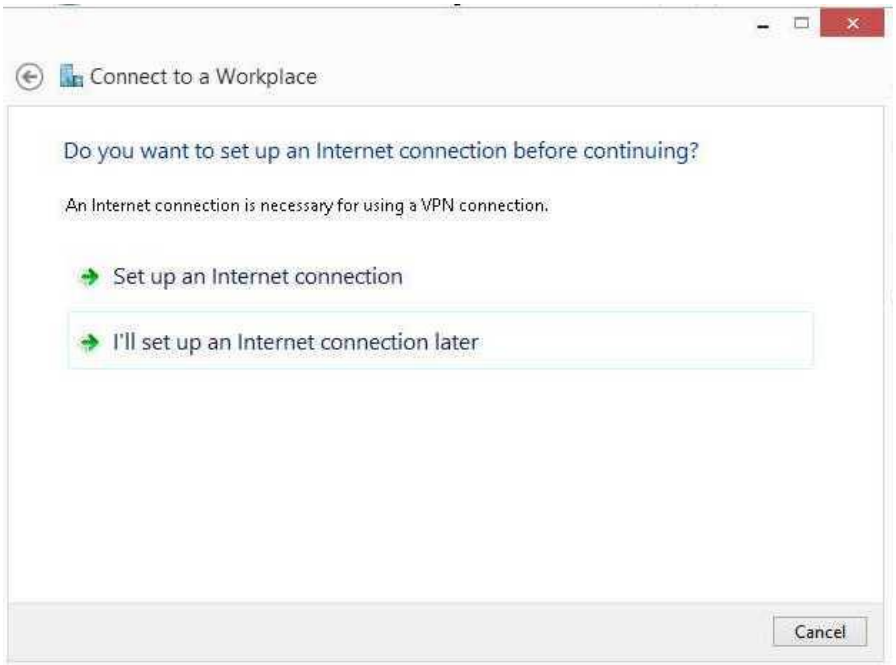
6. Cửa sổ **Choose a connection option**, chọn **Connect to a workplace**, và chọn **Next**.



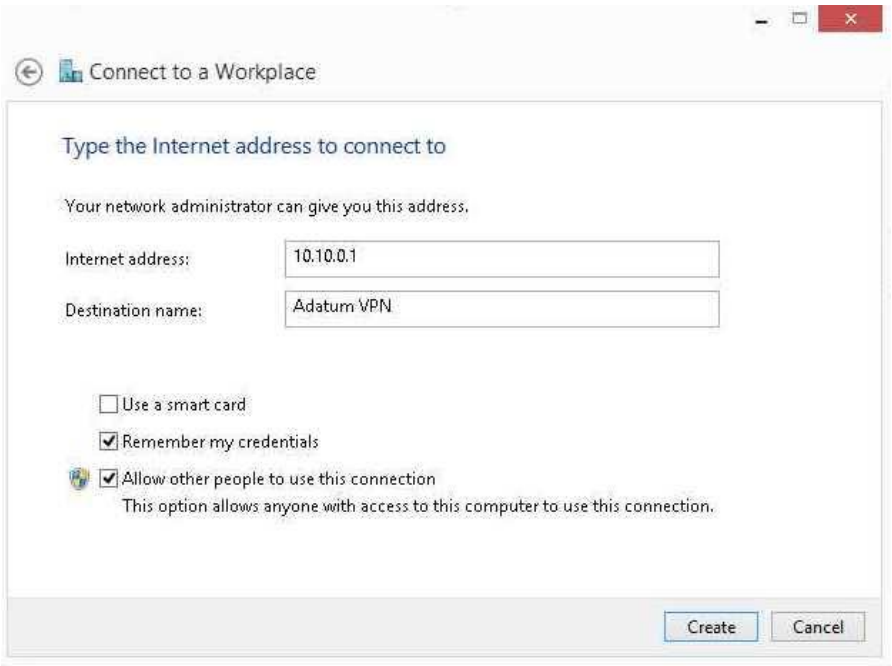
7. Cửa sổ **How do you want to connect**, chọn **Use my Internet connection (VPN)**.



8. Cửa sổ **Do you want to set up an Internet connection before continuing**, Chọn **I'll set up an Internet connection later**.



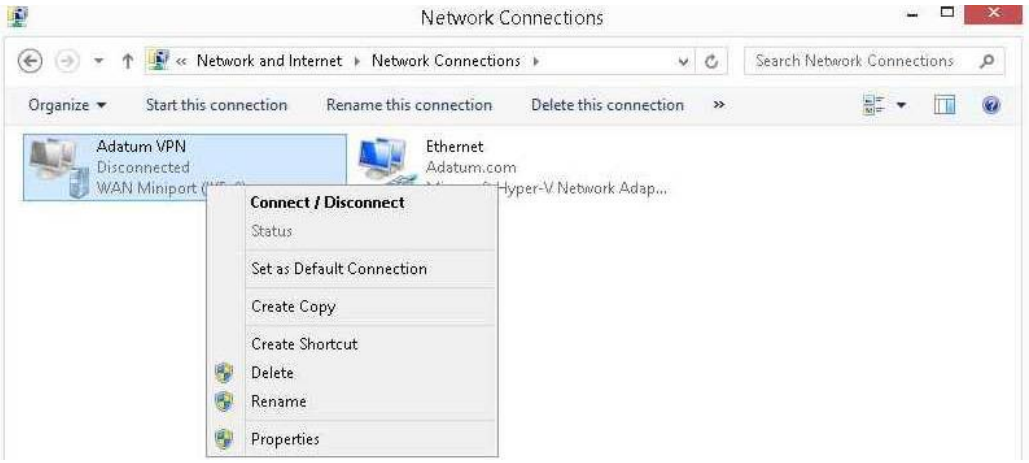
9. Cửa sổ **Type the Internet address to connect to**, trong ô **Internet address**, nhập **10.10.0.1**. Trong ô **Destination name**, nhập **Adatum VPN**. Đánh dấu chọn **Allow other people to use this connection**, và chọn **Create**.



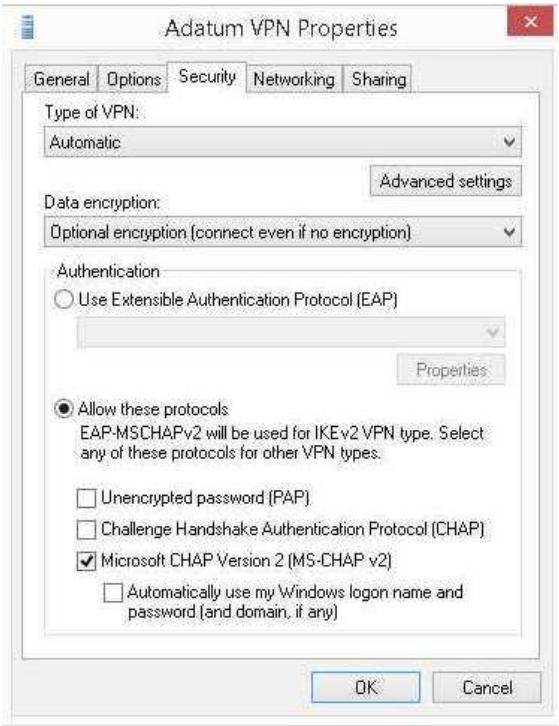
10. Trong cửa sổ **Network and Sharing Center**, chọn **Change adapter settings**.



11. Trong cửa sổ **Network Connections**, nhấn chuột phải **Adatum VPN**, chọn **Properties**.



12. Hộp thoại **Adatum VPN Properties**, qua tab **Security**, trong phần **Authentication**, chọn **Allow these protocols**, và chọn **OK**.



Bước 4. Kiểm tra kết nối VPN.

1. Trên **LON-CL2.**

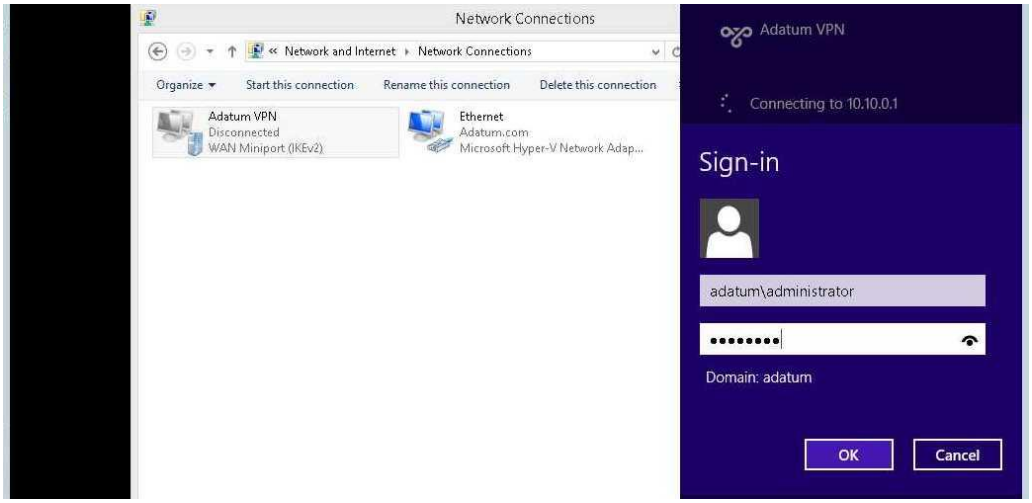
2. Trong cửa sổ **Network Connections**, nhấn chuột phải **Adatum VPN**, chọn **Connect/Disconnect**.



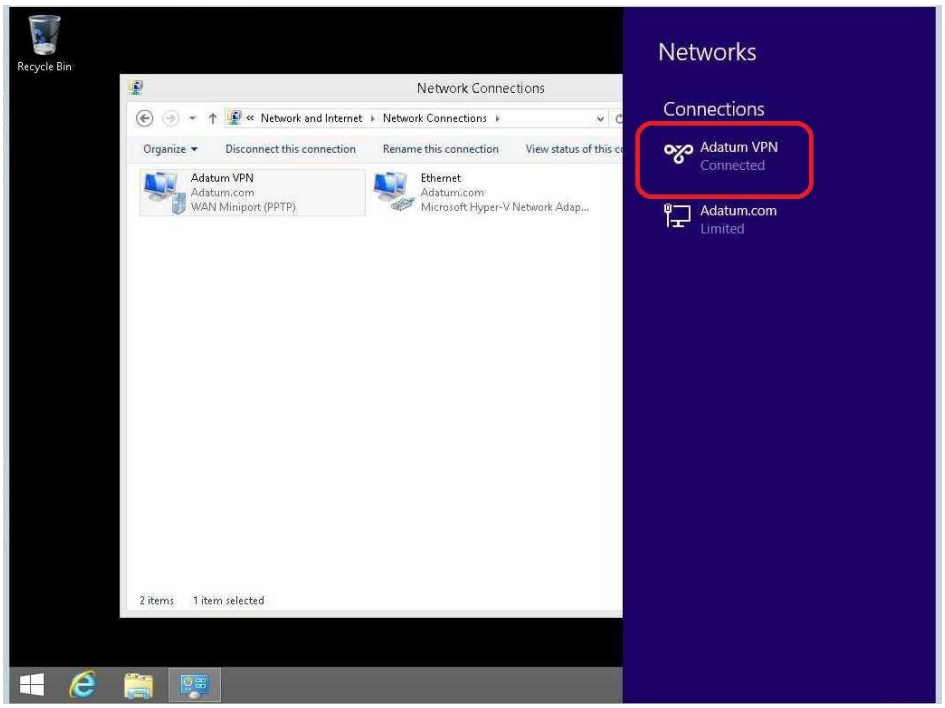
3. Trong danh sách **Networks**, chọn **Adatum VPN**, và chọn **Connect**.



4. Cửa sổ **Network Authentication**, trong ô **User name**, nhập **Adatum\Administrator**. Trong ô **Password**, nhập **Pa$$w0rd**, và chọn **OK**.



5. Kiểm tra kết nối thành công.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai giải pháp VPN thành công.

Bài tập 3: Triển khai Web Application Proxy

❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt Active Directory Federation Services (AD FS).
2. Cài đặt Web Application Proxy role.
3. Cấu hình truy cập vào Website nội bộ.
4. Kiểm tra truy cập vào Website nội bộ.

❖ **Thực hiện:**

Bước 1. Cài đặt Active Directory Federation Services (AD FS).

1. Trên máy **LON-DC1**.
2. Mở **Windows PowerShell**, gõ lệnh:

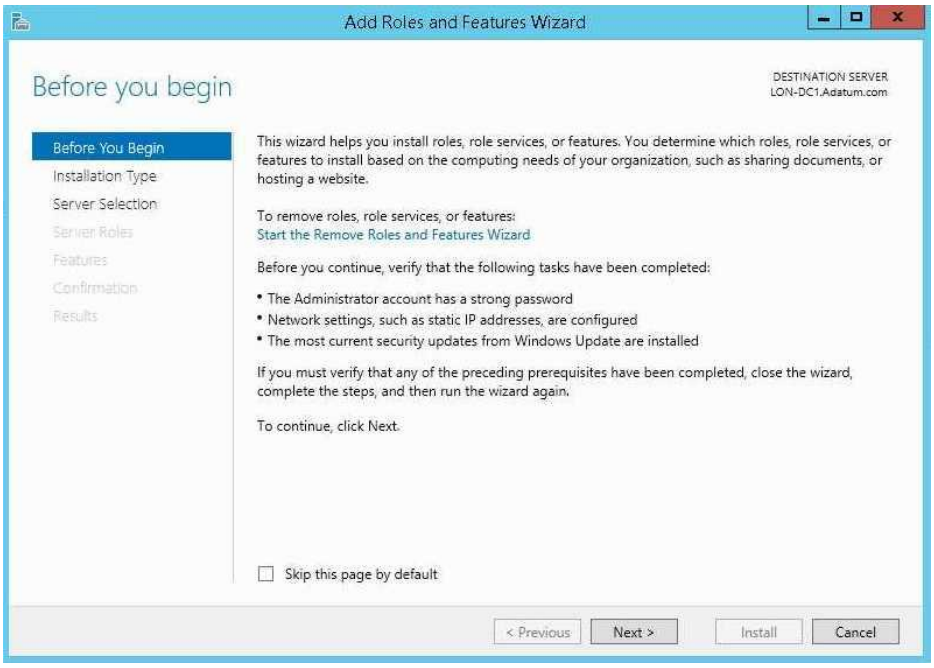
Add-KdsRootKey –EffectiveImmediately



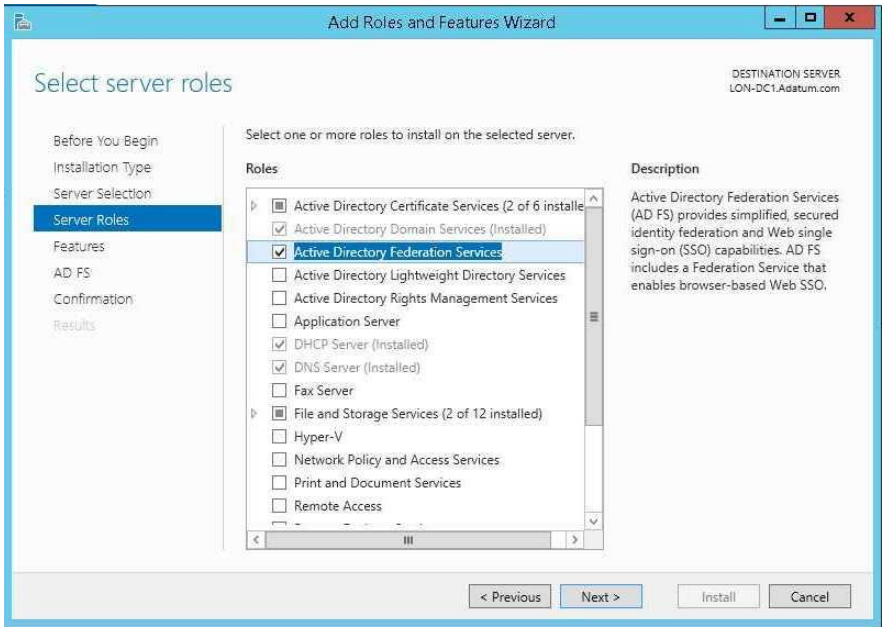
Chú ý: Lệnh này có chức năng tạo Key Distribution Services (KDS) Root Key

3. Mở **Server Manager**, chọn **Add Roles and Features**.

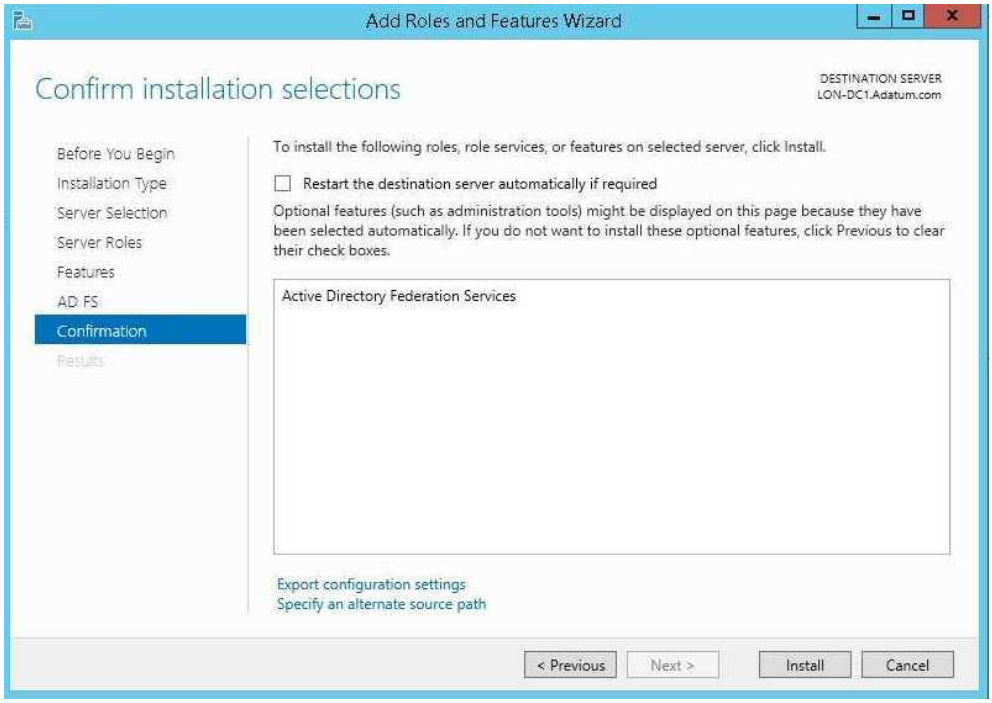
4. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



5. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Federation Services**, chọn **Next** 3 lần.

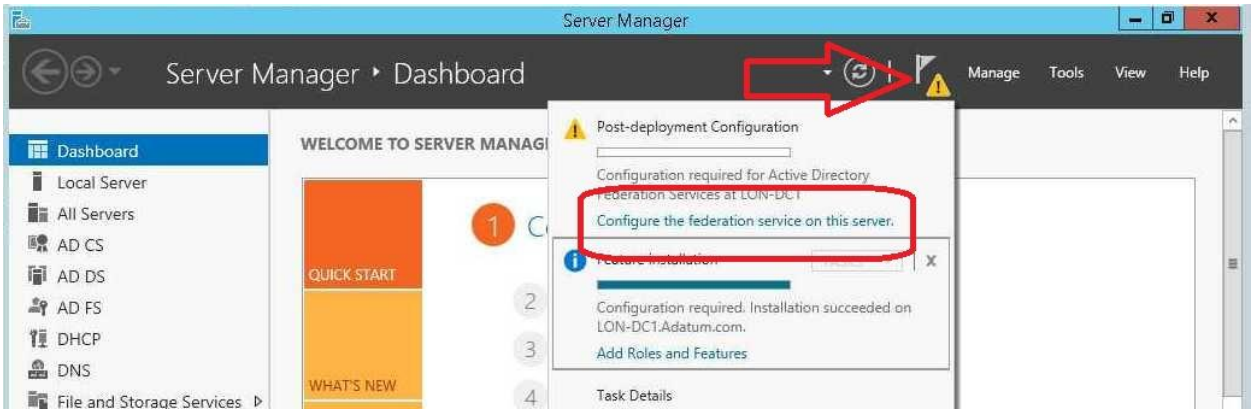


6. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.

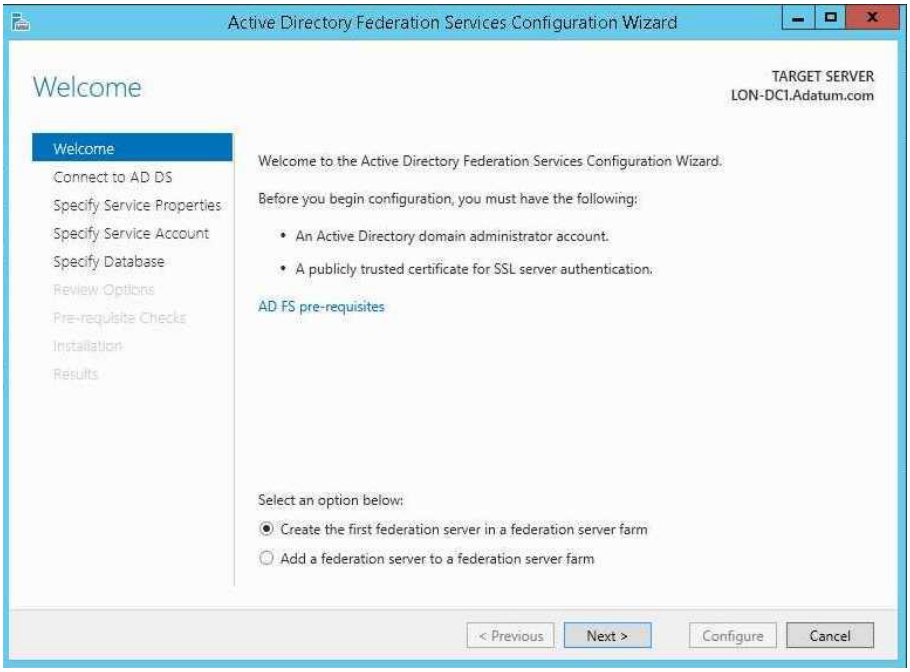


7. Sau khi cài đặt thành công, chọn **Close**.

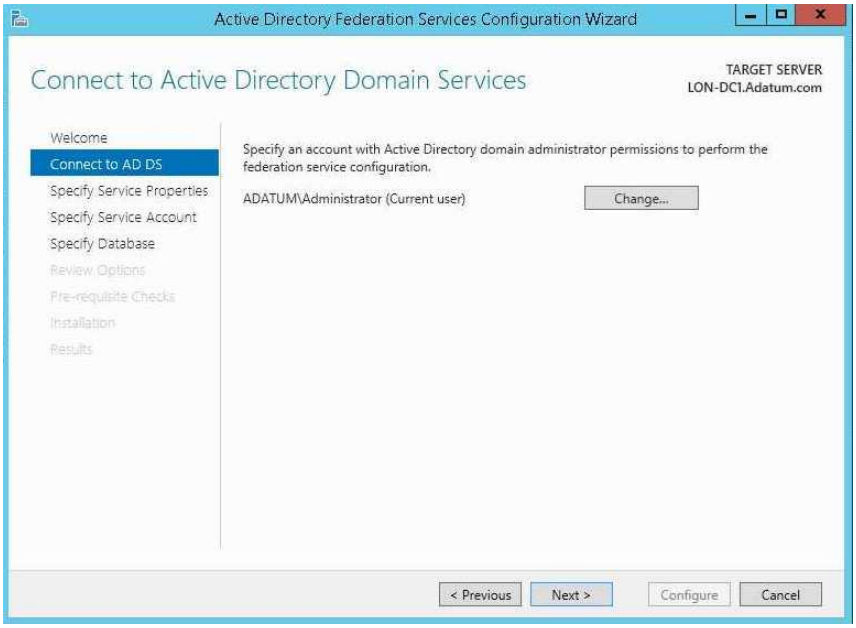
8. Trong cửa sổ **Server Manager**, nhấp chuột vào biểu tượng thông báo màu vàng, và chọn **Configure the federation service on this server**.



9. Cửa sổ **Welcome**, chọn **Create the first federation server in a federation server farm**, và chọn **Next**.

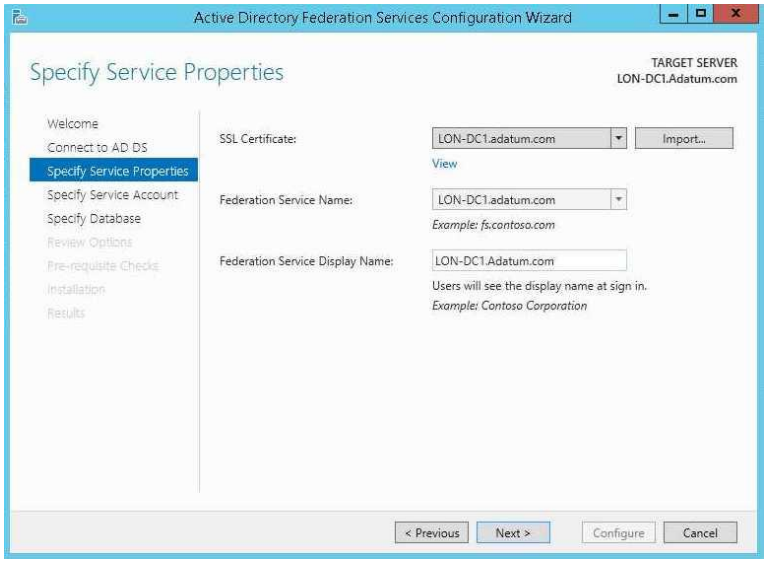


10. Cửa sổ **Connect to Active Directory Domain Services**, chọn **Next.**

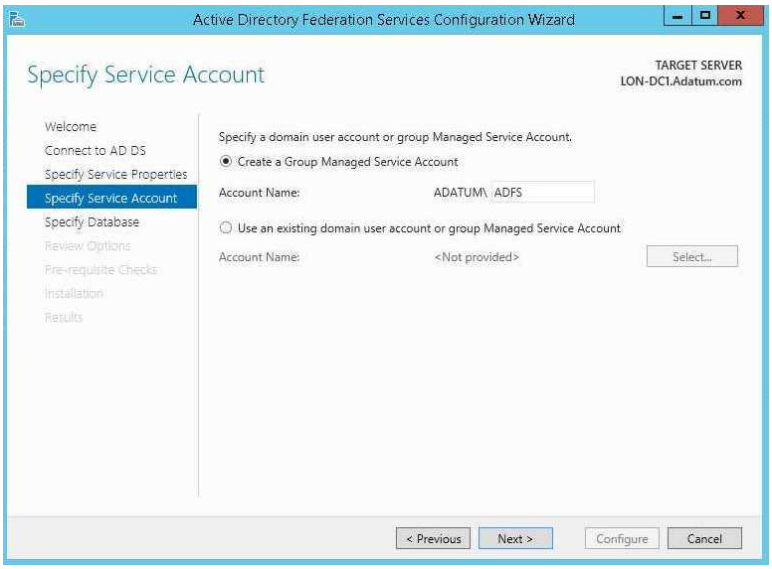


11. Cửa sổ **Specify Service Properties**, nhập thông tin như bên dưới, và chọn **Next**:

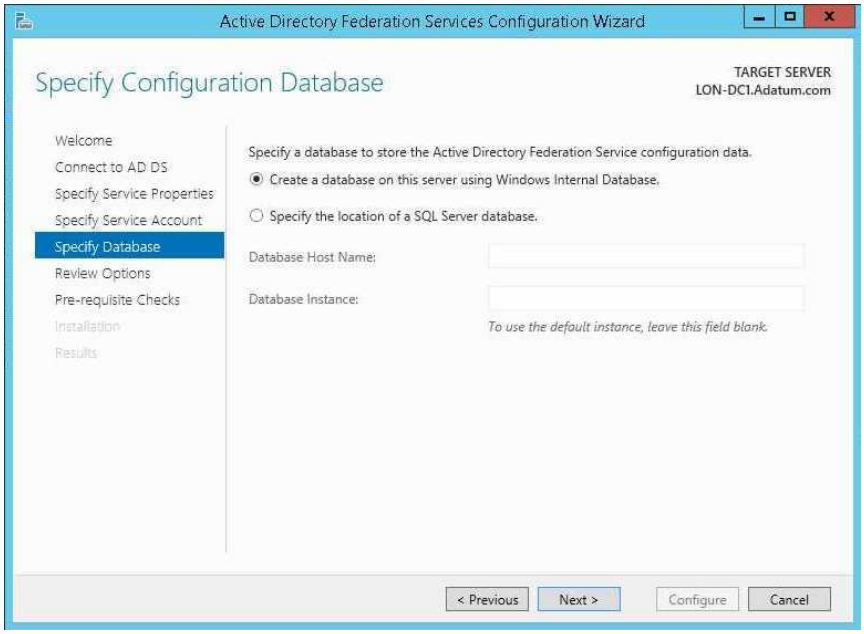
- Bung ô SSL certificate, chọn **LON-DC1.Adatum.com**
- Federation Service Name: **LON-DC1.Adatum.com**
- Federation Service Display Name: **LON-DC1.Adatum.com**



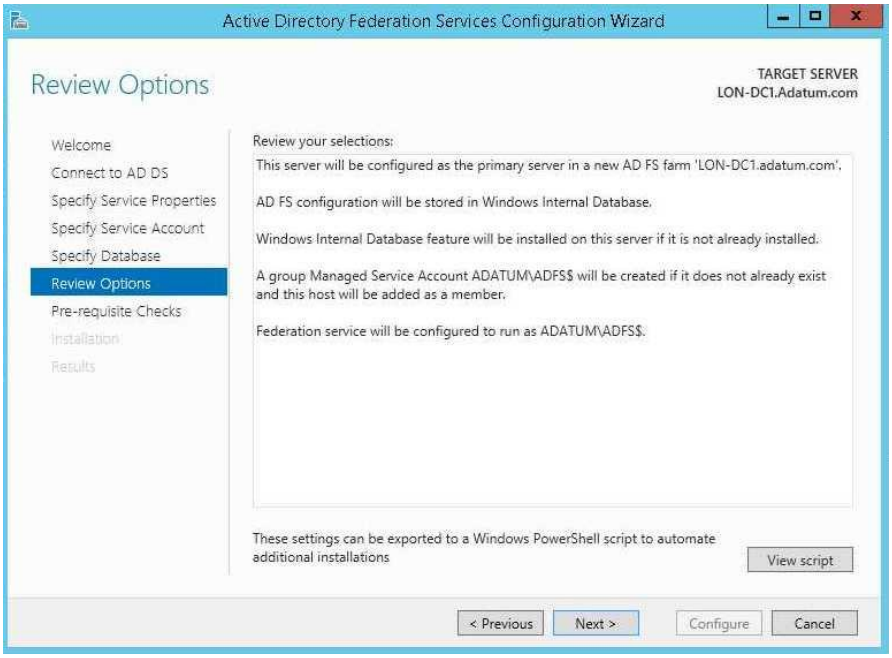
12. Cửa sổ **Specify Service Account**, chọn **Create a Group Managed Service Account**. Trong ô **Account Name**, nhập **ADFS**, và chọn **Next**.



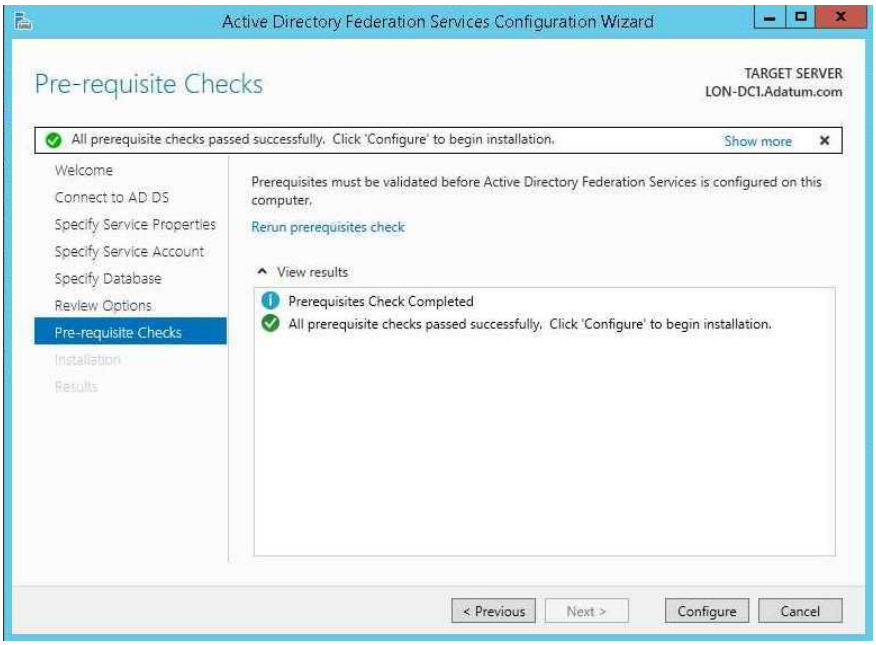
13. Cửa sổ **Specify Configuration Database**, chọn **Create a database on this server using Windows Internal Database**, và chọn **Next**.



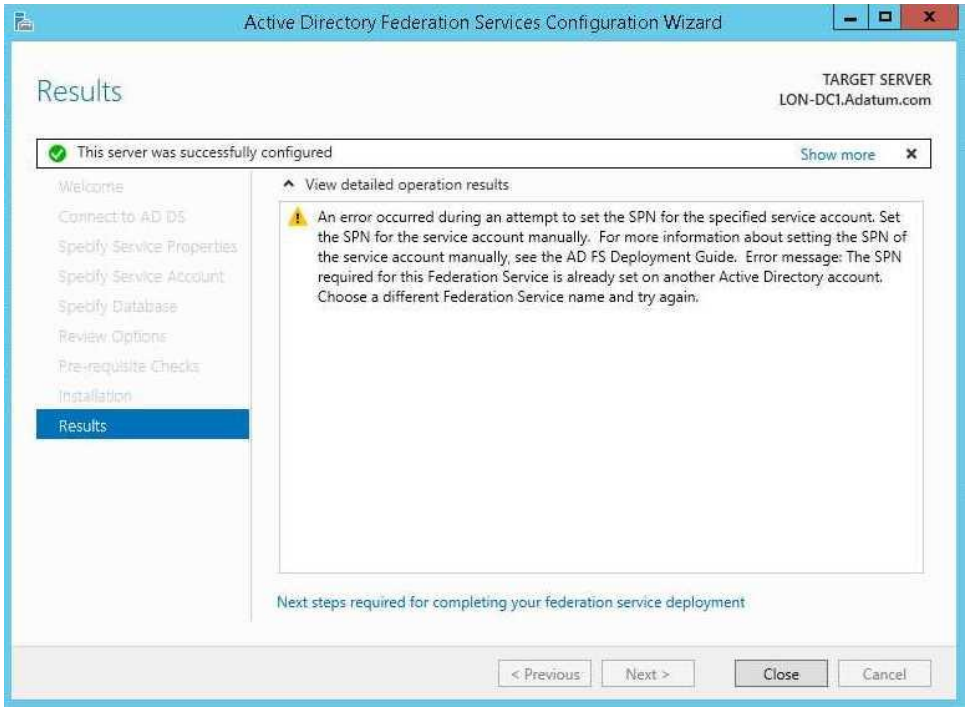
14. Cửa sổ **Review Options**, chọn **Next**.



15. Cửa sổ **Pre-requisite Checks**, chọn **Configure**.



16. Cửa sổ **Results** (lưu ý một lỗi dịch vụ đăng ký tên chính có thể xảy ra), chọn **Close**.



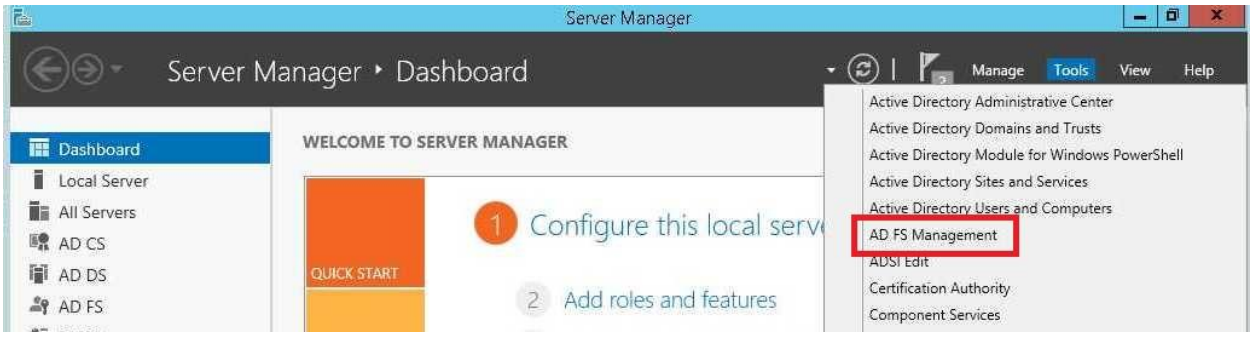
17. Mở **Windows PowerShell**, gõ lệnh:

Set-ADFSProperties –AutoCertificateRollover $False

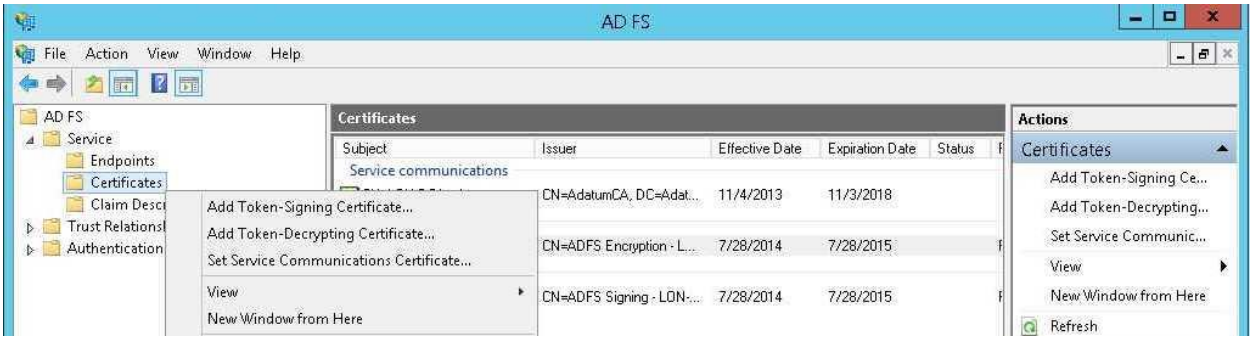


Chú ý: Lệnh này để tắt chức năng AutoCertificateRollover. Bạn phải thực hiện bước này để có thể sửa đổi các certificates được sử dụng trong hệ thống AD FS

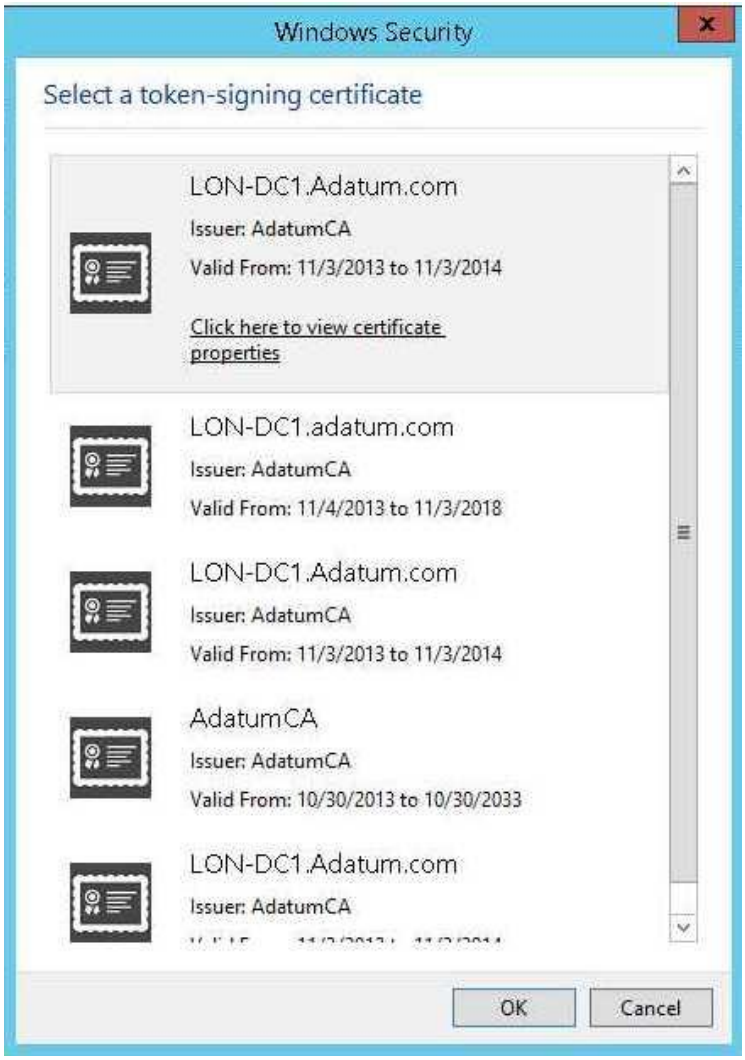
18. Trong **Server Manager**, bung menu **Tools**, mở **AD FS Management**.



19. Trong cửa sổ **AD FS**, bung **Service**, nhấn chuột phải **Certificates**, chọn **Add Token-Signing Certificate**.



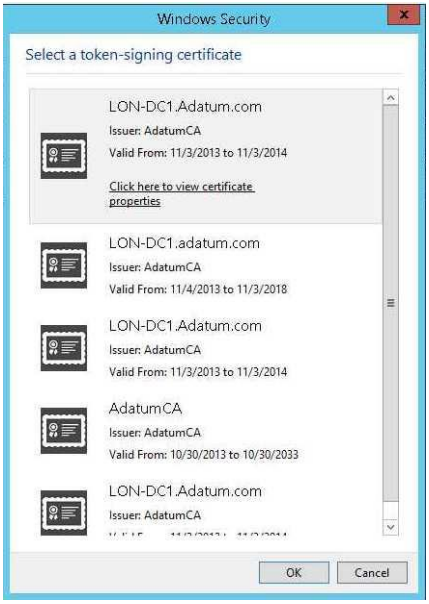
20. Trong hộp thoại **Select a token-signing certificate**, chọn certificate **LON-DC1.Adatum.com**, và chọn **Click here to view certificate properties**.



21. Kiểm tra certificate có chức năng **Proves your identity to a remote computer** và **Ensures the identity of a remote computer**, chọn **OK**.



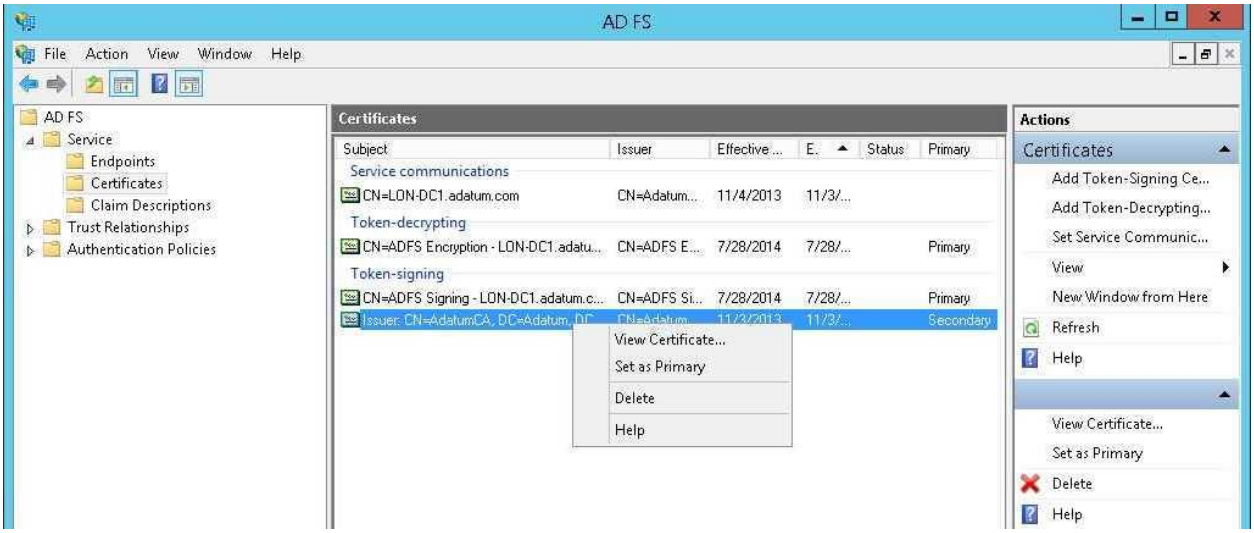
22. Trong hộp thoại **Select a token-signing certificate**, chọn **OK.**



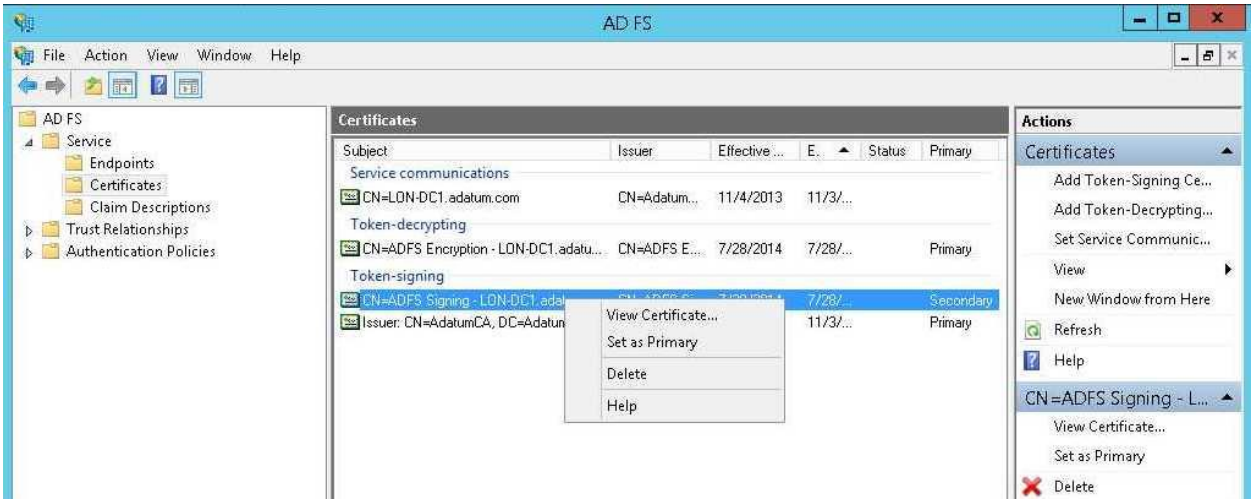
23. Hộp thoại cảnh báo **AD FS Management**, chọn **OK**.



24. Trong cửa sổ **AD FS**, bung **Service**, chọn **Certificates.** Trong phần **Token-signing**, nhấn chuột phải lên certificate đang có chế độ Secondary, chọn **Set as Primary**. Hộp thoại thông báo, chọn **Yes**.



25. Tiếp theo, nhấn chuột phải lên certificate mới được chuyển qua chế độ Secondary, chọn **Delete**. Hộp thoại thông báo, chọn **Yes**.

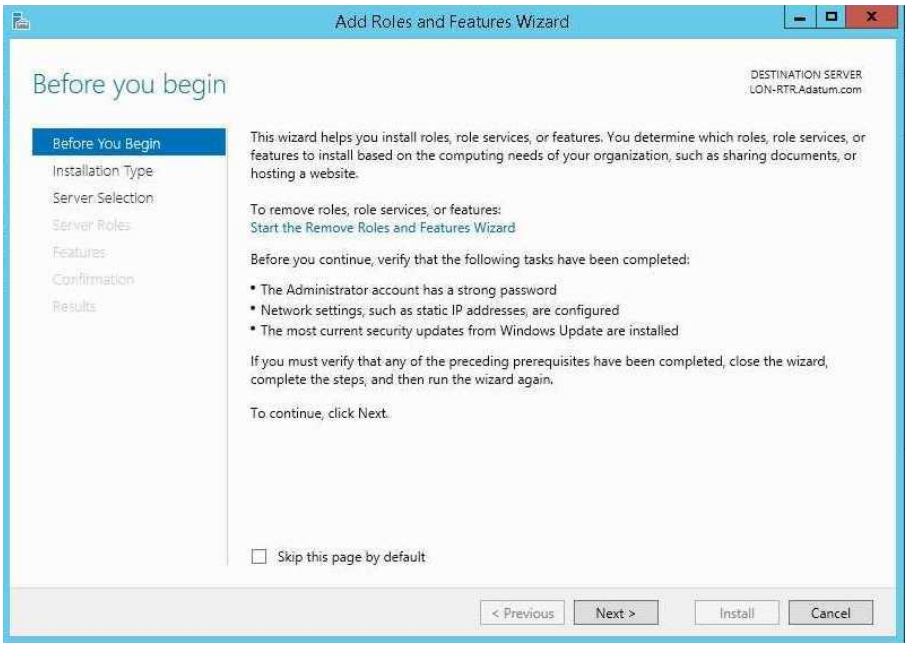


Bước 2. Cài đặt Web Application Proxy role.

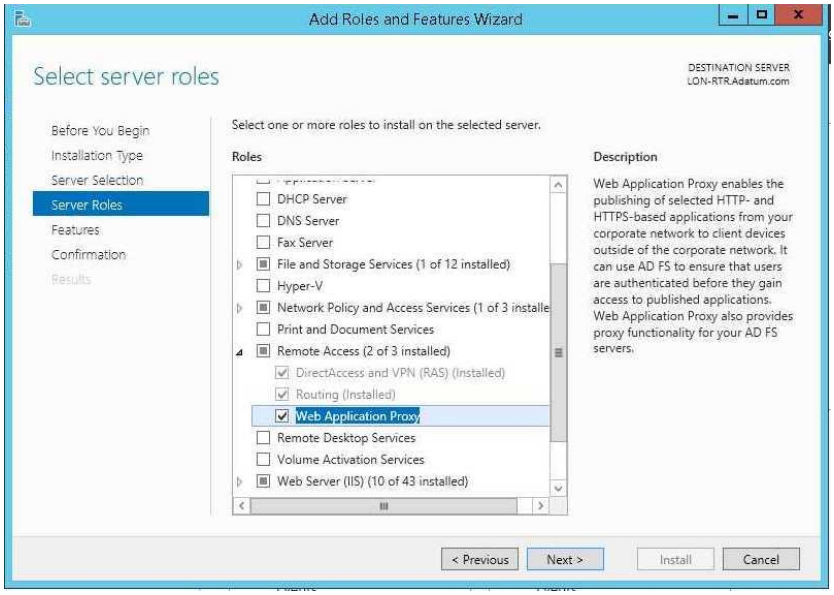
1. Qua máy **LON-RTR**.

2. Mở **Server Manager**, chọn **Add roles and features**.

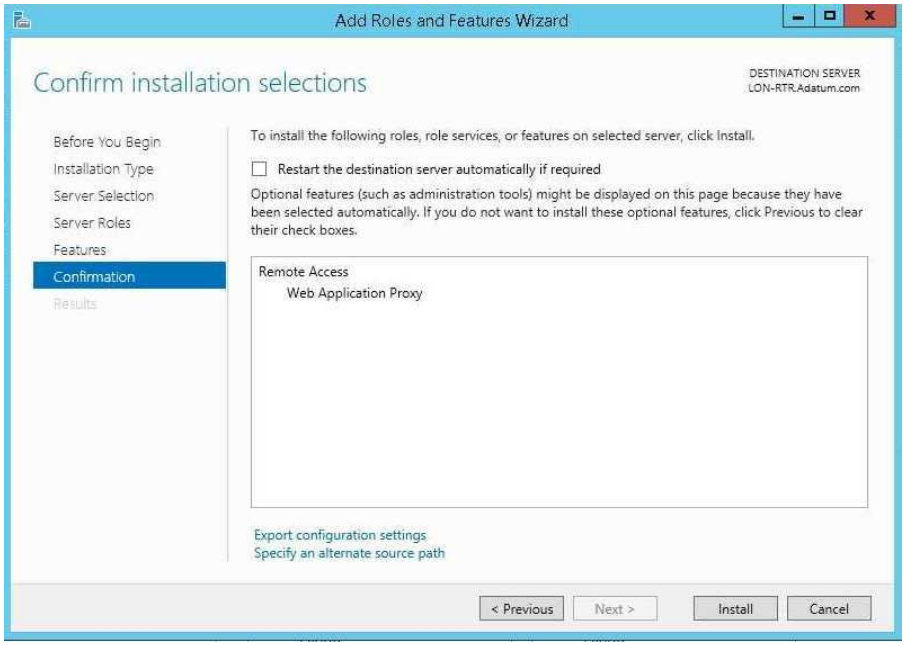
3. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



4. Cửa sổ **Select server roles**, bung **Remote Access**, đánh dấu chọn **Web Application Proxy**, và chọn **Next** 2 lần.



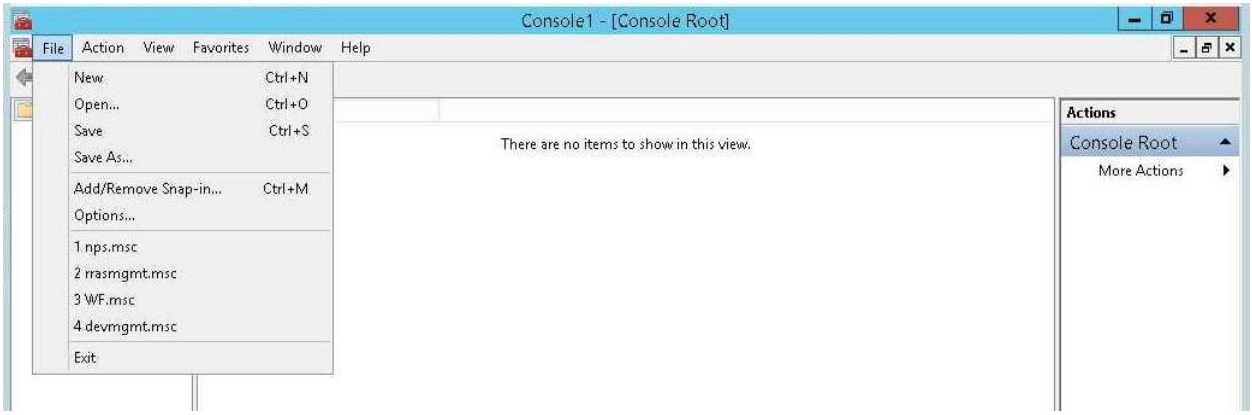
5. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.



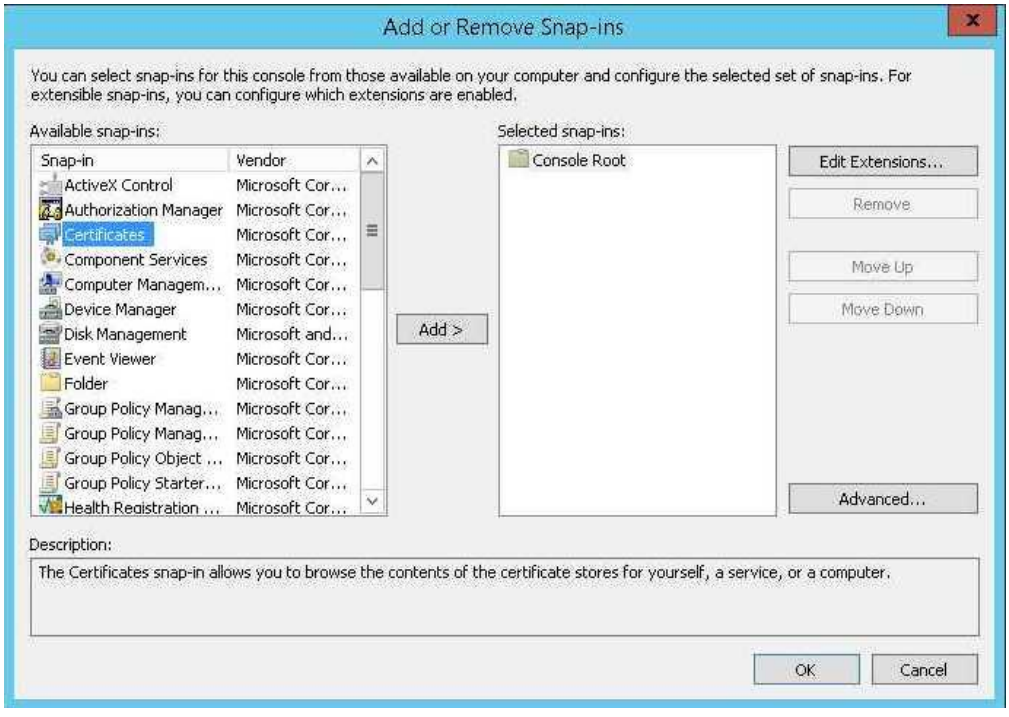
Bước 3. Cấu hình truy cập vào Website nội bộ.

1. Trên **LON-RTR.**

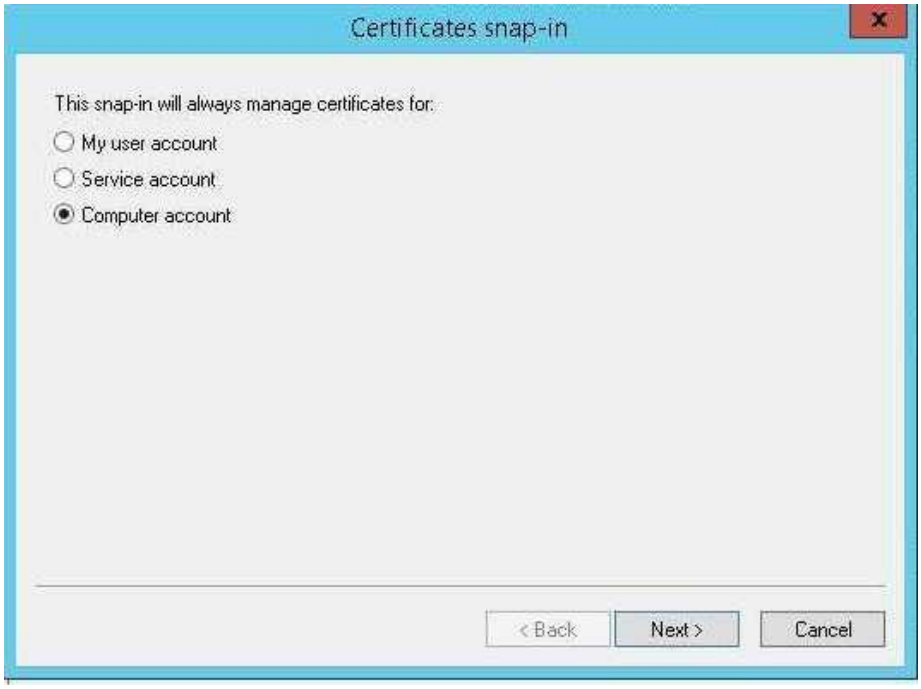
2. Mở **MMC**, bung menu **File**, chọn **Add or Remove Snap-In**.



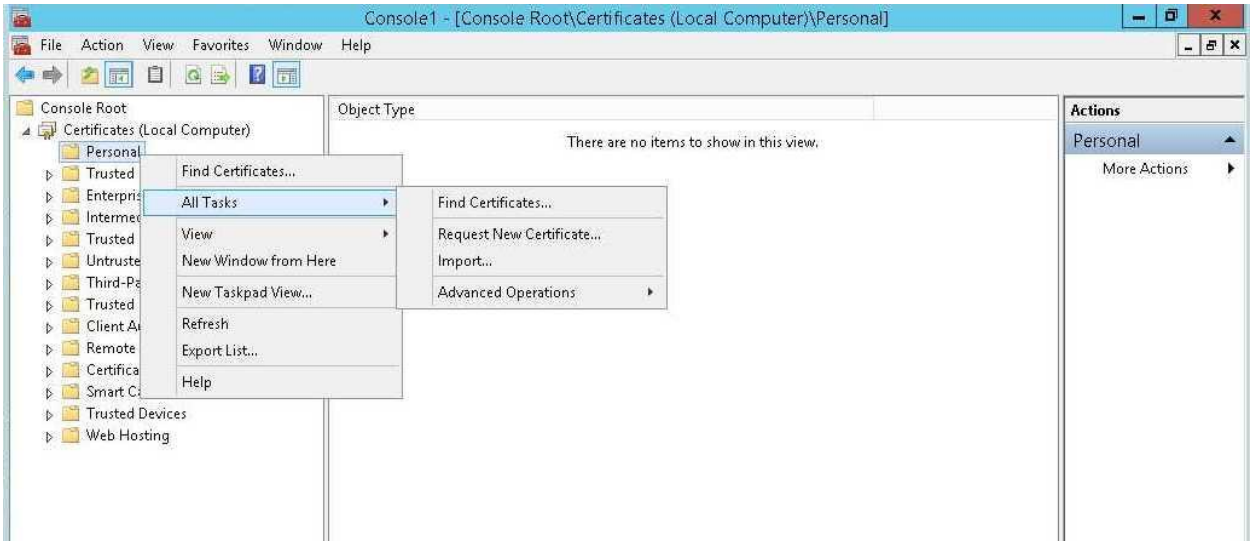
3. Cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add**



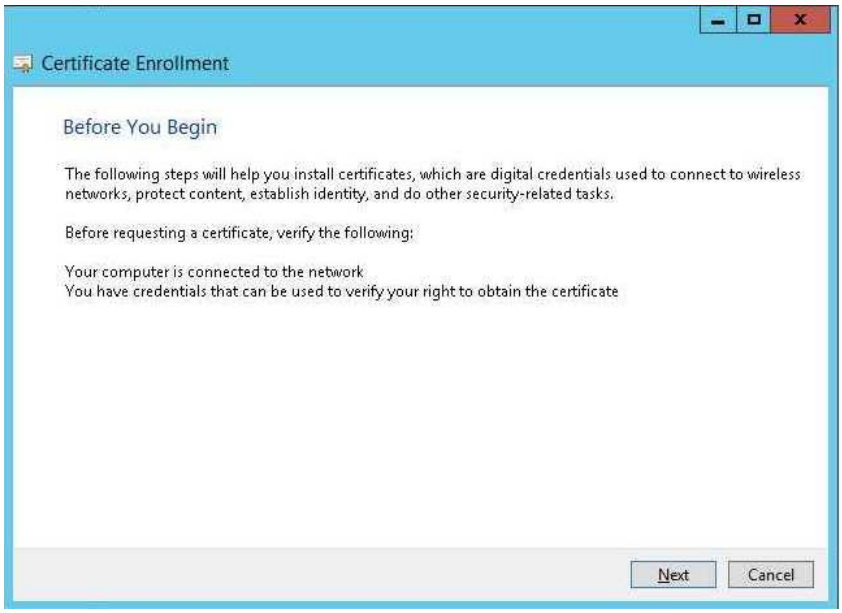
4. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**, chọn **Finish**, và chọn **OK**.



5. Trong cửa sổ **Console1**, bung **Certificates (Local Computer)** , nhấn chuột phải **Personal**, bung **All Tasks**, chọn **Request new Certificate**.



6. Cửa sổ **Before You Begin**, chọn **Next** 2 lần.



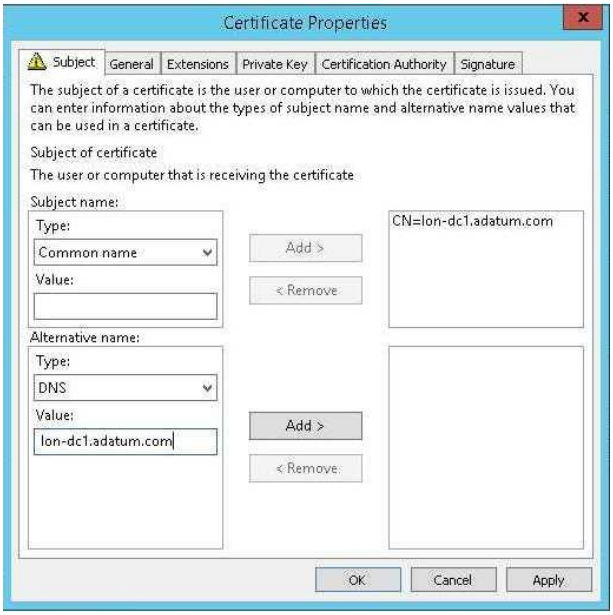
7. Cửa sổ **Request Certificates**, đánh dấu chọn **Adatum Web Server**, và chọn **More information is required to enroll for this certificate. Click here to configure settings.**



8. Hộp thoại **Certificate Properties**, trong phần **Subject Name**, bung ô **Type**, chọn **Common Name**, trong ô **Value**, nhập **lon-dc1.adatum.com**, và chọn **Add**.



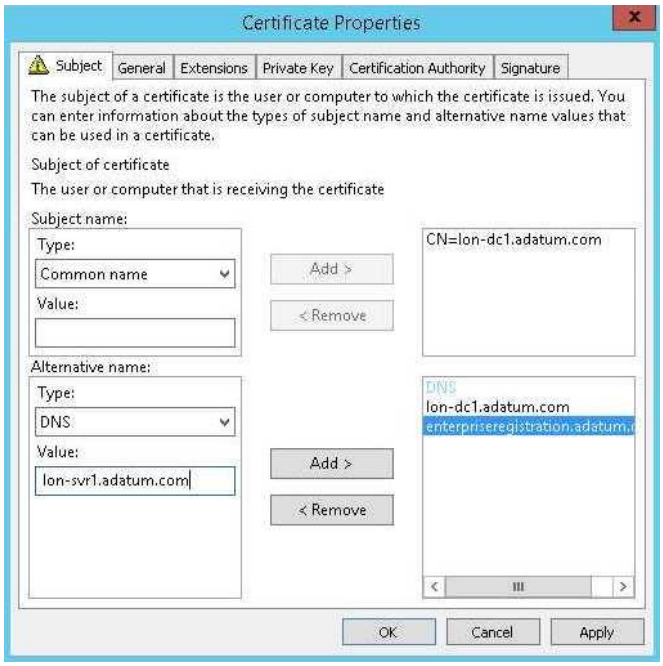
9. Trong phần **Alternative name**, bung ô **Type,** chọn **DNS**, trong ô **Value**, nhập **lon-dc1.adatum.com**, và chọn **Add**.



10. Trong phần **Alternative name**, bung ô **Type**, chọn **DNS**, trong ô **Value**, nhập **enterpriseregistration.adatum.com**, và chọn **Add**.



11. Trong phần **Alternative name**, bung ô **Type**, chọn **DNS**, trong ô **Value**, nhập **lon-svr1.adatum.com**, và chọn **Add**.



12. Hộp thoại **Certificate Properties**, chọn **OK.**



13. Cửa sổ **Request Certificate**, chọn **Enroll**, và chọn **Finish**.

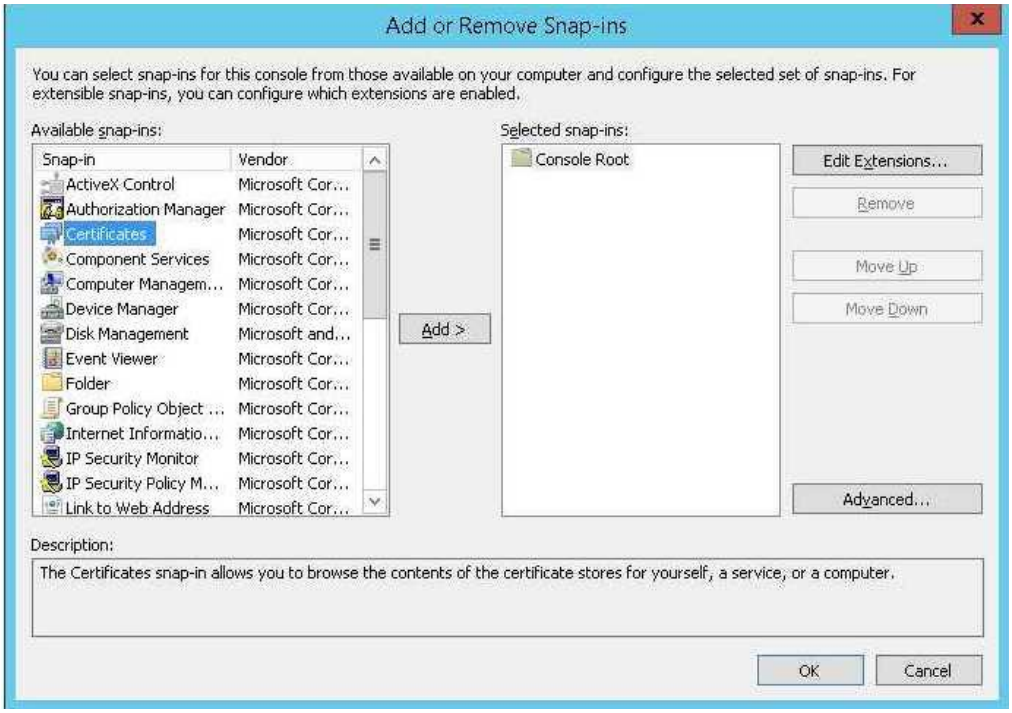


14. Qua máy **LON-SVR1.**

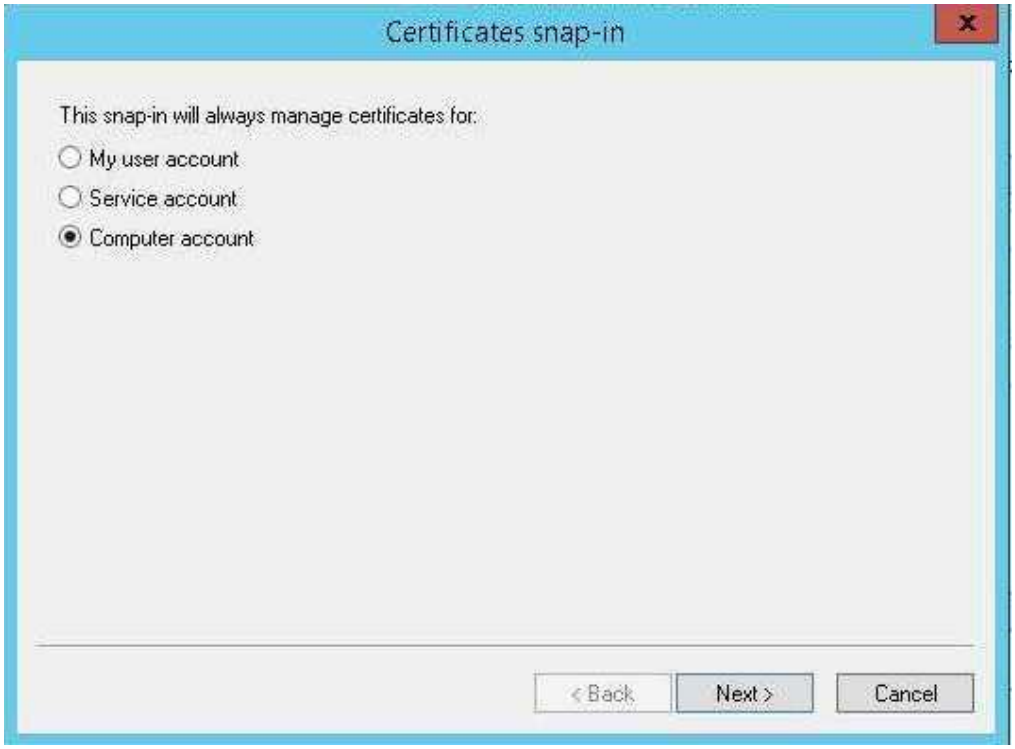
15. Mở **MMC**, bung menu **File**, chọn **Add or Remove Snap-In**.



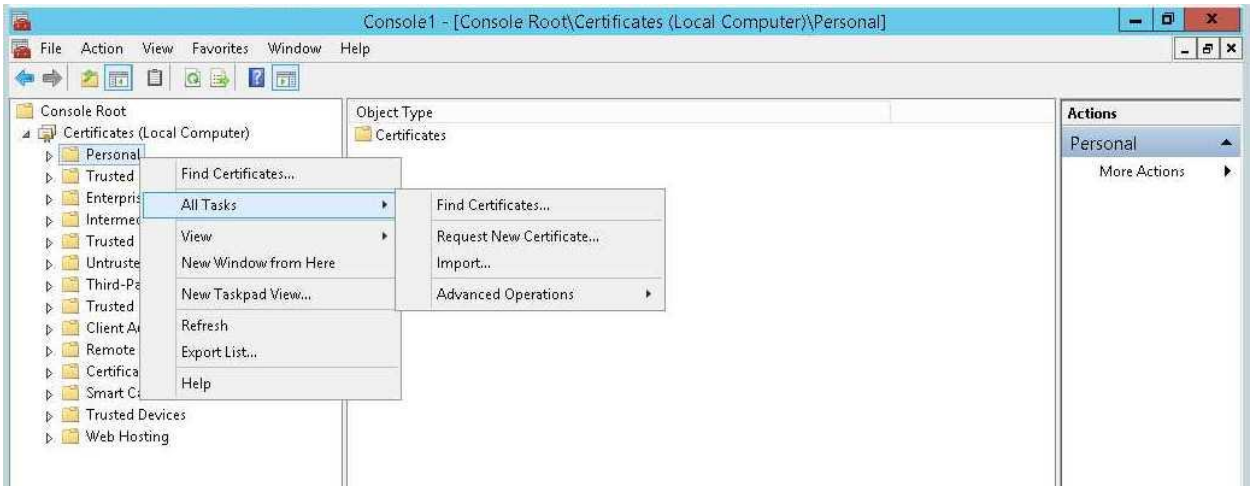
16. Cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add.**



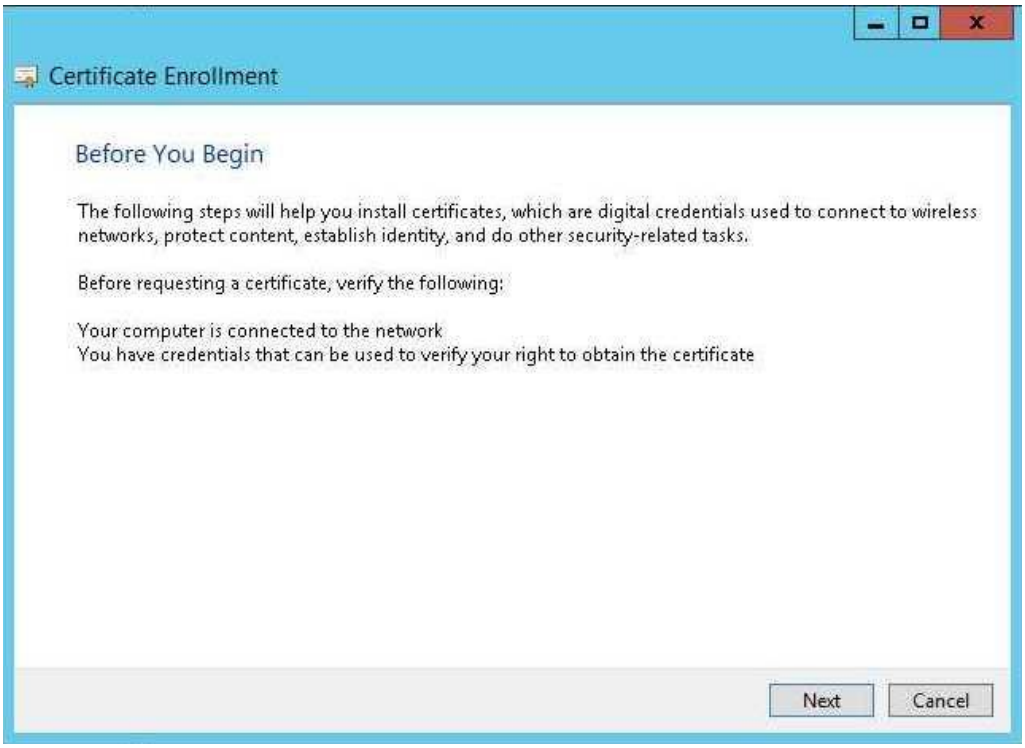
17. Cửa sổ **Certificates snap-in,** chọn **Computer account**, chọn **Next,** chọn **Finish,** và chọn **OK**



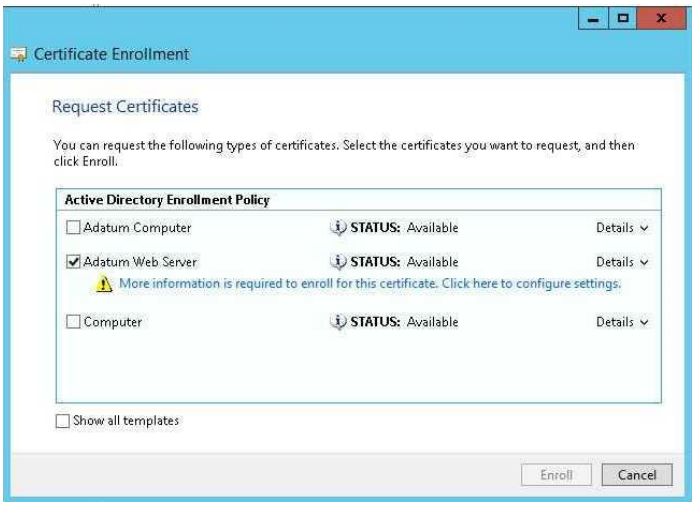
18. Trong cửa sổ **Console1**, bung **Certificates (local Computer)**, nhấn chuột phải **Personal**, bung **All Tasks**, chọn **Request new Certificate**.



19. Cửa sổ **Before You Begin**, chọn **Next** 2 lần.



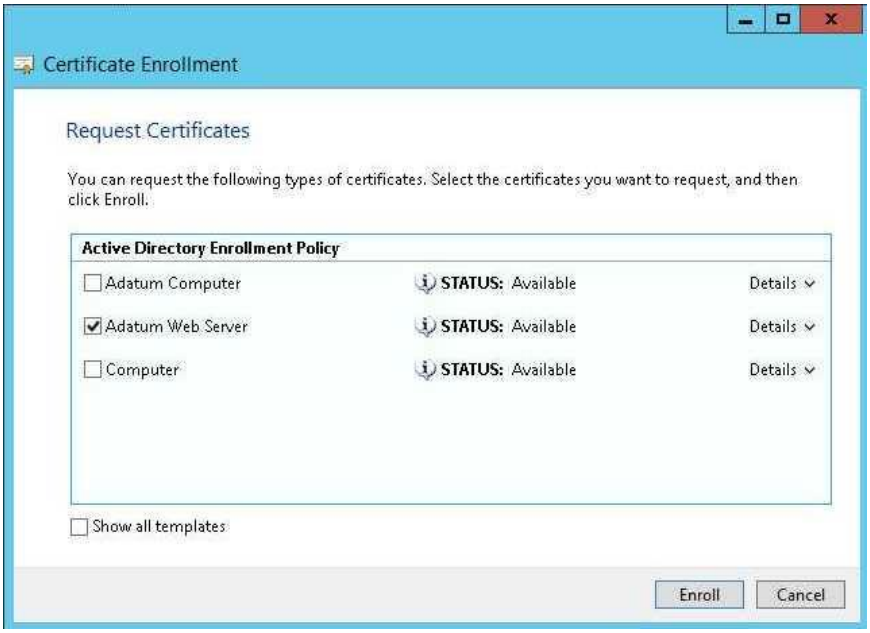
20. Cửa sổ **Request Certificates**, đánh dấu chọn **Adatum Web Server**, và chọn **More information is required to enroll for this certificate. Click here to configure settings**



21. Hộp thoại **Certificate Properties,** trong phần **Subject Name**, bung ô **Type**, chọn **Common Name**, trong ô **Value**, nhập **lon-svr1.adatum.com**, chọn **Add**, và chọn **OK.**



22. Cửa sổ **Request Certificates,** chọn **Enroll**, và chọn **Finish.**



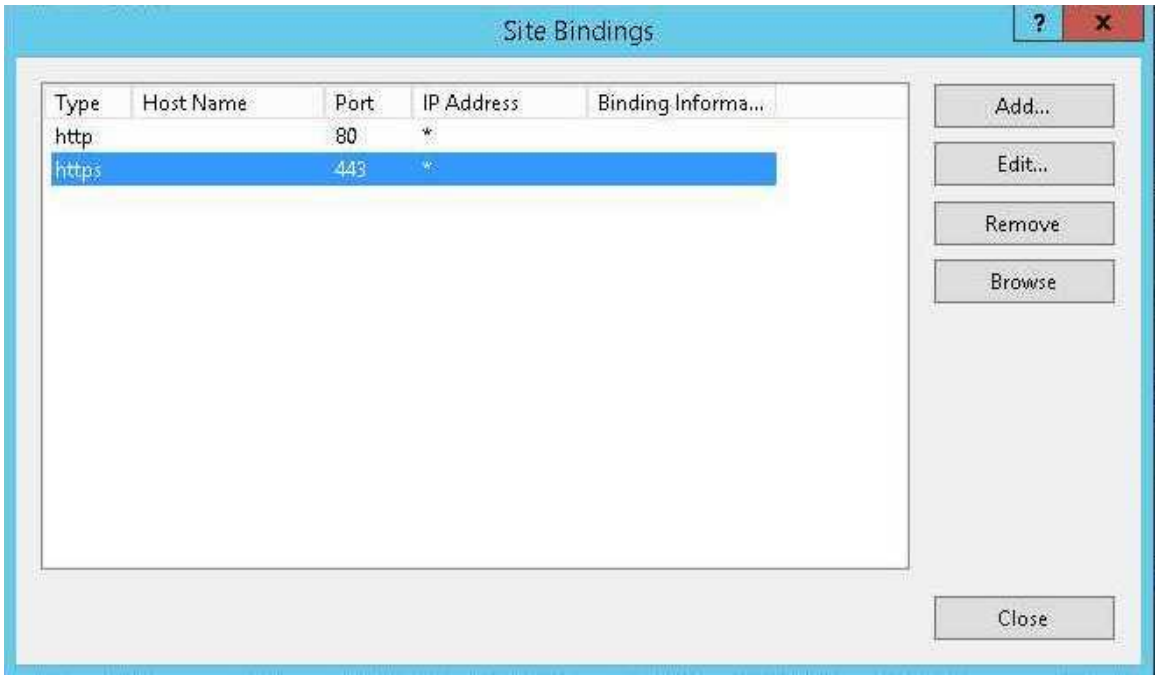
23. Tắt cửa sổ **Console1**, chọn **No**

24. Trong **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**.

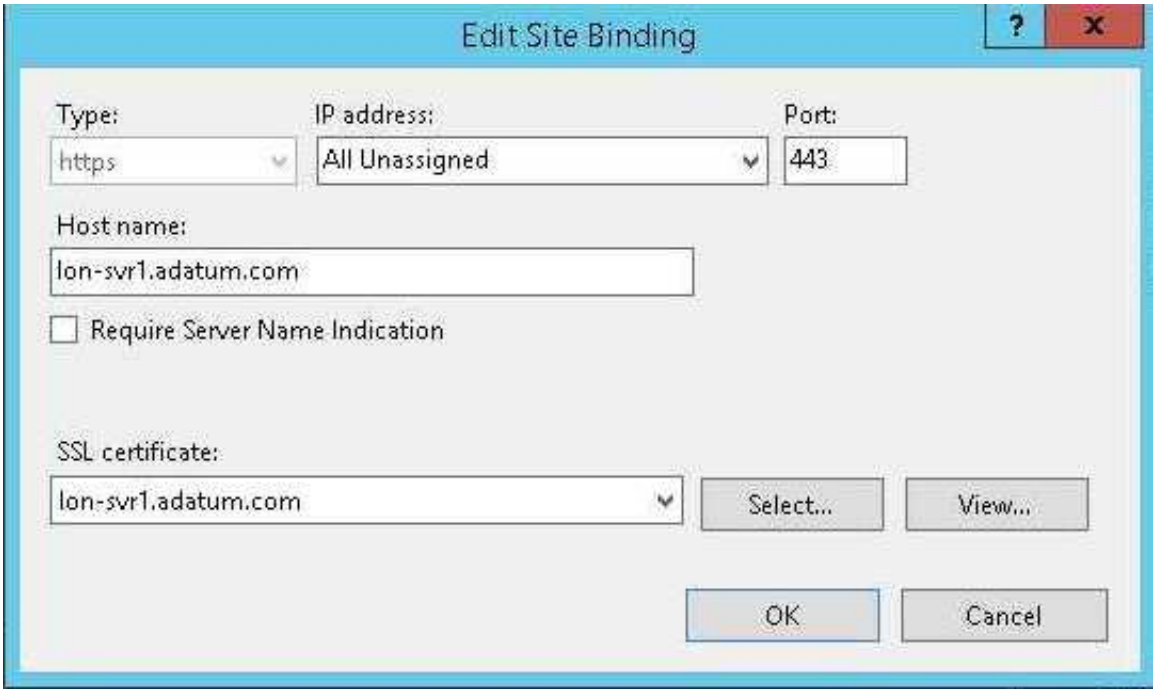
25. Trong cửa sổ **Internet Information Services (IIS) Manager**, bung **LON-SVR1,** bung **Sites**, chọn **Default Web site**. Trong cửa sổ **Actions**, chọn **Bindings**



26. Hộp thoại **Site Bindings**, chọn **https**, và chọn **Edit**.



27. Hộp thoại **Edit Site Bindings**, trong ô **Host name**, nhập **lon-svr1.adatum.com**, bung ô **SSL Certificate**, chọn **lon-svr1.adatum.com**, chọn **OK**, và chọn **Close**.



28. Tắt cửa sổ **Internet Information Services (IIS)**.

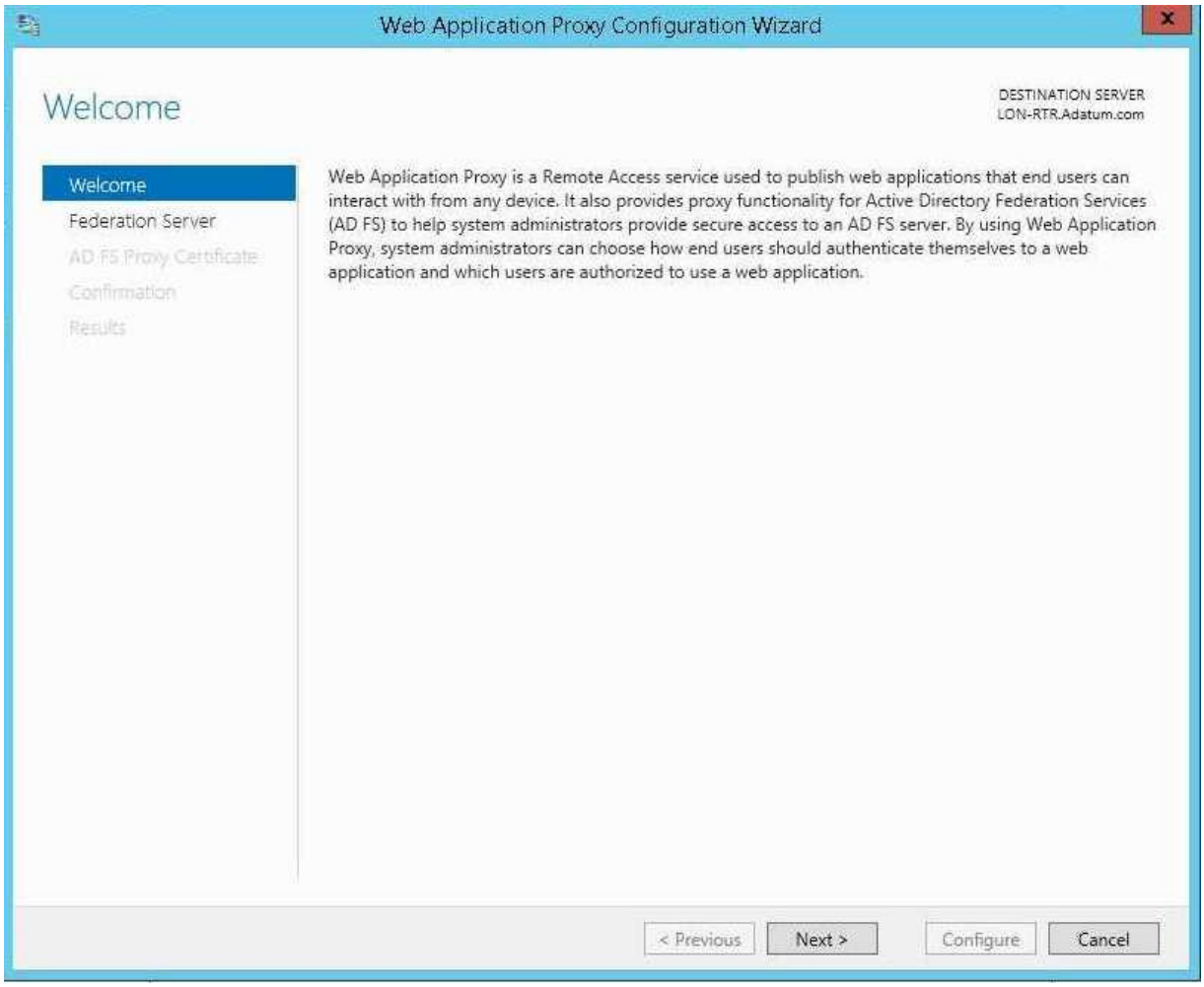
29. Qua máy **LON-RTR**.

30. Trong **Server Manager**, bung menu **Tools**, mở **Remote Access Management**.

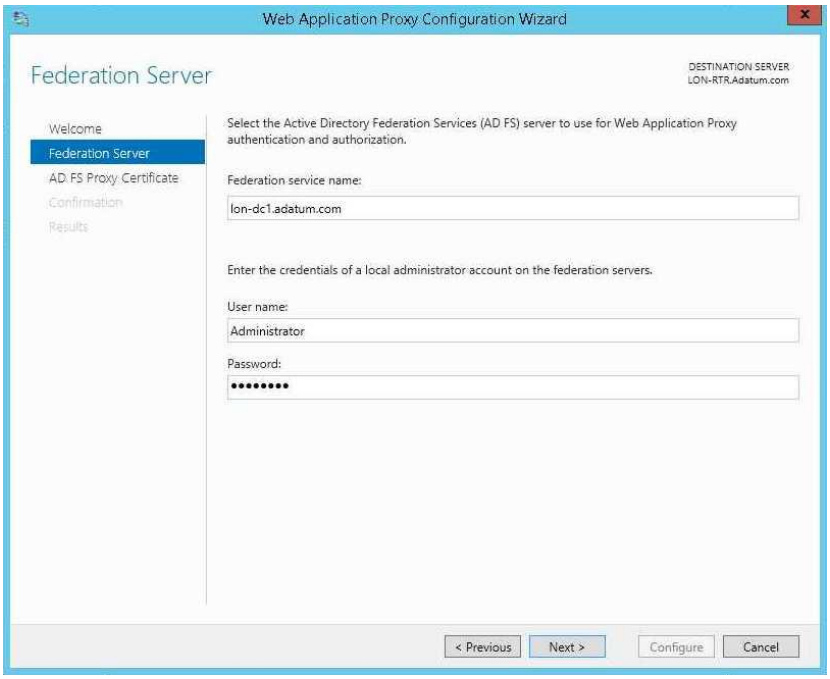
31. Trong cửa sổ **Remote Access Management Console**, chọn **Web Application Proxy**, chọn **Run the Web Application Proxy Configuration Wizard**.



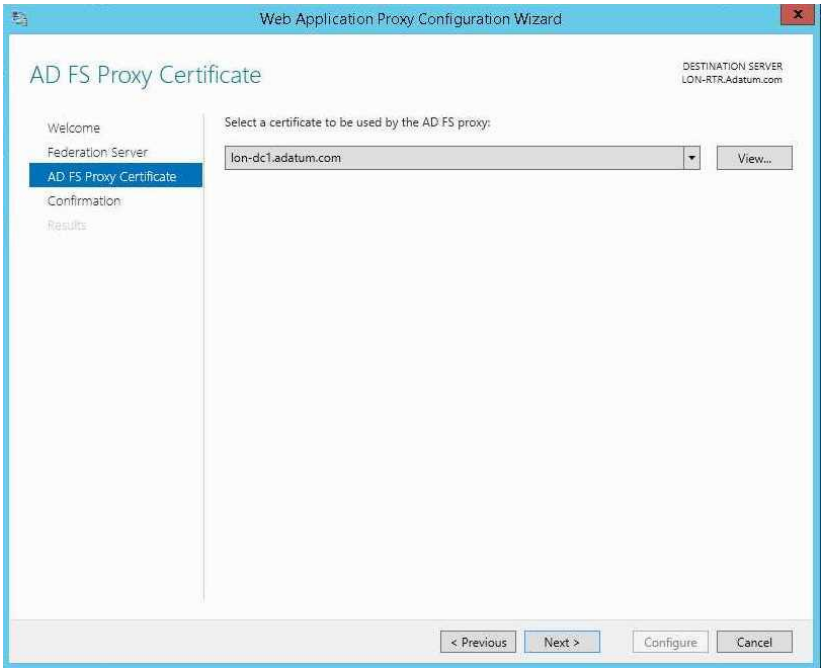
32. Cửa sổ **Welcome**, chọn **Next**.



33. Cửa sổ **Federation Server**, trong ô **Federation service name**, nhập **lon-dc1.adatum.com**, trong ô User name, nhập **Administrator,** trong ô Password, nhập: **Pa$$w0rd**, chọn **Next**

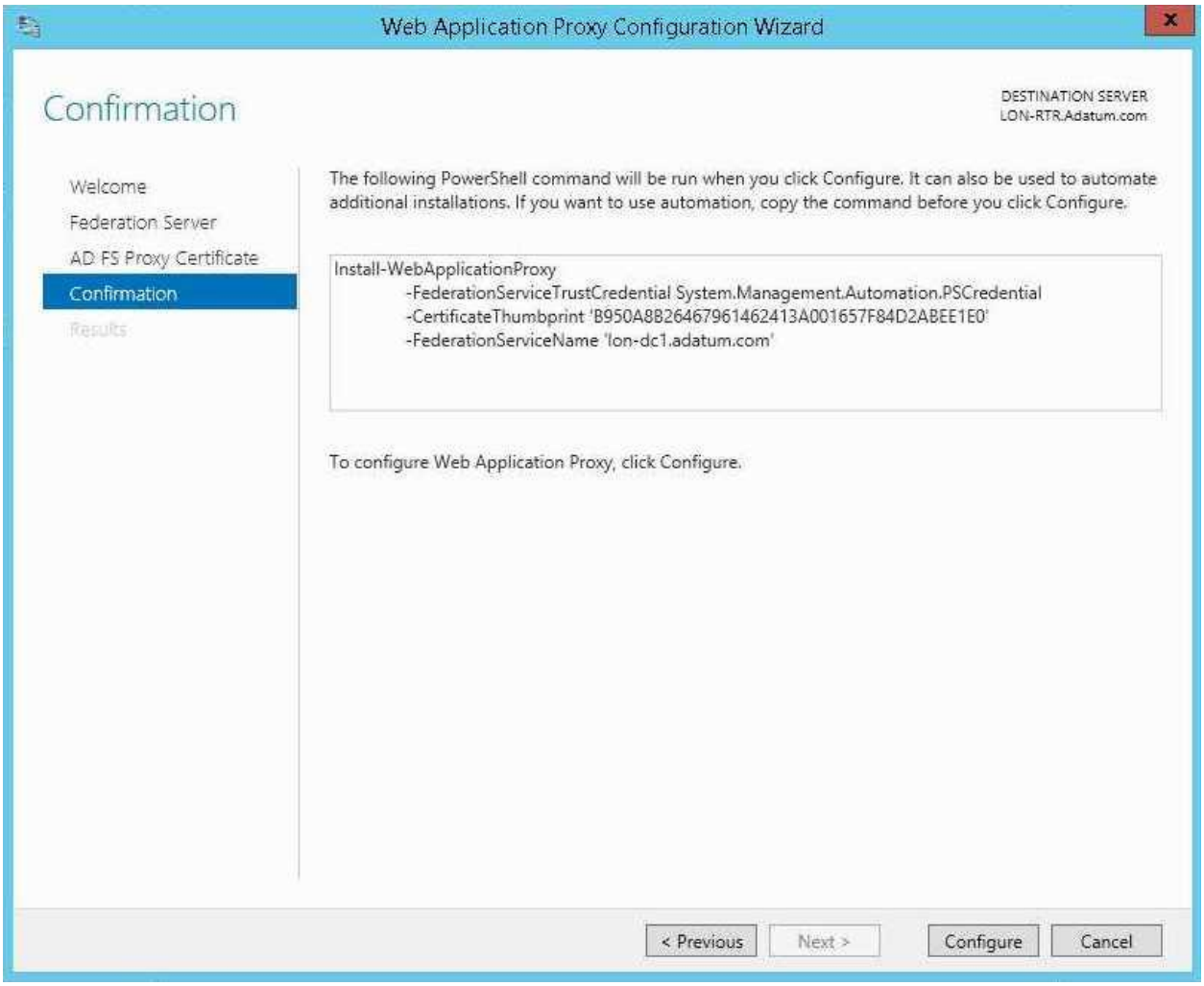


34. Cửa sổ **AD FS Proxy Certificate**, bung ô **Select a certificate to be used by the AD FS proxy**, chọn **lon-dc1.adatum.com**, và chọn **Next**.

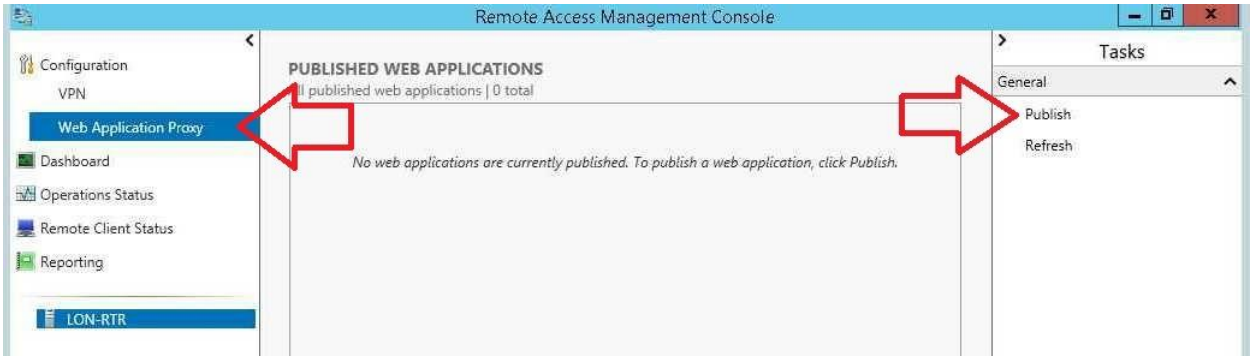


Lưu ý: Đây là certificate mà Web Application Proxy sẽ sử dụng cho chức năng AD FS proxy.

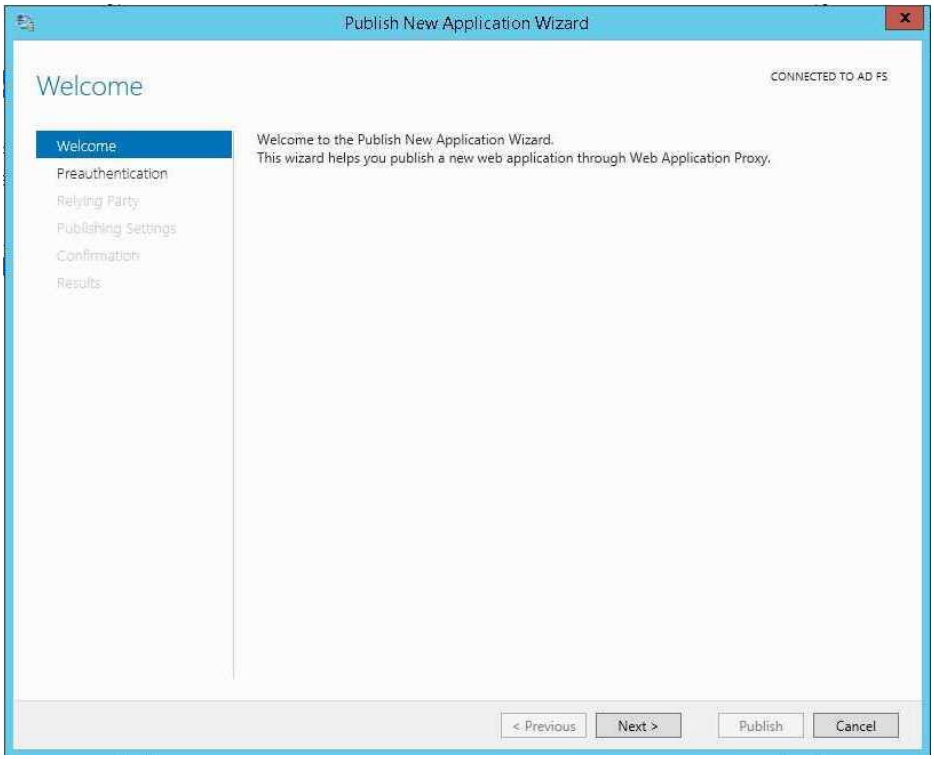
33. Cửa sổ **Confirmation**, chọn **Configure**, và chọn **Close.**



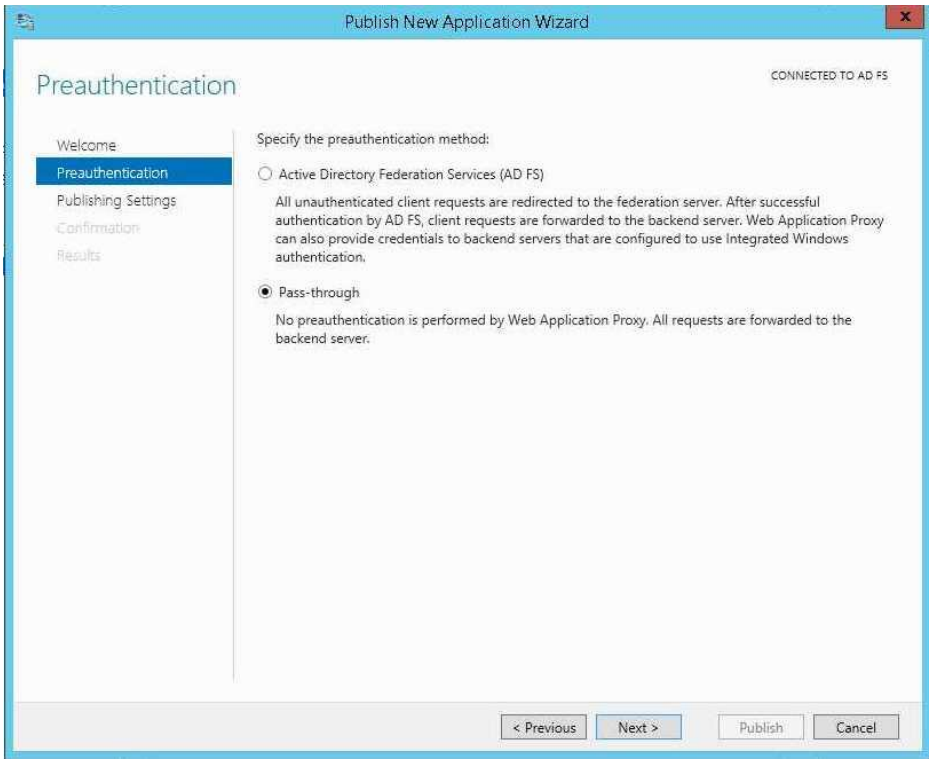
34. Trong cửa sổ **Remote Access Management Console**, chọn **Web Application Proxy**. Trong cửa sổ **Tasks**, chọn **Publish**.



35. Cửa sổ **Welcome**, chọn **Next**.

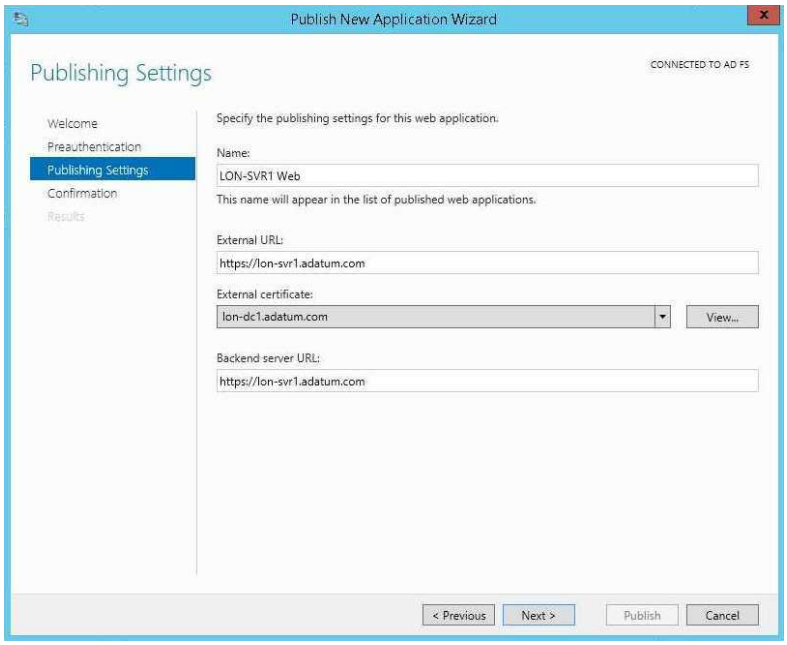


36. Cửa sổ **Preauthentication**, chọn **Pass-through**, và chọn **Next**.

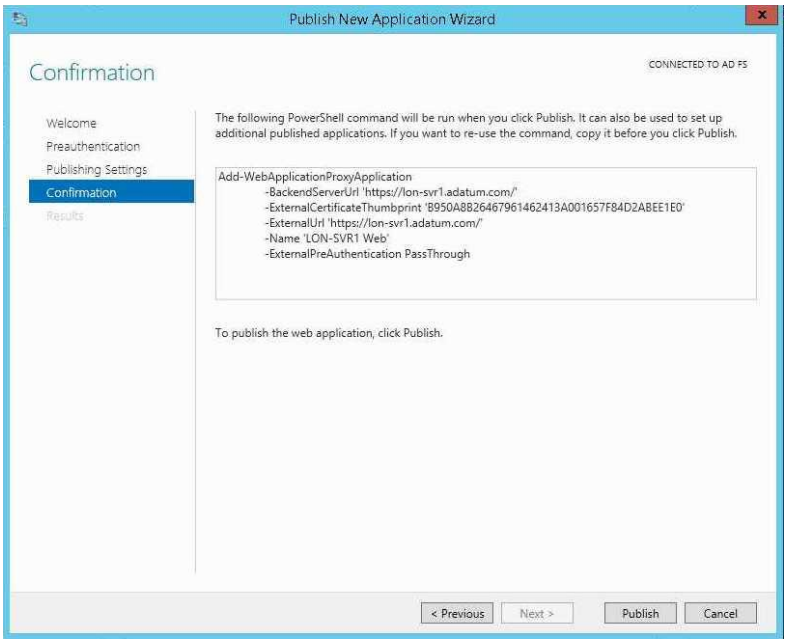


37. Cửa sổ **Publishing Settings**, nhập thông tin như bên dưới, và chọn **Next**:

- Name: **LON-SVR1 Web**
- External URL: **https://lon-svr1.adatum.com**
- External certificate: **lon-dc1.adatum.com**
- Backend server URL: **https://lon-svr1.adatum.com**



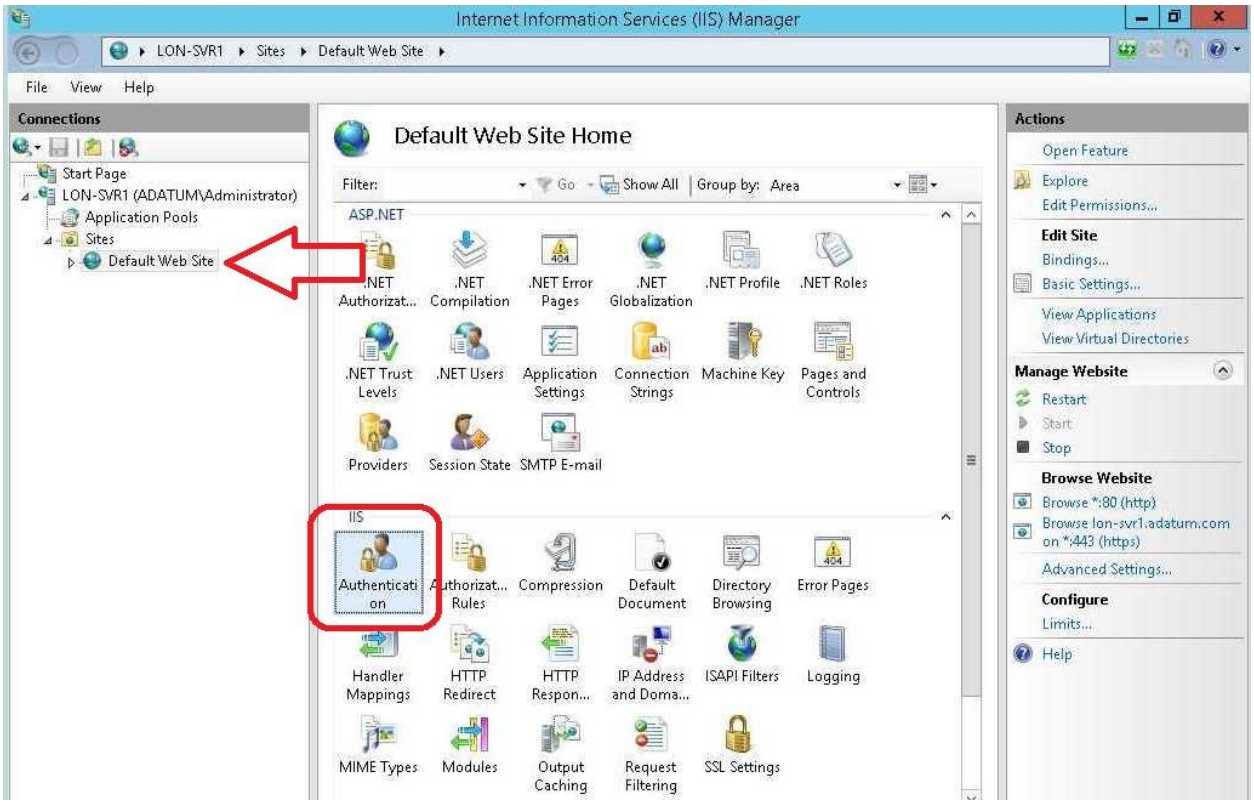
38. Cửa sổ **Confirmation**, chọn **Publish**, sau khi publish thành công, chọn **Close**



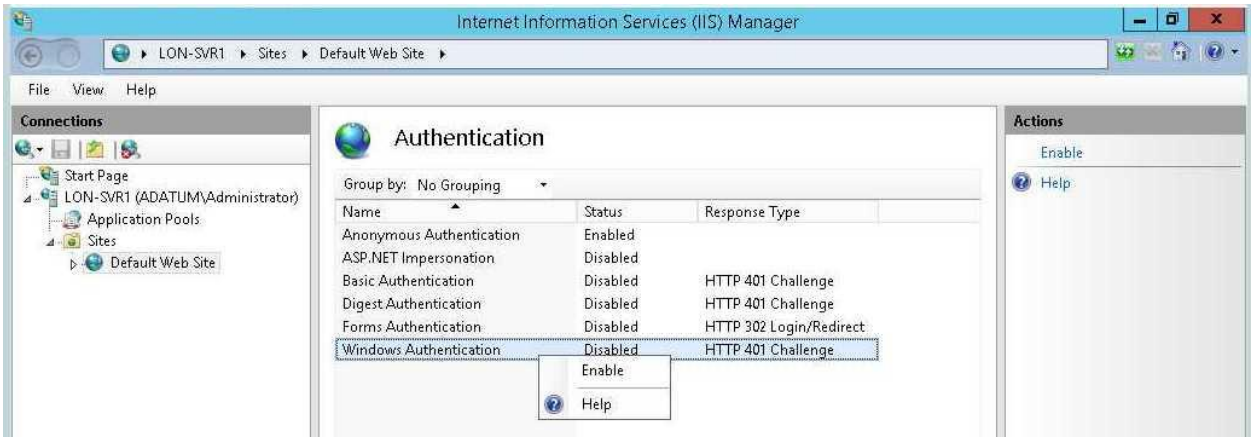
39. Qua máy **LON-SVR1.**

40. Trong **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**.

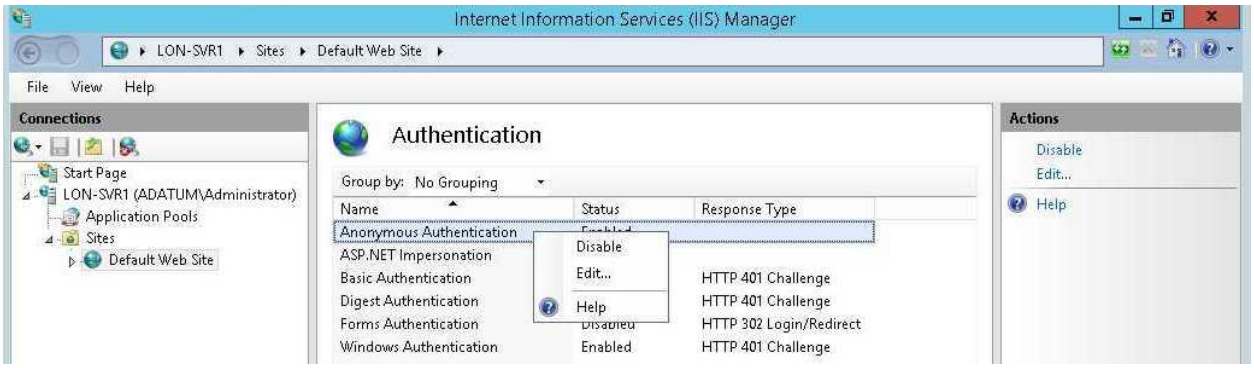
41. Trong cửa sổ **Internet Information Services (IIS) Manager**, bung **LON-SVR1 (ADATUM\Administrator)**, bung **Sites**, chọn **Default Web site**. Trong cửa sổ giữa, nhấp đôi chuột mở **Authentication**.



42. Cửa sổ **Authentication**, nhấn chuột phải **Windows Authentication**, chọn **Enable**.



43. Và nhấn chuột phải **Anonymous Authentication**, chọn **Disable**.



43. Tắt **Internet Information Services (IIS) Manager**.

Bước 4. Kiểm tra truy cập vào Website nội bộ.

1. Qua máy **LON-CL1**.

2. Mở **Control Panel**, chọn **System and Security**



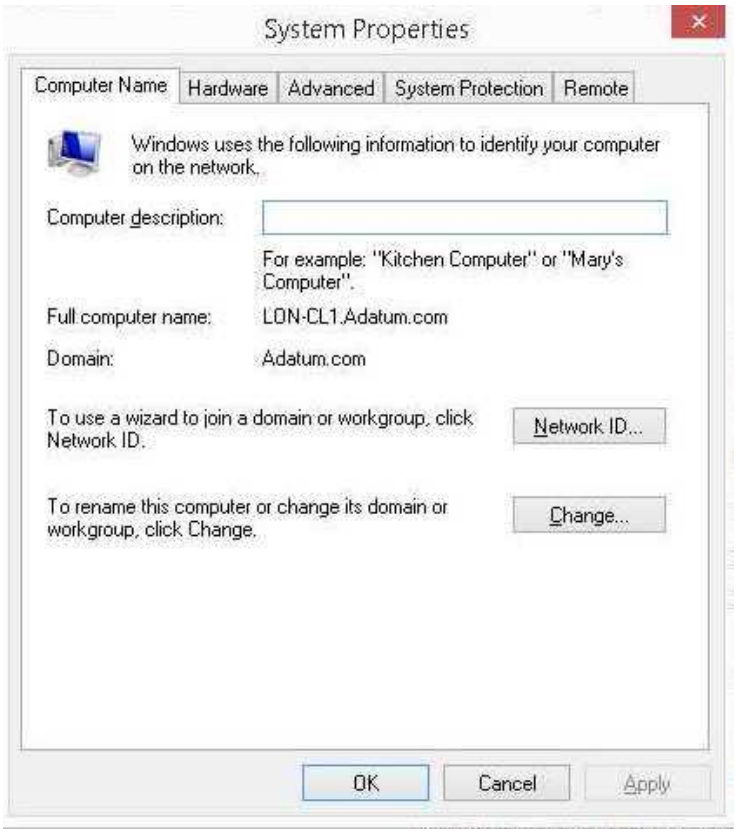
3. Cửa sổ **System and Security**, chọn **System**



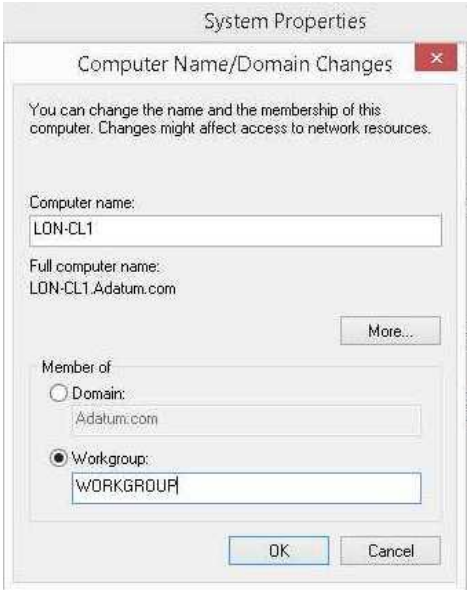
4. Cửa sổ **System,** chọn **Change Settings**.



5. Trong hộp thoại **System Properties**, chọn **Change**.



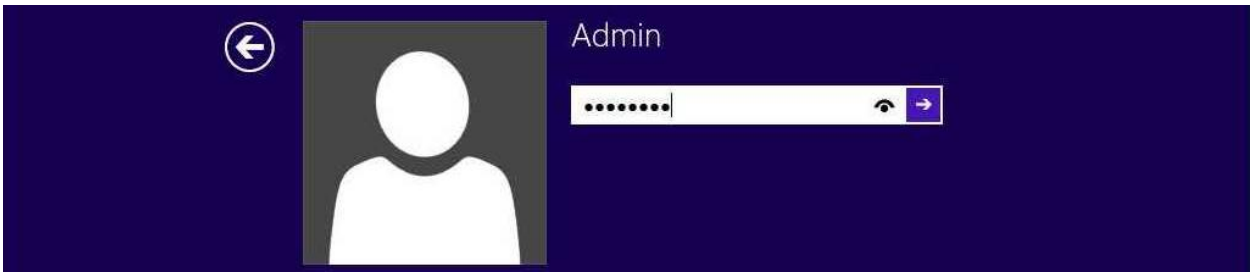
6. Hộp thoại **Computer Name/Domain Changes**, chọn **Workgroup**, nhập tên **WORKGROUP**, và chọn **OK** 4 lần.



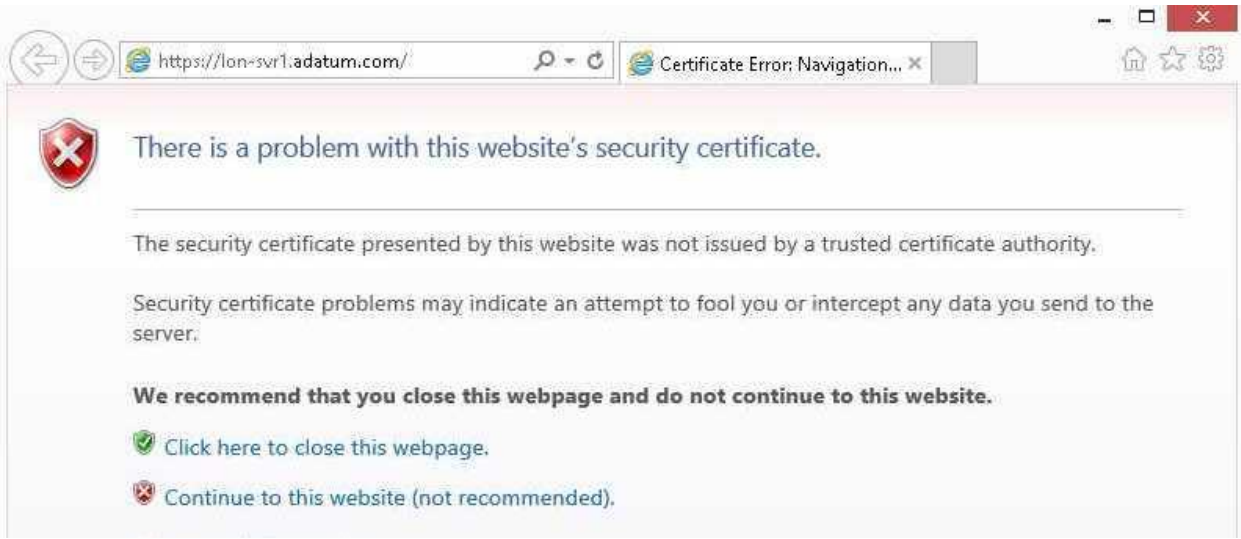
7. Hộp thoại **System Properties**, chọn **Close**, và chọn **Restart Now**.



8. Sau khi **LON-CL1** khởi động thành công, Logon **Admin** với password **Pa$$w0rd**.



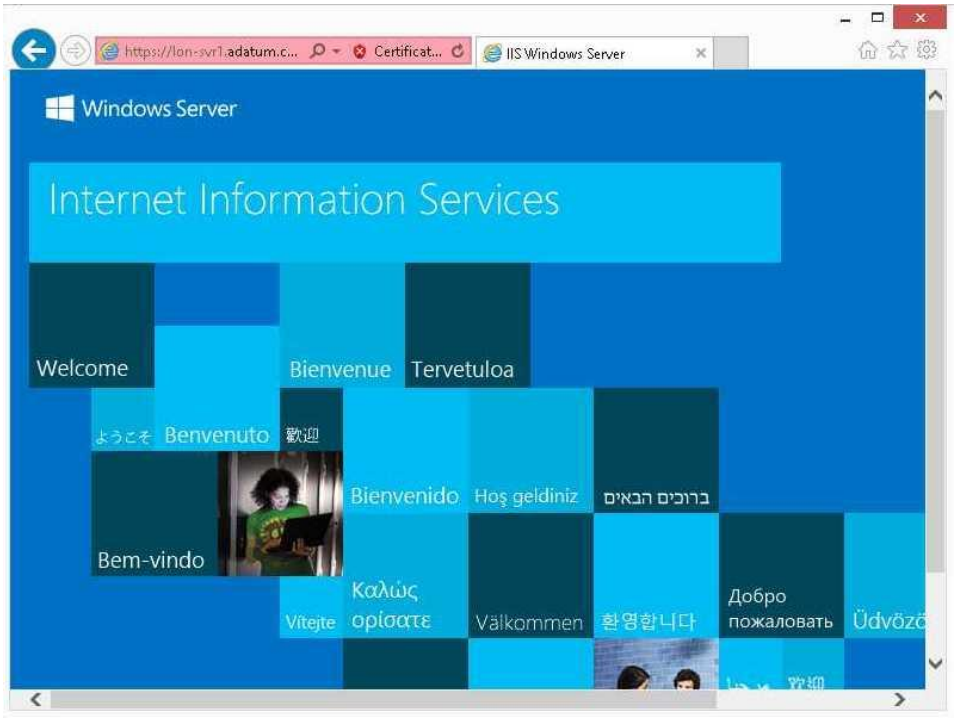
9. Mở **Internet Explorer,** truy cập địa chỉ **https://lon-svr1.adatum.com**. Chọn **Continue to this website (not recommended)**.



10. Hộp thoại **Internet Explorer**, khai báo thông tin đăng nhập như sau, và chọn **OK**:
    - Username: **Adatum\Bill**
    - Password: **Pa$$w0rd**



11. Kiểm tra truy cập thành công Website có giao diện IIS 8.0 của **LON-SVR1**.



Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công giải pháp Web Application Proxy.

❖ **Chuẩn bị cho bài tiếp theo:**

1. Trên máy thật, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20413C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho các máy ảo **20413C-LON-CL1, 20413C-LON-CL2, 20413C-LON-RTR, and 20413C-LON-SVR1.**