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

UPGRADING TECHNOLOGY EVERYDAY

# MCSE SERVER INFRASTRUCTURE

# 70-414

# MỤC LỤC

**Bài 1:** Triển khai giải pháp ảo hóa máy chủ - Server Virtualization. 4

**Bài 2:** Xây dựng cơ sở hạ tầng và giải pháp lưu trữ cho hệ thống ảo hóa. 36

**Bài 3:** Triển khai máy ảo với System Center Virtual Machine Manage. 124

**Bài 4:** Xây dựng giải pháp quản lý hệ thống ảo hóa bằng System Center 2012 R2**.** 160

**Bài 5:** Thực hiện giám sát hệ thống bằng Sytem Center Operations Manager. 232

**Bài 6:** Triển khai khả năng sẵn sàng cao (High Availability) cho dữ liệu và ứng dụng. 297

**Bài 7:** Triển khai khả năng sẵn sàng cao cho hệ thống ảo hóa bằng công nghệ Failover Clustering. 337

**Bài 8:** Sao lưu và phục hồi dữ liệu bằng Sytem Center Data Protection Manager. 414

**Bài 9:** Triển khai Active Directory Certificate Services (AD CS). 435

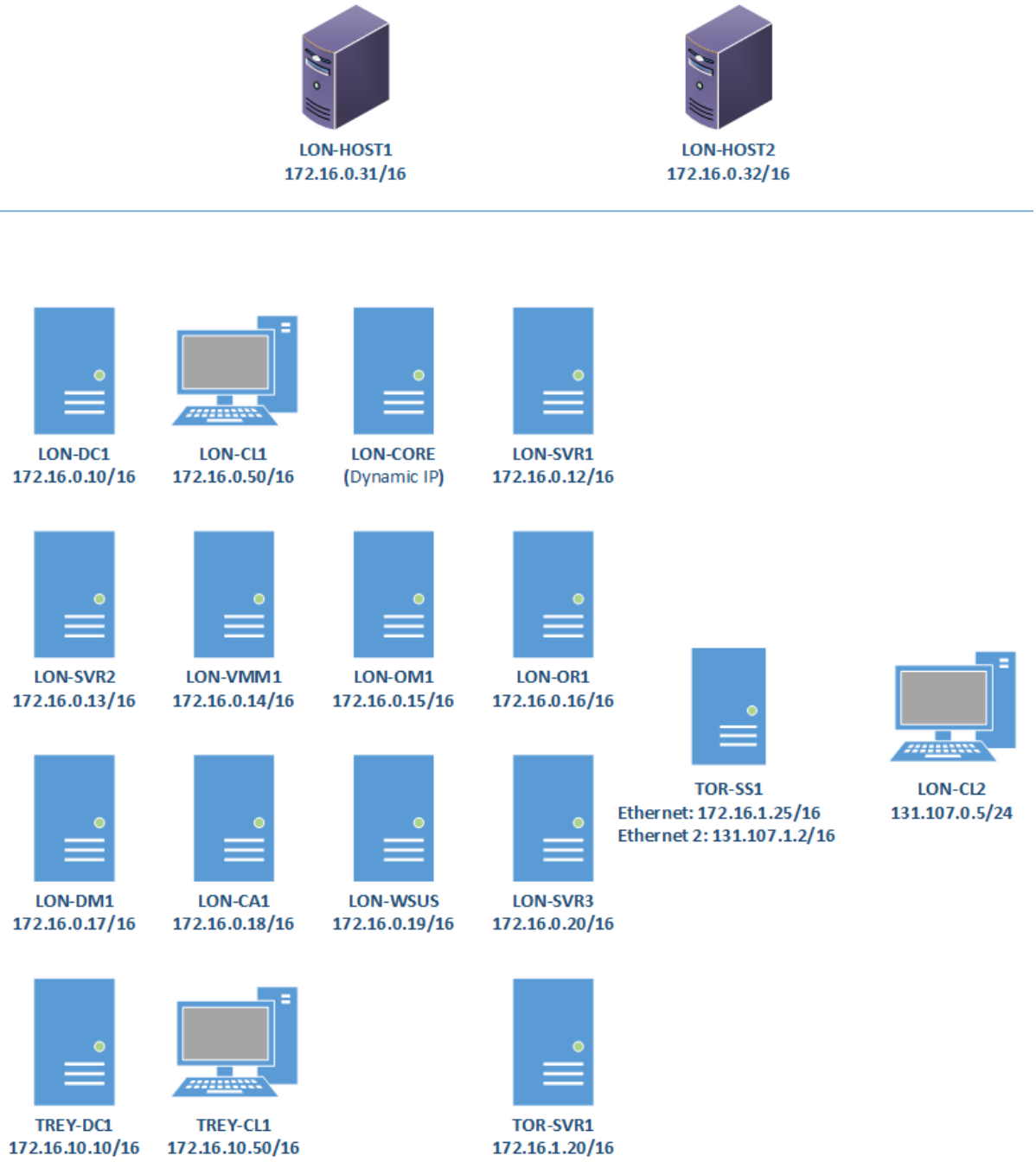
**Bài 10:** Triển khai Active Directory Federation Services (AD FS). 529

**Bài 11:** Triển khai Dynamic Access Control (DAC) và Access-Denied Assistance. 635

**Bài 12**: Triển khai chức năng Work Folders. 701

**Bài 13:** Triển khai Active Directory Rights Management Services (AD RMS). 755

# Mô hình LAB:


LON-HOST1
172.16.0.31/16
LON-HOST2
172.16.0.32/16
LON-DC1
172.16.0.10/16
LON-CL1
172.16.0.50/16
LON-CORE
(Dynamic IP)
LON-SVR1
172.16.0.12/16
LON-SVR2
172.16.0.13/16
LON-VMM1
172.16.0.14/16
LON-OM1
172.16.0.15/16
LON-OR1
172.16.0.16/16
TOR-SS1
Ethernet: 172.16.1.25/16
Ethernet 2: 131.107.1.2/16
LON-CL2
131.107.0.5/24
LON-DM1
172.16.0.17/16
LON-CA1
172.16.0.18/16
LON-WSUS
172.16.0.19/16
LON-SVR3
172.16.0.20/16
TREY-DC1
172.16.10.10/16
TREY-CL1
172.16.10.50/16
TOR-SVR1
172.16.1.20/16

## Chức năng của các máy ảo trong Mô hình LAB

| Máy ảo (VM) | Chức năng |
|---|---|
| **LON-HOST1**<br>**LON-HOST2** | Máy thật, chạy Windows Server 2012 (boot từ ổ cứng ảo vhd) |
| **LON-DC1** | Domain Controller của domain Adatum.com |
| **LON-SVR1**<br>**LON-SVR2**<br>**LON-SVR3** | 3 máy Member Servers của domain Adatum.com |
| **LON-VMM1** | System Center Virtual Machine Manager (VMM) 2012 Server |
| **TOR-SVR1** | Member Server của domain Adatum.com, đặt ở văn phòng chi nhánh |
| **TOR-SS1** | Windows Server 2012 có cấu hình sẵn iSCSI targets |
| **LON-OM1** | System Center Operations Manager (SCOM) 2012 Server |
| **LON-OR1** | System Center Orchestrator (Orchestrator) 2012 Server |
| **LON-DM1** | System Center Data Protection Manager (SCDPM) 2012 Server |
| **LON-WSUS** | Windows Server Update Services (WSUS) Server. |
| **LON-CA1** | Standalone Server |
| **LON-CL1** | Client của domain Adatum.com, có cài sẵn Microsoft® Office 2013 |
| **LON-CL2** | Standalone Client có cài sẵn Microsoft® Office 2013 |
| **LON-CORE** | Standalone Server chạy Windows Server 2012 Server Core |
| **TREY-DC1** | Domain Controller của domain TreyResearch.net domain |
| **TREY-CL1** | Client của domain TreyResearch.net, có cài sẵn Microsoft® Office 2013 |

# Bài 1: Lập kế hoạch và triển khai giải pháp ảo hóa máy chủ (Server Virtualization)

**I. Mục tiêu:**

- Lập kế hoạch triển khai Hyper-V Host.
- Cấu hình Hyper-V Hosts và Host Group trong System Center VMM.
- Cấu hình VMM Library.

**II. Kịch bản và các yêu cầu tổng quan:**

Cơ sở hạ tầng công nghệ thông tin của công ty A. Datum đang mở rộng nhanh chóng, nhưng công ty muốn giảm thiểu chi phí mở rộng. Trung tâm dữ liệu ở London đã gần như đạt đến công suất tối đa của không gian và điện năng, và công ty muốn tránh chi phí mở rộng hoặc xây dựng một trung tâm dữ liệu mới.

Vì vậy, một trong những mục tiêu quan trọng trong việc triển khai Windows Server 2012 là phải ảo hóa càng nhiều máy chủ, dịch vụ và ứng dụng càng tốt. Và một thành phần quan trọng của chiến lược ảo hóa này là phải tối ưu hóa công việc quản lý môi trường ảo hóa. Bước đầu tiên trong việc triển khai hệ thống ảo hóa tại A. Datum là lên kế hoạch triển khai các máy chủ Hyper-V (Hyper-V Hosts) và cấu hình Virtual Machine Manager (VMM) để quản lý hệ thống ảo hóa.

A. Datum đang có kế hoạch mua khoảng 30 server mới có cấu hình phần cứng không giống nhau để triển khai các Hyper-V Hosts. Hầu hết các Hyper-V Hosts đặt tại trung tâm dữ liệu ở London, một số khác đặt tại trung tâm dữ liệu ở Toronto và Sydney.

A. Datum đã triển khai một VMM Server tại London để quản lý tất cả các Hyper-V Hosts. A. Datum yêu cầu phải tạo ra một số máy ảo mẫu (VM Template), và các file cài đặt ISO sẽ lưu trong hệ thống VMM. Có một số lo ngại về lưu lượng băng thông giữa các văn phòng. Vì vậy,

thiết kế của bạn cho việc triển khai Hyper-V và VMM nên giảm thiểu băng thông mạng giữa London, Toronto, và Sydney.

A. Datum muốn tận dụng các tùy chọn có sẵn trong VMM để quản lý các Hyper-V Hosts khác nhau dựa trên vị trí của server. Bạn phải đảm bảo rằng các nhóm quản trị khác có thể quản lý các máy chủ ở London, Toronto, và Sydney, và đưa ra các quy định về việc phân phối các máy ảo tự động.

**III. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-HOST2**<br>**20414C-LON-DC1**<br>**20414C-LON-VMM1**<br>**20414C-TOR-SVR1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**IV. Chuẩn bị:**

Bài thực hành gồm 2 máy thật, 1 máy khởi động **20414C-LON-HOST1** và 1 máy khởi động **20414C-LON-HOST2**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
2. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
3. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
4. Thực hiên từ bước 1 đến 3 cho các máy ảo còn lại**.**

5. Logon vào máy **20414C-LON-HOST2** với thông tin sau:

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

**V. Thực hành:**

*Thời gian thực hành: 60 phút*

**Bài tập 1: Cấu hình Hyper-V Hosts và Host Groups**

Sau khi cài đặt các Hyper-V Hosts và VMM Server thành công, bạn cần phải bổ sung các Hyper-V Hosts vào VMM. Sau đó, bạn sẽ tạo và cấu hình Host Group trong VMM.

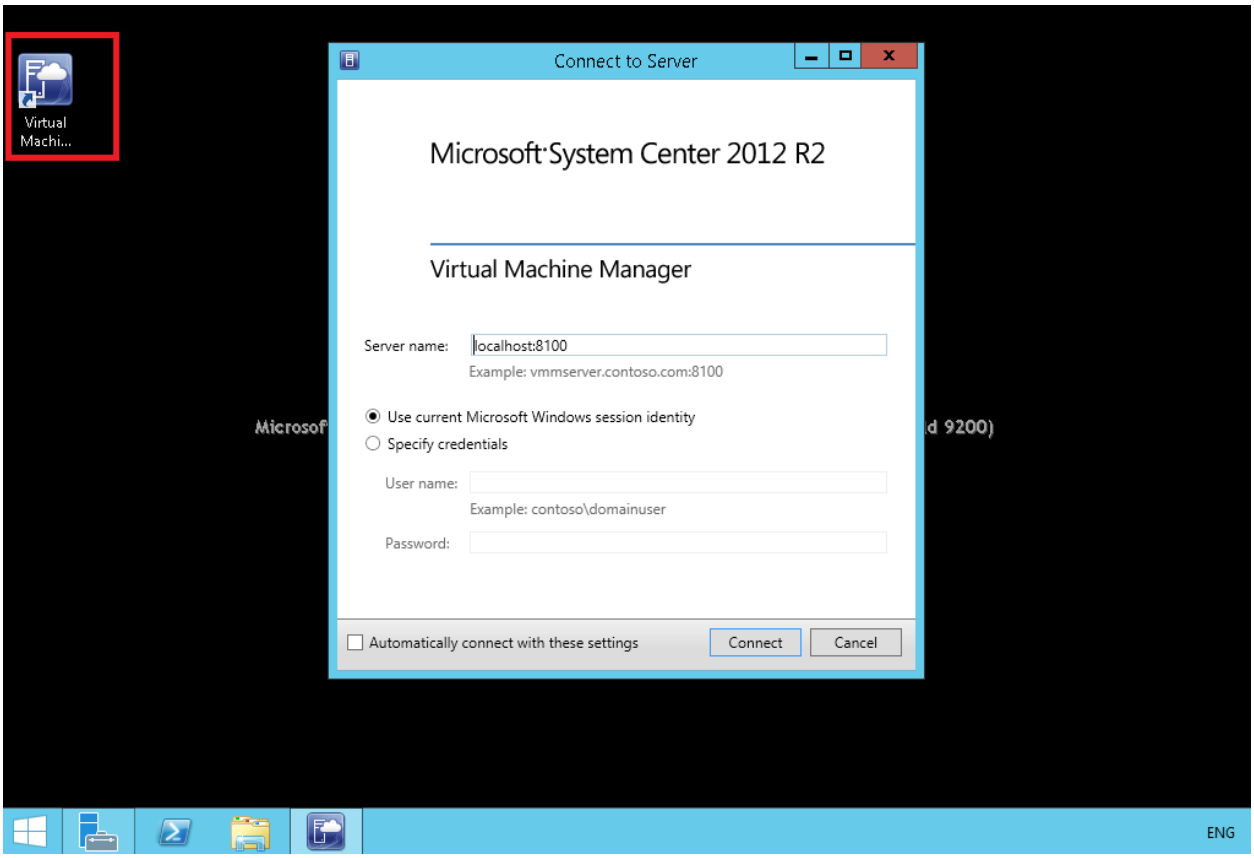
❖ **Bài thực hành bao gồm các bước:**

1. Đưa Hyper-V Host vào VMM.
2. Tạo Host Groups.
3. Cấu hình Host Groups.

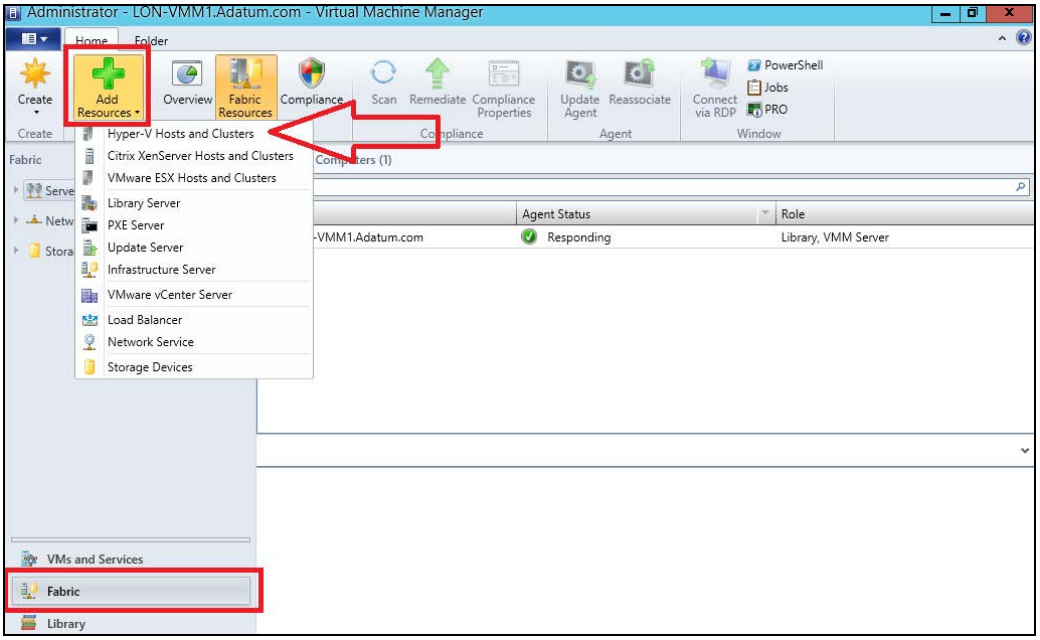
❖ **Thực hiện:**

**Bước 1: Đưa Hyper-V Host vào VMM.**

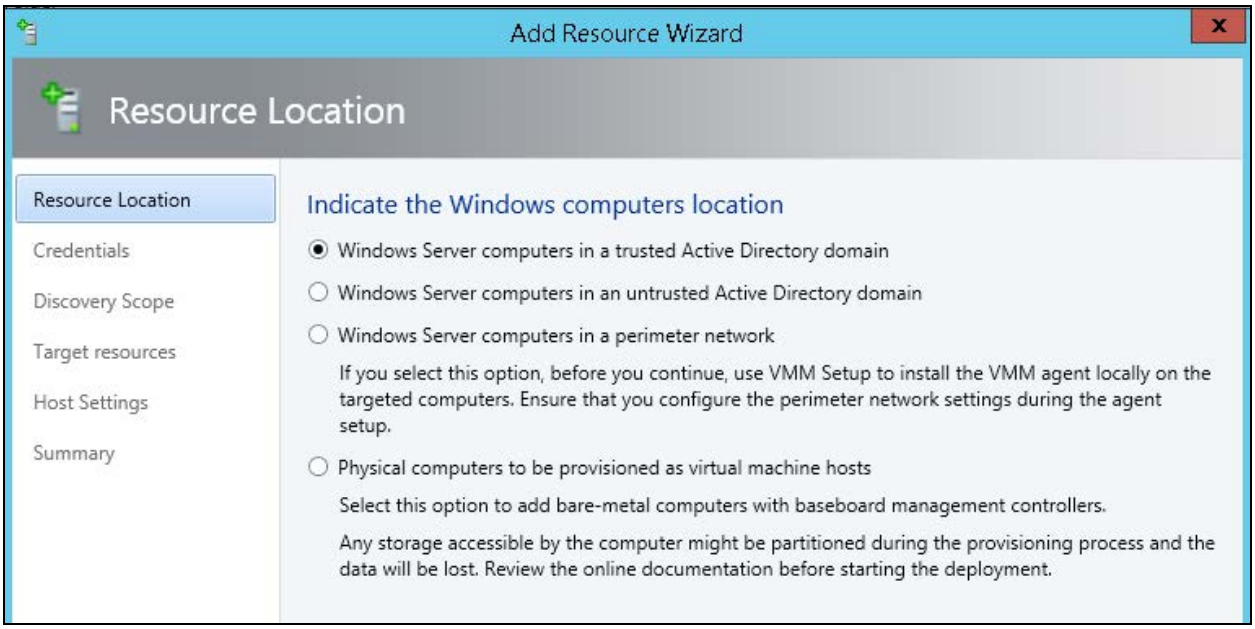
1. Trên máy **LON-VMM1**, ngoài Desktop, mở **Virtual Machine Manager Console**. Cửa sổ **Connect to Server**, chọn **Connect**.



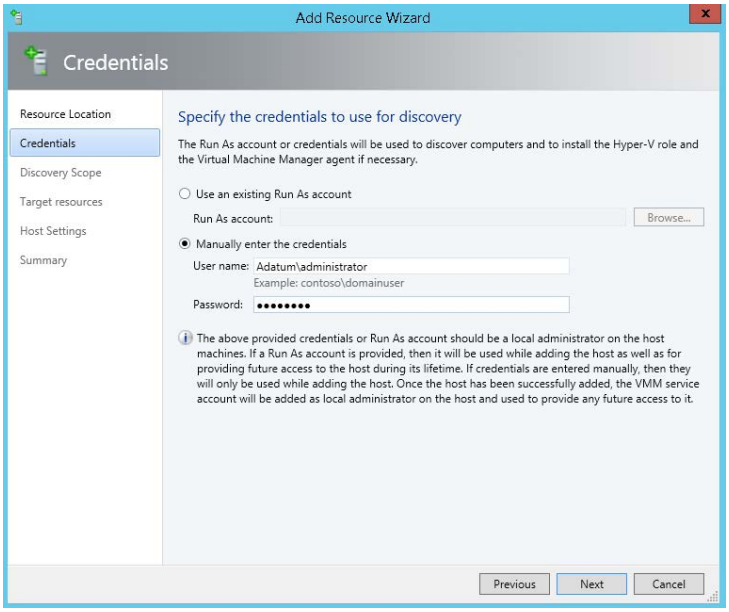
2. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric,** chọn **Add Resources**, và chọn **Hyper-V Hosts and Clusters**.



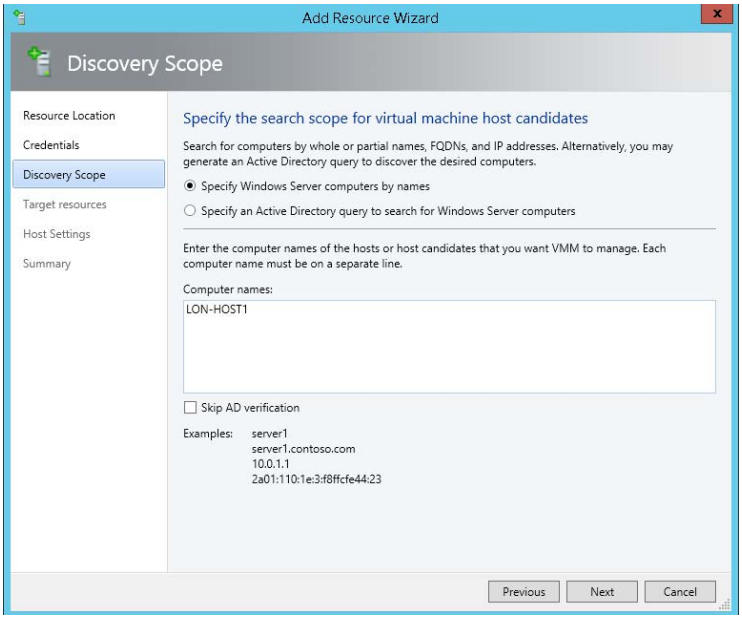

3. Cửa sổ **Resource Location**, chọn **Windows Server computers in a trusted Active Directory domain**, và chọn **Next**.



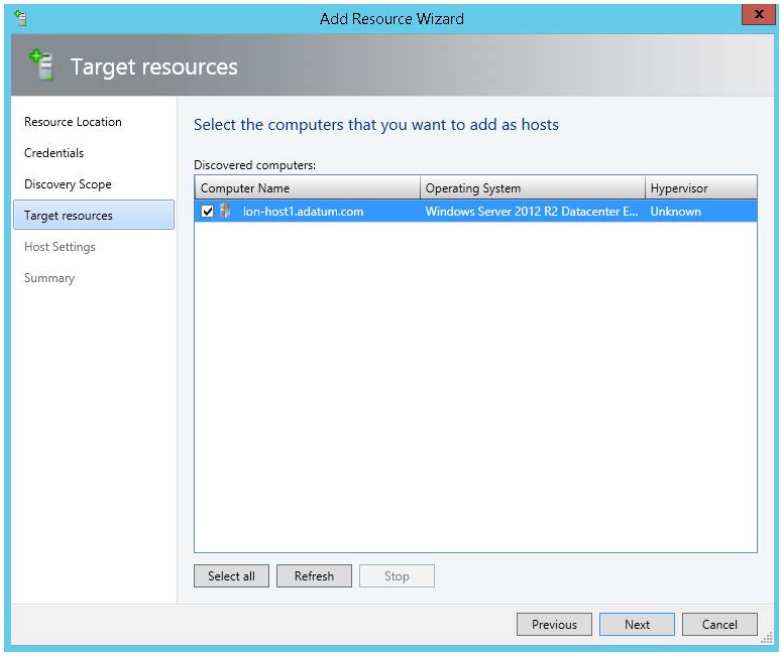
4. Cửa sổ **Credentials**, chọn **Manually enter the credentials**, trong ô **User name**, nhập **Adatum\Administrator,** trong ô **Password**, nhập **Pa$$w0rd**, và chọn **Next**.



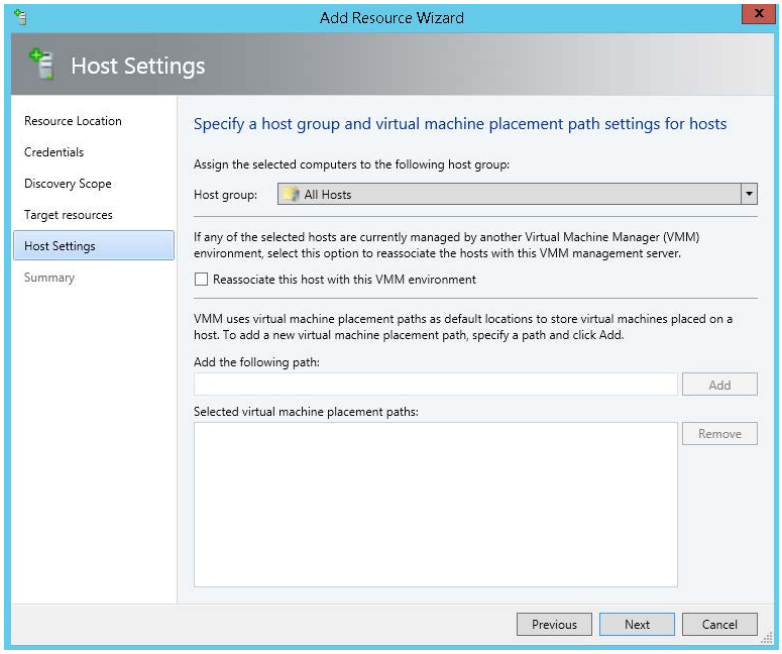

5. Cửa sổ **Discovery scope**, chọn **Specify Windows Server computers by names**, trong ô **Computer names**, nhập **LON-HOST1**, và chọn **Next**.



6. Cửa sổ **Target resources**, đánh dấu chọn **lon-host1.adatum.com**, chọn **Next**. Hộp thoại thông báo, chọn **OK.**

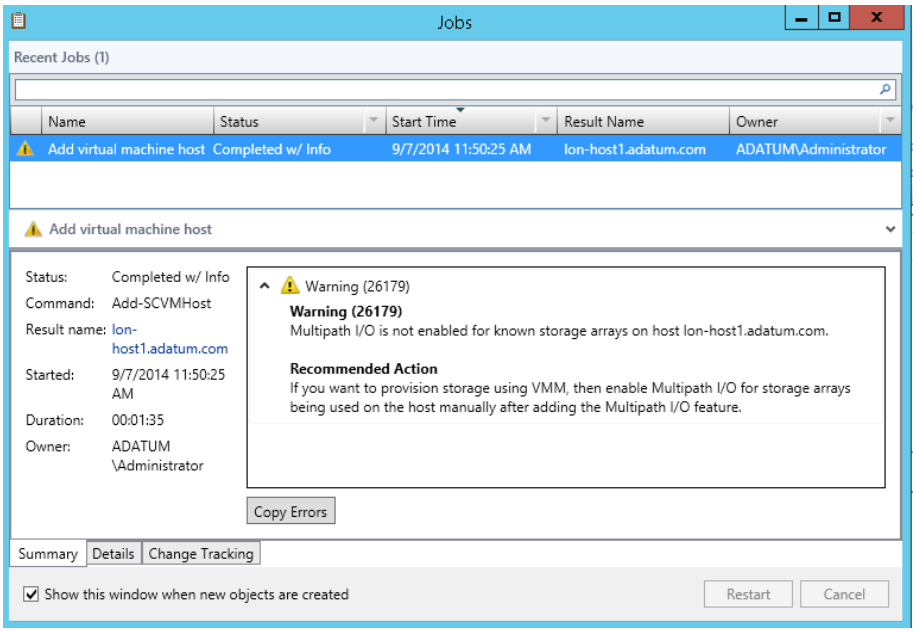



7. Cửa sổ **Host Settings**, chọn **All Hosts**, và chọn **Next**.

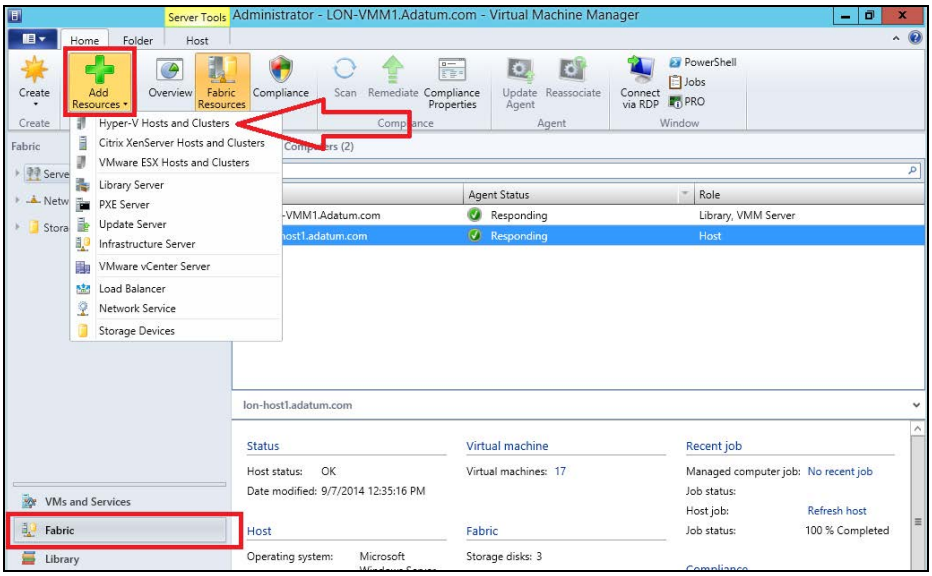


8. Cửa sổ **Summary**, chọn **Finish**.

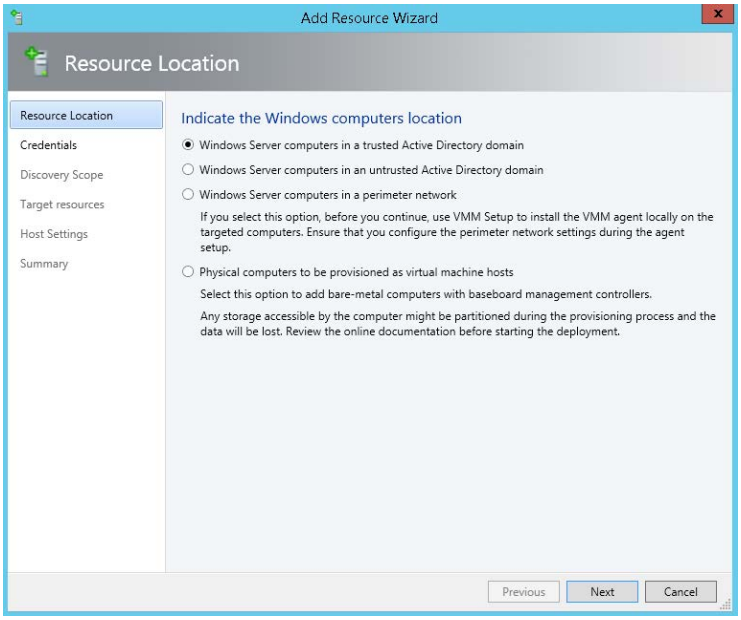
9. Trong cửa sổ **Jobs**, kiểm tra thông báo, sau khi công việc hoàn tất, tắt cửa sổ **Jobs**. (*Một cảnh báo có thể xuất hiện, liên quan đến multipath I / O không được kích hoạt. Cảnh báo này không quan trọng, bạn hãy bỏ qua cảnh báo này*)



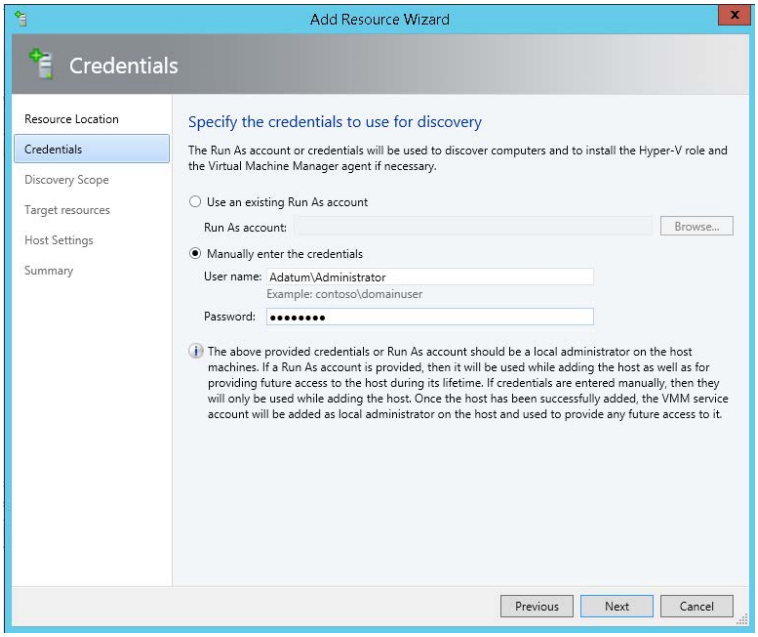

10. Chọn **Fabric**, chọn **Add Resources**, và chọn **Hyper-V Hosts and Clusters**.



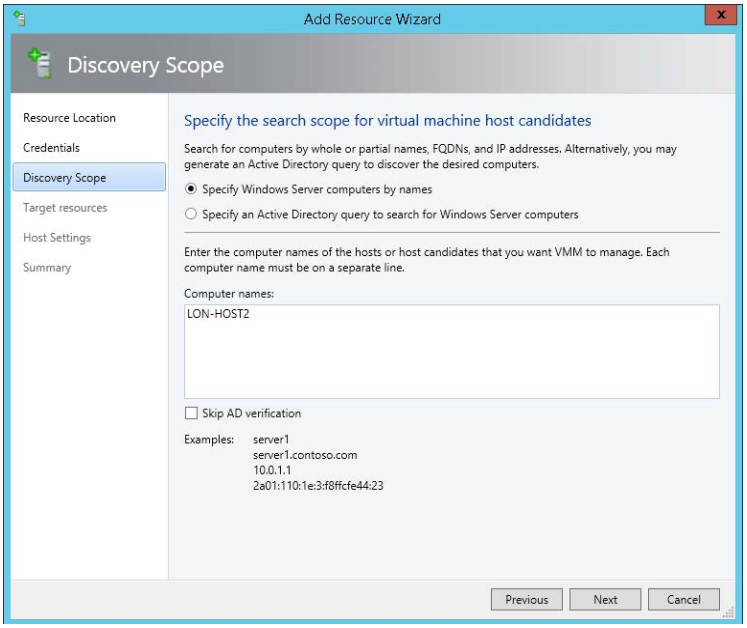
11. Cửa sổ **Resource location**, chọn **Windows Server computers in a trusted Active Directory domain**, và chọn **Next**.



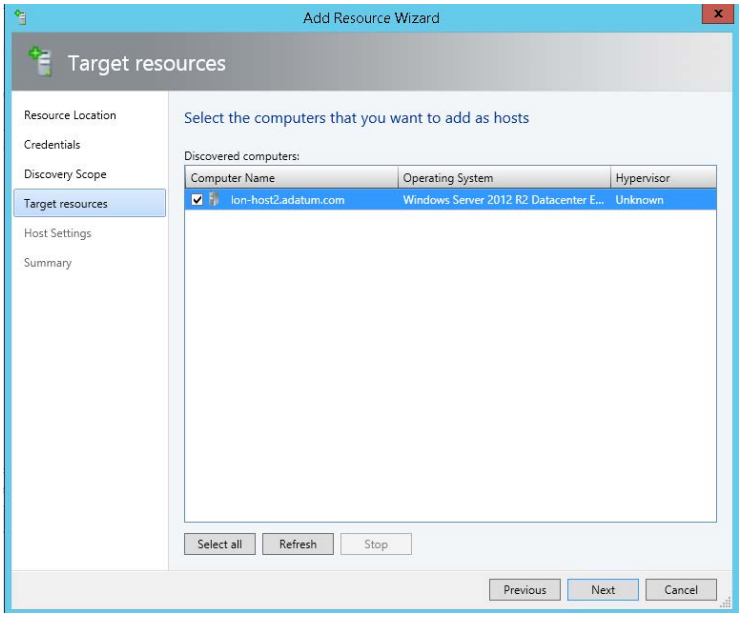

12. Cửa sổ **Credentials**, chọn **Manually enter the credentials**, trong ô **User name**, nhập **Adatum\Administrator,** trong ô **Password**, nhập **Pa$$w0rd,** chọn **Next**.



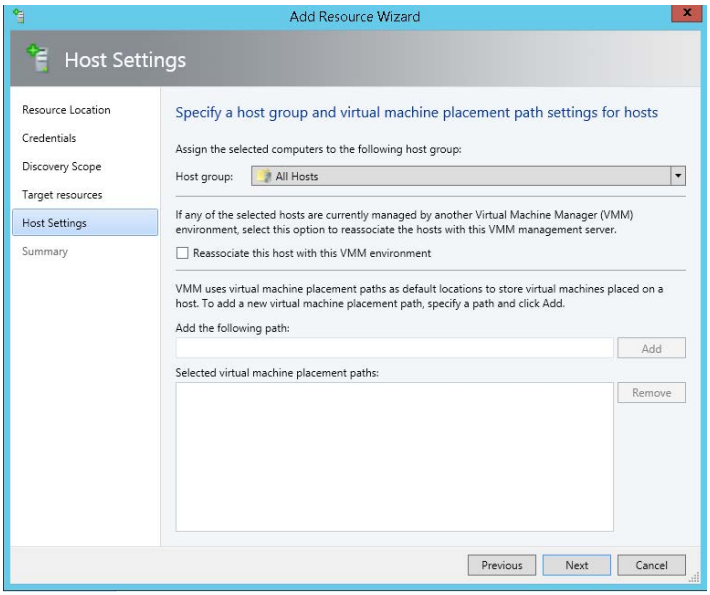
13. Cửa sổ **Discovery Scope**, chọn **Specify Windows Server computers by names**, trong ô **Computer names**, nhập **LON-HOST2**, và chọn **Next**.




14. Cửa sổ **Target resources**, đánh dấu chọn **lon-host2.adatum.com**, chọn **Next**. Hộp thoại thông báo, chọn **OK**.

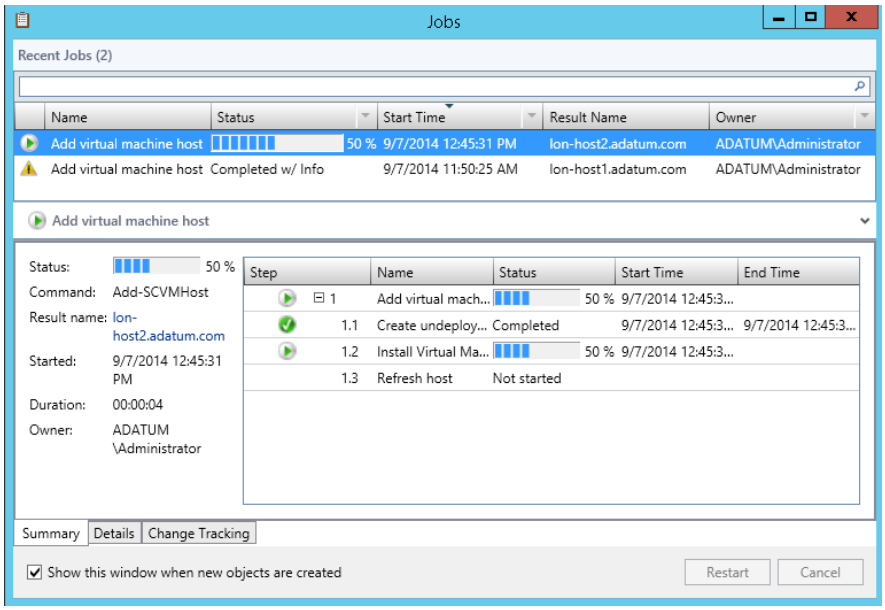


15. Cửa sổ **Host settings**, chọn **All Hosts**, và chọn **Next**.




16. Cửa sổ **Summary**, chọn **Finish**

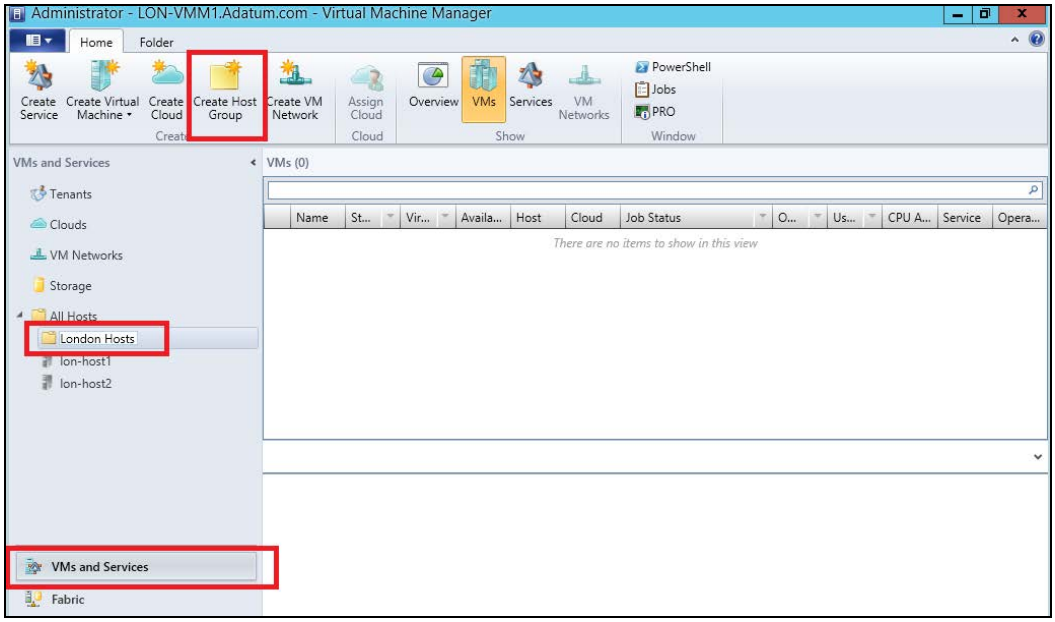
17. Trong cửa sổ **Jobs**, kiểm tra thông báo, sau khi công việc hoàn tất, tắt cửa sổ **Jobs**. (*Một cảnh báo có thể xuất hiện, liên quan đến multipath I / O không được kích hoạt. Cảnh báo này không quan trọng, bạn hãy bỏ qua cảnh báo này*)



## Bước 2: Tạo Host Groups.

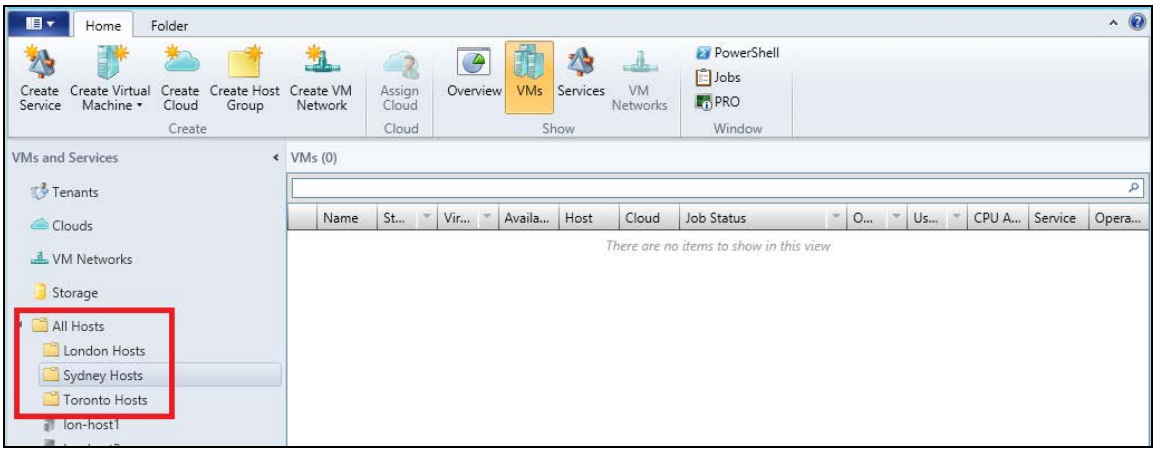
1. Trên máy **LON-VMM1**

2. Trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, chọn **All Hosts,** chọn **Create Host Group**, đặt tên cho host group là **London Hosts**.




3. Lặp lại bước 2 để tạo các host group sau:

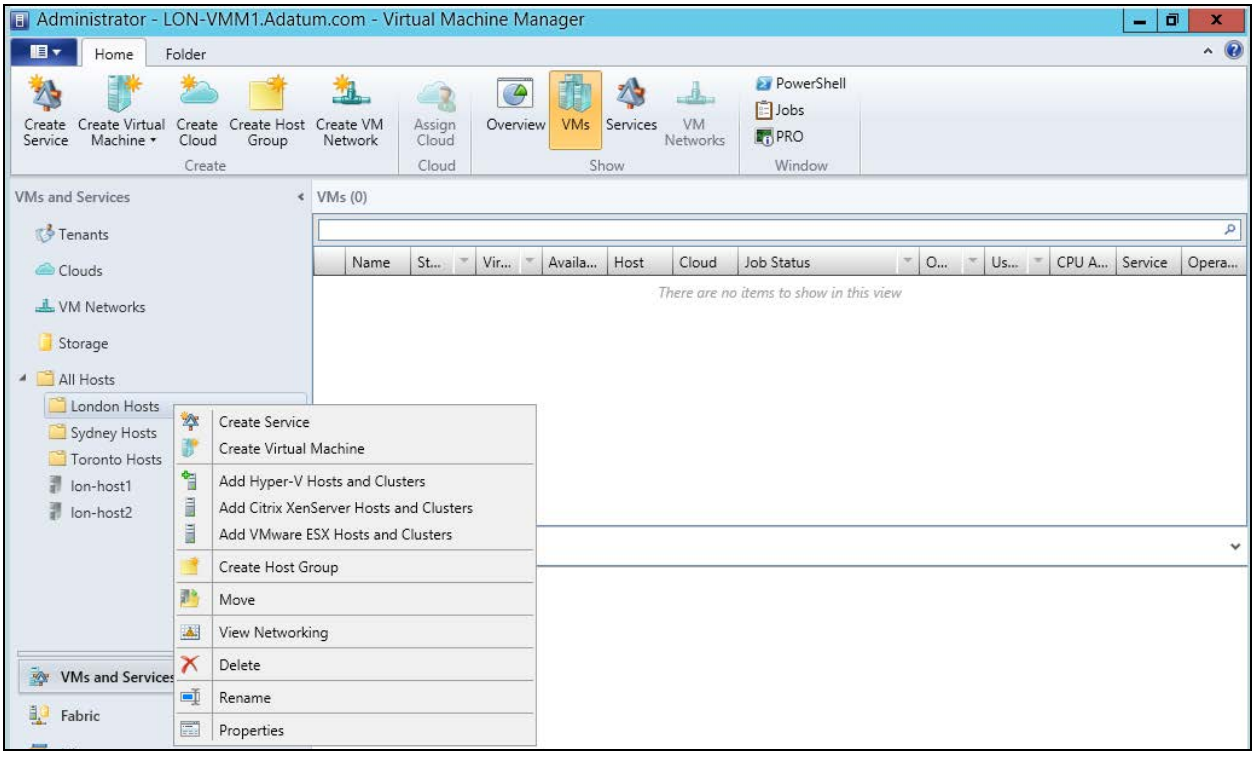
- **Toronto Hosts**
- **Sydney Hosts**



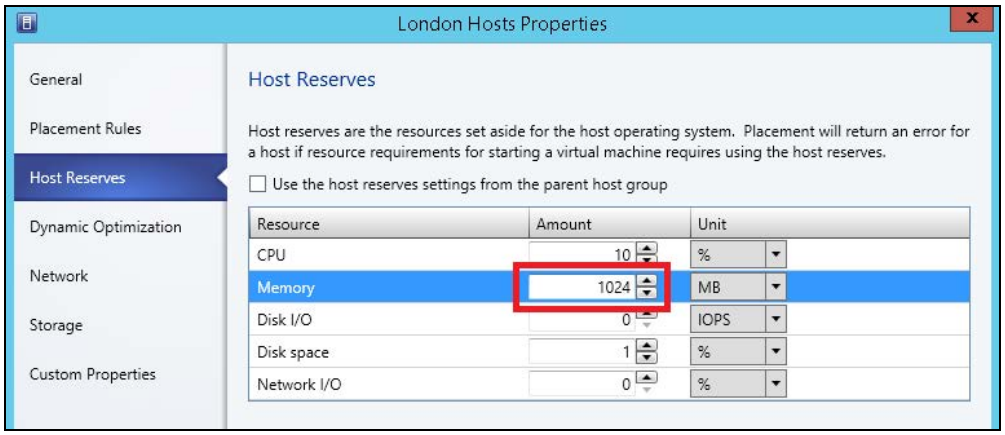
**Bước 3: Cấu hình Host Groups.**

1. Trên máy **LON-VMM1**.

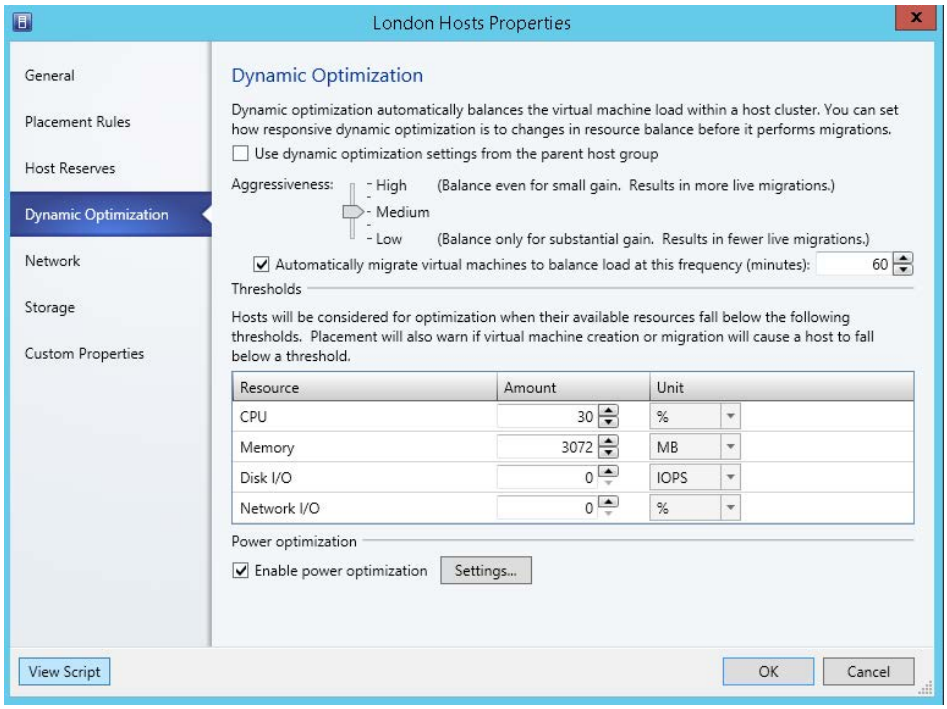
2. Trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, chuột phải **London Hosts**, và chọn **Properties**.



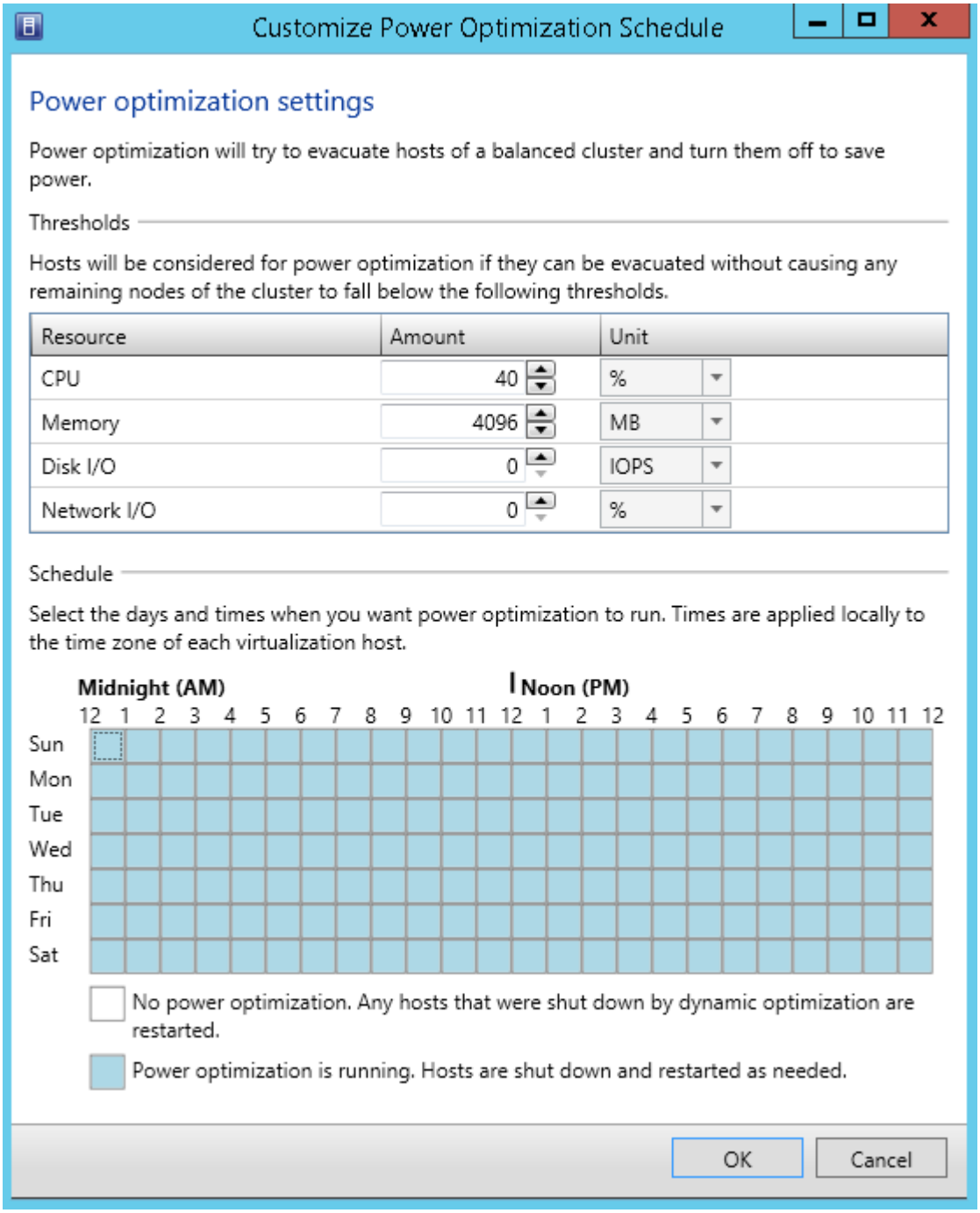
3. Cửa sổ **London Hosts Properties**, chọn mục **Host Reserves**, bỏ dấu chọn **Use the host reserves settings from the parent host group**, trong ô **Memory**, chỉnh thành **1024 MB**.



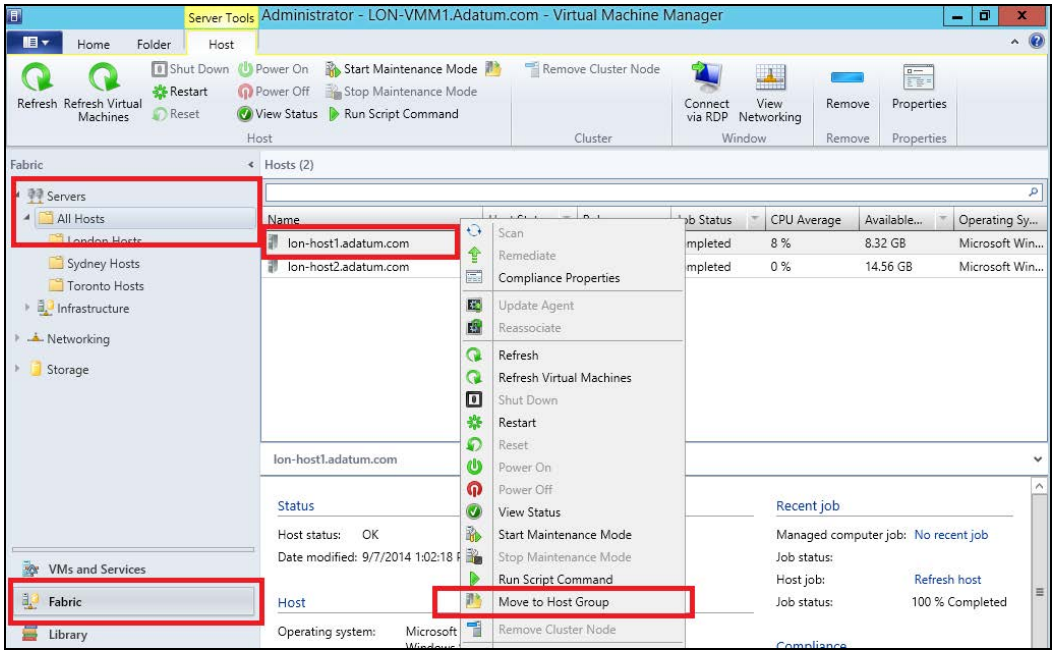

4. Chọn mục **Dynamic Optimization**, bỏ dấu chọn **Use dynamic optimization settings from the parent host group**, đánh dấu chọn **Automatically migrate virtual machines to balance load at this frequency**, và chỉnh thành **60 Minutes**. Đánh dấu chọn **Enable power optimization**, và chọn **Settings.**



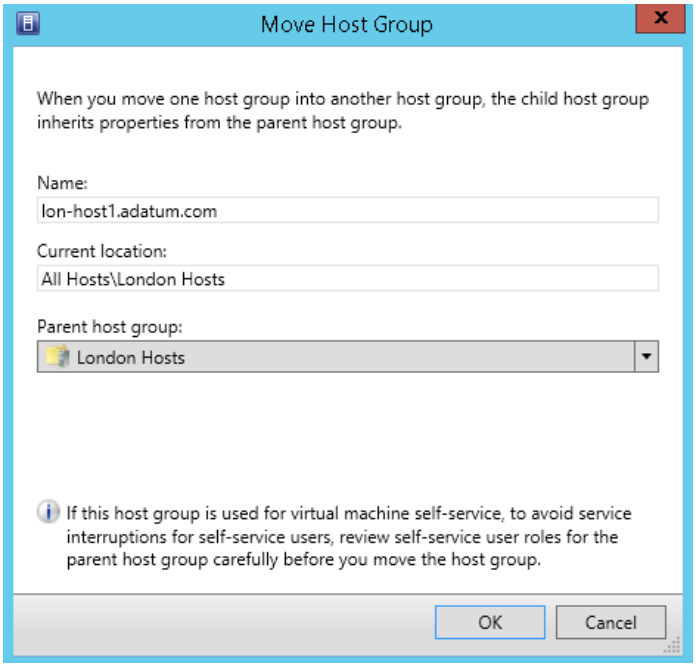
5. Trong cửa sổ **Customize Power Optimization Schedule,** kiểm tra thông tin, và chọn **OK** 2 lần.



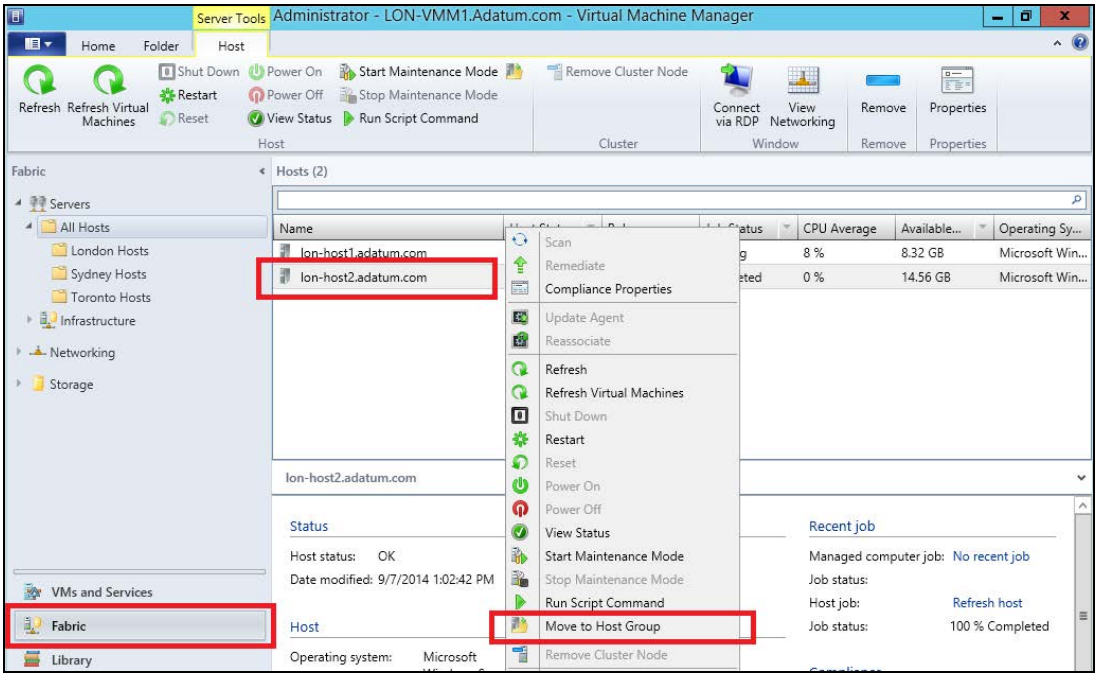
6. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric**, bung **Servers**, chọn **All Hosts**, chuột phải **lon-host1.adatum.com,** chọn **Move to Host Group**.



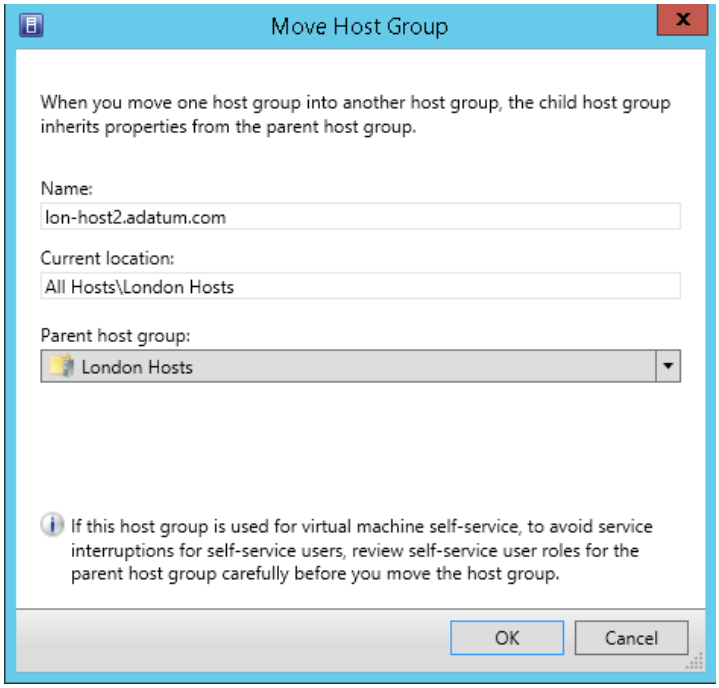

7. Hộp thoại **Move Host Group**, bung ô **Parent host group**, chọn **London Hosts**, chọn **OK**.



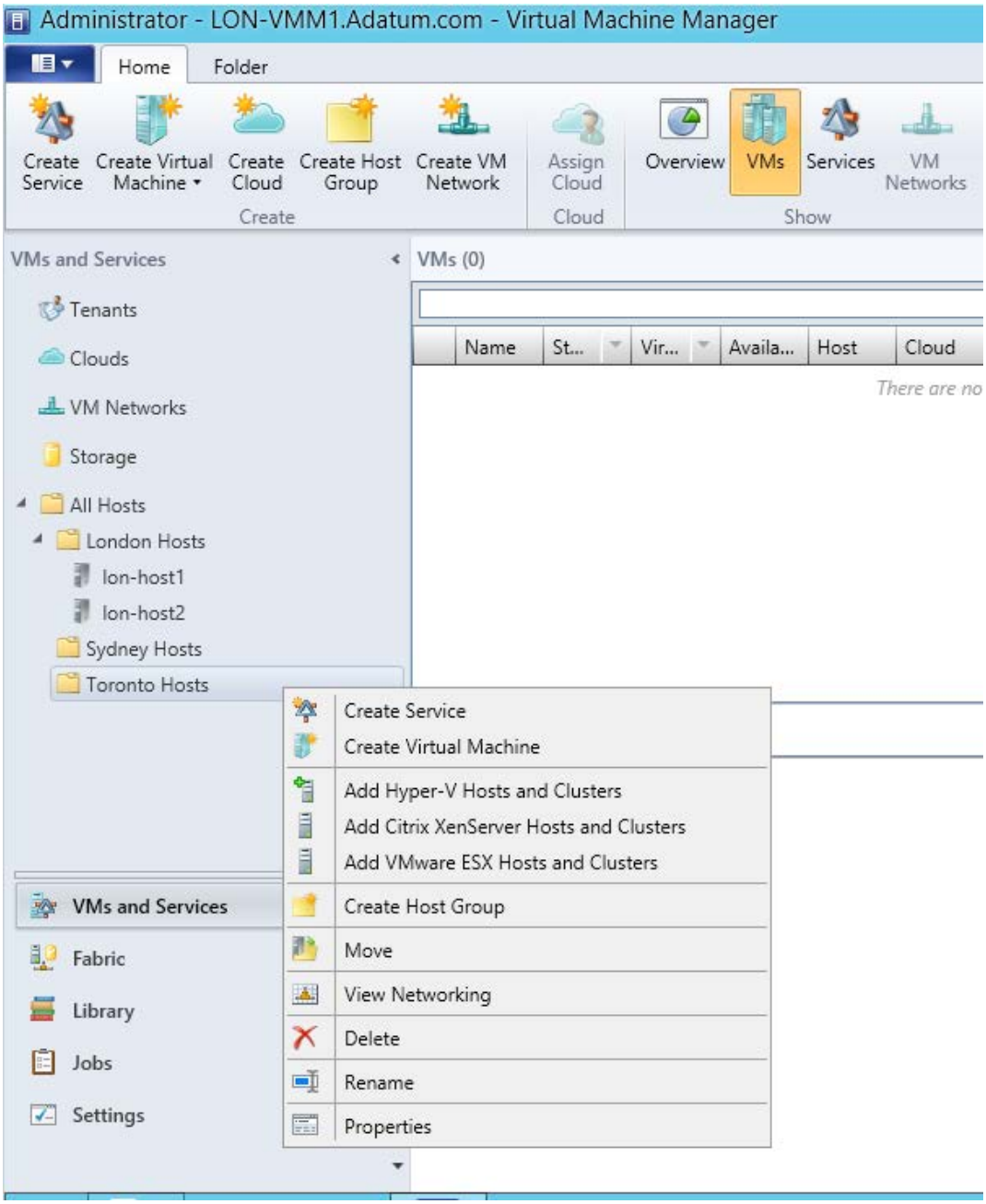
8. Chuột phải **lon-host2.adatum.com,** chọn **Move to Host Group**.



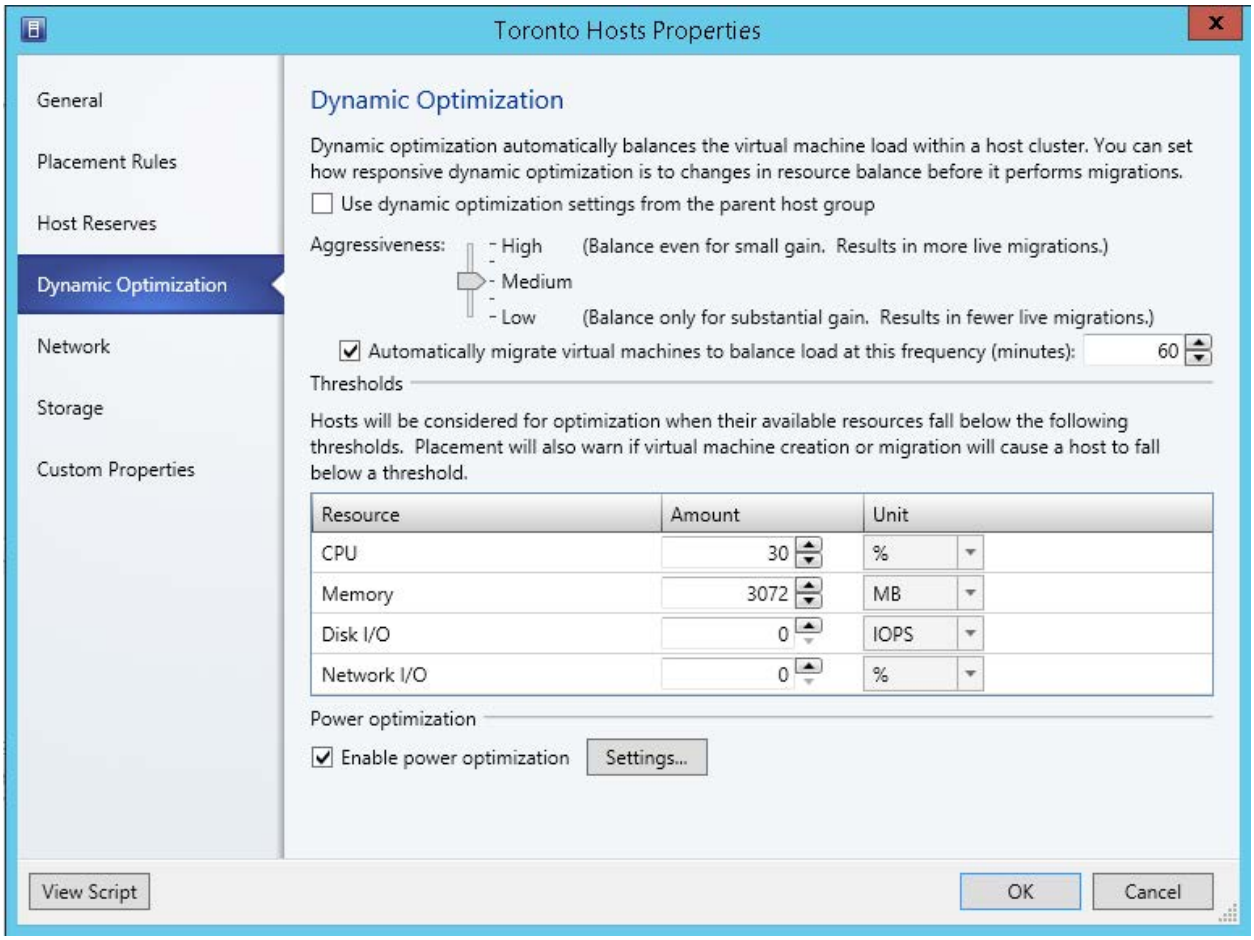

9. Hộp thoại **Move Host Group**, bung ô **Parent host group**, chọn **London Hosts**, chọn **OK**.



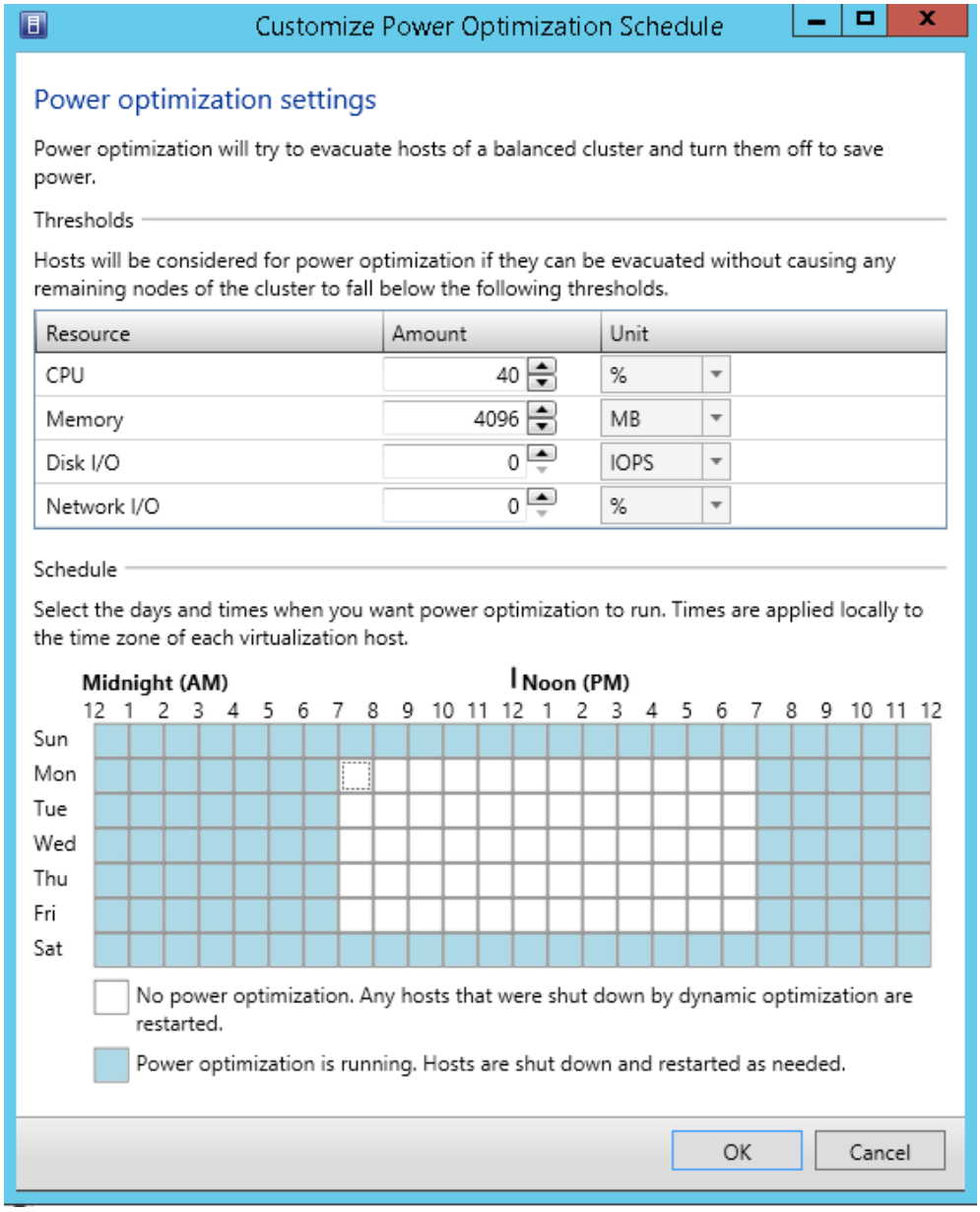
10. Trong cửa sổ **Virtual Machine Manager,** chọn **VMs and Services**, chuột phải **Toronto Hosts**, chọn **Properties**.



11. Cửa sổ **Toronto Hosts Properties**, vào mục **Dynamic Optimization**, bỏ dấu chọn **Use dynamic optimization settings from the parent host group**, đánh dấu chọn **Automatically migrate virtual machines to balance load at this frequency**, và chỉnh thành **60 Minutes**. Đánh dấu chọn **Enable power optimization**, và chọn **Settings**.



12. Trong cửa sổ **Customize Power Optimization Schedule,** cấu hình từ **7 AM** tới **7 PM**, từ **Monday** tới **Friday** là **No power optimization**, chọn **OK** 2 lần.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã tạo Host Groups, và add các Hyper-V Host vào Host Groups thành công.**

## Bài tập 2: Cấu hình VMM Library

Bạn đã quyết định triển khai VMM Library trên một File Server nằm trong trung tâm dữ liệu ở Toronto, để có thể giảm thiểu lưu lượng mạng liên quan đến việc triển khai Hyper-V. Bạn cần phải cấu hình VMM Library trên Server, và sau đó phân phối các thành phần VMM cho mỗi Library. Bạn cũng cần phải đảm bảo rằng các nhóm quản trị tại mỗi địa phương có quyền tạo ra các máy ảo trong trung tâm dữ liệu Toronto, và họ phải có quyền truy cập vào tất cả các file cần thiết trong Library.

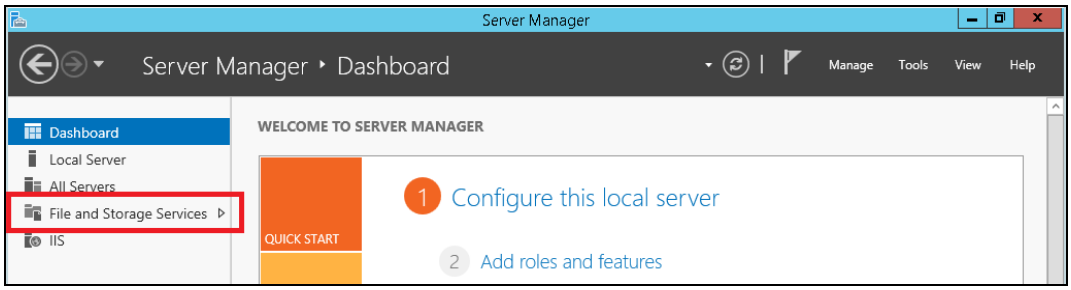
❖ **Bài thực hành bao gồm các bước:**

- Cấu hình Library Server và Library Share.
- Sao chép các file cần thiết đến trung tâm dữ liệu của văn phòng chi nhánh.
- Gán Library cho HostGgroup.

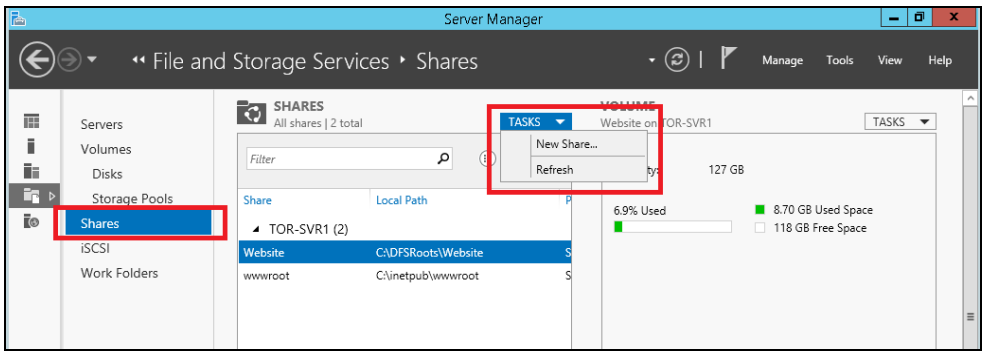
❖ **Thực hiện:**

### Bước 1: Cấu hình Library Server và Library Share.

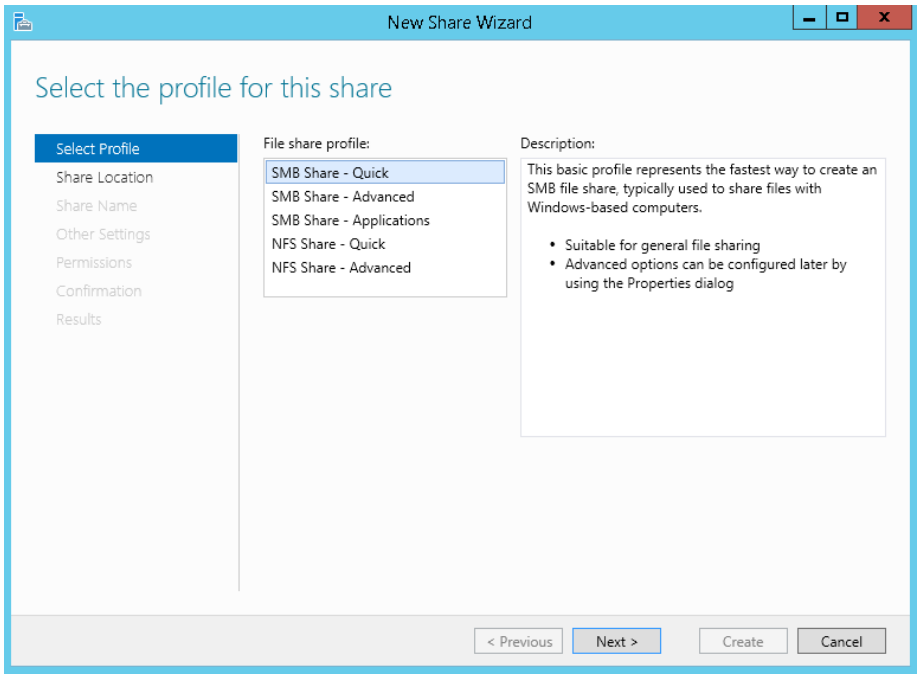
1. Qua máy **TOR-SVR1**, trong **Server Manager**, chọn **File and Storage Services**



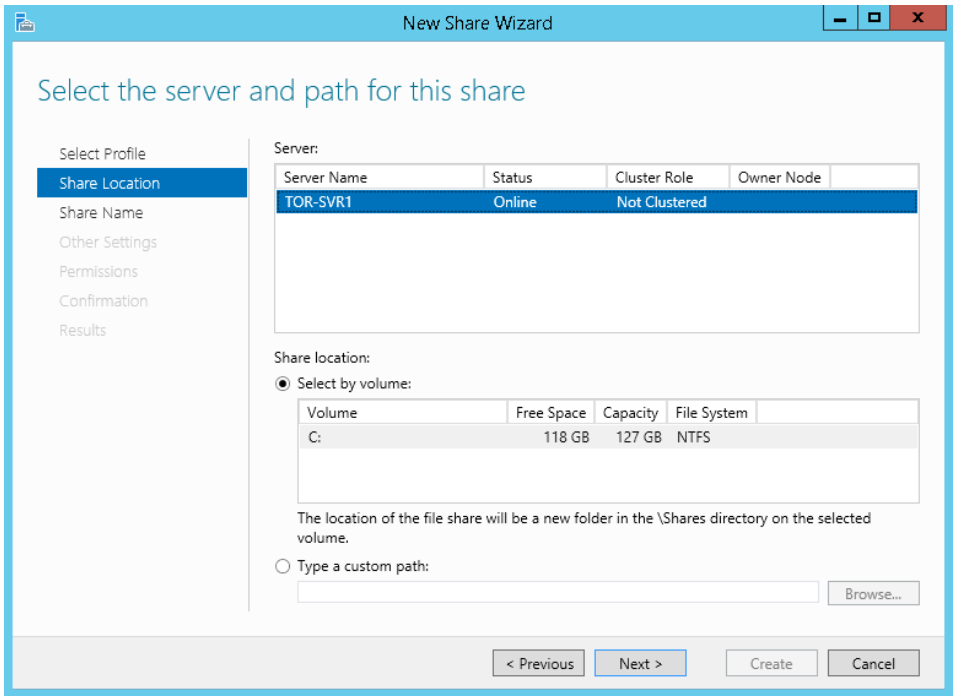

2. Chọn **Shares**, trong ô **Shares**, bung **Tasks**, và chọn **New Share**.



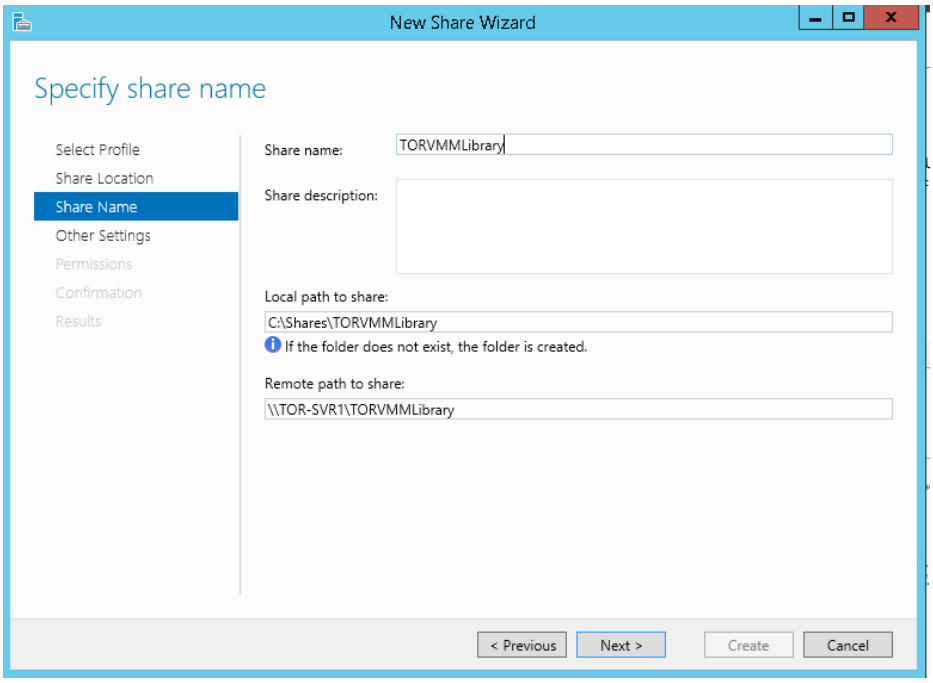
3. Cửa sổ **Select Profile**, chọn **SMB Share – Quick**, chọn **Next**



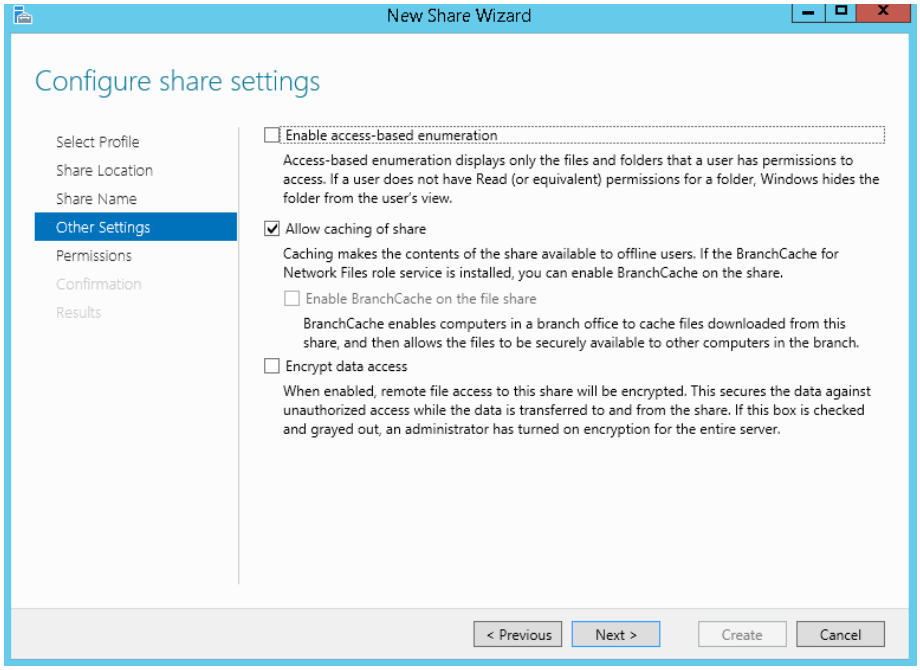

4. Cửa sổ **Share Location**, chọn **Next**.



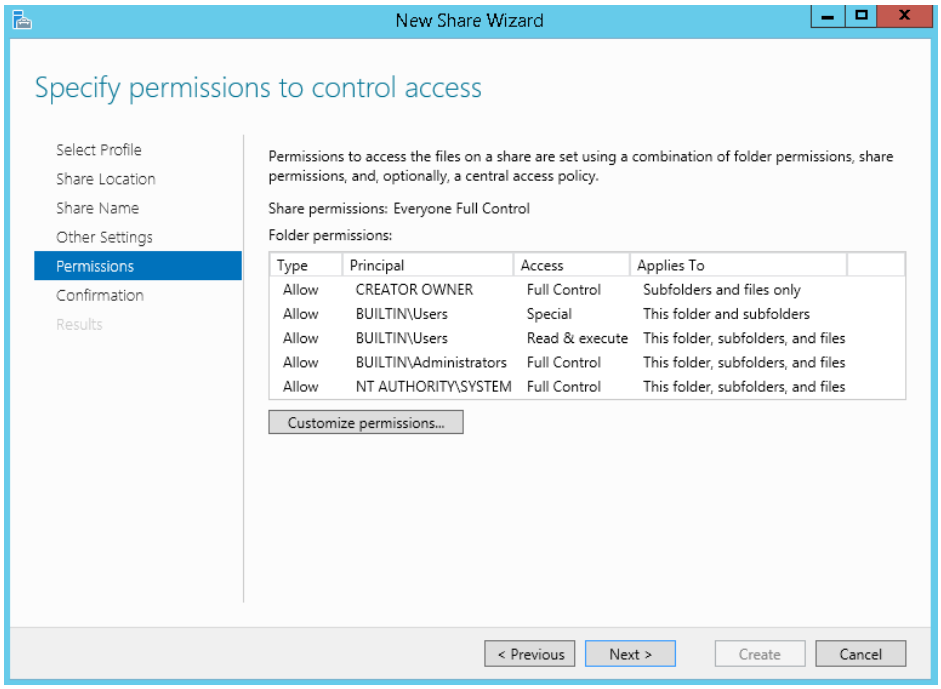
5. Cửa sổ **Share Name**, trong ô **Share name**, nhập **TORVMMLibrary**, và chọn **Next**.



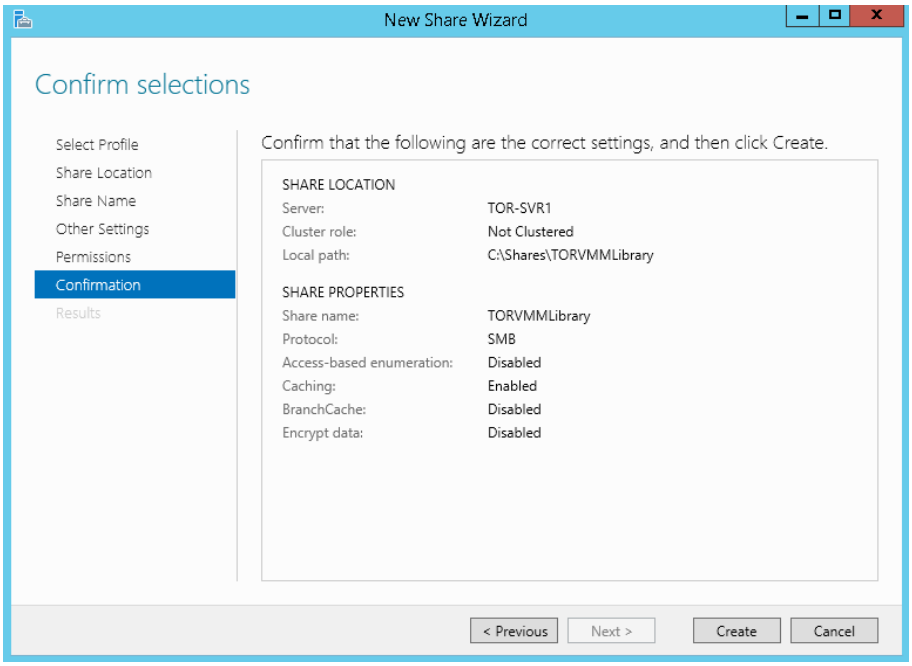

6. Cửa sổ **Other Settings**, chọn **Next**.



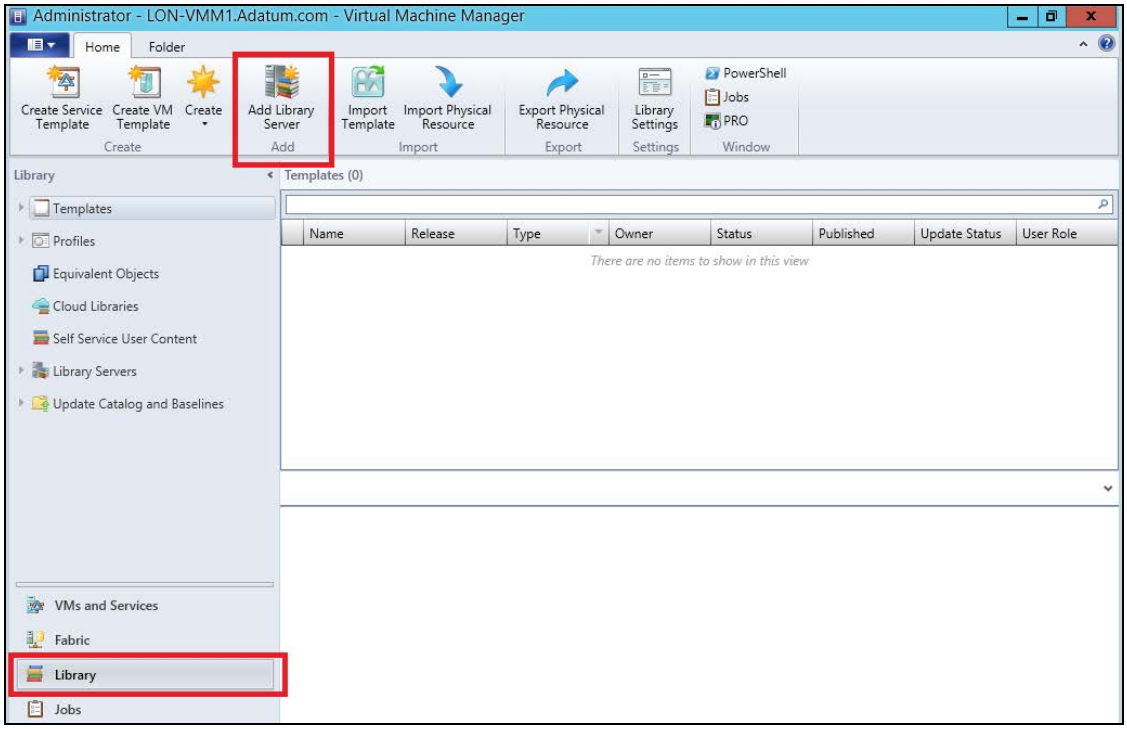
7. Cửa sổ **Permissions**, chọn **Next**.



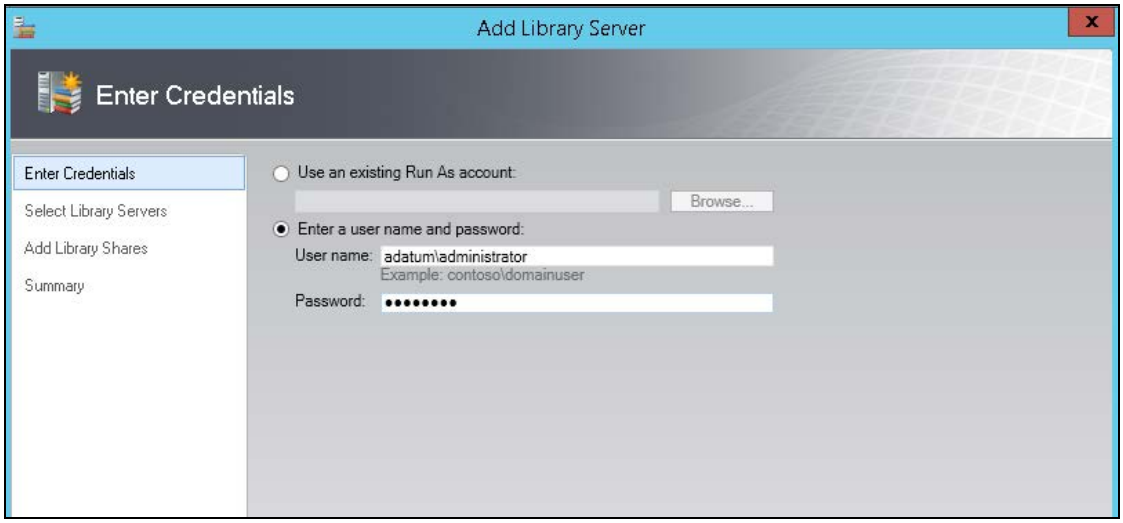

8. Cửa sổ **Confirmation**, chọn **Create**, sau khi tạo thành công, chọn **Close**.



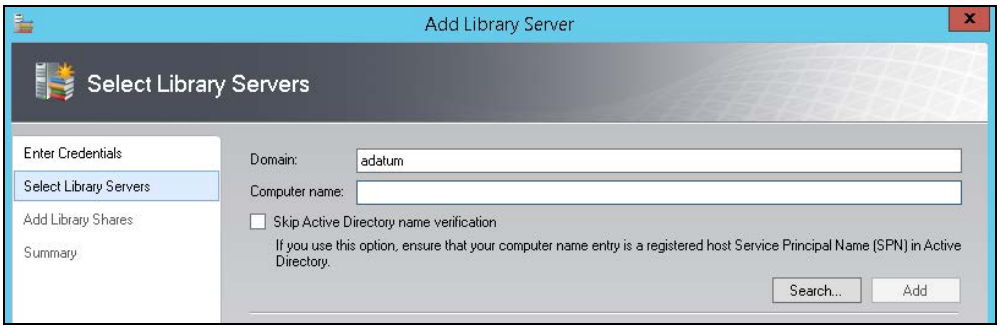
9. Qua máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **Library**, chọn **Add Library Server**.



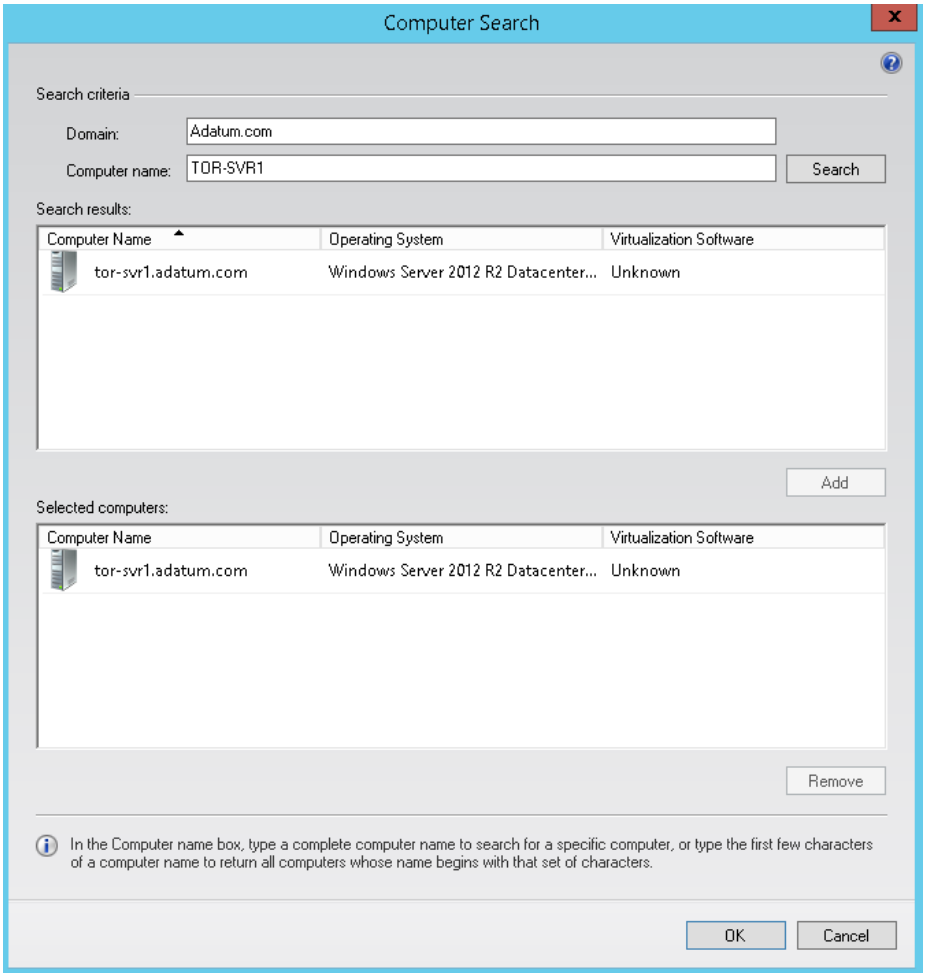

10. Cửa sổ **Enter Credentials**, chọn **Enter a user name and password**, trong ô **User name**, nhập **Adatum\Administrator,** trong ô **Password**, nhập **Pa$$w0rd,** chọn **Next**.



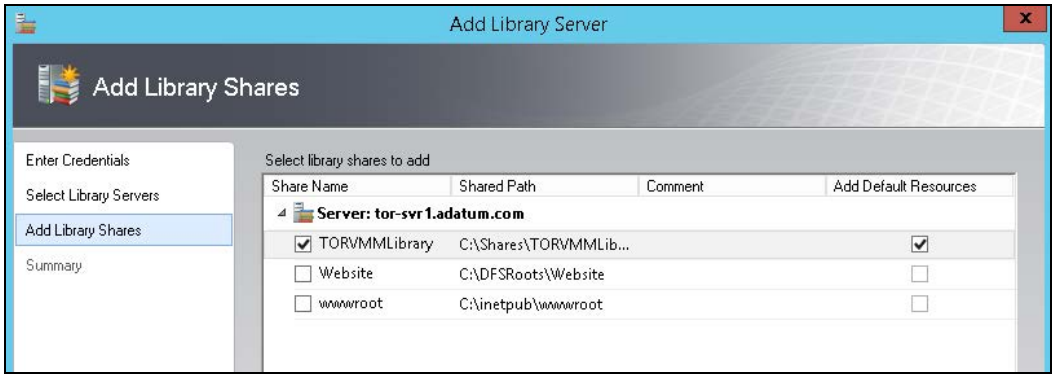
11. Cửa sổ **Select Library Servers**, chọn **Search**.



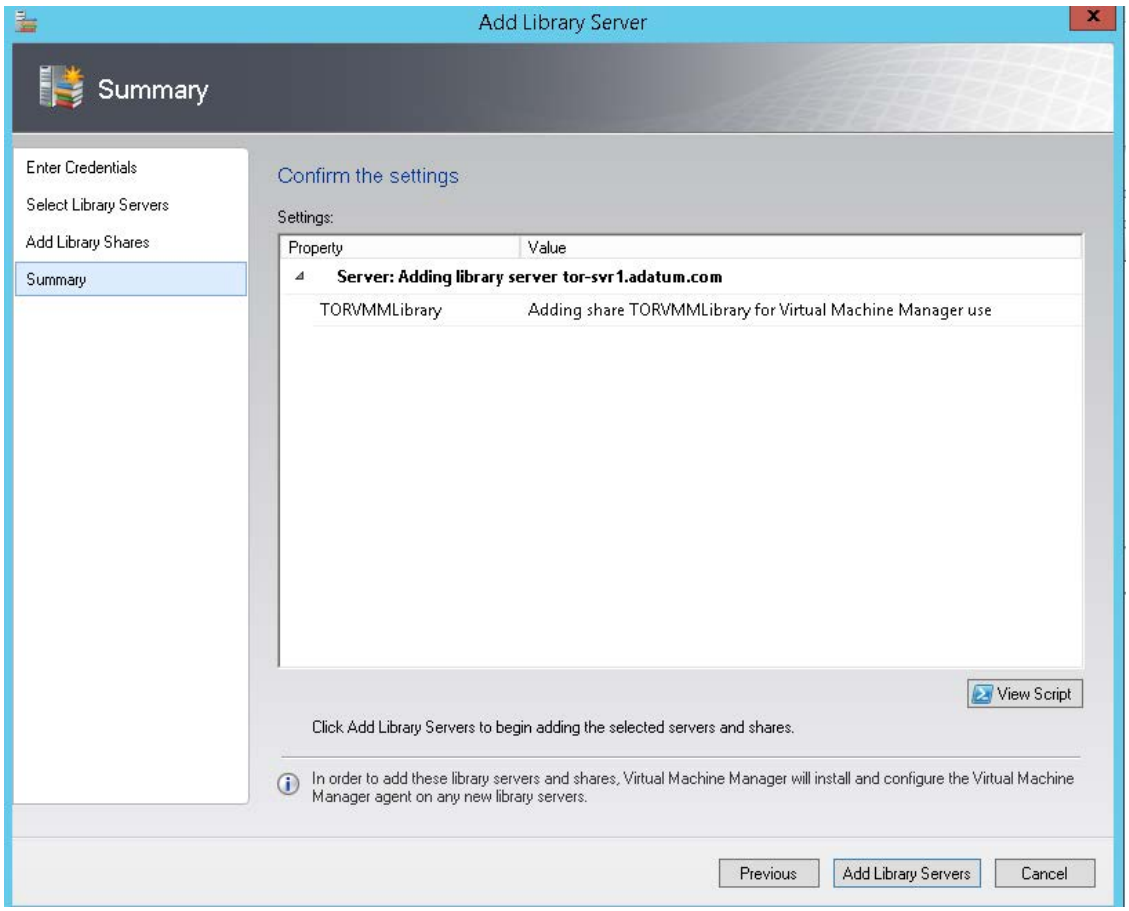

12. Cửa sổ **Computer Search**, trong ô **Computer name**, nhập **TOR-SVR1**, và chọn **Search**. Trong ô **Search results**, chọn **tor-svr1.adatum.com**, chọn **Add**, chọn **OK**, và chọn **Next**.



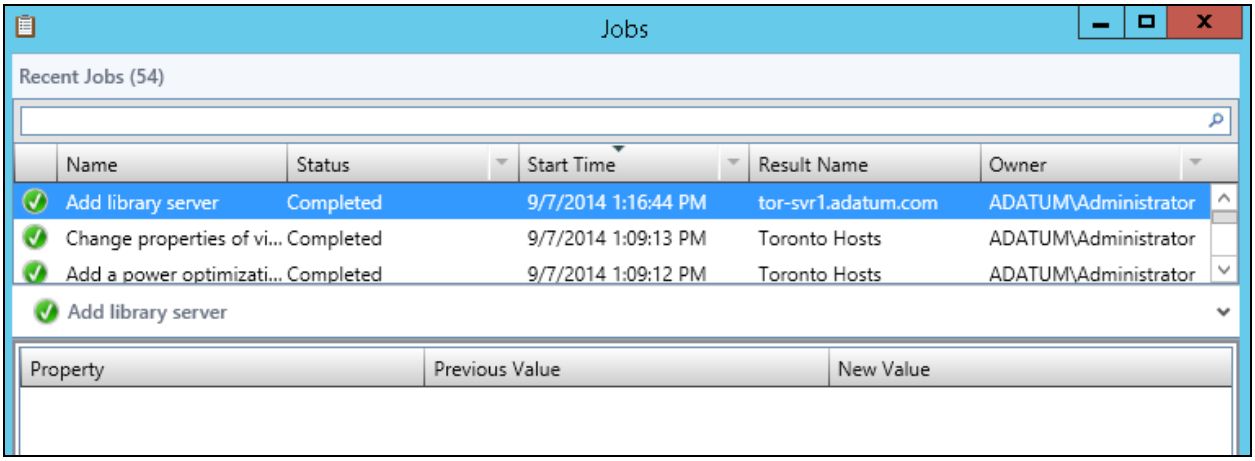
13. Cửa sổ **Add Library Shares**, đánh dấu chọn **TORVMMLibrary**, và đánh dấu chọn **Add Default Resources**, chọn **Next.**




14. Cửa sổ **Summary**, chọn **Add Library Servers**.



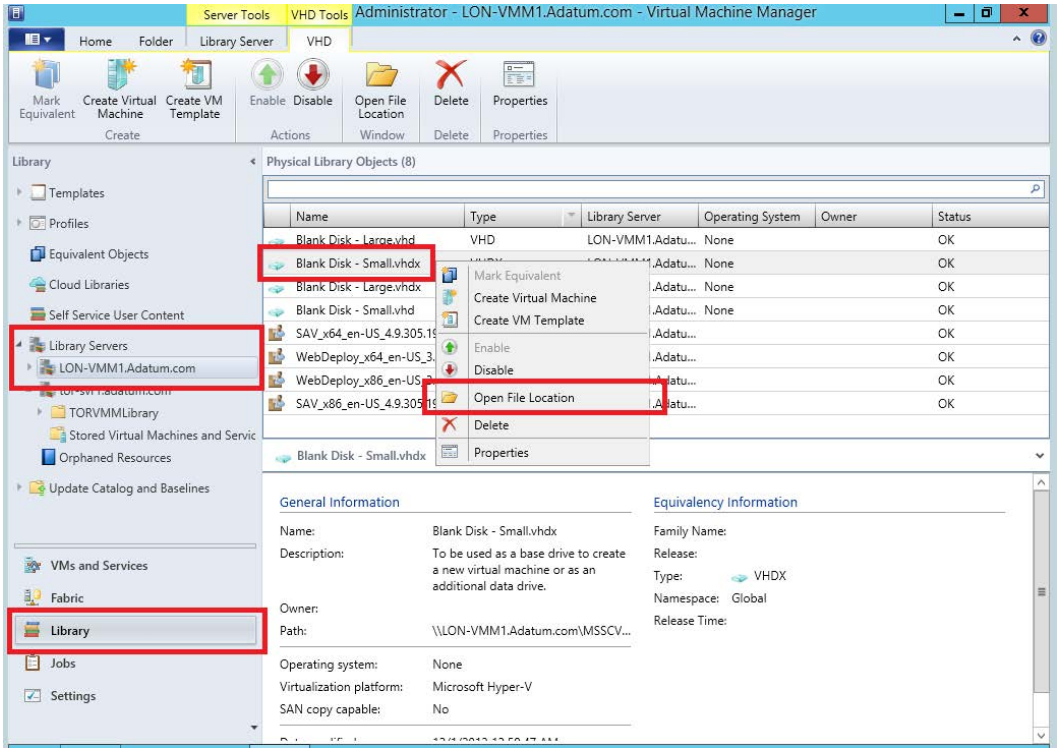
15. Trong cửa sổ **Jobs**, kiểm tra Add library server thành công, và tắt cửa sổ **Jobs.**



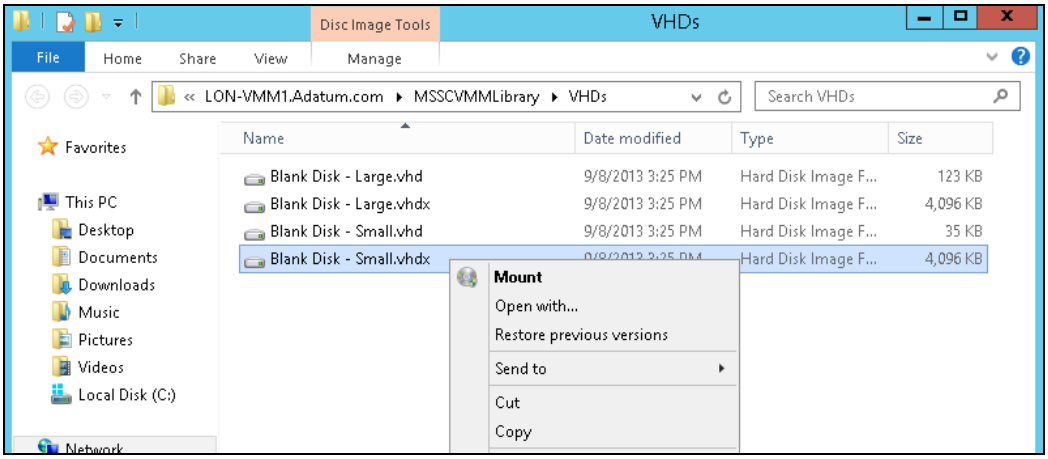

**Bước 2:Sao chép các file cần thiết đến trung tâm dữ liệu của văn phòng chi nhánh.**

1. Trên máy **LON-VMM1**.

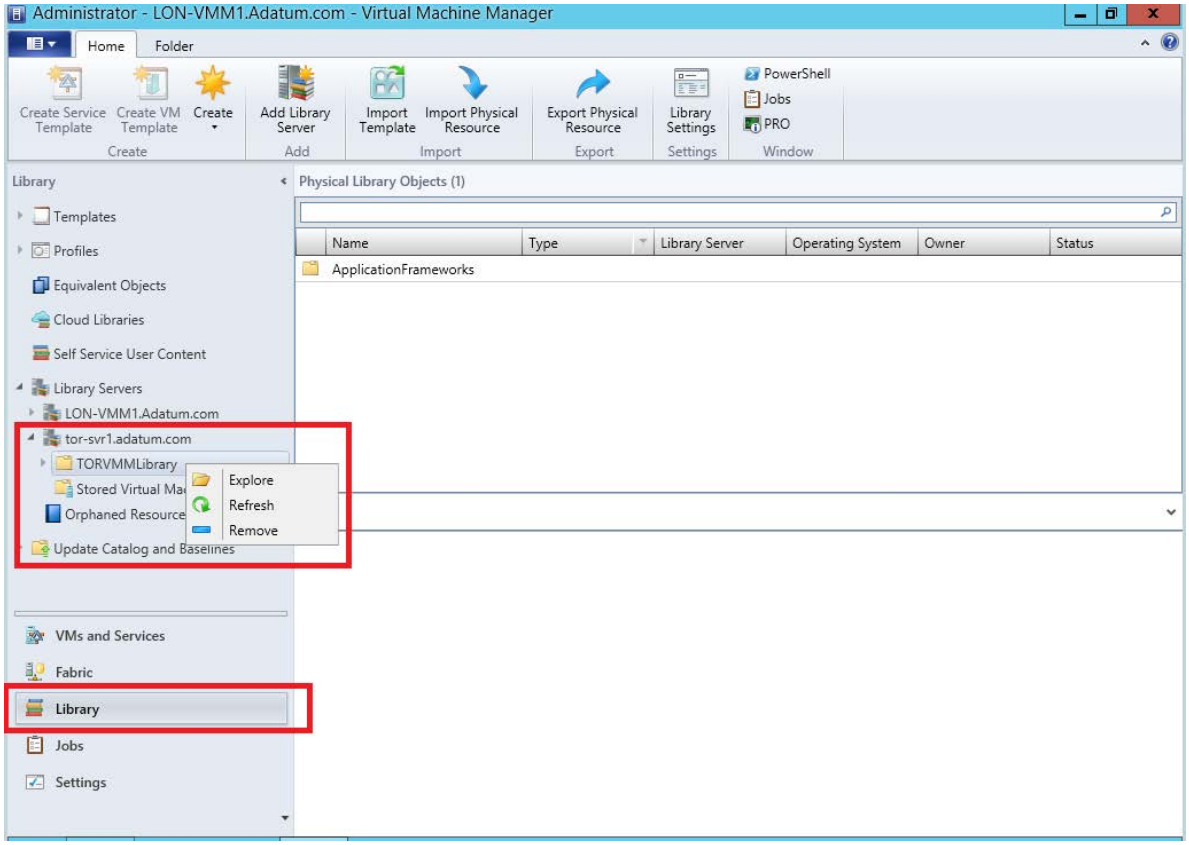
2. Trong cửa sổ **Virtual Machine Manager**, chọn **Library**, bung **Library Servers**, chọn **LON-VMM1.Adatum.com**, chuột phải **Blank Disk – Small.vhdx**, chọn **Open File Location**.



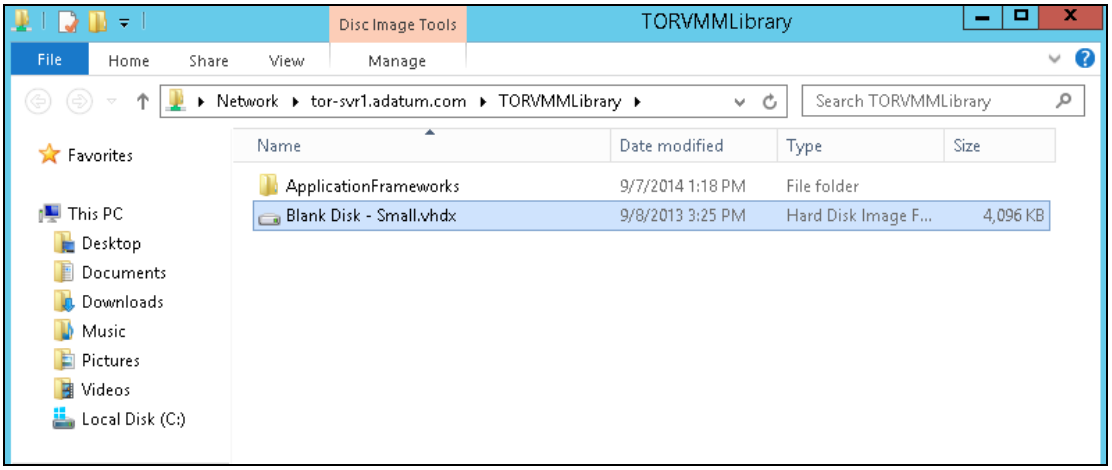
3. Cửa sổ **VHDs**, chuột phải **Blank Disk – Small.vhdx**, chọn **Copy**. Tắt cửa sổ VHDs



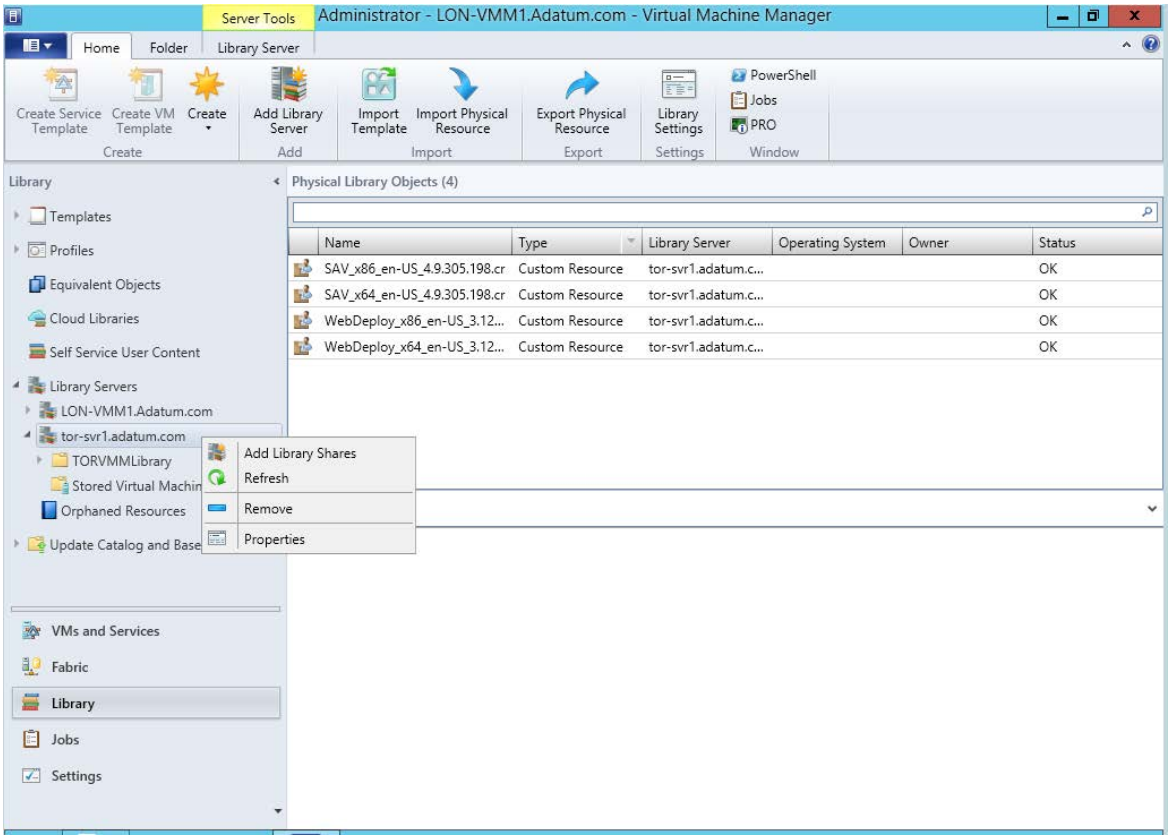

4. Bung **Library Servers**, bung **tor-svr1.adatum.com**, chuột phải **TORVMMLibrary**, chọn **Explore**.



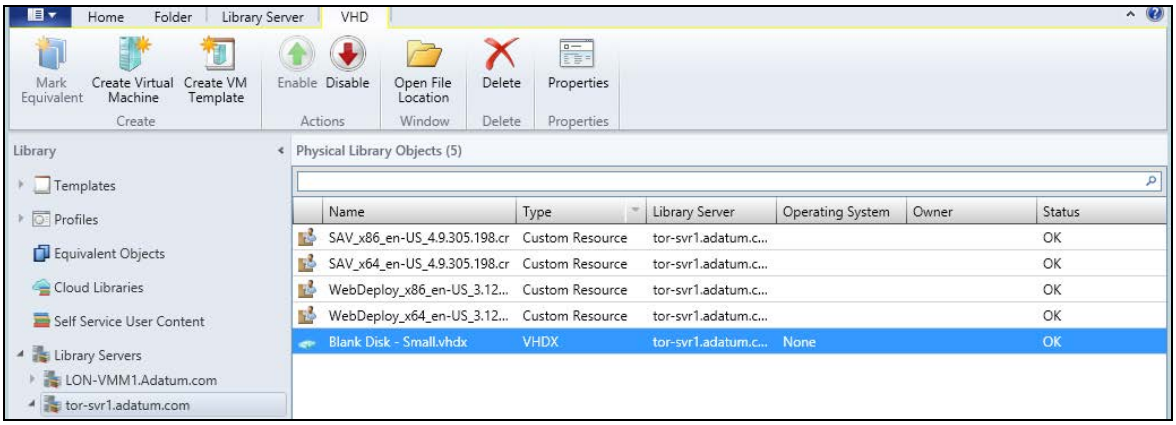
5. Trong cửa sổ **TORVMMLibrary**, chuột phải lên khoảng trắng, chọn **Paste**. Tắt cửa sổ **TORVMMLibrary**. Kiểm tra chép file **Blank Disk – Small.vhdx** thành công.




6. Cửa sổ **Virtual Machine Manager,** chuột phải **TOR-SVR1.adatum.com**, chọn **Refresh**.



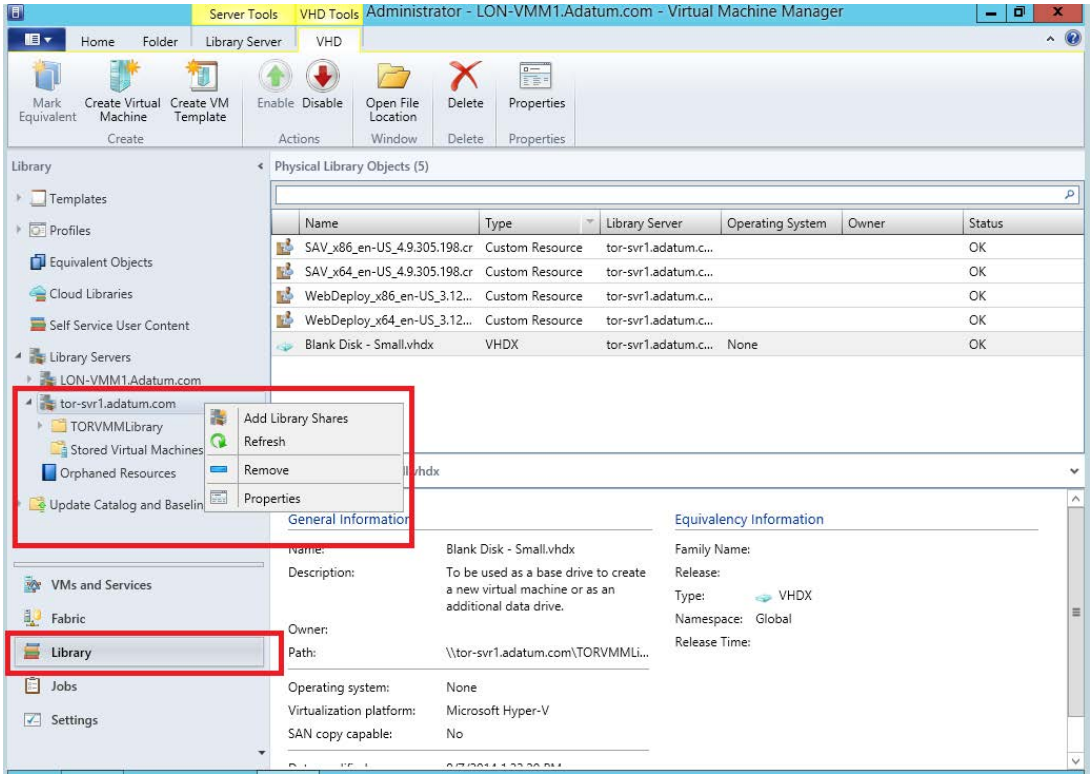
7. Kiểm tra có file **Blank Disk - small.vhdx**.



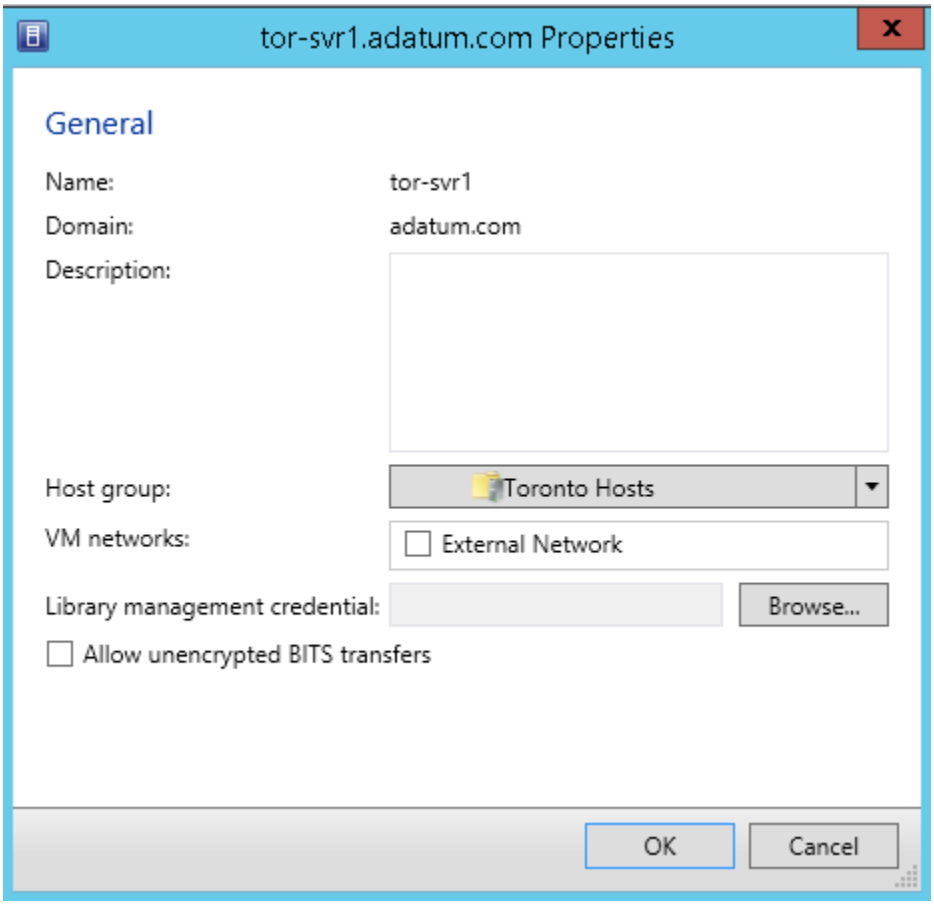

## Bước 3:Gán Library cho Host Group.

1. Trên máy **LON-VMM1**.

2. Trong cửa sổ **Virtual Machine Manager**, chọn **Library,** bung **Library Servers**, chuột phải **tor-svr1.adatum.com**, chọn **Properties**.



3. Hộp thoại **tor-svr1.adatum.com Properties,** bung ô **Host group**, chọn **Toronto Hosts**, chọn **OK**.




4. Tắt cửa sổ **Virtual Machine Manager**.

**Kết quả: Sau khi hoàn thành bài tập này, bạn cấu hình một VMM Library Server, sao chép file vhdx vào trung tâm dữ liệu của văn phòng chi nhánh, và gán Library cho một Host Group thành công.**

**VI. Chuẩn bị cho bài tiếp theo:**

Không phục hồi các máy ảo, vì bạn sẽ sử dụng các máy ảo này trong các bài tiếp theo.

# Bài 2: Xây dựng cơ sở hạ tầng và giải pháp lưu trữ cho hệ thống ảo hóa

**I. Mục tiêu:**

- Lập kế hoạch xây dựng cơ sở hạ tầng và giải pháp lưu trữ.
- Triển khai giải pháp lưu trữ cho hệ thống ảo hóa.
- Triển khai cơ sở hạ tầng cho hệ thống ảo hóa.

**II. Kịch bản:**

Sau khi thiết kế và triển khai các Hyper-V Hosts và VMM, bước tiếp theo là lên kế hoạch xây dựng cơ sở hạ tầng và giải pháp lưu trữ cho hệ thống ảo hóa.

Bởi vì nhiều máy ảo sẽ được lưu trữ cùng 1 nơi và sử dụng chung cơ sở hạ tầng mạng, nên vấn đề quan trọng là phải có khả năng sẵn sàng cao.

Các quản trị viên ở London thiết kế cơ sở hạ tầng và giải pháp lưu trữ bằng cách sử dụng Fibre Channel SAN. Các quản trị viên ở London chịu trách nhiệm thiết kế cấu hình mạng. Bạn phải chịu trách nhiệm thiết kế cơ sở hạ tầng và giải pháp lưu trữ cho việc triển khai ảo hóa ở Toronto.

**III. Yêu cầu tổng quan:**

Quy hoạch một chiến lược lưu trữ để hỗ trợ các mục tiêu sau đây:

- Cung cấp nơi lưu trữ các máy ảo.
- Hỗ trợ khả năng sẵn sàng cao nếu có thể.
- Xác định rủi ro và tắc nghẽn mạng.

**IV. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-HOST2**<br>**20414C-LON-DC1**<br>**20414C-LON-VMM1**<br>**20414C-LON-SVR1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

Bài thực hành gồm 2 máy thật, 1 máy khởi động **20414C-LON-HOST1** và 1 máy khởi động **20414C-LON-HOST2**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
2. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
3. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
4. Thực hiên từ bước 1 đến 3 cho máy ảo **20414C-LON-VMM1.**
5. Không khởi động máy **20414C-LON-SVR1** cho tới khi có yêu cầu.
6. Logon vào máy **20414C-LON-HOST2** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**

**VI. Thực hành:**

*Thời gian thực hành: 60 phút*

## Bài tập 1: Triển khai giải pháp lưu trữ cho hệ thống ảo hóa.

A. Datum đã quyết định lưu trữ máy ảo tại trung tâm dữ liệu ở Toronto bằng cách triển khai iSCSI Storage. Bạn phải cấu hình các iSCSI Targets và iSCSI Initiators để đáp ứng yêu cầu này.

❖ **Bài thực hành bao gồm các bước:**

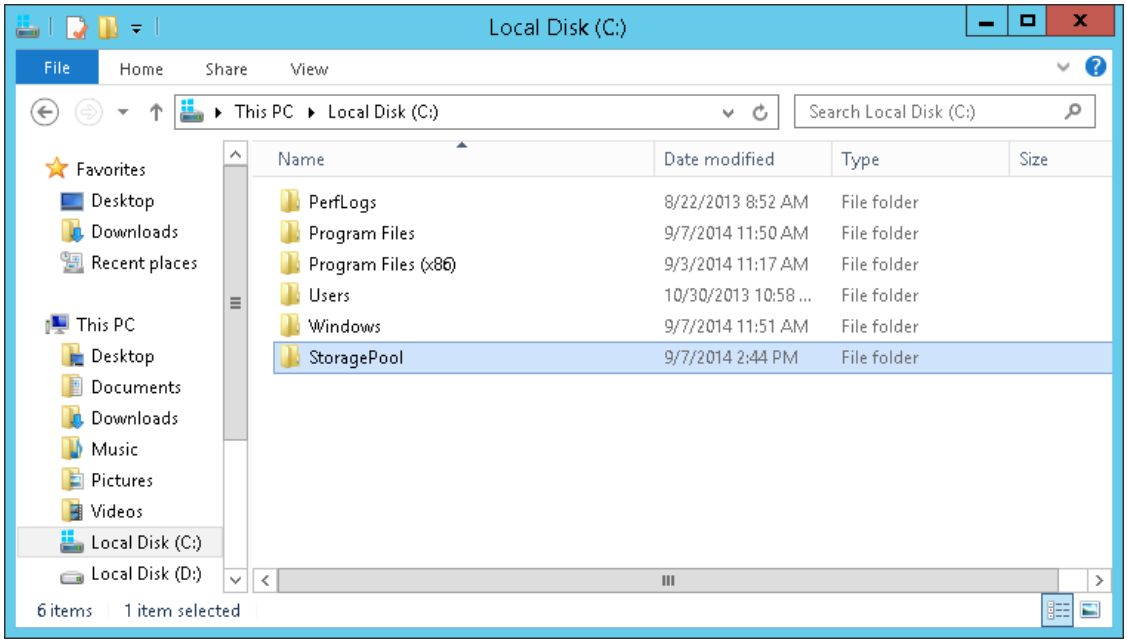
1. Cấu hình iSCSI Target.
2. Cấu hình iSCSI Initiator.

❖ **Thực hiện:**

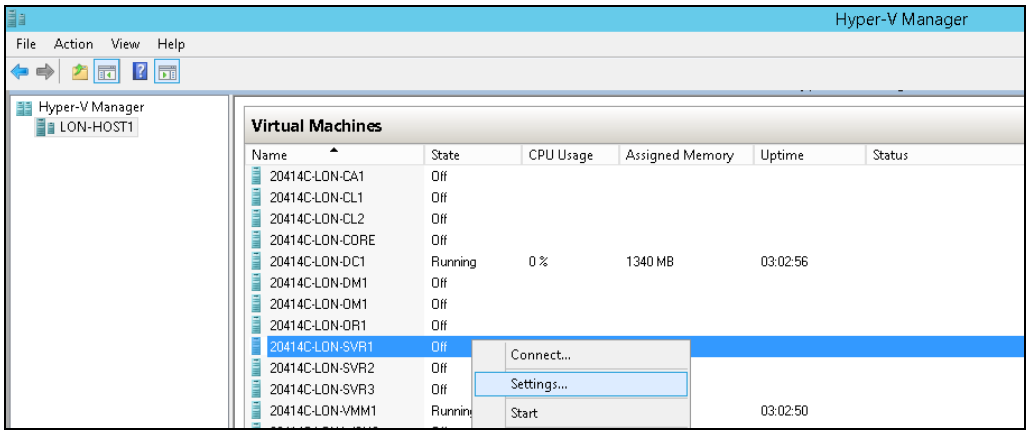
### Bước 1. Cấu hình iSCSI Target.

➢ **Tạo Virtual Disks cho máy LON-SVR1**

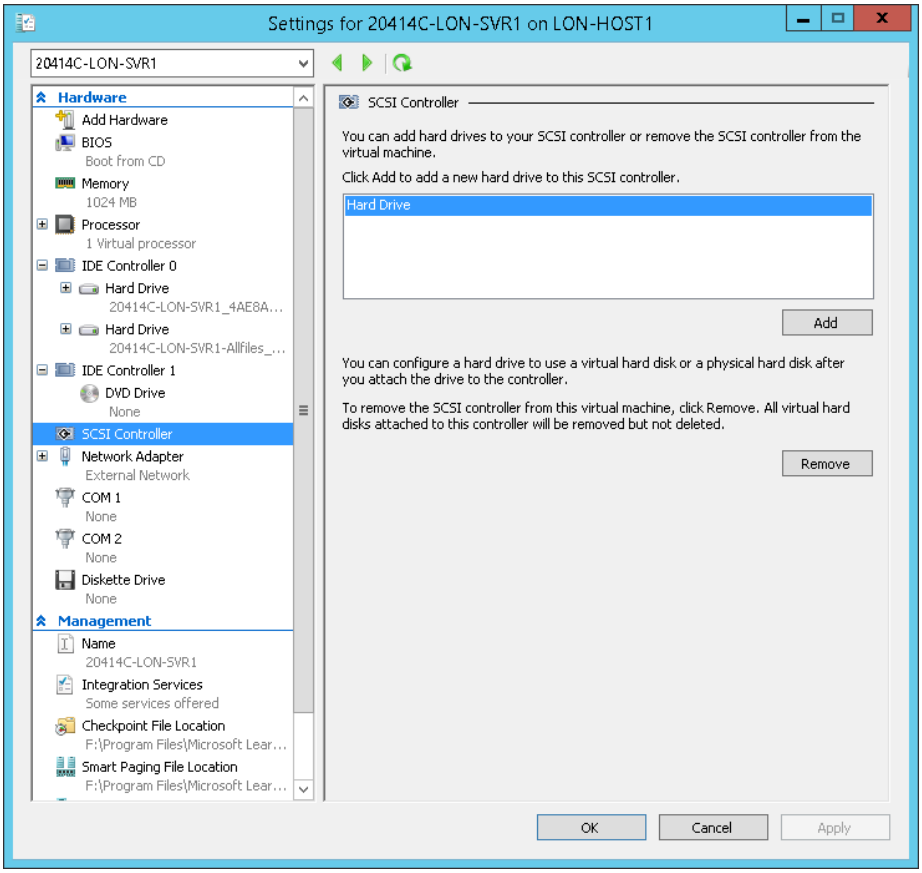
1. Trên máy **LON-HOST1** (Máy thật).
2. Mở **File Explorer**, vào ổ đĩa **Local Disk (C:)**, tạo folder mới đặt tên **StoragePool**.



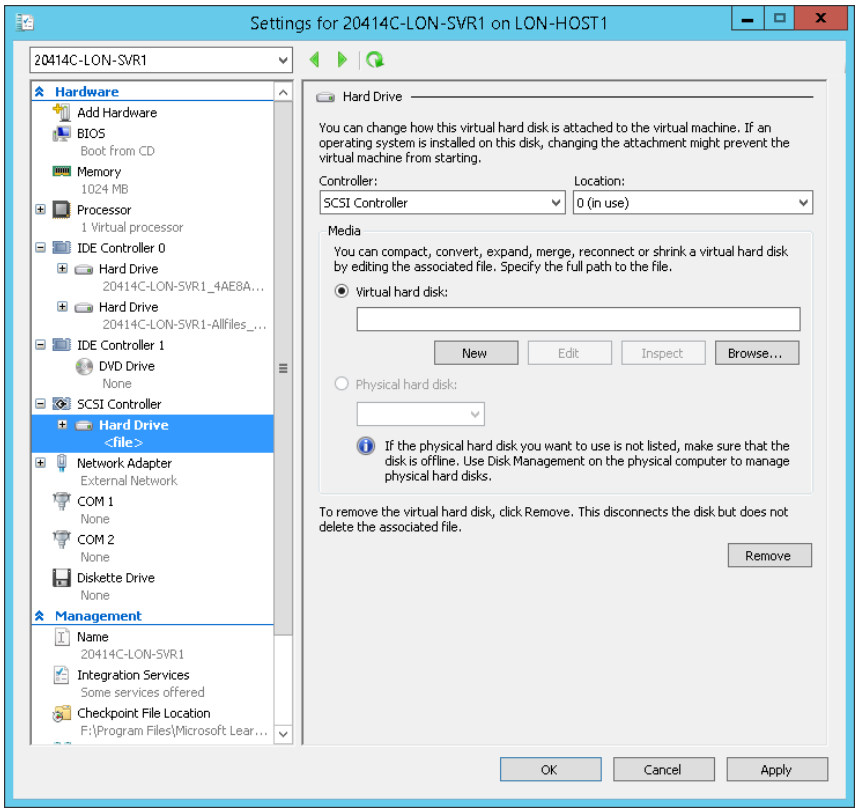
3. Mở công cụ **Hyper-V Manager**, chuột phải máy ảo **20414C-LON-SVR1**, chọn **Settings**.



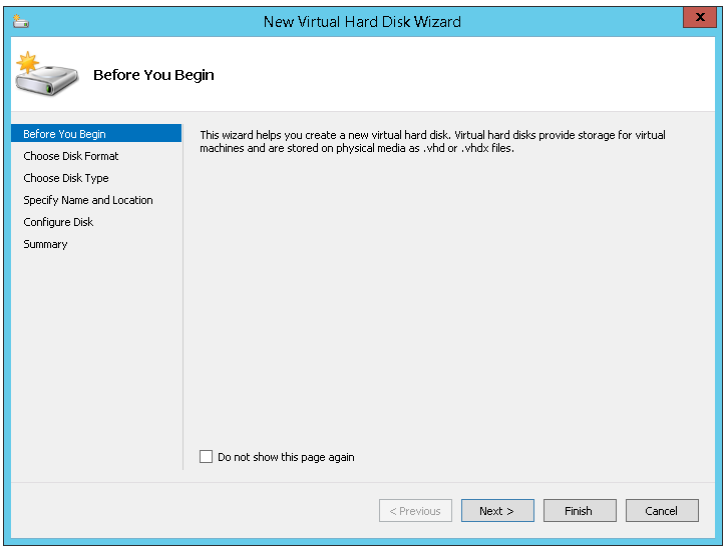

4. Cửa sổ **Settings for 20414C-LON-SVR1 on LON-HOST1**, chọn **SCSI Controller**, chọn **Hard Drive**, và chọn **Add**.



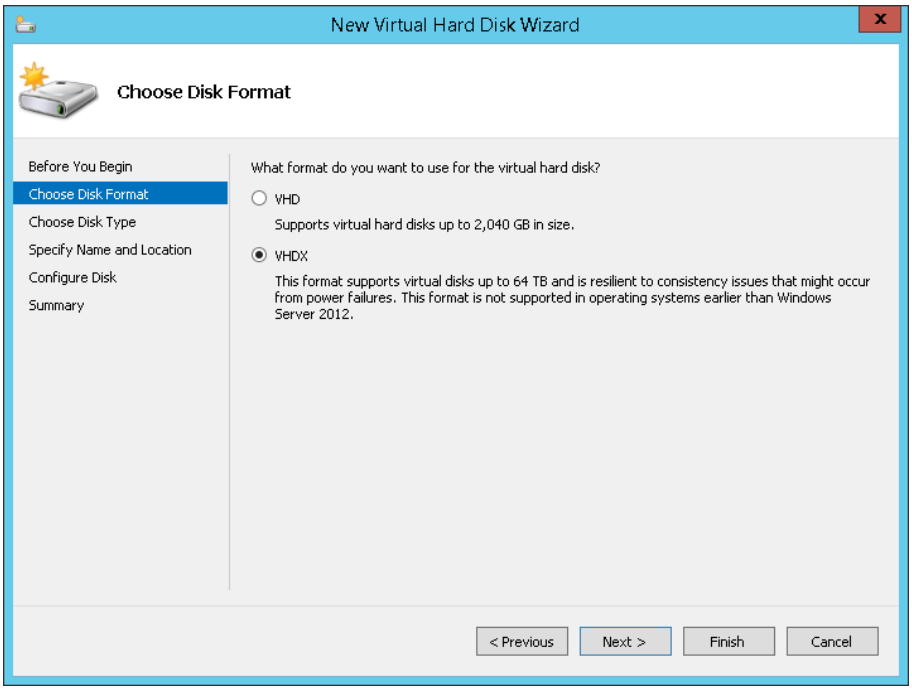
5. Trong phần **Media,** chọn **New**.



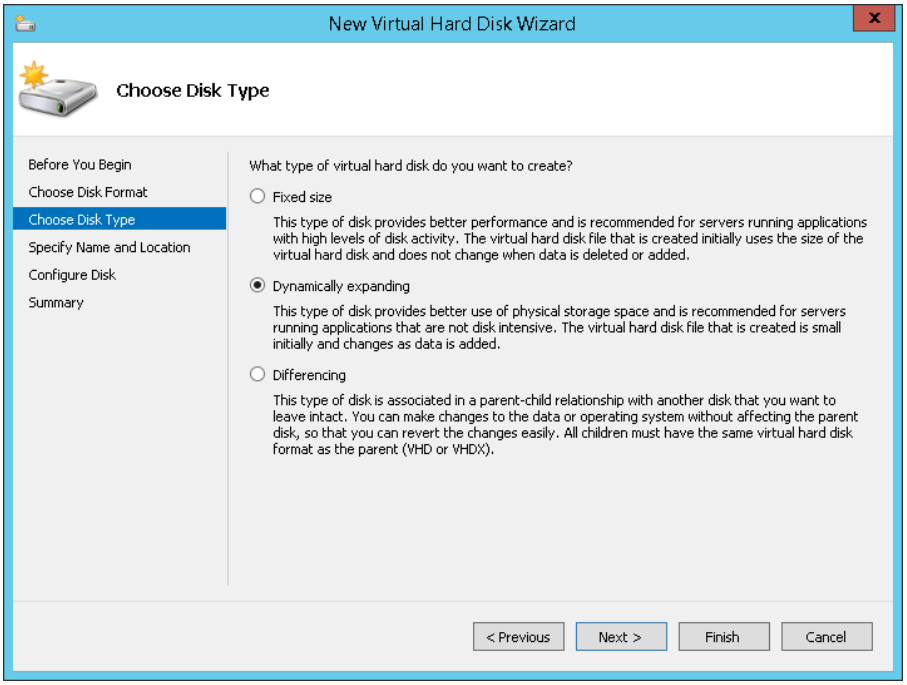

6. Cửa sổ **Before You Begin**, chọn **Next**.



7. Cửa sổ **Choose Disk Format**, chọn **VHDX**, chọn **Next**.

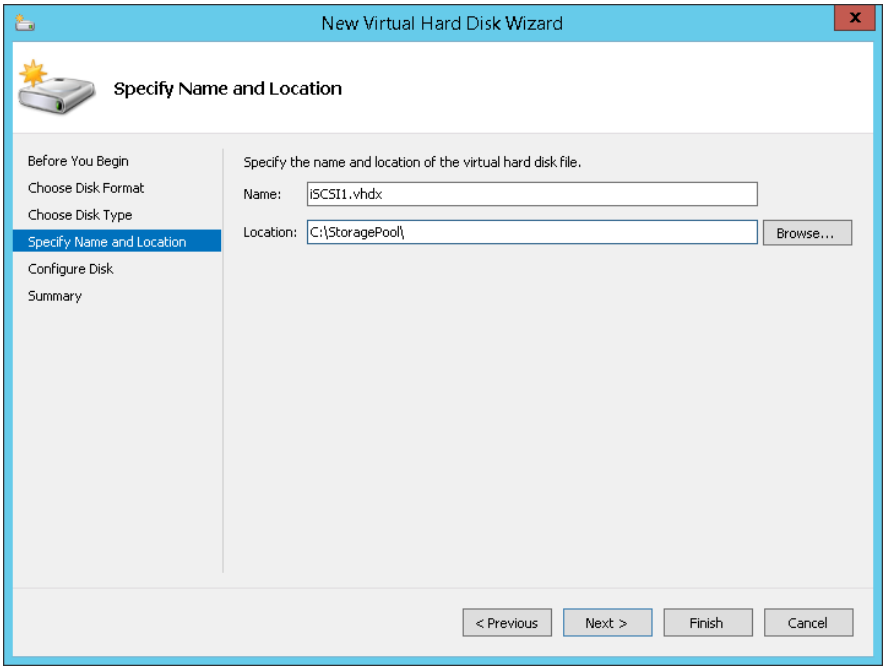



8. Cửa sổ **Choose Disk Type**, chọn **Dynamically expanding**, chọn **Next**.

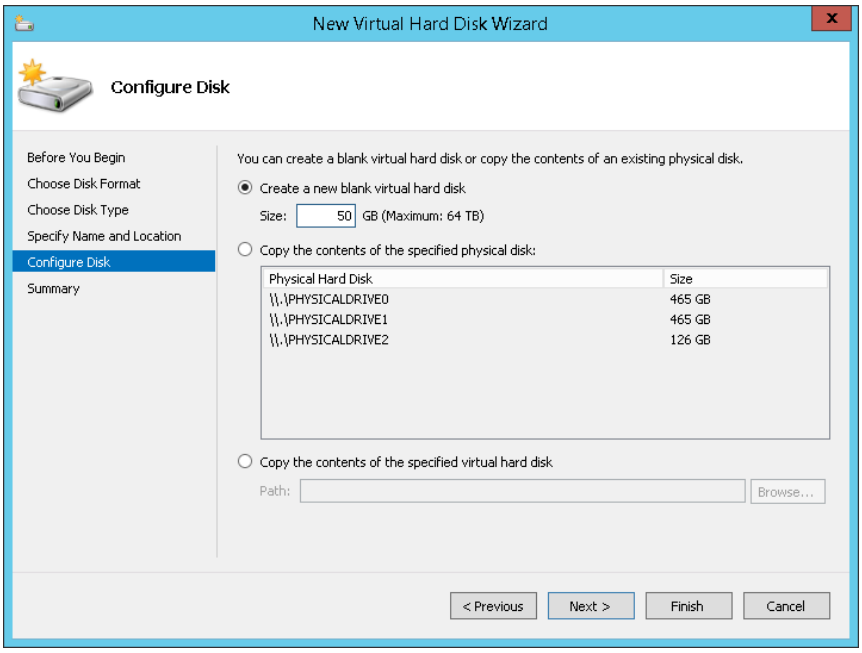


9. Cửa sổ **Specify Name and Location**, nhập **iSCSI1.vhdx**, chọn **Browse**.

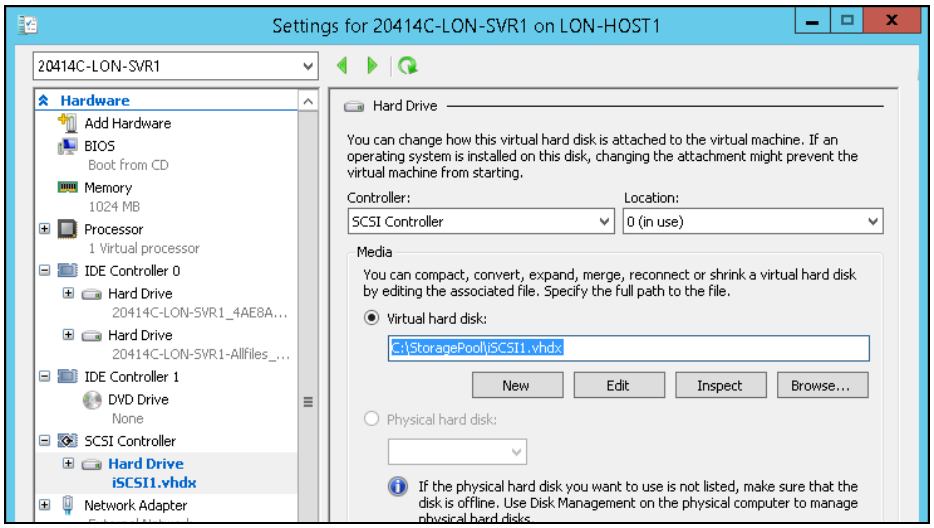
10. Trỏ vào đường dẫn **C:\StoragePool**, chọn **Select Folder**, chọn **Next**.




11. Cửa sổ **Configure Disk,** nhập **50** vào ô **Size**, và chọn **Finish**.

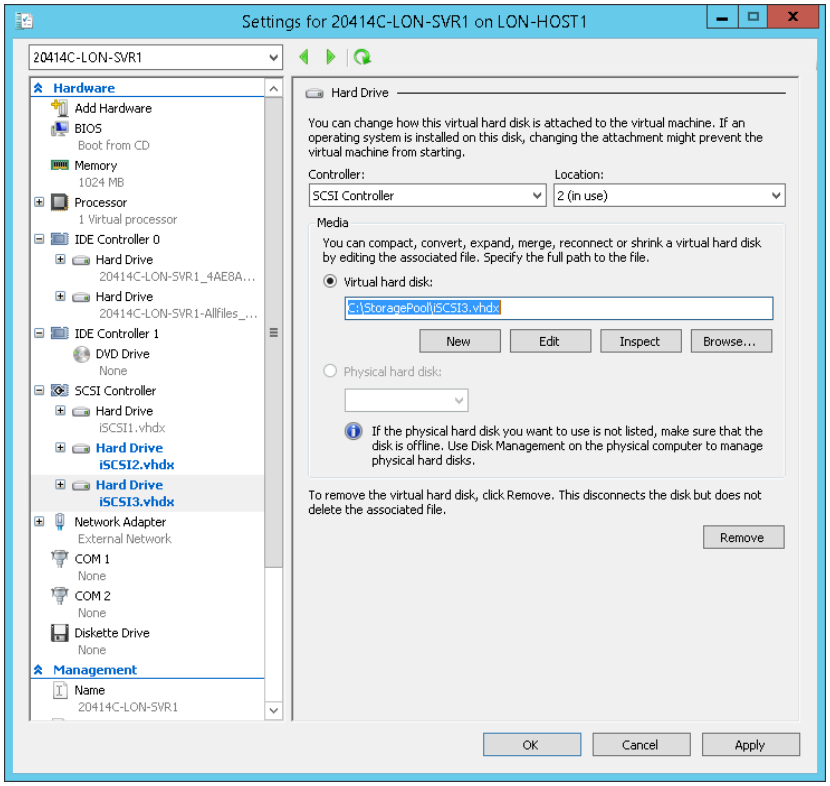


12. Cửa sổ **Setting**, chọn **Apply**.

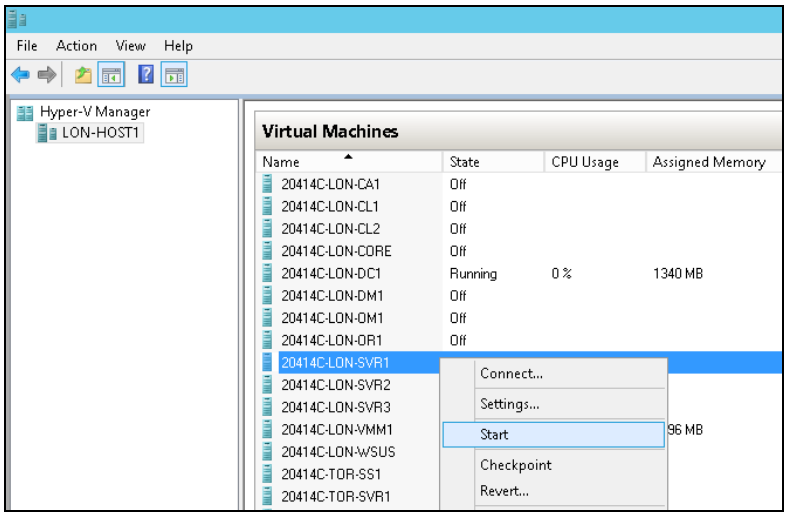



13. Lặp lại từ bước 4 to 12 để tạo thêm 2 virtual disk tên **iSCSI2.vhdx** và **iSCSI3.vhdx**.

14. Chọn **OK** để tắt cửa sổ **Settings for 20414C-LON-SVR1 on LON-HOST1**.



15. Trong cửa sổ **Hyper-V Manager**, chuột phải máy ảo **20414C-LON-SVR1,** chọn **Start**, và chọn **Connect**.

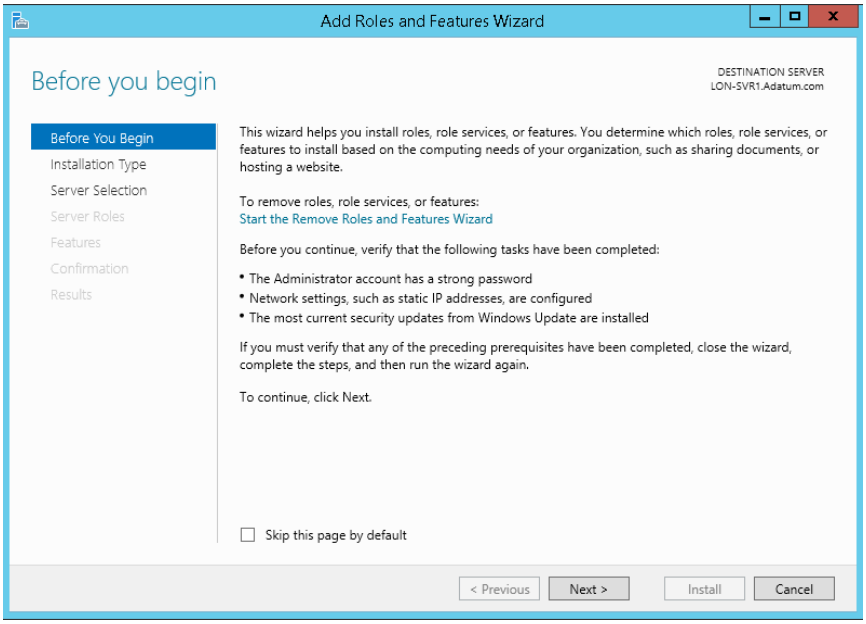



16. Sign in vào máy **LON-SVR1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

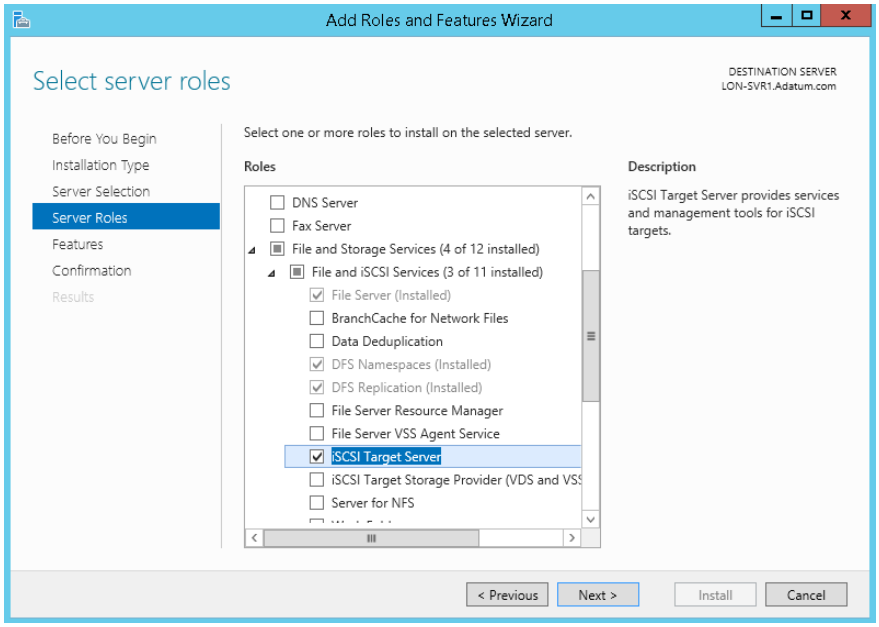
➢ **Cài đặt iSCSI Target Server Role**

1. Qua máy **LON-SVR1**, trong cửa sổ **Server Manager**, chọn **Add roles and features**.

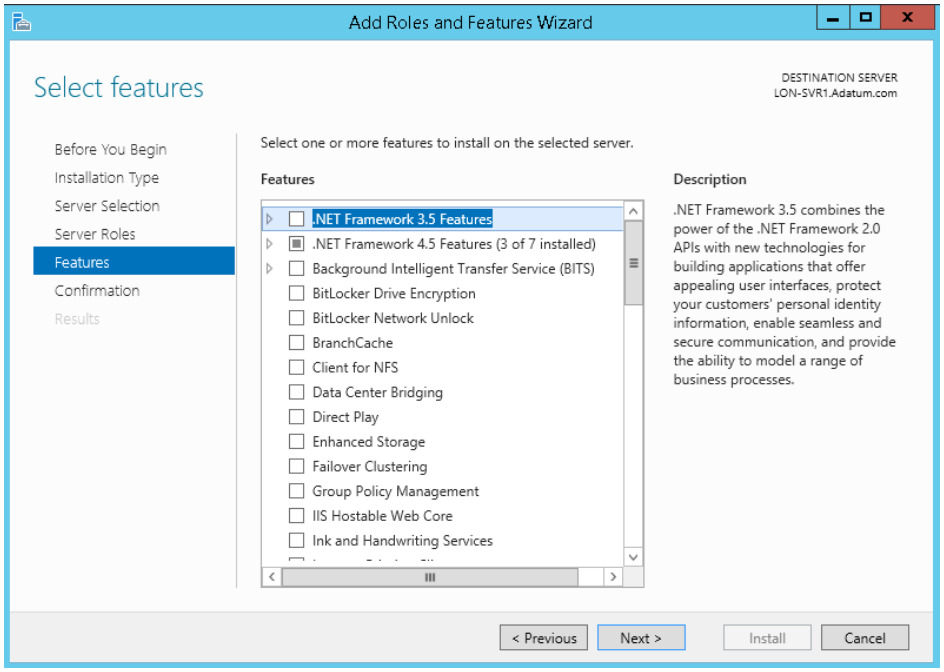
2. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



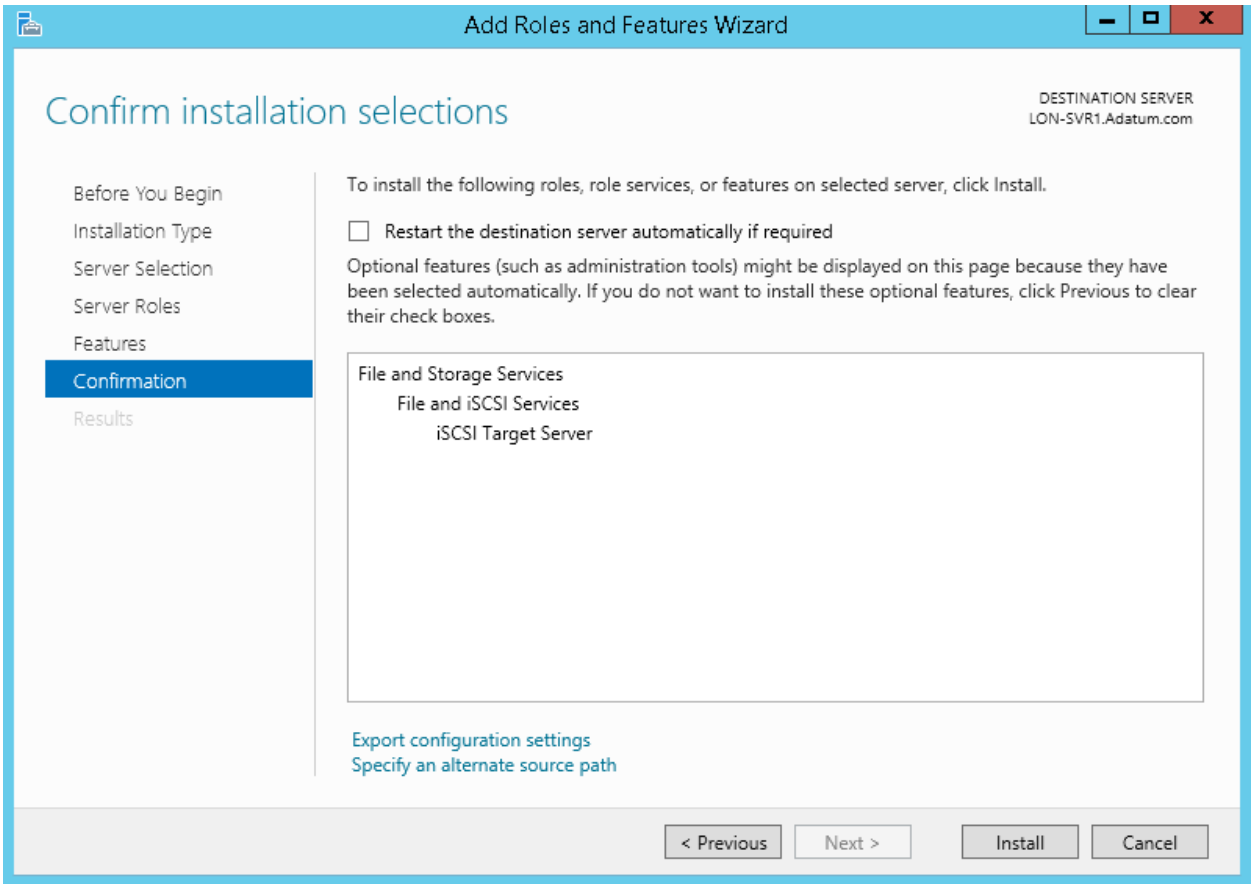
3. Cửa sổ **Select server roles**, bung **File and Storage Services (Installed)**, bung **File and iSCSI Services**, đánh dấu chọn **iSCSI Target Server**, và chọn **Next**.




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



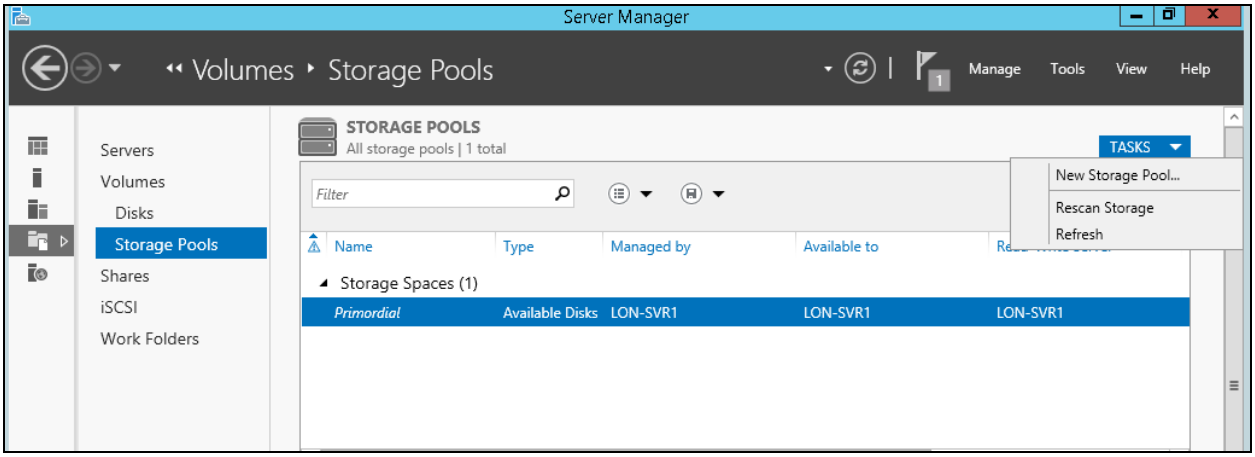
5. Cửa sổ **Confirm installation selections**, chọn **Install**.



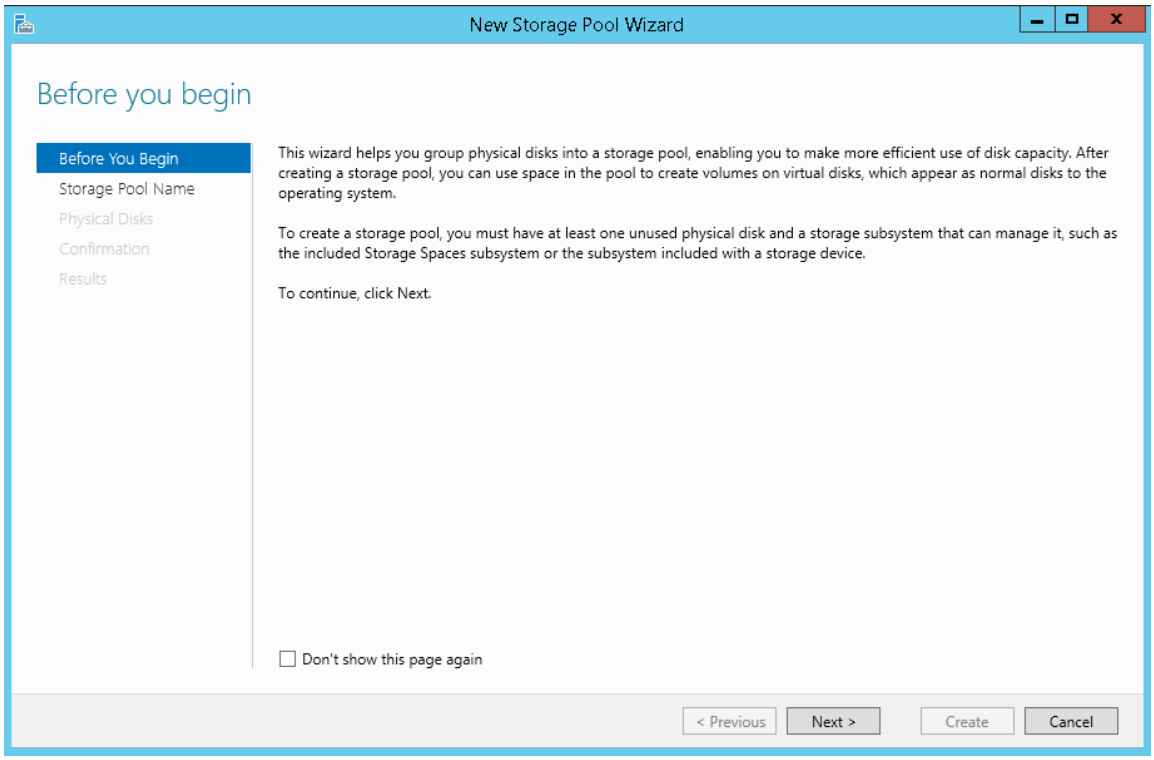

6. Sau khi cài đặt thành công, chọn **Close**.

## ➢ Tạo Storage Pool

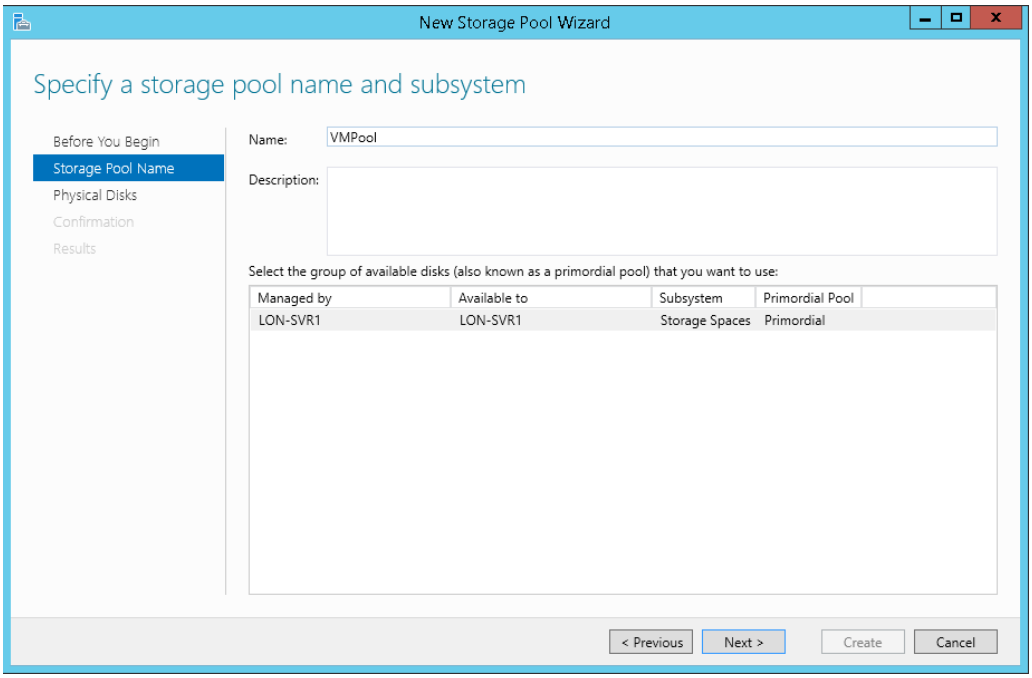
1. Trên máy **LON-SVR1,** trong **Server Manager**, chọn **File and Storage Services**, chọn **Storage Pools**. Trong phần **STORAGE POOL**, bung **TASKS**, chọn **New Storage Pool**.



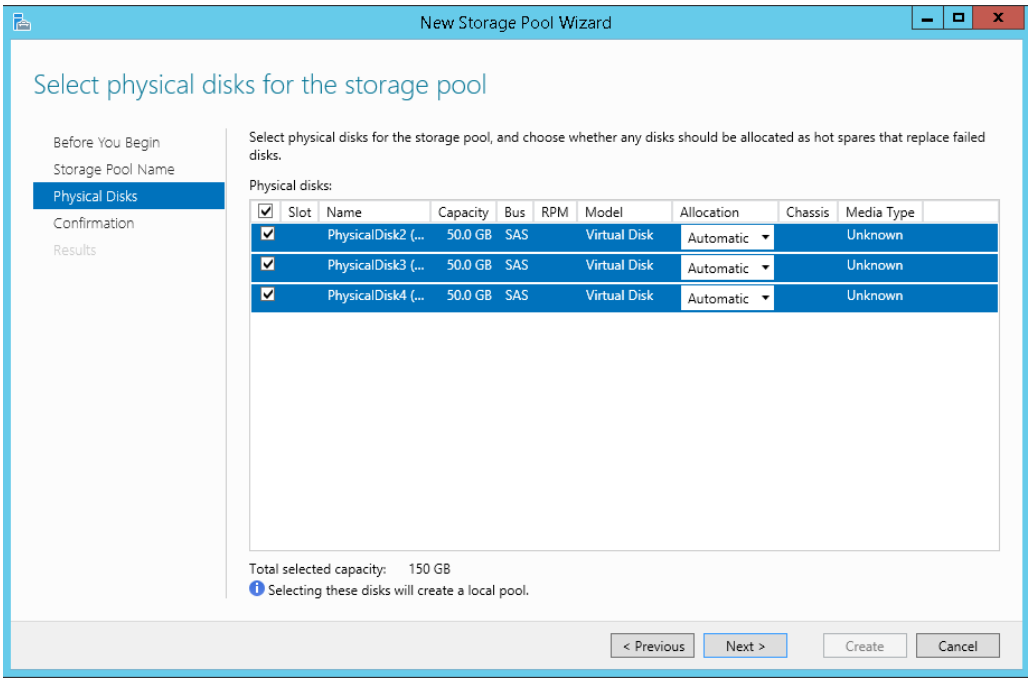

2. Cửa sổ **Before You Begin**, chọn **Next**.



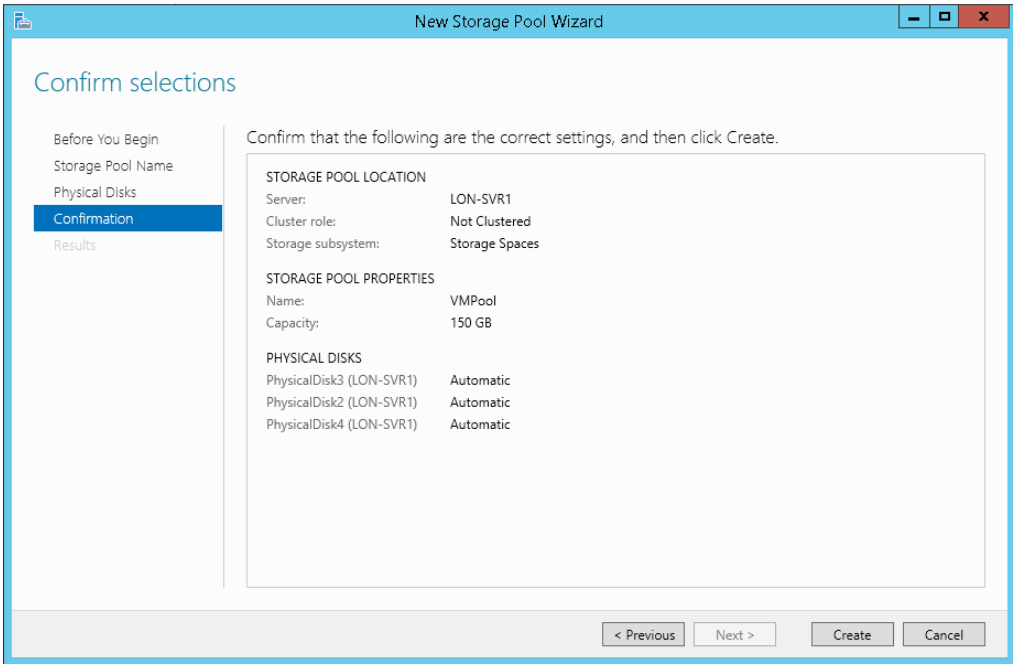
3. Cửa sổ **Storage Pool Name**, trong ô **Name**, nhập **VMPool**, chọn **Next**.



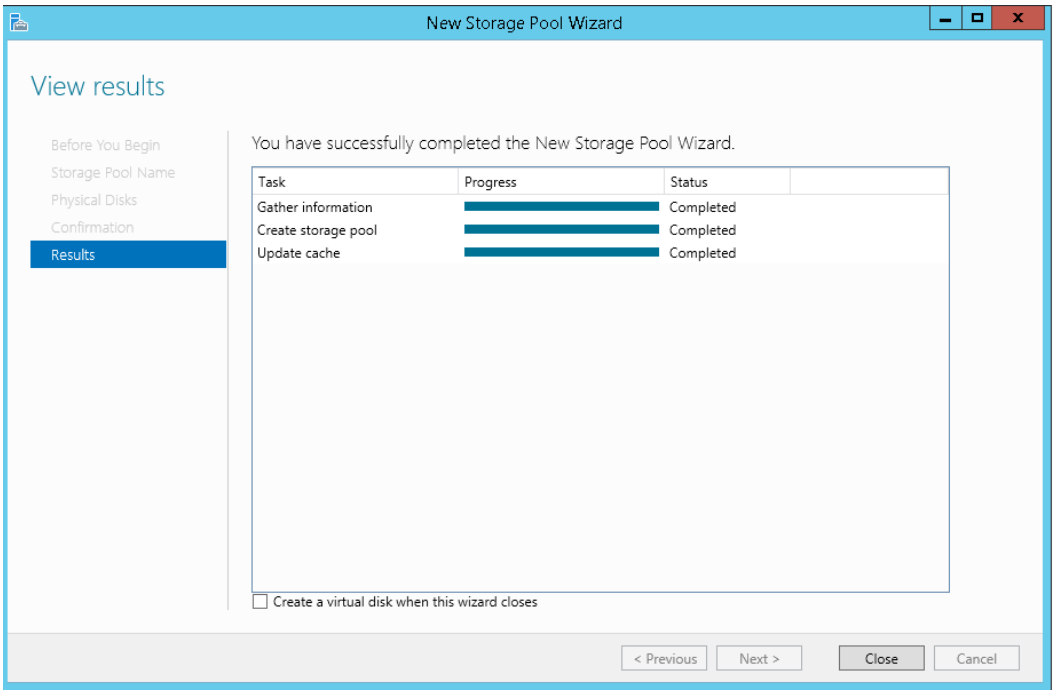

4. Cửa sổ **Physical Disks**, đánh dấu chọn cả 3 ổ đĩa, chọn **Next**.



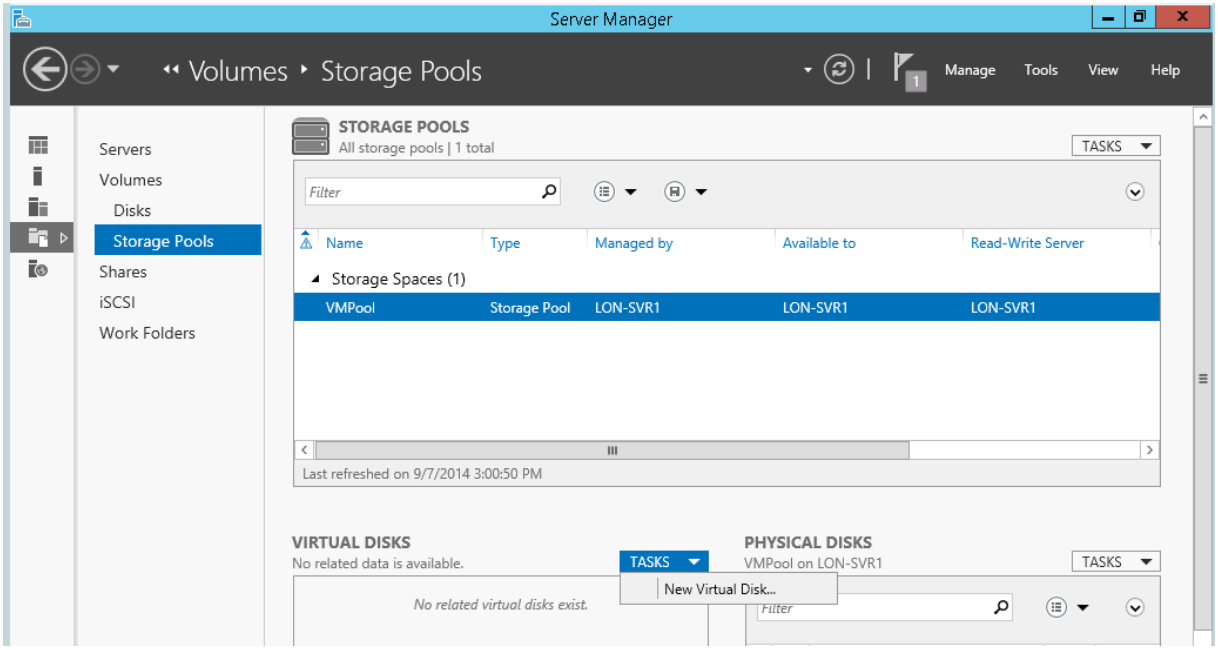
5. Cửa sổ **Confirmation**, chọn **Create**.



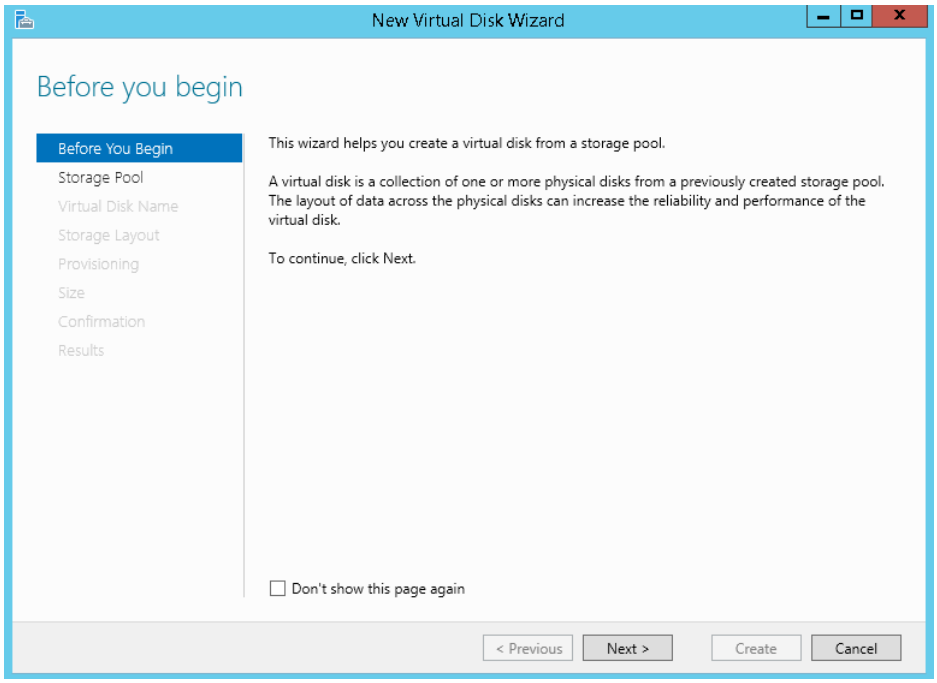

6. Cửa sổ **Results**, chọn **Close**.



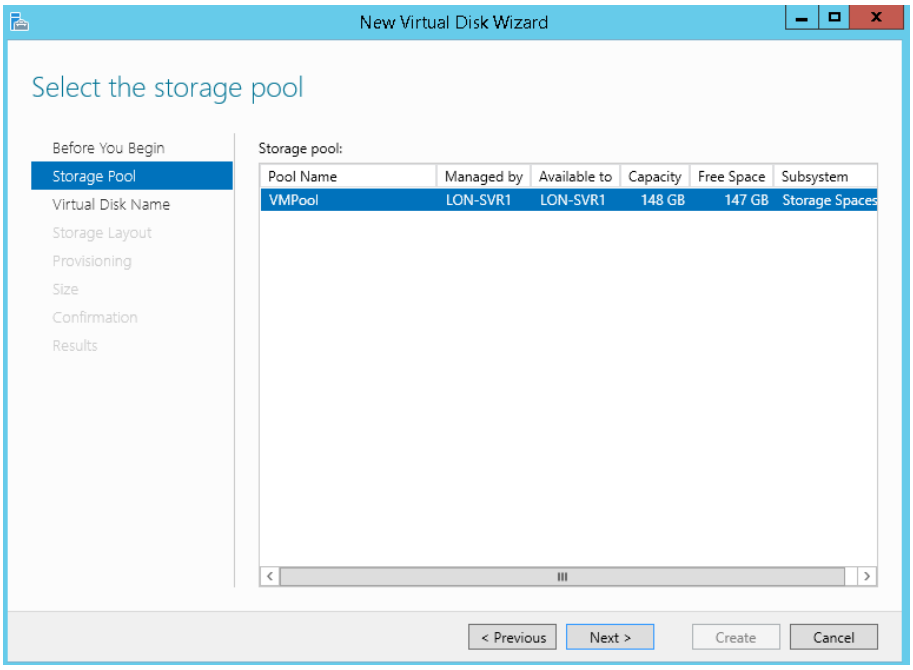
7. Trong phần **VIRTUAL DISK**, bung **TASKS,** chọn **New Virtual Disk**



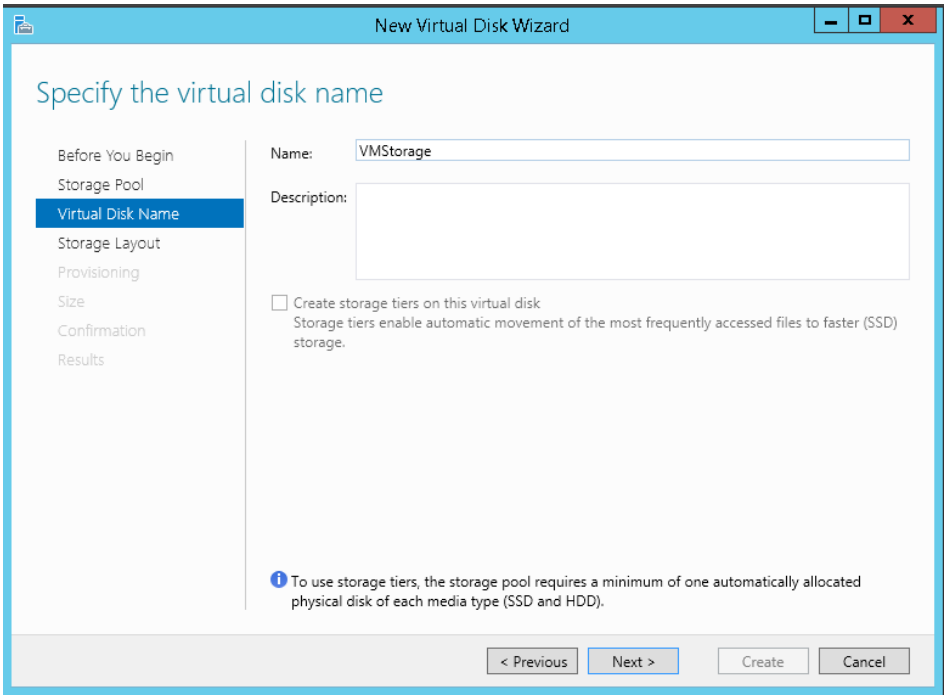

8. Cửa sổ **Before you begin**, chọn **Next**,



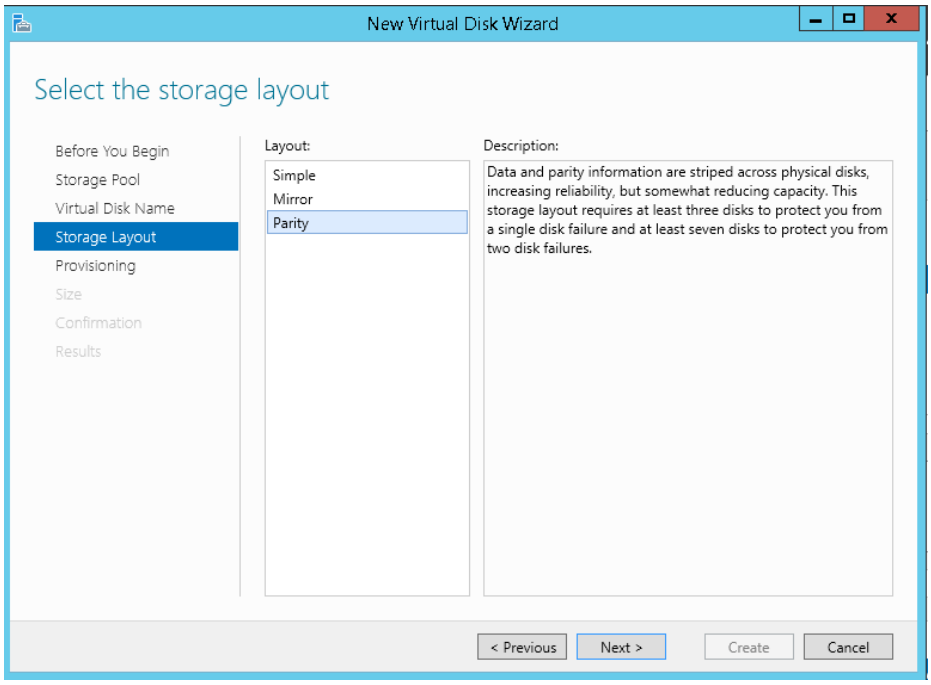
9. Cửa sổ **Storage Pool**, chọn **Next**.



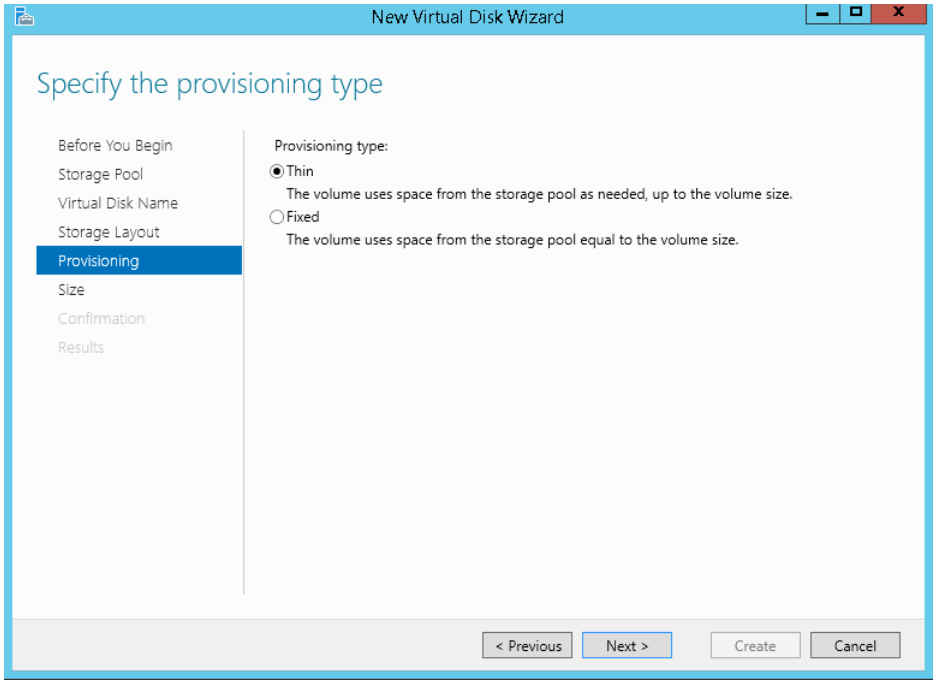

10. Cửa sổ **Virtual Disk Name**, trong ô **Name**, nhập **VMStorage**, nhập **Next**.



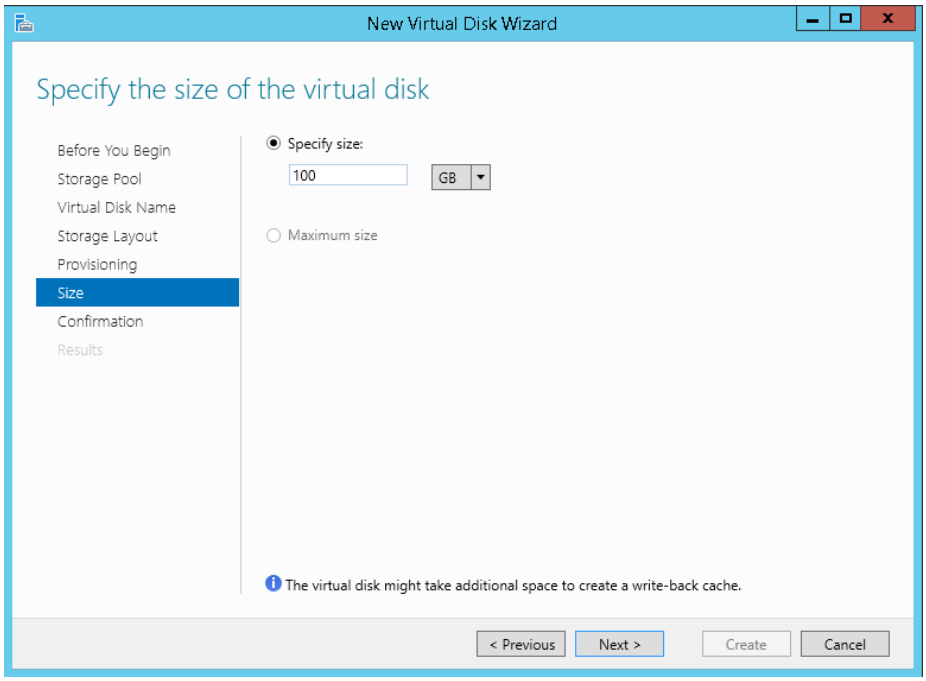
11. Cửa sổ **Storage Layout**, chọn **Parity**, chọn **Next**.



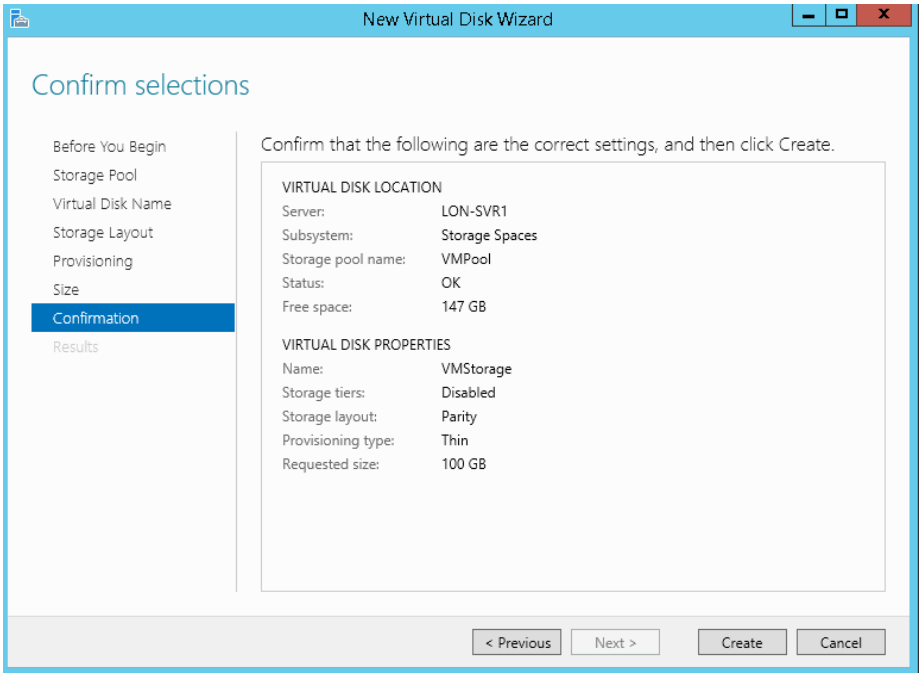

12. Cửa sổ **Provisioning**, chọn **Thin**, và chọn **Next**.



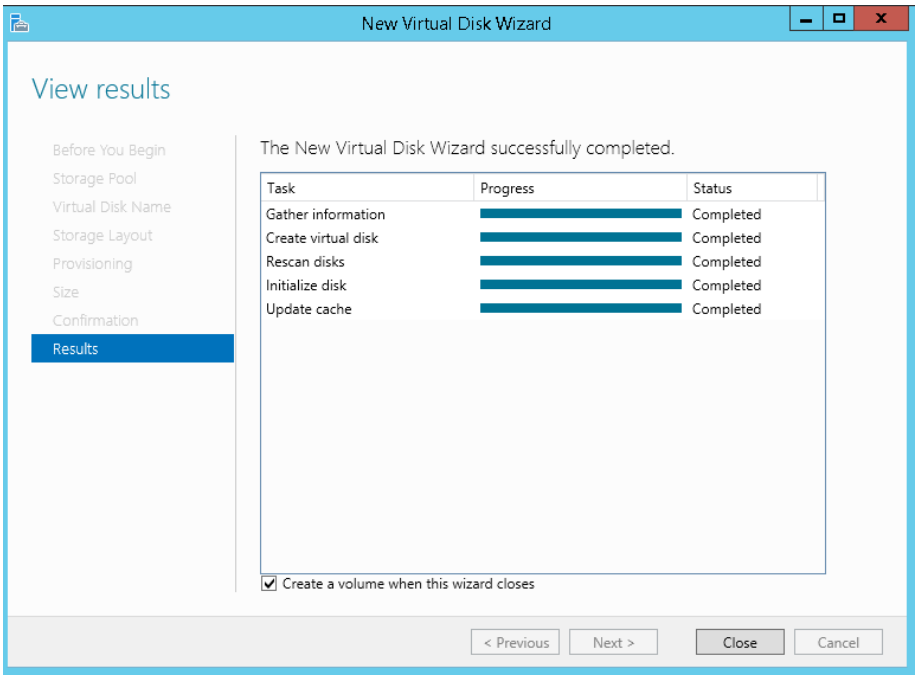
13. Cửa sổ **Size**, trong ô **Specify size**, nhập **100**, và chọn **Next**.



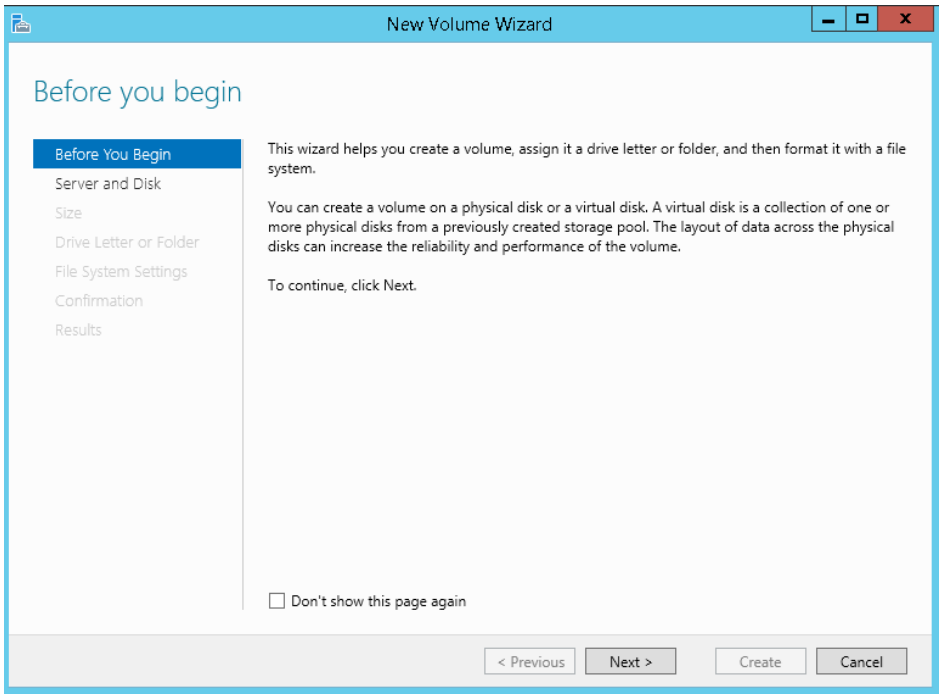

14. Cửa sổ **Confirmation** page, chọn **Create**.



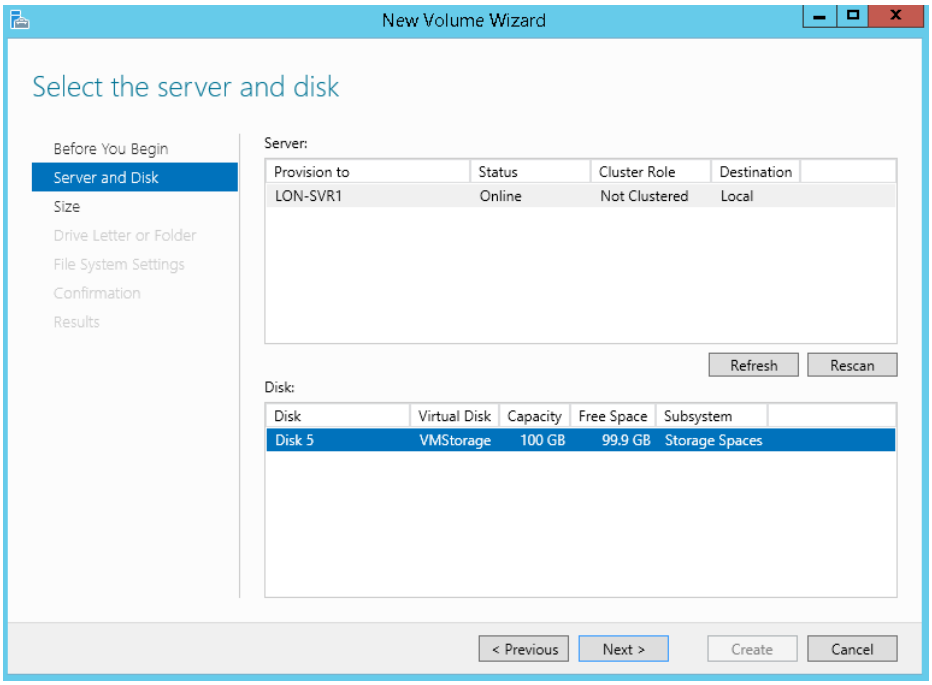
15. Cửa sổ **View results**, click **Close**.



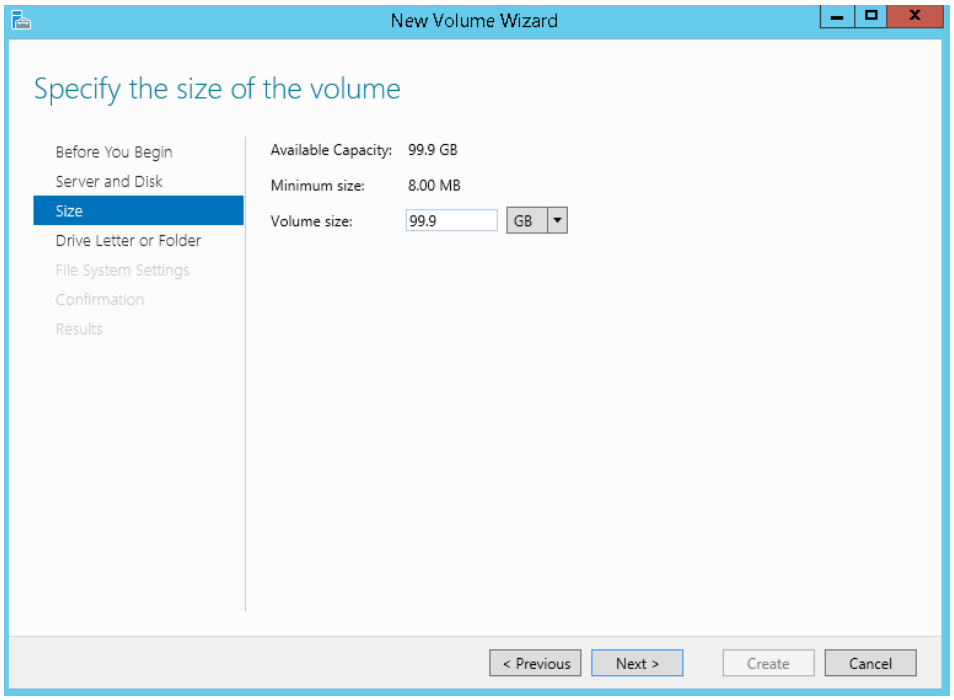

16. Cửa sổ **Before You Begin**, chọn **Next**.



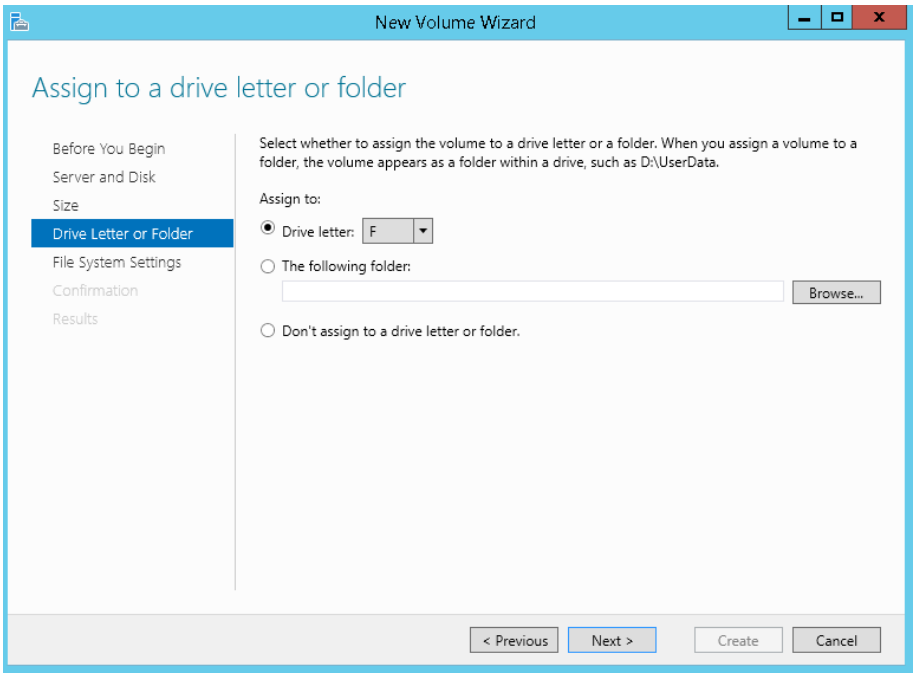
17. Cửa sổ **Server and Disk**, trong ô **Disk**, chọn **VMStorage**, và chọn **Next**.



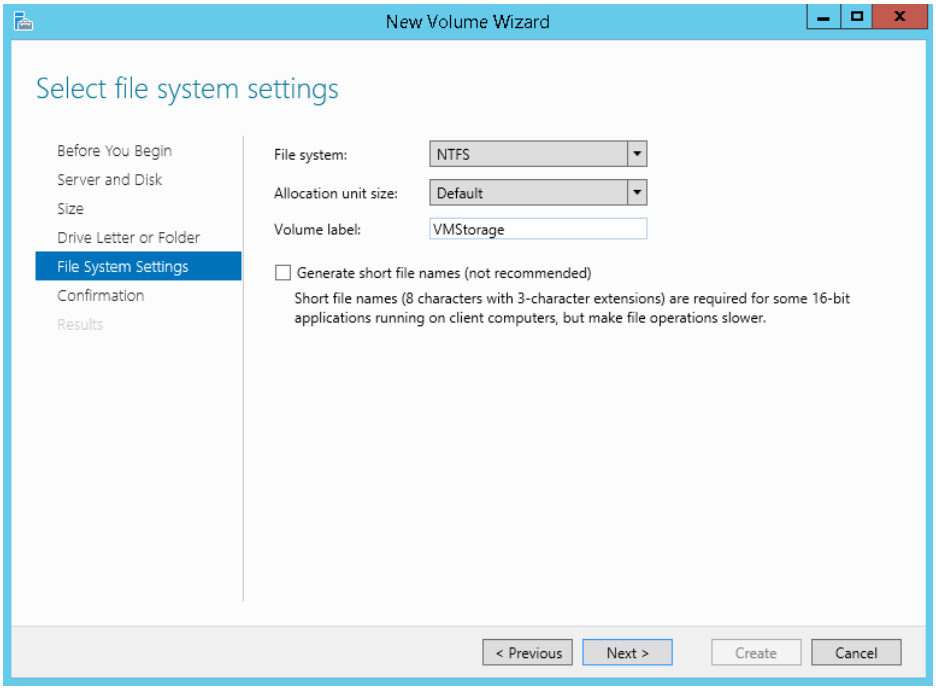

18. Cửa sổ **Size**, giữ mặc định **(99.9) GB**, chọn **Next**.



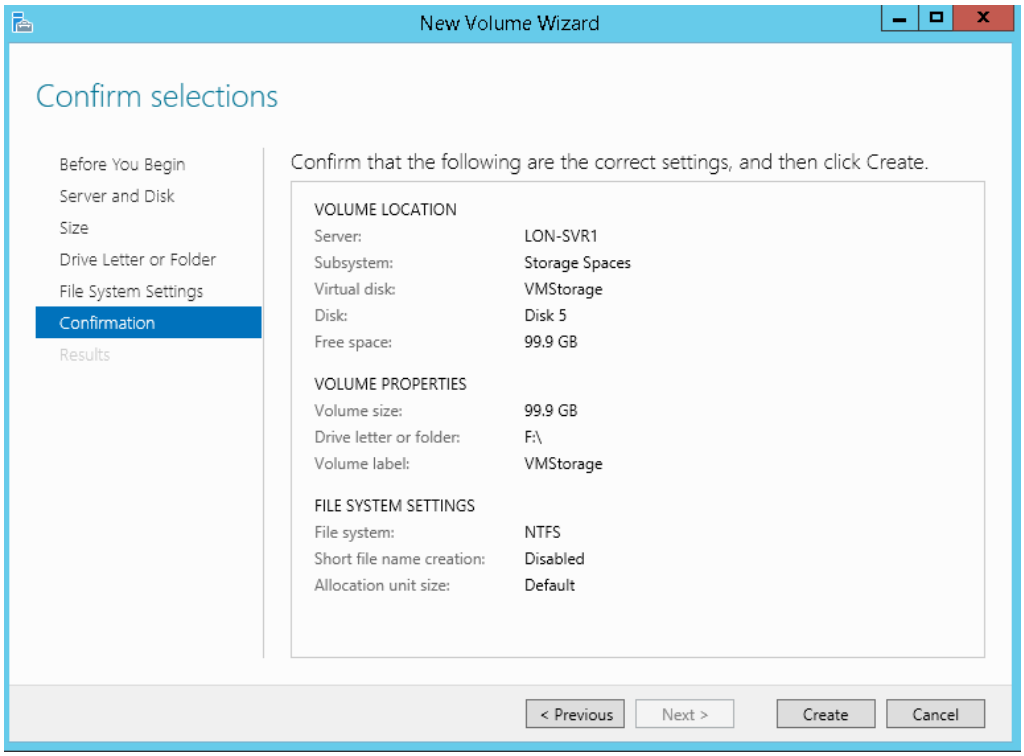
19. Cửa sổ **Drive Letter or Folder**, trong ô **Drive letter,** chọn **F**, và chọn **Next**.




20. Cửa sổ **File System Settings**, trong ô **Volume Label**, nhập **VMStorage**, chọn **Next**.



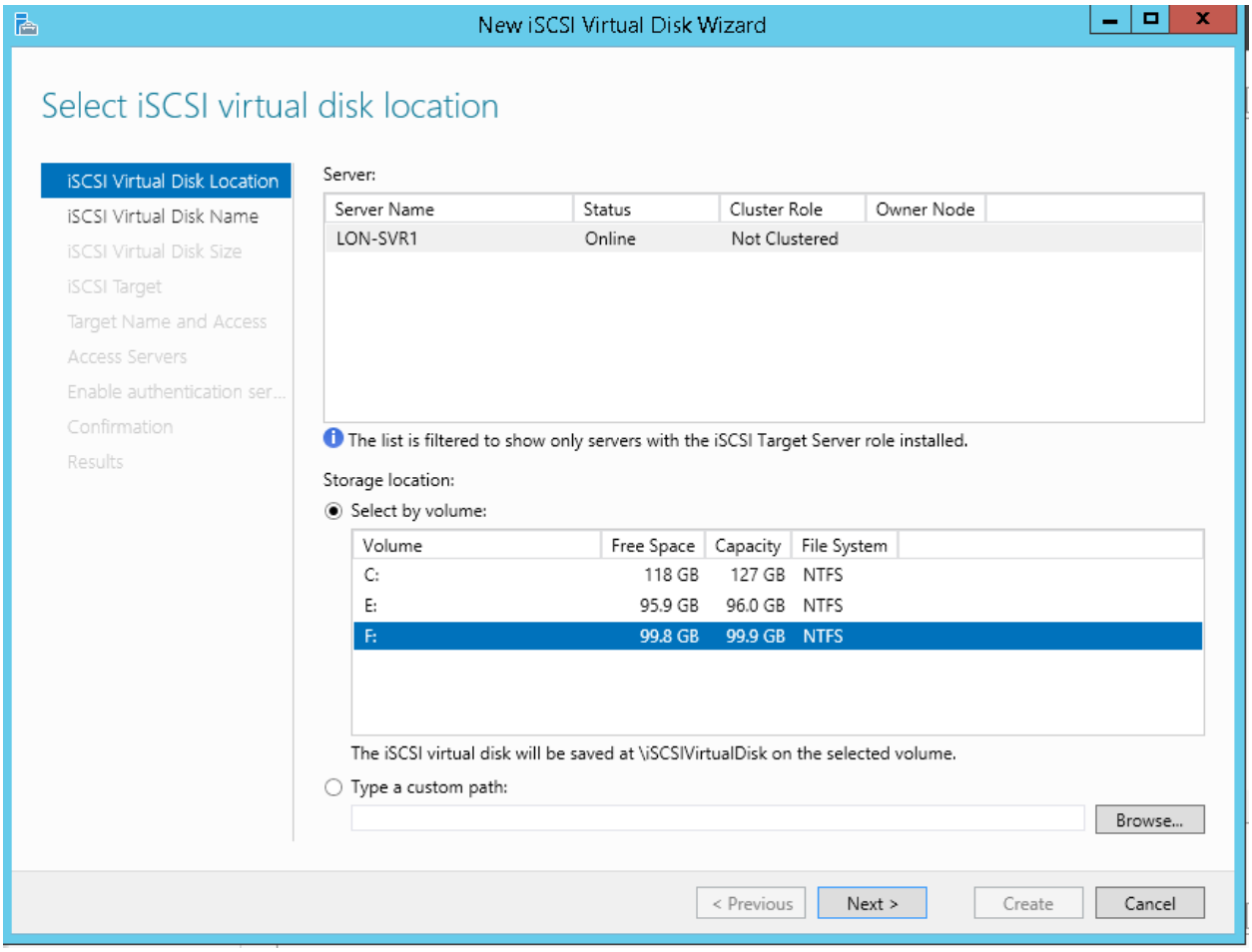
21. Cửa sổ **Confirm selections**, chọn **Create**. Sau khi tạo thành công, chọn **Close**.



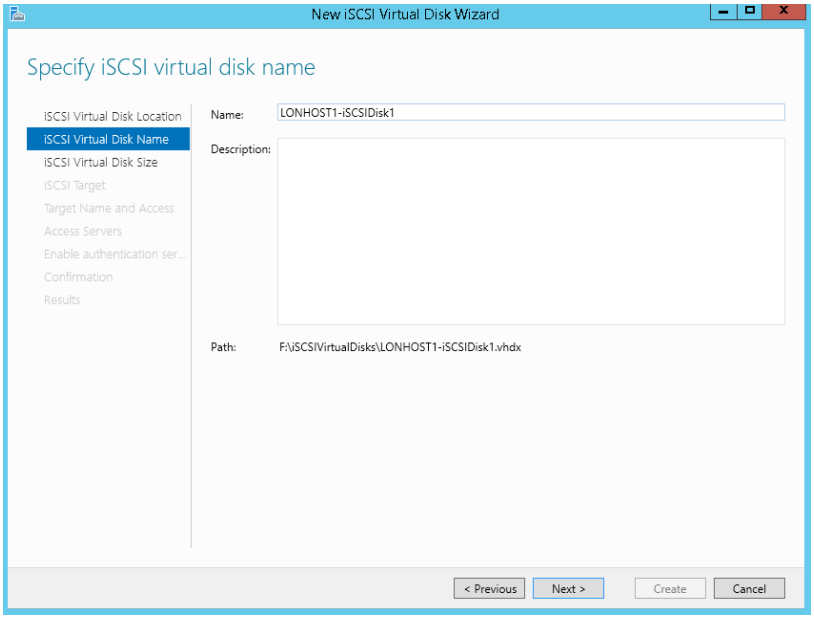

22. Trong cửa sổ **File and Storage Services**, chọn mục **iSCSI**, bung **TASKS**, chọn **New iSCSI Virtual Disk**.



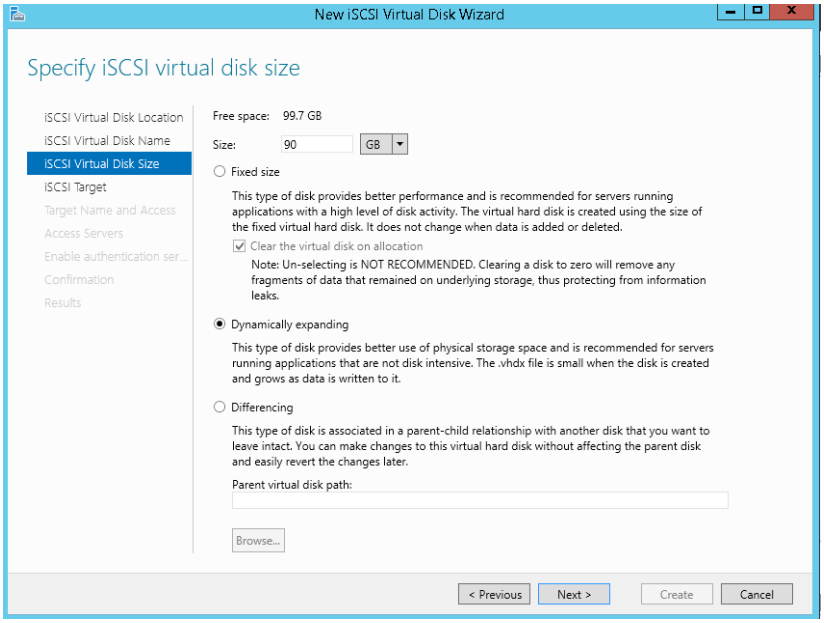
23. Cửa sổ **Select iSCSI virtual disk location**, chọn **F:**, và chọn **Next**.



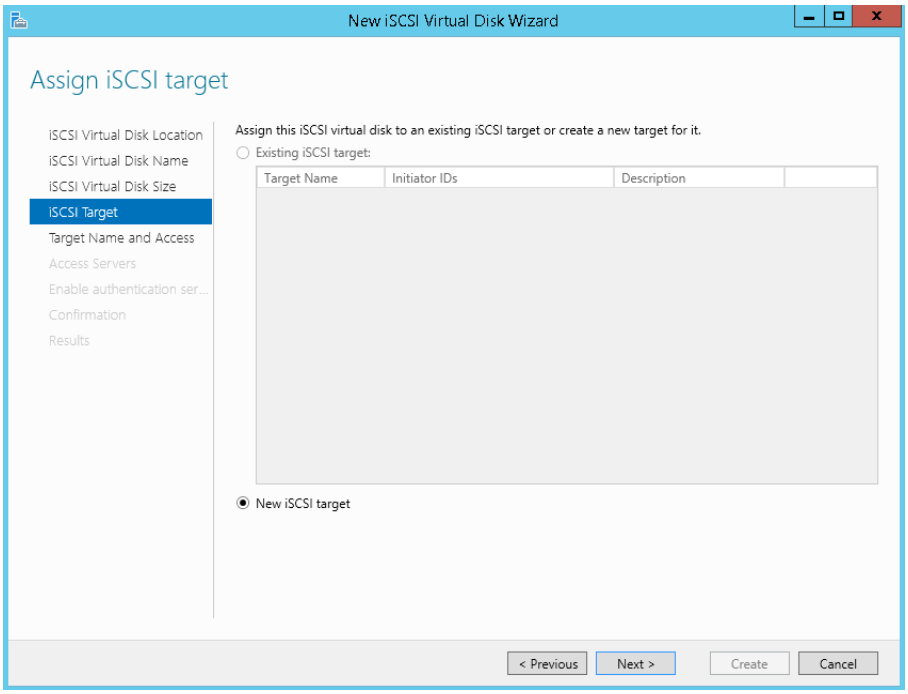
24. Cửa sổ **Specify iSCSI virtual disk name**, trong ô **Name**, nhập **LONHOST1-iSCSIDisk1**, và chọn **Next**.



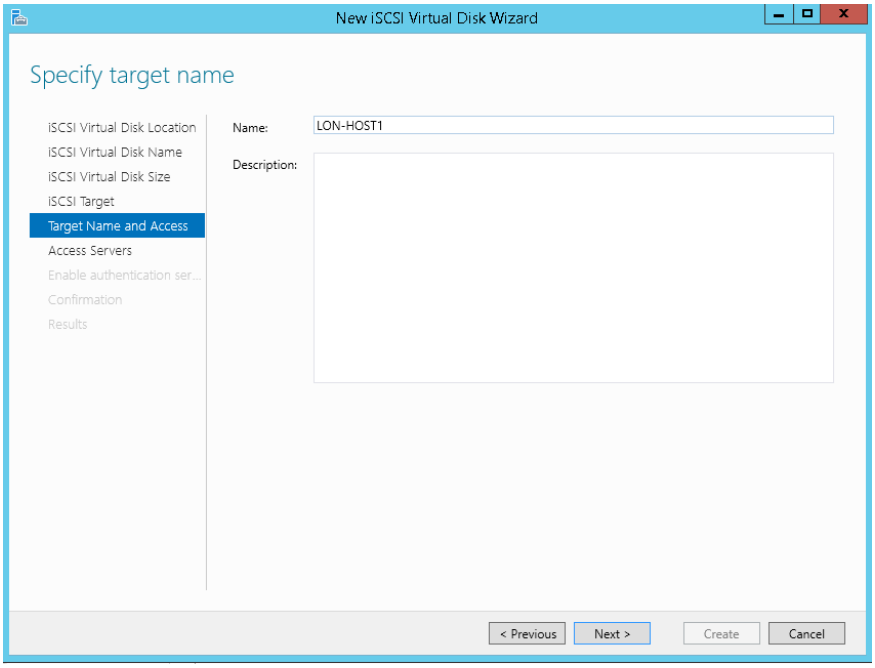

25. Cửa sổ **Specify iSCSI virtual disk size**, trong ô **Size**, nhập **90**, chọn **GB**, chọn **Dynamically expanding**, và chọn **Next**.



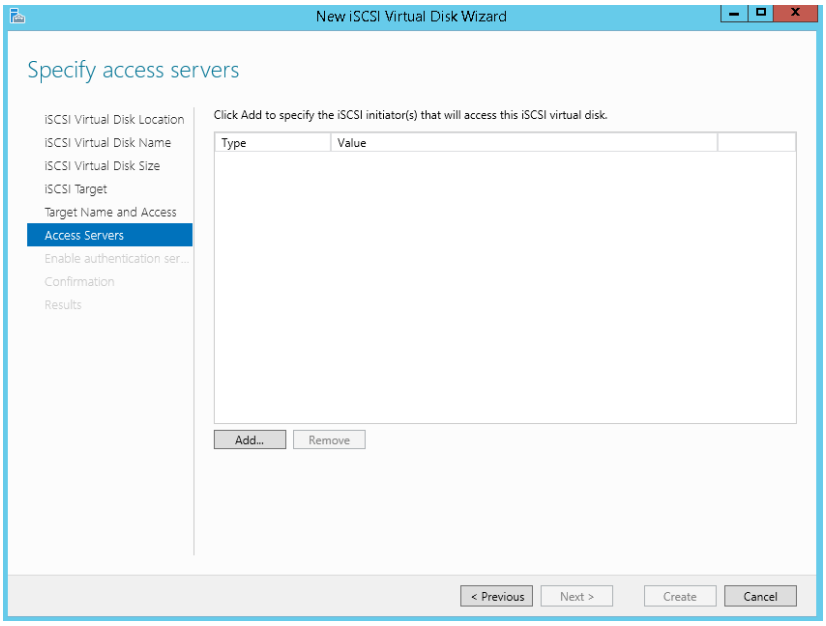
26. Cửa sổ **Assign iSCSI target**, chọn **New iSCSI target**, chọn **Next**.



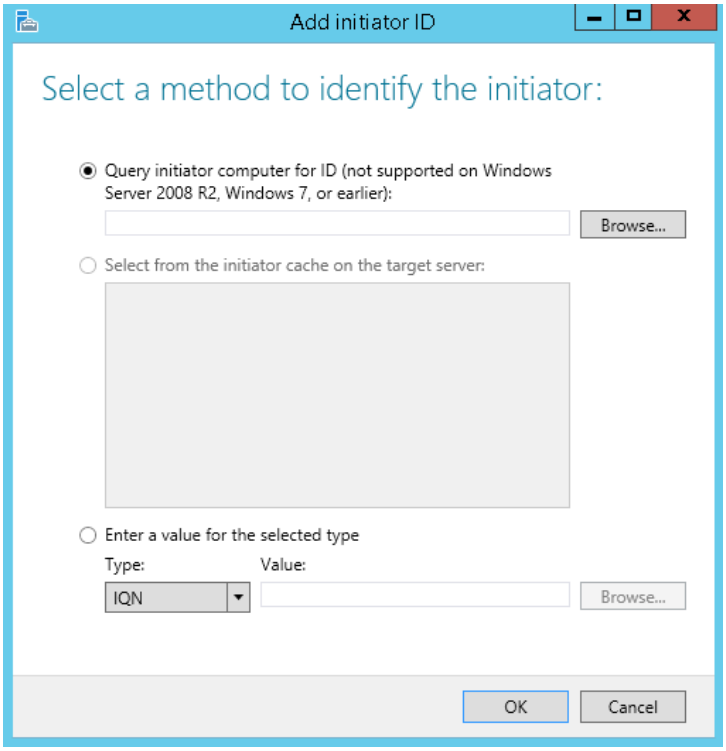

27. Cửa sổ **Specify target name**, trong ô **Name**, nhập **LON-HOST1**, chọn **Next**.



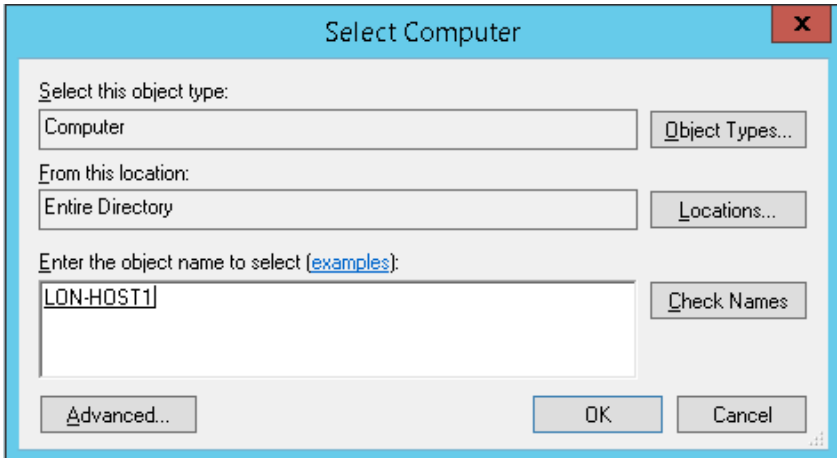
28. Cửa sổ **Specify access servers**, chọn **Add**.



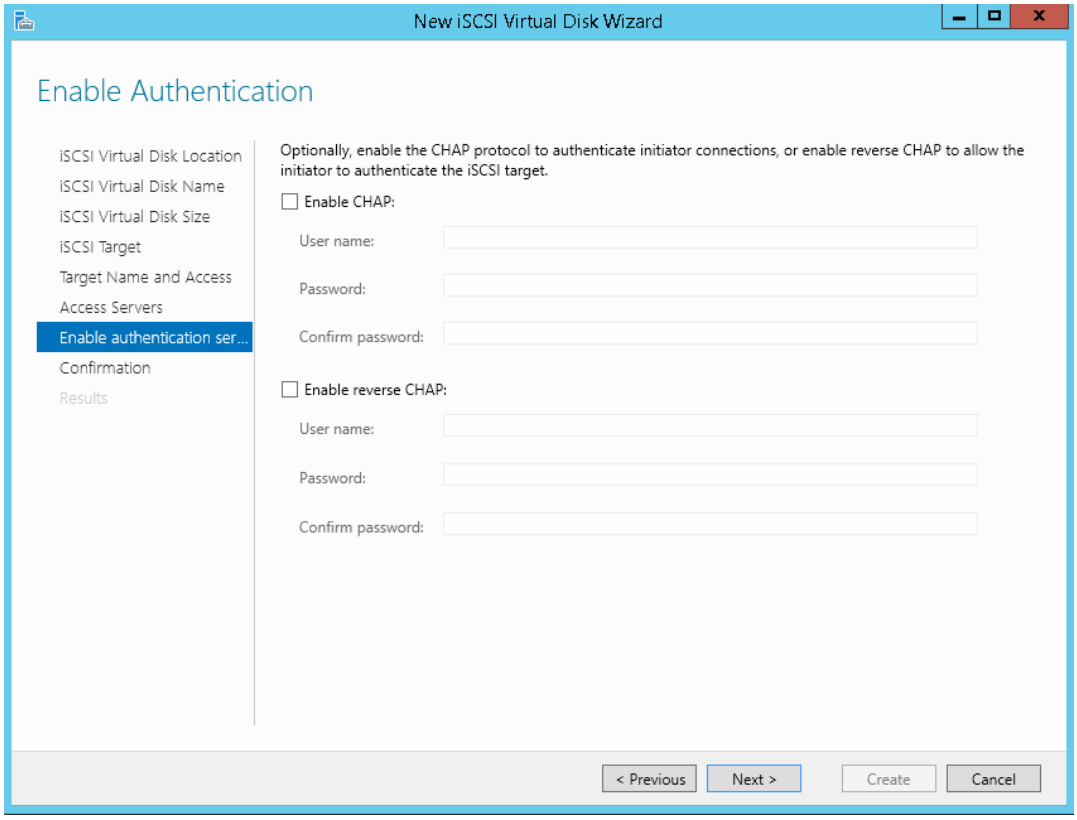

29. In the **Add Initiator ID**, chọn **Browse**.



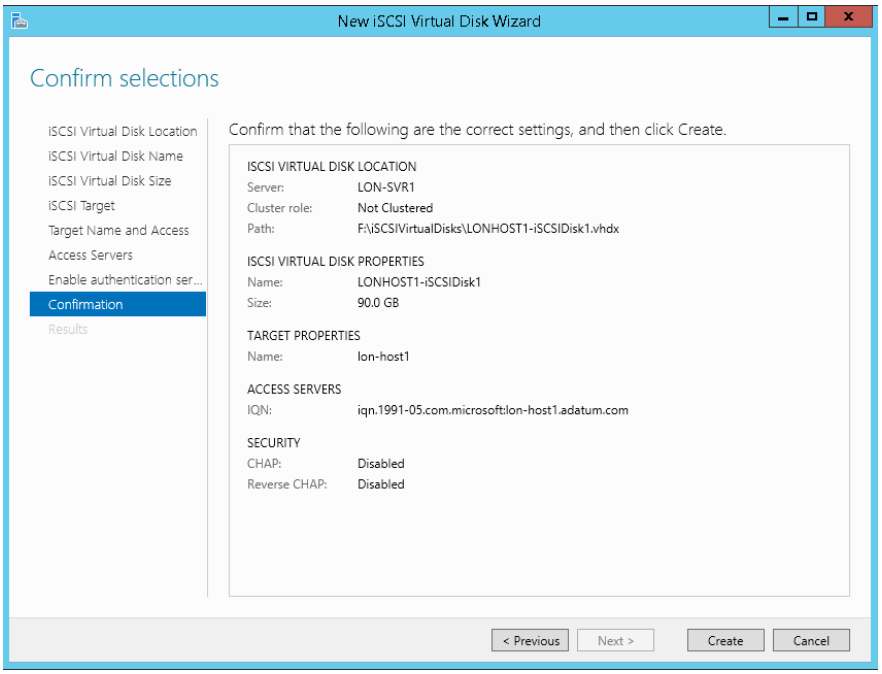
30. In the **Select Computer**, nhập **LON-HOST1**, chọn **Check Names**, chọn **OK** 2 lần, và chọn **Next**.



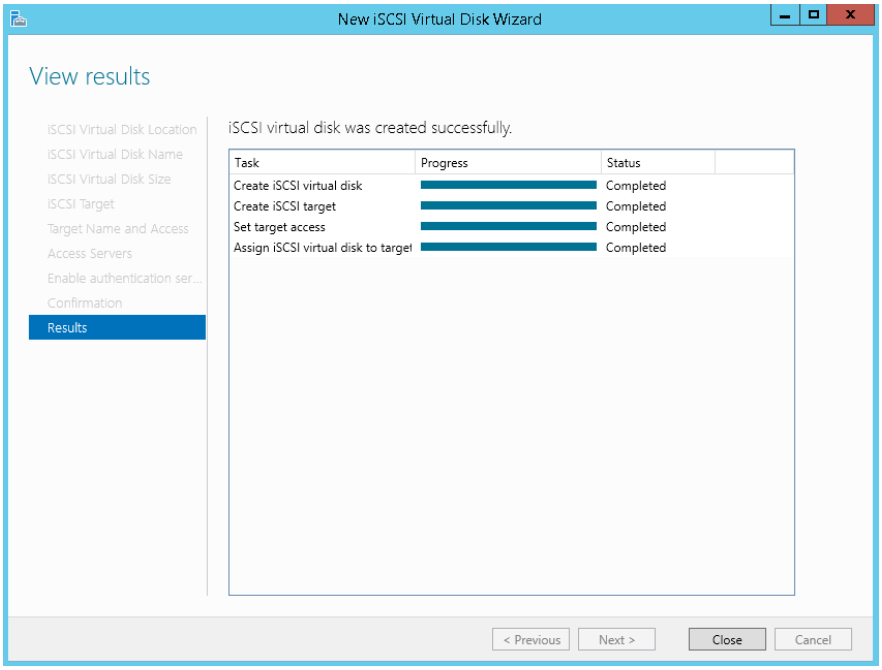

31. Cửa sổ **Enable Authentication**, chọn **Next**.



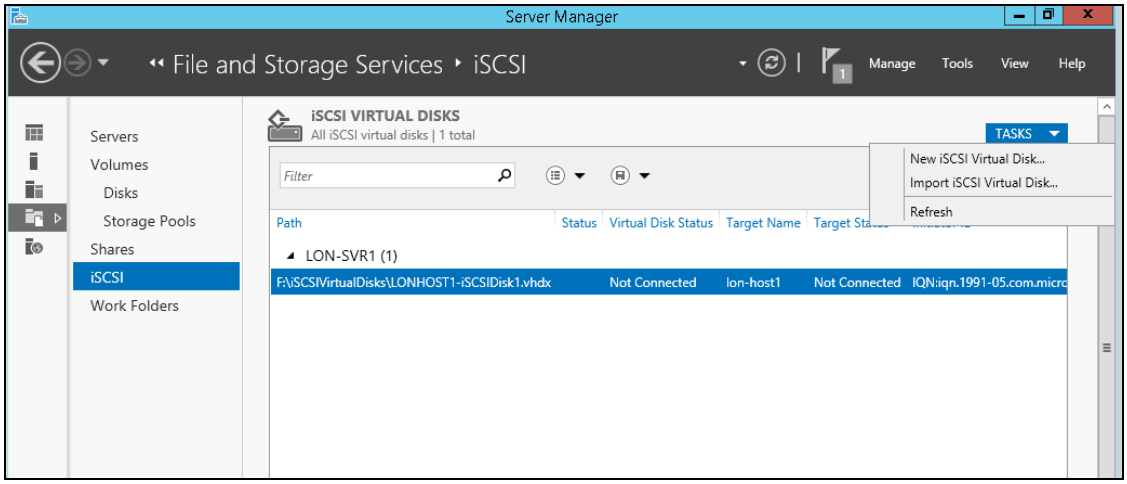
32. Cửa sổ **Confirm selections**, chọn **Create**.



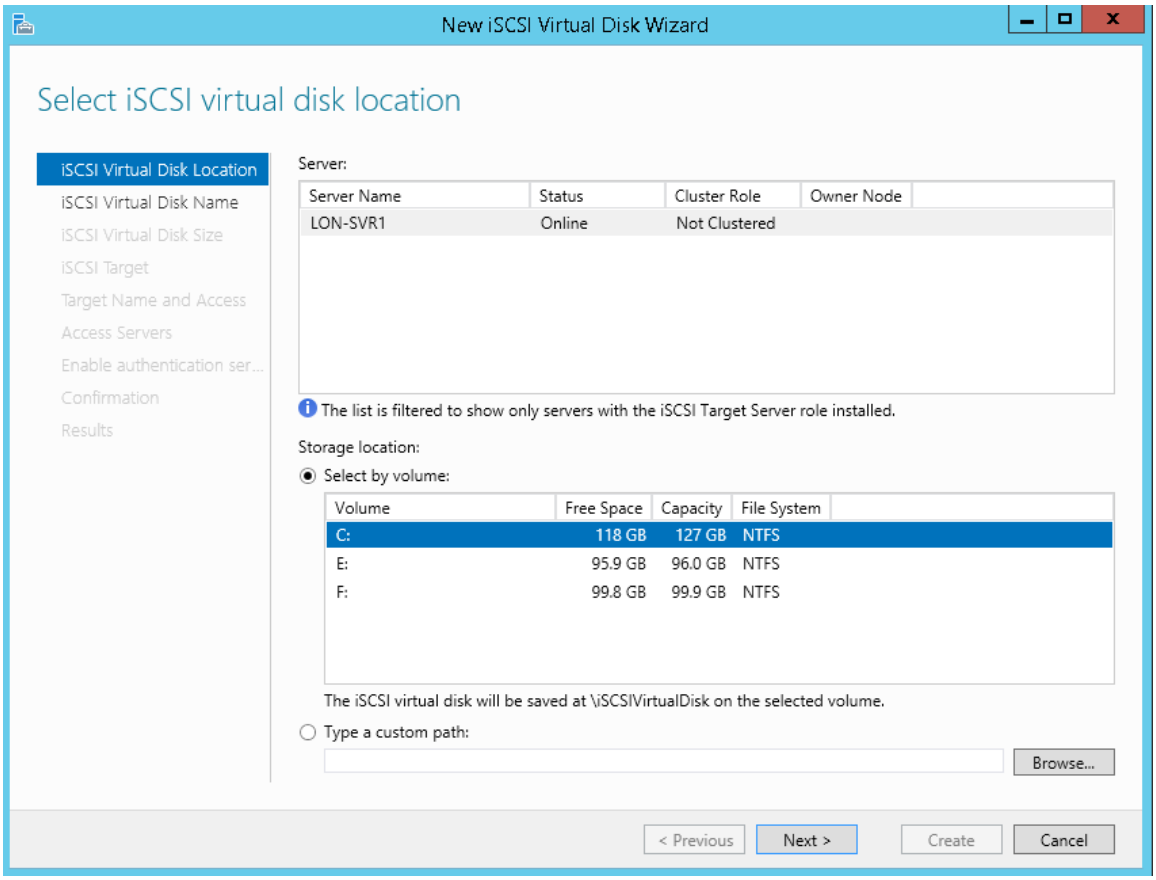

33. Cửa sổ **View results**, sau khi tạo thành công, chọn **Close**.



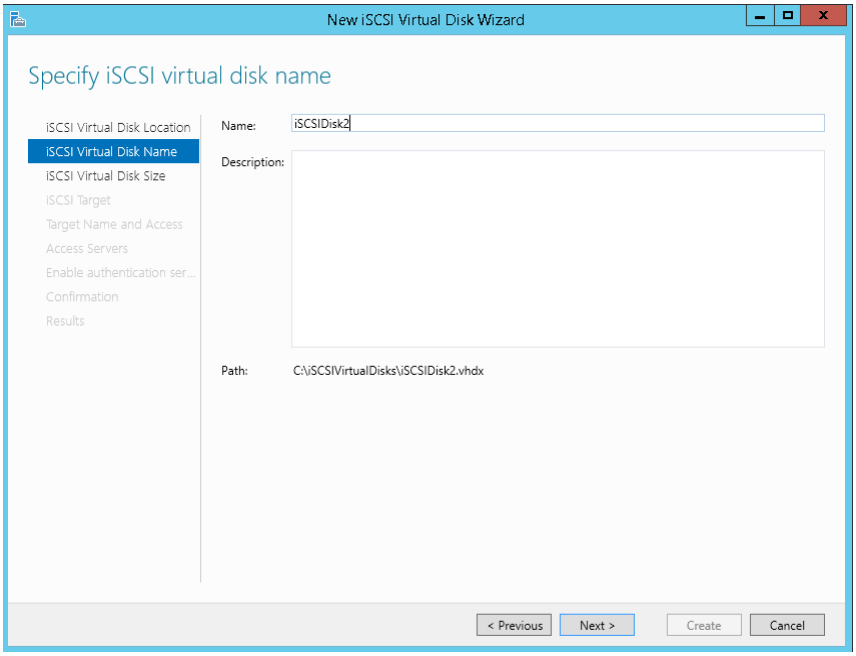
34. Trong phần **iSCSI VIRTUAL DISK**, bung **TASKS**, chọn **New iSCSI Virtual Disk**.



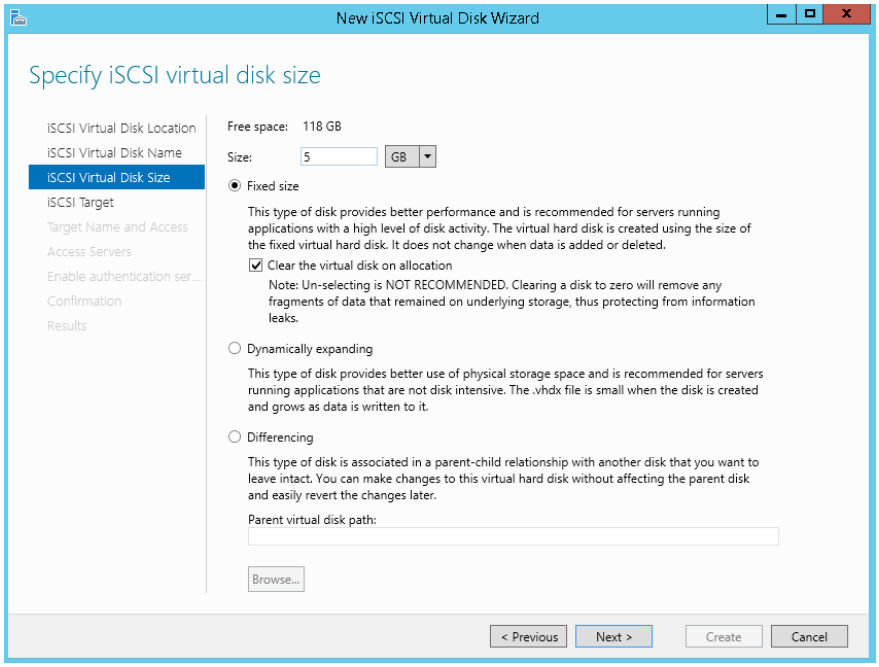

35. Cửa sổ **Select iSCSI virtual disk location**, chọn **C:**, và chọn **Next**.



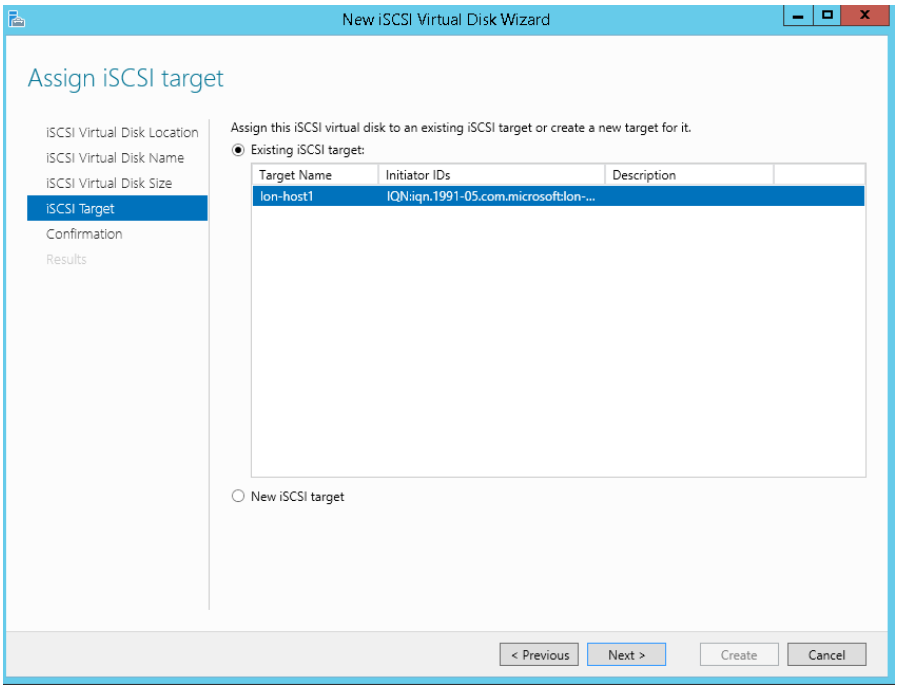
36. Cửa sổ **Specify iSCSI virtual disk name**, trong ô **Name,** nhập **iSCSIDisk2**, avà chọn **Next**.



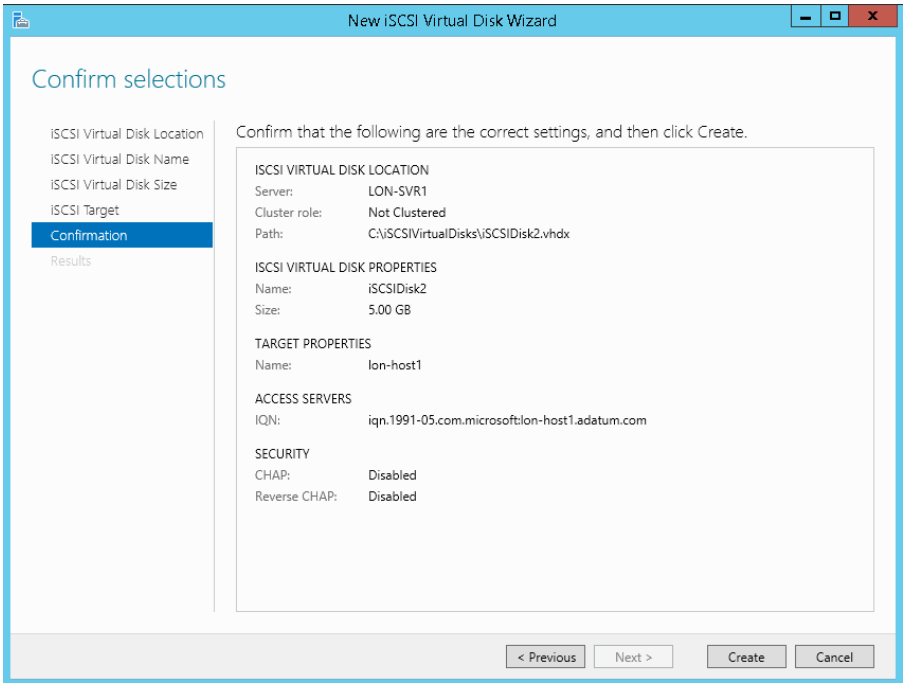

37. Cửa sổ **Specify iSCSI virtual disk size**, trong ô **Size**, nhập **5**, chọn **GB**, và chọn **Next**.



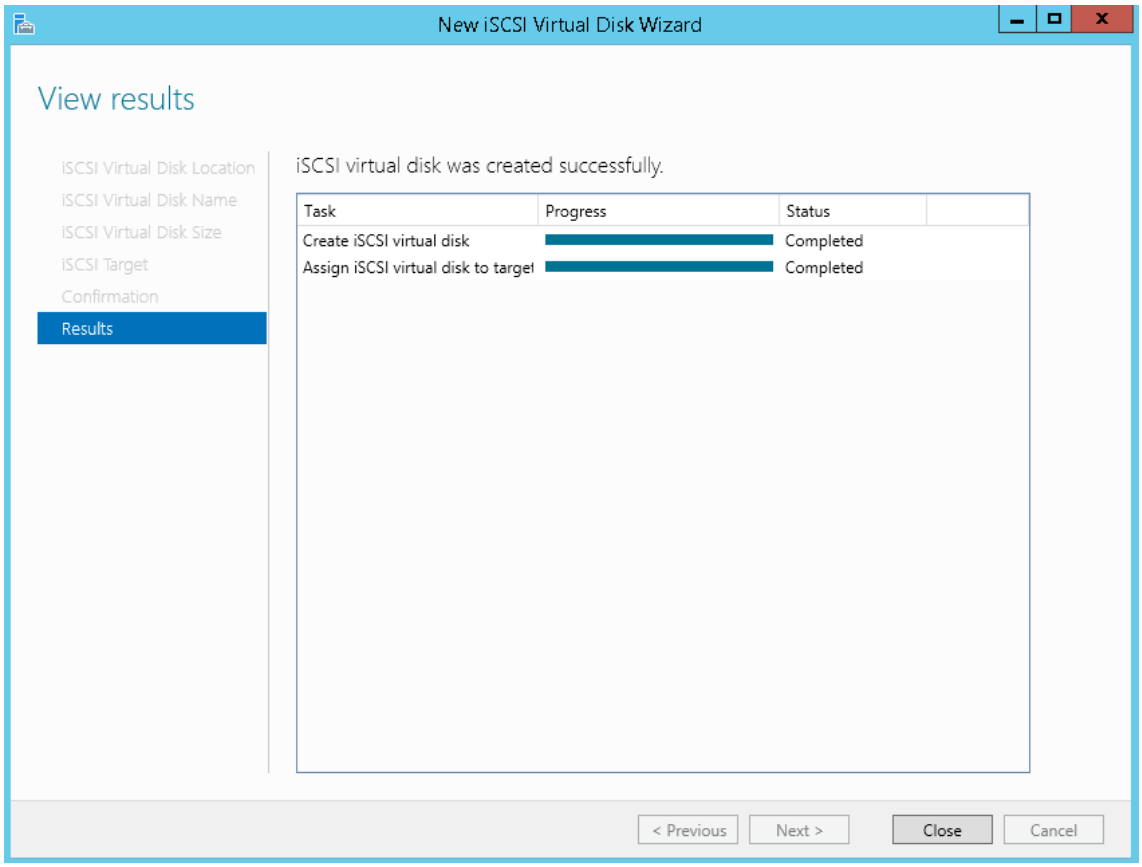
38. Cửa sổ **Assign iSCSI target**, chọn **LON-HOST1**, và chọn **Next**.




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

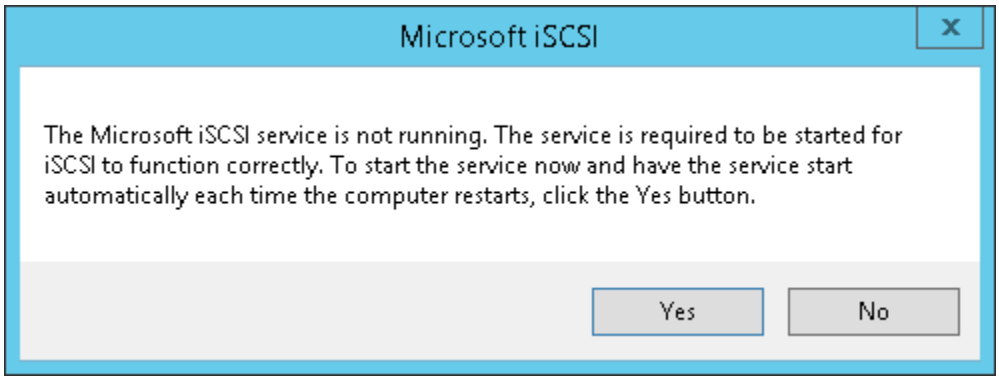


40. Cửa sổ **View results**, sau khi tạo thành công, chọn **Close**.

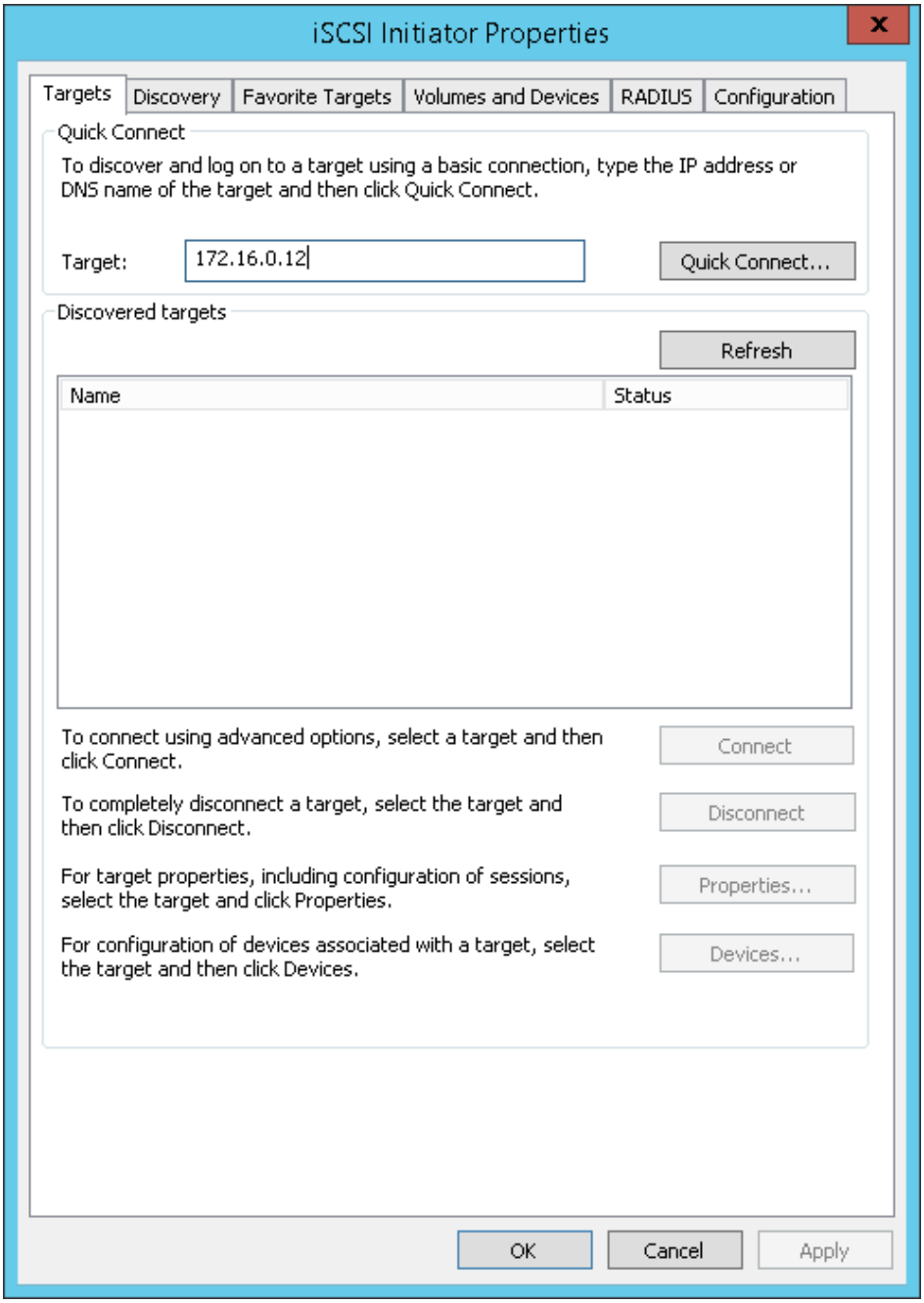



## Bước 2. Cấu hình iSCSI Initiator.

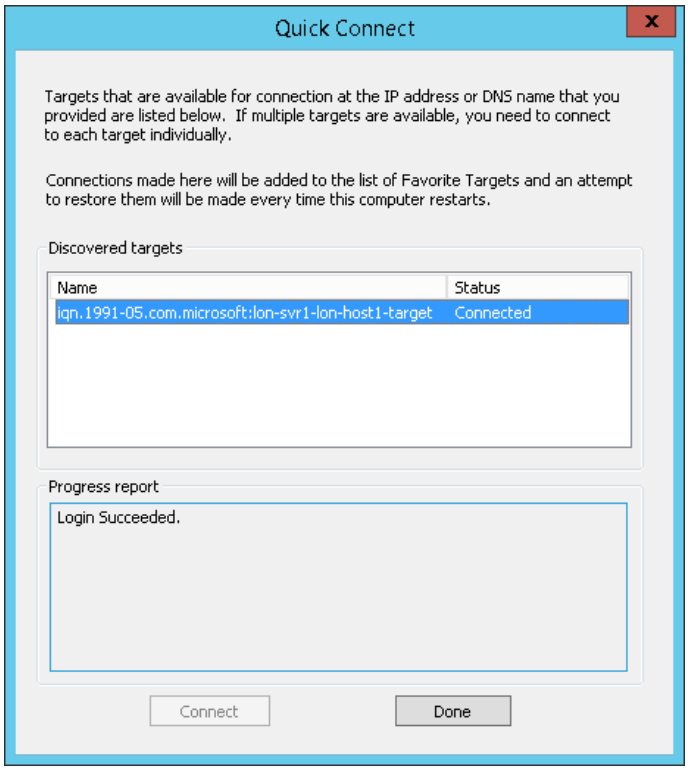
1. Qua máy **LON-HOST1** (Máy thật), trong cửa sổ **Server Manager**, bung menu **Tools**, mở **iSCSI Initiator**. Hộp thoại thông báo, chọn **Yes**.



2.Hộp thoại **iSCSI Initiator Properties**, trong ô **Target**, nhập **172.16.0.12**, chọn **Quick connect**.

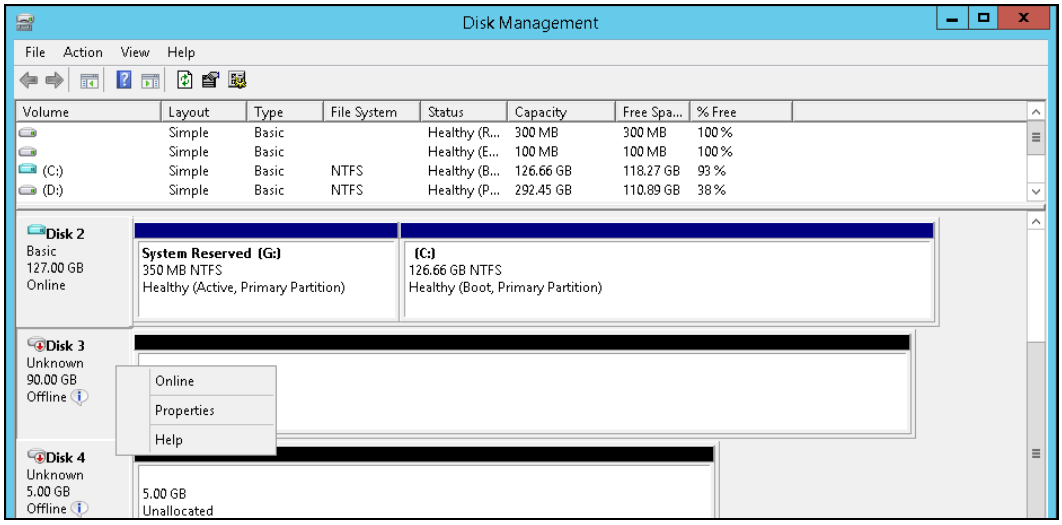


3. Hộp thoại **Quick connect,** chọn **Done**, và chọn **OK**.

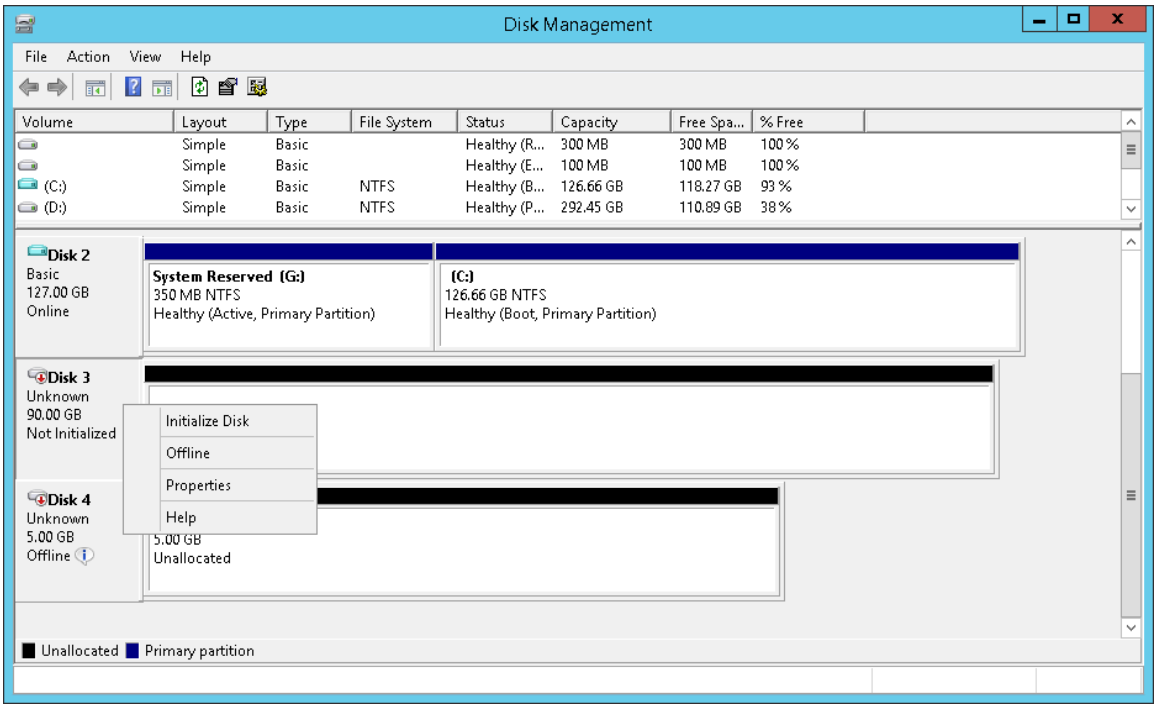



4. Chuột phải **Start menu**, chọn **Disk Management**.

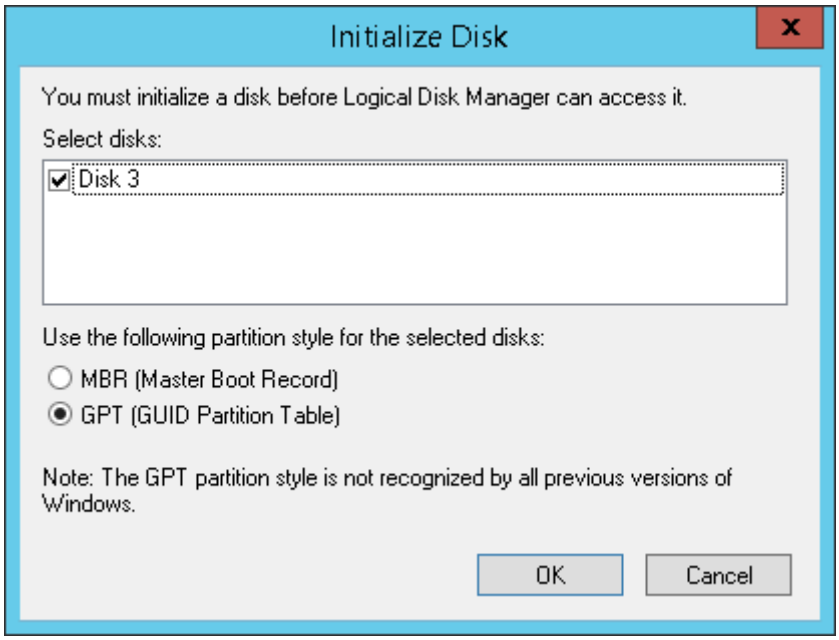
5. Cửa sổ **Disk Management,** chuột phải lên ổ đĩa có dung lượng **90 GB**, chọn **Online**.



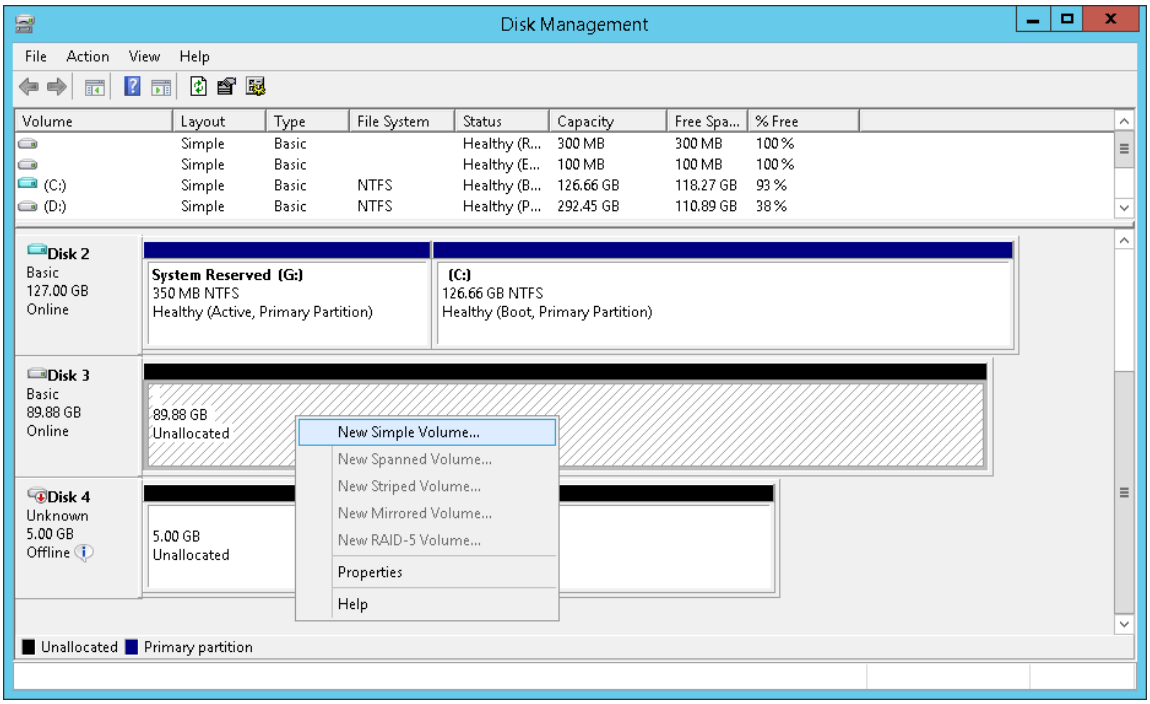
6. Chuột phải lên ổ đĩa có dung lượng **90 GB**, chọn **Initialize Disk**.



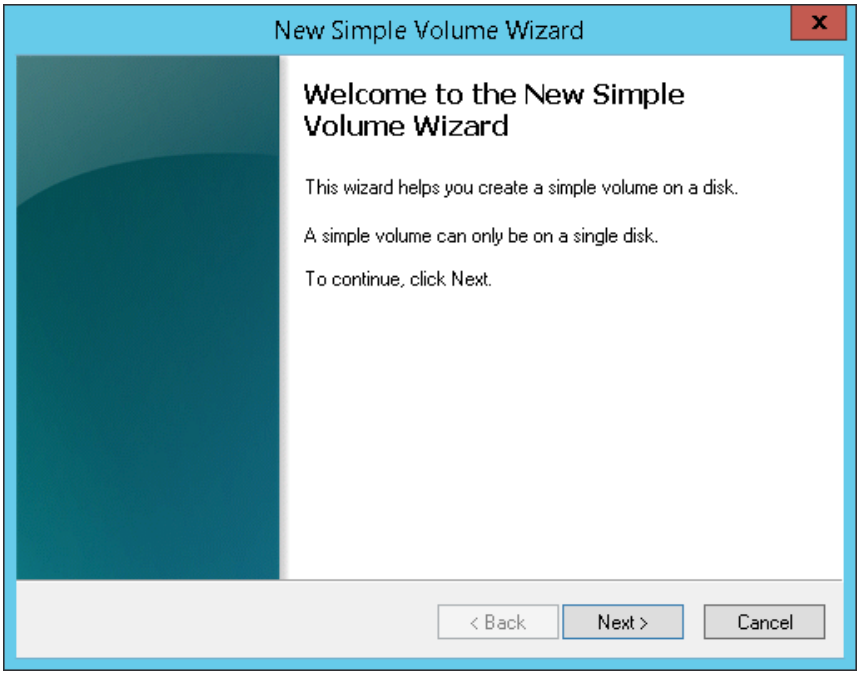

7. Hộp thoại **Initialize disk**, chọn **OK**.



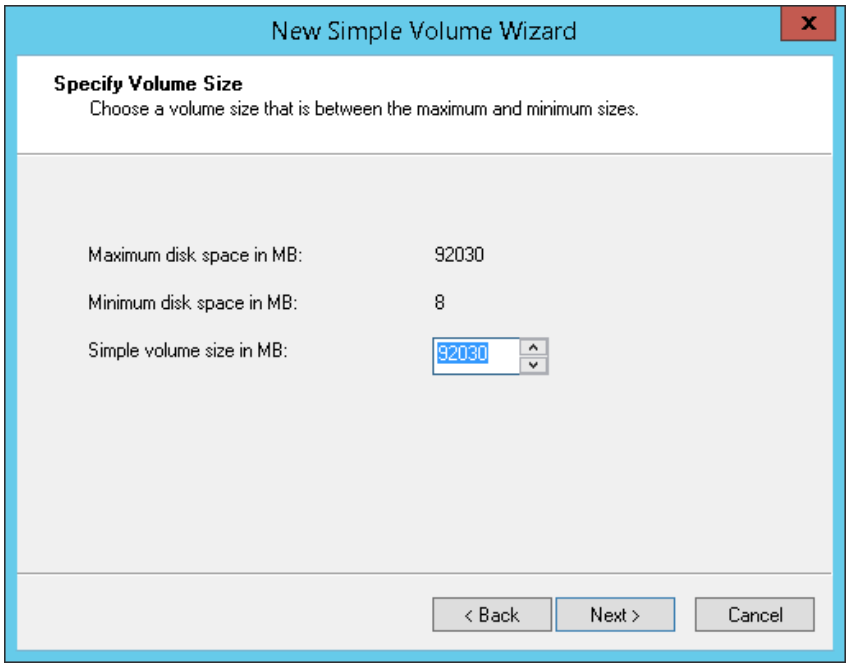
8. Chuột phải lên phần **Unallocated**, chọn **New Simple Volume**.



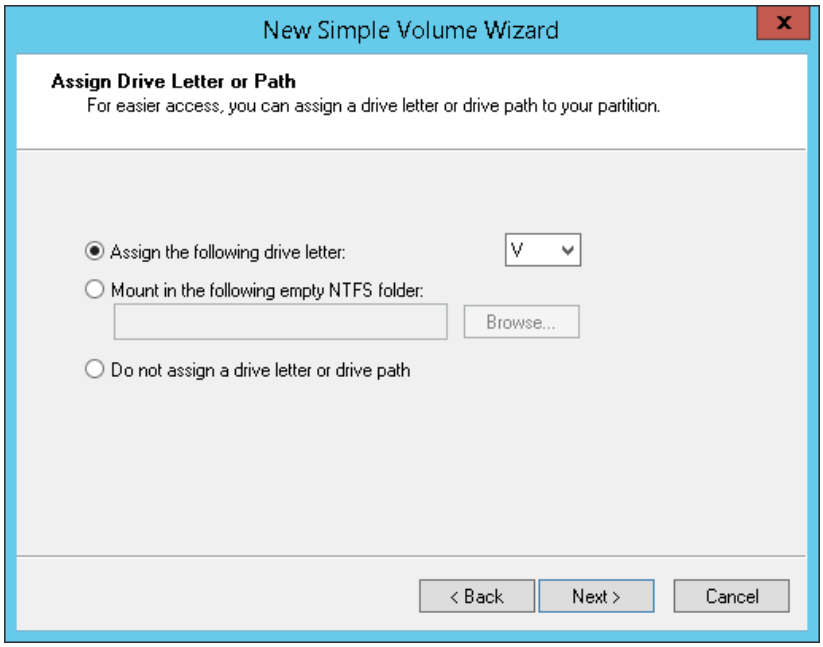

9. Cửa sổ **Welcome**, click **Next**



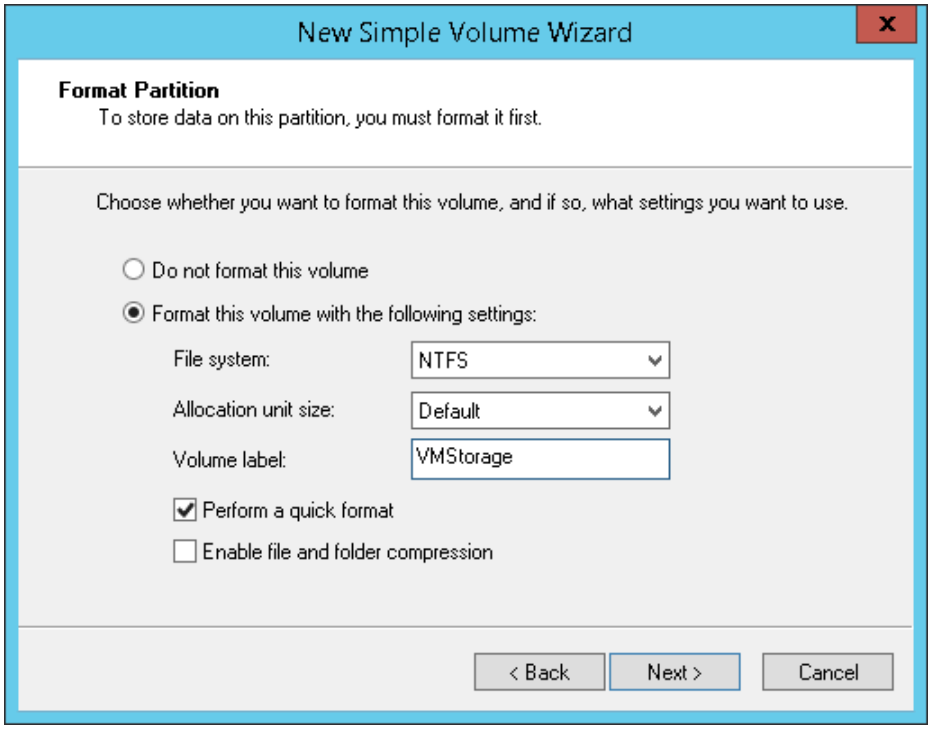
10. Cửa sổ **Specify Volume Size**, chọn **Next**.




11. Cửa sổ **Assign Driver letter or Path**, bung ô **Assign the following drive letter**, chọn **V**, chọn **Next**



12. Cửa sổ **Format Partition**, trong ô **Volume label**, nhập **VMStorage**, chọn **Next**, và chọn **Finish**.




13. Tắt **Disk Management**.

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công iSCSI Target và iSCSI Initiator cho việc triển khai iSCSI Storage.**

## Bài tập 2: Triển khai cơ sở hạ tầng cho hê thống ảo hóa.

Bây giờ bạn sẽ cấu hình cơ sở hạ tầng cho việc triển khai hệ thống ảo hóa.

❖ **Bài thực hành bao gồm các bước:**

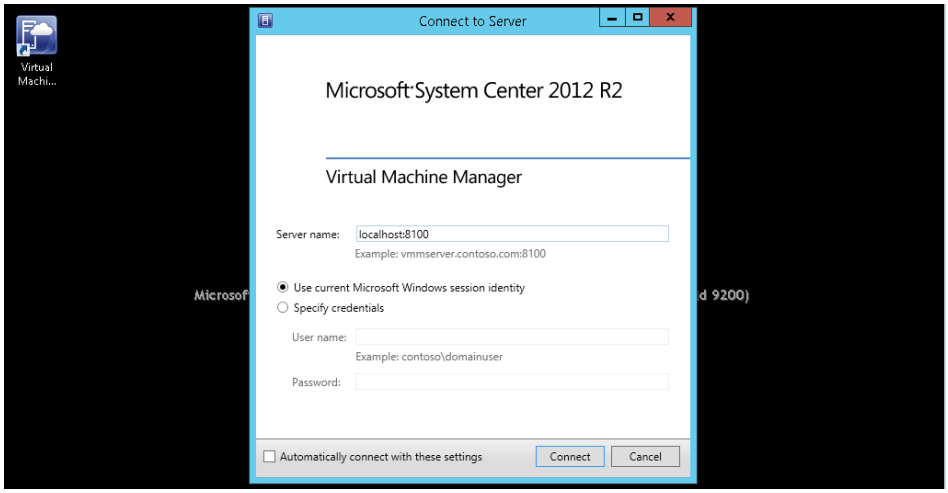
1. Cấu hình Logical Networks.
2. Cấu hình Network Virtualization.
3. Chỉ định máy ảo vào VM networks.

❖ **Thực hiện:**

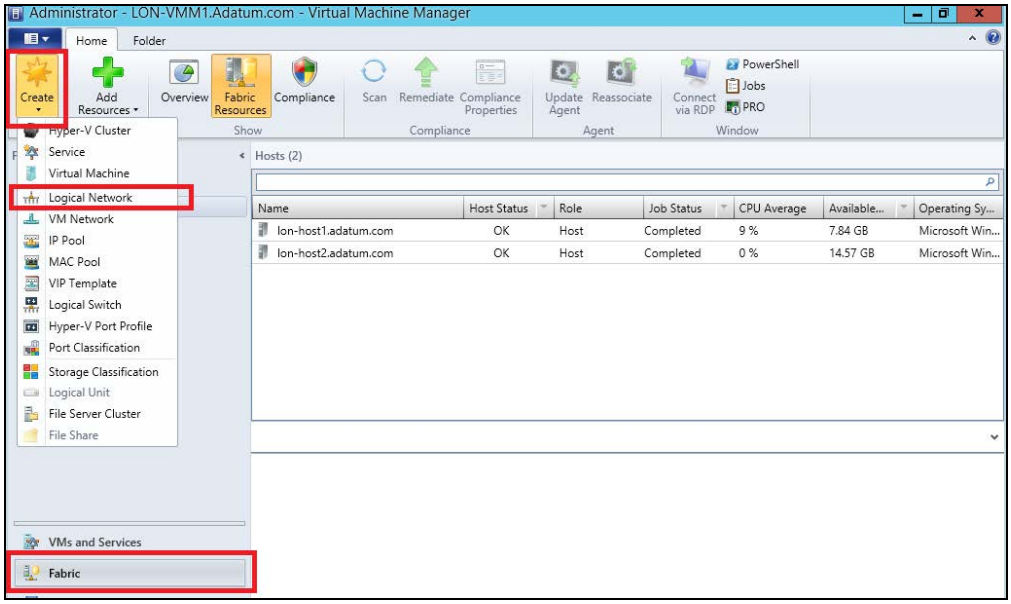
### Bước 1. Cấu hình Logical Networks.

➢ **Tạo Logical Network**

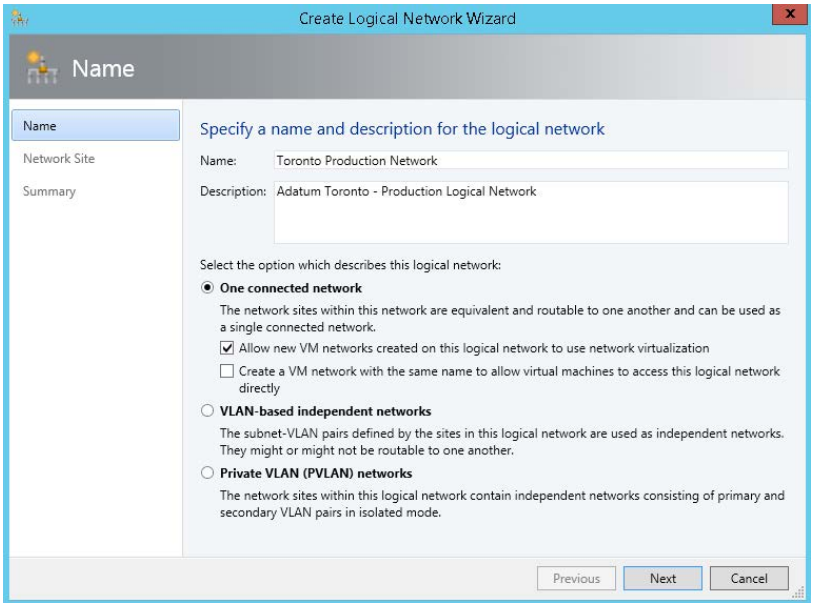
1. Qua máy **LON-VMM1**, trên desktop, mở **Virtual Machine Manager Console**. Cửa sổ **Connect to Server**, chọn **Connect**.



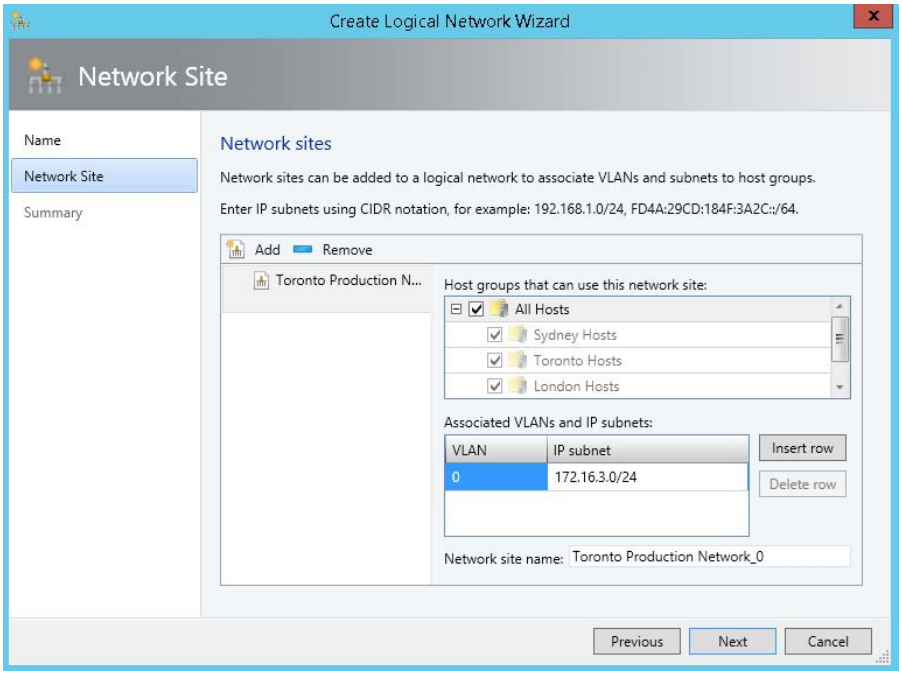
2. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric**, chọn **Create**, và chọn **Logical Network**.



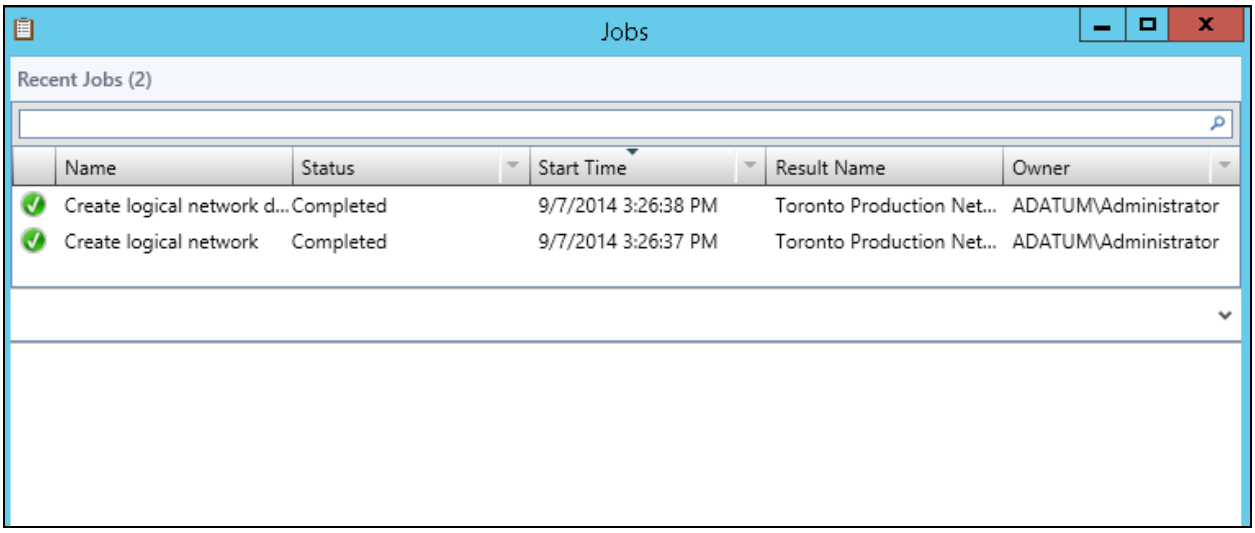

3. Trong ô **Name**, nhập **Toronto Production Network**, trong ô **Description**, nhập **Adatum Toronto – Production Logical Network**. Đánh dấu chọn **Allow new VM networks created on this logical network to use network virtualization**, và chọn **Next**.



4. Cửa sổ **Network site**, chọn **Add**, đánh dấu chọn **All Hosts**, chọn **Insert row**, trong ô **VLAN**, nhập **0**, trong ô **IP subnet**, nhập **172.16.3.0/24**, chọn **Next**, và chọn **Finish**.

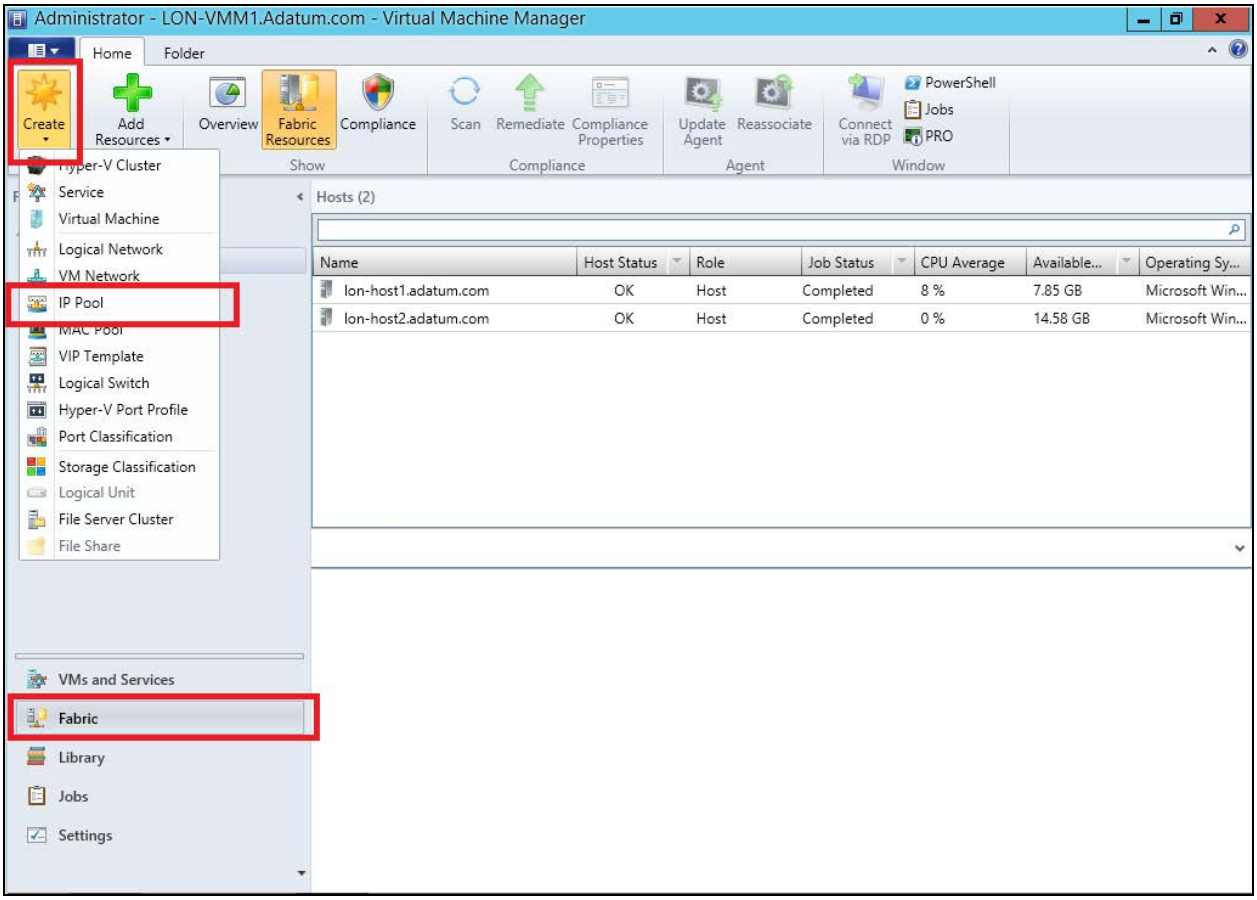



5. Tắt cửa sổ **Jobs**.

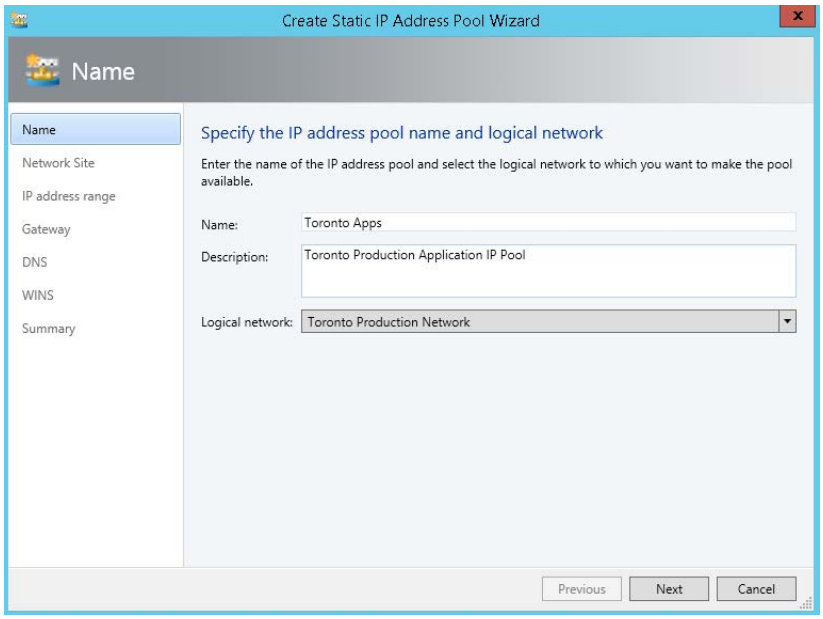


## ➢ Tạo IP pool

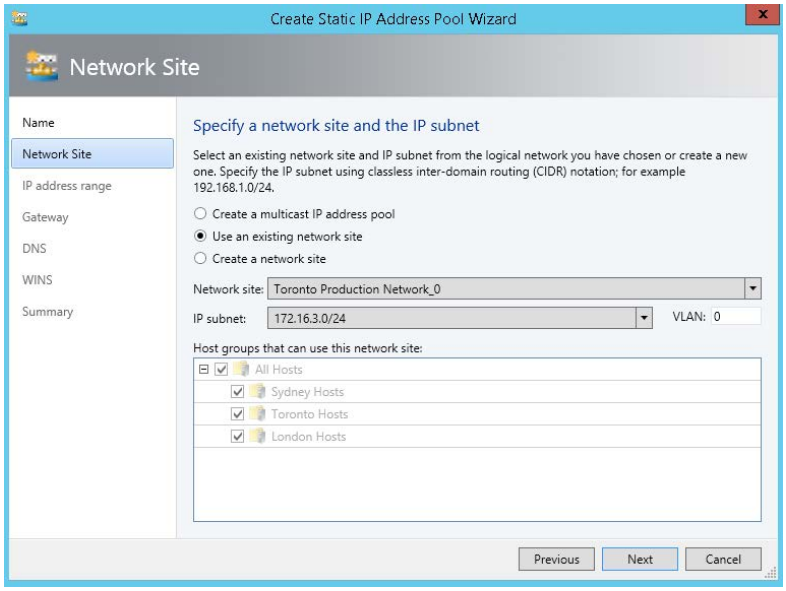
1. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric**, chọn **Create**, và chọn **IP Pool**.



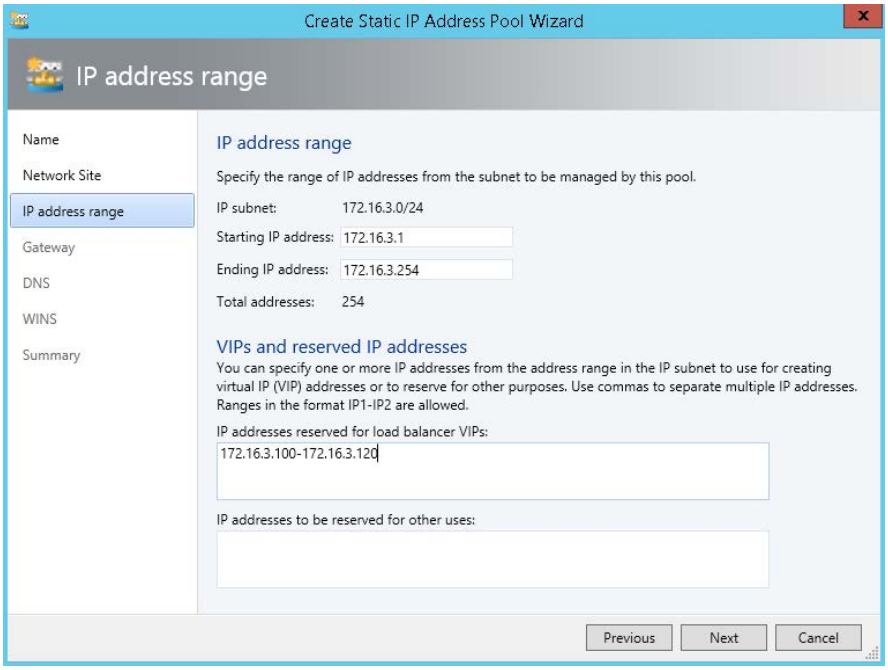
2. Cửa sổ **Name**, trong ô **Name**, nhập **Toronto Apps**, trong ô **Description**, nhập **Toronto Production Application IP Pool**. Bung ô **Logical network**, chọn **Toronto Production Network**, và chọn **Next**.



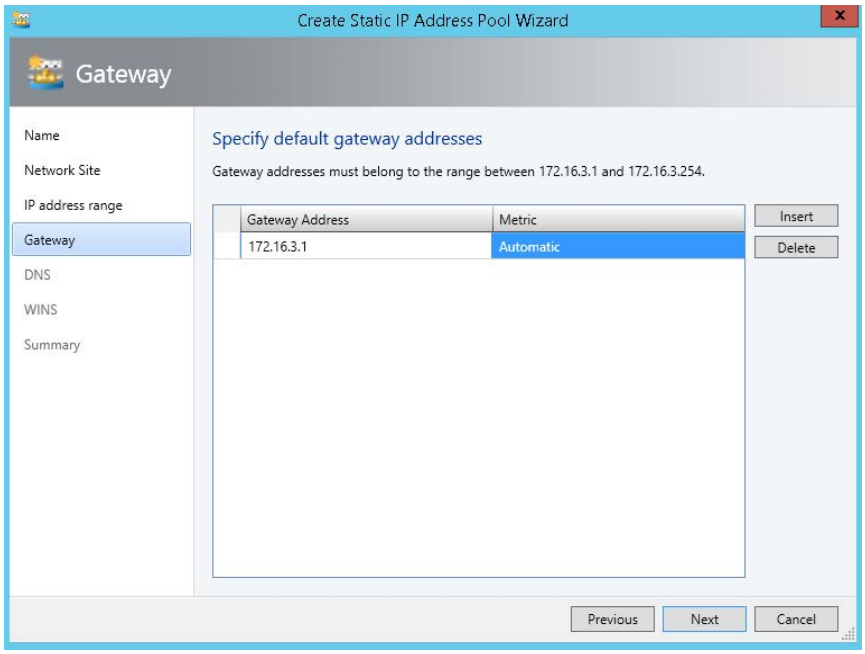

3. Cửa sổ **Network site**, chọn **Use an existing network site**, bung ô **Network site**, chọn **Toronto Production Network_0**, bung ô **IP subnet**, chọn **172.16.3.0/24**, và chọn **Next**.



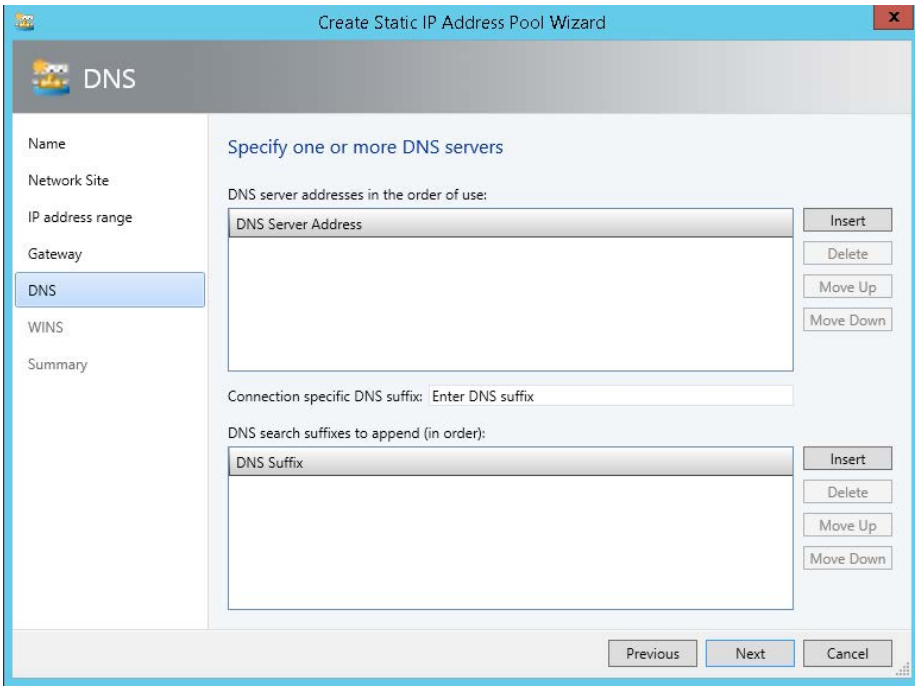
4. Cửa sổ **IP address range**, trong ô **VIPs and Reserved IP addresses**, nhập **172.16.3.100- 172.16.3.120**, chọn **Next**.



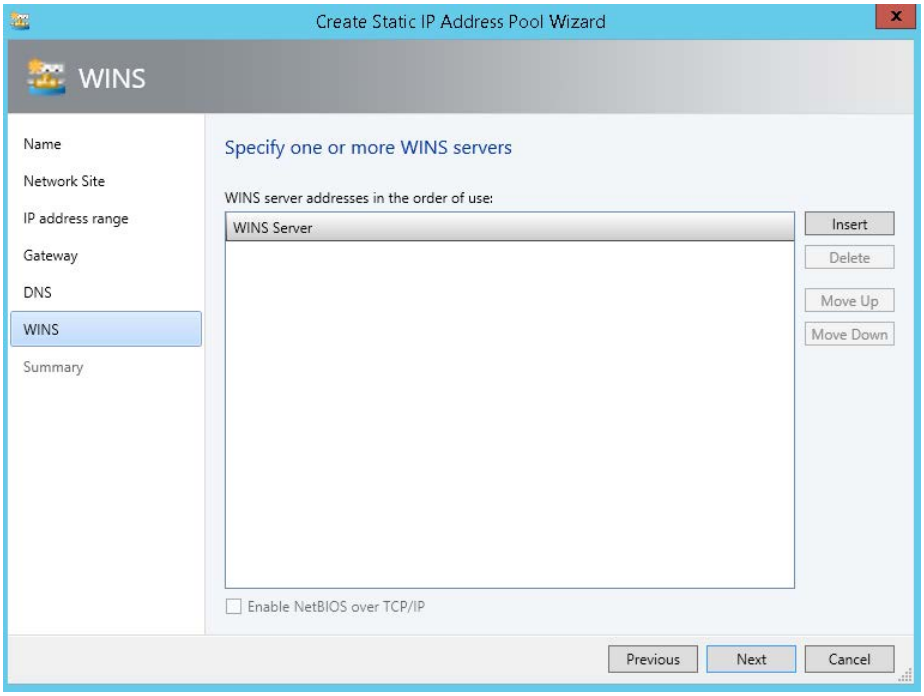

5. Cửa sổ **Gateway**, chọn **Insert**, trong ô **Gateway address**, nhập **172.16.3.1**, và chọn **Next**.



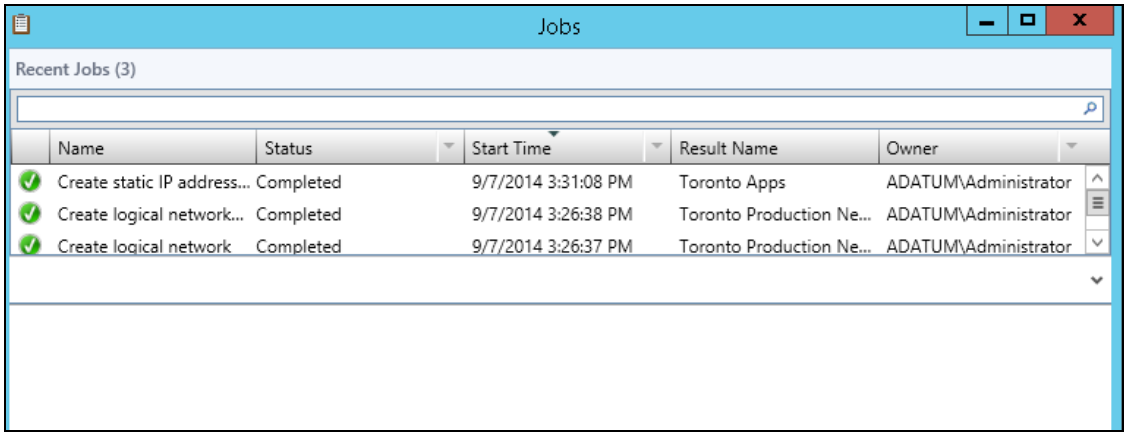
6. Cửa sổ **DNS**, chọn **Next.**




7. Cửa sổ **WINS**, chọn **Next**, và chọn **Finish**.

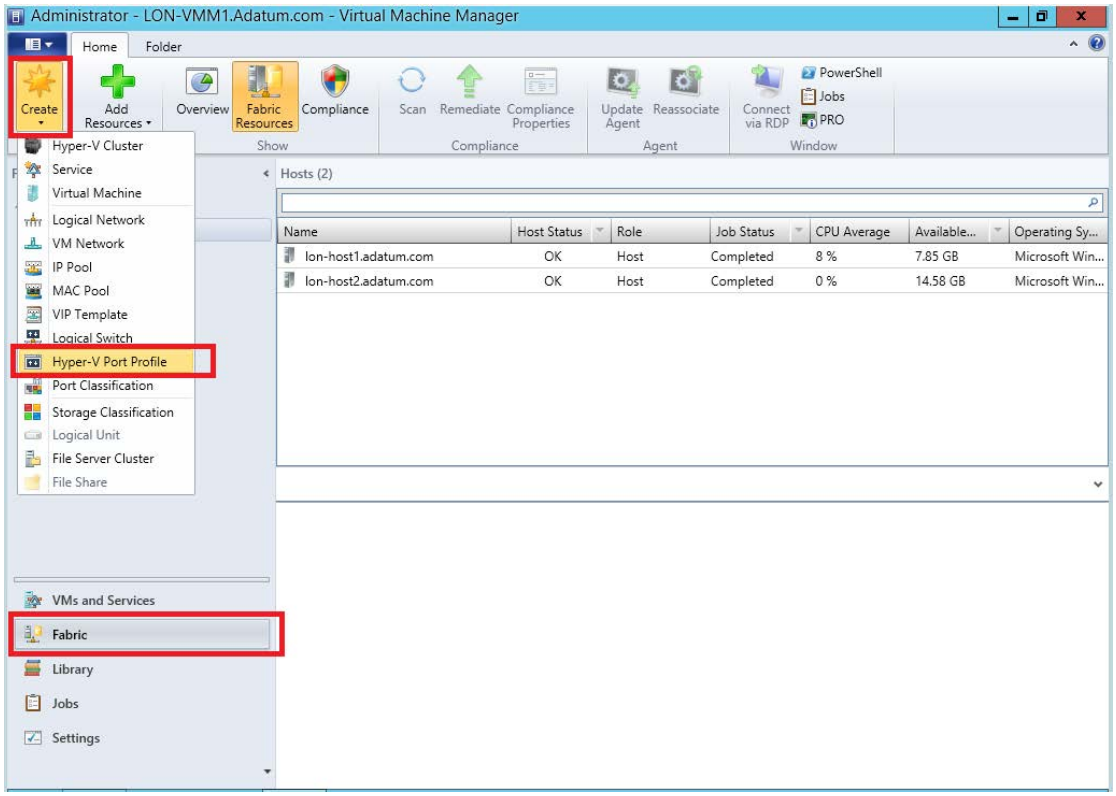


8. Tắt cửa sổ **Jobs**.

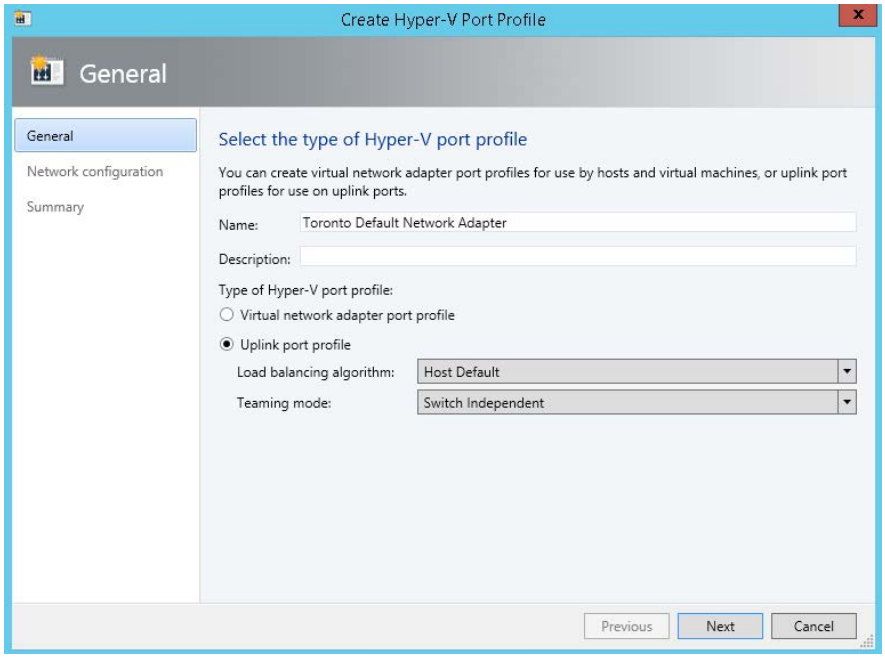



➢ **Tạo Native Port Profile**

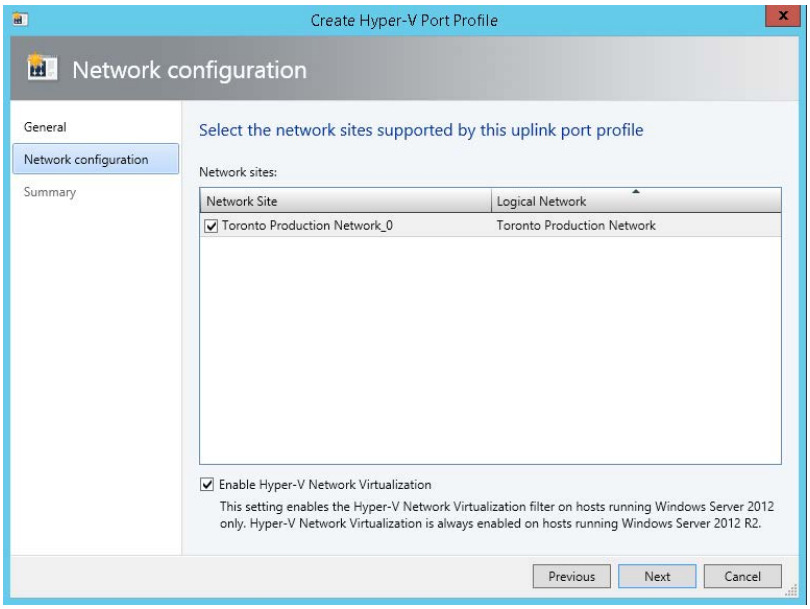
1. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric**, chọn **Create**, và chọn **Hyper-V Port Profile**.



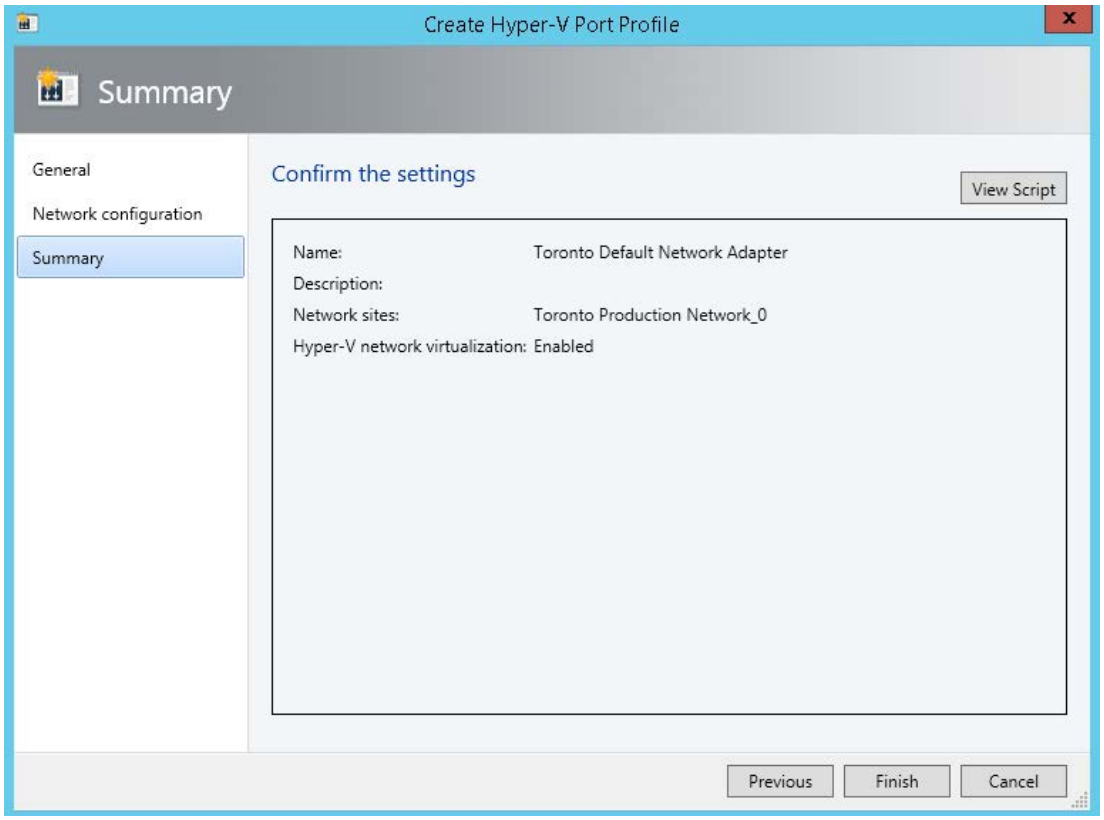
2. Cửa sổ **General**, trong ô **Name**, nhập **Toronto Default Network Adapter**, chọn **Uplink port profile**, và chọn **Next**.



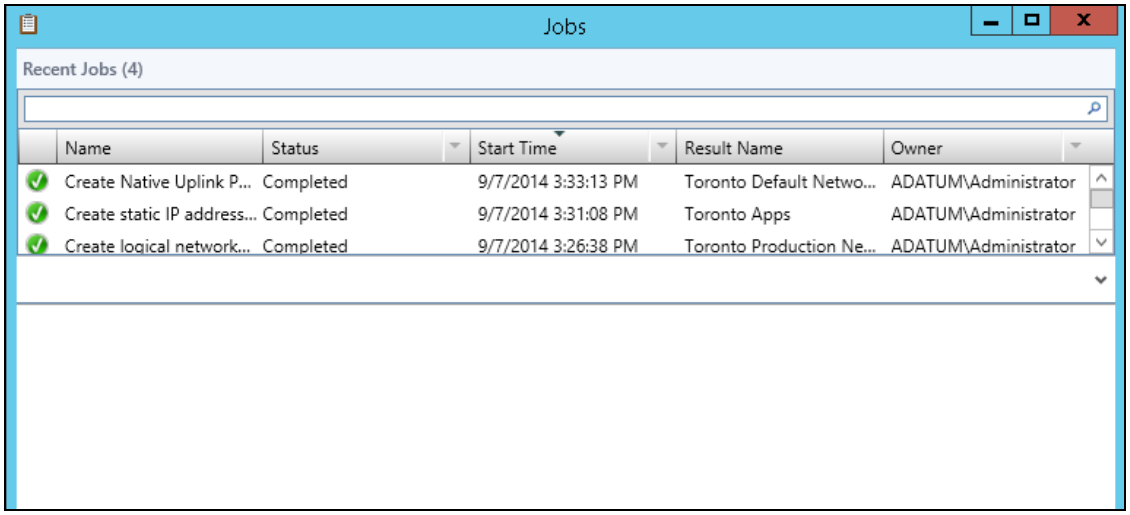

3. Cửa sổ **Network configuration**, đánh dấu chọn 2 ô **Toronto Production Network_0**, và **Enable Hyper-V Network Virtualization**, chọn **Next**.



4. Cửa sổ **Summary**, chọn **Finish**.

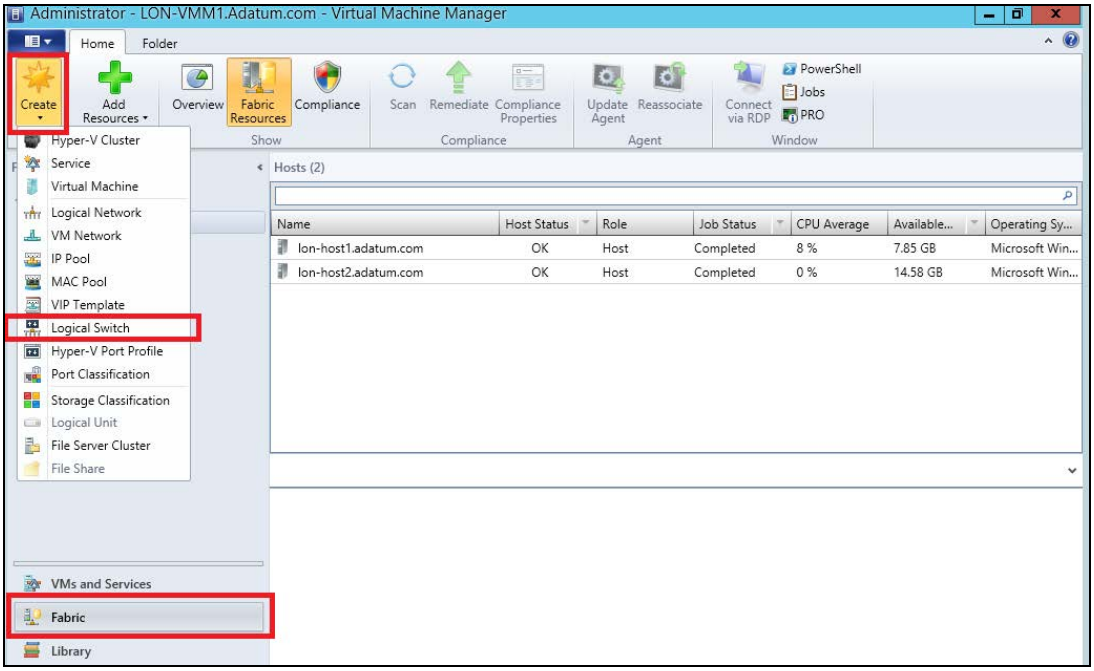



5. Tắt cửa sổ **Jobs**.

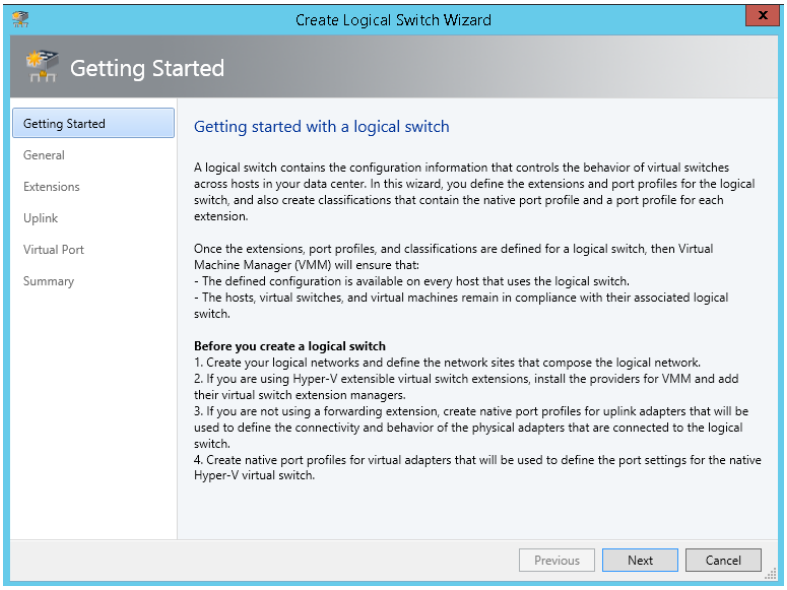


## ➢ Tạo Logical Switch

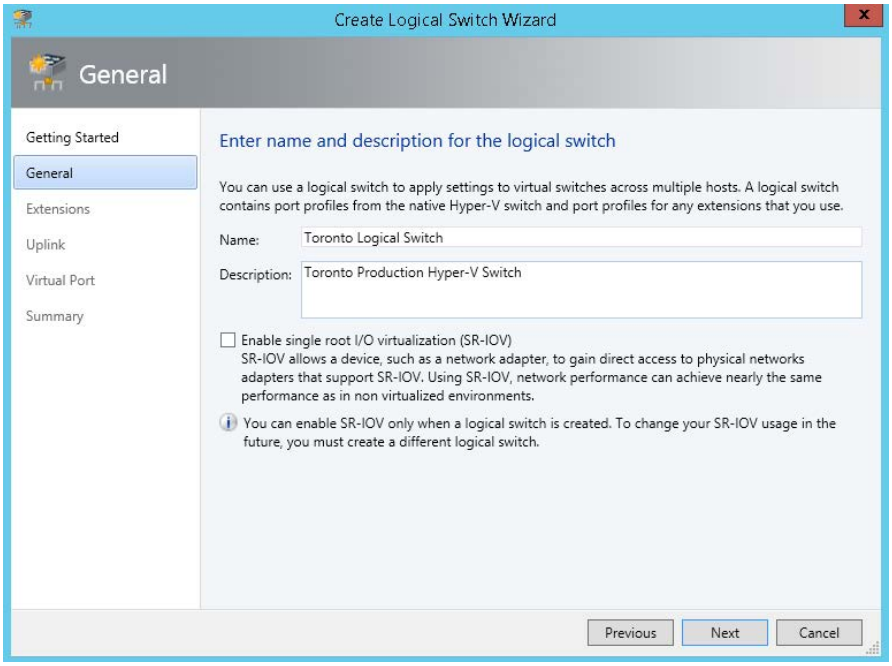
1. Trong cửa sổ **Virtual Machine Manager,** chọn **Fabric**, chọn **Create**, và chọn **Logical Switch**.



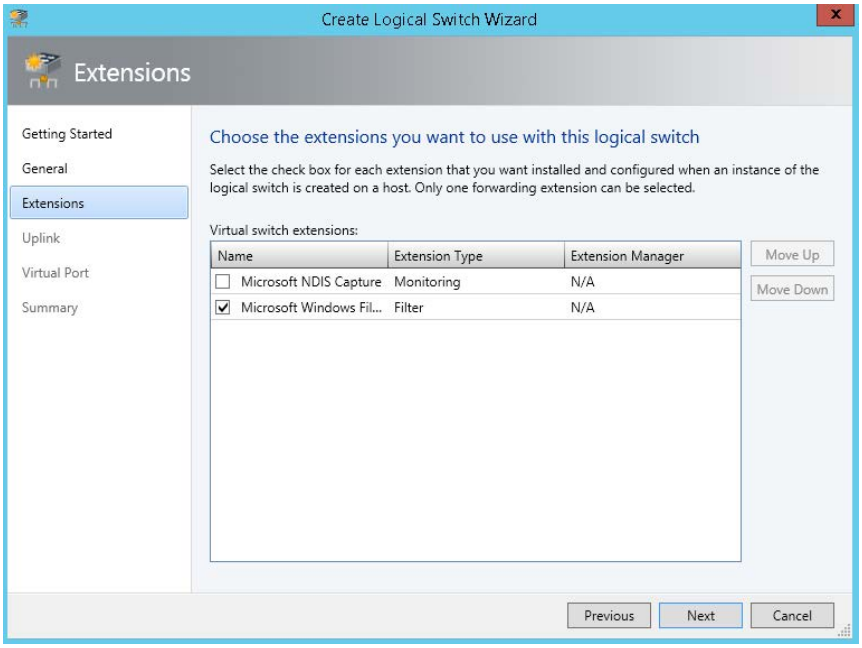

2. Cửa sổ **Getting Started** page, click **Next**.



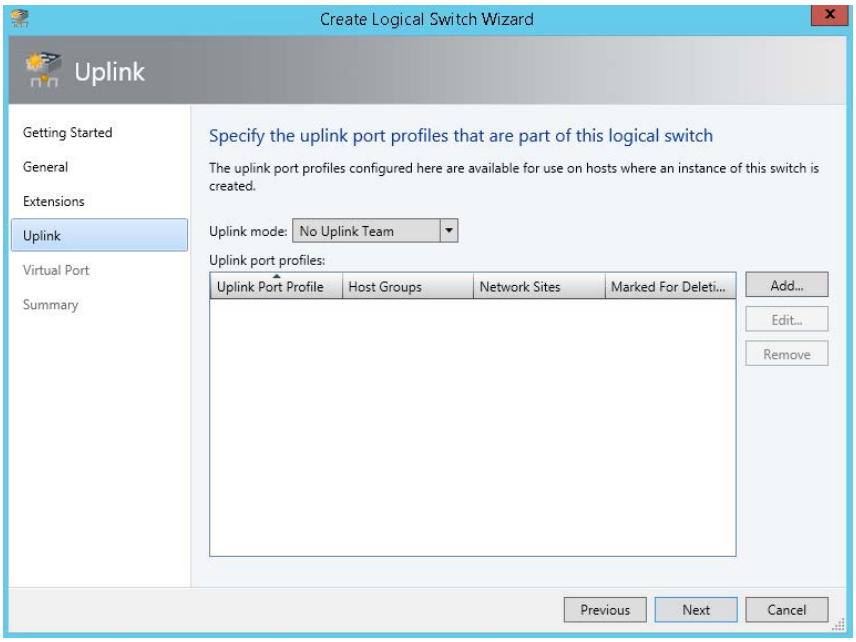
3. Cửa sổ **General**, trong ô **Name**, nhập **Toronto Logical Switch**, trong ô **Description**, nhập **Toronto Production Hyper-V Switch**, và chọn **Next**.



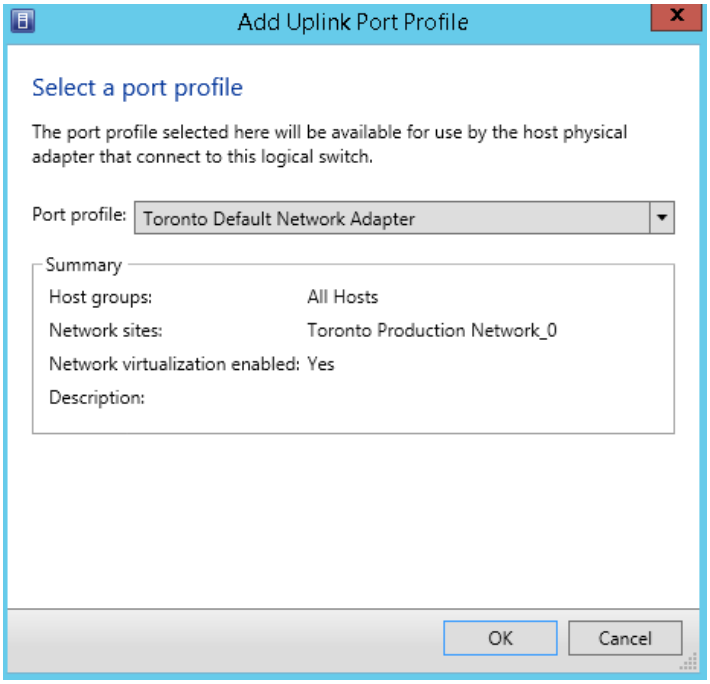

4. Cửa sổ **Extensions**, chọn **Next**.



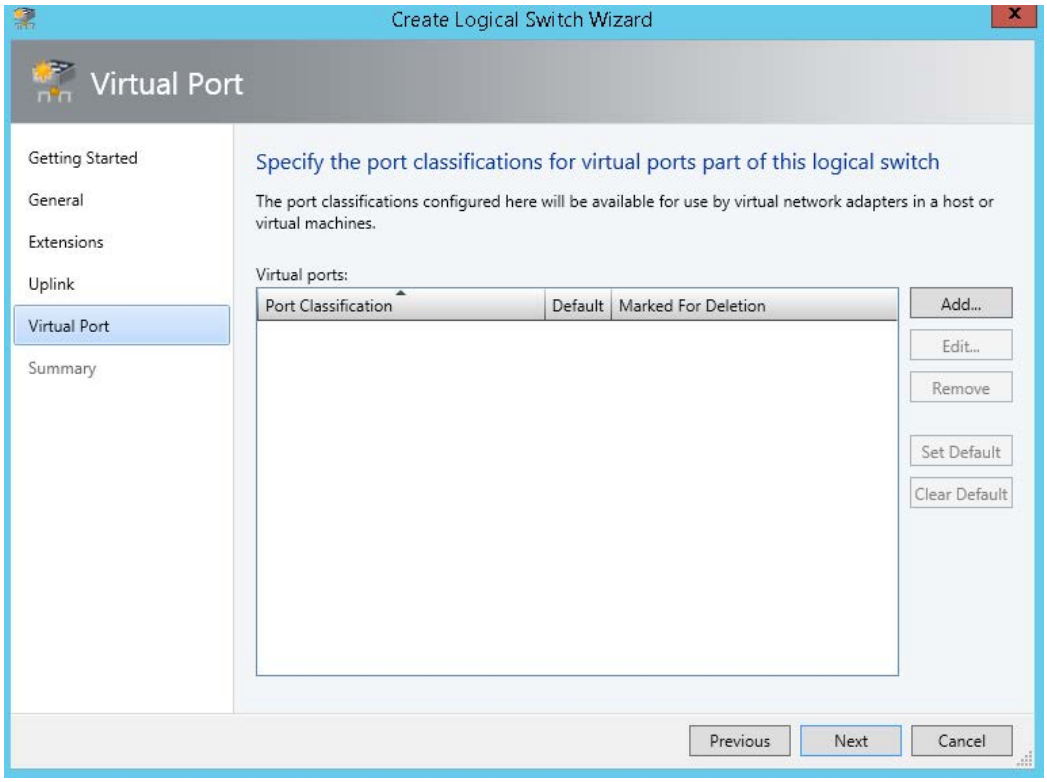
5. Cửa sổ **Uplink**, chọn **Add**.



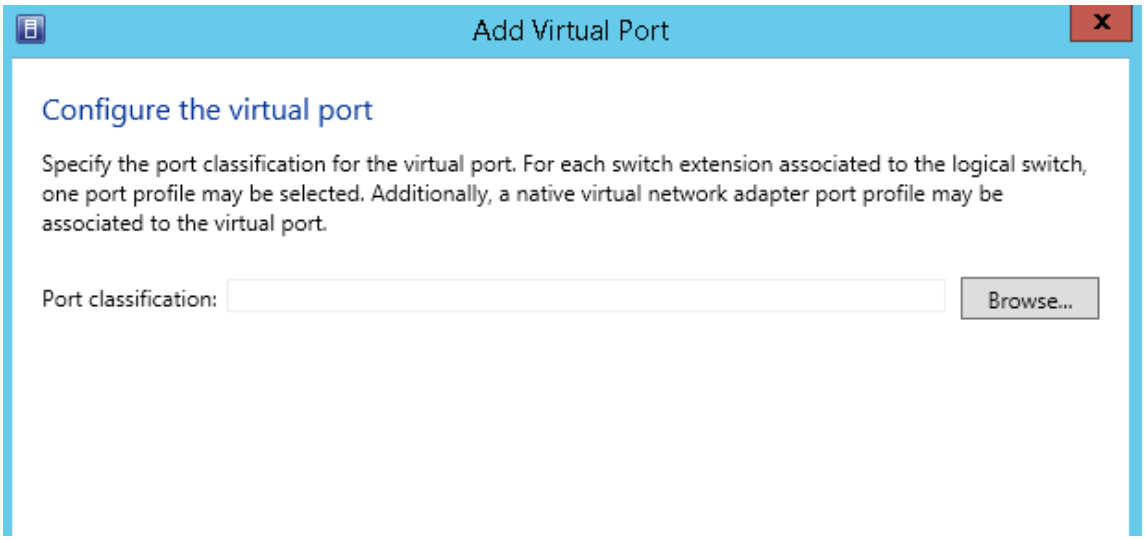

6. Hộp thoại **Add Uplink Port Profile,** bung ô **Port profile**, chọn **Toronto Default Network Adapter**, chọn **OK**, và chọn **Next**.



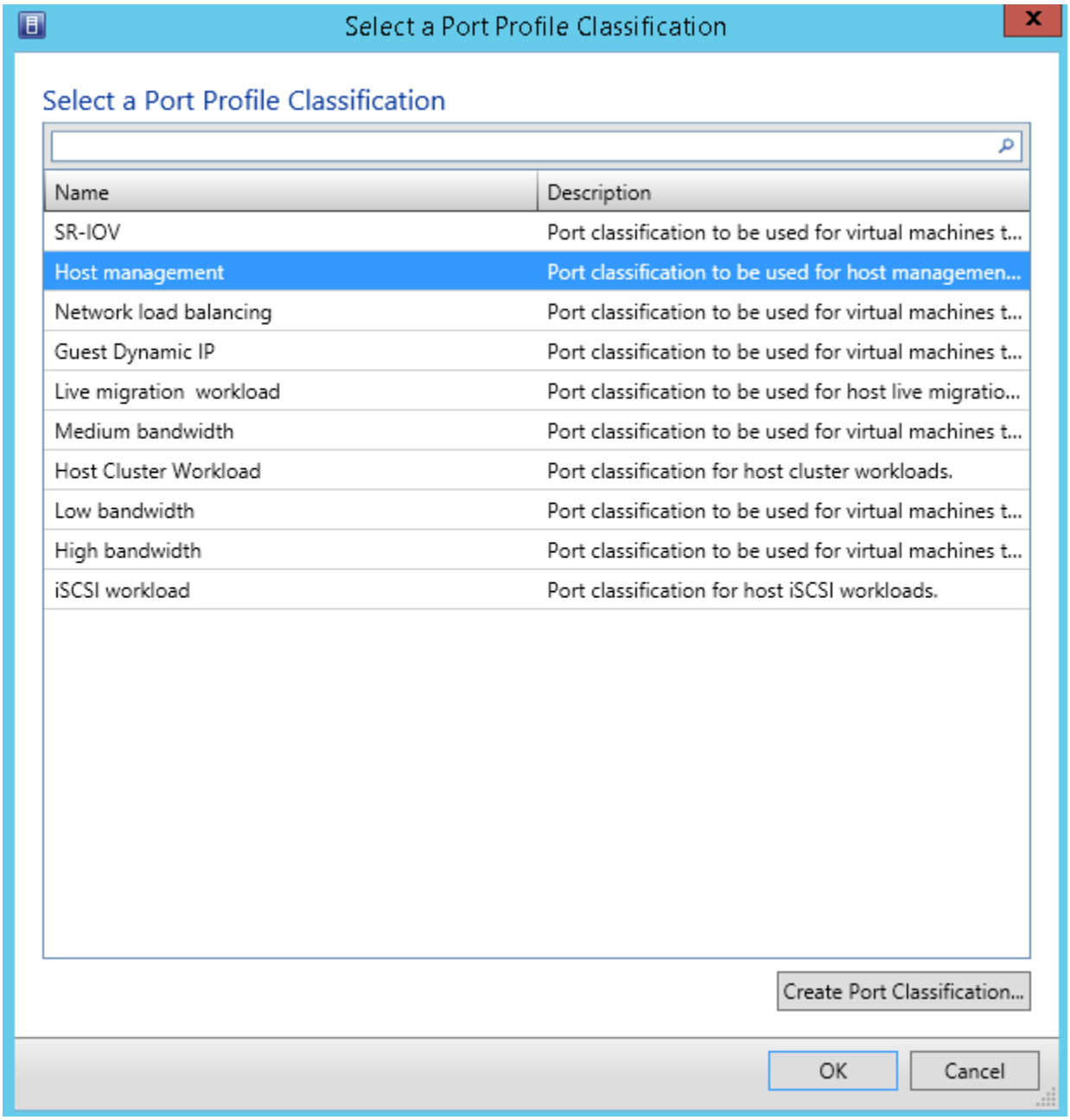
7. Cửa sổ **Virtual Port**, chọn **Add.**



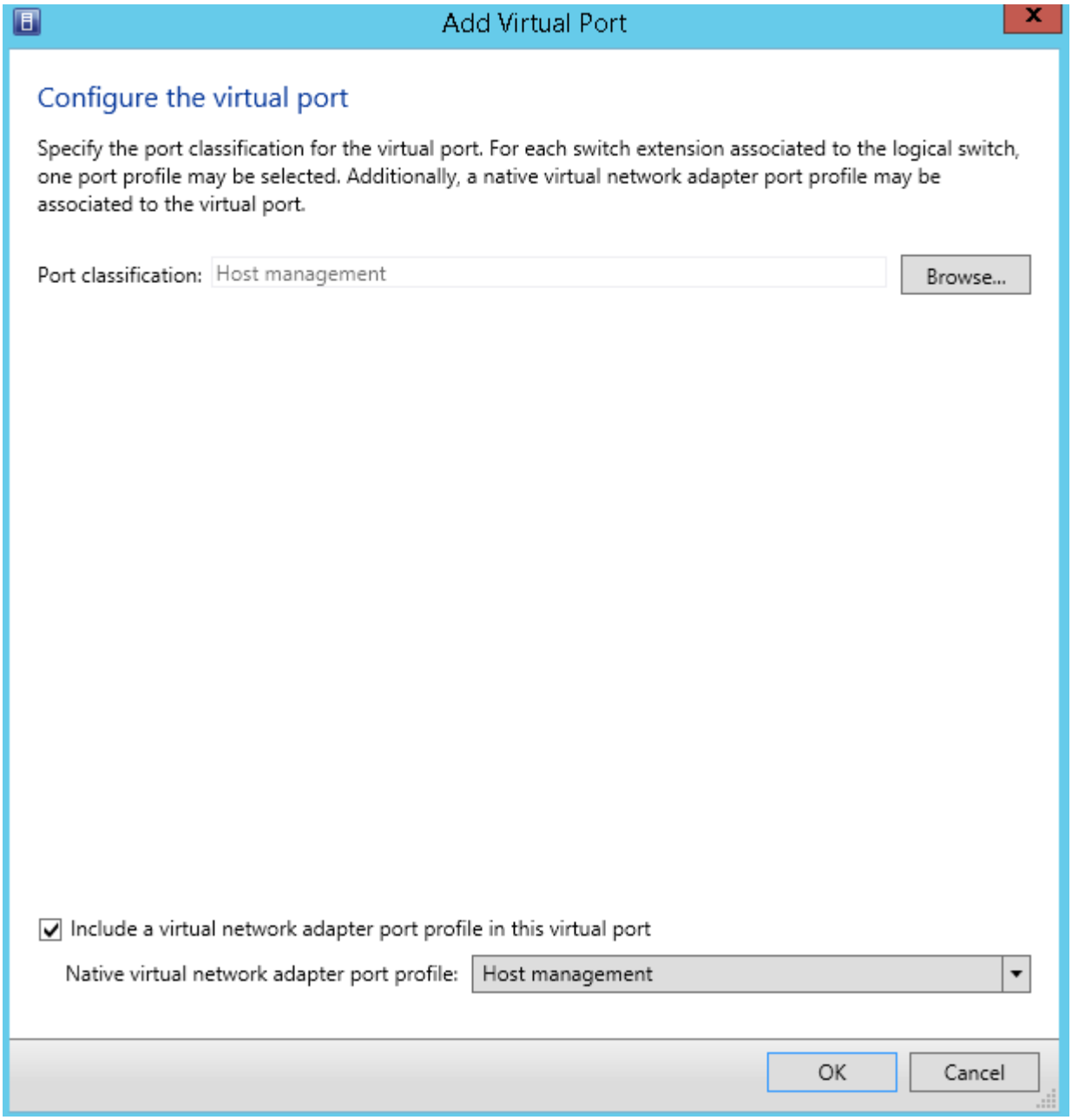

8. Hộp thoại **Add Virtual Port,** chọn **Browse**.



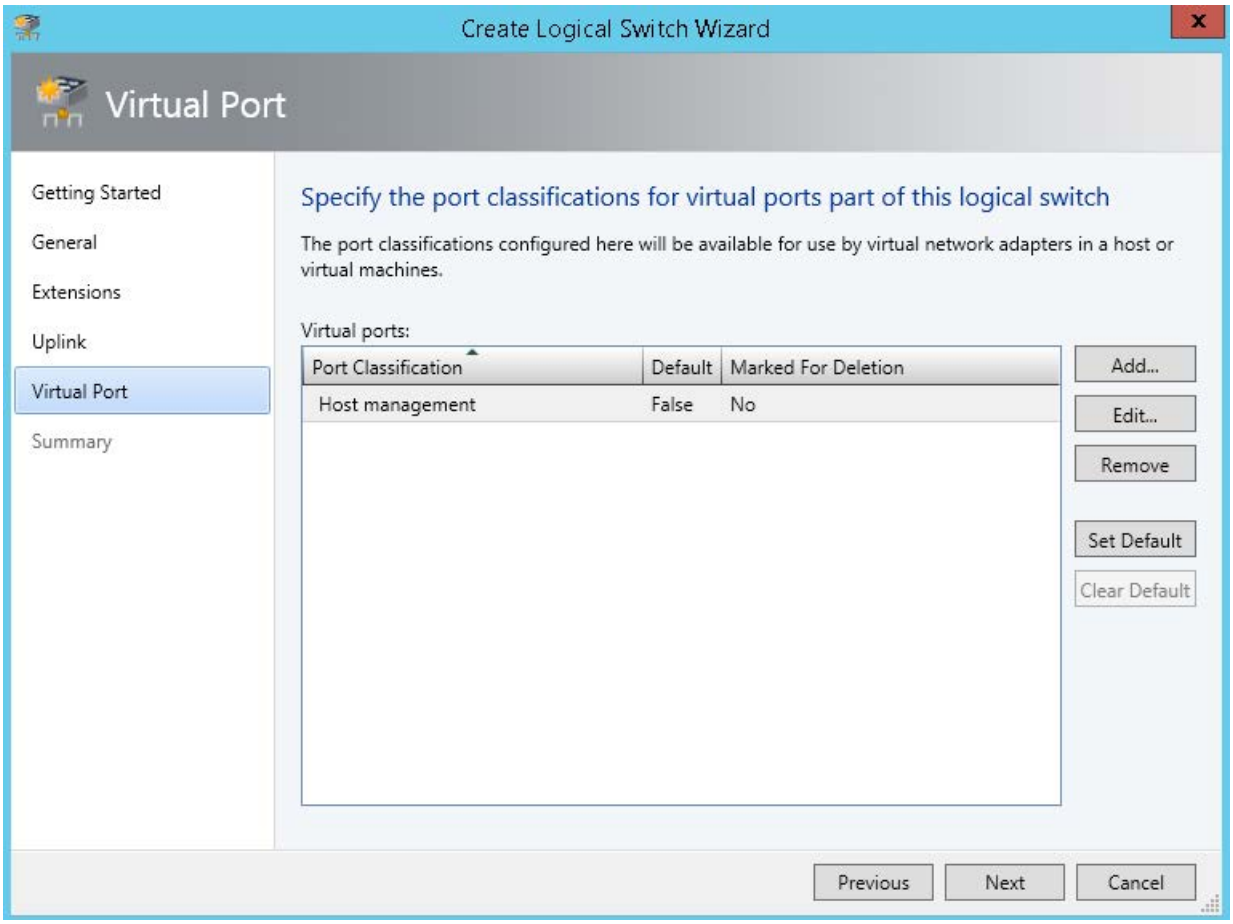
9. Chọn **Host management**, chọn **OK**.



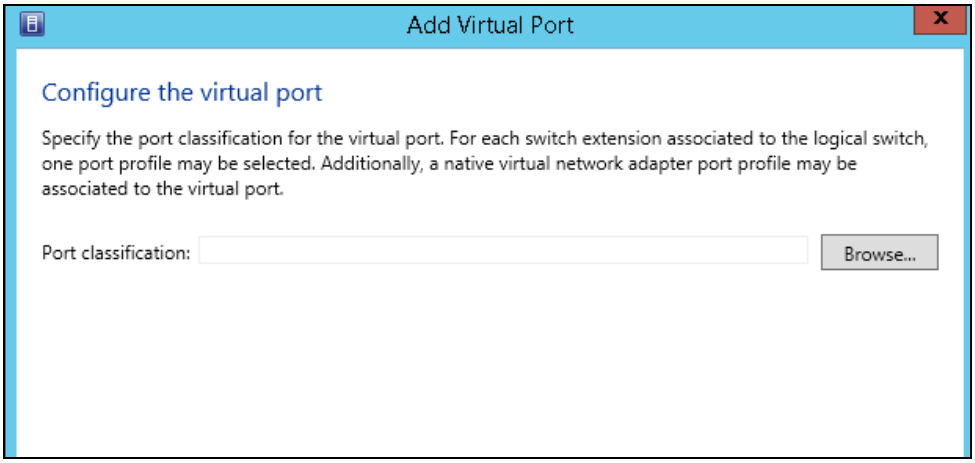
10. Hộp thoại **Add Virtual Port,** đánh dấu chọn **Include a virtual network adapter port profile in this virtual port**, bung ô **Native virtual network adapter port profile**, chọn **Host management**, và chọn **OK**.



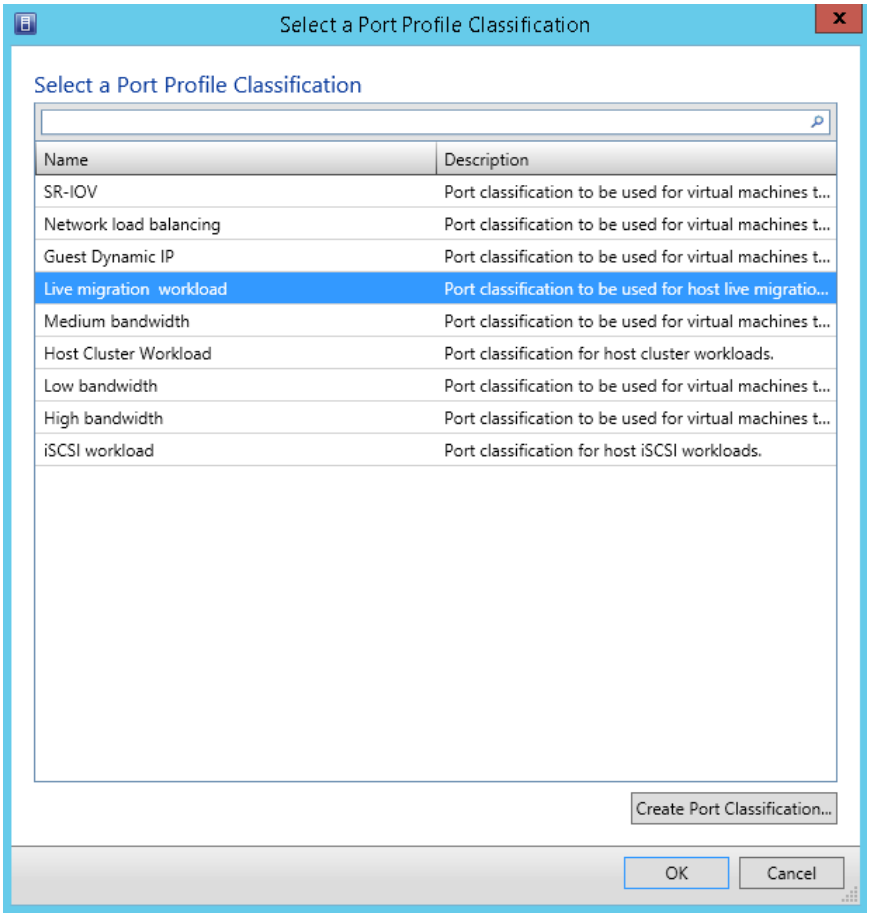
11. Cửa sổ **Virtual Port**, chọn **Add**.



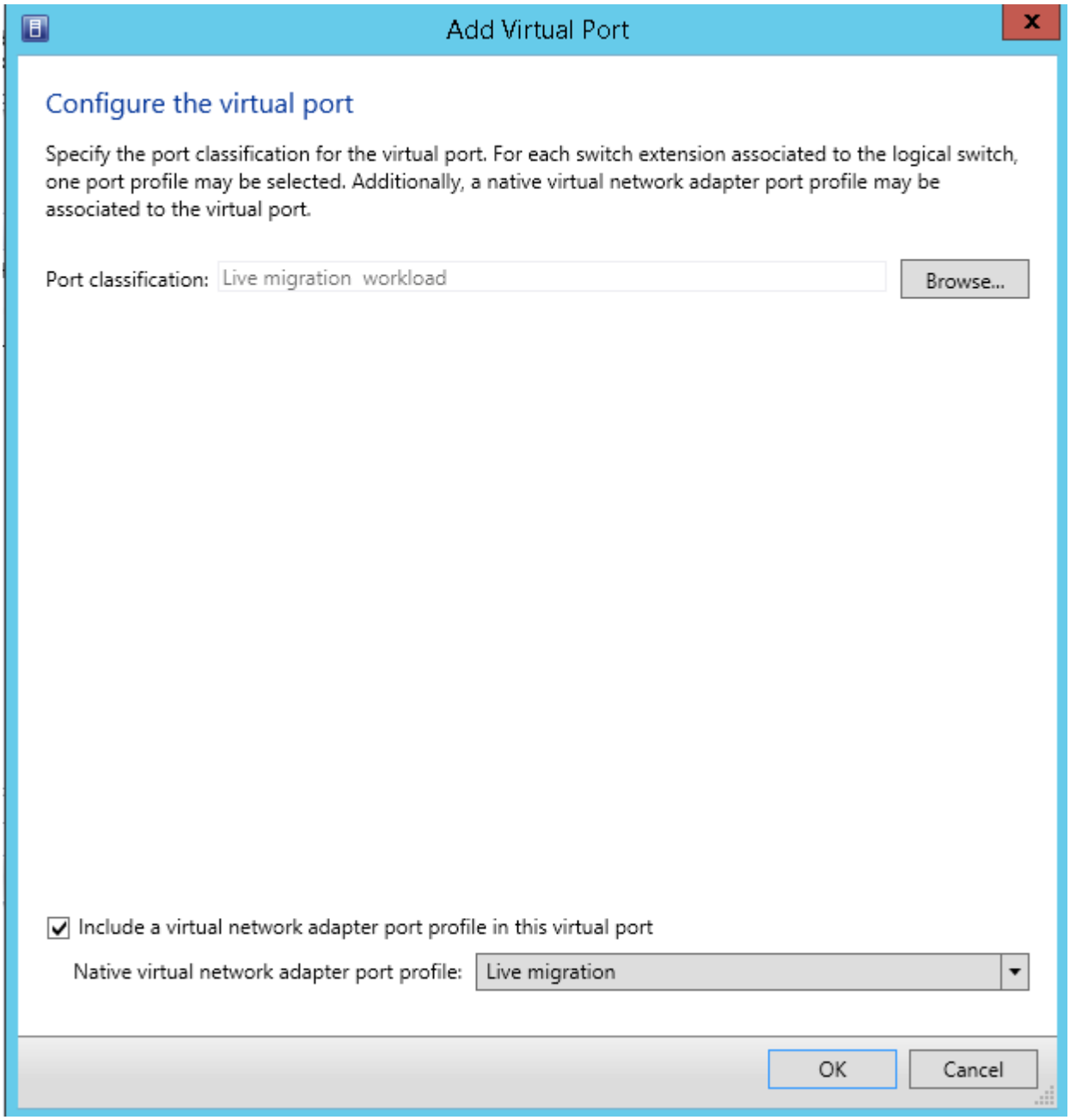
12. Hộp thoại **Add Virtual Port,** chọn **Browse**.



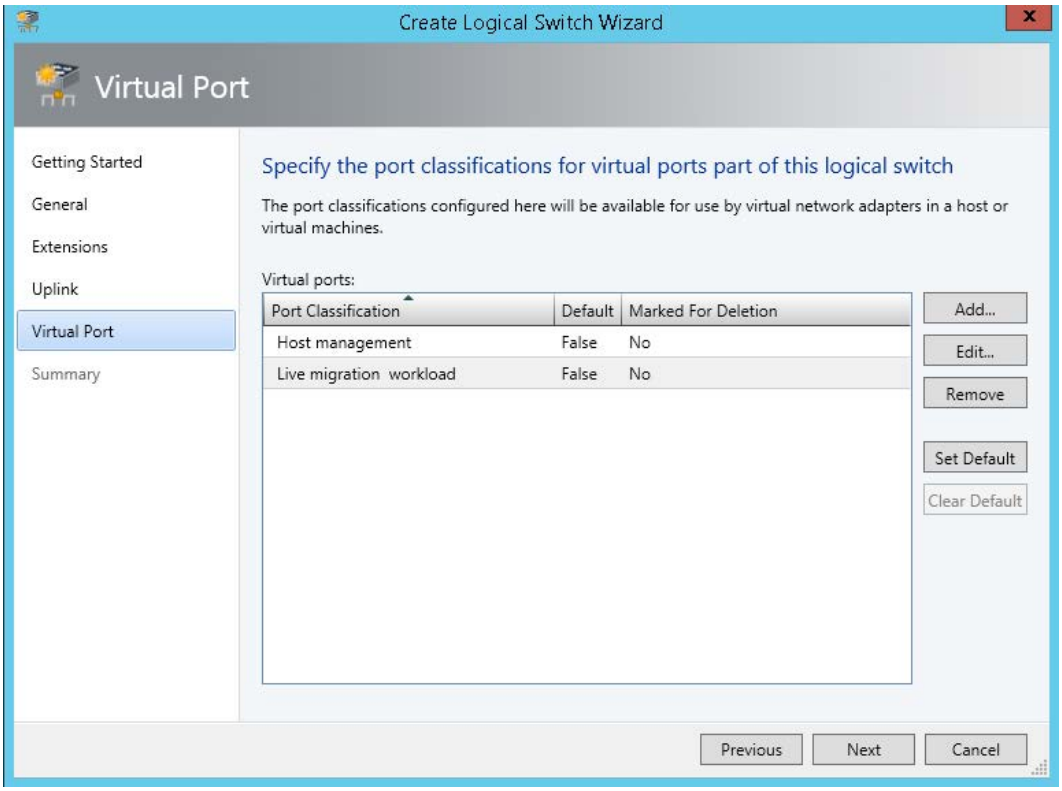

13. Chọn **Live migration workload**, chọn **OK.**



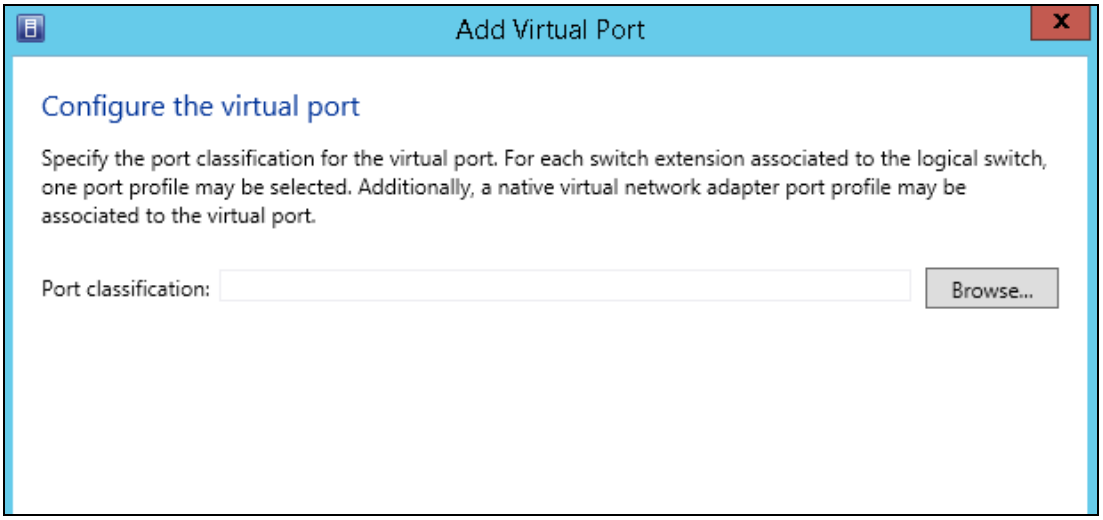
14. Hộp thoại **Add Virtual Port**, đánh dấu chọn **Include a virtual network adapter port profile in this virtual port**, bung ô **Native virtual network adapter port profile**, chọn **Live migration**, và chọn **OK**.



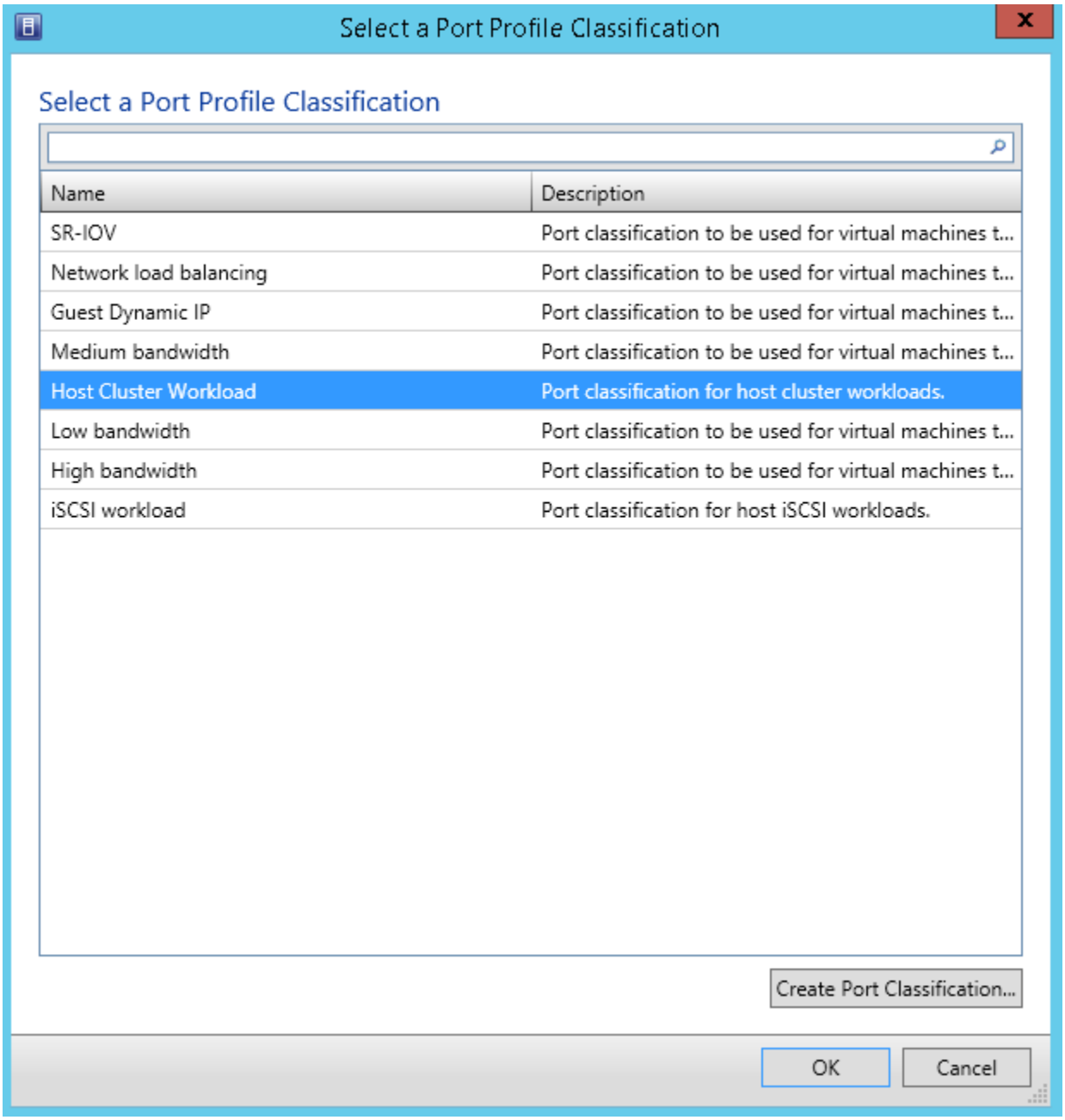
15. Cửa sổ **Virtual Port**, chọn **Add**.



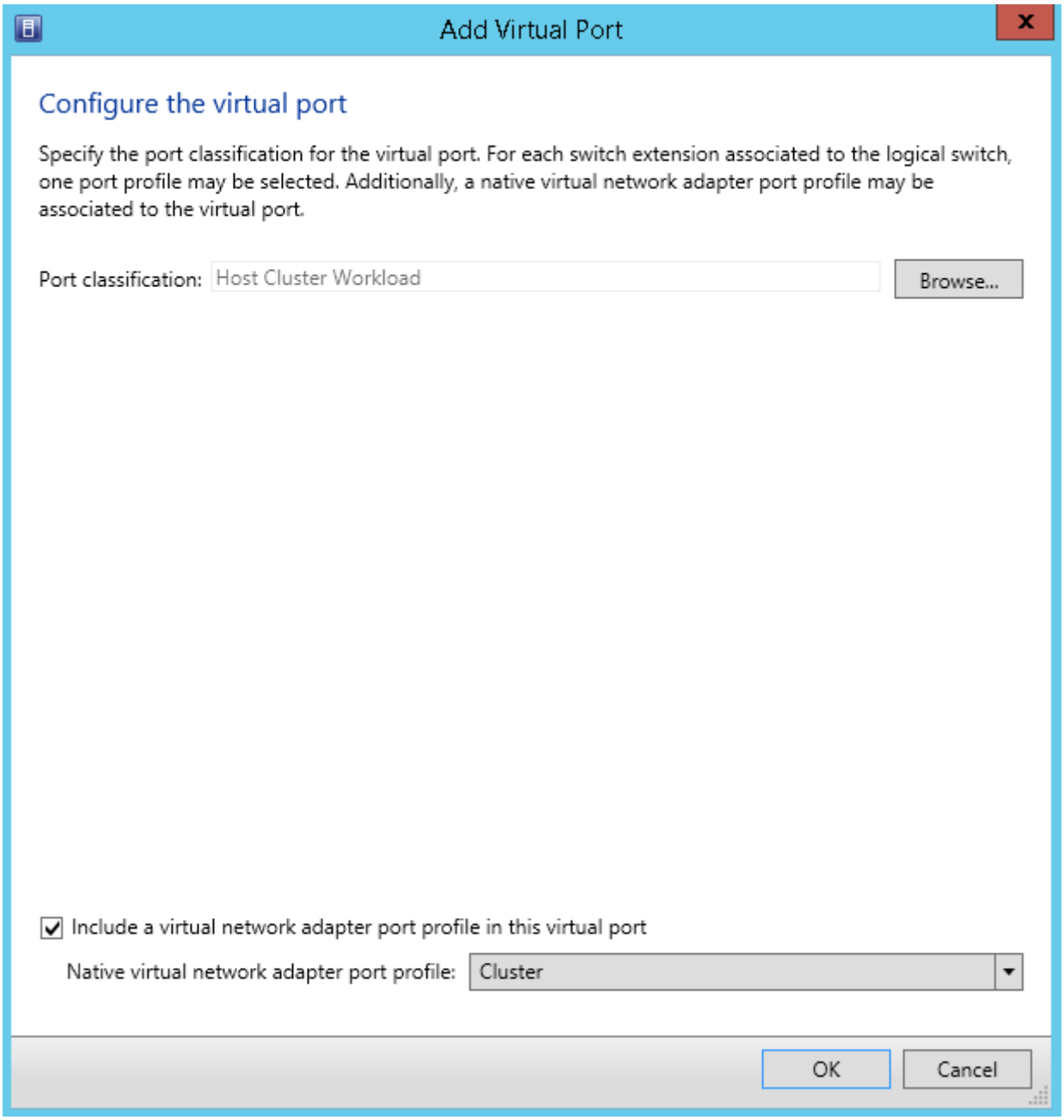

16. Hộp thoại **Add Virtual Port,** chọn **Browse**.



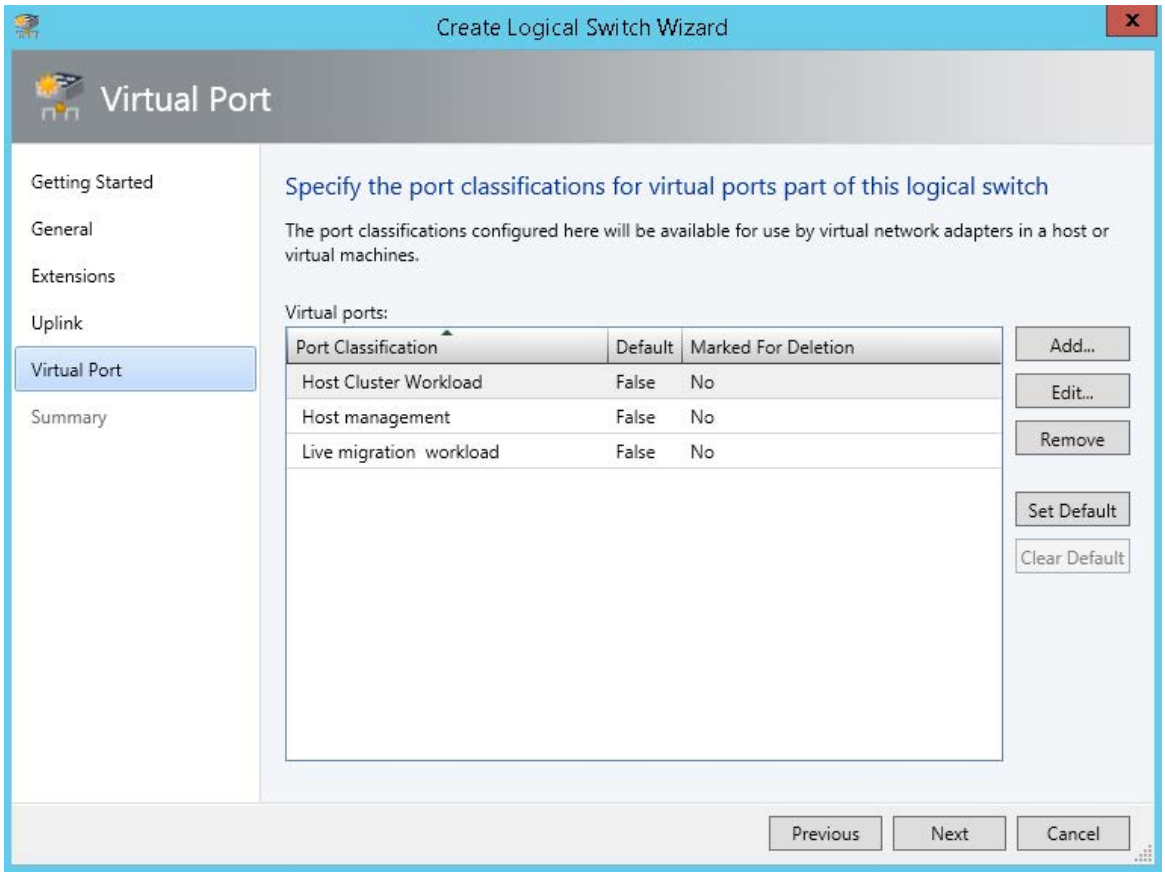
17. Chọn **Host Cluster Workload**, chọn **OK.**



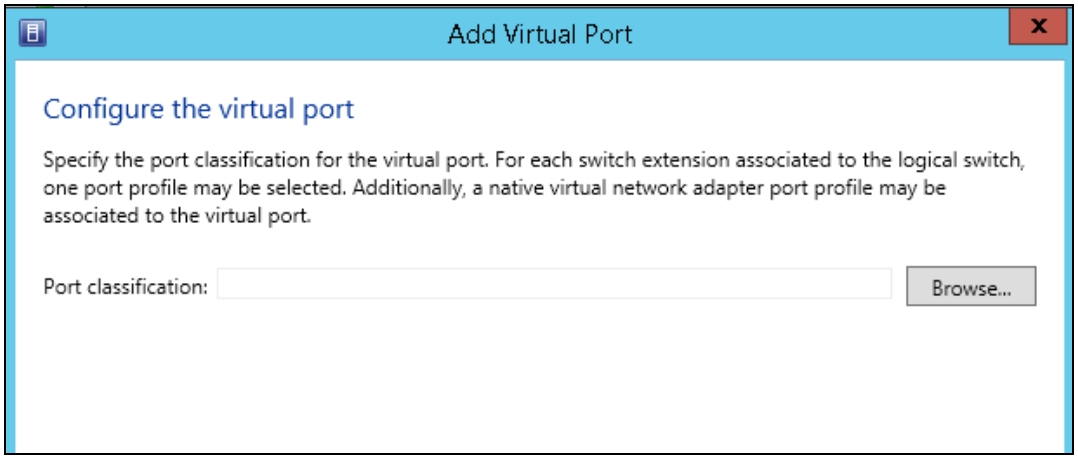
18. Hộp thoại **Add Virtual Port**, đánh dấu chọn **Include a virtual network adapter port profile in this virtual port**, bung ô **Native virtual network adapter port profile**, chọn **Cluster**, và chọn **OK**.



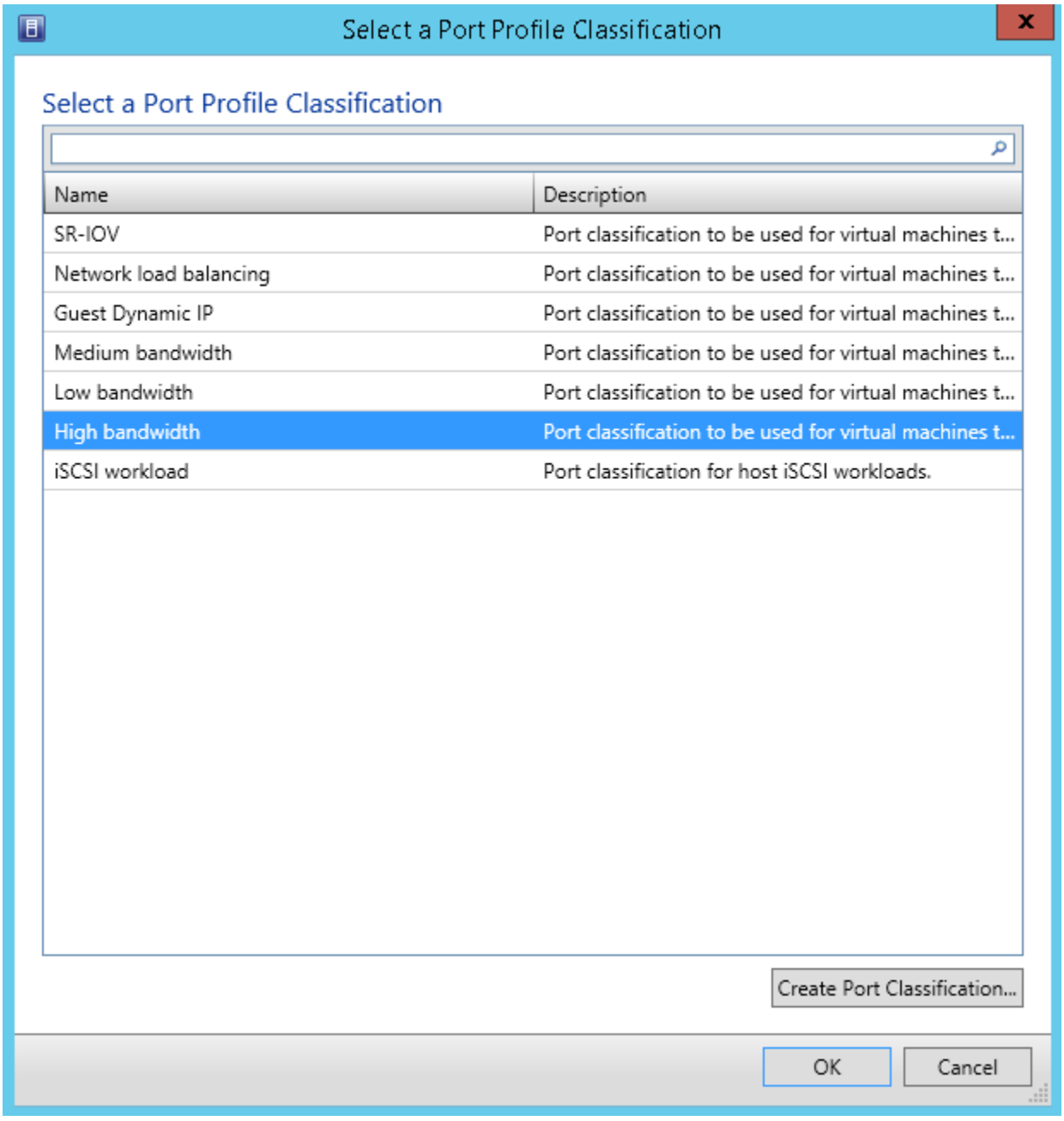
19. Cửa sổ **Virtual Port**, chọn **Add**.



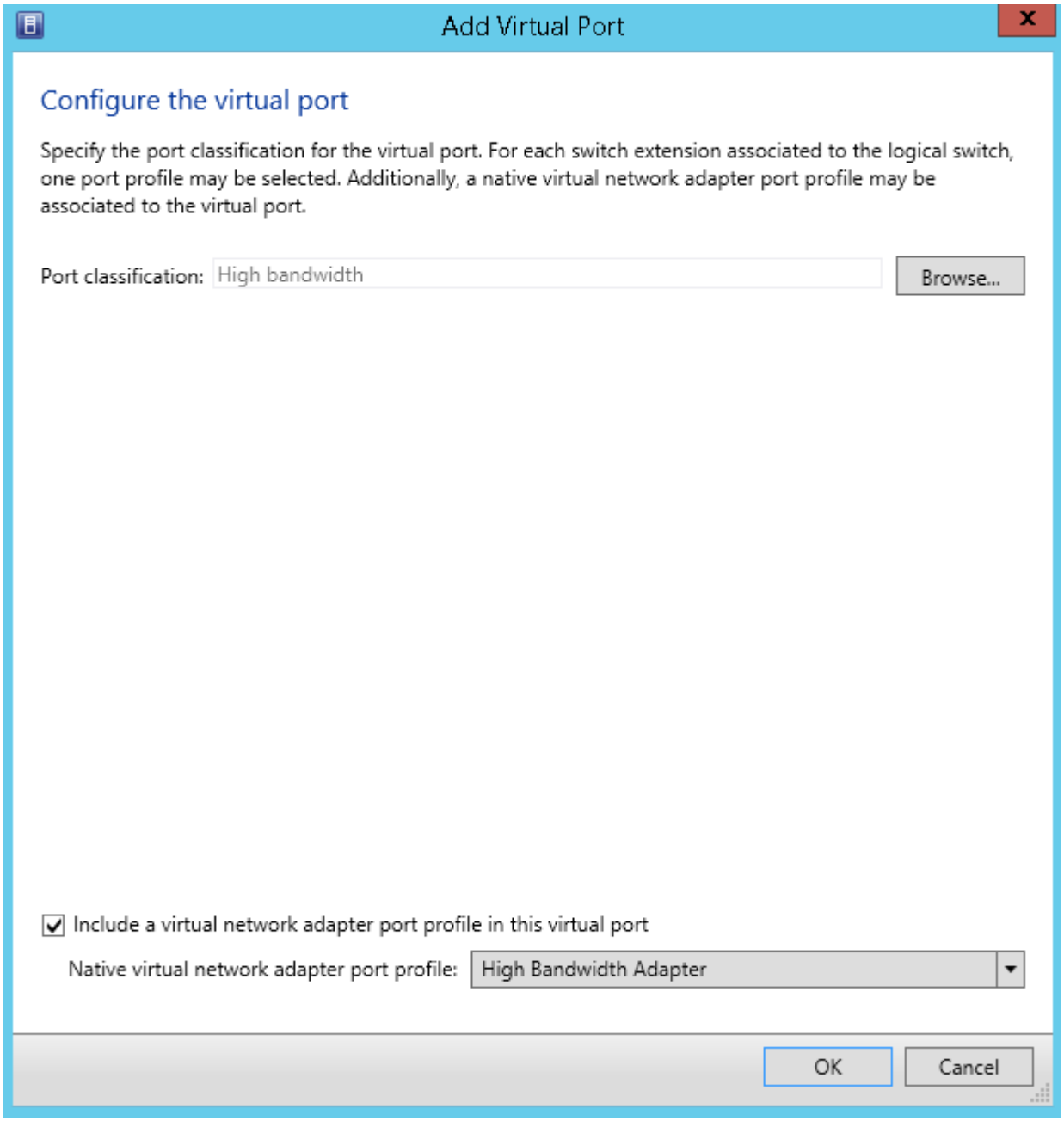

20. Hộp thoại **Add Virtual Port,** chọn **Browse**.



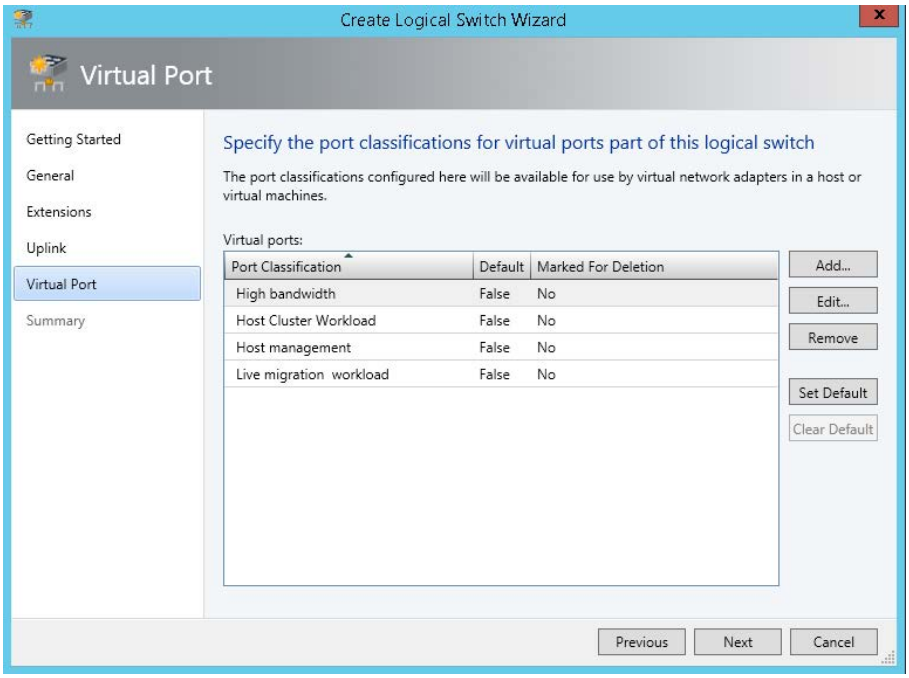
21. Chọn **High bandwidth**, chọn **OK**.



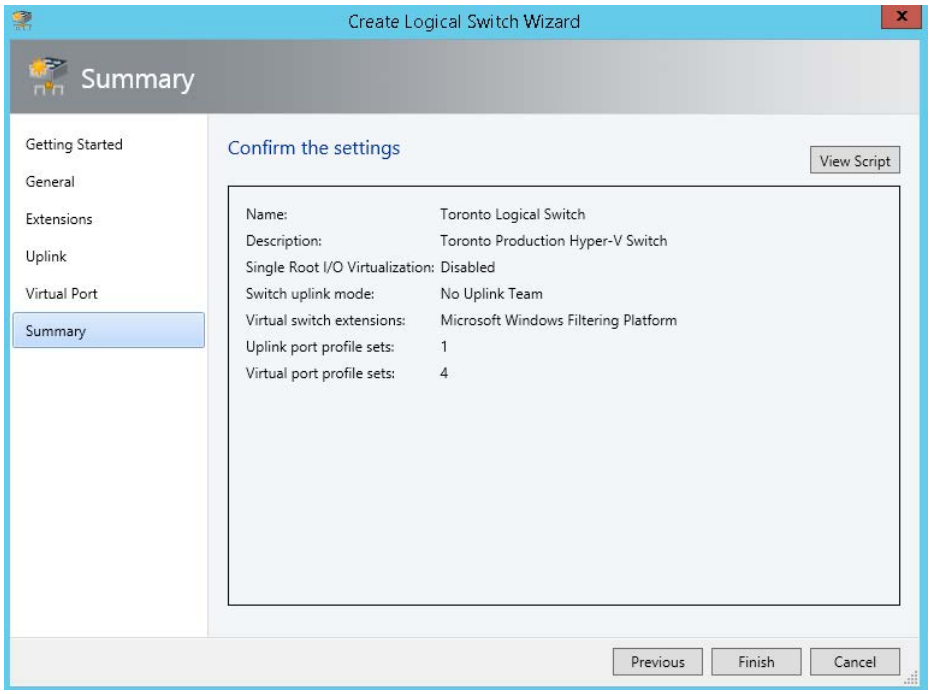
22. Hộp thoại **Add Virtual Port,** đánh dấu chọn **Include a virtual network adapter port profile in this virtual port**, bung ô **Native virtual network adapter port profile**, chọn **High bandwidth adapter**, và chọn **OK**.



23. Cửa sổ **Virtual Port**, chọn **Next**.



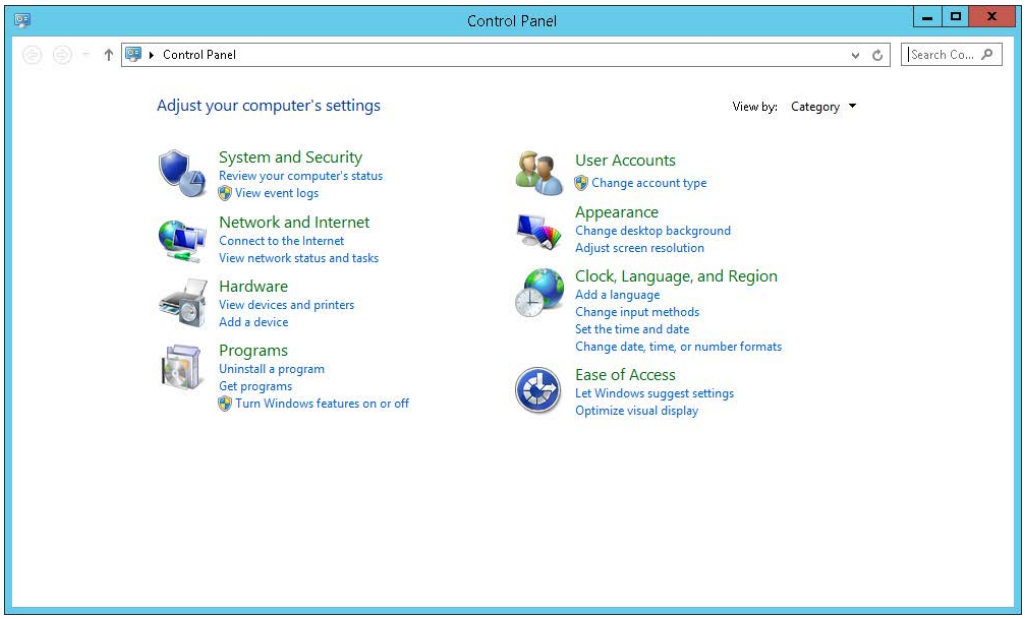

24. Cửa sổ **Summary**, chọn **Finish**. Tắt cửa sổ **Jobs**.



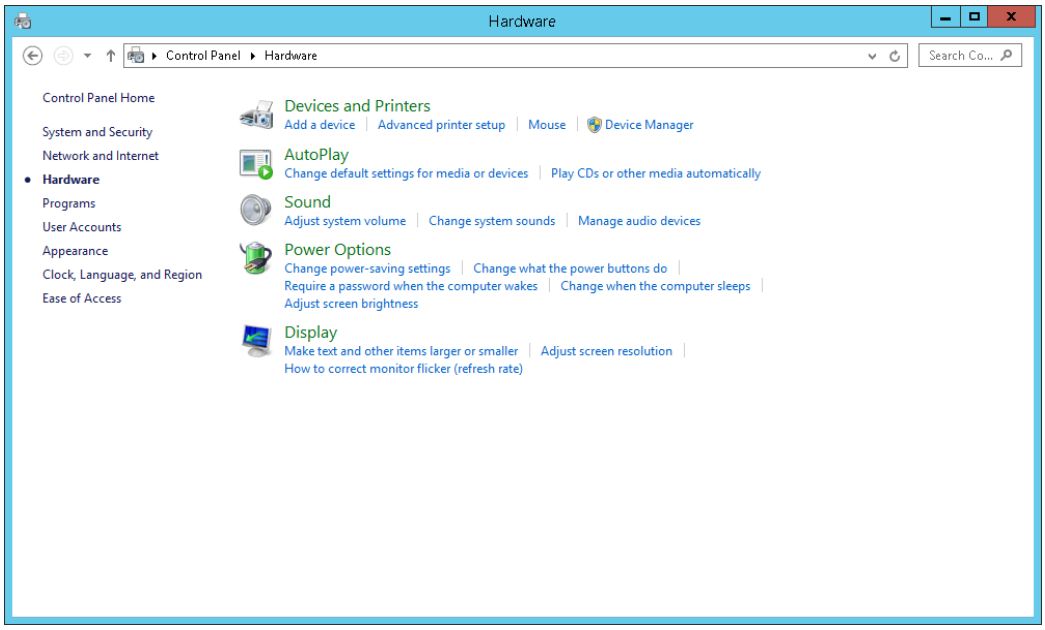
➢ **Cài đặt card Microsoft Loopback**

1. Qua máy **LON-HOST1** (Máy thật), mở **Control Panel**

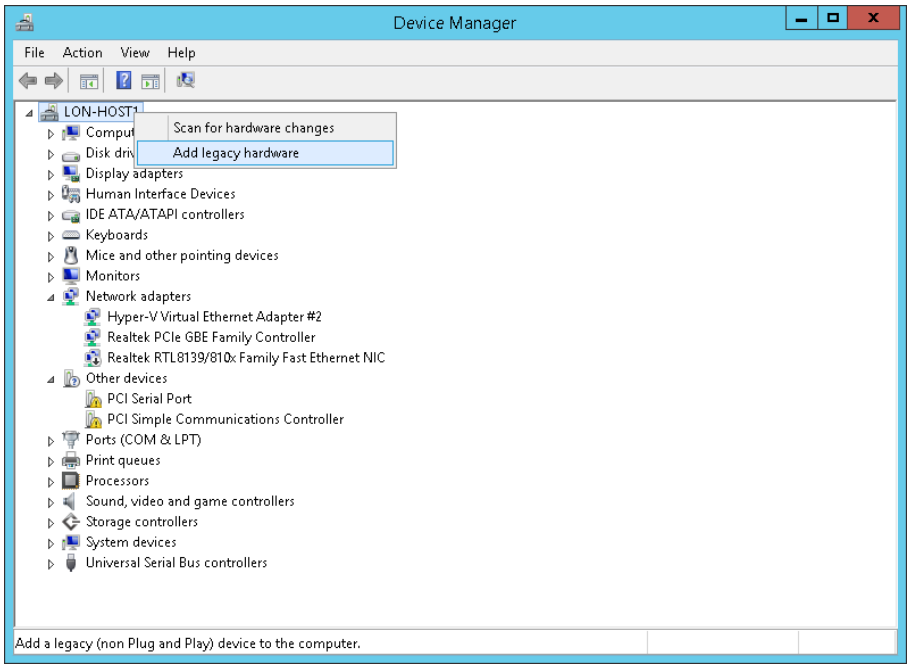
2. Trong cửa sổ **Control Panel**, chọn **Hardware**.



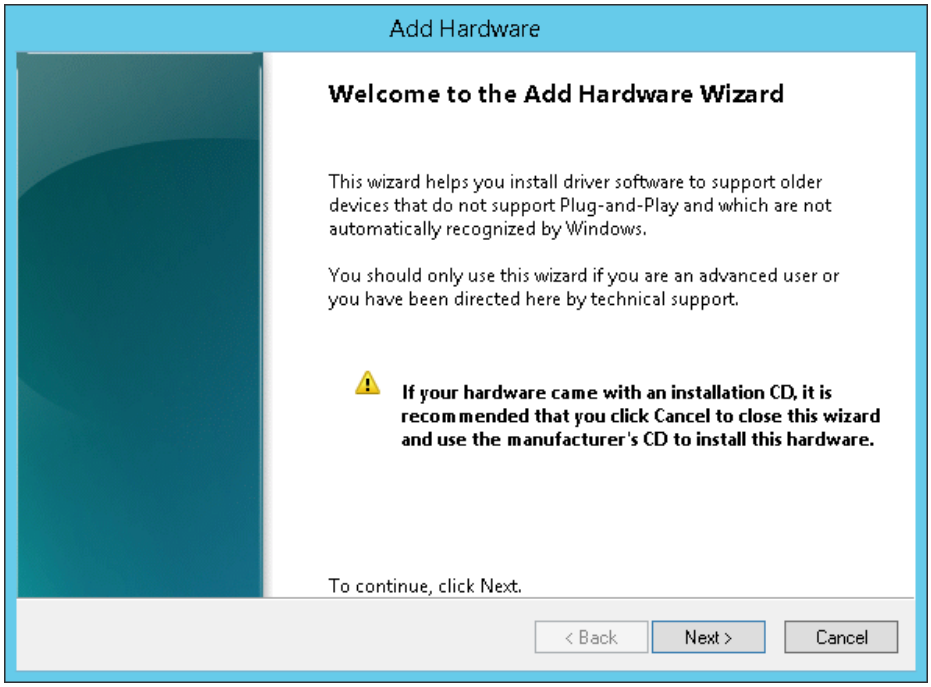

3. Cửa sổ **Hardware**, chọn **Device Manager**.



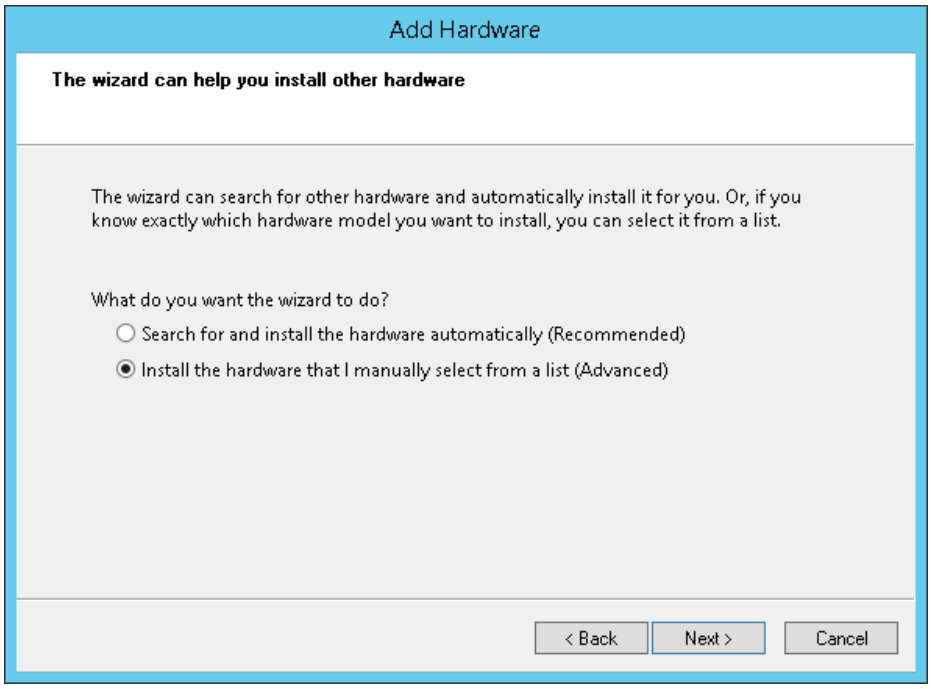
4. Cửa sổ **Device Manager**, chuột phải **LON-HOST1**, chọn **Add legacy hardware.**



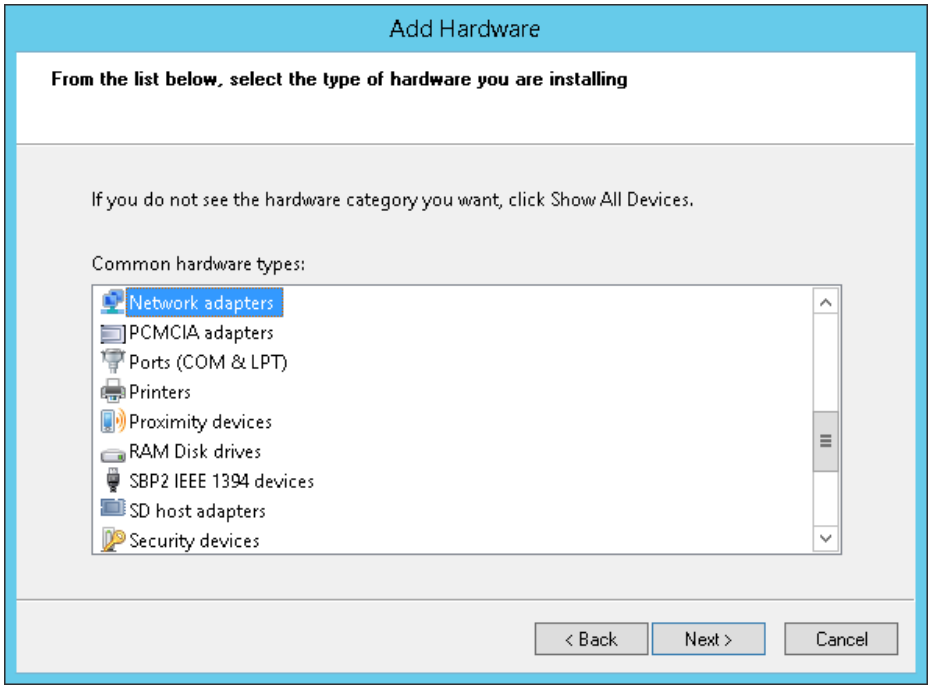

5. Cửa sổ **Welcome**, chọn **Next**.



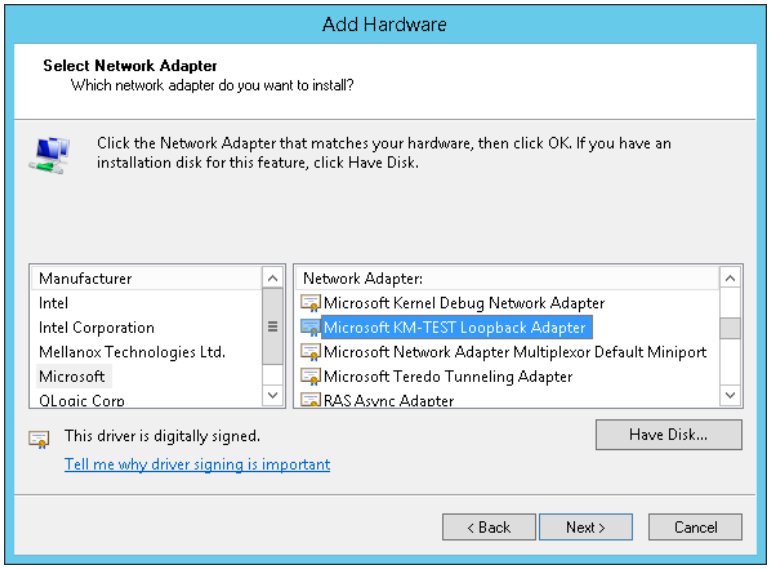
6. Chọn **Install the hardware that I manually select from a list**, và chọn **Next**.




7. Chọn **Network adapters**, và chọn **Next**.



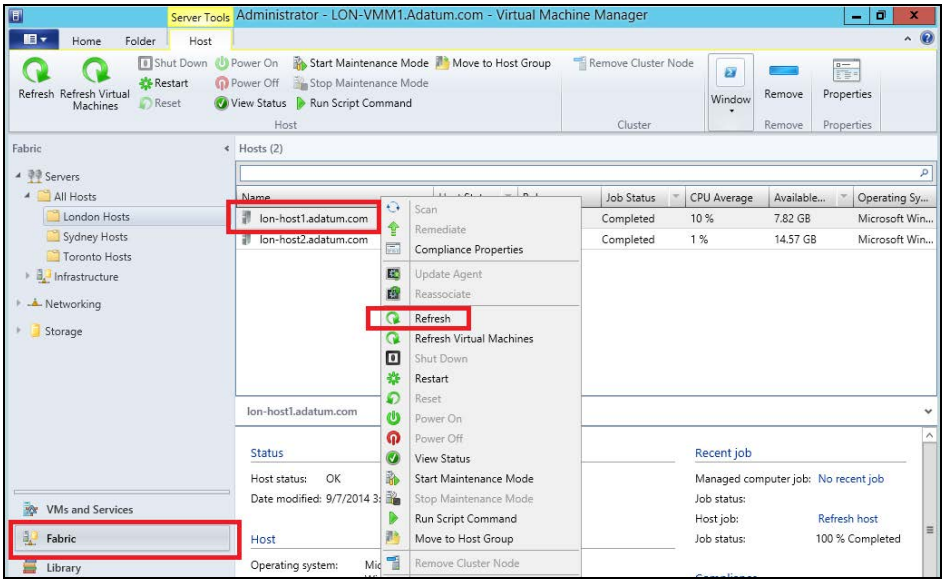
8. Trong ô **Manufacturer**,chọn **Microsoft**, trong ô **Network Adapter**, chọn **Microsoft KM-TEST Loopback Adapter**, chọn **Next** 2 lần, và **Finish.**



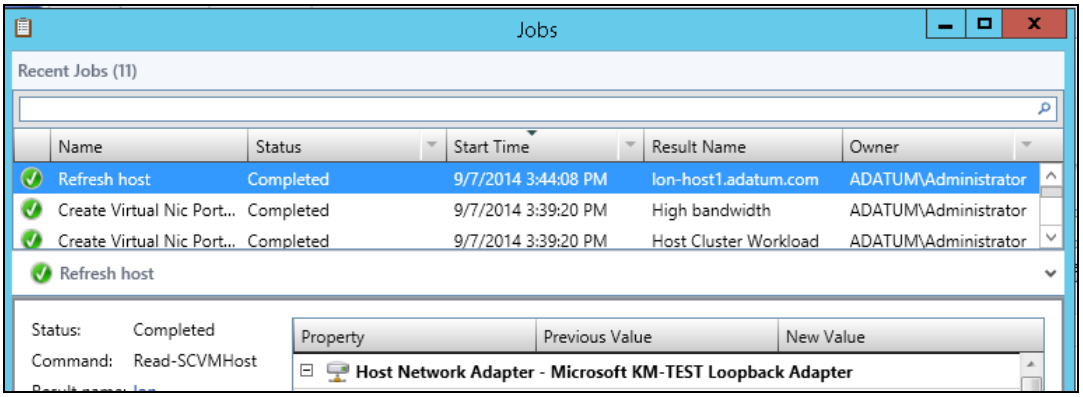

9. Tắt cửa sổ **Device Manager** và **Control Panel**.

➢ **Refresh LON-HOST1**

1. Qua máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **Fabric**, bung **Servers**, bung **All Hosts**, chọn **London Hosts**, chuột phải **LON-HOST1**, chọn **Refresh**.

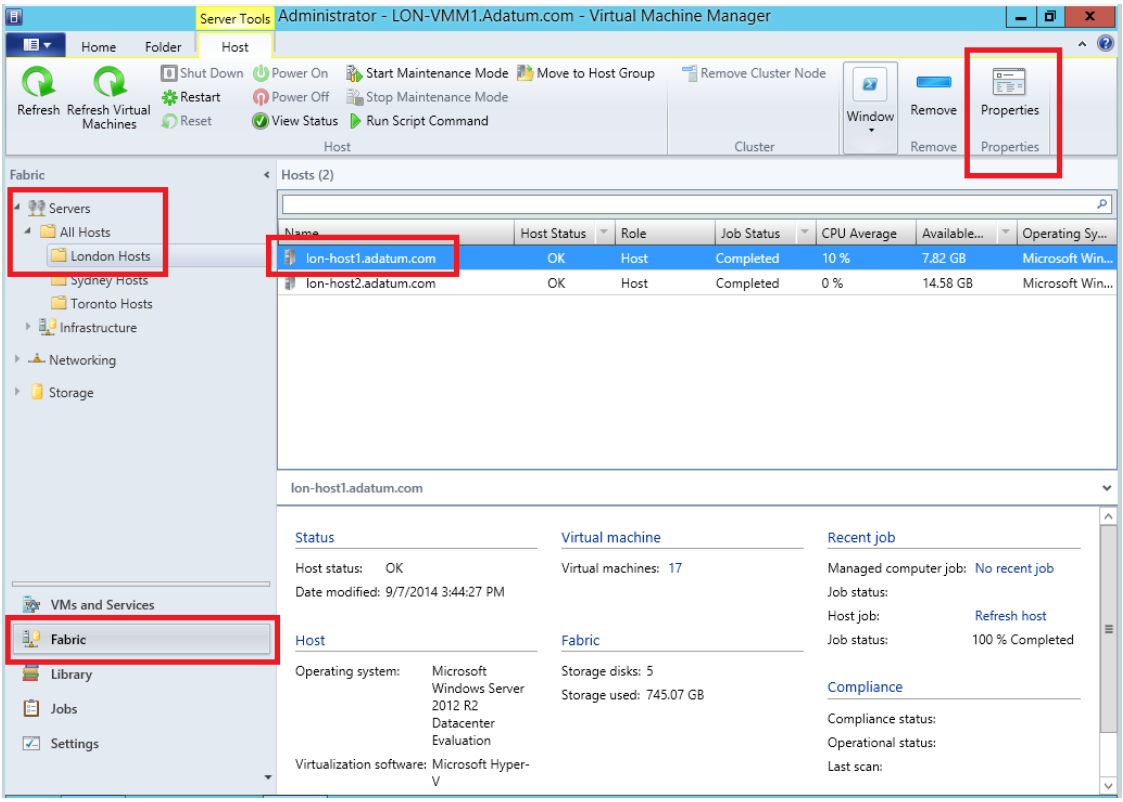


2. Trong cửa sổ **Virtual Machine Manager,** qua tab **Home**, chọn **Jobs**, kiểm tra refresh host thành công.

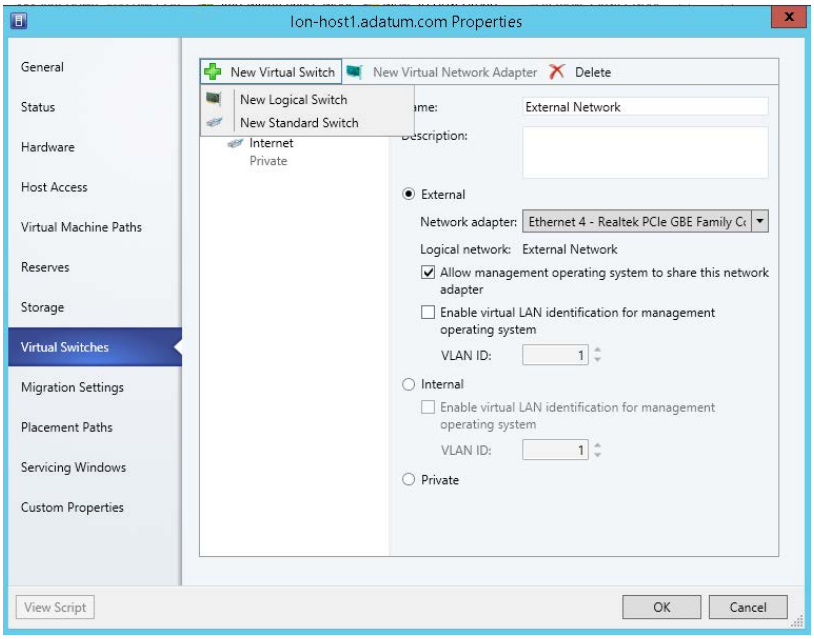



➢ **Cấu hình Hyper-V hosts sử dụng Logical Networks**

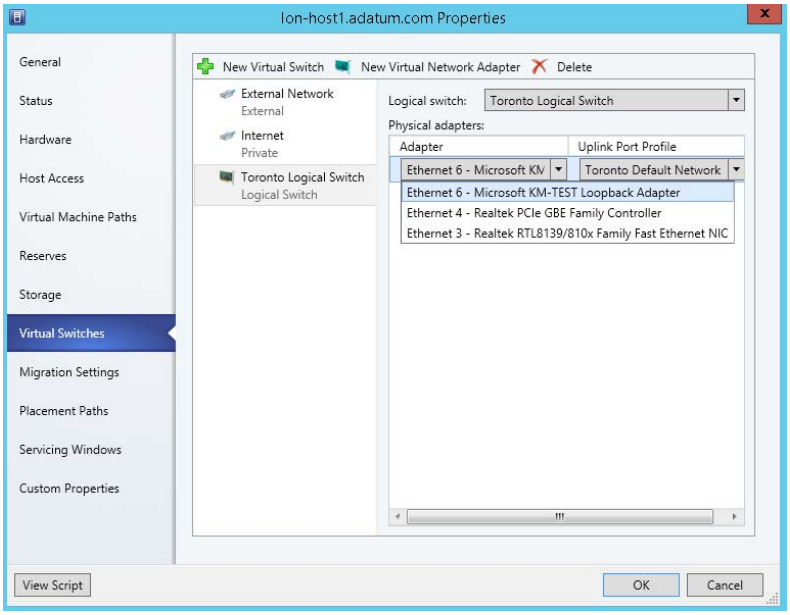
1. Trên máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **Fabric**, chọn **LON-HOST1.adatum.com**, chọn **Properties**.



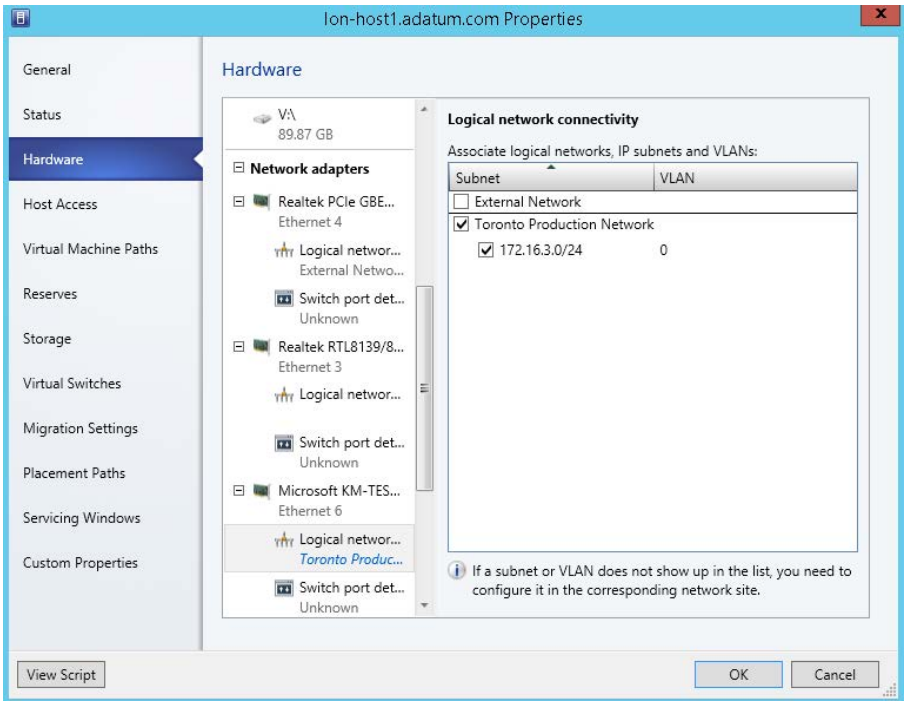
2. Cửa sổ **LON-HOST1.adatum.com Properties**, chọn mục **Virtual Switches**, chọn **New Virtual Switch**, và chọn **New Logical Switch**.




3. Chọn mục **Toronto Logical Switch**, trong phần **Physical adapters**, bung ô **Adapter**, chọn **Microsoft KM-TEST Loopback Adapter**.



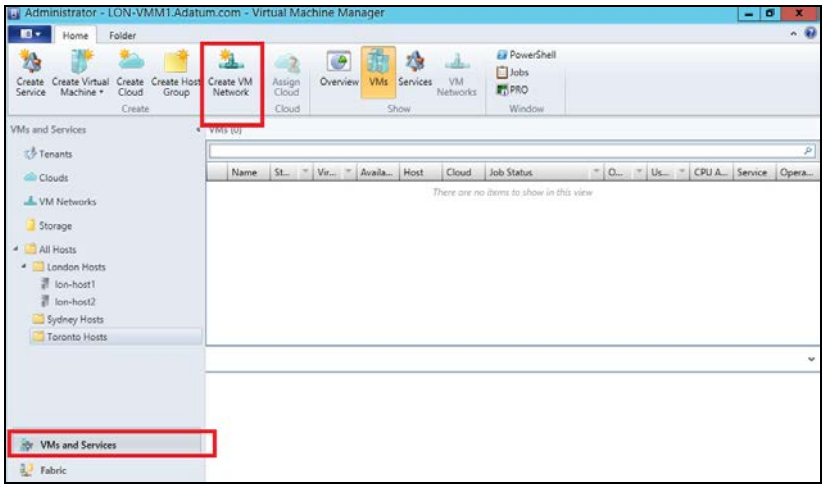
4. Cửa sổ **Properties**, chọn mục **Hardware**, kéo thanh trượt xuống tới mục **Network adapters**, bung **Microsoft KM-TEST Loopback Adapter**, chọn **Logical network,** đánh dấu chọn **Toronto Production Network**, chọn **OK**, hộp thoại thông báo, chọn **OK**.



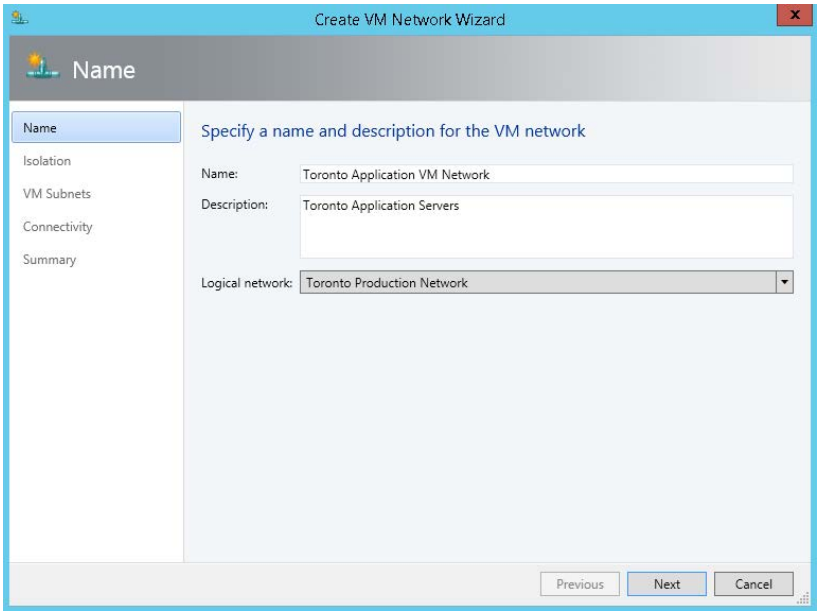
## Bước 2. Cấu hình Network Virtualization.

➢ **Tạo VM Network**

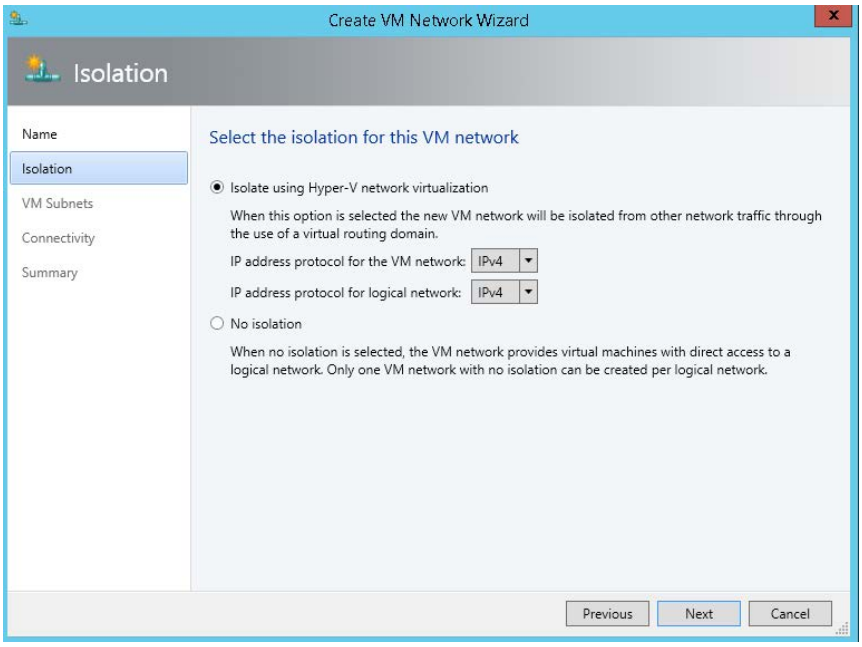
1. Trên máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, chọn **Create VM Network**.



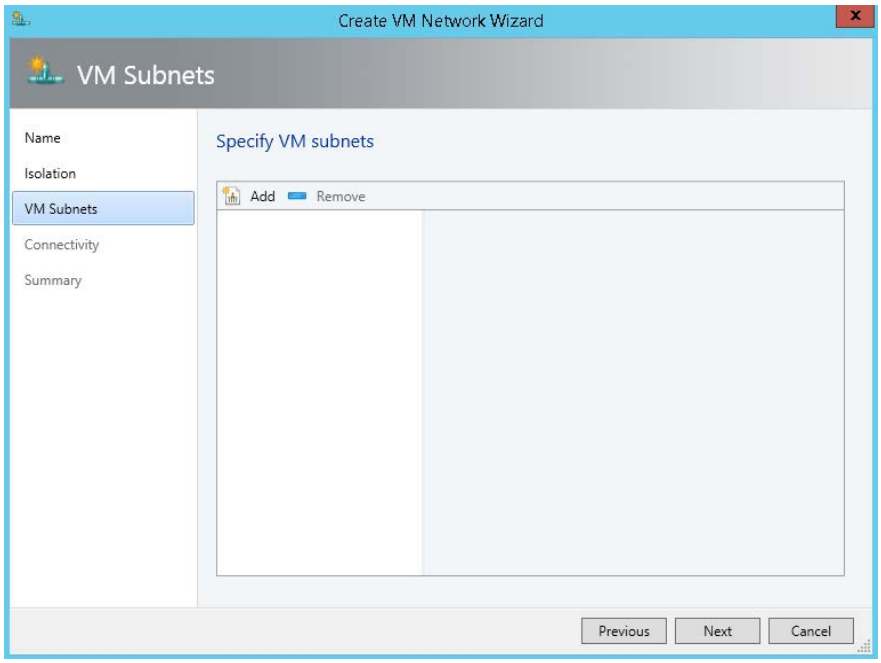

2. Cửa sổ **Name**, trong ô **Name**, nhập **Toronto Applications VM Network**, trong ô **Description**, nhập **Toronto Application Servers**. Bung ô **Logical network**, chọn **Toronto Production Network**, và chọn **Next**.



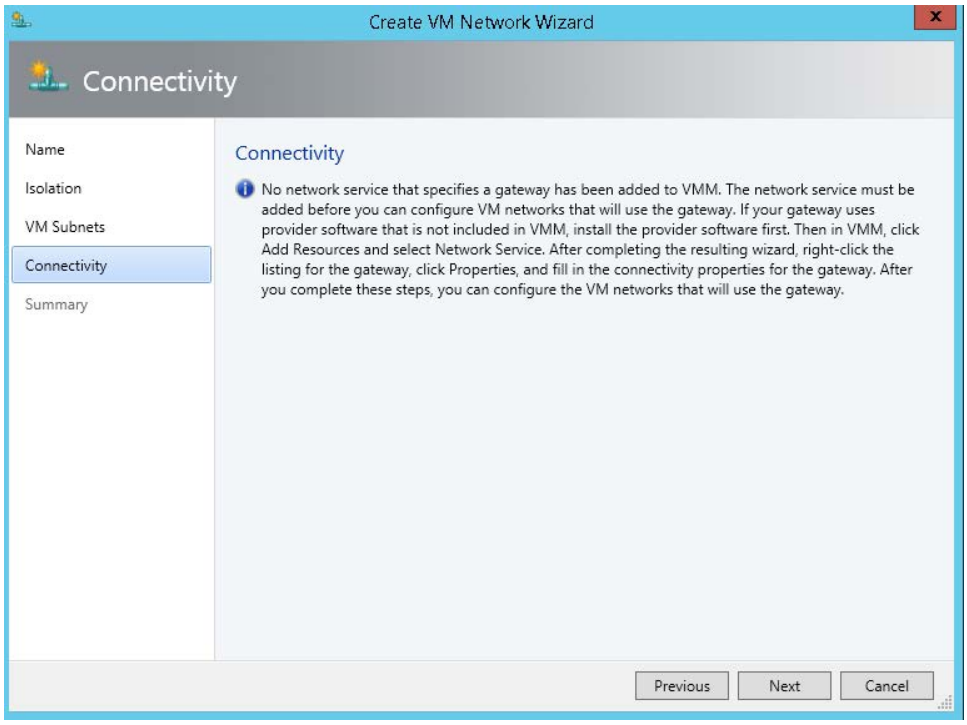
3. Cửa sổ **Isolation**, chọn **Isolate using Hyper-V network-virtualization**, và chọn **Next**.



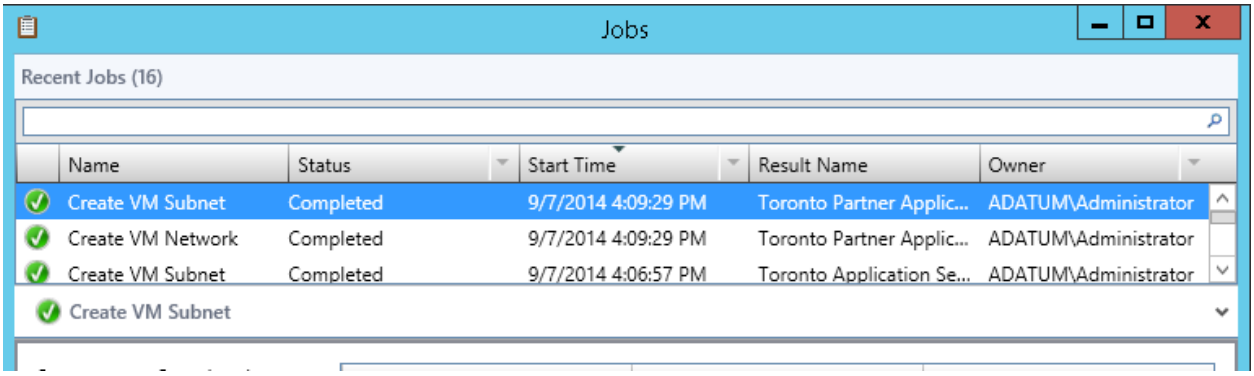

4. Cửa sổ **VM Subnets**, chọn **Add**. Trong ô **Name**, nhập **Toronto Application Servers**, trong ô **Subnet**, nhập **172.16.3.0/24**, chọn **Next**.



5. Cửa sổ **Connectivity**, chọn **Next**, và chọn **Finish**.




6. Tắt cửa sổ **Jobs**.

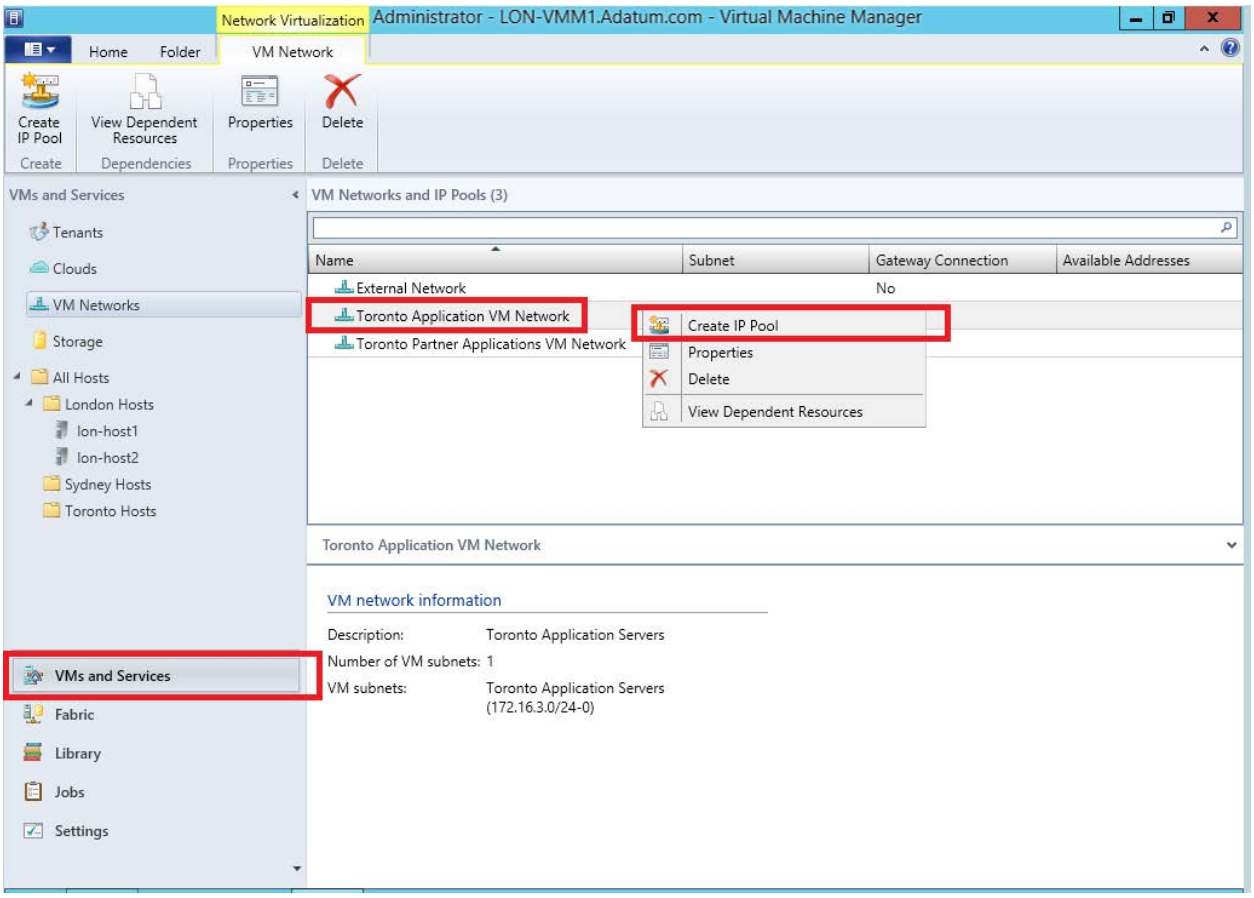



7. Lặp lại từ bước 1 đến 6 để tạo thêm một VM network tên:

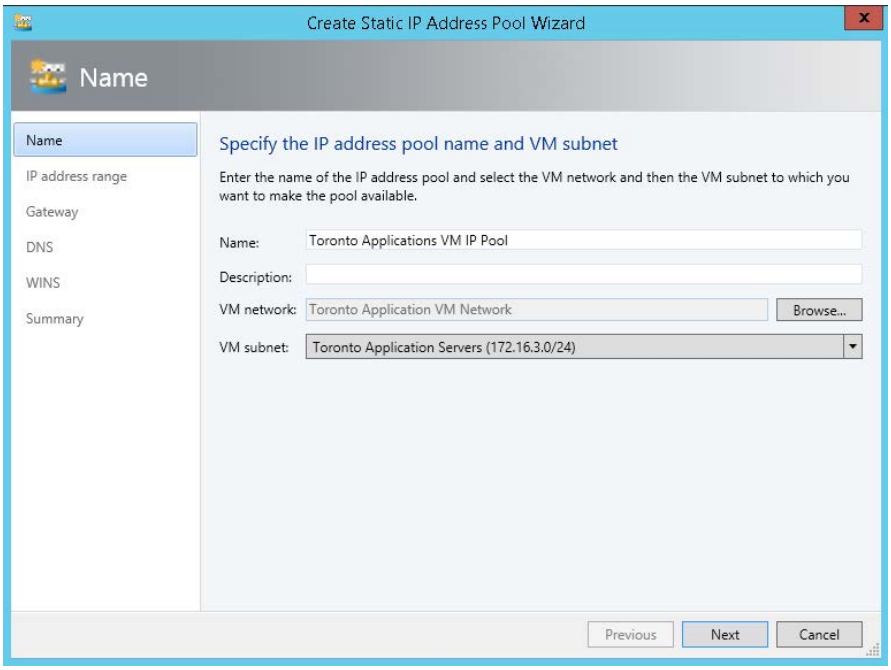
- **Toronto Partner_Applications VM Network**.

➢ **Tạo VM Network IP pools**

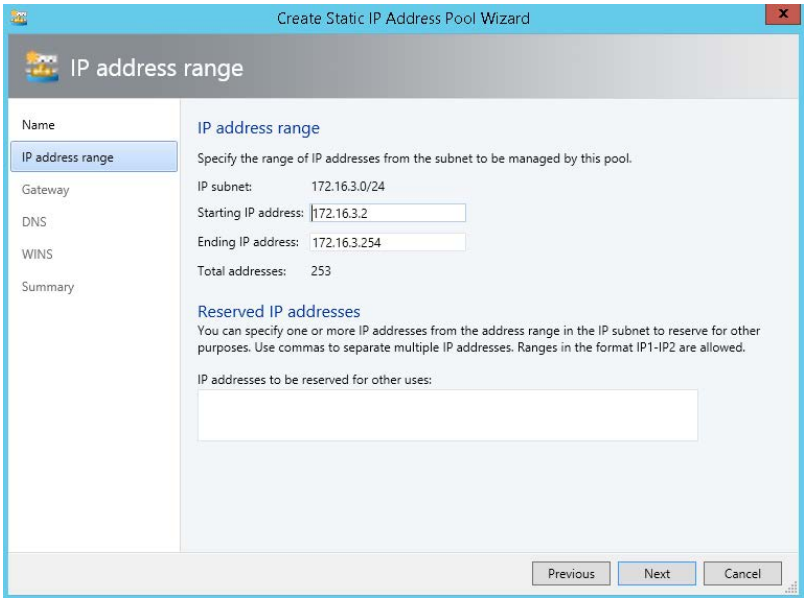
1. Trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, chọn **VM Networks**, chuột phải **Toronto Applications VM Network**, chọn **Create IP Pool**.



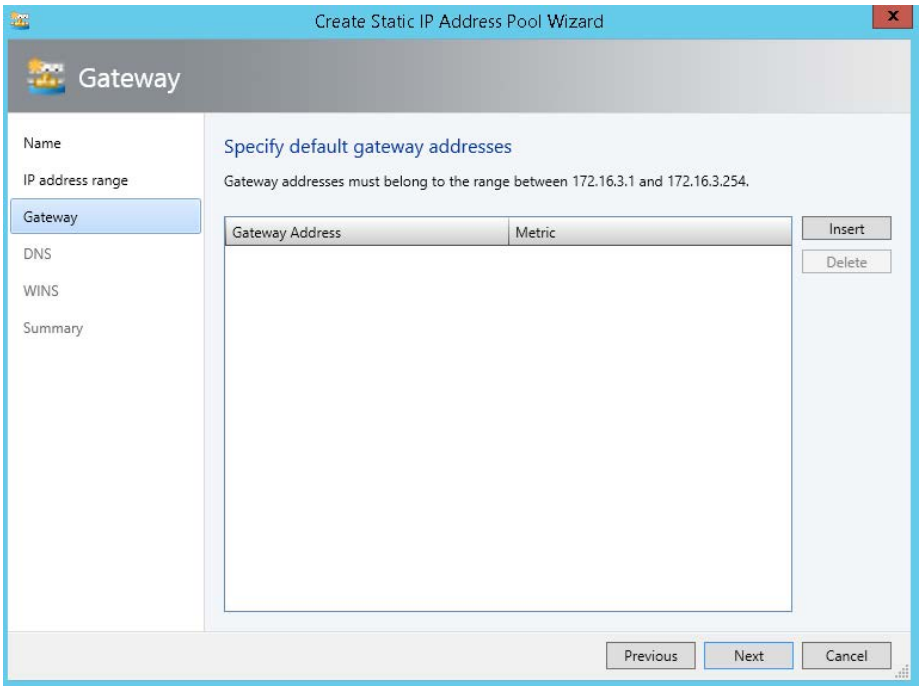
2. Cửa sổ **Name**, trong ô **Name**, nhập **Toronto Applications VM IP Pool**. Đảm bảo ô **VM Network** chọn **Toronto Applications VM Network,** và ô **VM subnet**, chọn **Toronto Application Servers (172.16.3.0/24)**, chọn **Next**.



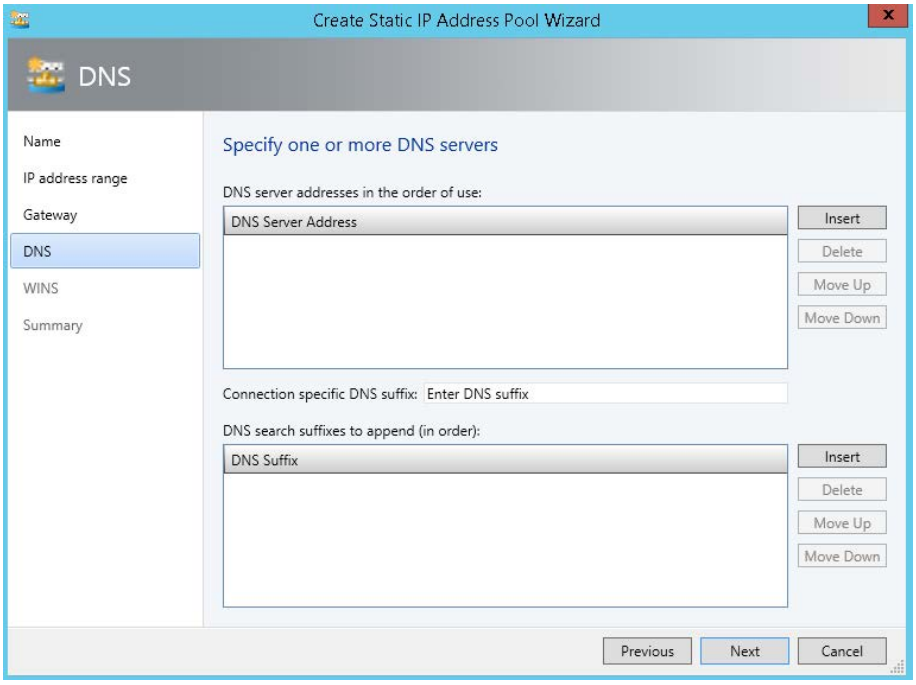

3. Cửa sổ **IP address range**, chọn **Next**.



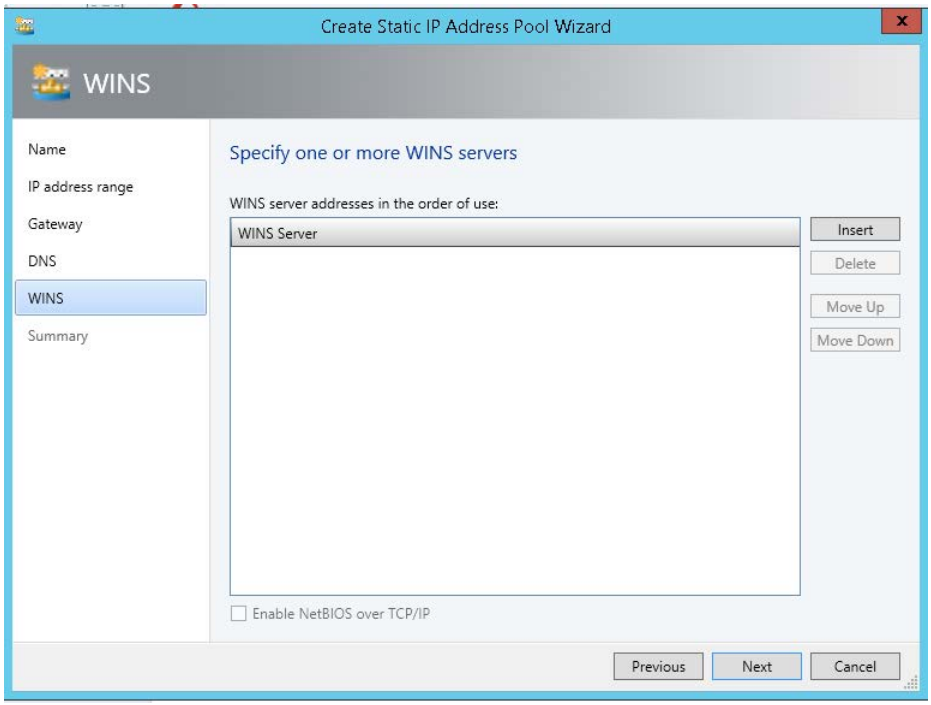
4. Cửa sổ **Gateway**, chọn **Next**.



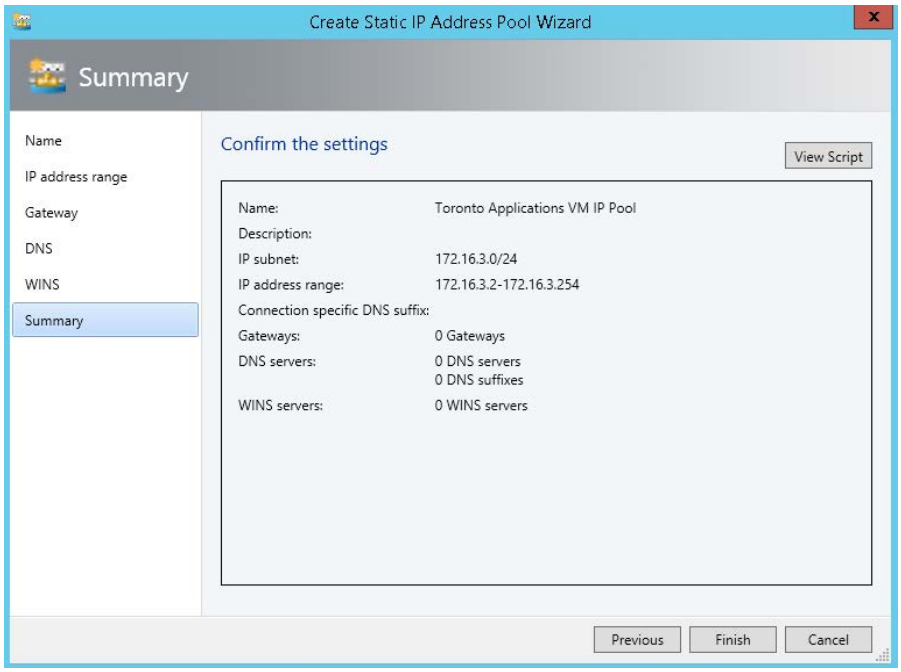

5. Cửa sổ **DNS**, chọn **Next**.



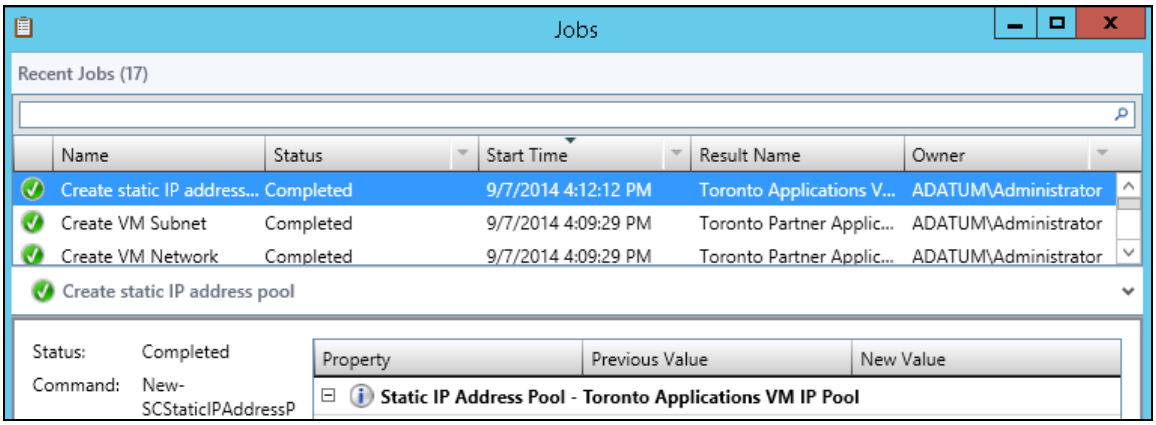
6. Cửa sổ **WINS**, chọn **Next**.




7. Cửa sổ **Summary**, chọn **Finish**.



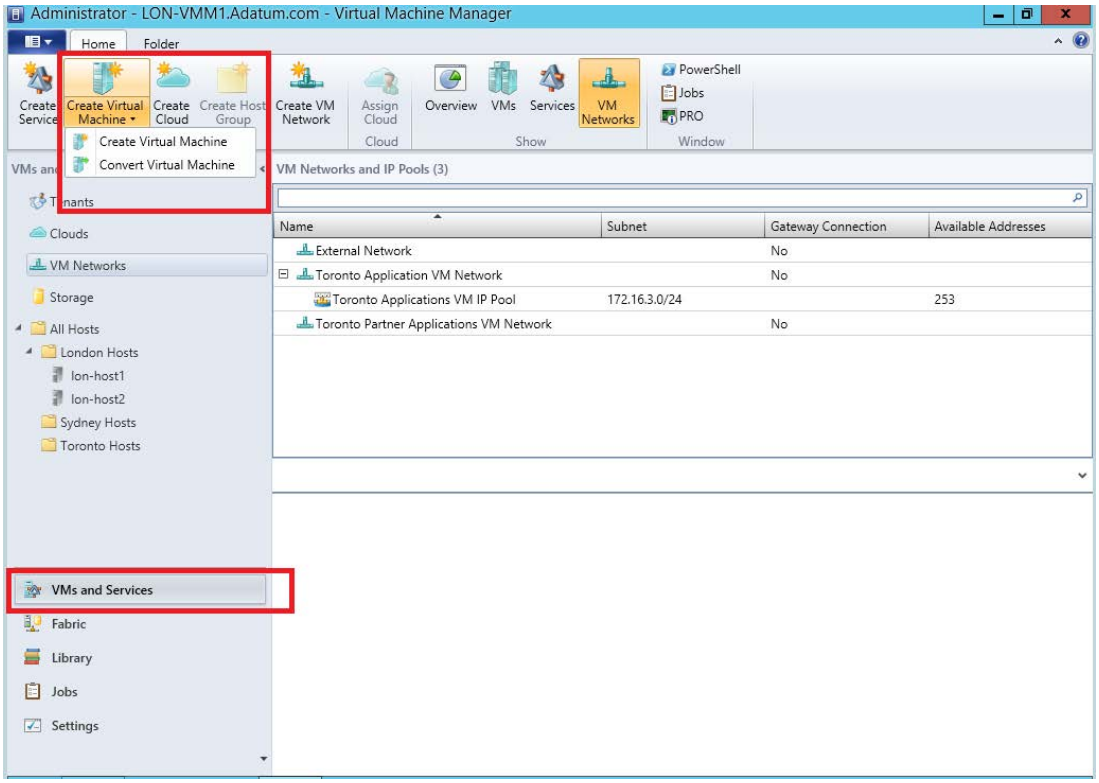
8. Tắt cửa sổ **Jobs**.




## Bước 3. Chỉ định máy ảo vào VM networks.

### ➢ Chỉ định máy ảo vào VM Networks

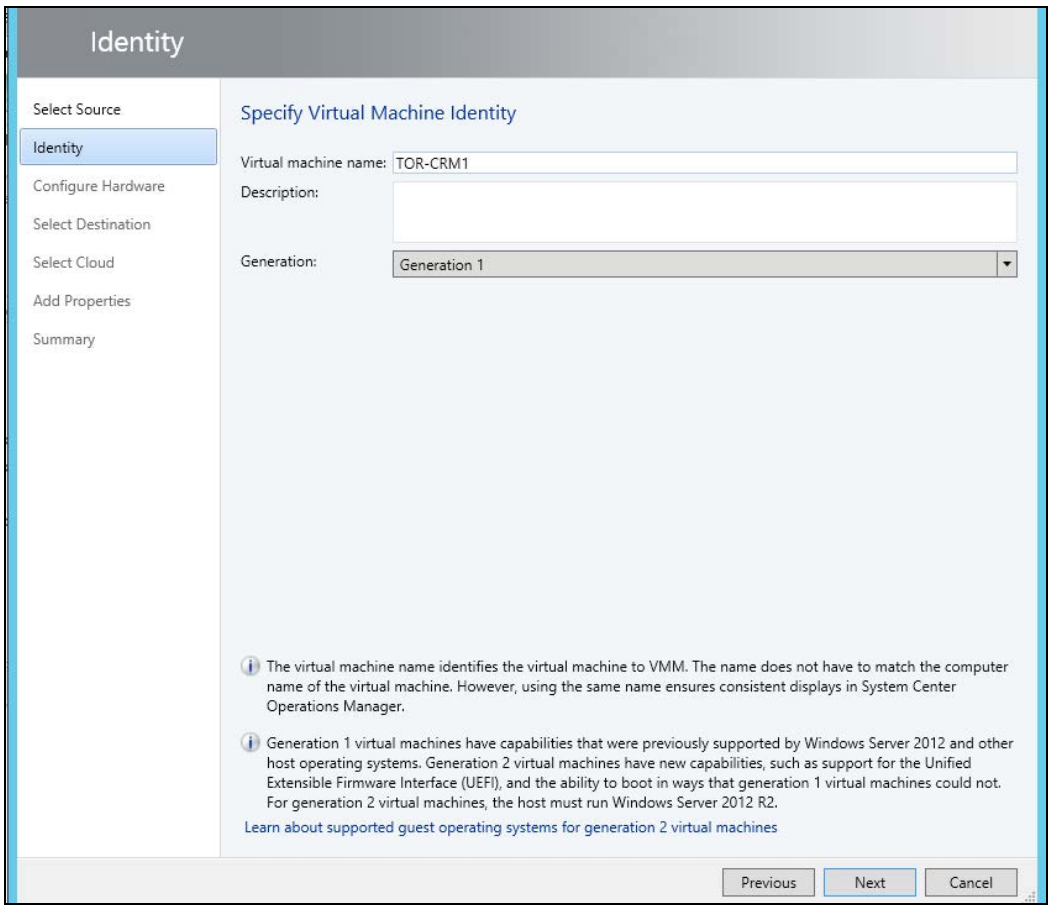
1. Trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, qua tab **Home**, bung **Create Virtual Machine,** chọn **Create Virtual Machine**.



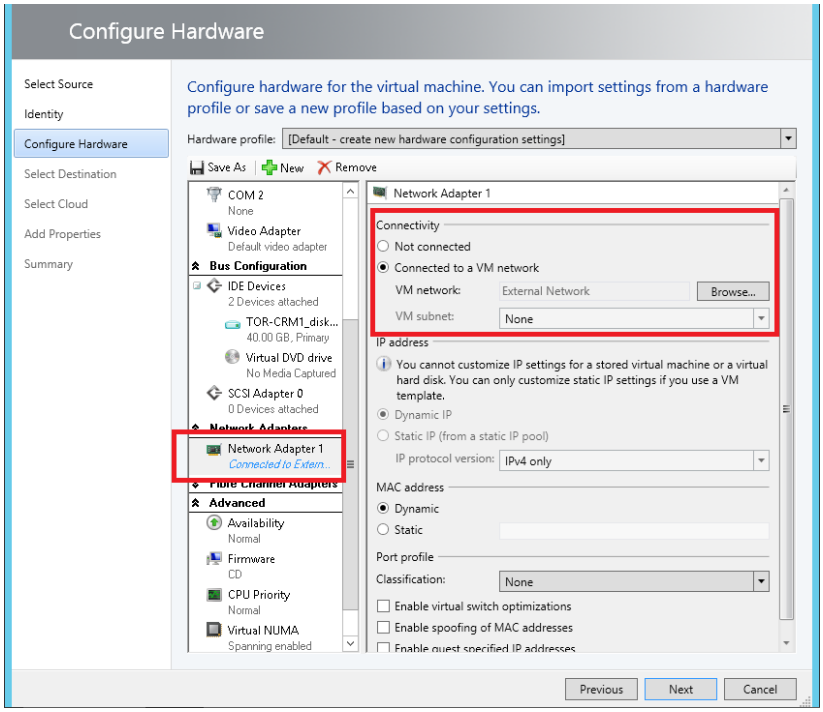
2. Cửa sổ **Select Source**, chọn **Create the new virtual machine with a blank virtual hard disk**, và chọn **Next**.



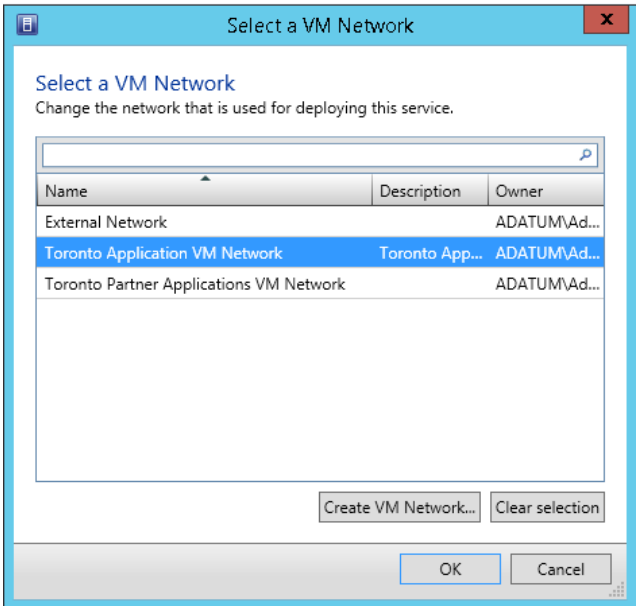

3. Cửa sổ **Specify Virtual Machine Identity**, trong ô **Virtual machine name**, nhập **TOR-CRM1**, và chọn **Next**.



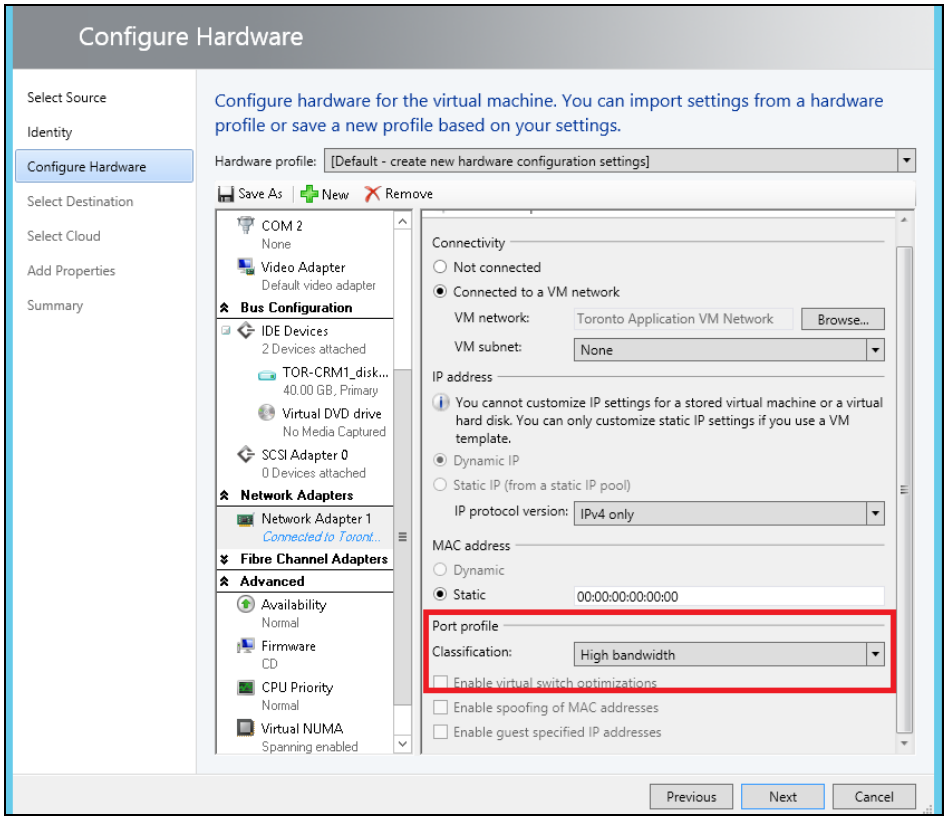
4. Cửa sổ **Configure Hardware**, chọn **Network Adapter 1**, trong phần **Connectivity**, chọn **Connected to a VM Network**, chọn **Browse.**



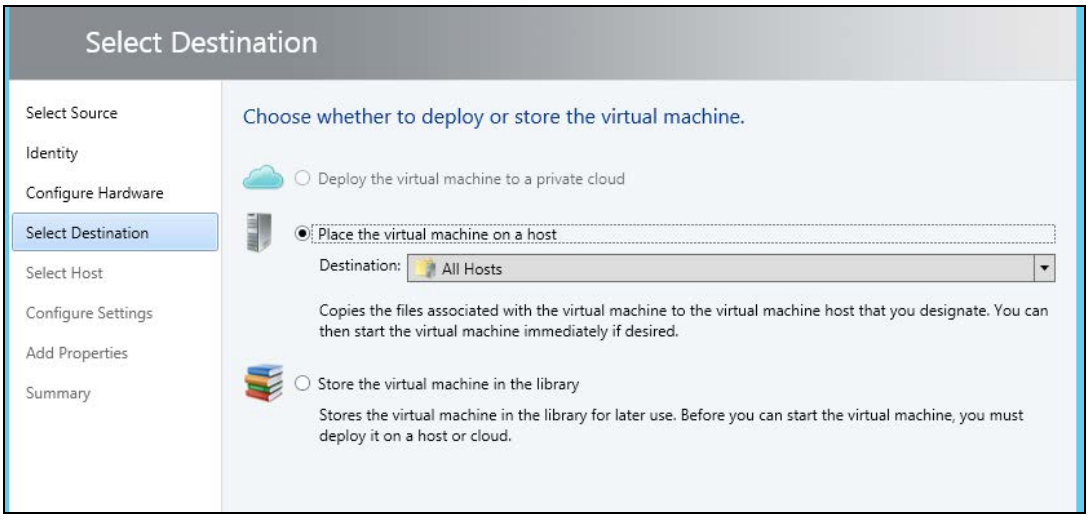

5. Hộp thoại **Select a VM Network,** chọn **Toronto_Applications VM Network**, chọn **OK**.



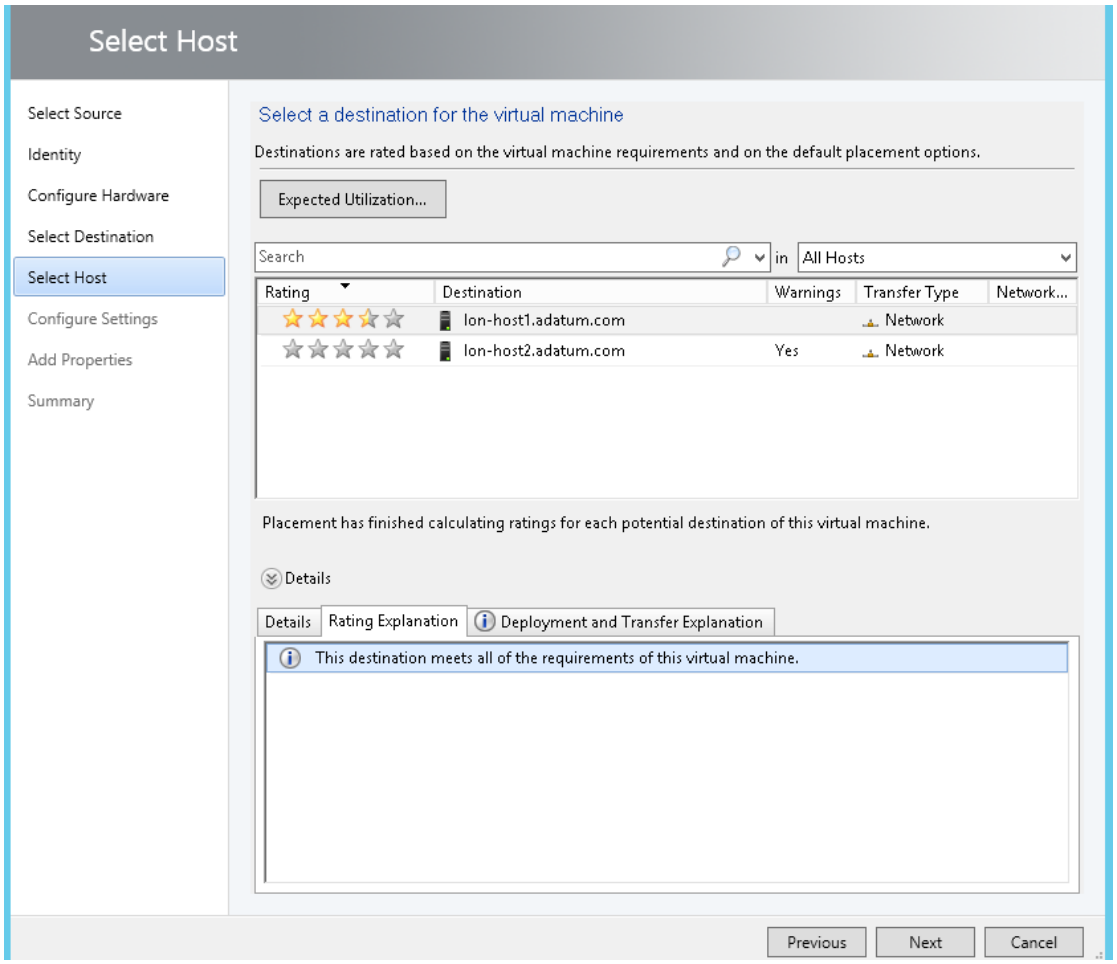
6. Trong phần **Port Profile**, bung ô **Classification**, chọn **High bandwidth**, và chọn **Next**.



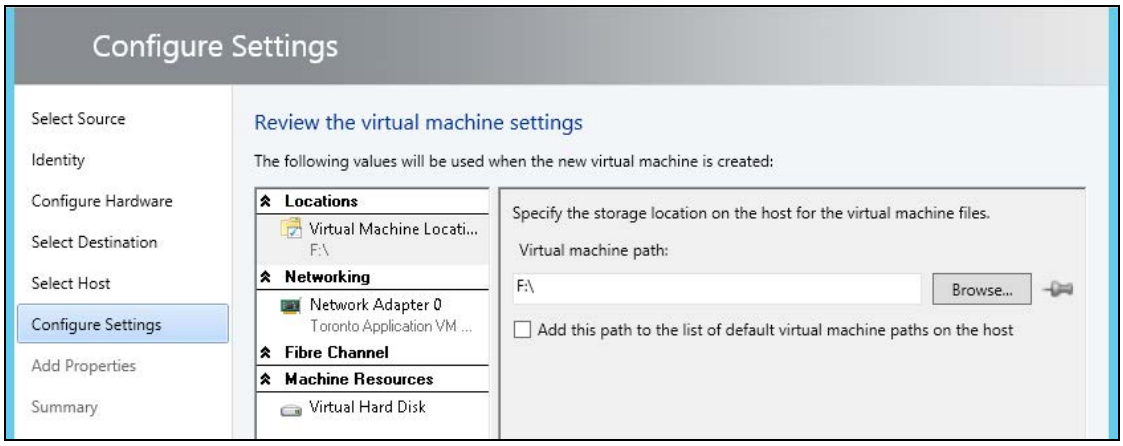

7. Cửa sổ **Select Destination**, chọn **Next**.



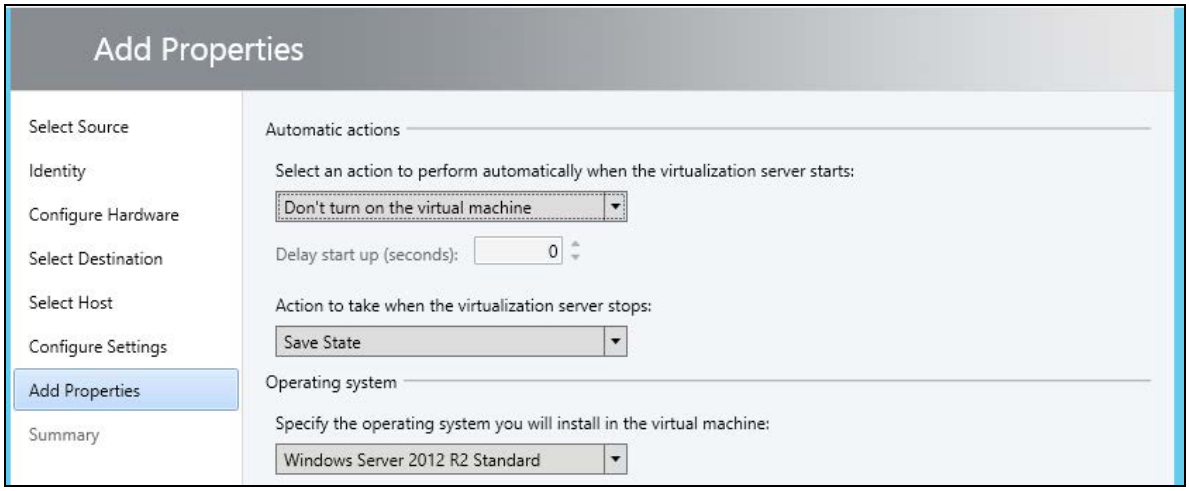
8. Cửa sổ **Select Host**, chọn **lon-host1.adatum.com**, qua tab **Rating Explanation**. Kiểm tra có dòng **This destination meets all the requirements of this virtual machine**, chọn **Next**.



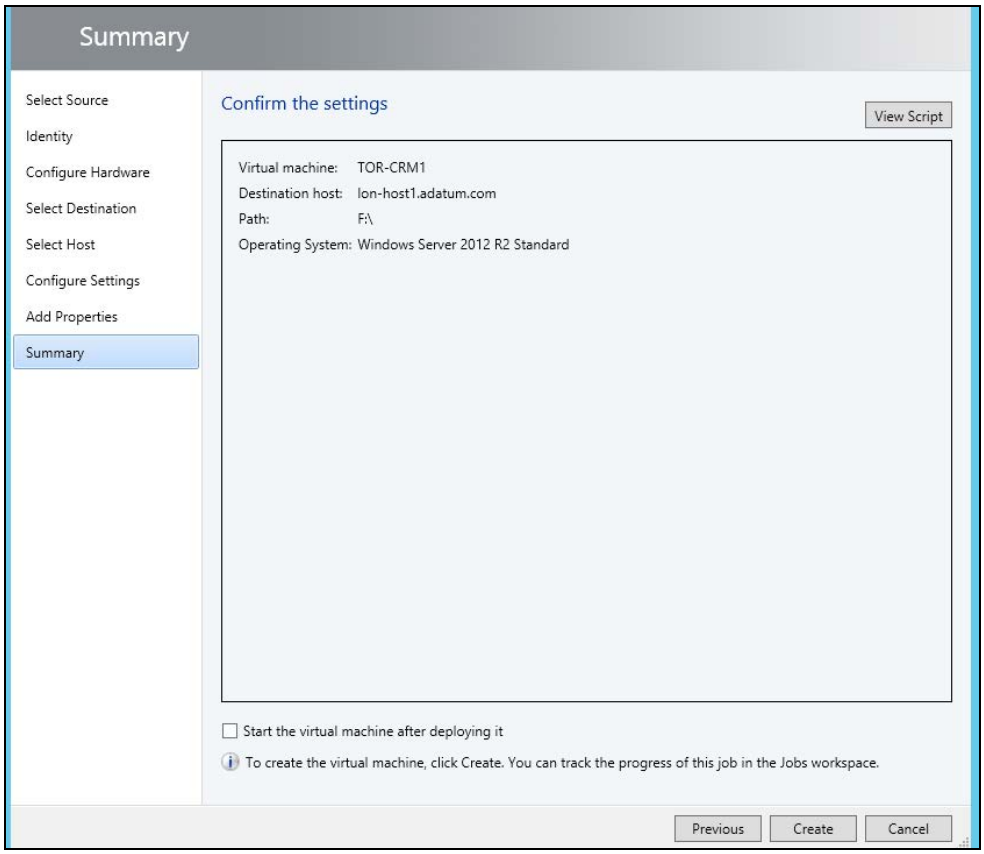
9. Cửa sổ **Configure Settings**, chọn **Next**.



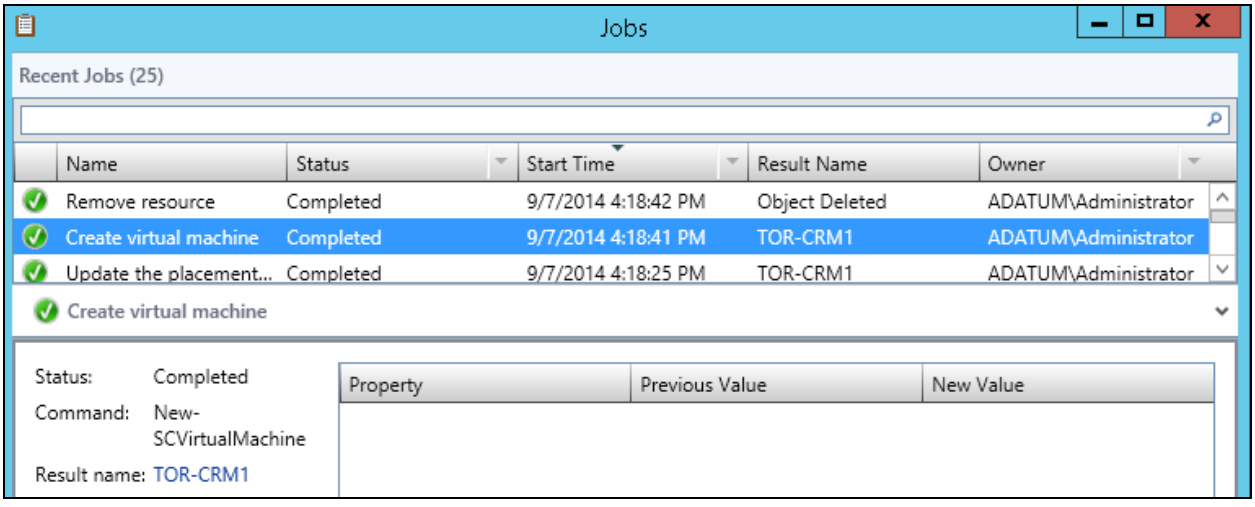

10. Cửa sổ **Add Properties**, chọn **Next**.



11. Cửa sổ **Summary**, chọn **Create**.

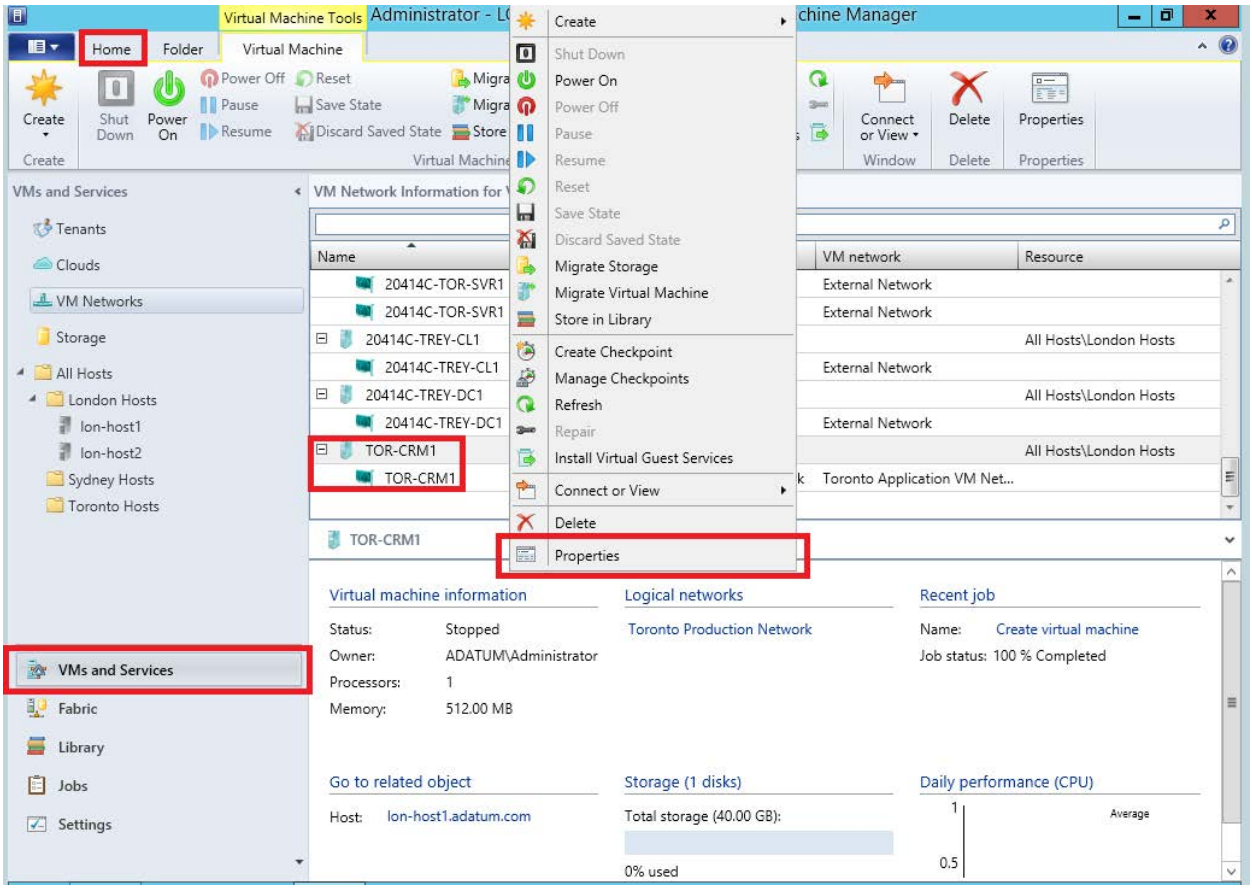



12. Tắt cửa sổ **Jobs**.

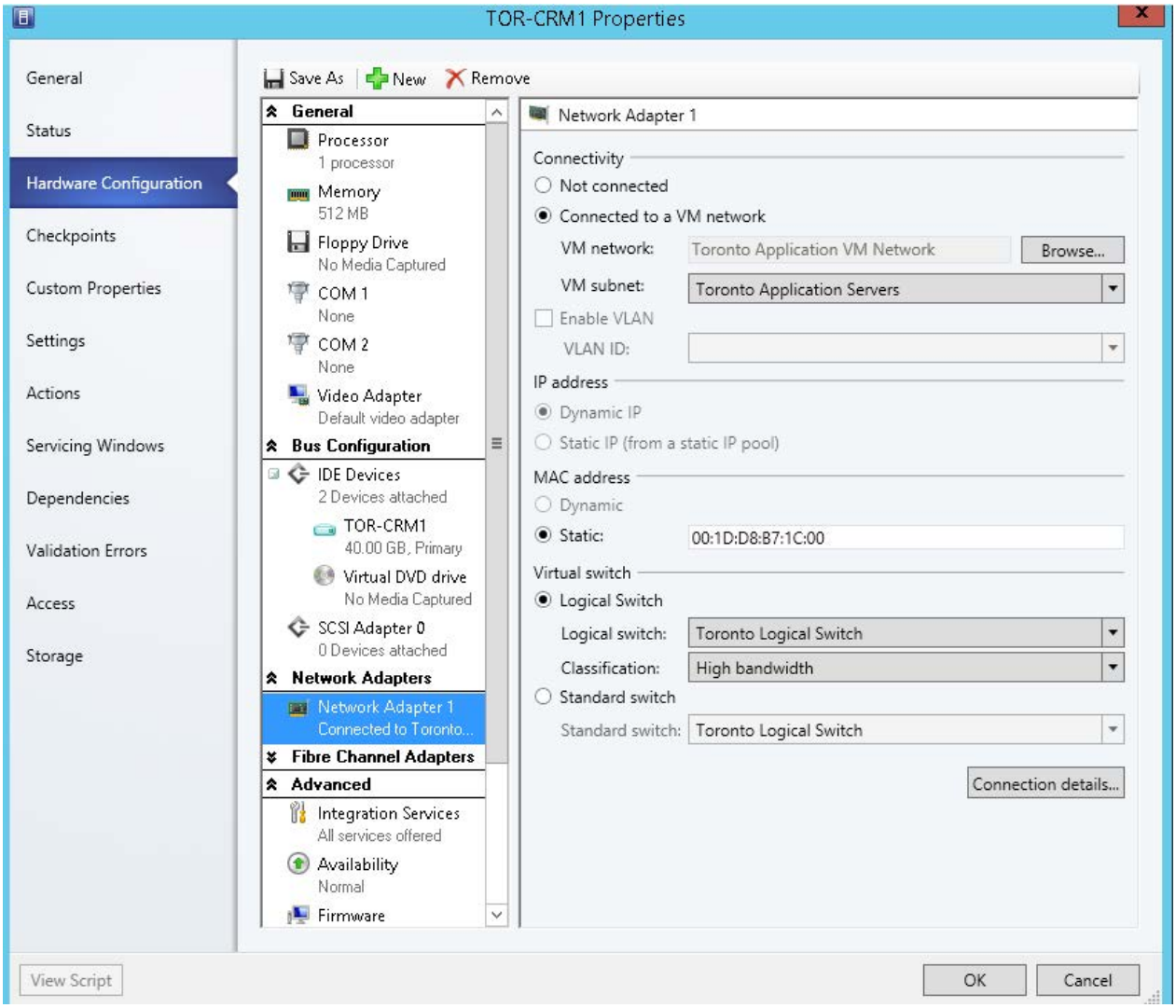


➢ **Kiểm tra máy ảo**

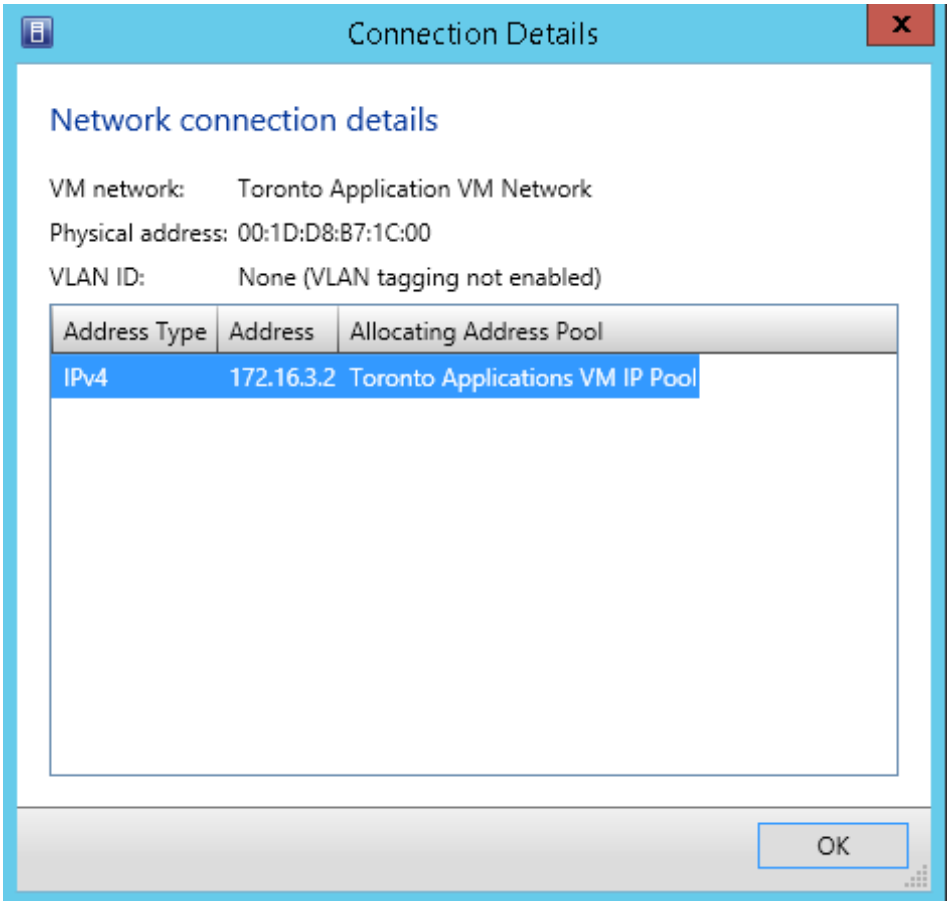
1. Trong cửa sổ **Virtual Machine Manager**, chọn **VMs and Services**, qua tab **Home**, chọn **VMs**, chuột phải **TOR-CRM1**, chọn **Properties**.



2. Cửa sổ **TOR-CRM1 Properties,** chọn mục **Hardware Configuration**, chọn **Network Adapter 1**. Kiểm tra VM Network và Logical switch. Chọn **Connection details**.



3. Kiểm tra địa chỉ IP được gán từ Toronto Applications VM IP Pool, chọn **OK**, và chọn **Cancel**.




**VII. Chuẩn bị cho bài tiếp theo:**

Không phục hồi các máy ảo, vì bạn sẽ sử dụng các máy ảo này trong các bài tiếp theo.

# Bài 3: Lập kế hoạch và triển khai máy ảo với System Center Virtual Machine Manage

**I. Mục tiêu:**

- Lập kế hoạch triển khai máy ảo bằng VMM.
- Cấu hình VMM Profiles và Templates.
- Triển khai Hyper-V Replica.

**II. Kịch bản và yêu cầu tổng quan:**

Sau khi đã triển khai các Hyper-V Hosts, iSCSI Storage, và cơ sở hạ tầng cho hê thống ảo hóa, bước tiếp theo là lên kế hoạch và thực hiện việc triển khai máy ảo.

Một trong những mục tiêu chính trong việc triển khai là ảo hóa được càng nhiều server càng tốt. Là một phần của kế hoạch này, bạn phải xác định được những server nào thích hợp với ảo hóa, bao gồm các server vật lý mà bạn có thể chuyển đổi thành máy ảo. Ngoài ra, kế hoạch triển khai và quản lý máy ảo phải đơn giản và tuân thủ một tiêu chuẩn chung.

Để đơn giản hóa việc triển khai các máy ảo tại A. Datum, bạn cần phải tạo sẵn các máy ảo mẫu (Virtual Machine Template) và dịch vụ mẫu (Service Template) để sử dụng cho việc triển khai các máy ảo mới.

**III. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-HOST2**<br>**20414C-LON-DC1**<br>**20414C-LON-VMM1** |
| User name | **Adatum\Administrator** |

**IV. Chuẩn bị:**

Bài thực hành gồm 2 máy thật, 1 máy khởi động **20414C-LON-HOST1** và 1 máy khởi động **20414C-LON-HOST2**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
2. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
3. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
4. Thực hiên từ bước 1 đến 3 cho máy ảo **20414C-LON-VMM1.**
5. Logon vào máy **20414C-LON-HOST2** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**

**V. Thực hành:**

*Thời gian thực hành: 60 Phút*

## Bài tập 1: Cấu hình VMM Profiles và Templates.

Bây giờ, bạn sẽ sử dụng VMM để cấu hình các Guest Operating System Profile, Hardware Profile, và SQL Server Profile. Sau đó bạn sẽ tạo ra các Virtual Machine Template và Service Template.

❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Guest Operating System Profile
2. Cấu hình Hardware Profile
3. Cấu hình SQL Server Profile
4. Cấu hình Virtual Machine Template
5. Cấu hình a Service Template

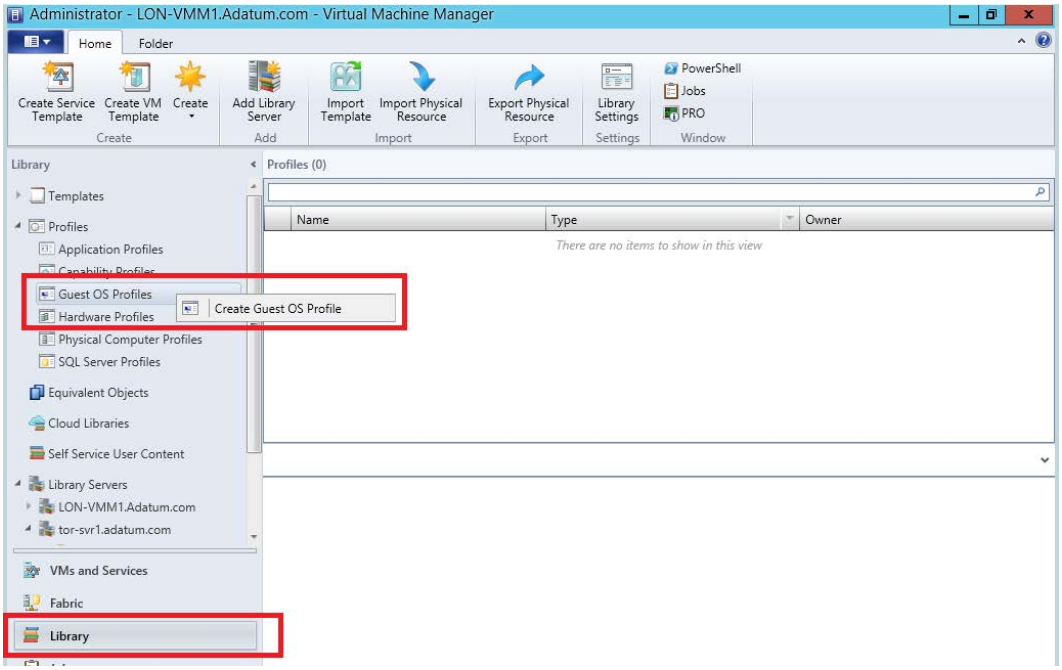
❖ **Thực hiện:**

**Bước 1. Cấu hình Guest Operating System Profile.**

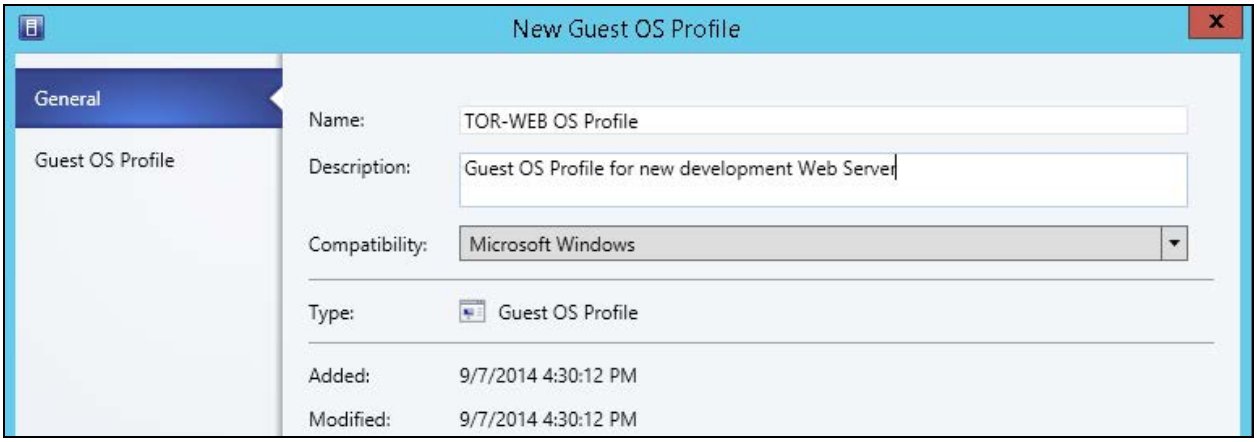
1. Trên desktop của máy **LON-VMM1**, mở **Virtual Machine Manager Console**. Cửa sổ **Connect to Server**, chọn **Connect**.



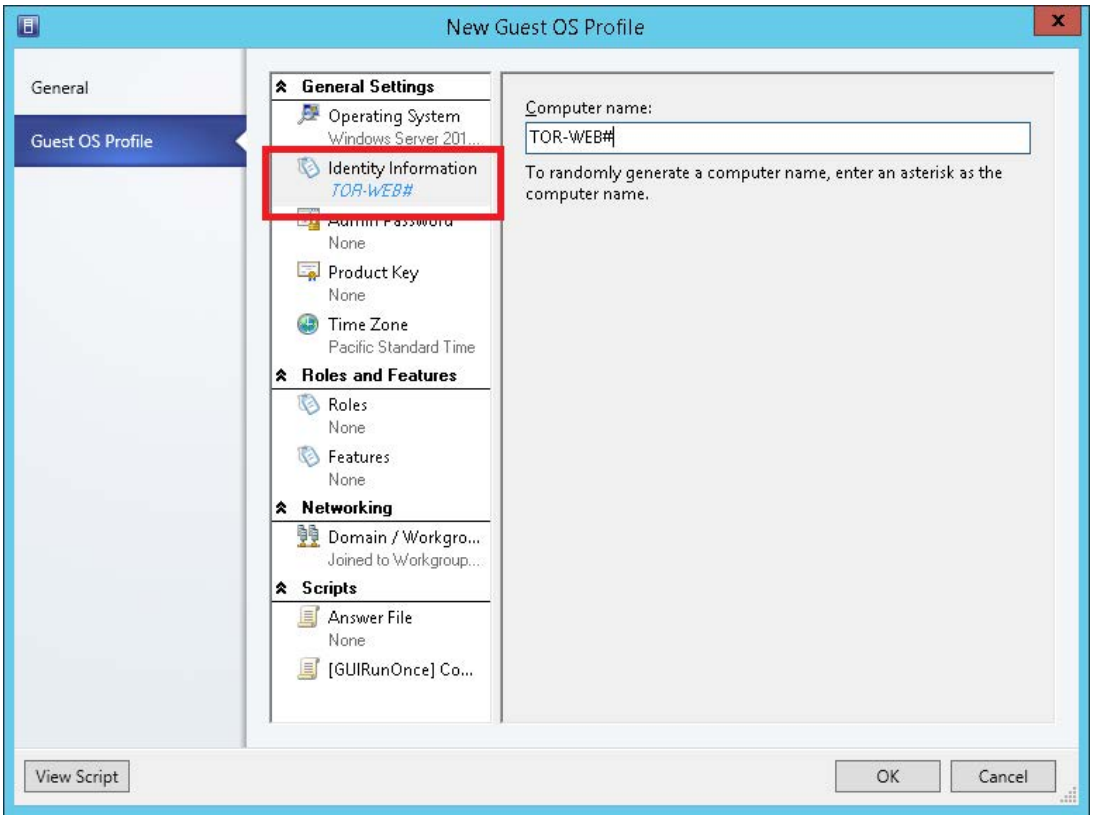

2. Trong cửa sổ **Virtual Machine Manager**, chọn **Library**, bung **Profiles**, chuột phải **Guest OS Profiles**, chọn **Create Guest OS Profile**.



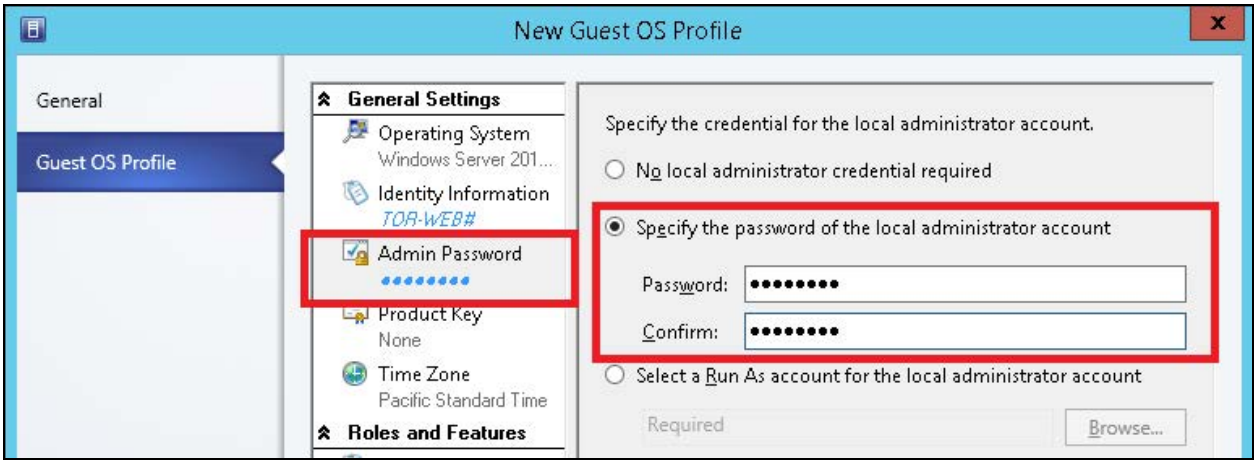
3. Hộp thoại **New Guest OS Profile,** trong ô **Name**, nhập **TOR-WEB OS Profile**, trong ô **Description**, nhập **Guest OS Profile for new development Web Server**.



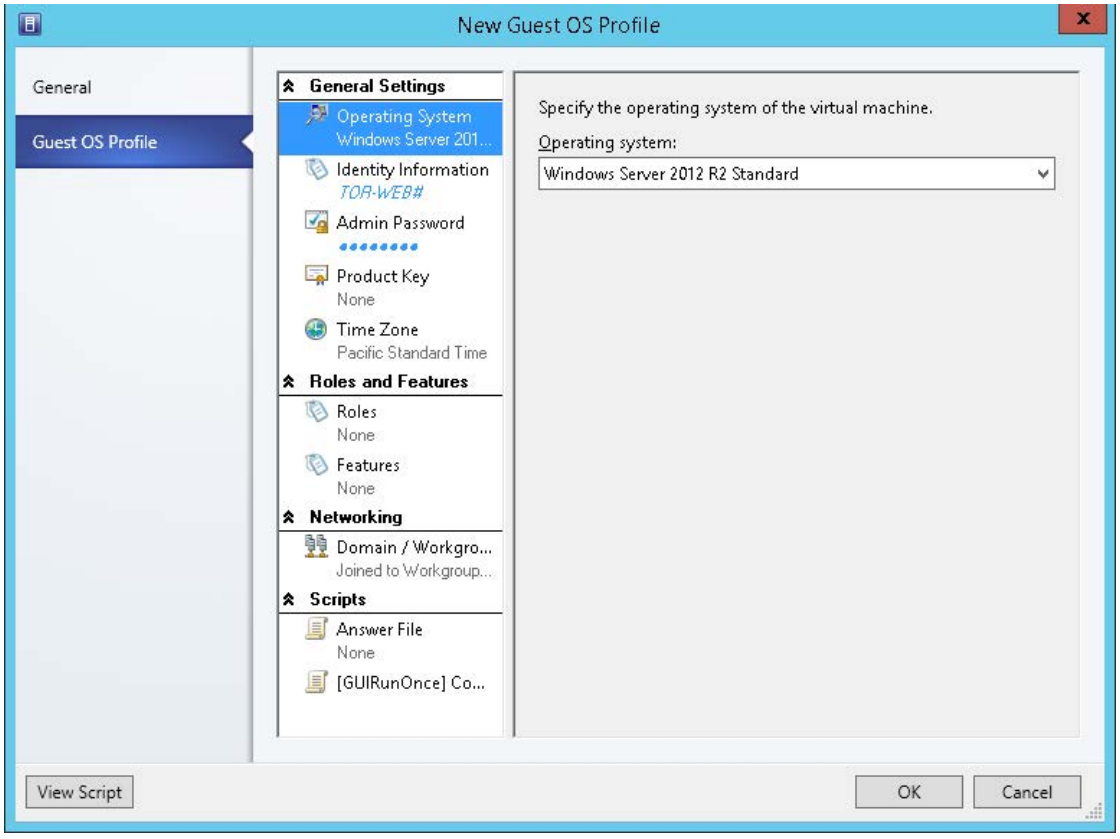

4. Chọn mục **Guest OS Profile**, trong phần **General Settings**, chọn **Identity Information**, nhập **TOR-WEB#** vào ô **Computer name**.



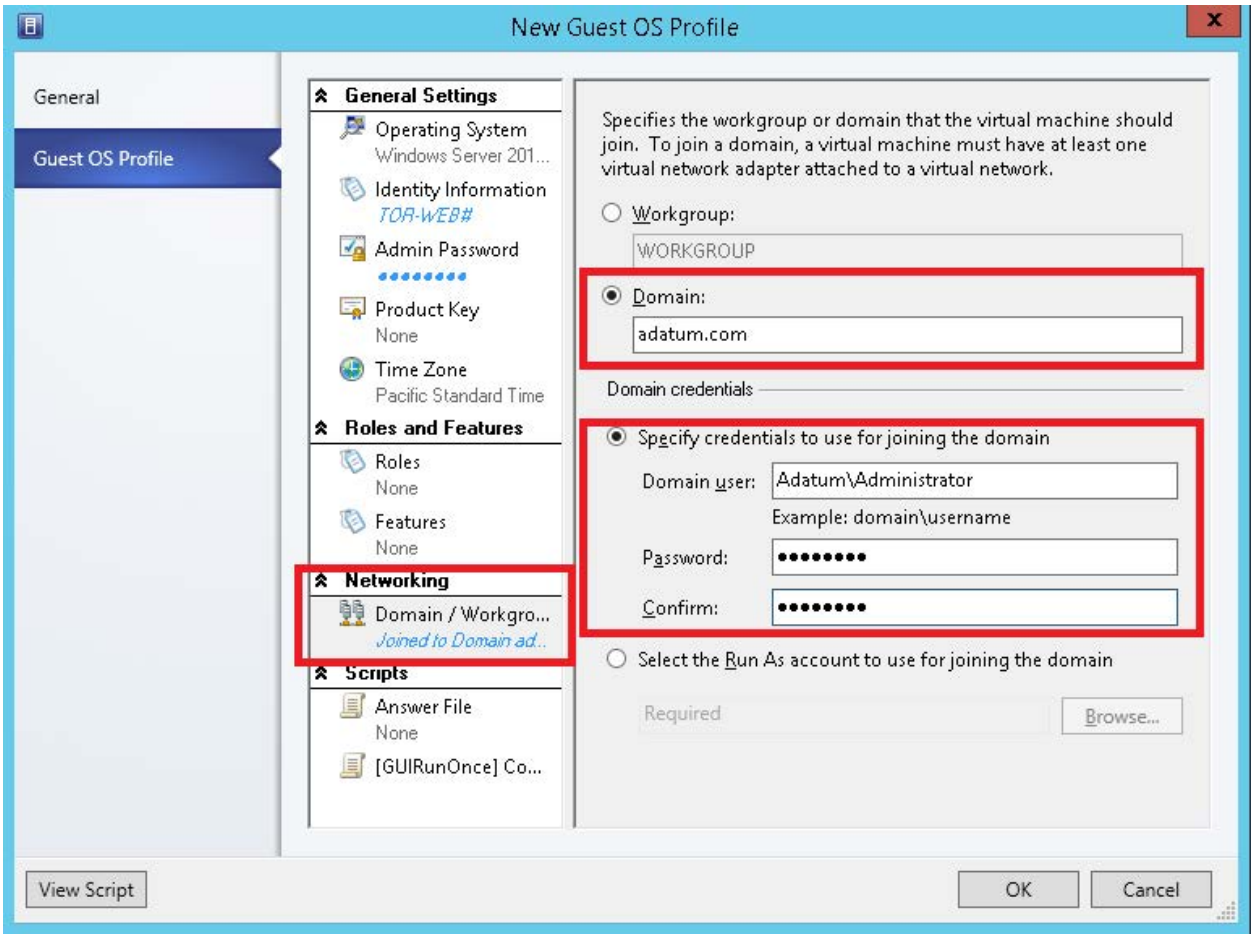
5. Chọn **Admin Password**, chọn **Specify the password of the local administrator account**, nhập **Pa$$w0rd** vào ô **Password** và **Confirm.**




6. Chọn **Operating System**, đảm bảo đang chọn **Windows Server 2012 R2 Standard**.

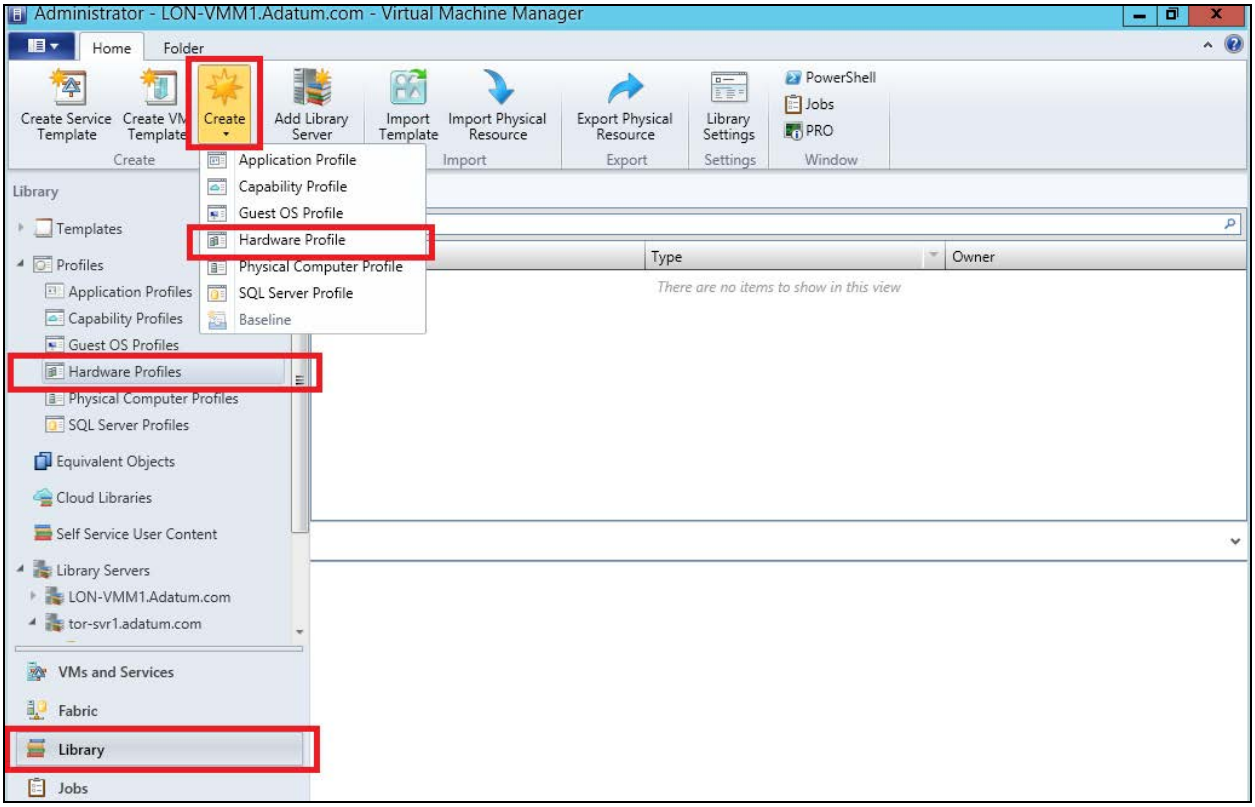


7. Trong phần **Networking**, chọn mục **Domain/Workgroup**, chọn **Domain**, nhập a**datum.com.** Chọn **Specify credentials to use for joining the domain**, trong ô **Domain user**, nhập **Adatum\Administrator**, trong ô **Password** và **Confirm,** nhập **Pa$$w0rd**, chọn **OK**.

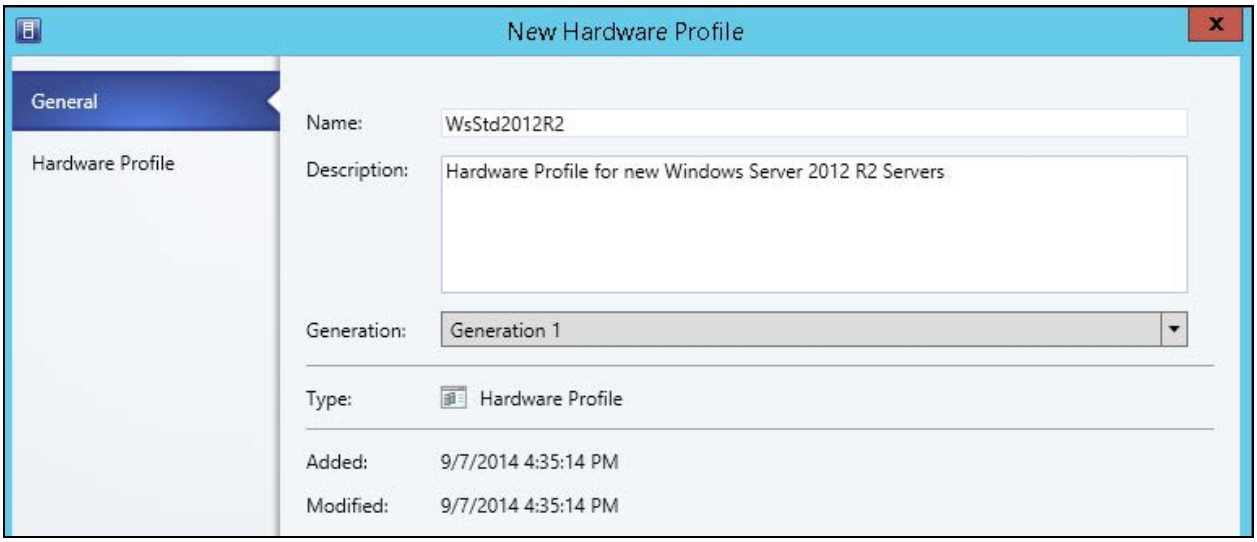


## Bước 2. Cấu hình Hardware Profile.

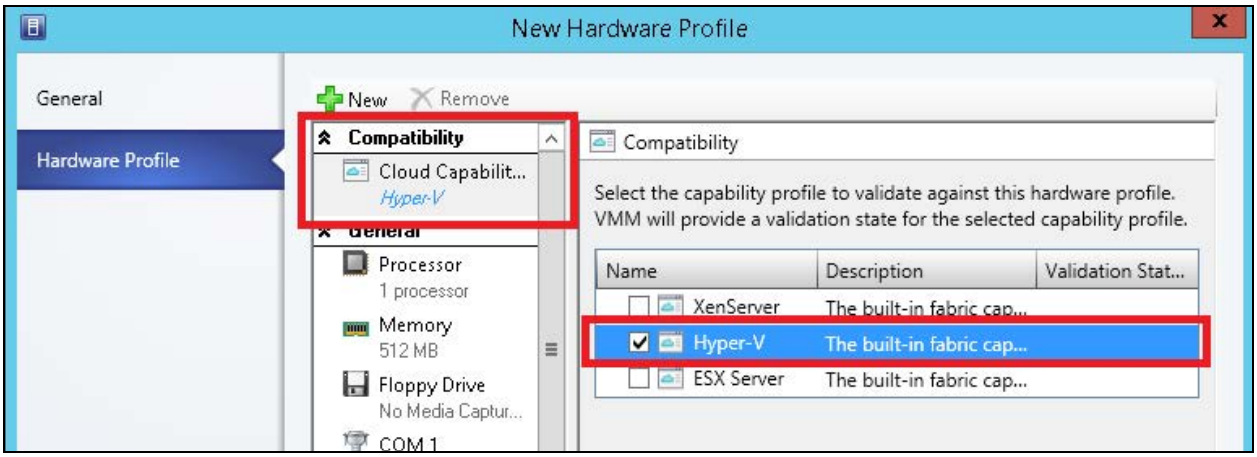
1. Trên máy **LON-VMM1,** trong cửa sổ **VMM**, chọn **Library**, bung **Profiles**, chọn **Hardware Profiles**, chọn **Create**, và chọn **Hardware Profile**.



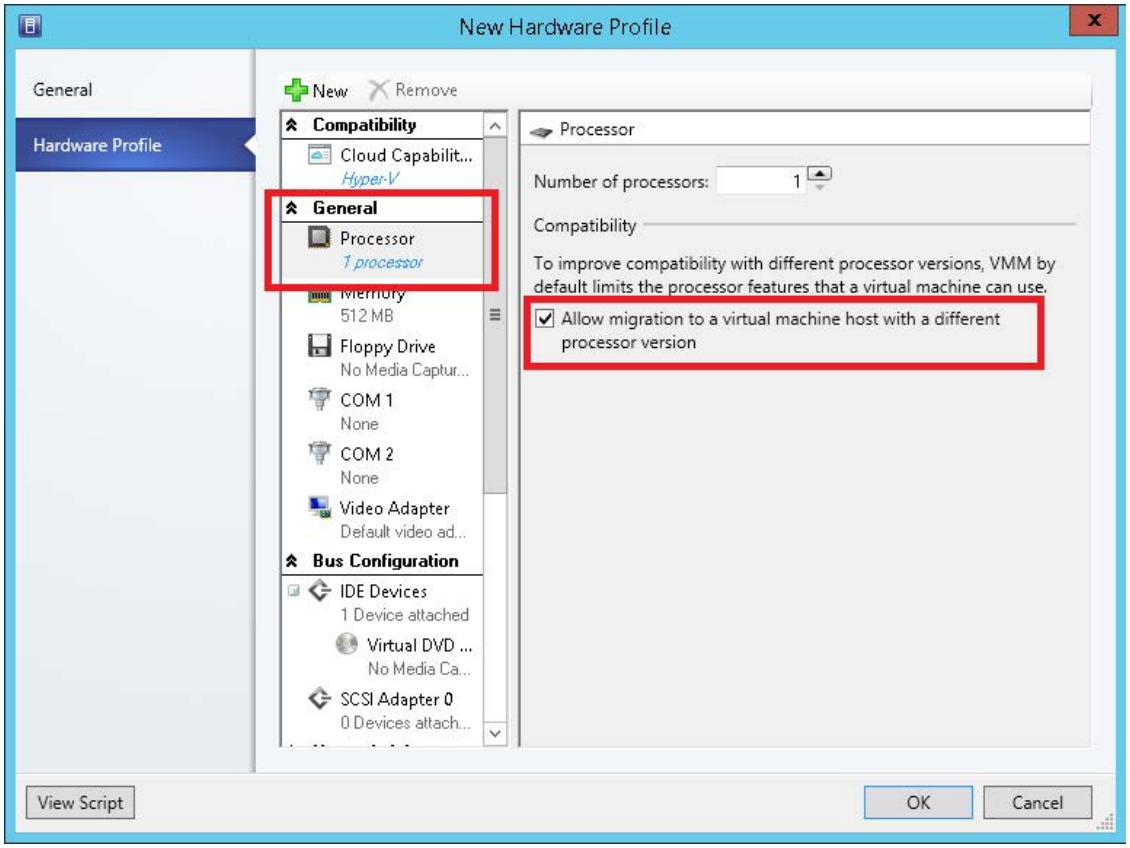
2. Hộp thoại **New Hardware Profile**, trong ô **Name**, nhập **WsStd2012R2**, trong ô **Description**, nhập **Hardware Profile for new Windows Server 2012 R2 Servers**.



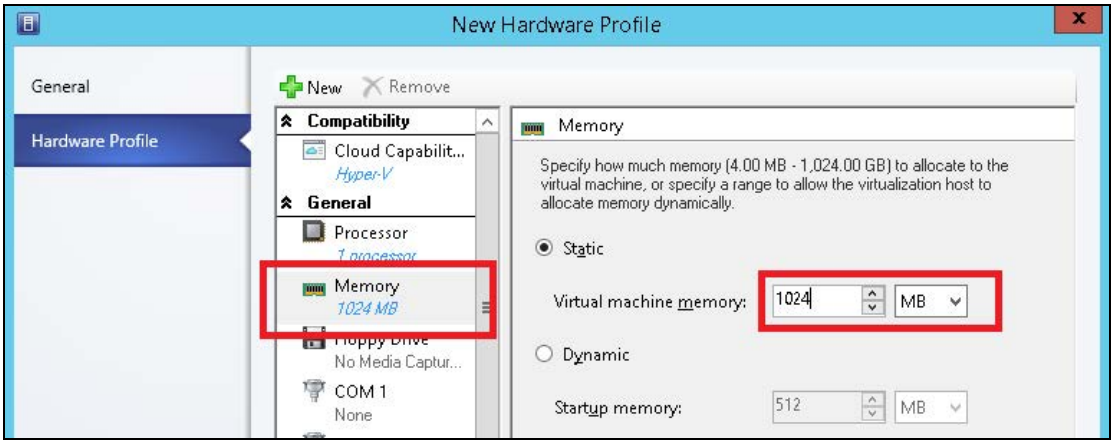

3. Chọn mục **Hardware Profile**, trong phần **Compatibility**, chọn **Cloud Capability Profile**, đánh dấu chọn **Hyper-V**.



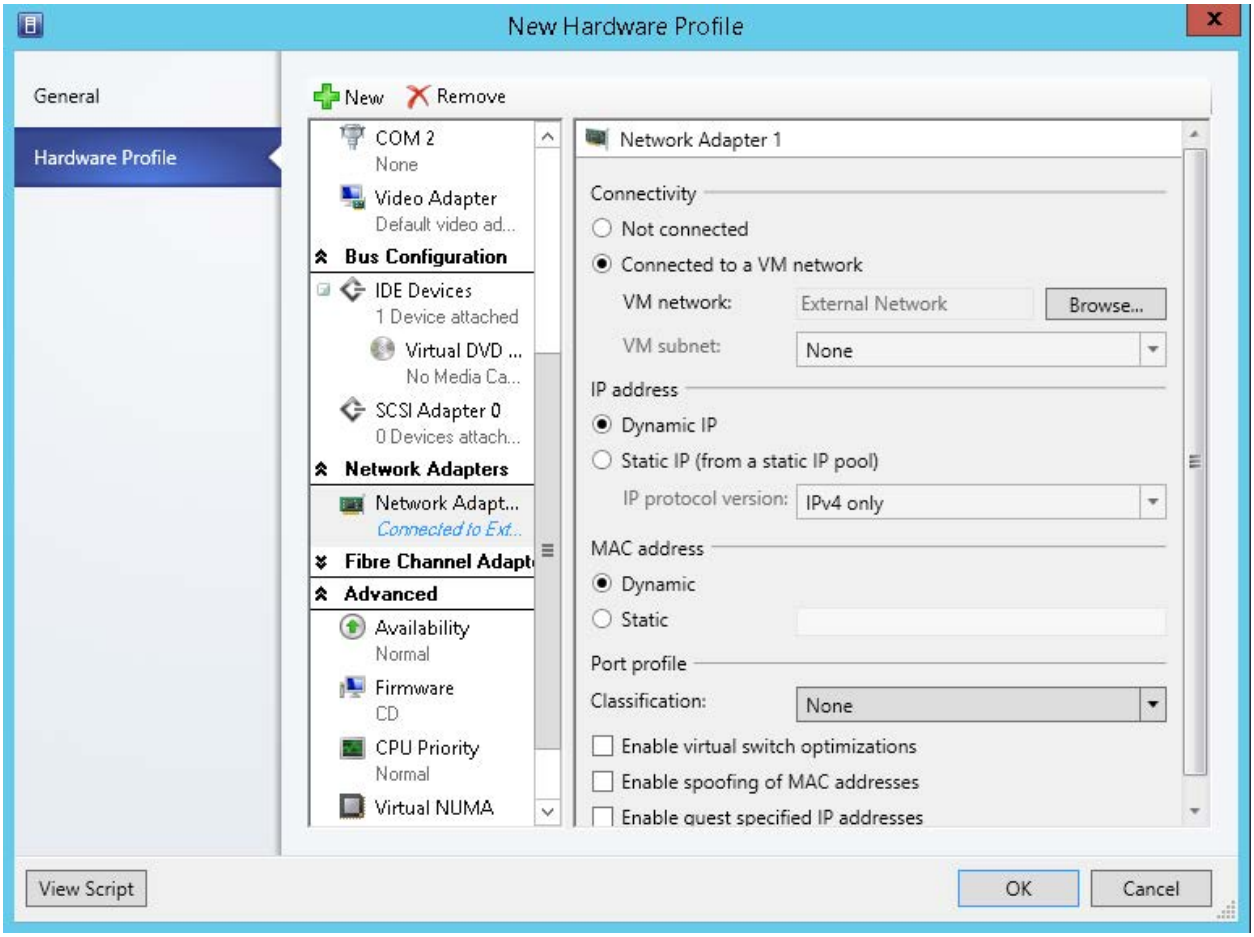
4. Trong phần **General**, chọn **Processor**, đánh dấu chọn **Allow migration to a virtual machine host with a different processor version**.



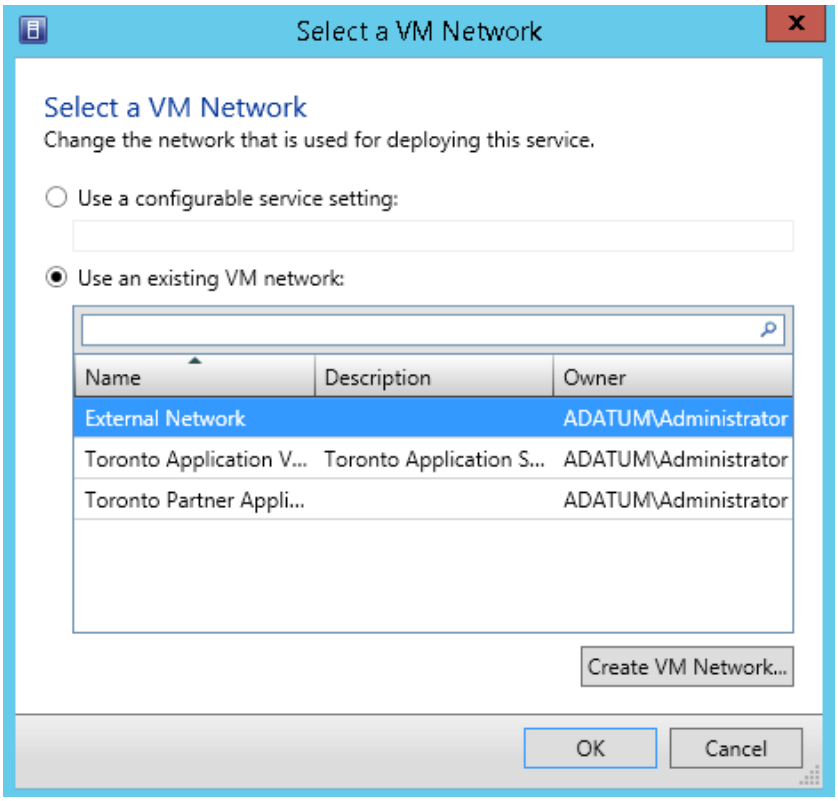

5. Chọn **Memory**, chọn **Static**, trong ô **Virtual machine memory** nhập**1024 MB**.



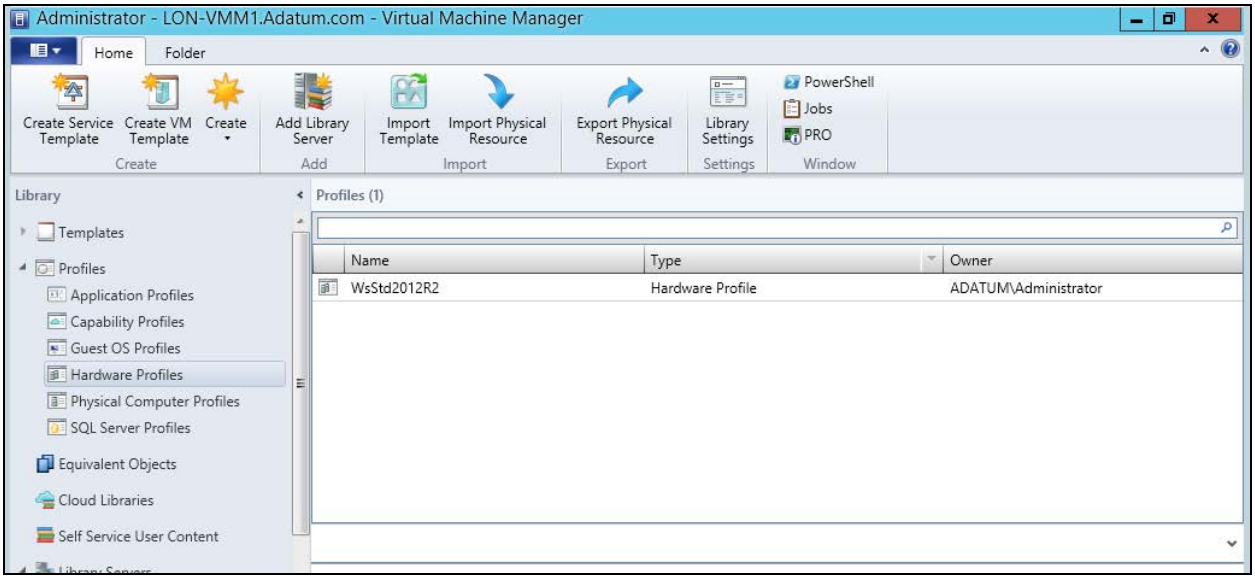
6. Trong phần **Network Adapters**, chọn **Network Adapter 1**, chọn **Connected to a VM network**, chọn **Browse**.



7. Hộp thoại **Select a VM Network**, chọn **External Network**, và chọn **OK** 2 lần.

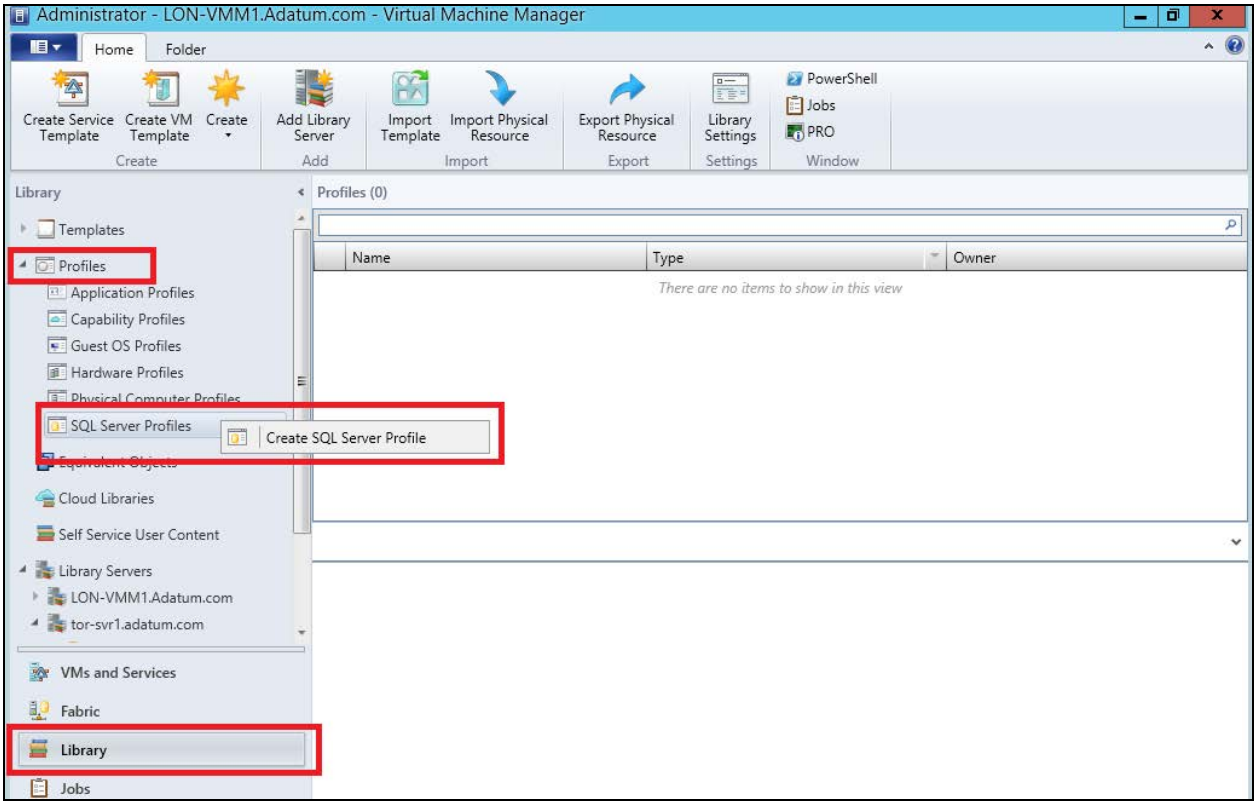



8. Kiểm tra có **Hardware Profile** mới tên **WsStd2012R2**



## Bước 3. Cấu hình SQL Server Profile.

1. Trên máy **LON-VMM1,** trong cửa sổ **VMM,** chọn **Library**, bung **Profiles**, chuột phải **SQL Server Profiles**, chọn **Create SQL Server Profile.**

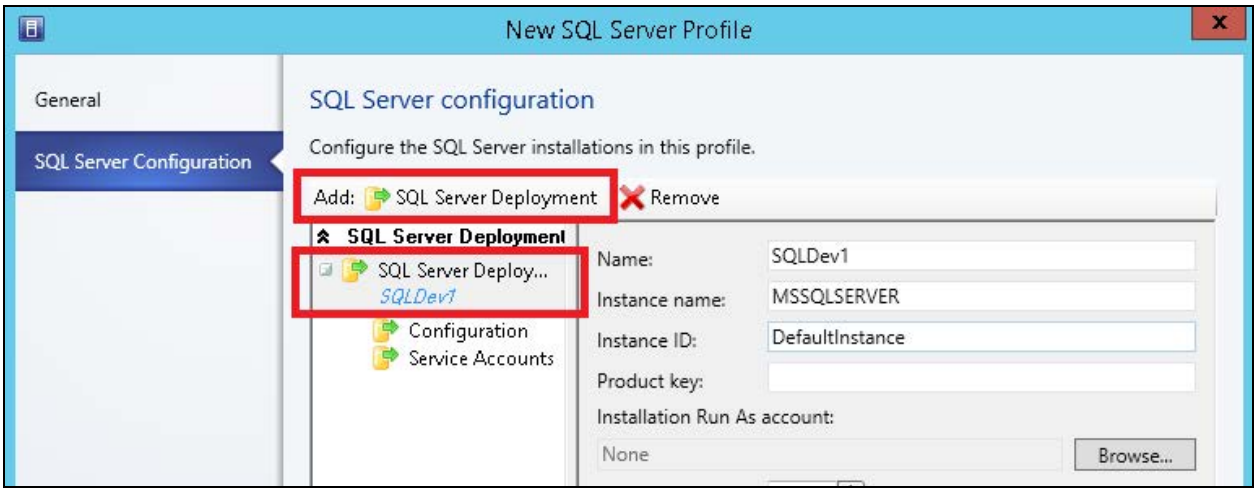


2. Hộp thoại **New SQL Server Profile**, trong ô **Name**, nhập **SQLDev1**, trong ô **Description**, nhập **Template for new SQL servers**.

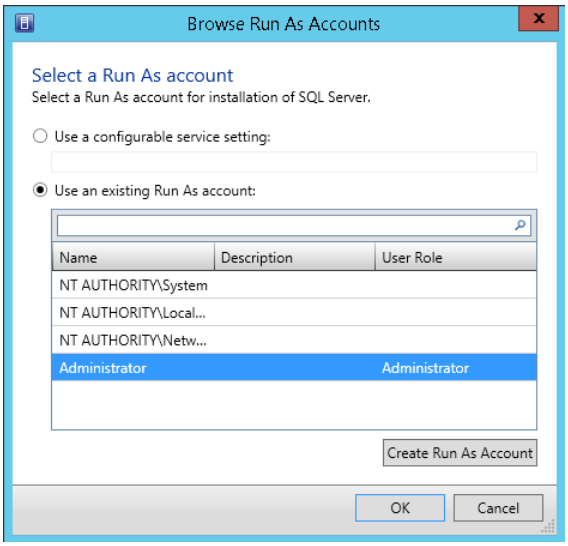



3. Chọn mục **SQL Server Configuration**, bung **Add**, chọn **SQL Server Deployment**, chọn **Add**. Khai báo thông tin như bên dưới, sau đó chọn **Browse**:

- Name: **SQLDev1**
- Instance name**: MSSQLSERVER**
- Instance ID: **DefaultInstance**

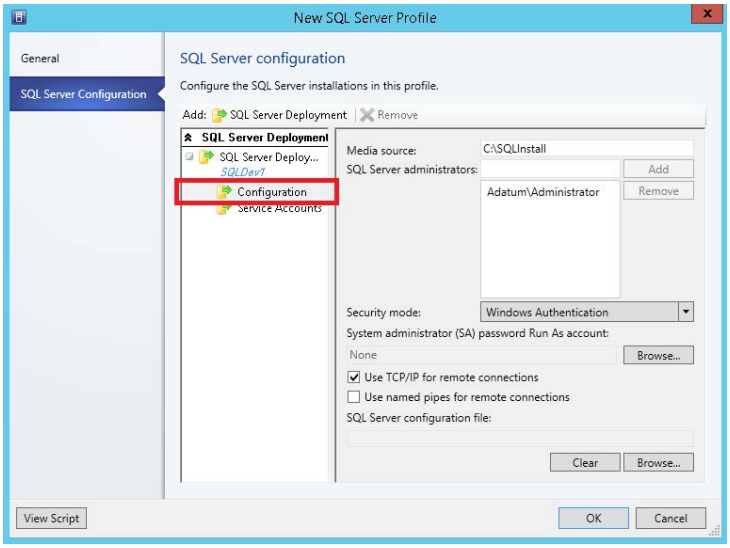


4. Hộp thoại **Browse Run As Accounts**, chọn **Administrator**, và chọn **OK**.



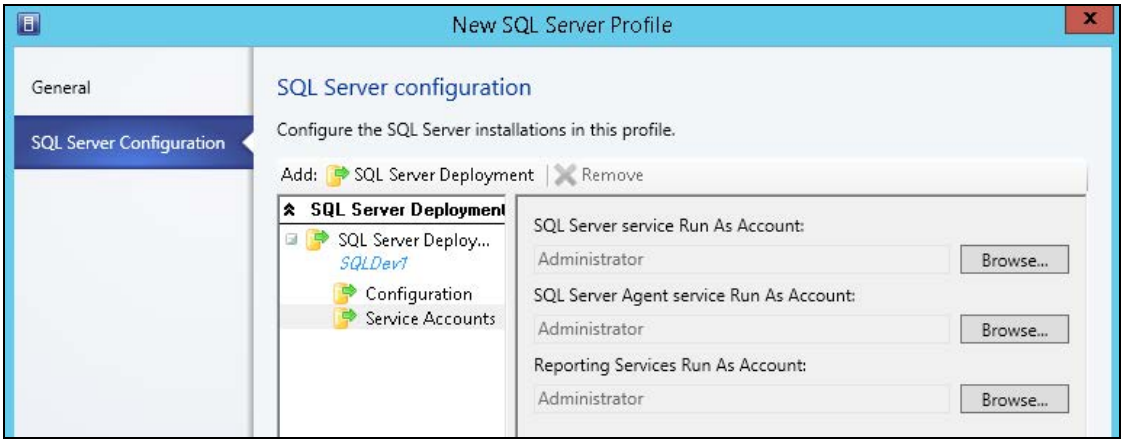

5. Hộp thoại **New SQL Server Profile,** chọn **Configuration**, khai báo thông tin như bên dưới:

- Media source: **C:\SQLInstall**
- Trong ô **SQL Server administrators**, nhập **Adatum\Administrator**, và chọn **Add.**
- Security mode: **Windows Authentication**
- Đánh dấu chọn **Use TCP\IP for remote connections**



6. Chọn **Service Accounts,** lần lượt chọn **Browse** và chọn **Administrator** cho cả 3 ô. Sau đó chọn **OK.**

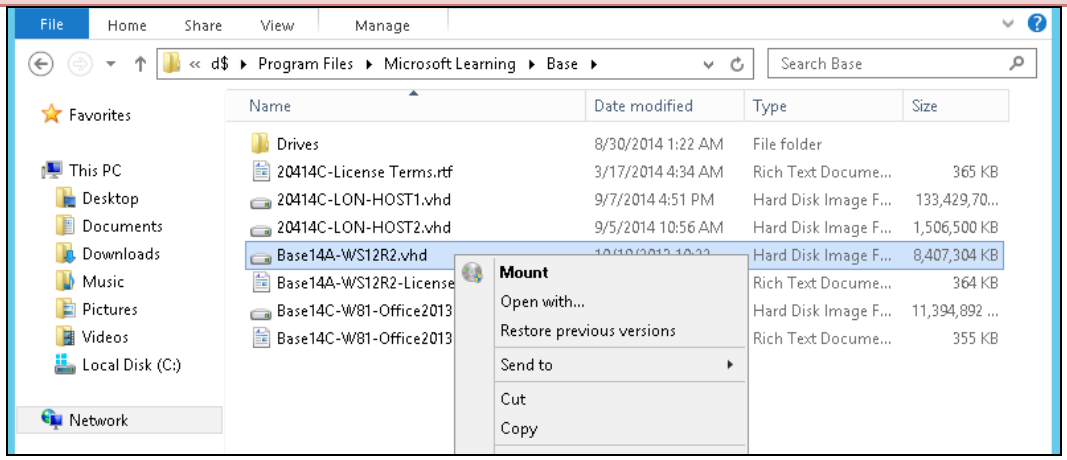
- SQL Server service Run As Account: **Administrator**
- SQL Agent service Run As Account: **Administrator**
- Reporting Services service Run As Account: **Administrator**



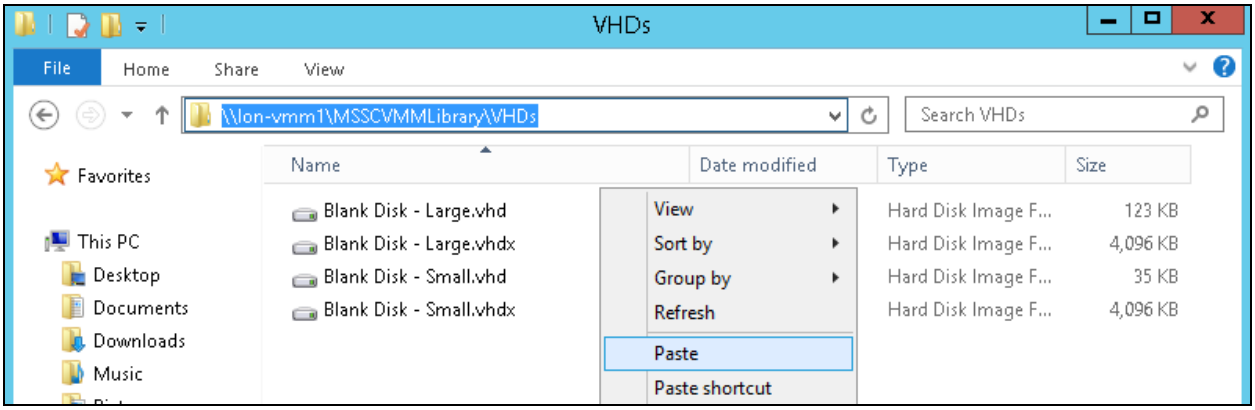

## Bước 4. Cấu hình Virtual Machine Template.

1. Trên máy **LON-VMM1**, mở **File Explorer**, truy cập **\\LON-HOST1\e$\Program Files\Microsoft Learning\Base**, copy file **Base14A-WS12R2.vhd**

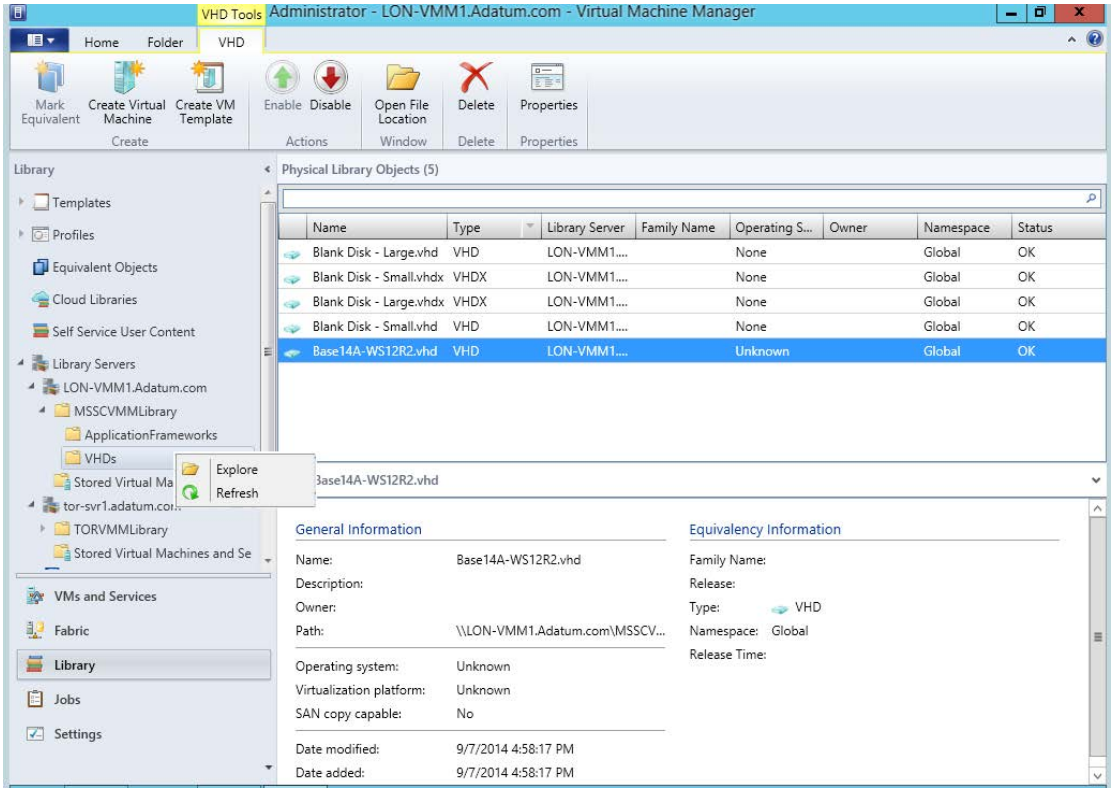
**Chú ý:** E$ là ổ đĩa chứa file máy ảo, nếu file máy ảo lưu ở ổ đĩa khác thì sửa lại đường dẫn cho phù hợp.



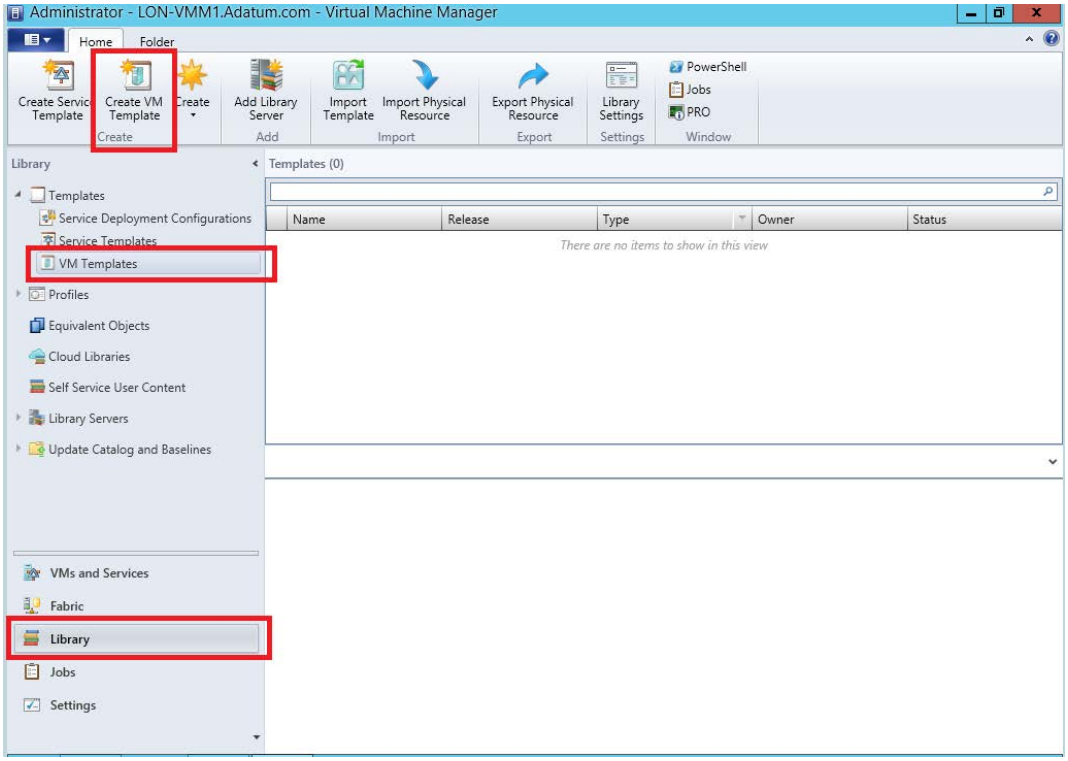
2. Truy cập **\\lon-vmm1\MSSCVMMLibrary\vhds\,** chuột phải lên khoảng trắng, chọn **Paste**. Đợi đến khi copy file thành công (khoảng vài phút).



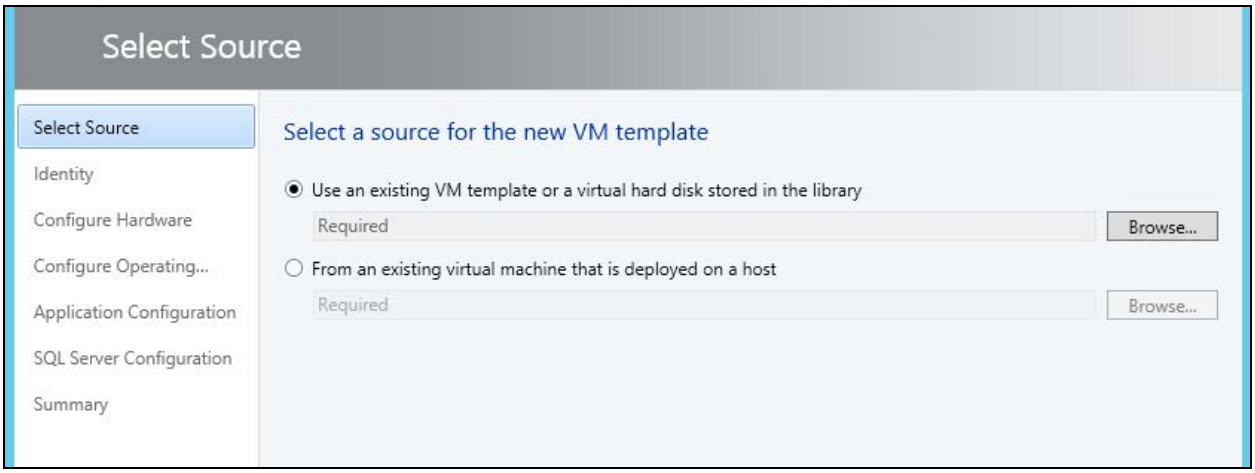

3. Trong cửa sổ **VMM**, chọn **Library**, bung **Library Servers**, bung **LON-VMM1.Adatum.com**, bung **MSSCVMMLibrary**, chuột phải **VHDs**, chọn **Refresh**. Kiểm tra có file **Base14A-WS12R2.vhd.**



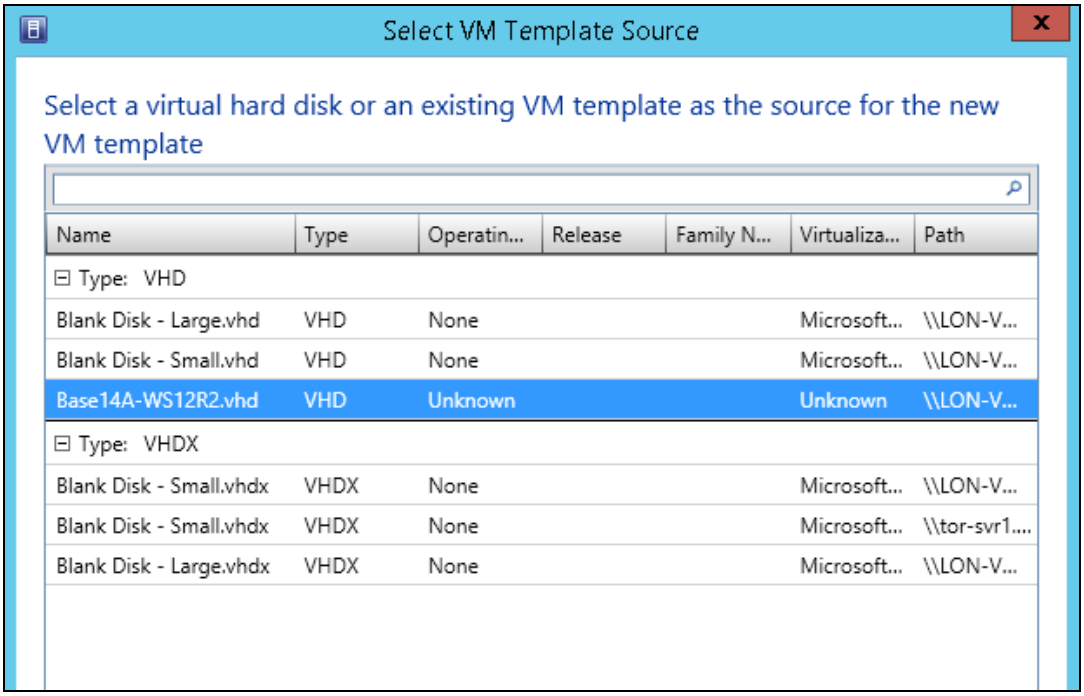
4. Trong cửa sổ **VMM**, chọn **Library**, bung **Templates**, chọn **VM Templates**, chọn **Create VM Template**.



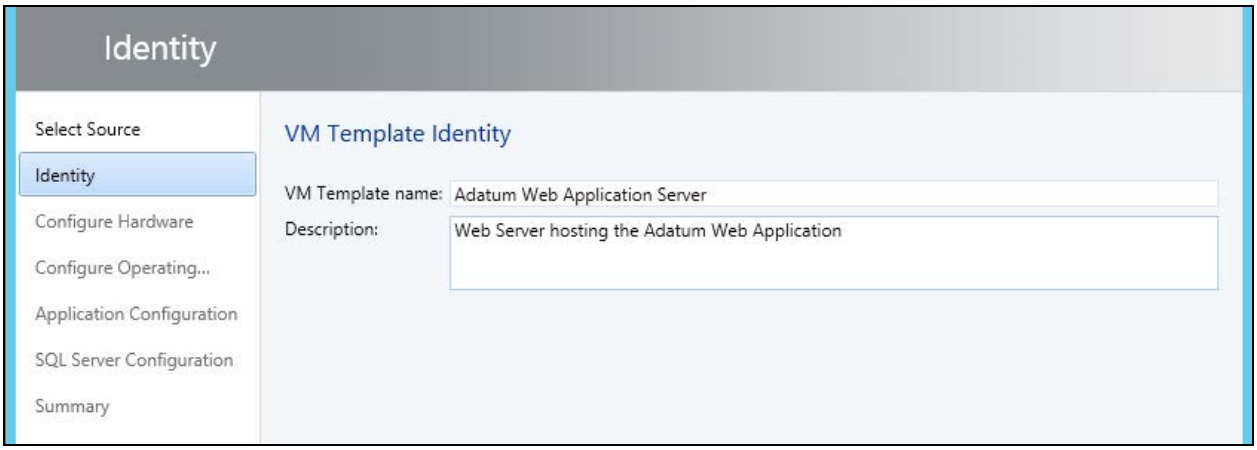

5. Cửa sổ **Select Source**, chọn **Use an existing VM template or a virtual hard disk stored in the library**, chọn **Browse**.



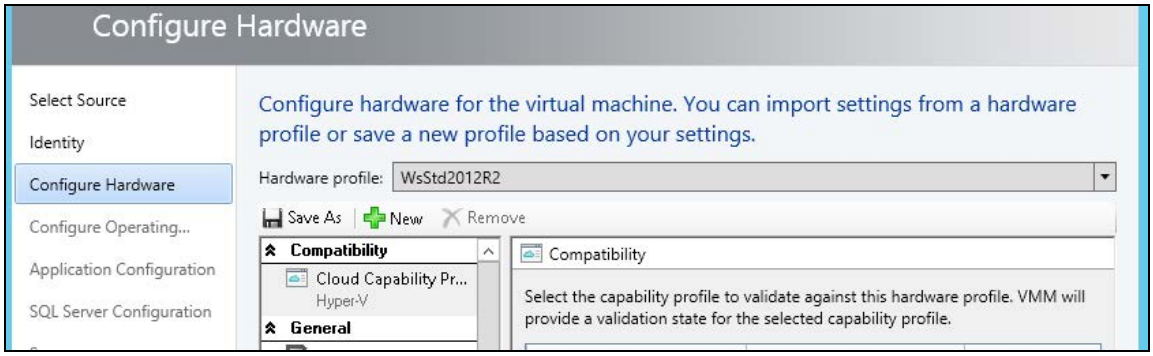
6. Hộp thoại **Select VM Template Source**, chọn **Base14A-WS12R2.vhd**, chọn **OK**, và chọn **Next**.



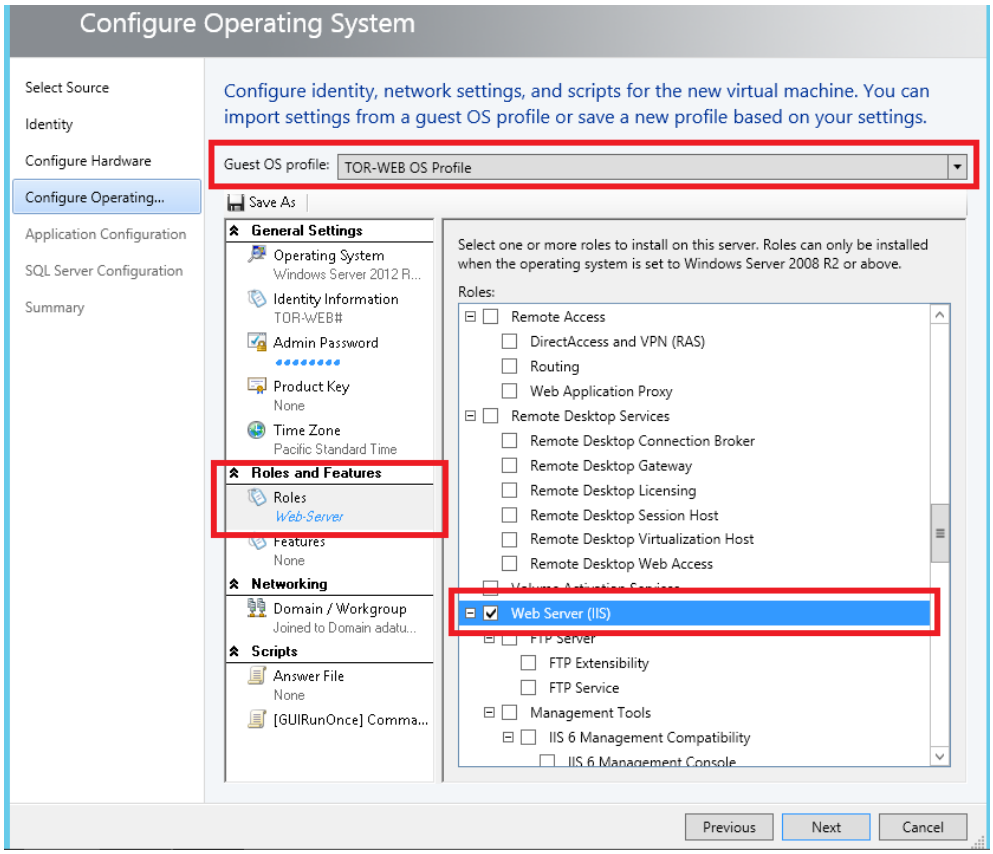

7. Cửa sổ **VM Template Identity**, trong ô **VM Template name**, nhập **Adatum Web Application Server**, tron gô **Description**, nhập **Web Server hosting the Adatum Web Application**, và chọn **Next**.



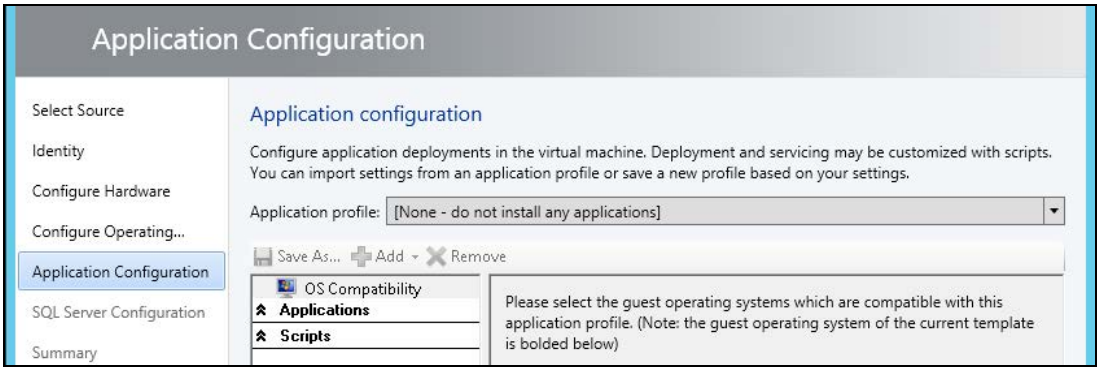
8. Cửa sổ **Configure Hardware**, bung ô **Hardware profile**, chọn **WsStd2012R2**, và chọn **Next**.



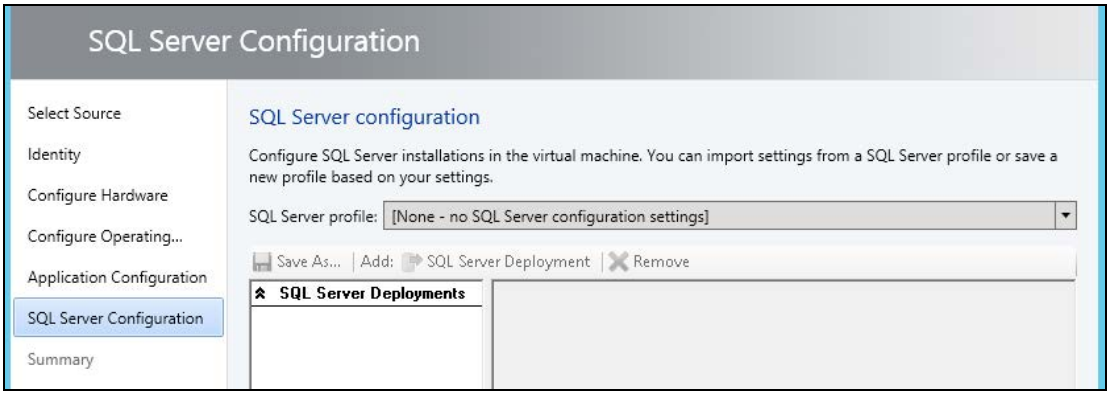

9. Cửa sổ **Configure Operating System**, bung ô **Guest OS profile**, chọn **TOR-WEB OS Profile**. Trong phần **Roles and Features**, chọn **Roles**, đánh dấu chọn **Web Server (IIS)**, và chọn **Next**.



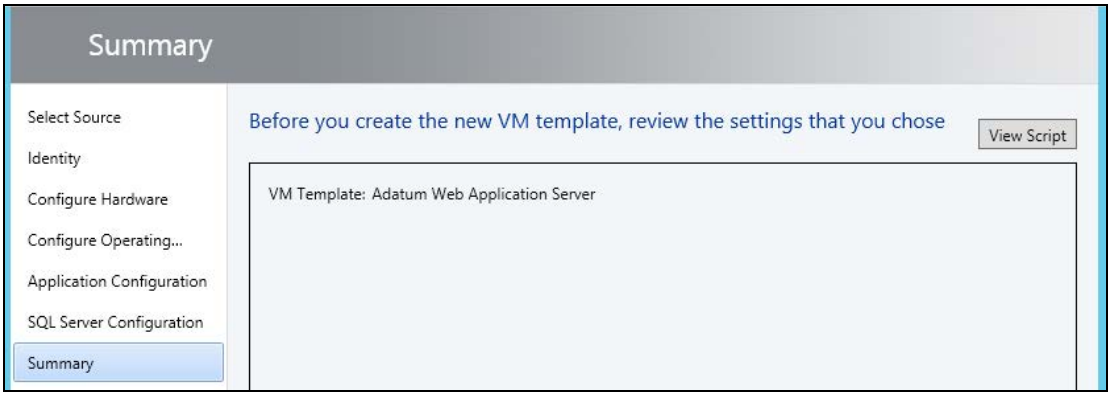
10. Cửa sổ **Applications Configuration**, bung ô **Application profile**, chọn **None – do not install any applications**, và chọn **Next**.



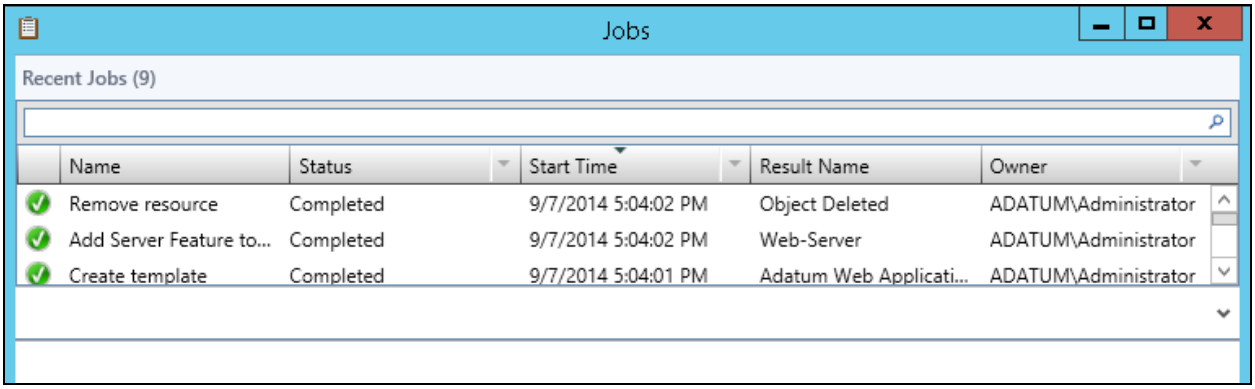

11. Cửa sổ **SQL Server Configuration**, bung ô **SQL Server profile**, chọn **None - no SQL Server configuration settings**, và chọn **Next**.




12. Cửa sổ **Summary**, chọn **Create**.

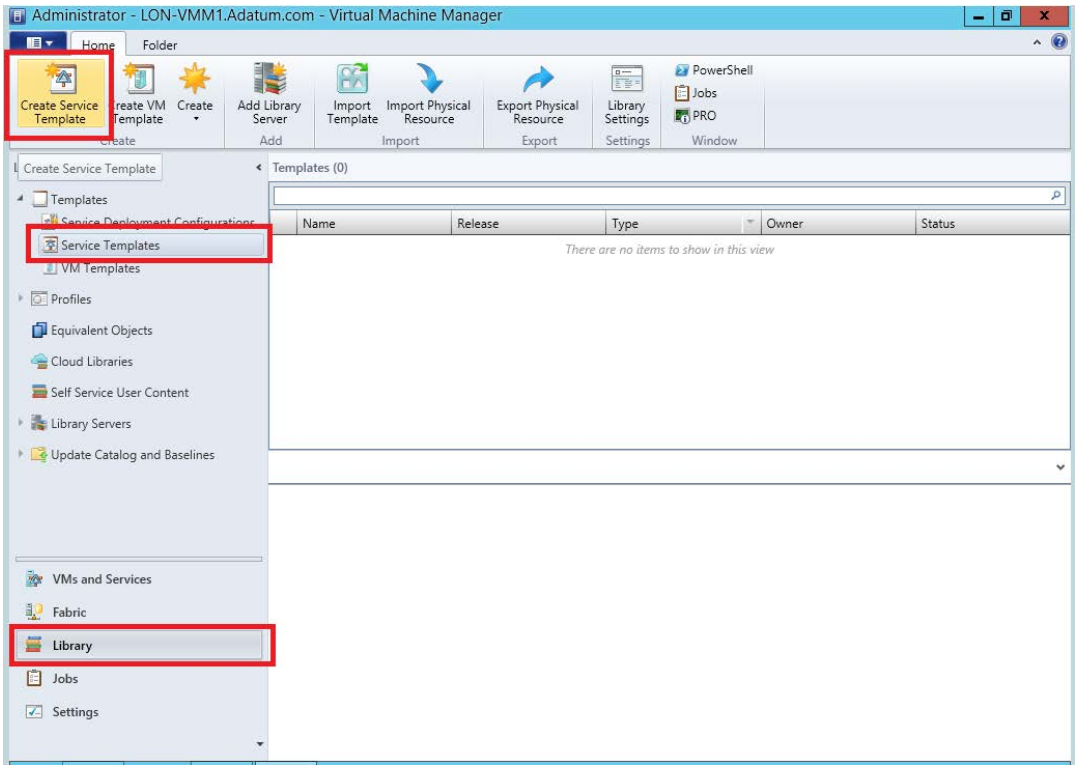


13. Kiểm tra và tắt cửa sổ **Jobs**.

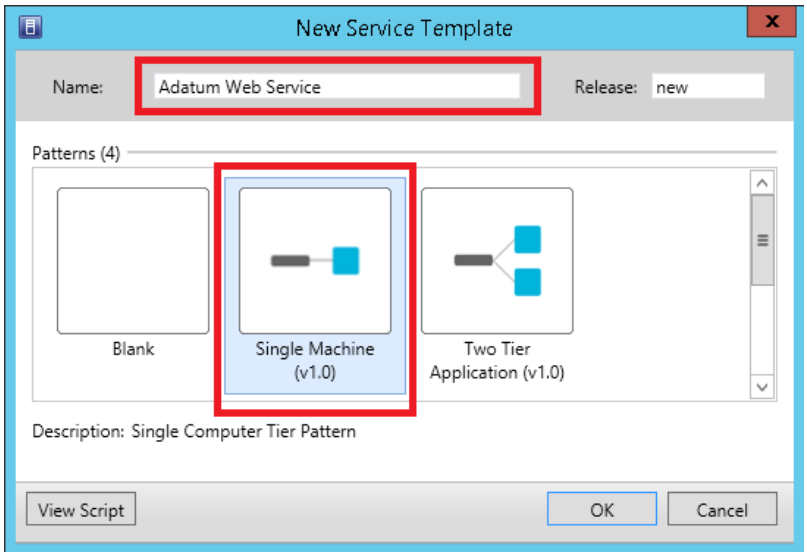



## Bước 5. Cấu hình a Service Template.

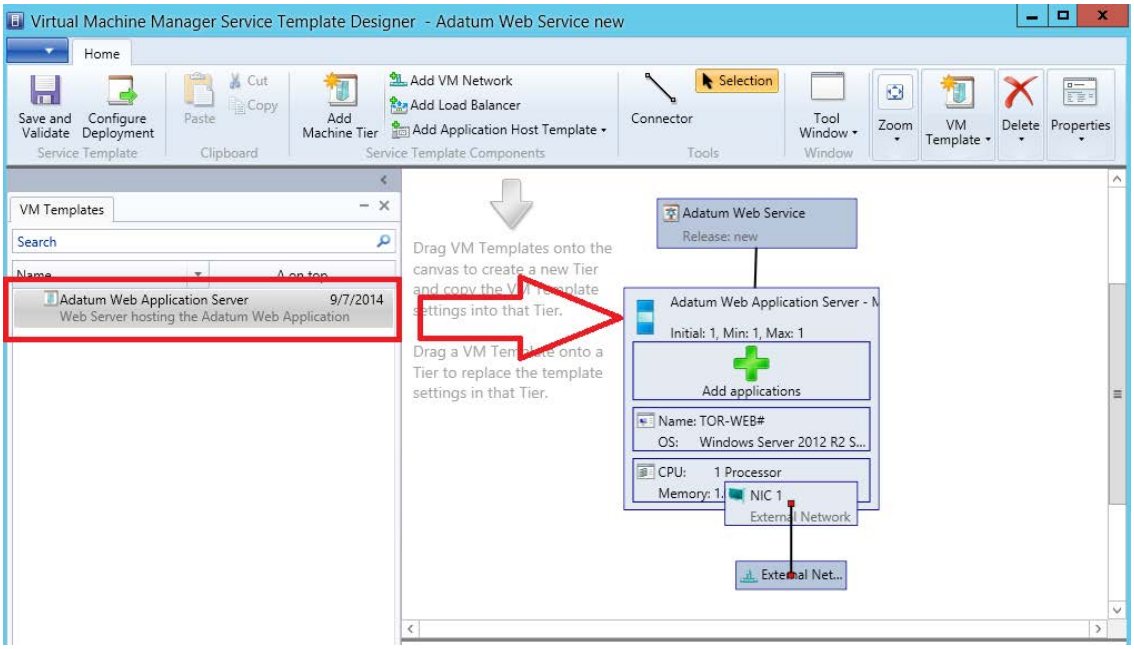
1. Trên máy **LON-VMM1**, trong cửa sổ **VMM**, chọn **Library**, bung **Templates**, và chọn **Service Templates**, và chọn **Create Service Template**.



2. Hộp thoại **New Service Template**, trong ô **Name**, nhập **Adatum Web Service**, trong phần **Patterns**, chọn **Single Machine**, và chọn **OK**. Đợi đến khi giao diện Adatum Web Service Template Designer hiển thị.




3. Cửa sổ **VMM Service Template Designer,** trong phần **VM Templates**, chọn và kéo **Adatum Web Application Server** vào ô **Add applications**. Chọn **Save and Validate**.



4. Tắt cửa sổ **VMM Service Template Designer.**

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công các VMM Profiles và VMM Templates.**

## Bài tập 2: Triển khai Hyper-V Replica.

Một trong những lựa chọn để cung cấp khả năng sẵn sàng cao máy ảo là cấu hình Hyper-V Replica. A.Datum đã quyết định thực hiện Hyper-V Replica cho một trong các server quan trọng nằm ở trung tâm dữ liệu Toronto. Tuy nhiên, đầu tiên họ chỉ muốn kiểm tra chức năng Hyper-V Replica, vì vậy họ sử dụng máy ảo 20414C-LON-CORE như một nền tảng thử nghiệm để đánh giá chức năng Hyper-V Replica.

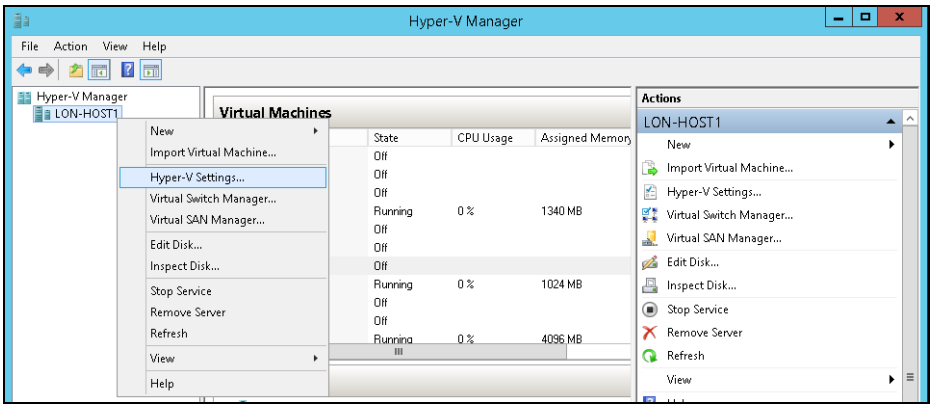
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Hyper-V Replica trên LON-HOST1 và LON-HOST2.
2. Cấu hình đồng bộ cho máy ảo 20414C-LON-CORE.
3. Kiểm tra chức năng Hyper-V Replica

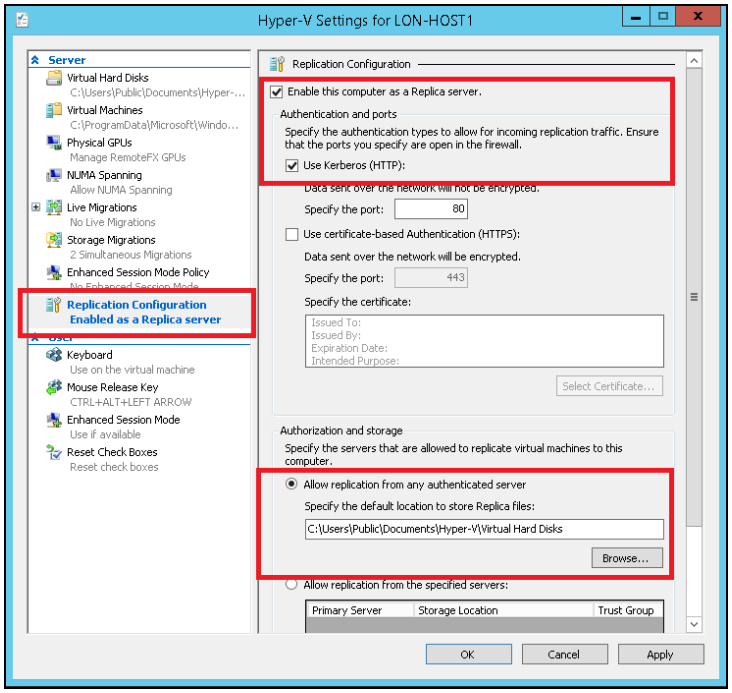
❖ **Thực hiện:**

**Bước 1. Cấu hình Hyper-V Replica trên LON-HOST1 và LON-HOST2.**

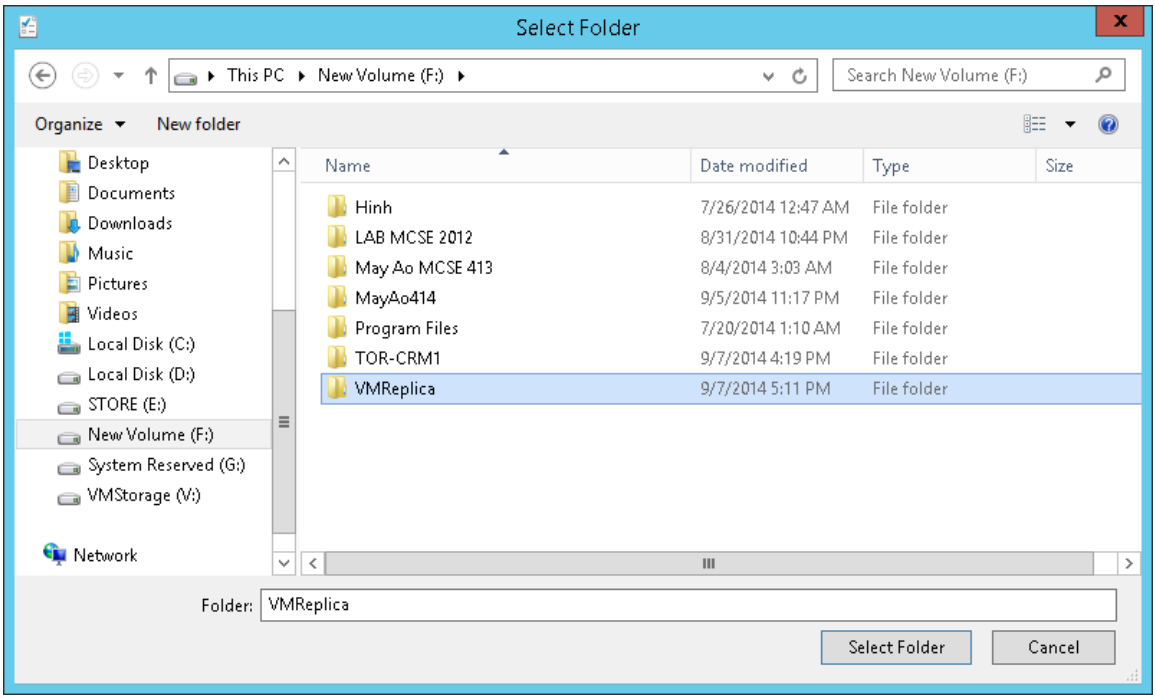
1. Trên máy **LON-HOST1** (máy thật). Mở **Hyper-V Manager**, chuột phải **LON-HOST1**, chọn **Hyper-V Settings**.



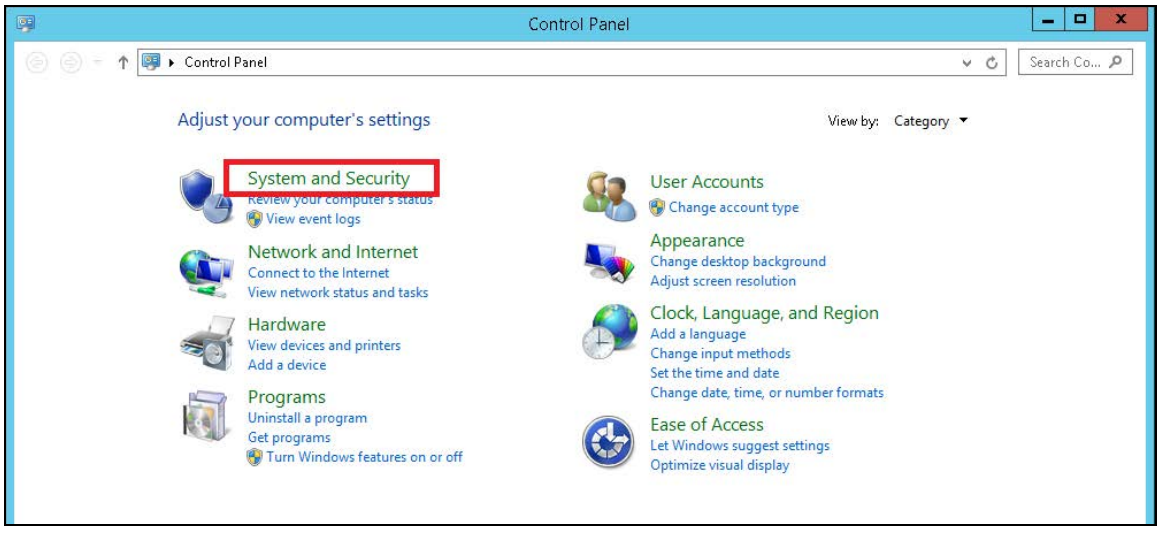

2. Trong cửa sổ **Hyper-V Settings for LON-HOST1**, chọn **Replication Configuration**, đánh dấu chọn 2 ô **Enable this Computer as a Replica Server** và **Use Kerberos (HTTP)**. Chọn **Allow replication from any authenticated server**, và chọn **Browse.**



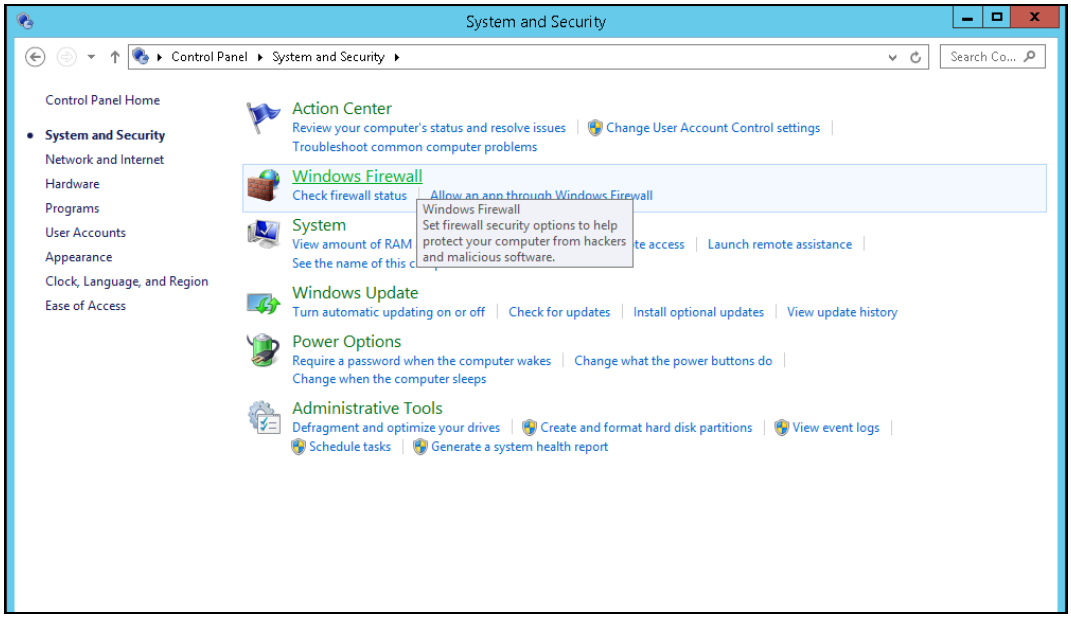
3. Hộp thoại Select Folder, trỏ đường dẫn vào ổ **Local Disk (E:)**, Tạo folder mới, đặt tên **VMReplica.** Chọn folder **VMReplica**, chọn **Select Folder**, và chọn **OK** (*Chú ý: Các ký tự ổ đĩa có thể thay đổi tùy thuộc vào cấu hình phần cứng của mỗi máy.*)



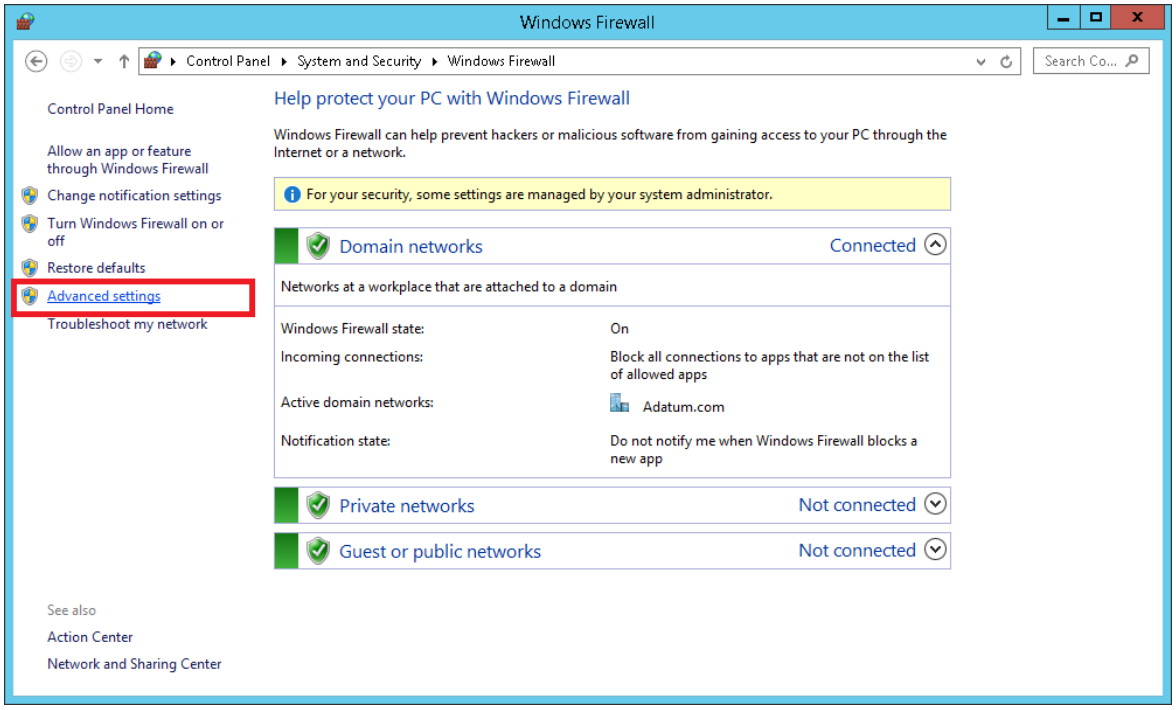

4. Mở **Control Panel**, chọn **System and Security**



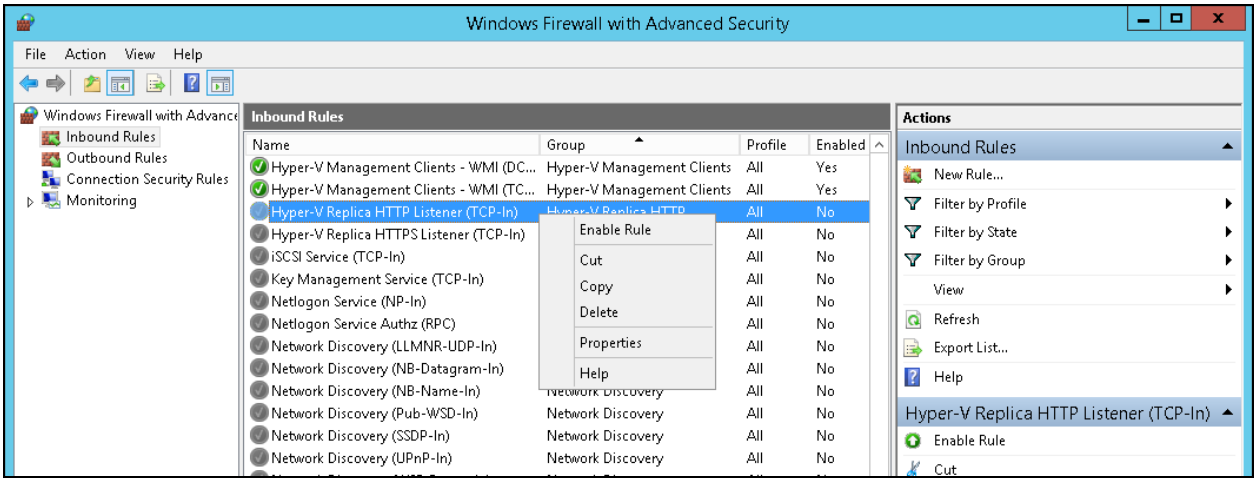
5. Cửa sổ **System and Security**, chọn **Windows Firewall**.




6. Cửa sổ **Windows Firewall,** chọn **Advanced settings**.



7. Cửa sổ **Windows Firewall with Advanced Security,** chọn **Inbound Rules**, chuột phải lên rule **Hyper-V Replica HTTP Listener (TCP-In)**, chọn **Enable Rule**.

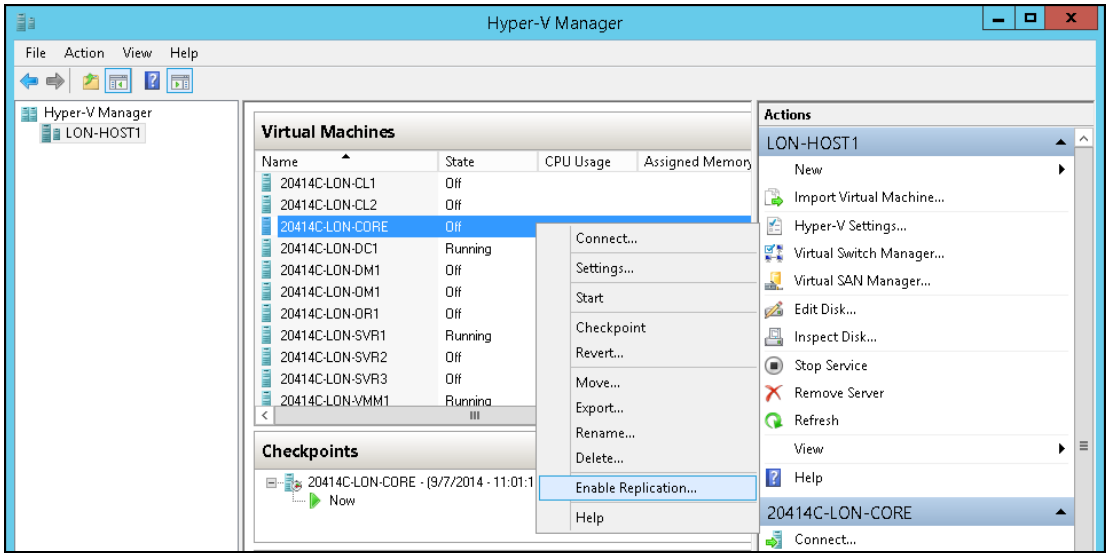



8. Tắt cửa sổ **Windows Firewall with Advanced Security**, và **Windows Firewall**.

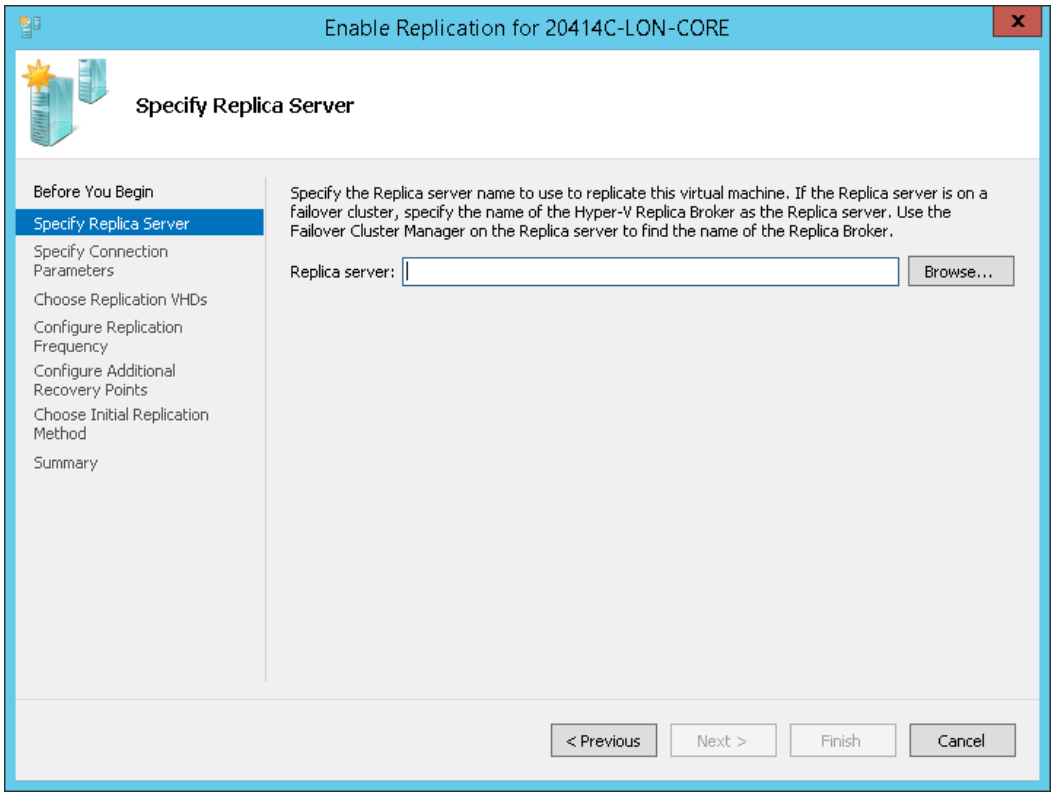
9. Qua máy **LON-HOST2** (máy thật), Lặp lại từ bước 1 đến 8 .

## Bước 2. Cấu hình đồng bộ cho máy ảo 20414C-LON-CORE.

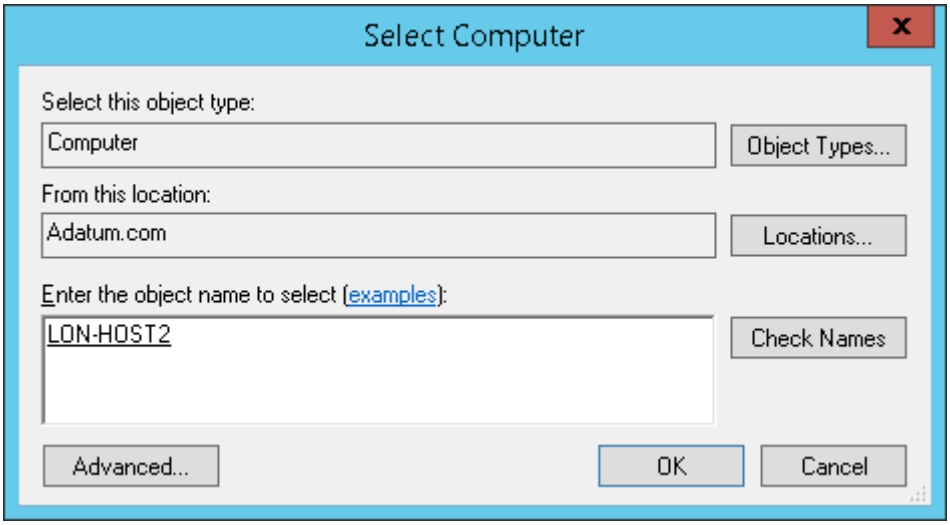
1. Qua máy **LON-HOST1** (máy thật), mở **Hyper-V Manager**, chuột phải máy ảo **20414C-LON-CORE**, chọn **Enable Replication**.



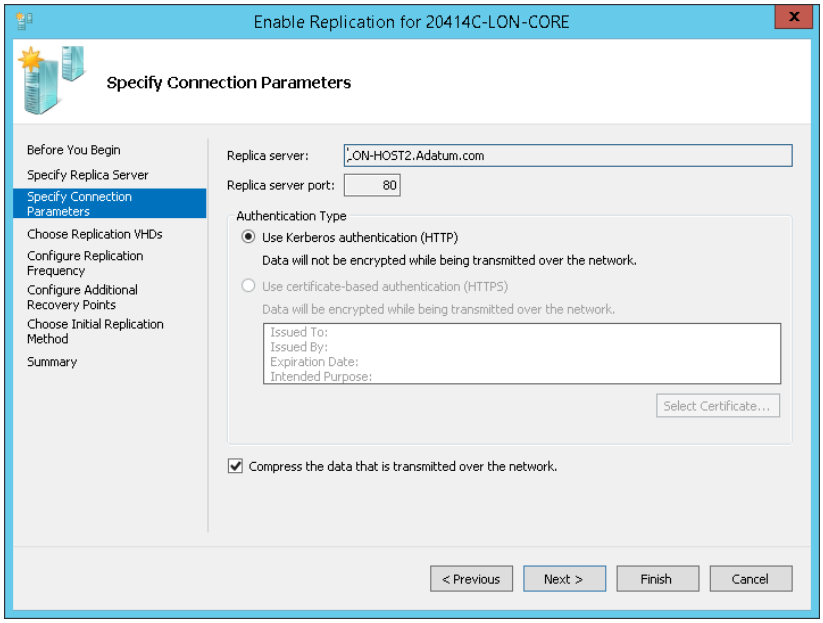
2. Cửa sổ **Before You Begin**, chọn **Next**. Cửa sổ **Specify Replica Server**, chọn **Browse**.



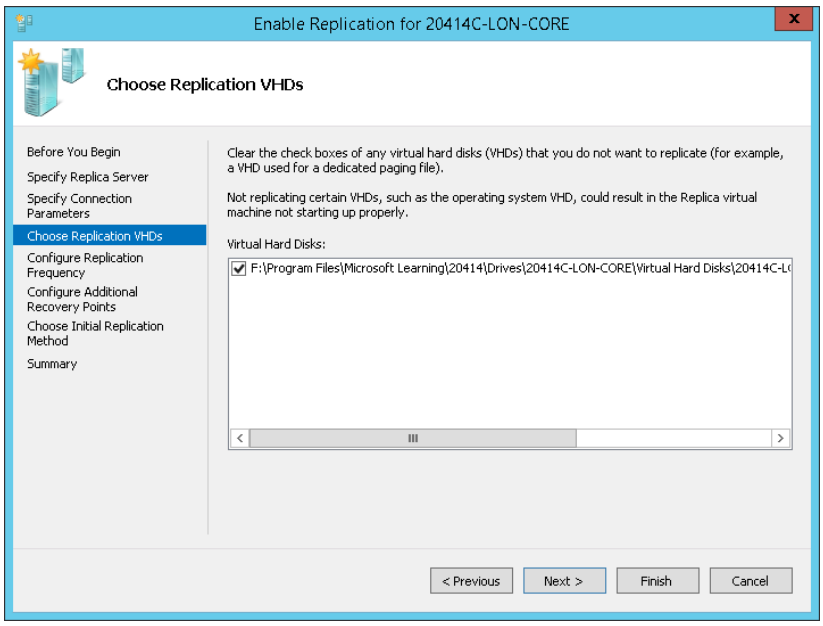

3. Hộp thoại **Select Computer**, nhập **LON-HOST2**, chọn **Check Names**, chọn **OK**, và chọn **Next**.



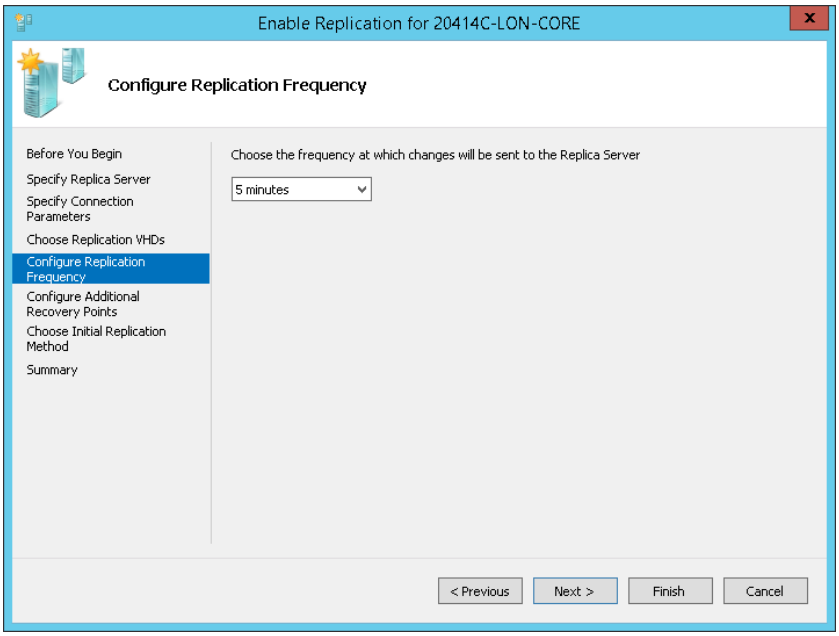
4. Cửa sổ **Specify Connection Parameters**, đảm bảo chọn **Use Kerberos Authentication (HTTP)**, chọn **Next**.



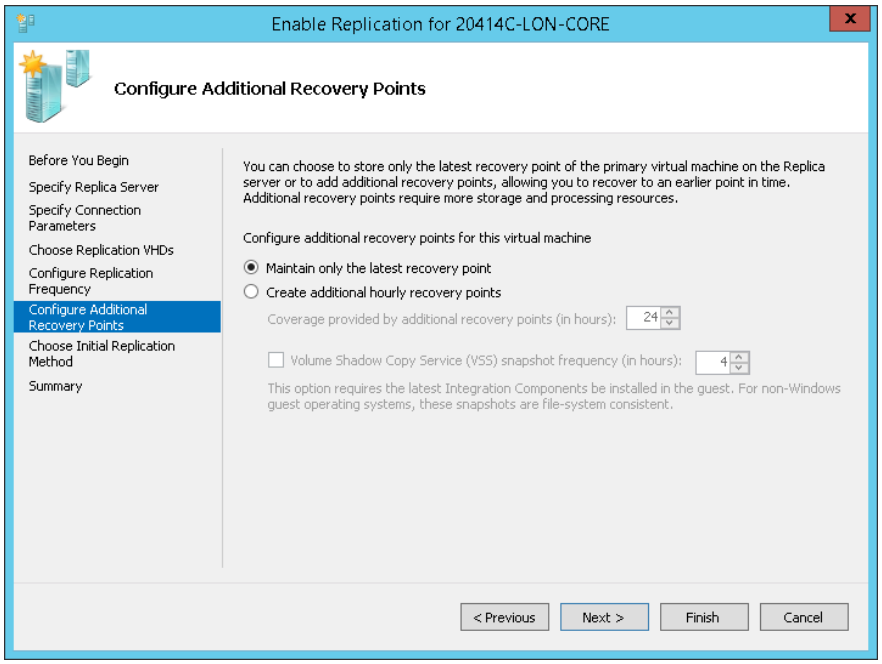

5. Cửa sổ **Choose Replication VHDs**, đảm bảo chọn file **20414C-LON-CORE.avhd**, chọn **Next**.



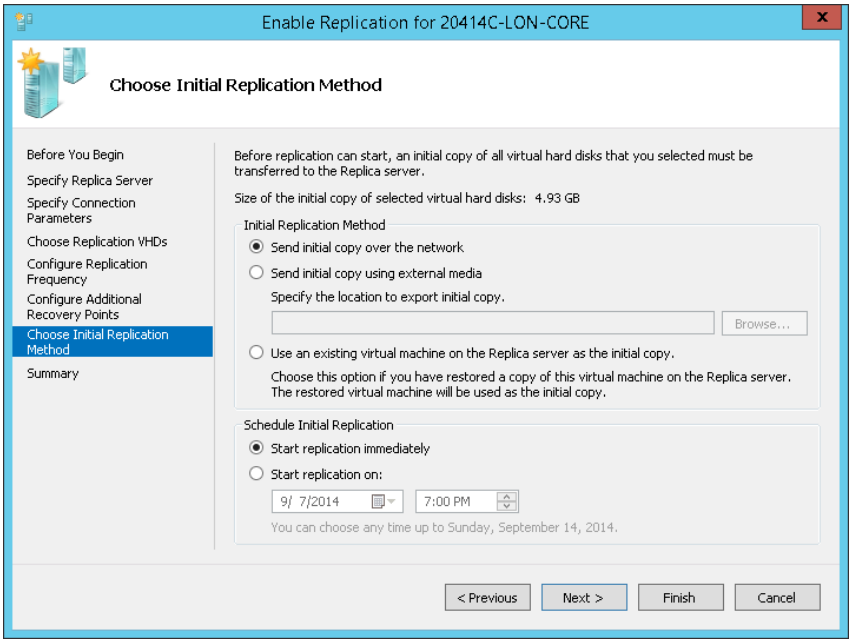
6. Cửa sổ **Configure Replication Frequency**, chọn **Next.**



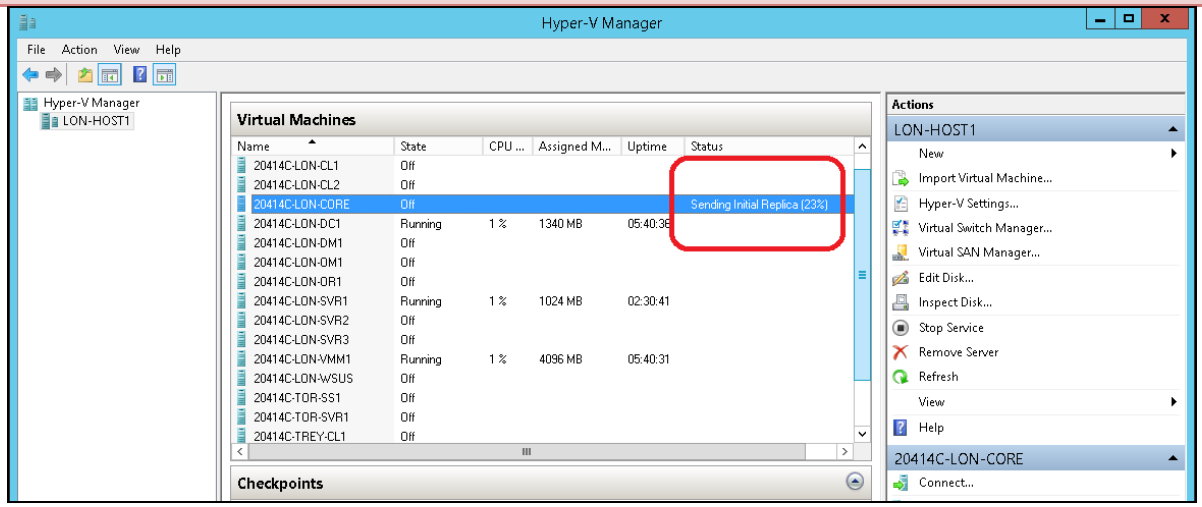

7. Cửa sổ **Configure Additional Recovery Points**, chọn **Maintain only the latest recovery point**, và chọn **Next**.



8. Cửa sổ **Choose Initial Replication Method**, chọn **Send initial copy over the network**, chọn **Start replication immediately**, và chọn **Next**. Và chọn **Finish**

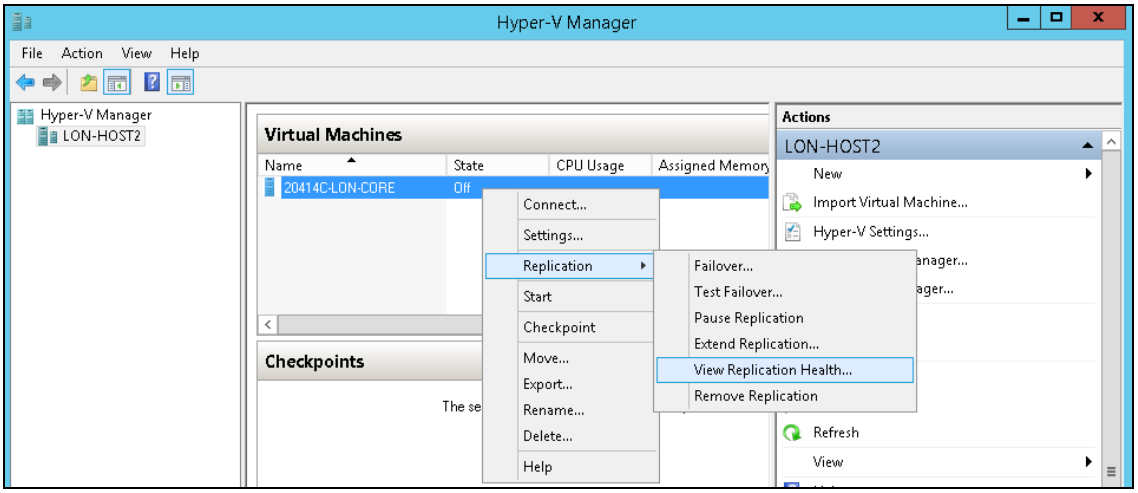



**Chú ý: Thời gian đồng bộ khoảng 5 đến 10 phút. Trên máy LON-HOST1, bạn có thể kiểm tra tình trạng đồng bộ ở cột Status trong cửa sổ Hyper-V Manager. Khi đồng bộ thành công (100%), kiểm tra máy ảo 20414C-LON-CORE đã được hiển thị trong cửa sổ Hyper-V Manager trên máy LON-HOST2.**

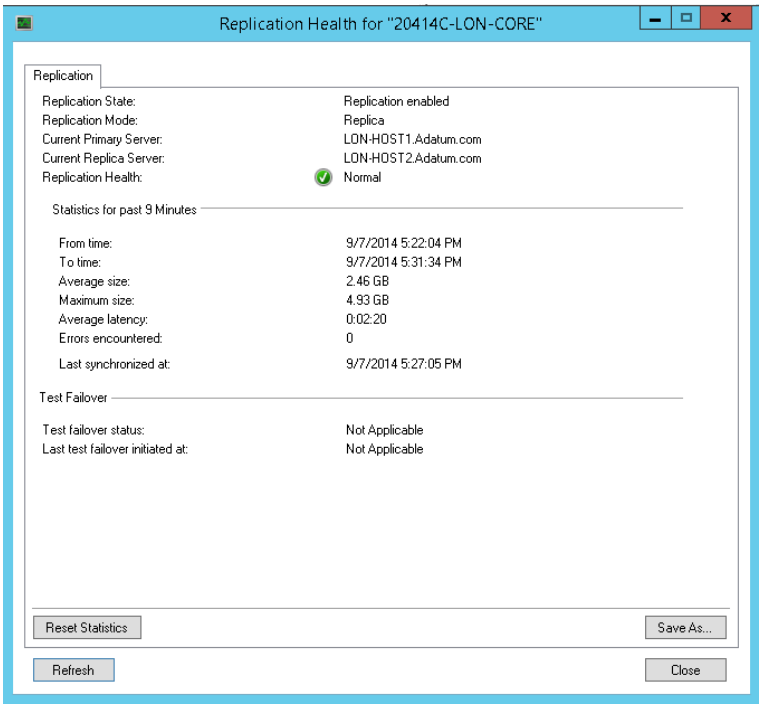


## Bước 3. Kiểm tra chức năng Hyper-V Replica.

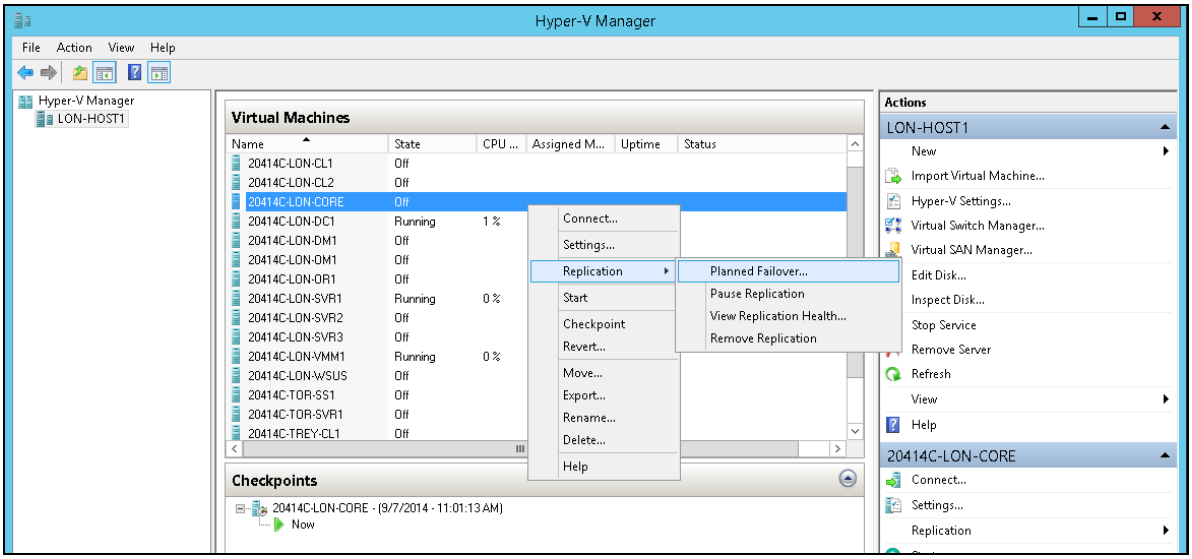
1. Qua máy **LON-HOST2,** trong cửa sổ **Hyper-V Manager**, chuột phải **20414C-LON-CORE**, chọn **Replication**, chọn **View Replication Health**.



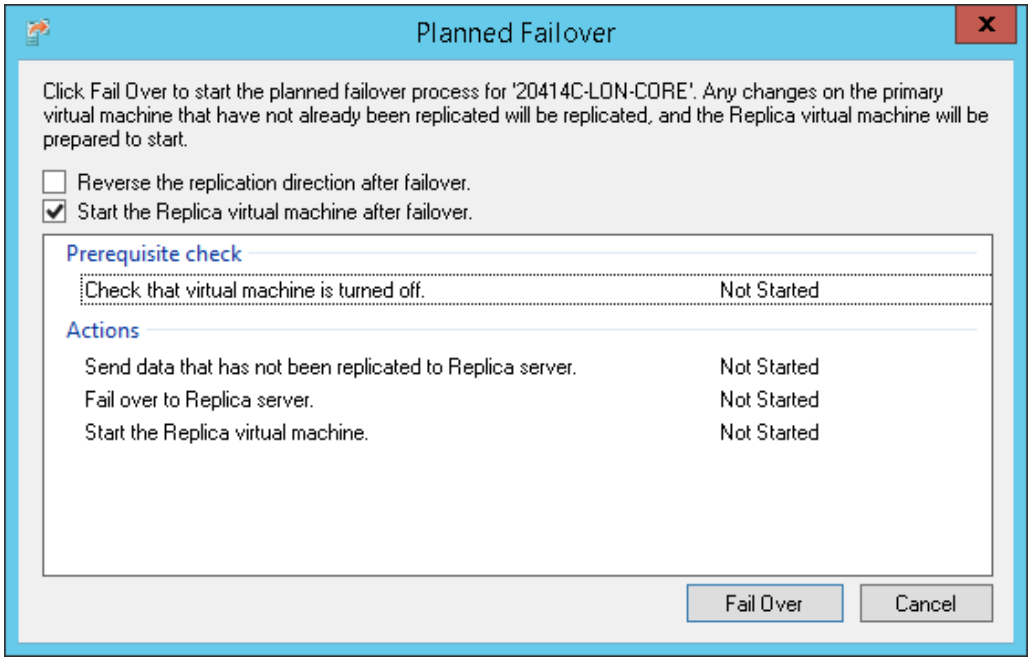

2. Trong hộp thoại **Replication Health for "20414C-LON-CORE".** Kiểm tra không xảy ra lỗi, và chọn **Close**.



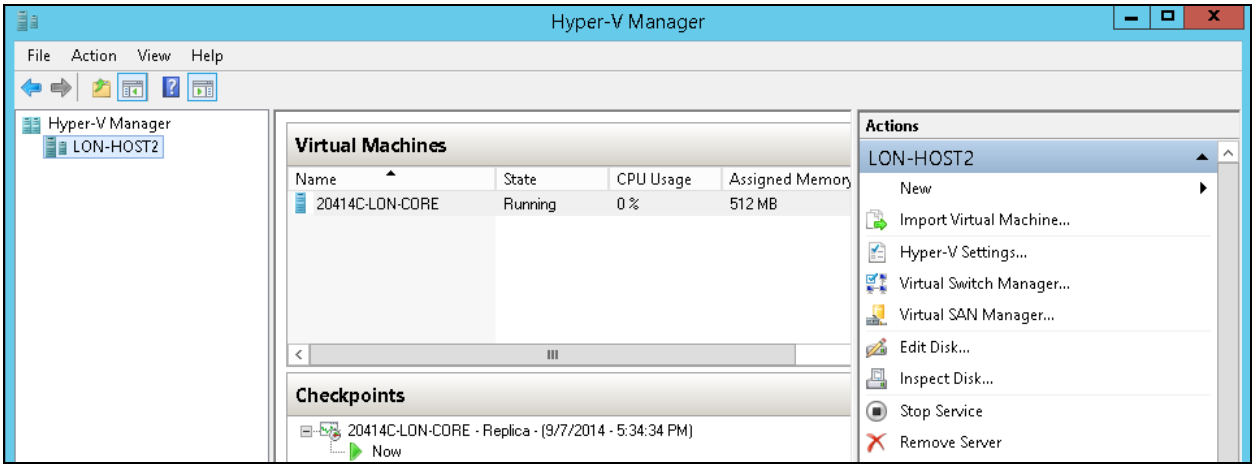
3. Qua máy **LON-HOST1**, mở **Hyper-V Manager**, kiểm tra máy ảo **20414C-LON-CORE** chưa khởi động. Chuột phải **20414C-LON-CORE**, chọn **Replication**, và chọn **Planned Failover**.



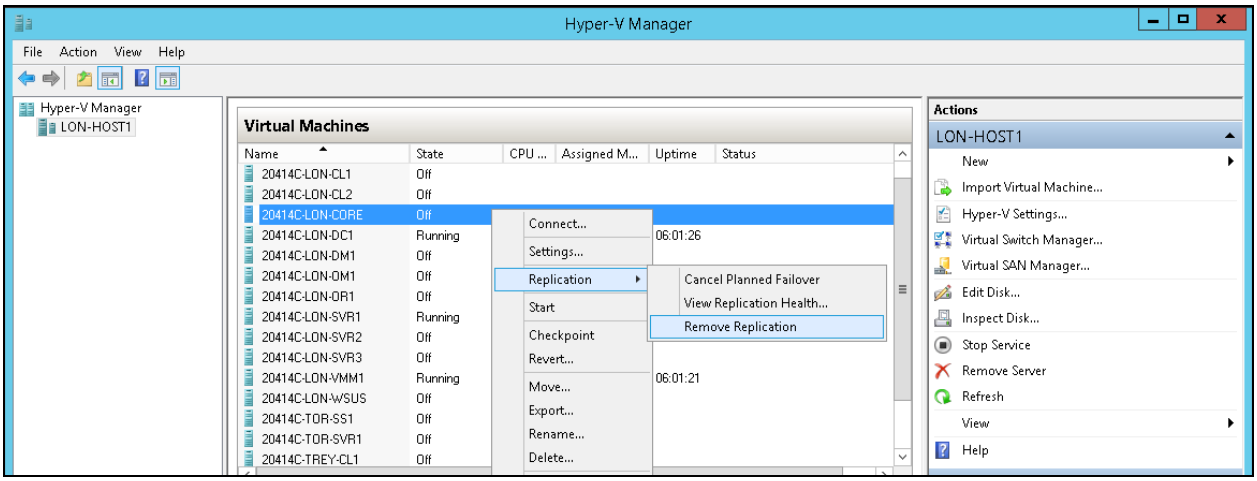

4. Hộp thoại **Planned Failover**, đảm bảo đánh dấu chọn **Start the replica virtual machine after failover**, và chọn **Fail Over**.



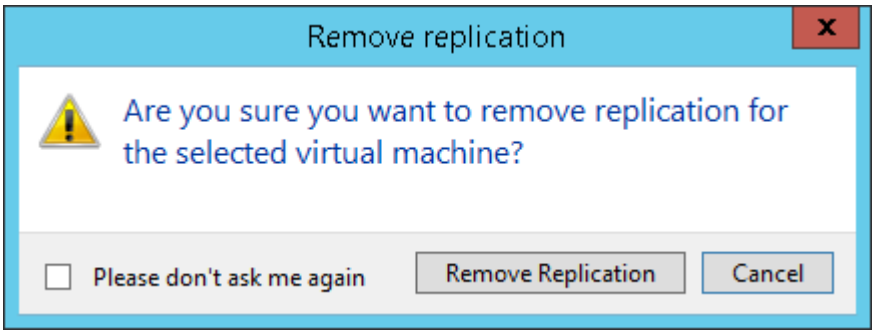
5. Qua máy **LON-HOST2**, trong cửa sổ **Hyper-V Manager**, kiểm tra máy ảo**20414C-LON-CORE** đang ở trạng thái **Running**.



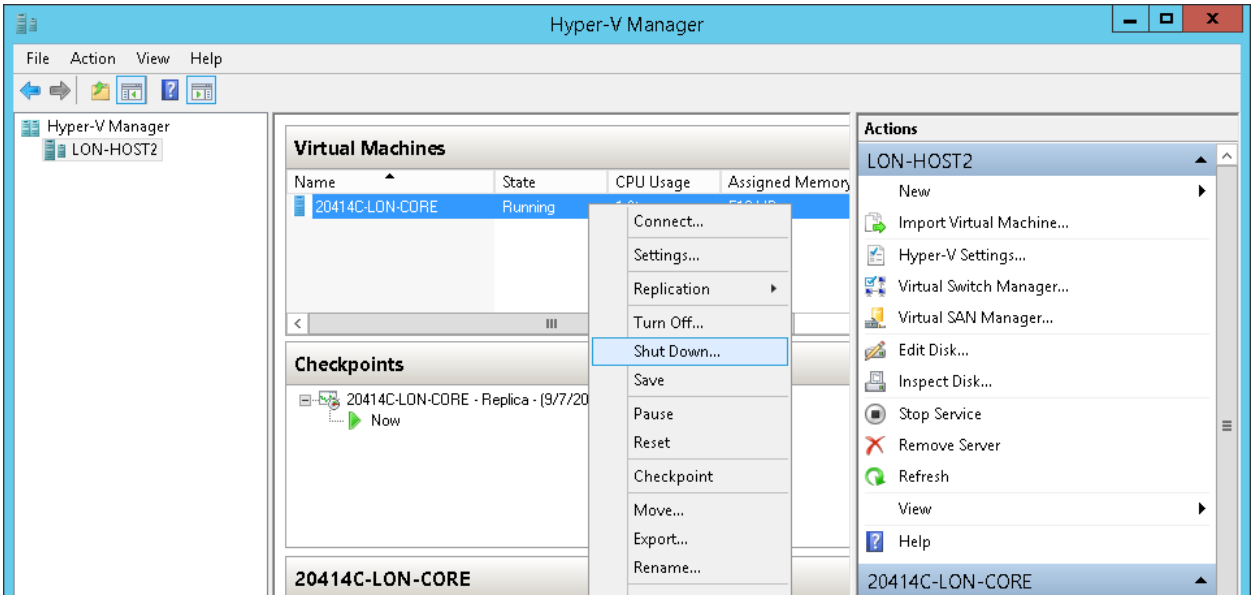

6. Qua máy **LON-HOST1**, chuột phải **20414C-LON-CORE**, chọn **Replication**, và chọn **Remove Replication**.



7. Hộp thoại **Remove Replication**, chọn **Remove Replication**.




8. Qua máy **LON-HOST2**, chuột phải **20414C-LON-CORE**, chọn **Shut Down**. Hộp thoại **Shut Down Machine**, chọn **Shut Down**.

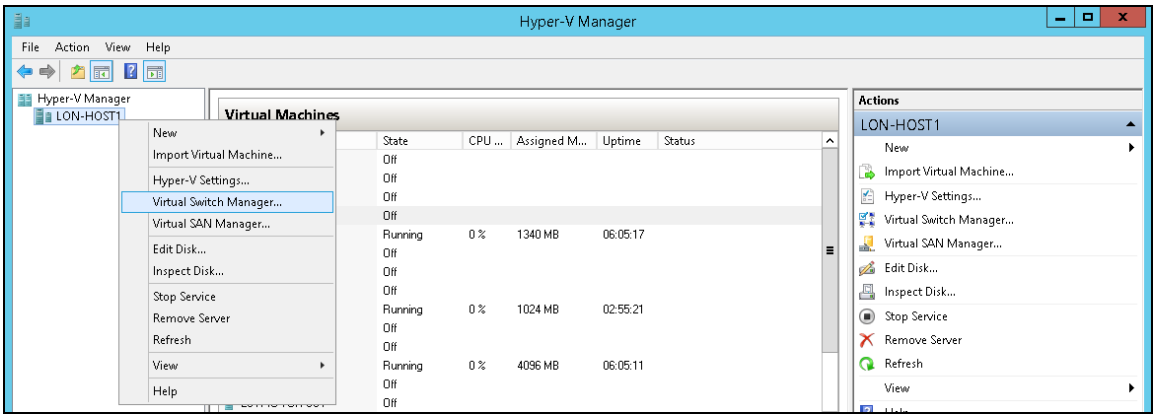



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công chức năng Hyper-V Replica.**

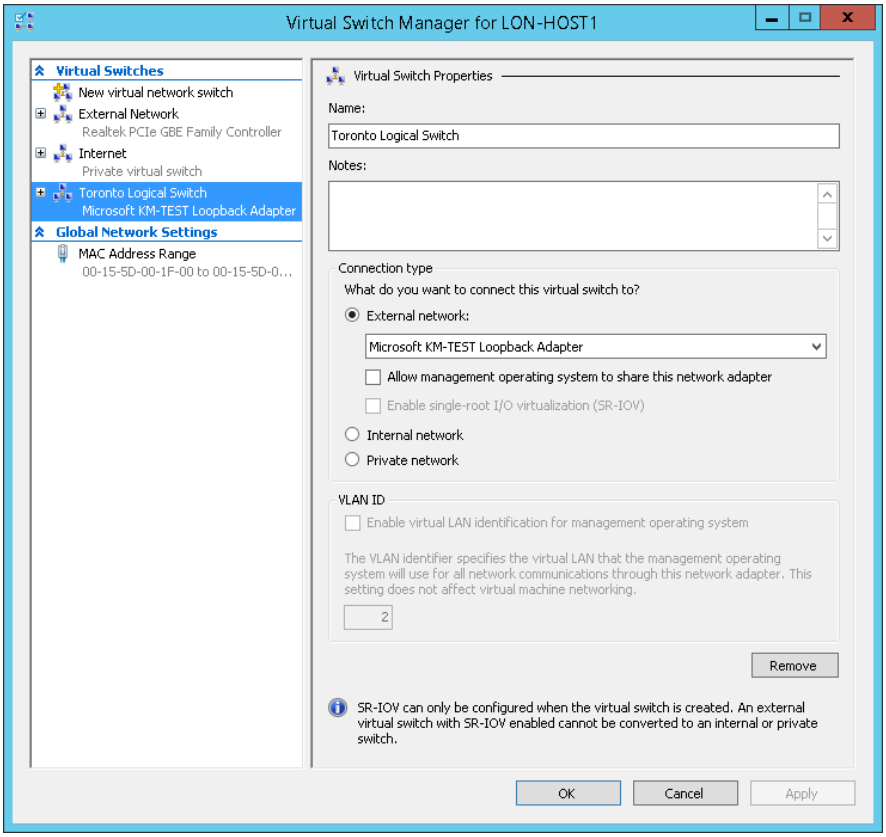
## VI. Chuẩn bị cho bài tiếp theo:

1. Không phục hồi các máy ảo, vì bạn sẽ sử dụng các máy ảo này trong các bài tiếp theo.

2. Trên máy **LON-HOST1**, mở **Hyper-V Manager**, chuột phải **LON-HOST1**, chọn **Virtual Switch Manager**.




3. Trong cửa sổ **Virtual Switch Manager,** chọn **Toronto Logical Network,** và chọn **Remove**, chọn **OK**. Hộp thoại thông báo, chọn **Yes**.



# Bài 4: Xây dựng giải pháp quản lý hệ thống ảo hóa bằng System Center 2012 R2

**I. Mục tiêu:**

- Cấu hình tự động hóa trong System Center Orchestrator.
- Ủy quyền quản lý VMM và Self-Service.
- Triển khai chức năng Host Updating trong VMM.

**II. Kịch bản:**

Công ty A. Datum đã triển khai một số Server ảo. Và bây giờ, họ cần phải sắp xếp công việc quản lý môi trường ảo này. Nhóm Development yêu cầu phải có thêm quyền truy cập môi trường ảo, và được kiểm soát nhiều hơn đối với việc triển khai và cấu hình các máy ảo. Hơn nữa, họ cũng muốn có thể quản lý môi trường ảo của họ.

Khi số lượng các máy vật lý và máy ảo phát triển, sẽ làm gia tăng công việc quản lý System Center 2012 của các quản trị viên tại A. Datum. Vì vậy, để giảm thời gian và công việc quản trị, họ muốn ủy quyền một số công việc và nhiệm vụ phổ biến cho các nhóm Development.

**III. Yêu cầu tổng quan:**

Lập kế hoạch quản lý hệ thống ảo hóa để hỗ trợ các mục tiêu sau đây:

- Cấp quyền cho nhóm Development Administrators kiểm soát các Host Groups của họ và các tài nguyên liên quan.
- Cho quyền nhóm Developments tạo ra các tài khoản Self-service để triển khai máy nhanh chóng.
- Cấp quyền cho nhóm Developments giám sát các server, bao gồm các tùy chọn để cài đặt cấu hình nâng cao.

**IV. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-VMM1**<br>**20414C-LON-OR1**<br>**20414C-LON-WSUS** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên từ bước 1 đến 3 cho các máy ảo còn lại.

**VI. Thực hành:**

*Thời gian thực hành: 60 phút*

## Bài tập 1: Cấu hình tự động hóa trong System Center Orchestrator.

A. Datum đã cài đặt System Center Orchestrator và họ muốn bạn cấu hình nó để tạo ra một quy trình triển khai máy ảo tự động.

❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt và cấu hình System Center Integration Packs cho VMM

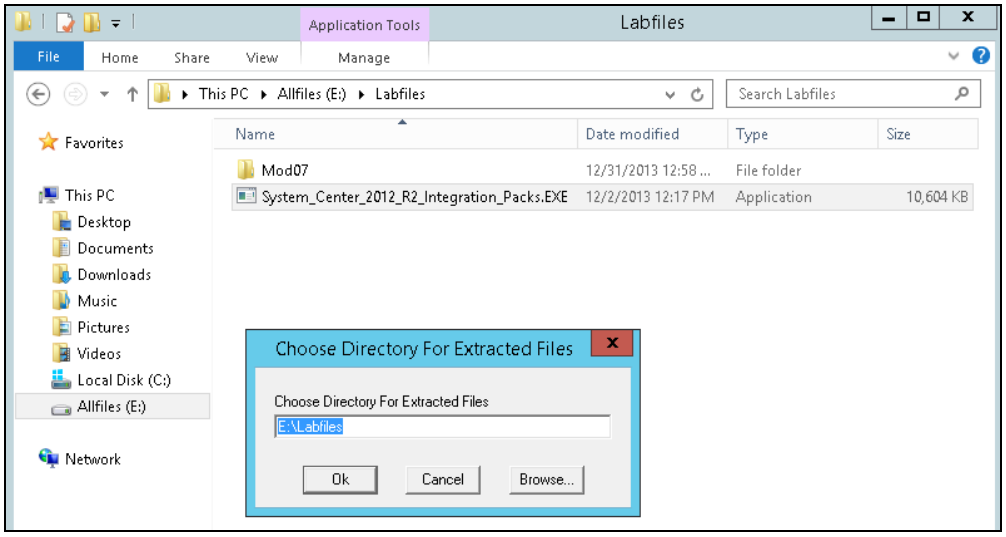
2. Cấu hình tự động hóa trong Orchestrator

❖ **Thực hành:**

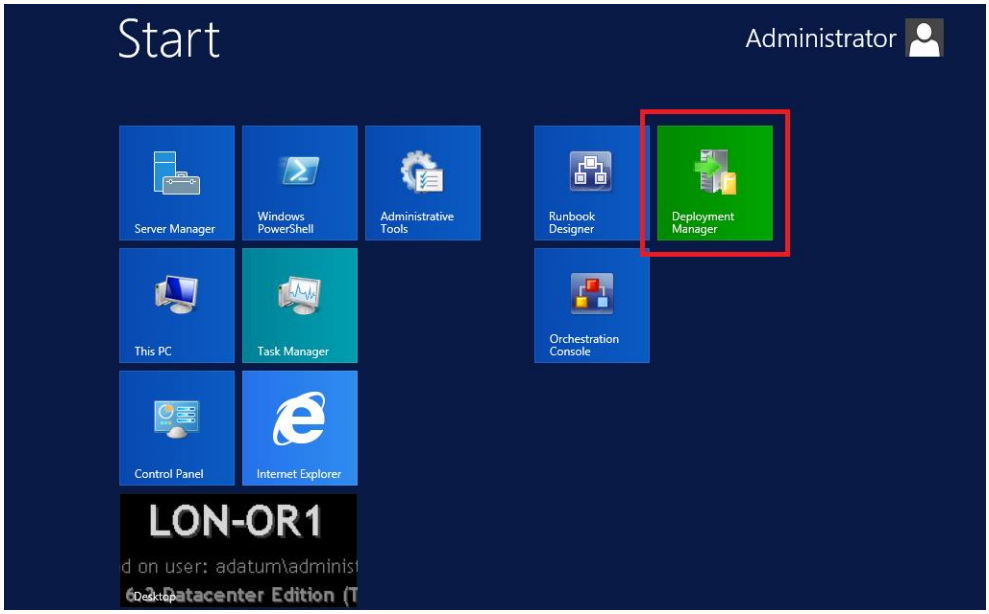
## Bước 1: Cài đặt và cấu hình System Center Integration Packs cho VMM

➢ **Cài đặt System Center Integration Pack cho VMM**

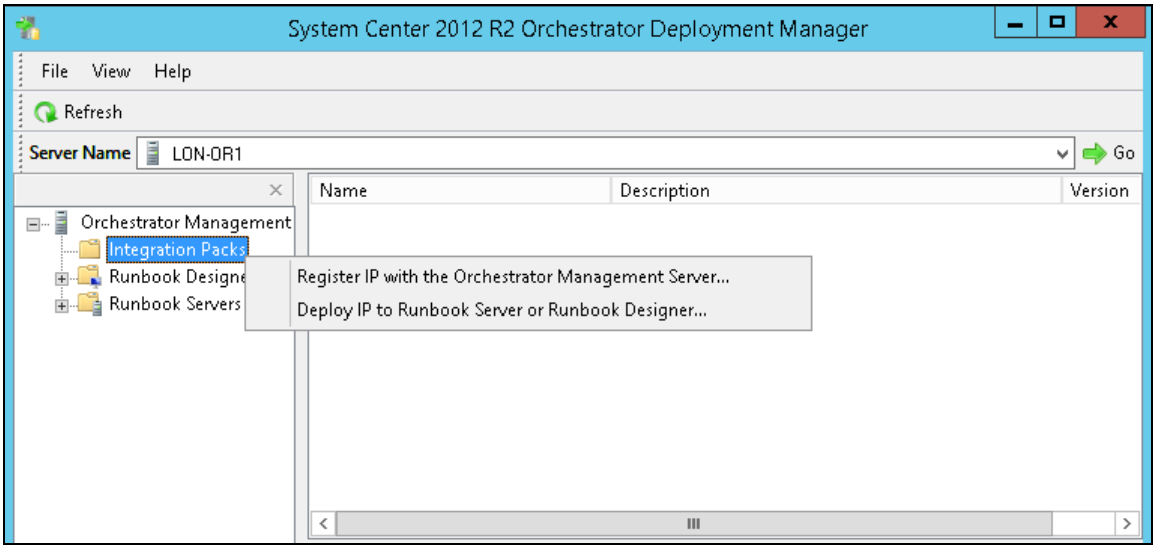
1. Trên máy **LON-DC1**, mở **File Explorer**, vào **E:\Labfiles**, chạy file **System_Center_2012_R2_Integration_Packs.EXE**. Chọn **OK** 2 lần và tắt **File Explorer**.




2. Qua máy **LON-OR1**, bung **Start** menu, mở công cụ **Deployment Manager**.

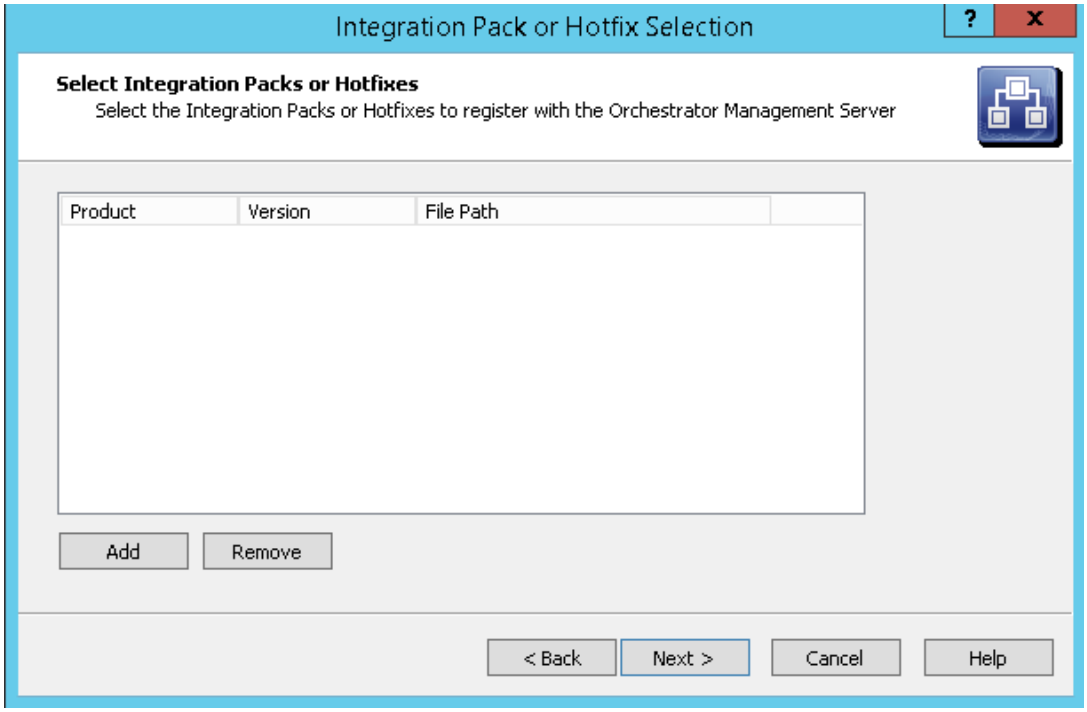


3. Trong cửa sổ **Deployment Manager**, chuột phải **Integration Packs**, chọn **Register IP with the Orchestrator Management Server**.

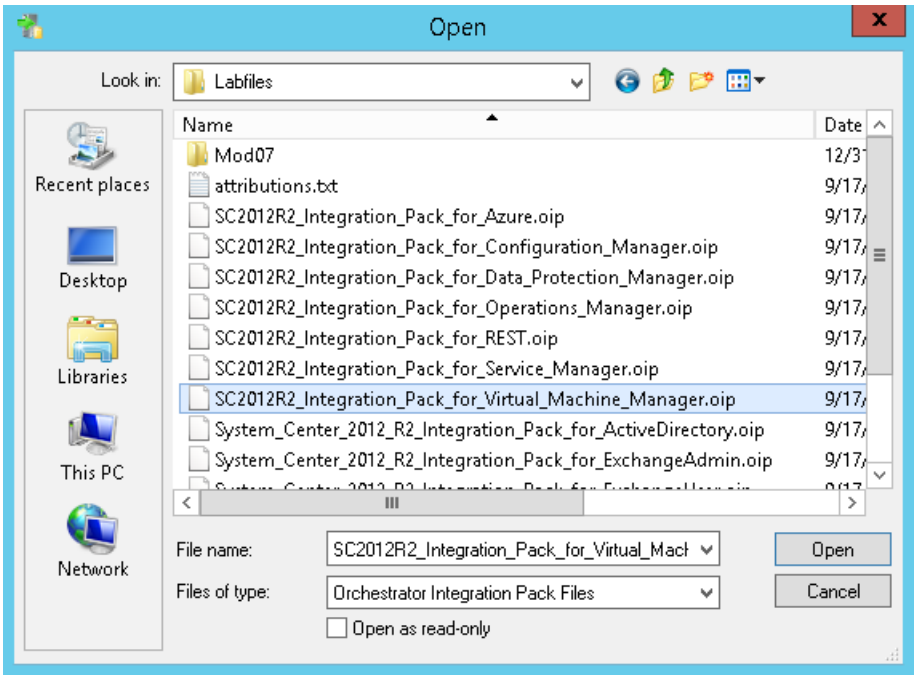



4. Cửa sổ **Welcome to the Integration Pack Registration Wizard**, chọn **Next**.

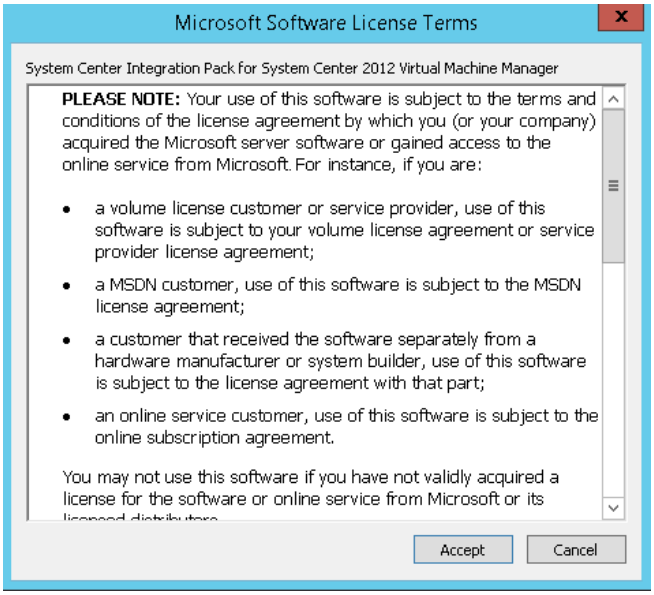
5. Cửa sổ **Select Integration Packs or Hotfixes**, chọn **Add**.



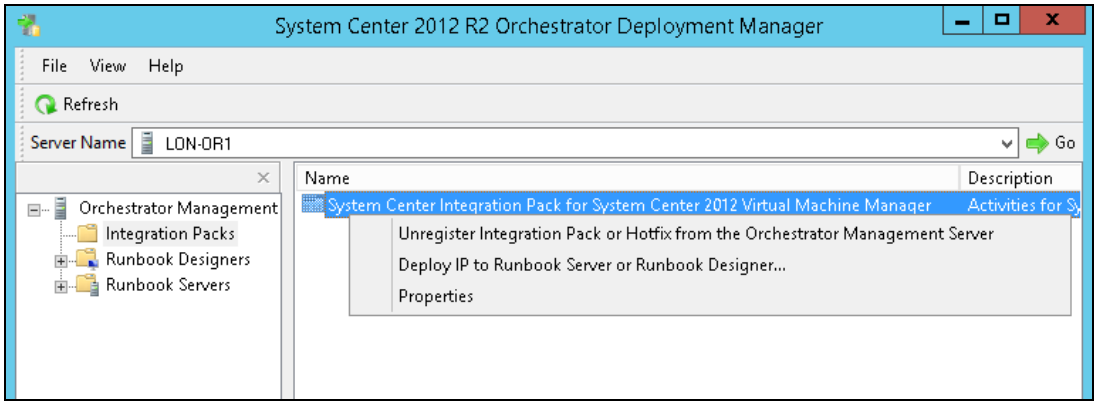
6. Cửa sổ **Open**, trong ô **File name**, nhập **\\lon-dc1\e$\Labfiles\SC2012R2_Integration_Pack_for_Virtual_Machine_Manager.oip**. Chọn **Open**, chọn **Next**, và chọn **Finish**




7. Hộp thoại **Microsoft Software License Terms**, chọn **Accept**.

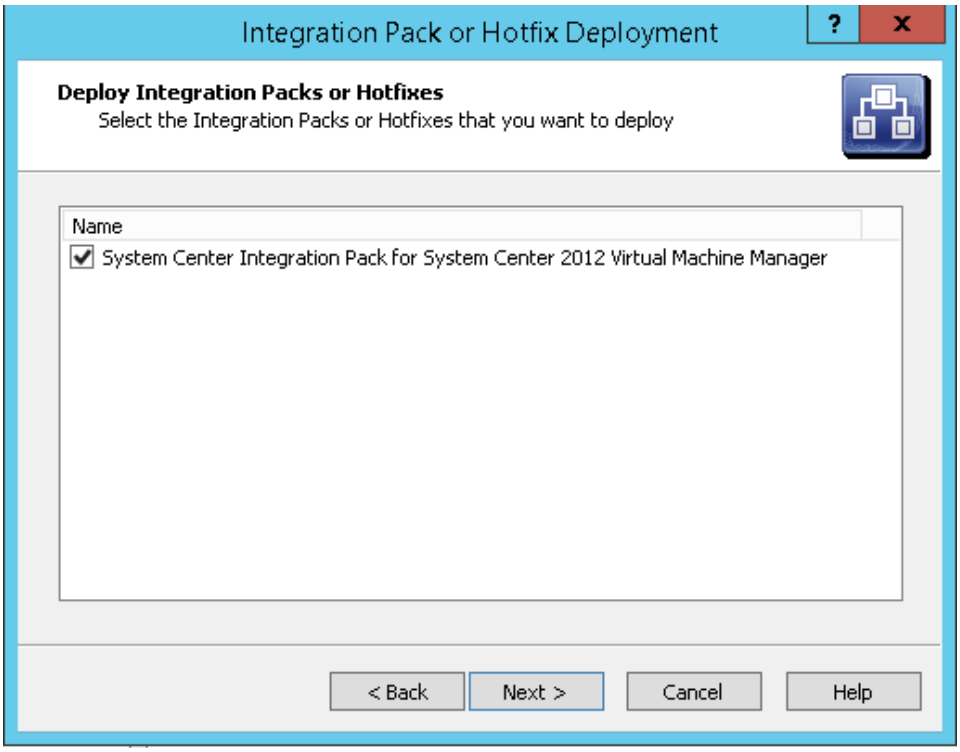


8. Đợi sau khi đăng ký thành công, bung **Orchestration Management Server**, chọn **Integration Packs**, chuột phải **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, chọn **Deploy IP to Runbook Server or Runbook Designer**.

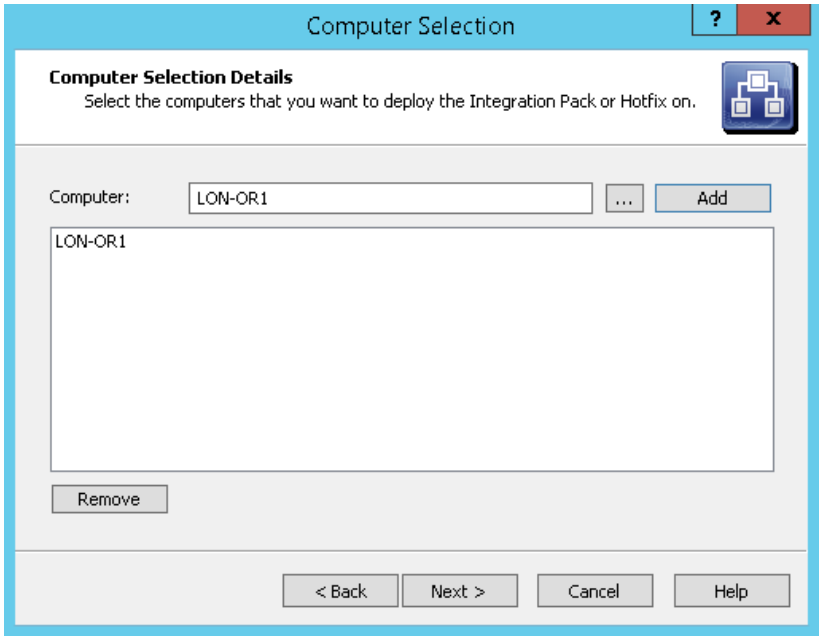



9. Cửa sổ **Welcome to the Integration Pack Deployment Wizard**, chọn **Next**.

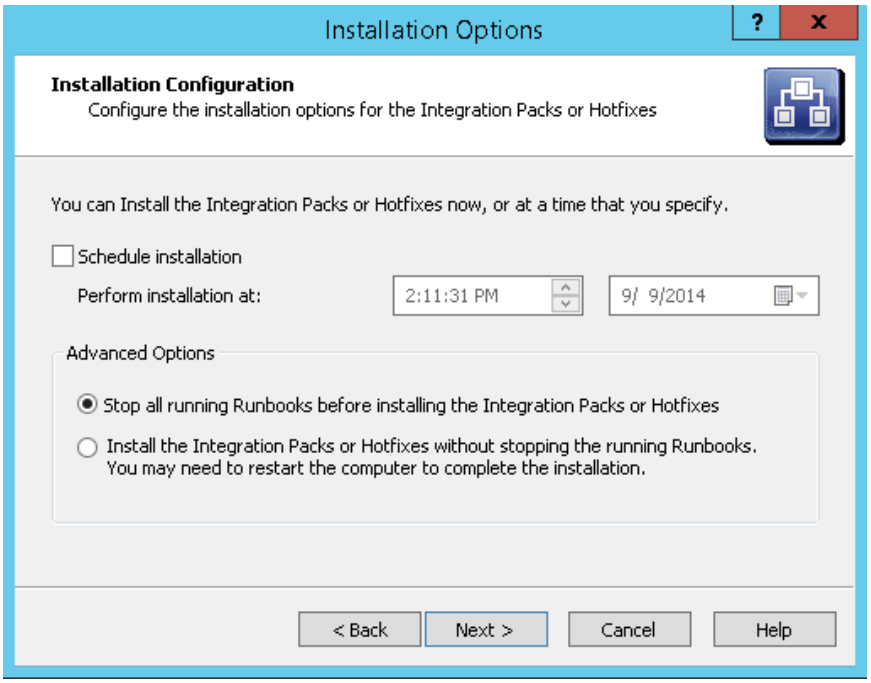
10. Cửa sổ **Deploy Integration Packs or Hotfixes**, đánh dấu chọn **System Center Integration Pack for System Center 2012 Virtual Machine Manager**, và chọn **Next**.



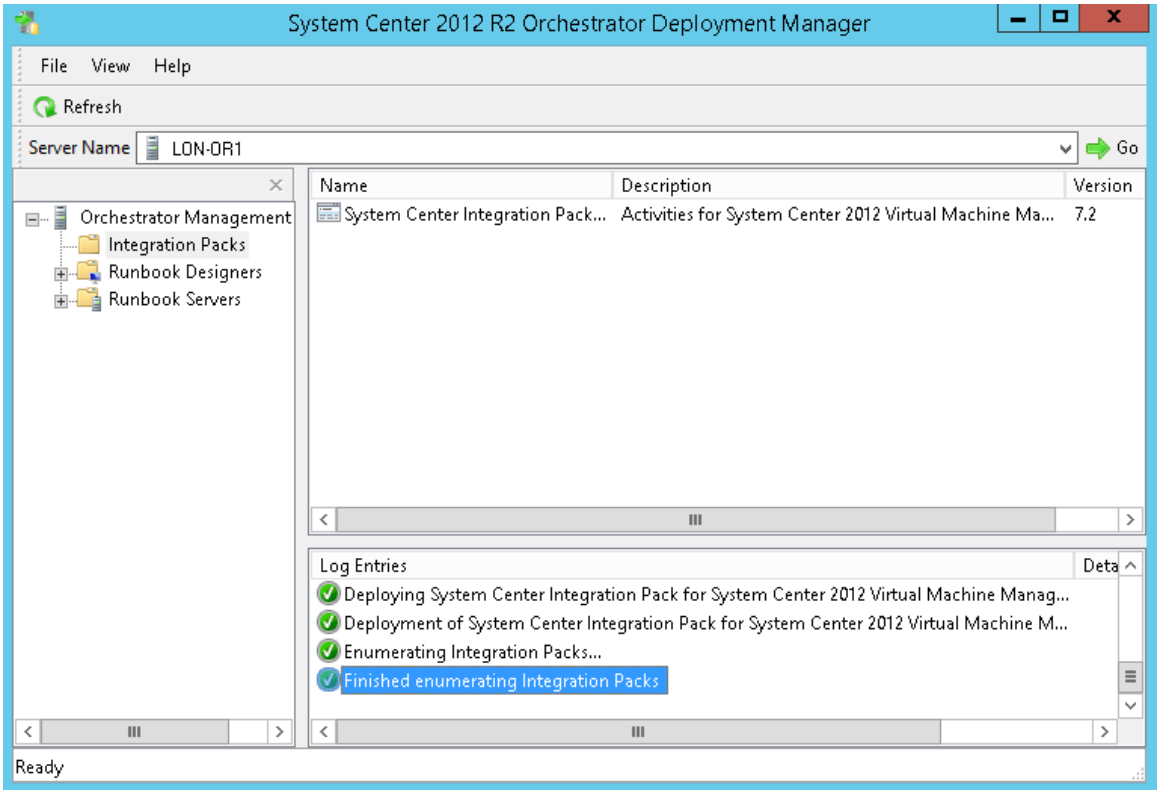
11. Cửa sổ **Computer Selection**, trong ô **Computer**, nhập **LON-OR1**, chọn **Add**, và chọn **Next**.




12. Cửa sổ **Installation Options**, chọn **Next**, và chọn **Finish**



13. Kiểm tra thông báo trong phần **Log Entries**, và tắt cửa sổ **Orchestrator Deployment Manager.**

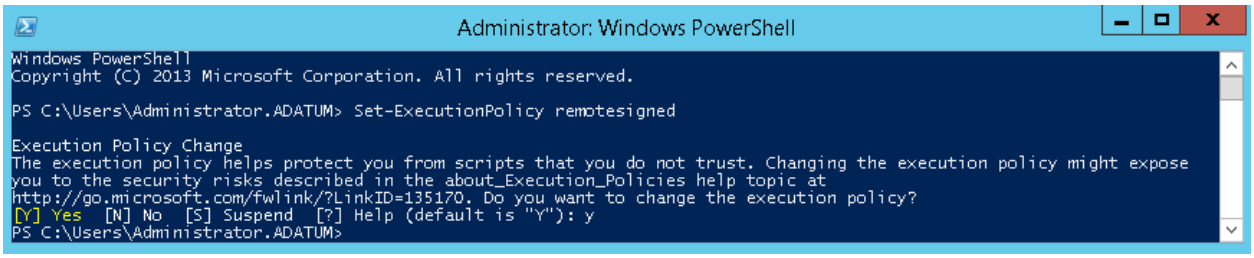



➢ **Thiết lập Execution Policy để RemoteSigned**

1. Qua máy **LON-OR1**, trên thanh task bar, chuột phải **Windows PowerShell**, chọn **Run as Administrator**.

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

**set-executionpolicy remotesigned** , nhấn Enter, gõ **Y**, nhấn Enter.

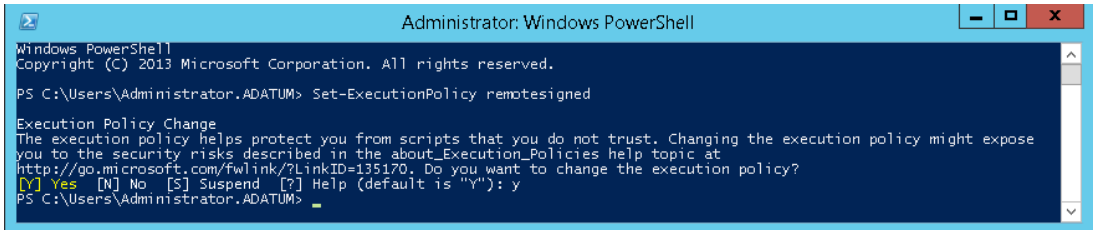


3. Tắt **Windows PowerShell**.

4. Qua máy **LON-VMM1**, trên thanh task bar, chuột phải **Windows PowerShell**, chọn **Run as Administrator**.

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

**set-executionpolicy remotesigned**, nhấn Enter, gõ **Y**, nhấn Enter.

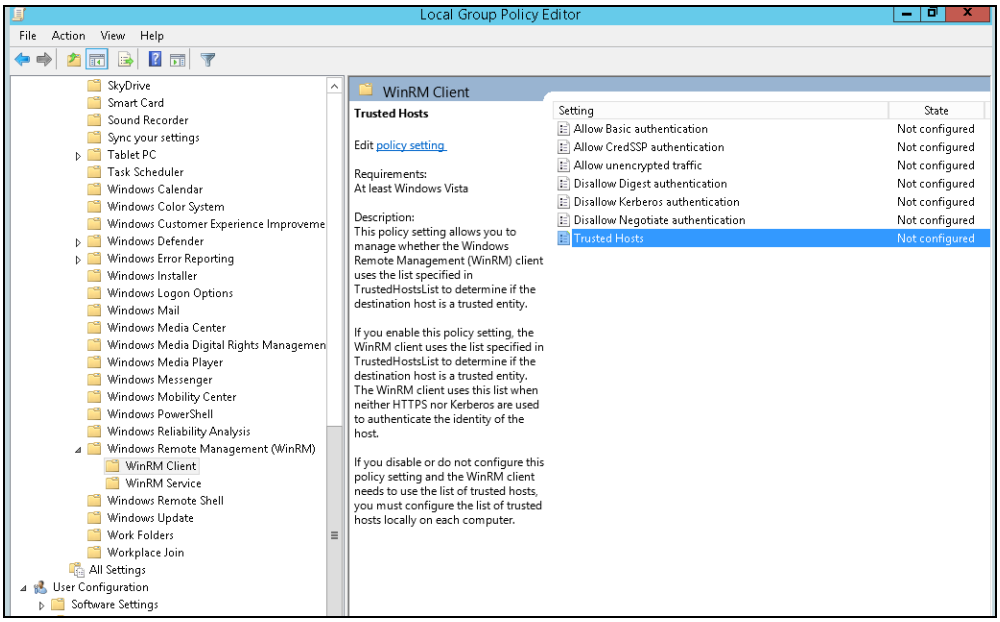



6. Tắt **Windows PowerShell**.

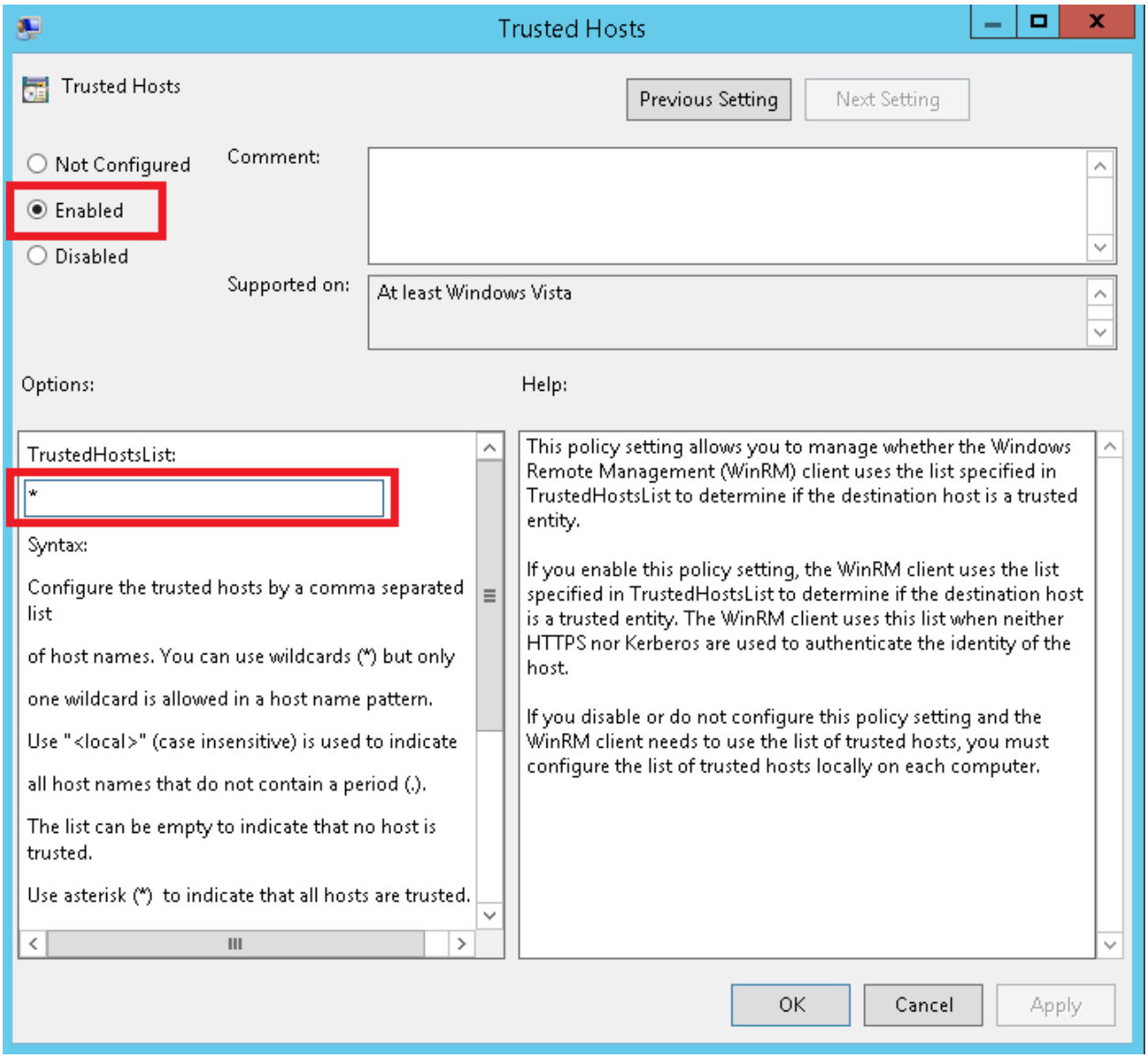
➢ **Bật chức năng Remote Management Trusted Hosts**

1. Qua máy **LON-OR1**, chuột phải **Start** menu, chọn **Run**, nhập **gpedit.msc**, chọn **OK**.

2. Trong cửa sổ Local Group Policy Editor, bung **Computer Configuration**, bung **Administrative Templates**, bung **Windows Components**, bung **Windows Remote Management (WinRM)**, chọn **WinRM Client**, mở policy **Trusted Hosts**.



3. Cửa sổ **Trusted Hosts**, chọn **Enabled**, trong ô **TrustedHostList**, nhập * **,** và chọn **OK**.

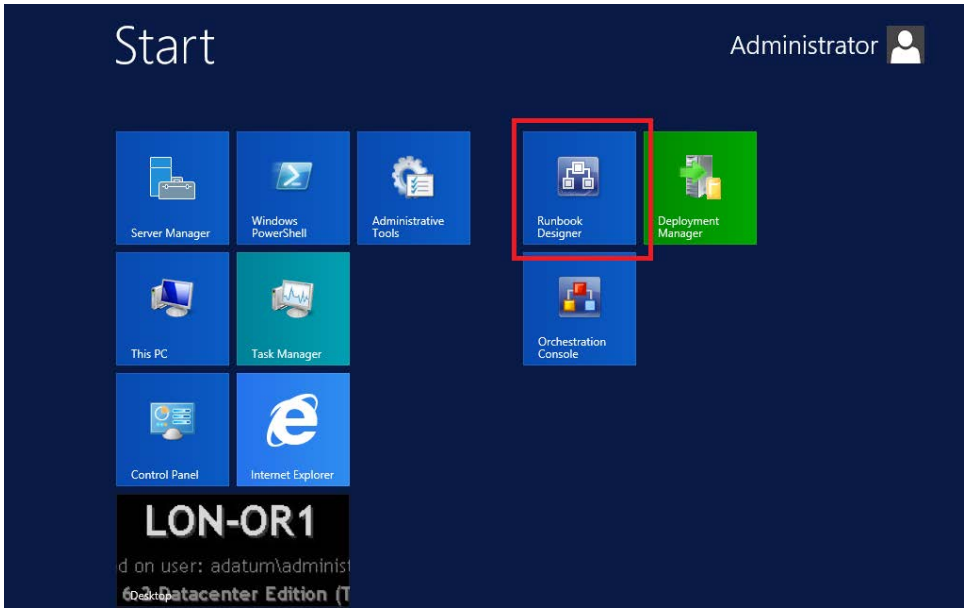



4. Tắt **Local Group Policy Editor**.

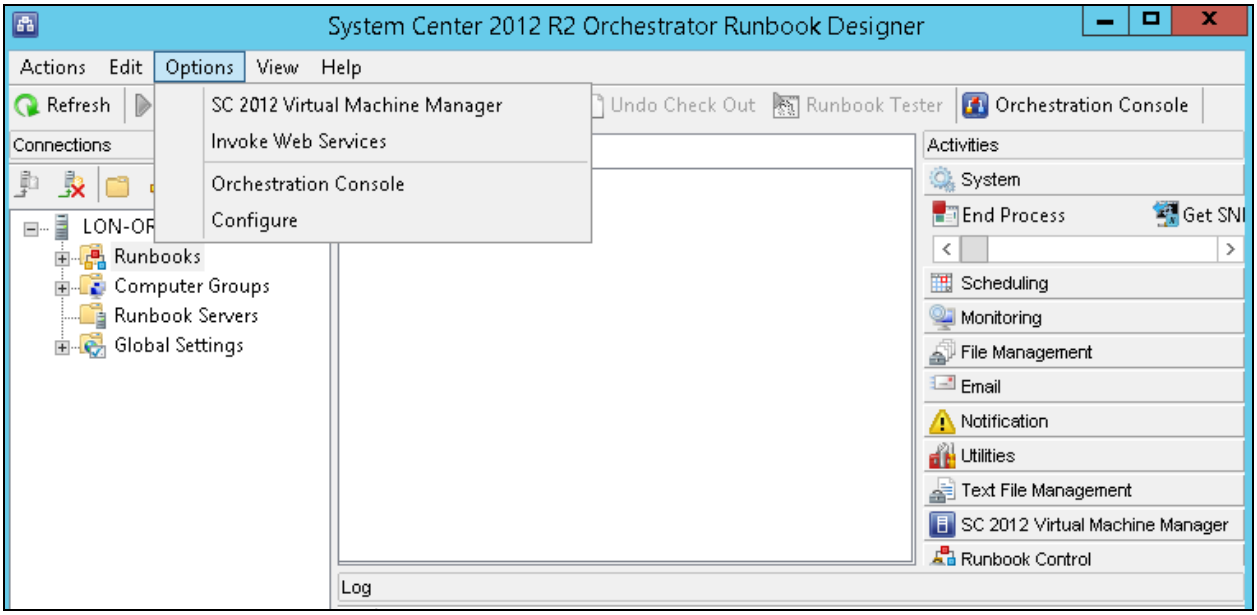
5. Qua máy **LON-VMM1**, Lặp lại từ bước **1** đến **4**.

➢ **Cấu hình System Center Integration Pack cho VMM**

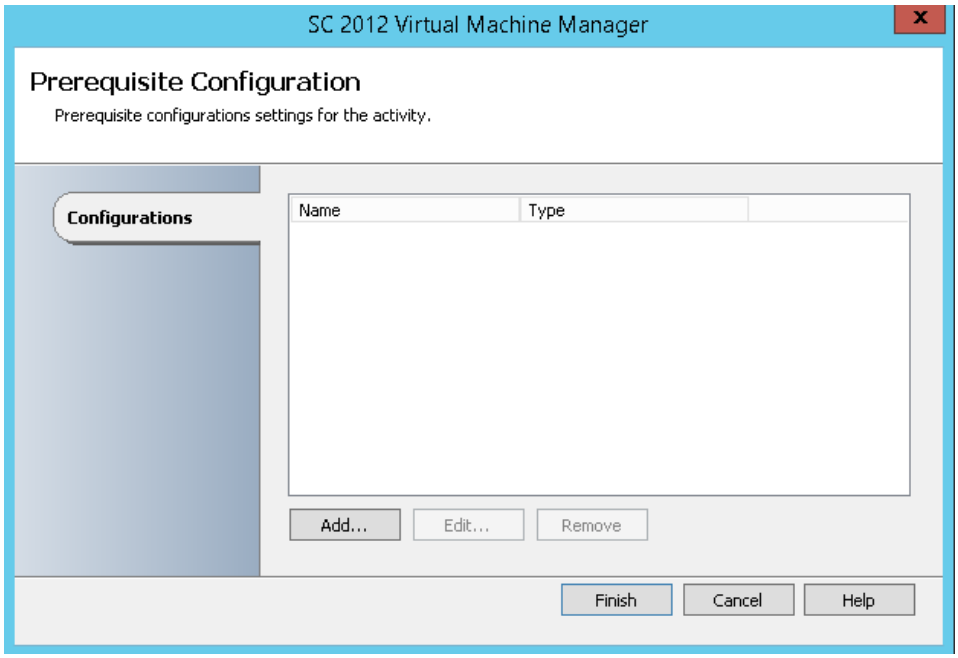
1. Qua máy **LON-OR1**, bung **Start menu**, mở công cụ **Runbook Designer**.



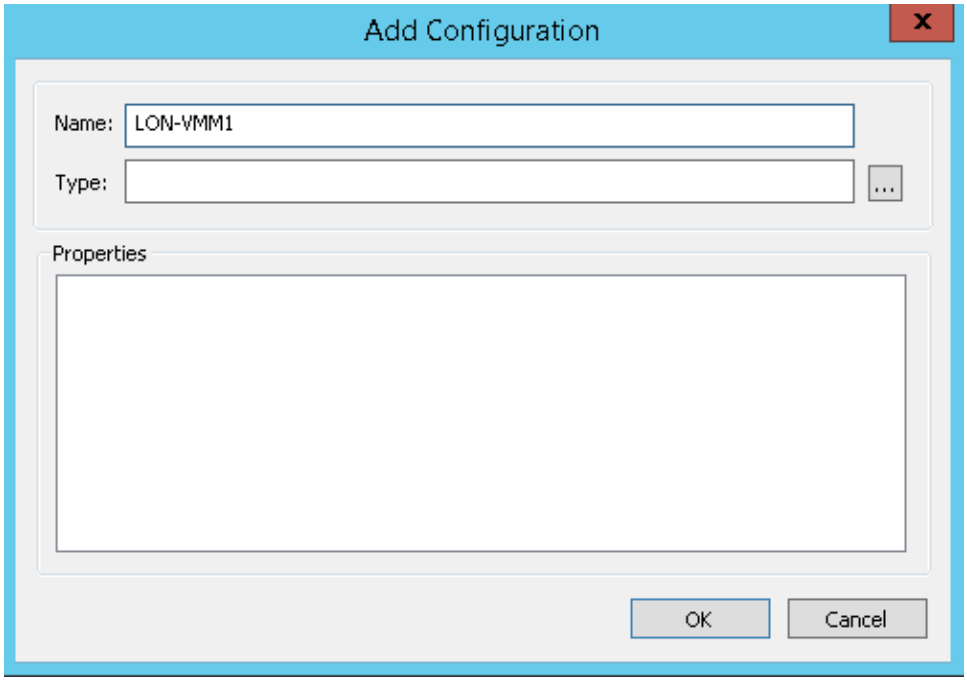

2. Tong cửa sổ **Runbook Designer**, bung menu **Options**, chọn **SC 2012 Virtual Machine Manager**.



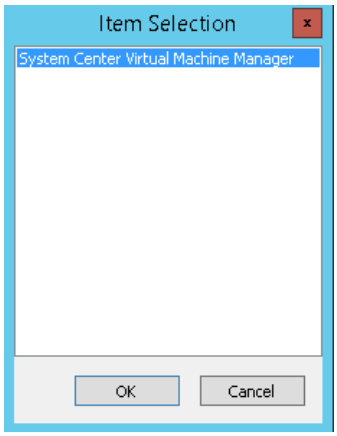
3. Cửa sổ **Configurations**, chọn **Add.**




4. Hộp thoại **Add Configuration**, trong ô **Name**, nhập **LON-VMM1**, chọn **(...)**.

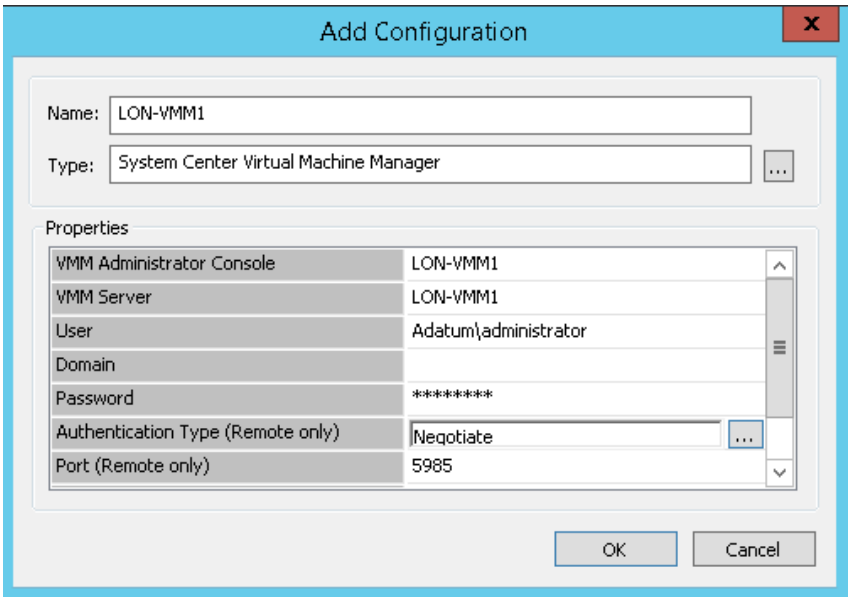


5. Hộp thoại **Item Selection**, chọn **System Center Virtual Machine Manager**, và chọn **OK**.

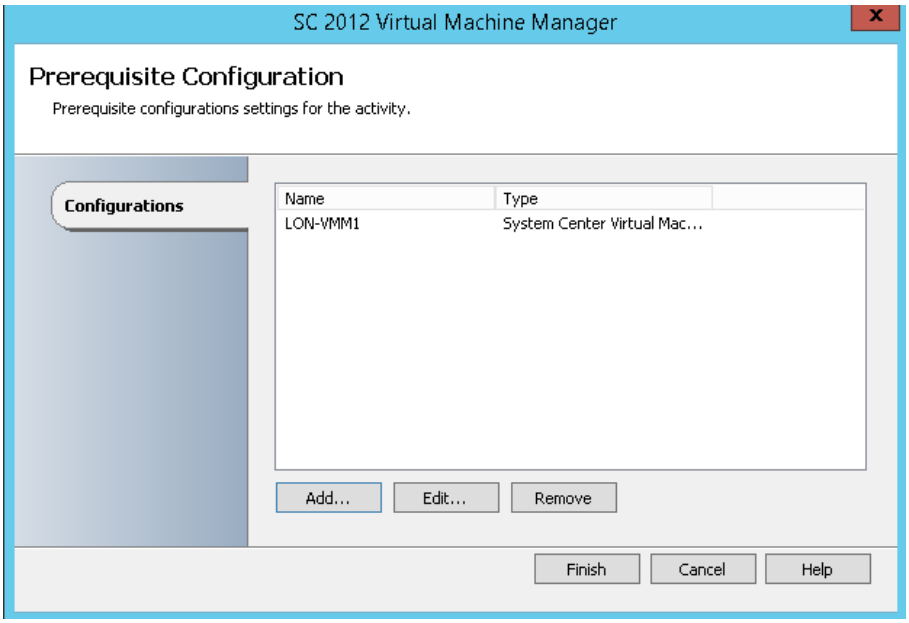



6. Hộp thoại **Add Configuration**, thiết lập thông tin như bên dưới, và chọn **OK**

- VMM Administrator Console: **LON-VMM1**
- VMM Server: **LON-VMM1**
- User: **Adatum\Administrator**
- Domain: **Bỏ trắng**
- Password: **Pa$$w0rd**.
- Authentication Type (Remote only): **Negotiate**



7. Cửa sổ **Prerequisite Configuration**, chọn **Finish**.

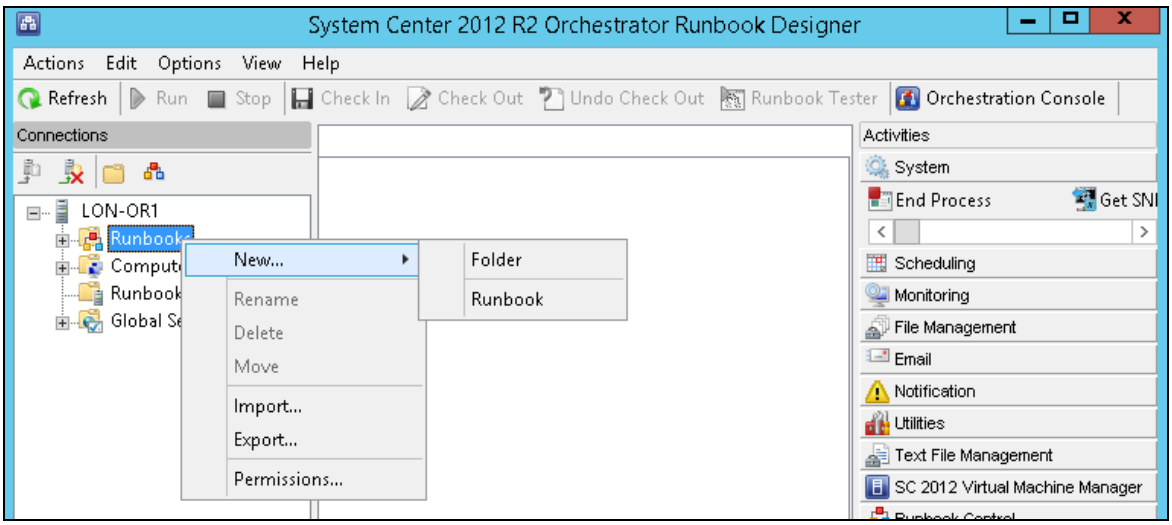



## Bước 2: Cấu hình tự động hóa trong Orchestrator

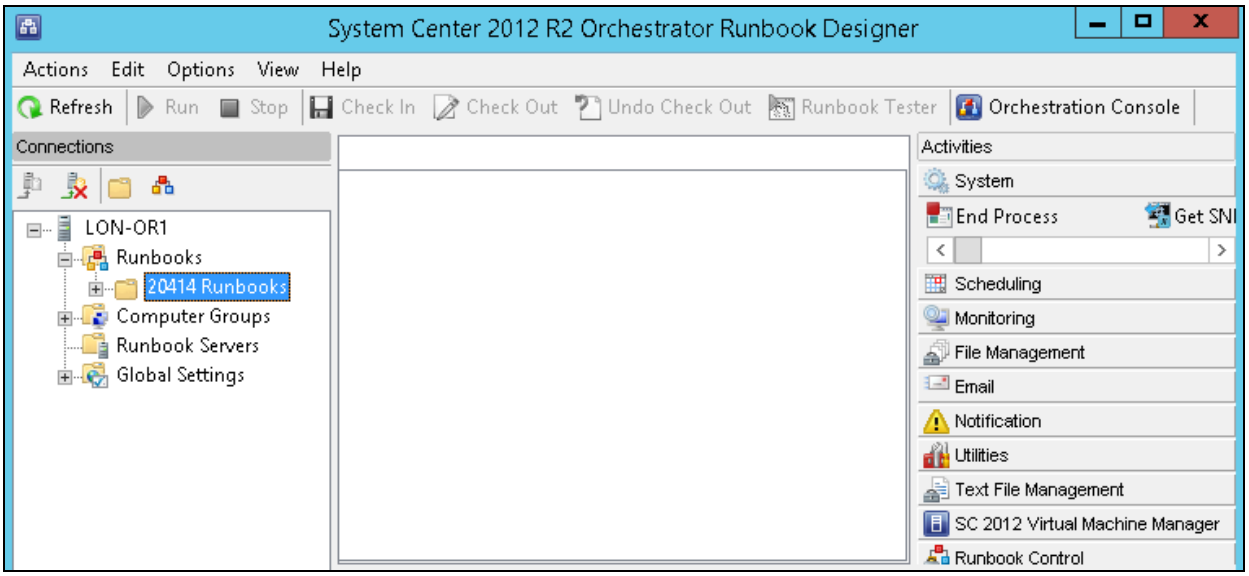
### ➢ Tạo Runbook cơ bản

1. Trên **LON-OR1**, bung **Start** menu, mở công cụ **Runbook Designer**.

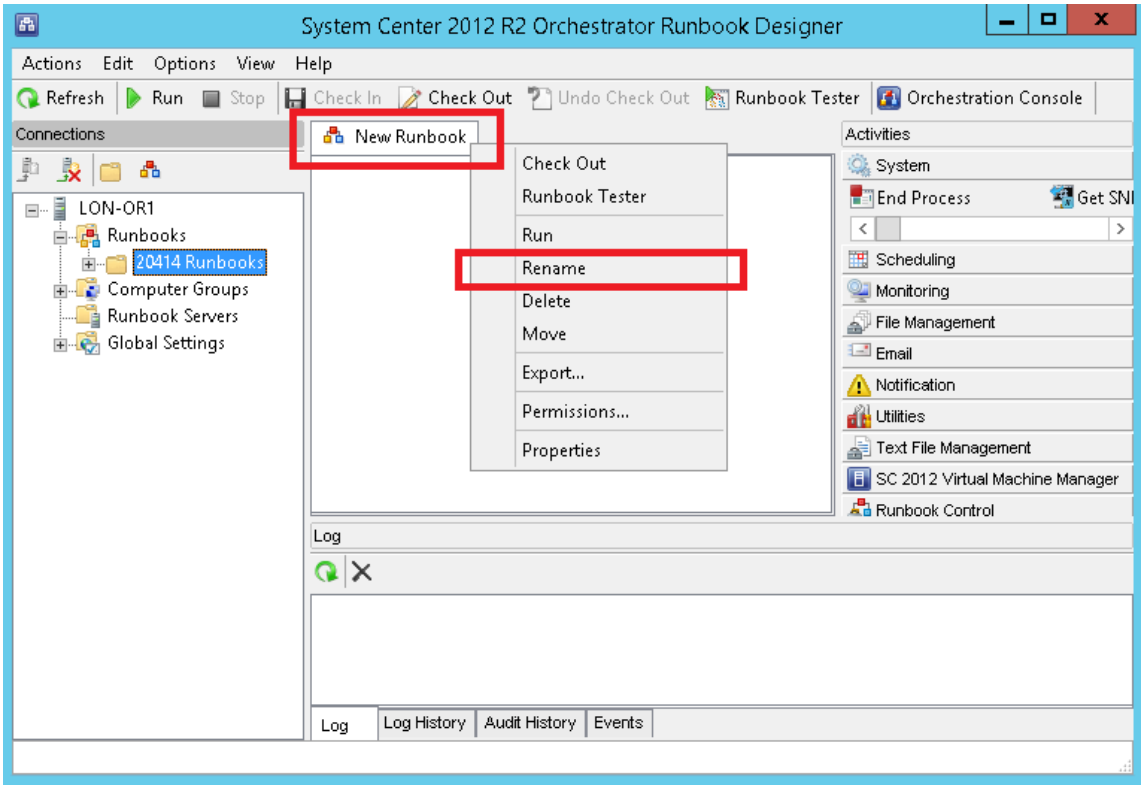
2. Trong cửa sổ **Runbook Designer**, chuột phải **Runbooks**, chọn **New**, chọn **Folder**, đặt tên cho folder mới là **20414 Runbooks**



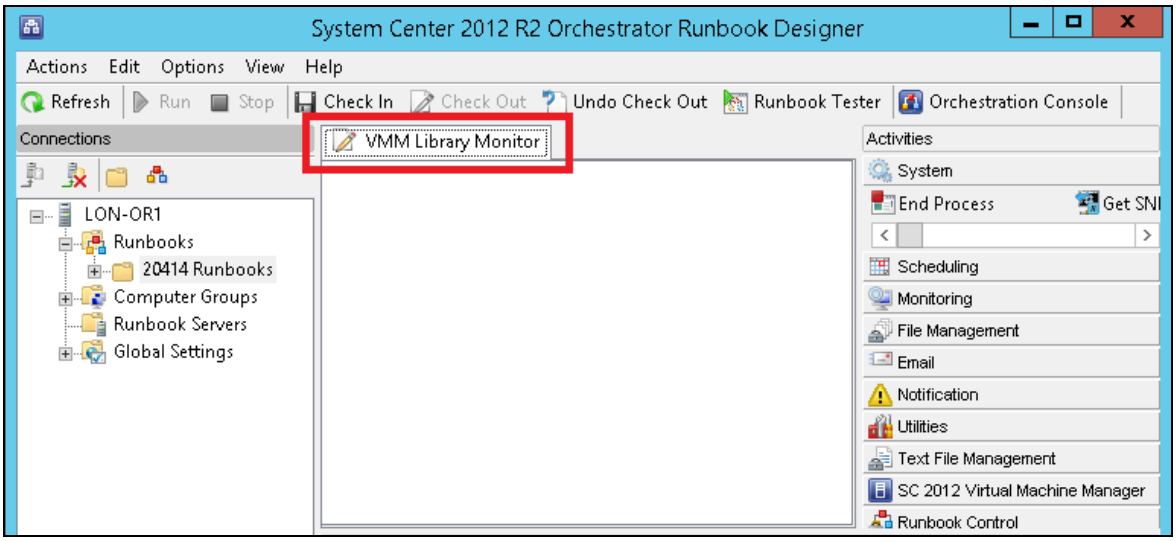
3.Chuột phải folder **20414 Runbooks**, chọn **New**, chọn **Runbook**



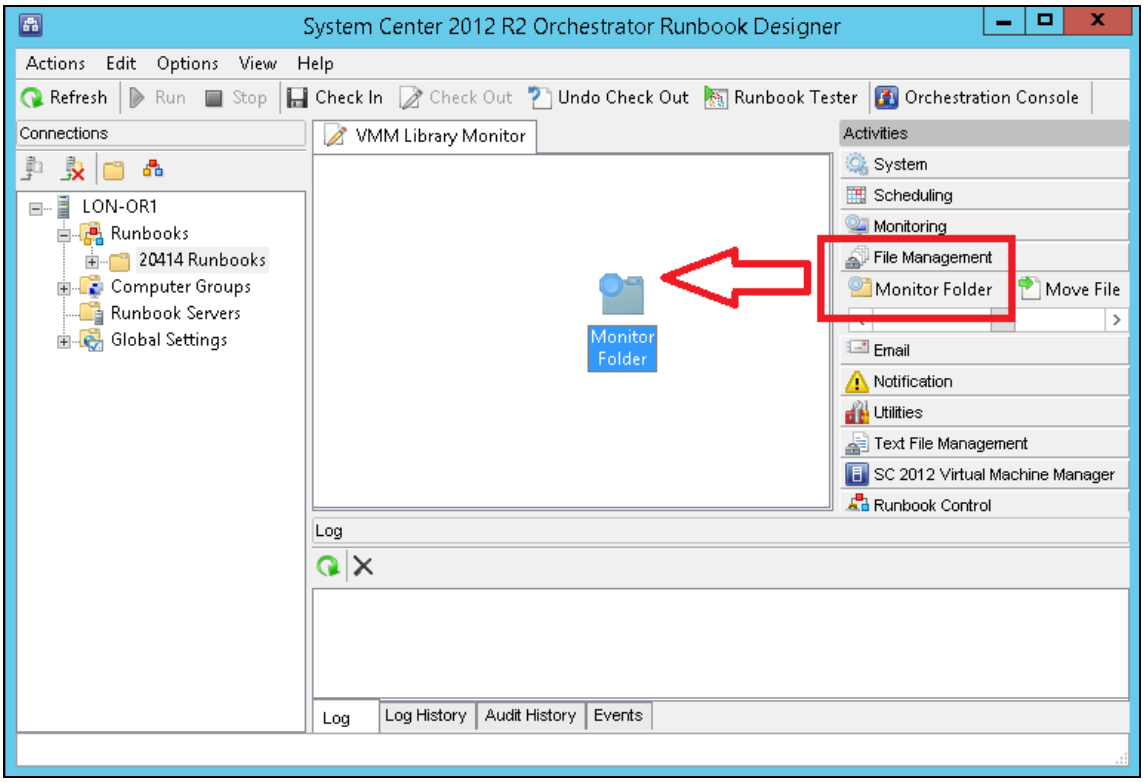

4. Chuột phải **New Runbook**, chọn **Rename**, chọn **Yes.**



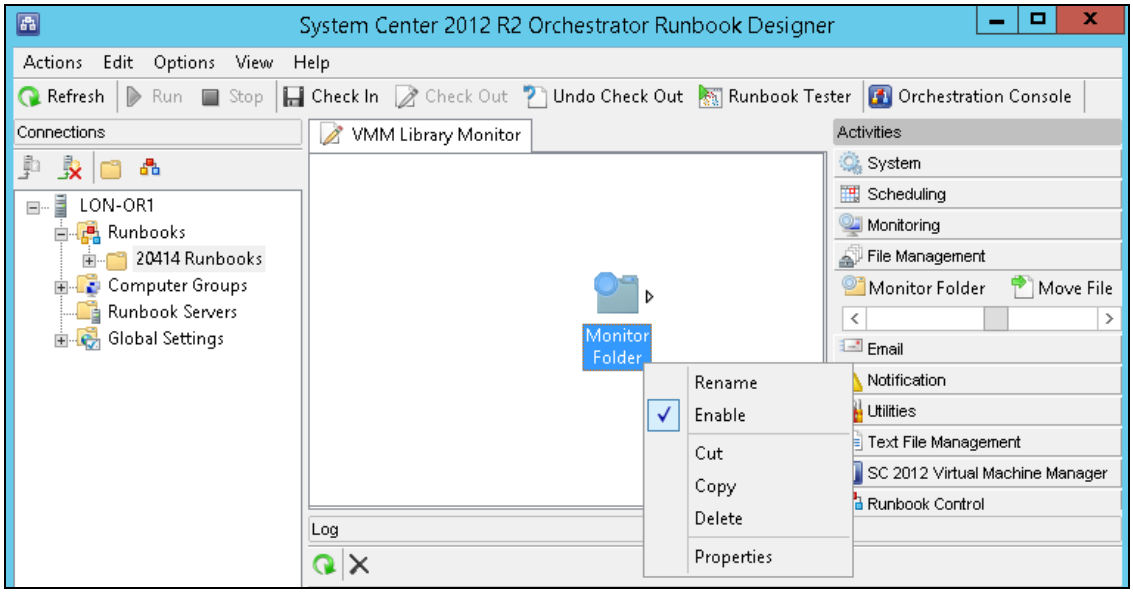
5. Đặt tên mới cho Runbook là **VMM Library Monitor**.



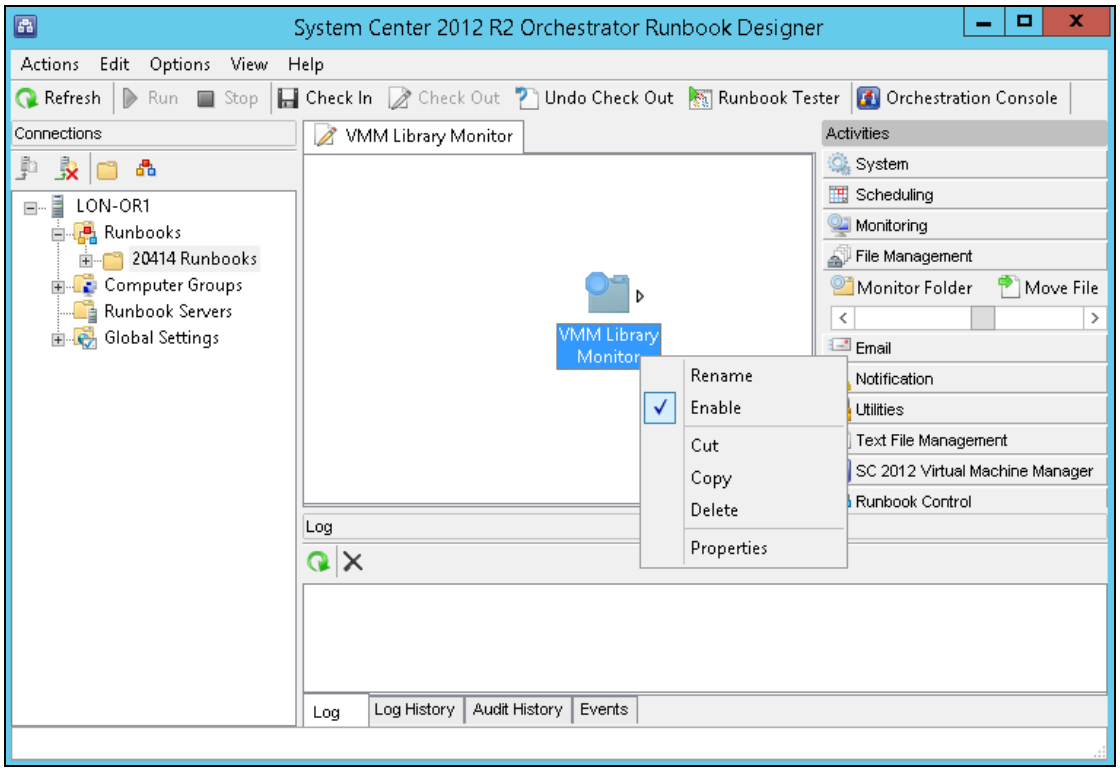

6. Trong phần **Activities**, bung **File Management**, chọn và kéo mục **Monitor Folder** và cửa sổ giữa.



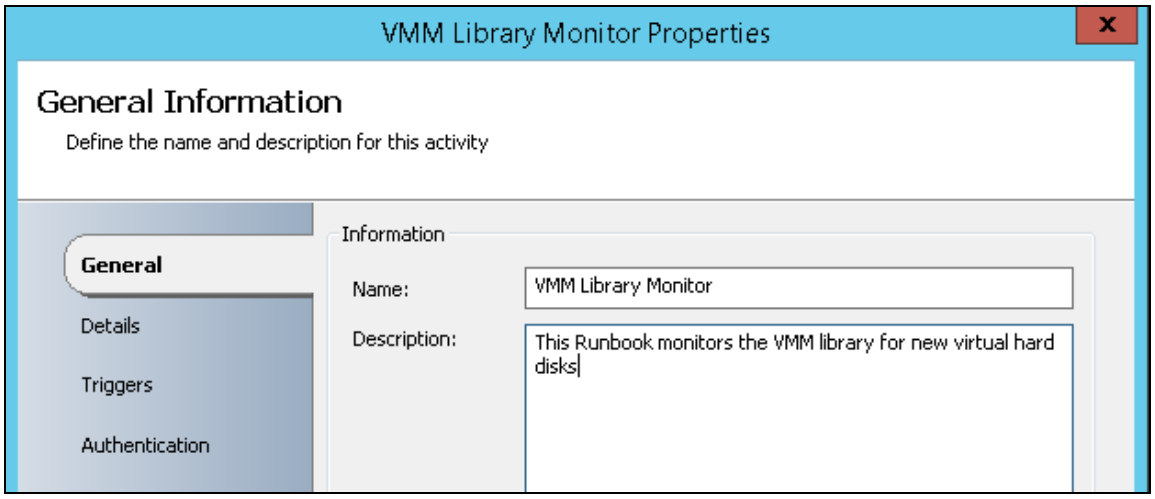
7. Chuột phải **Monitor Folder**, chọn **Rename**. Đặt tên mới là **VMM Library Monitor**.



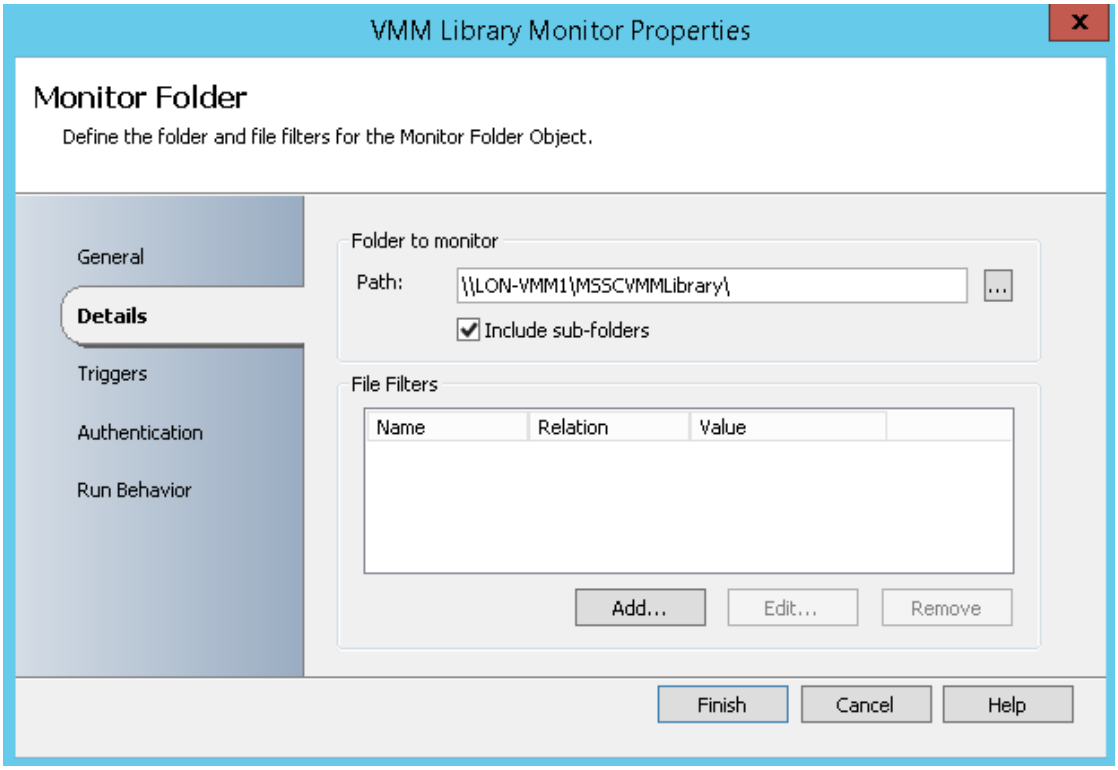

8. Chuột phải **VMM Library Monitor**, chọn **Properties.**



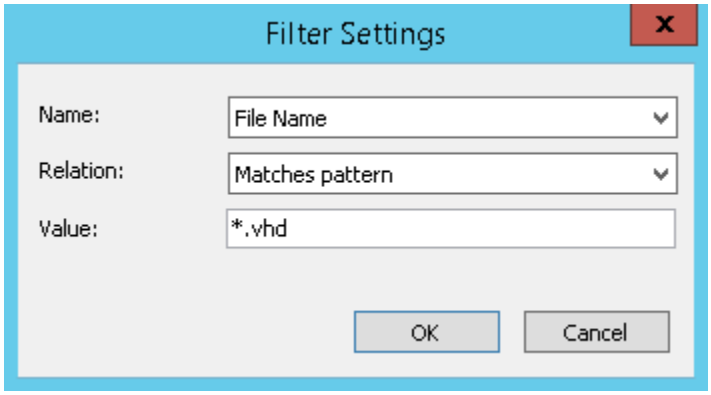
9. Cửa sổ **General Information**, trong ô **Description**, nhập **This Runbook monitors the VMM library for new virtual hard disks**.



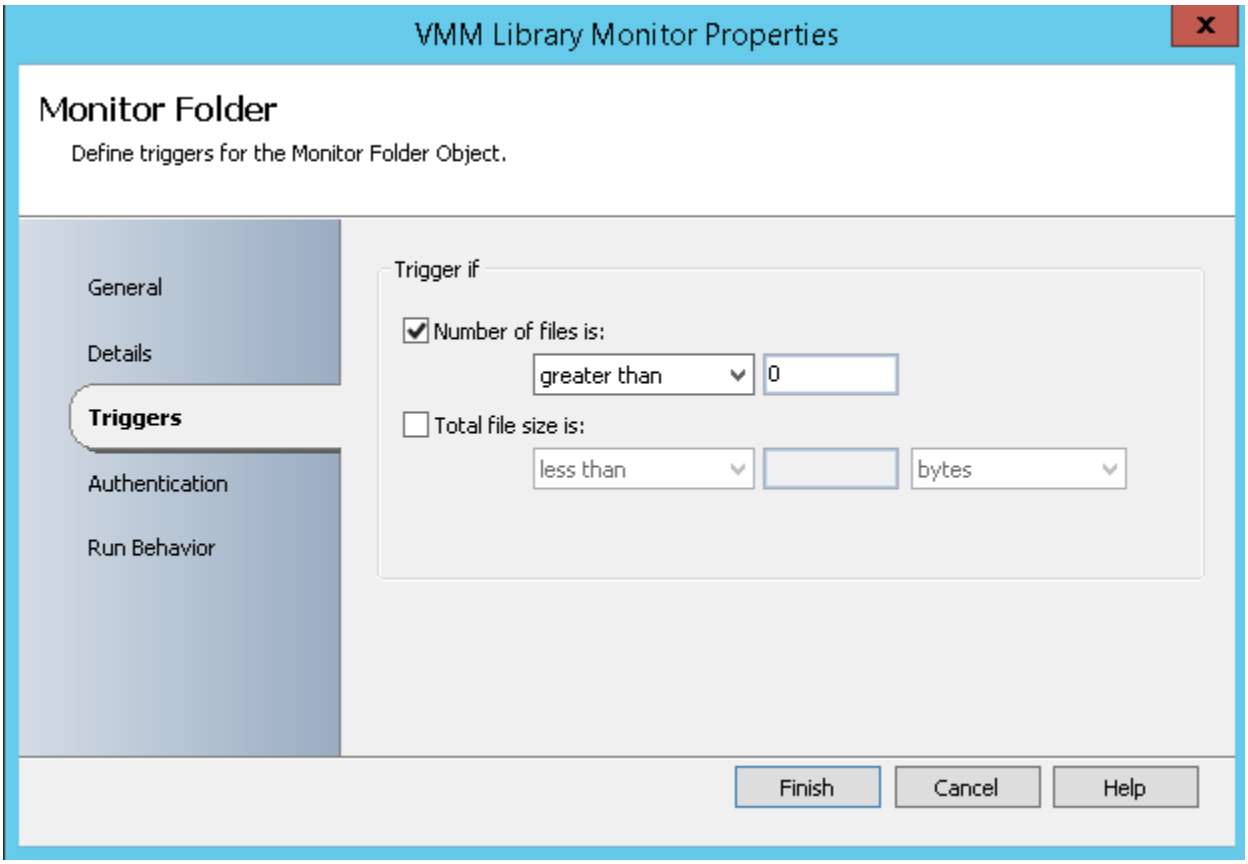

10. Chọn mục **Details**, trong ô **Path**, nhập **\\LON-VMM1\MSSCVMMLibrary**, đánh dấu chọn **Include sub-folders**, chọn **Add**.



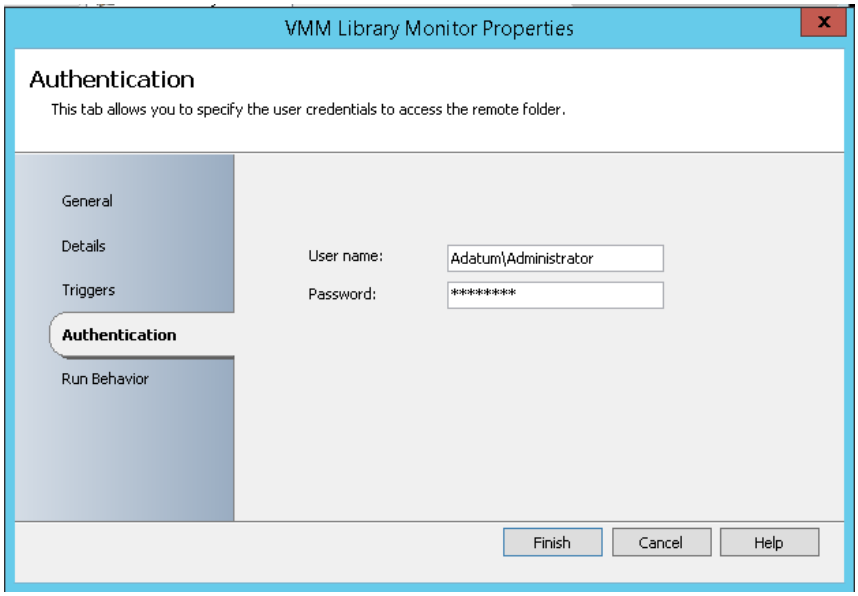
11. Hộp thoại **Filter Settings**, bung ô **Name**, chọn **File Name**, trong ô **Value**, nhập ***.vhd**, và chọn **OK**.



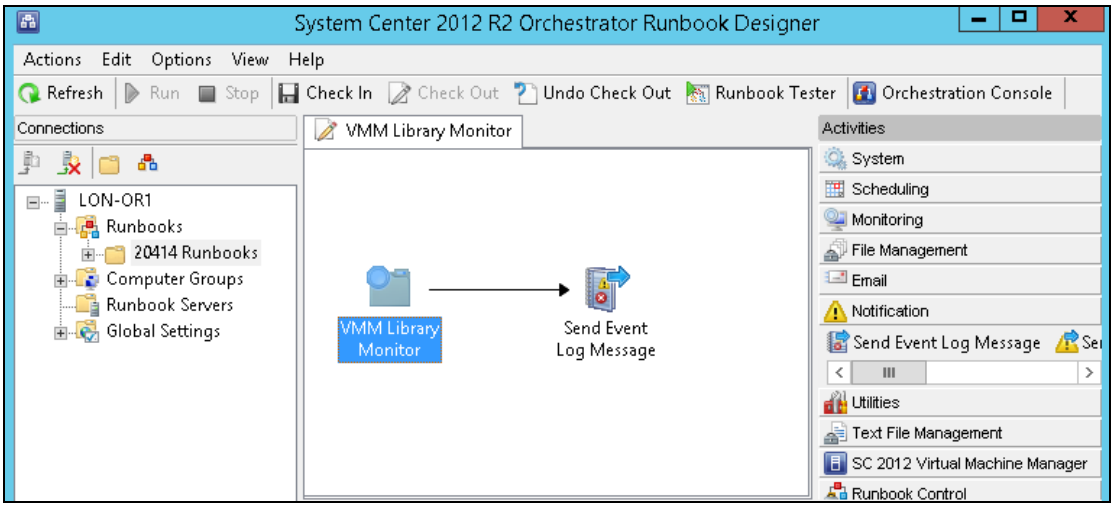

12. Cửa sổ **General Information,** chọn mục **Triggers**, đánh dấu chọn **Number of files is**, chọn **greater than**, và nhập **0**.



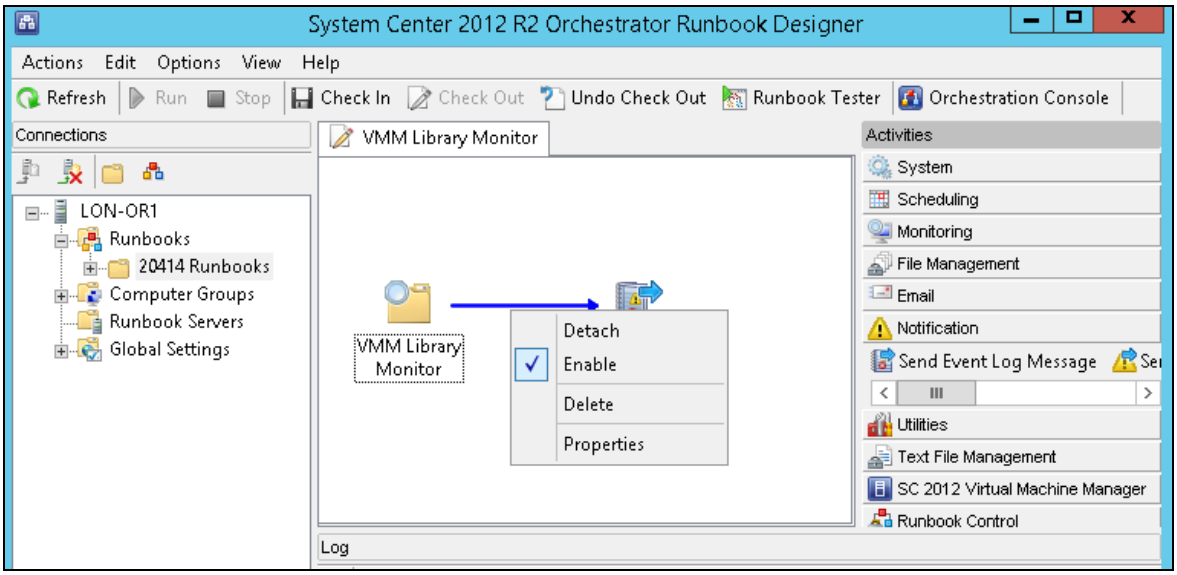
13. Chọn mục **Authentication**, trong ô **User name**, nhập **Adatum\Administrator**, trong ô **Password**, nhập **Pa$$w0rd**, và chọn **Finish**.



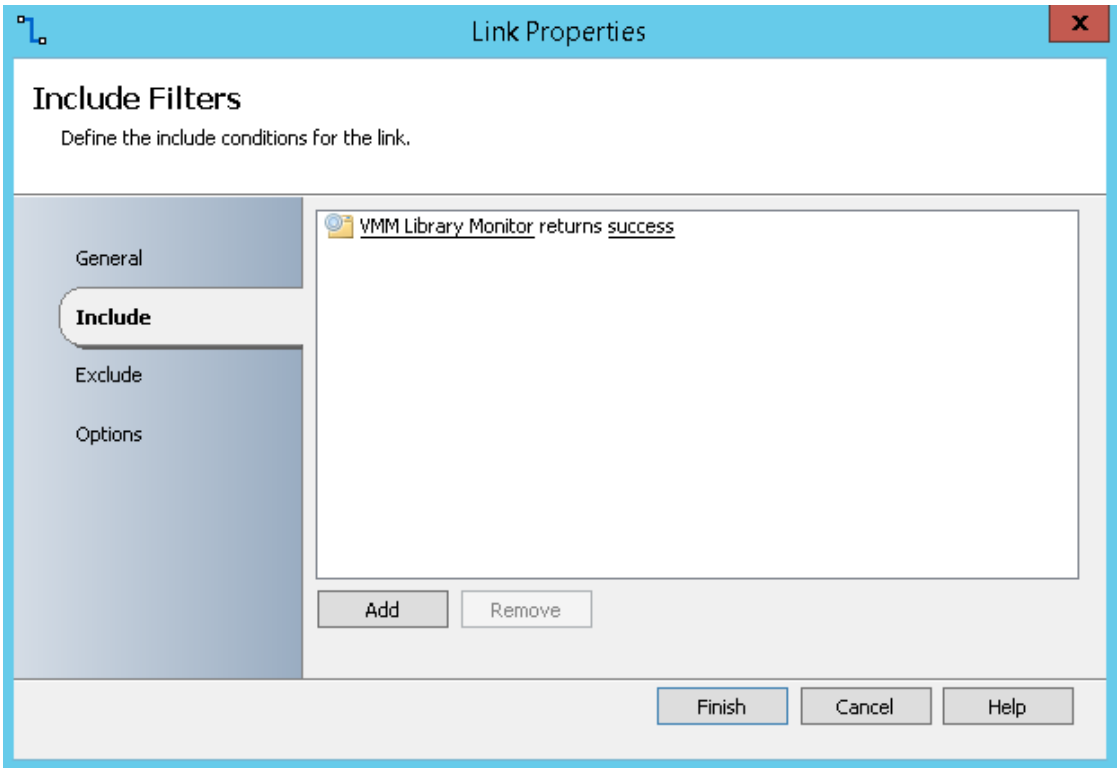

14. Trong phần **Activities**, chọn **Notification**, chọn và kéo mục **Send Event Log Message** và cửa sổ giữa và nằm bên phải của **VMM Library Monitor**. Đưa chuột vào biểu tượng **VMM Library Monitor** đến khi xuất hiên mũi tên nhỏ bên phải, chọn vào mũi tên và kéo vào mục **Send Event Log Message**. Một liên kết một mũi tên sẽ xuất hiện giữa hai biểu tượng.



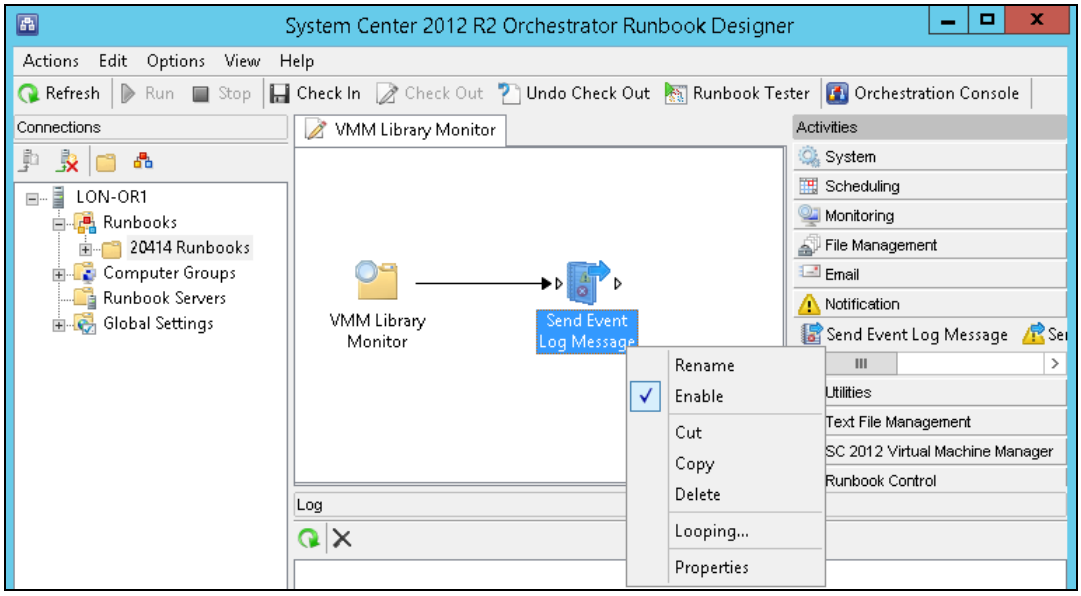
15. Chuột phải lên mũi tên, chọn **Properties.**



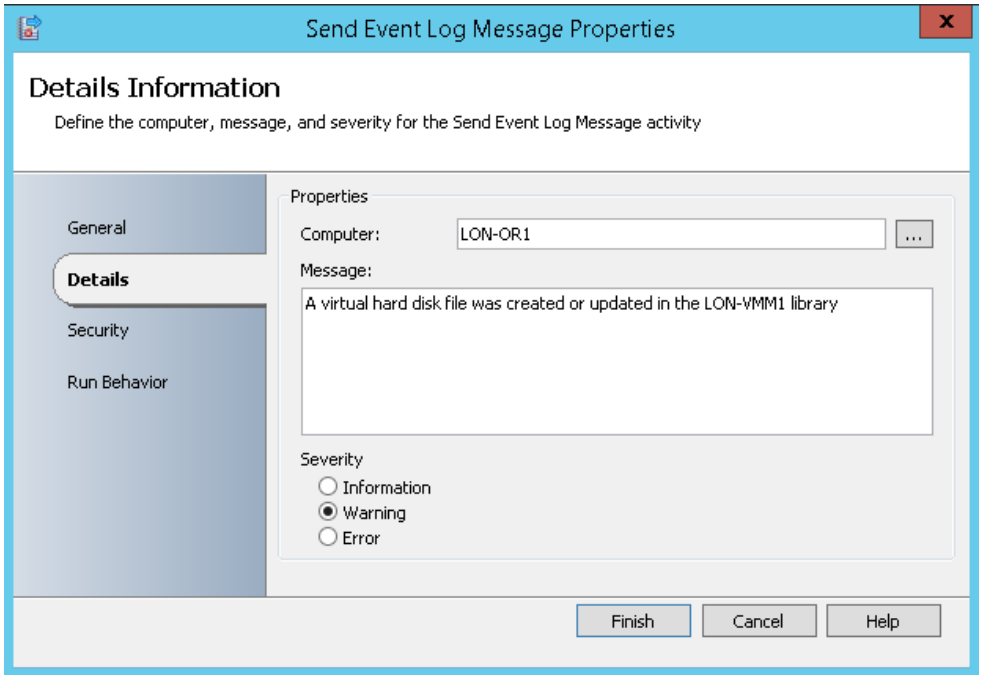

16. Cửa sổ **Link Properties**, kiểm tra thông tin và chọn **Finish**.



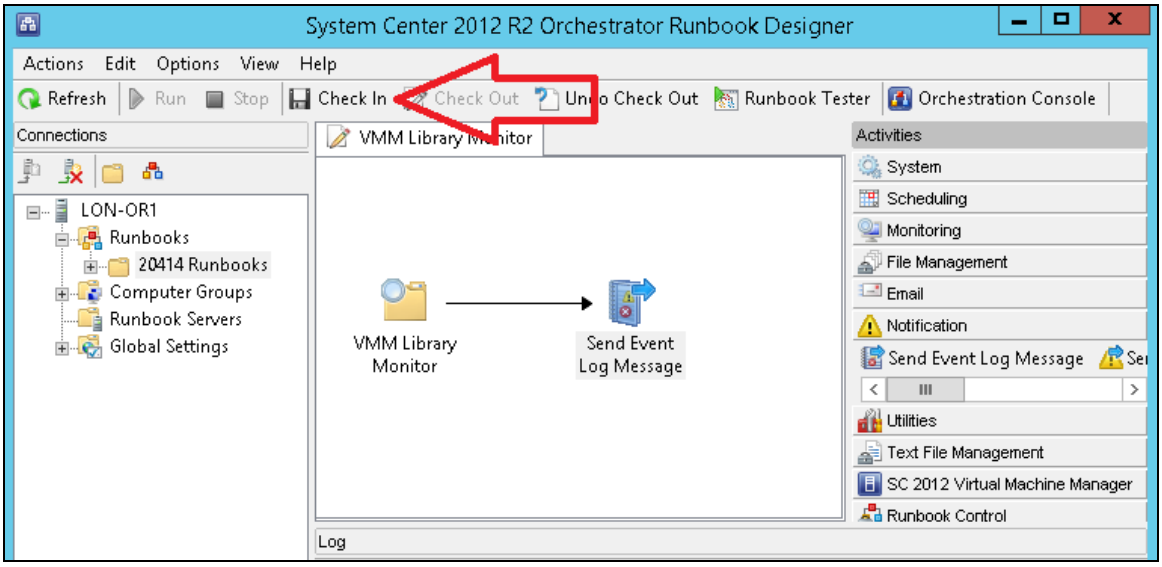
17. Chuột phải **Send Event Log Message**, chọn **Properties**.



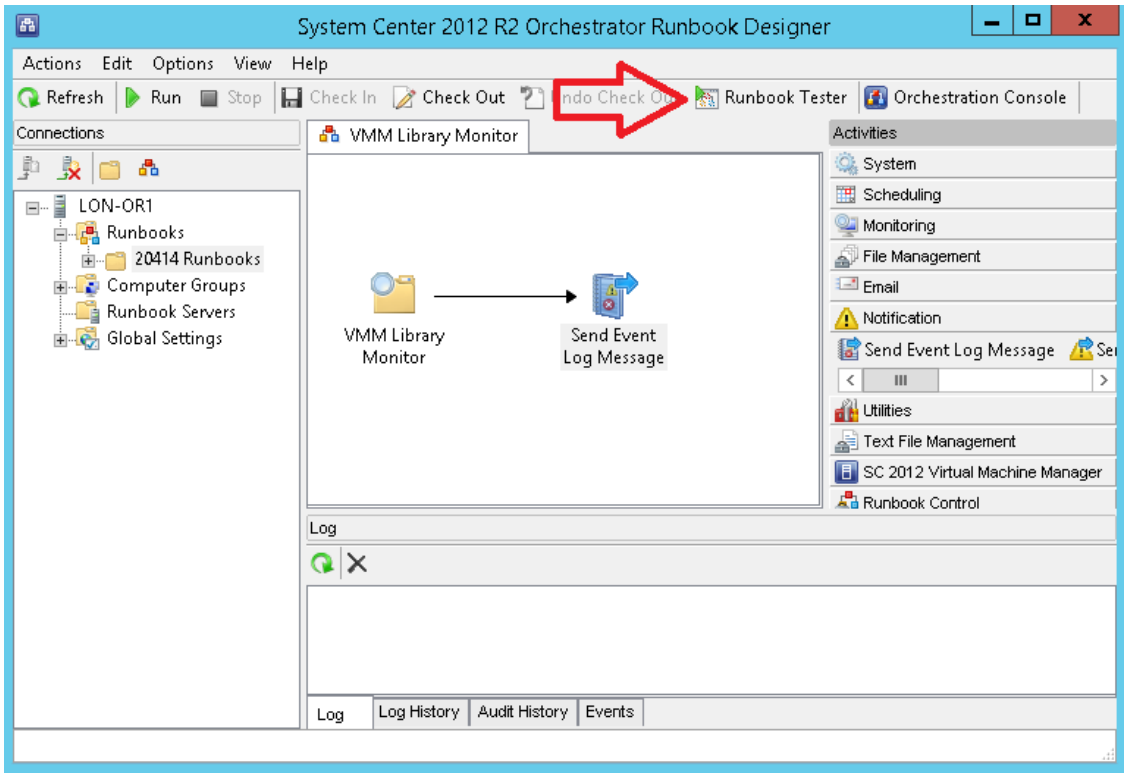

18. Cửa sổ **Details**, trong ô **Computer**, nhập **LON-OR1**, trong ô **Message**, nhập **A virtual hard disk file was created or updated in the LON-VMM1 library**, trong **Severity**, chọn **Warning**, và chọn **Finish**.



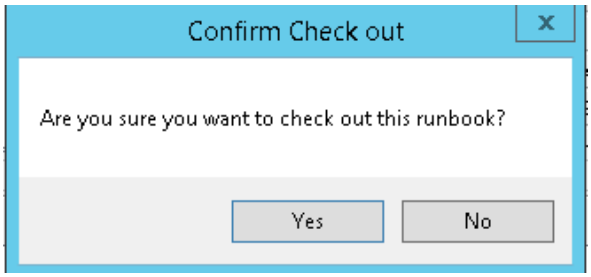
19. Trong cửa sổ **Runbook Designer**, chọn **Check In**.



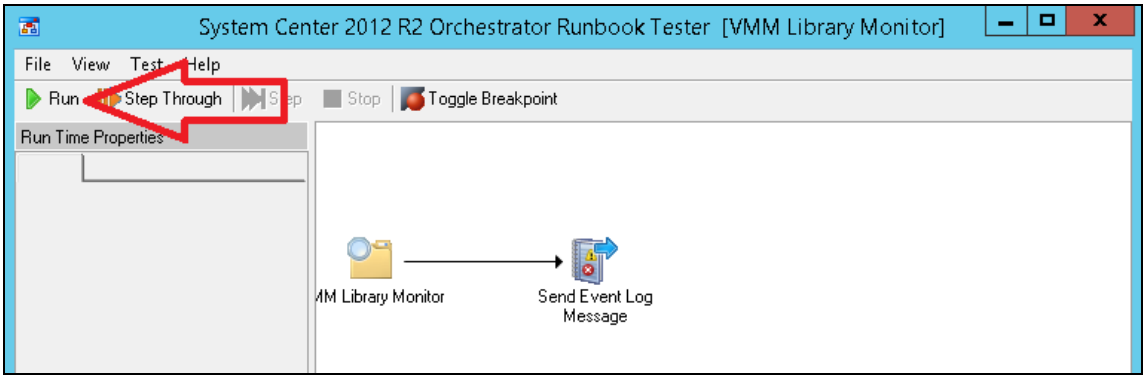

20. Sau đó chọn **Runbook Tester**.



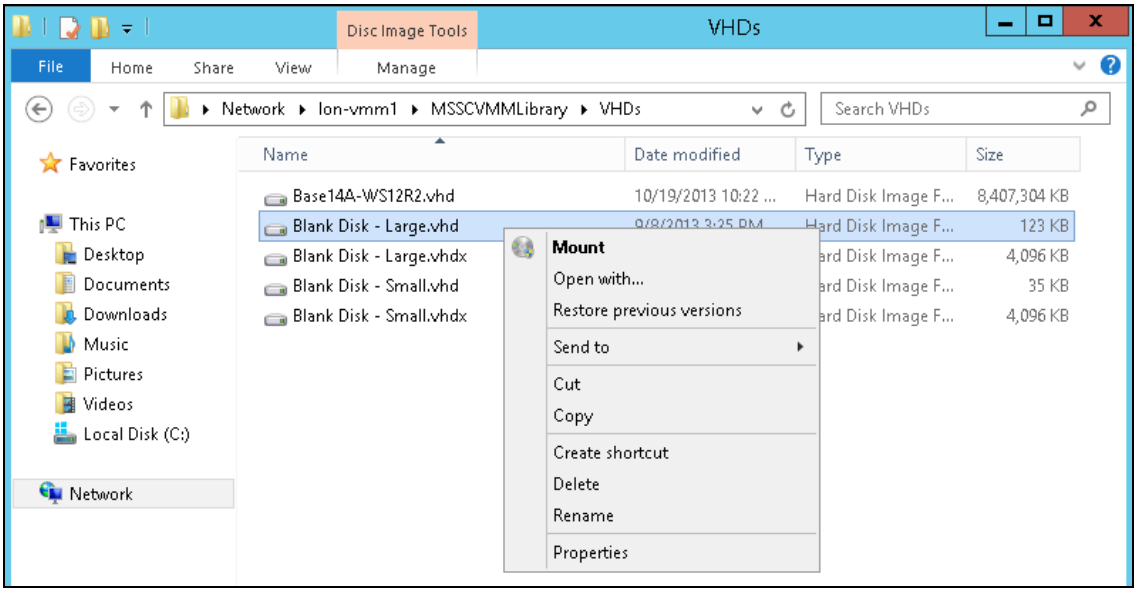
21. Hộp thoại **Confirm Check out**, chọn **Yes**.



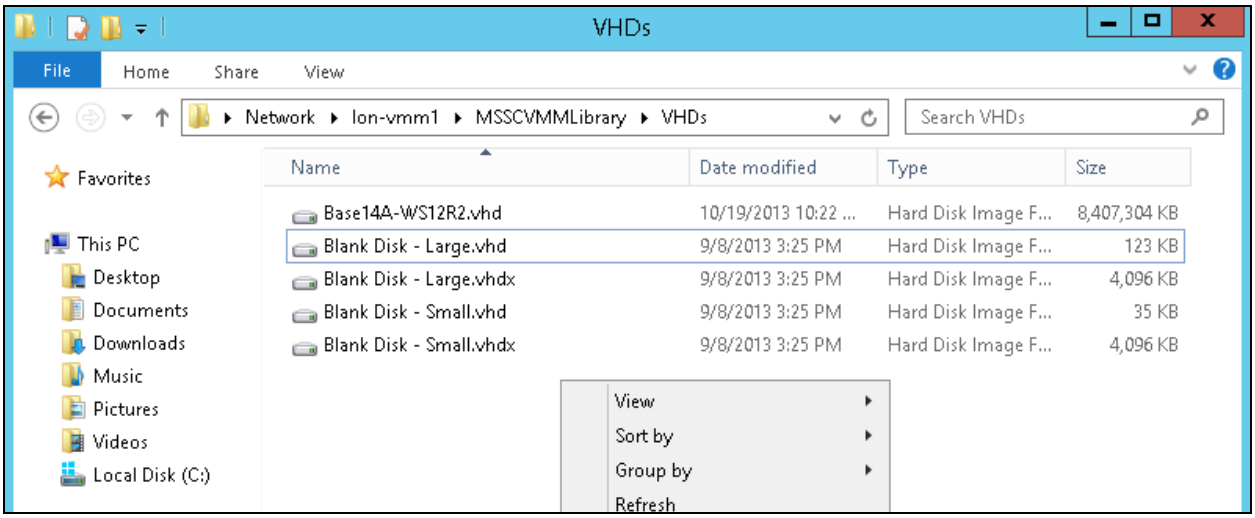

22. Trong cửa sổ **Runbook Tester**, chọn **Run**.



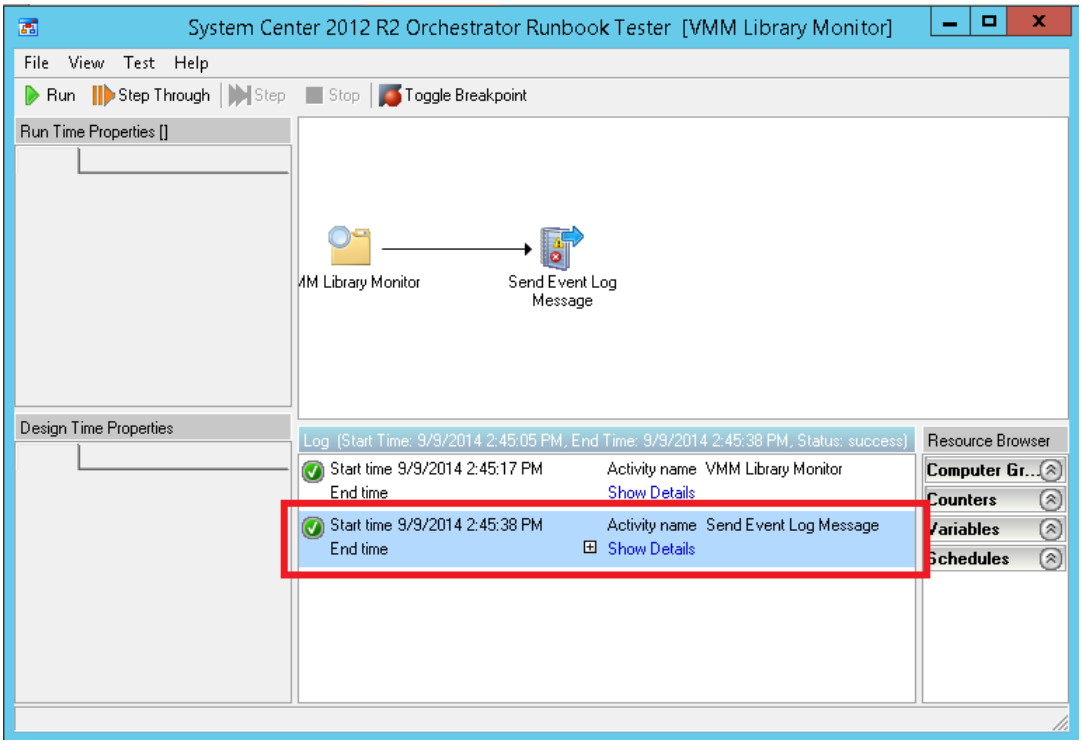

23. Mở **File Explorer,** truy cập **\\lon-vmm1\MSSCVMMLibrary\VHDs,** copy file **Blank Disk – Large.vhd**



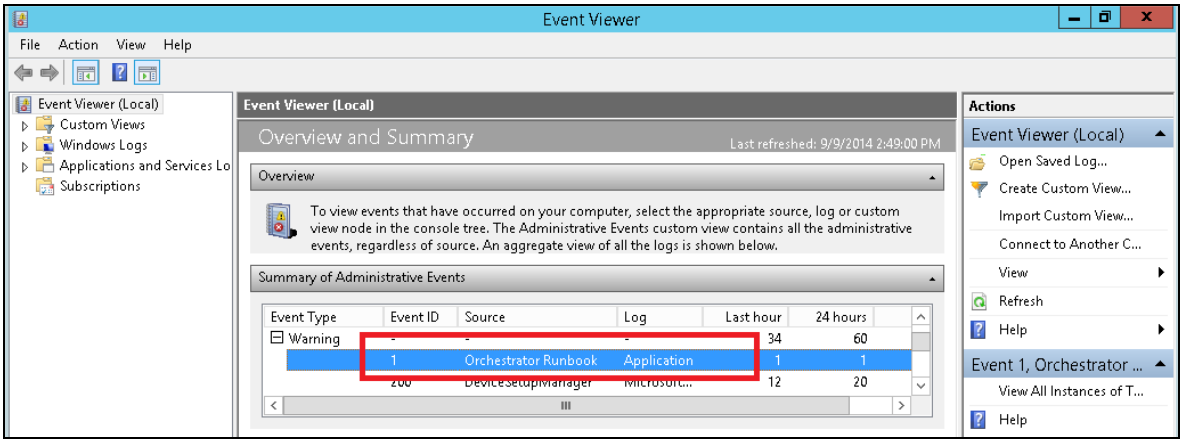
24. Chuột phải lên khoảng trắng, chọn **Paste**. Kiểm tra file mới có tên **Blank Disk – Large – Copy.vhd.**



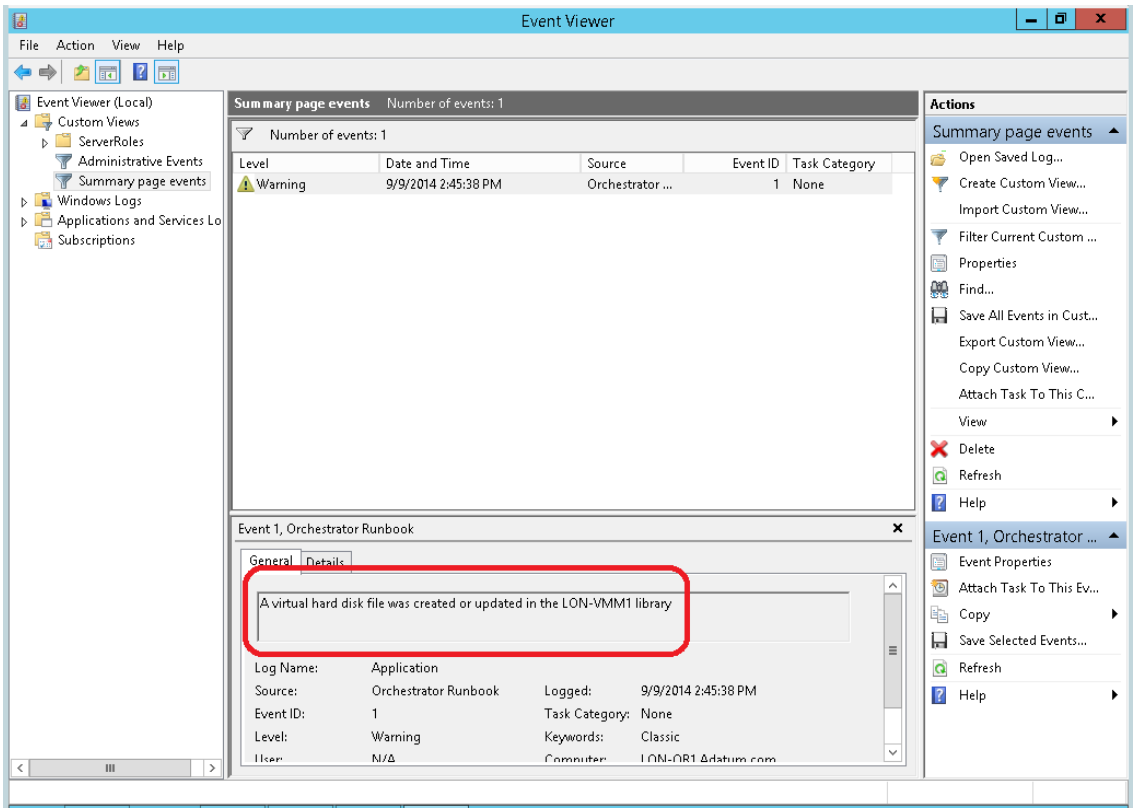

25. Qua cửa sổ **Runbook Tester**, trong phần **Log**, đợi đến khi có thông báo**Activity name Send Event Log Message**.



26. Bung **Start** menu, gõ **Event**, mở **Event Viewer**. Trong phần **Summary of Administrative Events**, bung **Warning**, tìm **Event ID 1,** trong cột **Source** có tên **Orchestrator Runbook**. Nhấp đôi chuột lên dòng **Orchestrator Runbook**.




27. Kiểm tra thông báo trong event. Tắt **Event Viewer**, **File Explorer** và **Runbook Tester**.



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cài đặt thành công Microsoft® System Center 2012 Integrations Pack cho Virtual Machine Manager (VMM). Và bạn đã tạo ra một Runbook cơ bản trong System Center 2012 Orchestrator Runbook Designer**

## Bài tập 2: Ủy quyền quản lý VMM và Self-Service.

Để giải quyết các yêu cầu quản lý của nhóm Developments, bạn sẽ thực hiện phân quyền quản lý VMM và Self-service. Bạn cần phải cấu hình các Delegated Administration Roles và Self-service Roles, sau đó kiểm tra cấu hình.

❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Delegated Administrator Role trong VMM.
2. Cấu hình Self-service Administration trong VMM.
3. Kiểm tra cấu hình bằng VMM.
4. Kiểm tra cấu hình bằng App Controller.

❖ **Thực hiện:**

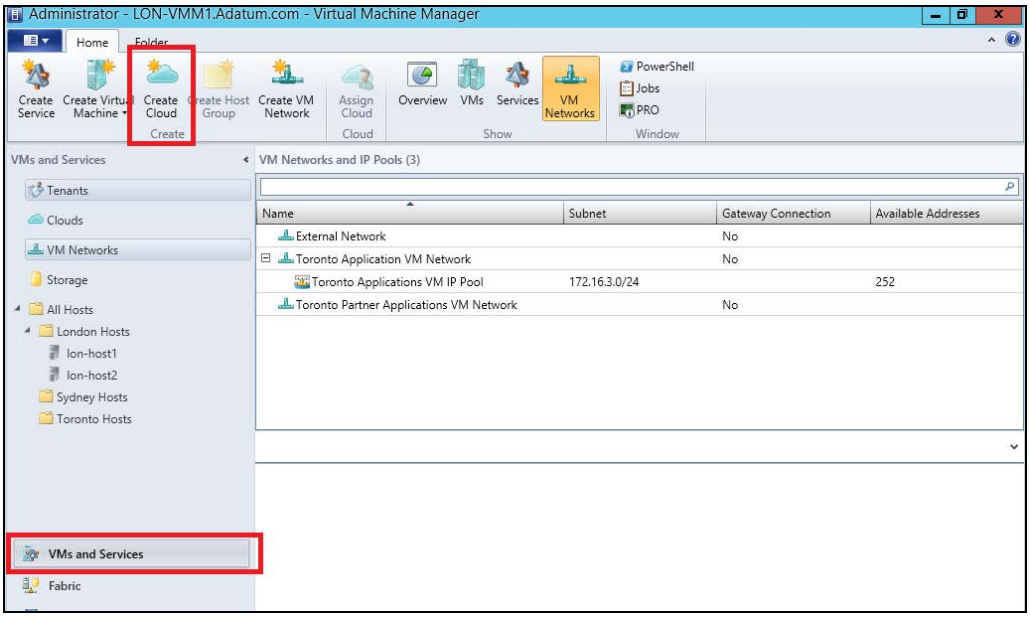
## Bước 1: Cấu hình Delegated Administrator Role trong VMM.

➢ **Tạo Private Cloud**

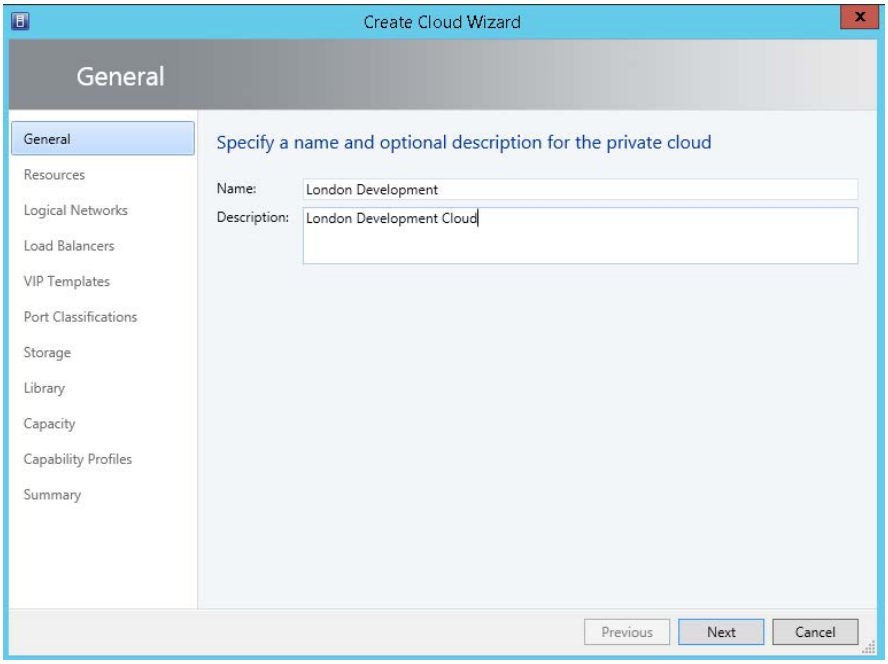
1. Trên máy **LON-VMM1**, mở **Virtual Machine Manager**, cửa sổ **Connect to Server,** chọn **Connect**.



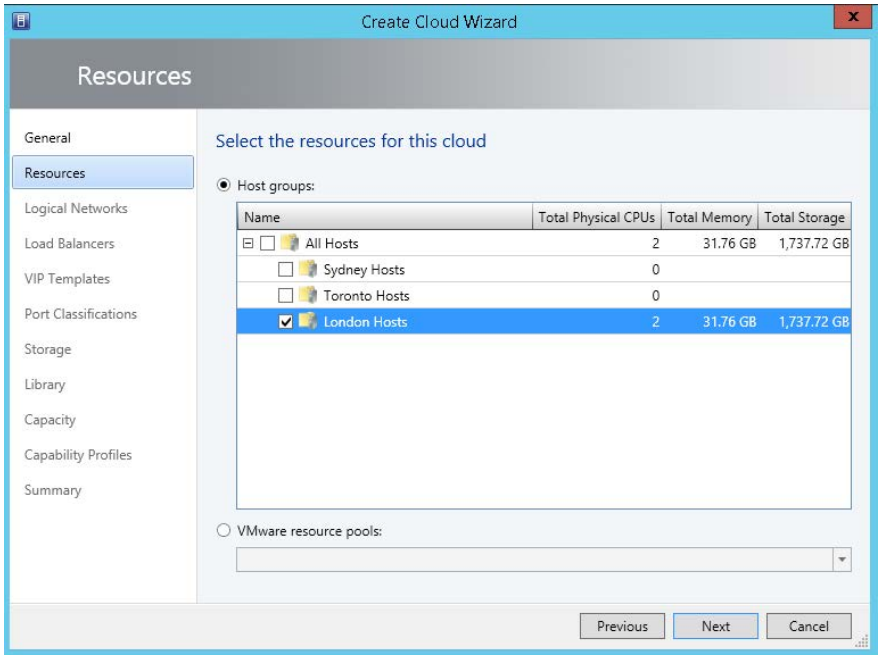

2. Trong cửa sổ **VMM**, chọn **VMs and Service**, chọn **Create Cloud**.



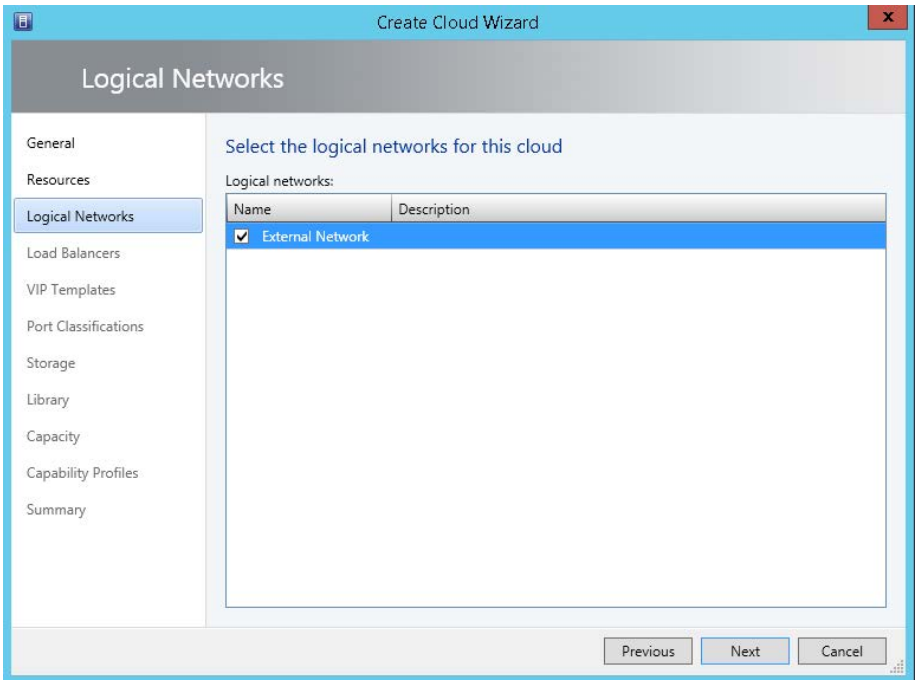
3. Cửa sổ **General**, trong ô **Name**, nhập **London Development**, trong ô **Description**, nhập **London Development Cloud**, và chọn **Next**.



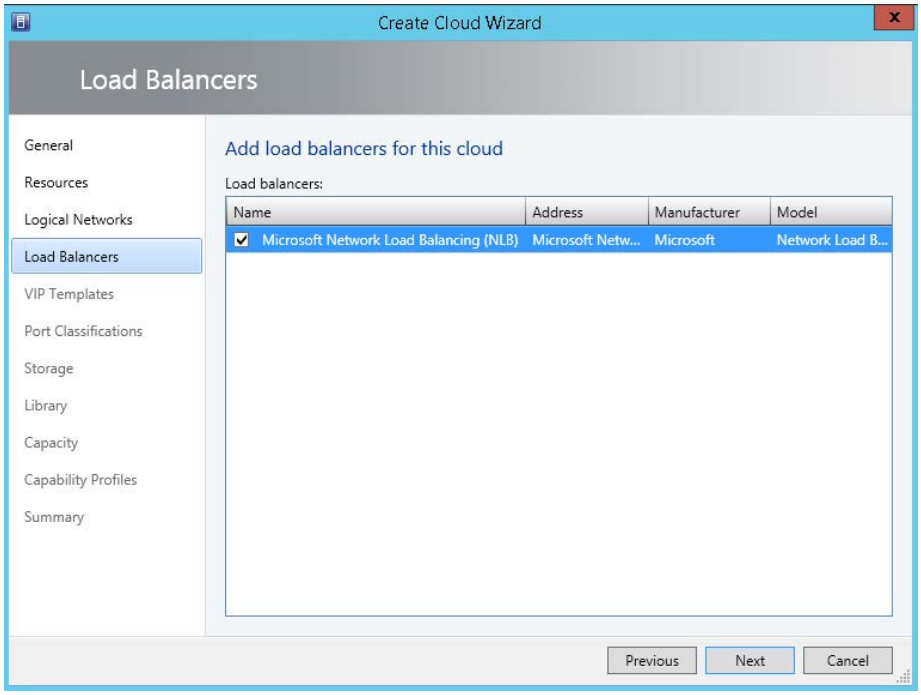

4. Cửa sổ **Resources**, đánh dấu chọn **London Hosts**, và chọn **Next**.



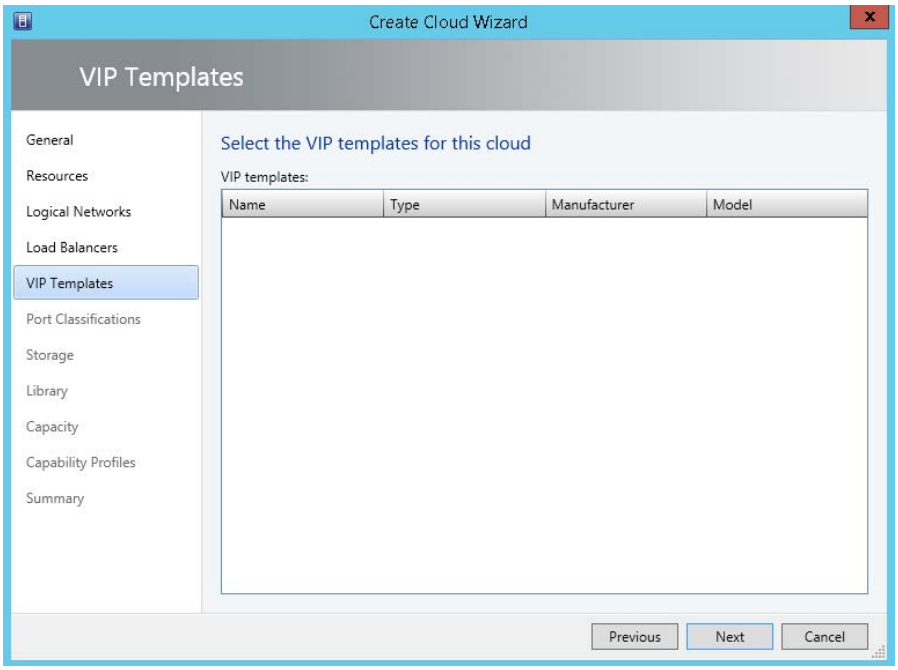
5. Cửa sổ **Logical Networks**, đánh dấu chọn **External Network**, chọn **Next**.



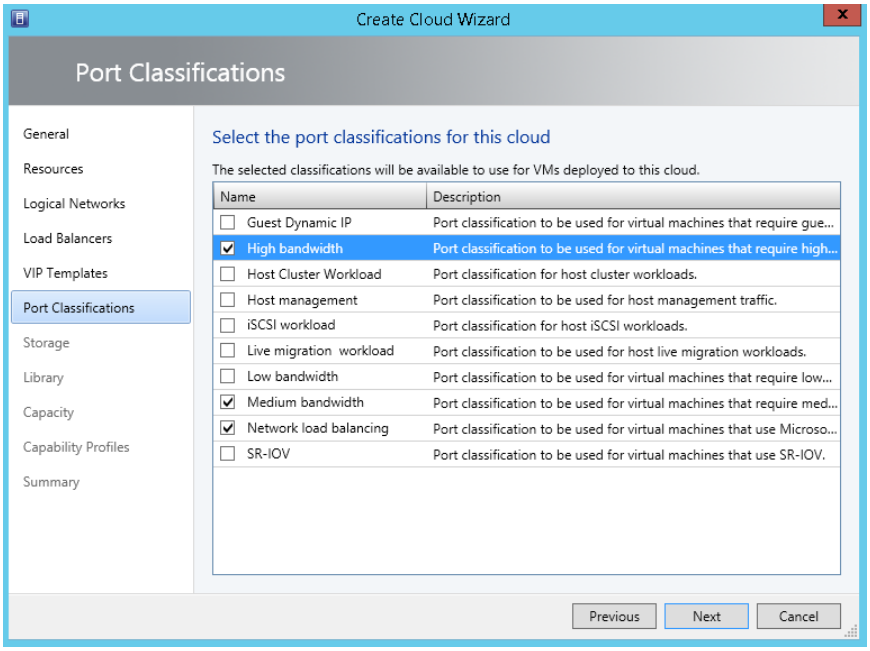

6. Cửa sổ **Load Balancers**, đánh dấu chọn **Microsoft Load Balancing (NLB)**, chọn **Next**.



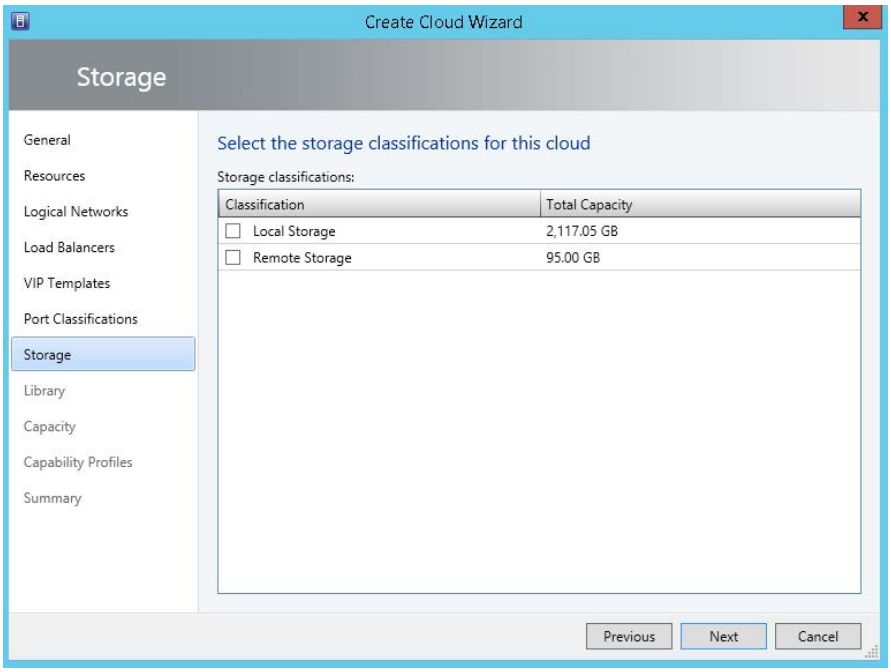
7. Cửa sổ **VIP Template**, chọn **Next**.



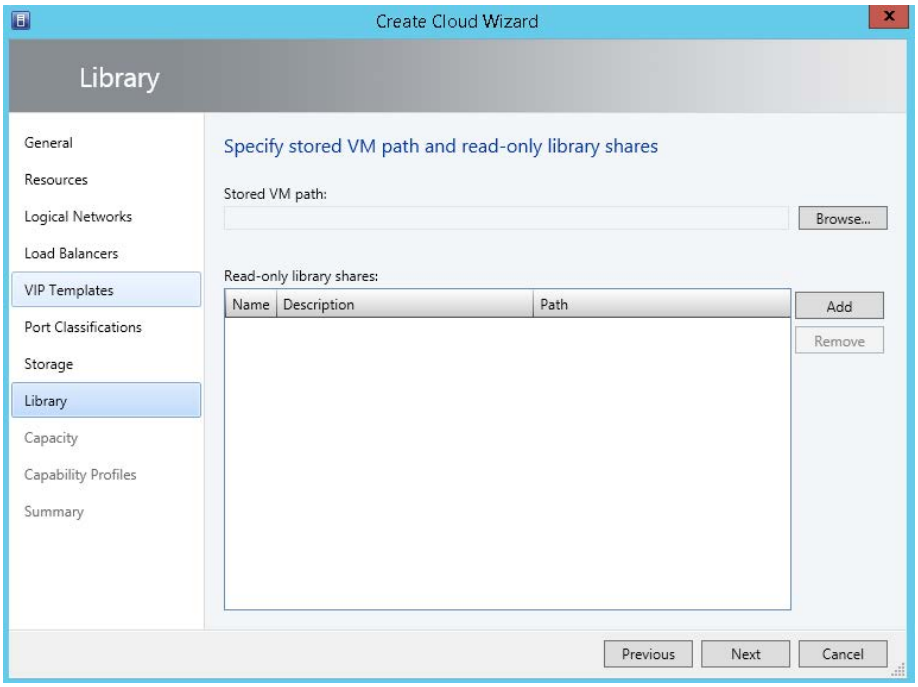

8. Cửa sổ **Port Classifications**, đánh dấu chọn 3 ô **Network load balancing**, **Medium Bandwidth**, và **High Bandwidth**, chọn **Next**.



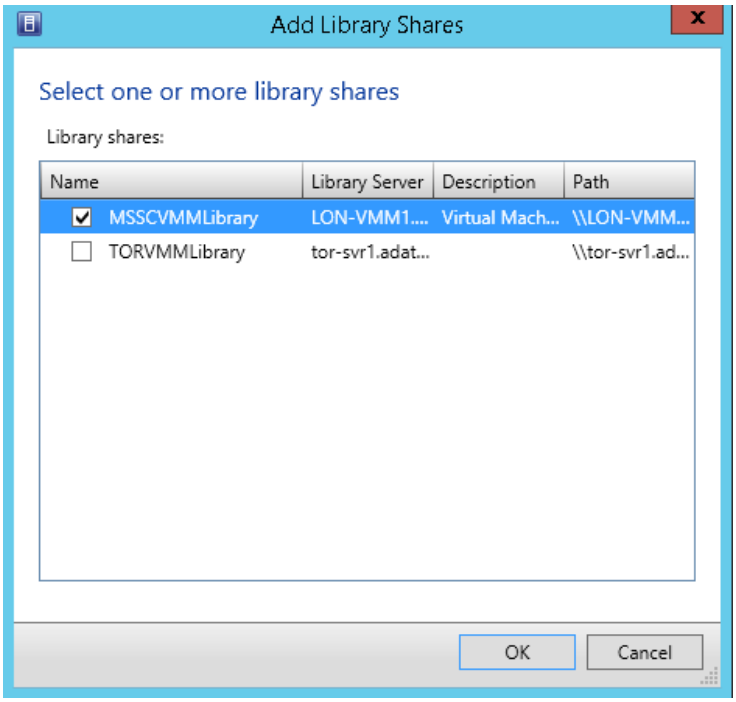
9. Cửa sổ **Storage**, chọn **Next**.



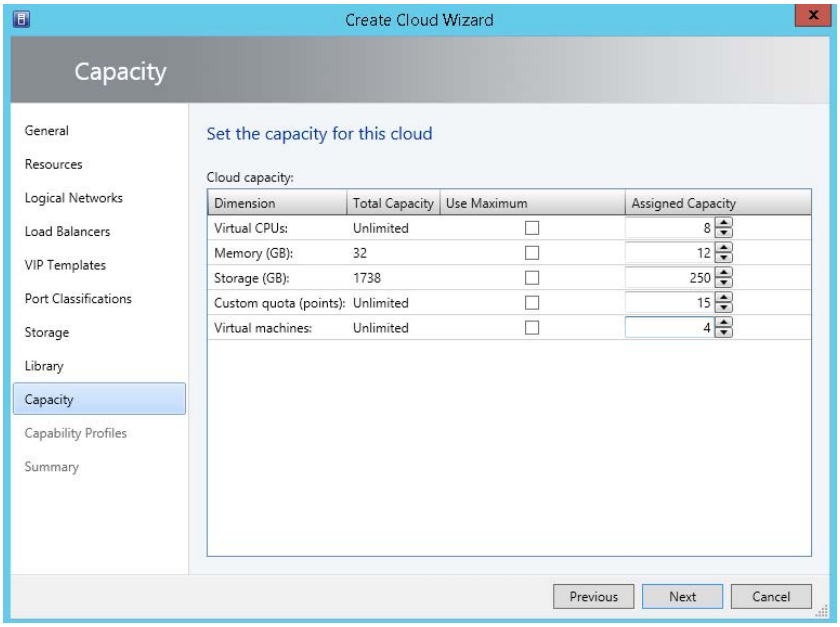

10. Cửa sổ **Library**, chọn **Add**.



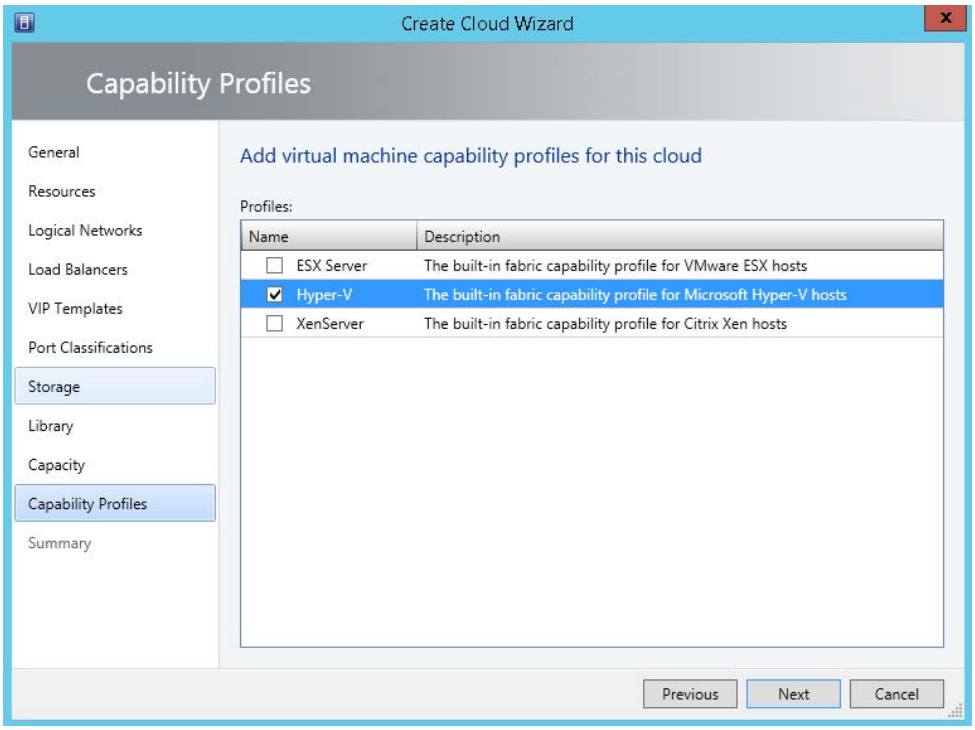
11. Hộp thoại Add Library Shares, đánh dấu chọn **MSSCVMMLibrary**, chọn **OK**, chọn **Next**.




12. Cửa sổ **Capacity**, bỏ trắng tất cả các ô chọn, khai báo thông số như trong hình bên dưới, và chọn **Next**.



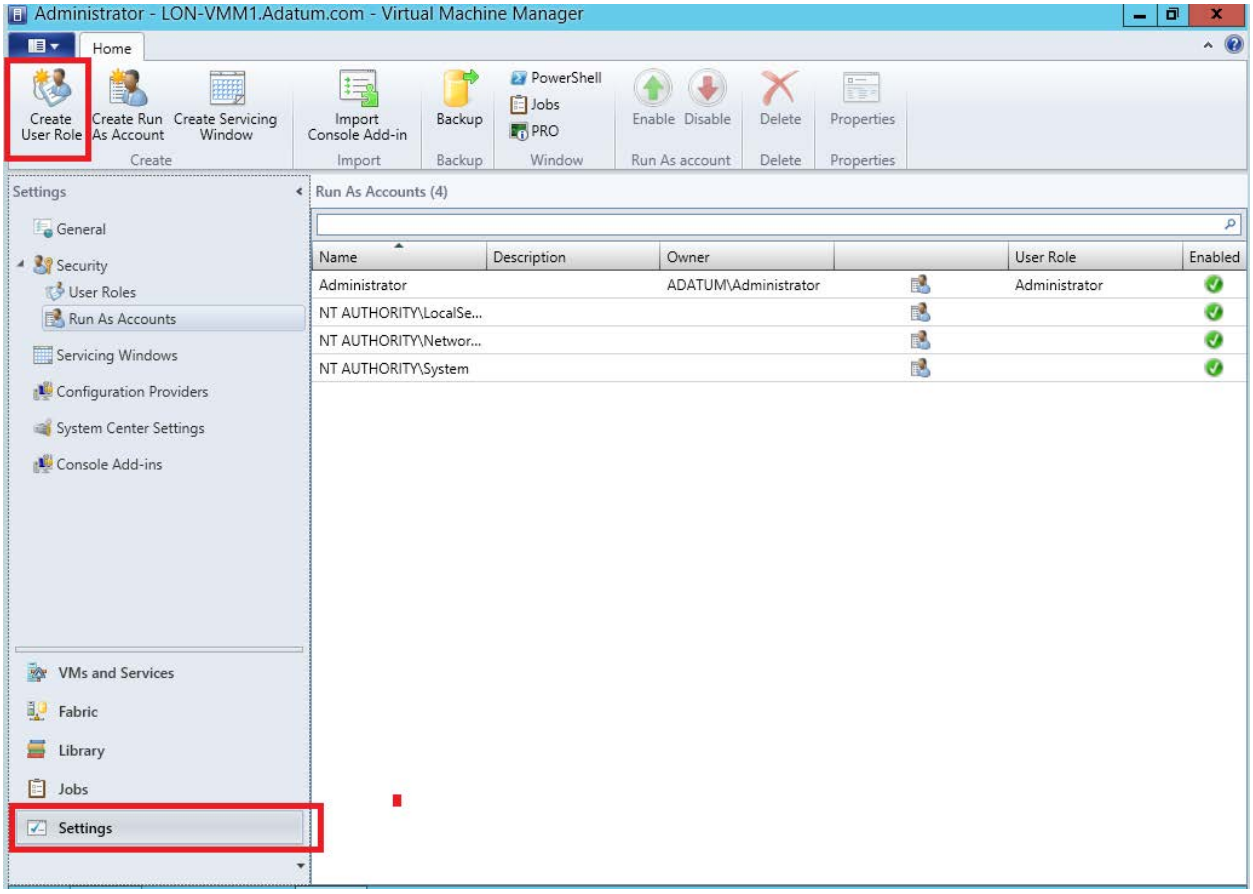
13. Cửa sổ **Capability Profiles**, đánh dấu chọn **Hyper-V**, chọn **Next**, và chọn **Finish.**



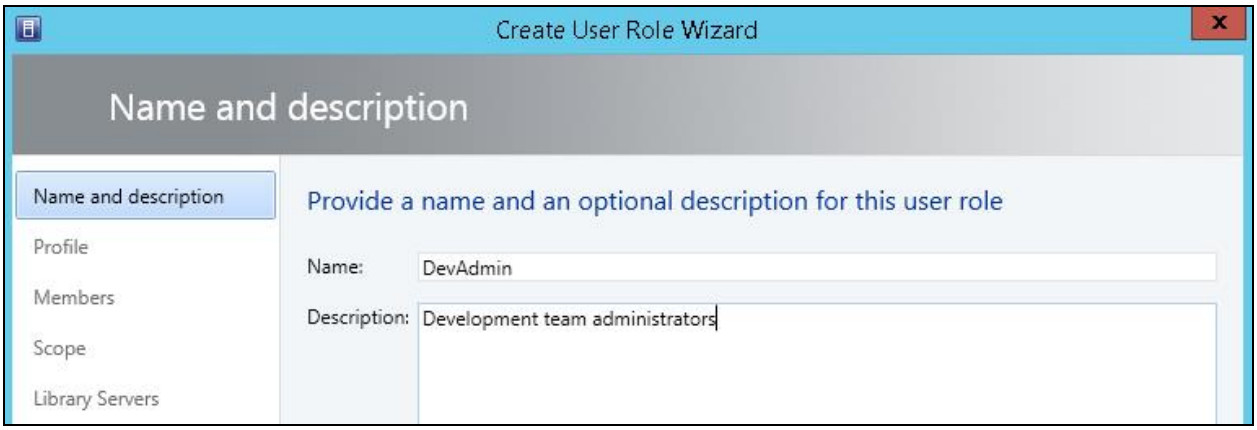

14. Kiểm tra và tắt cửa sổ **Jobs**.

## ➢ Ủy quyền quản lý trong VMM

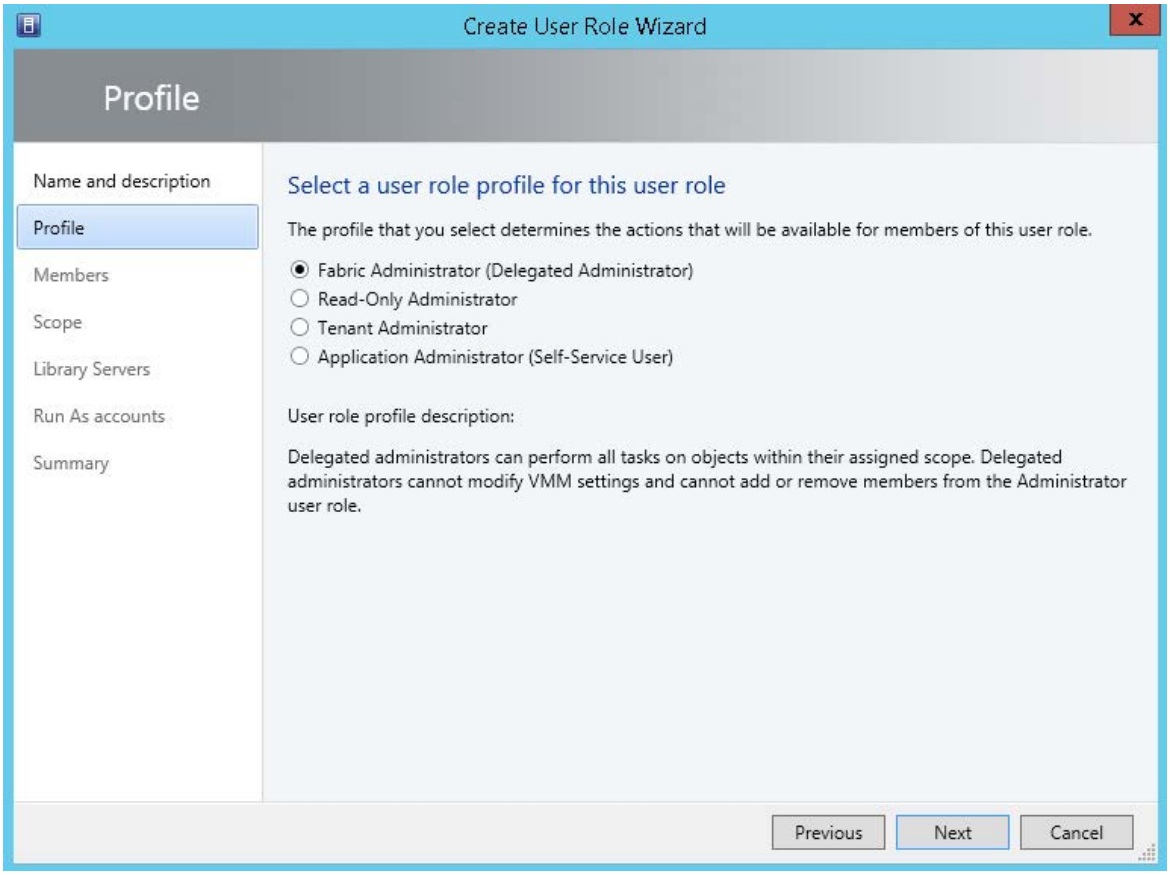
1. Trong cửa **sổ Virtual Machine Manager**, chọn **Settings**, và chọn **Create User Role**.



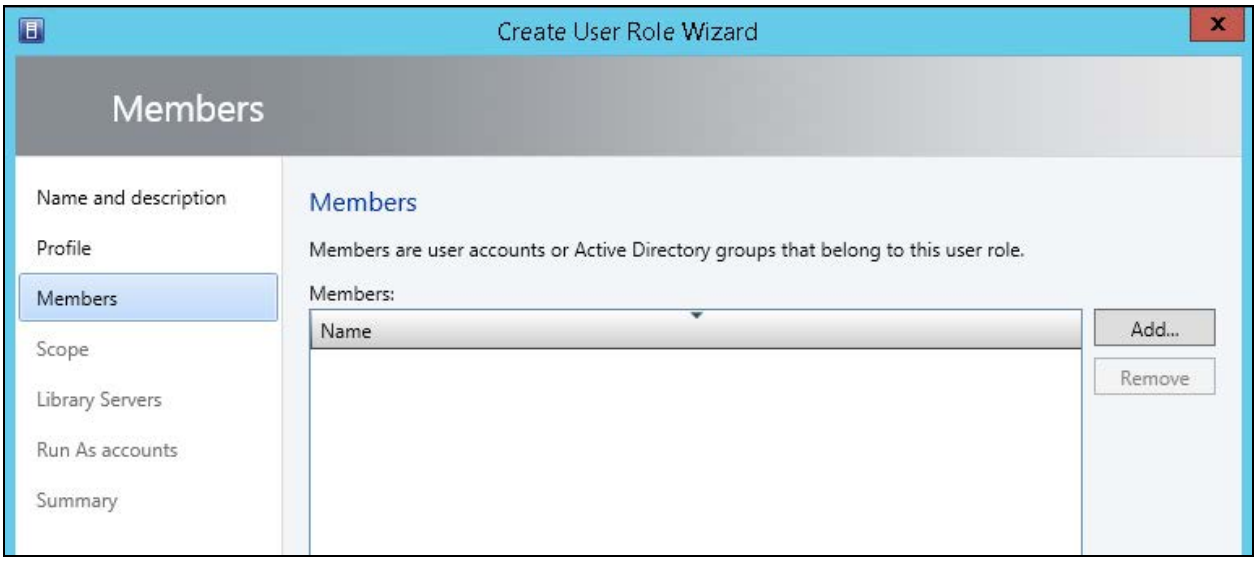
2. Cửa sổ **Name and description**, trong ô **Name**, nhập **DevAdmin**, trong ô **Description**, nhập **Development team administrators**, và chọn **Next**.



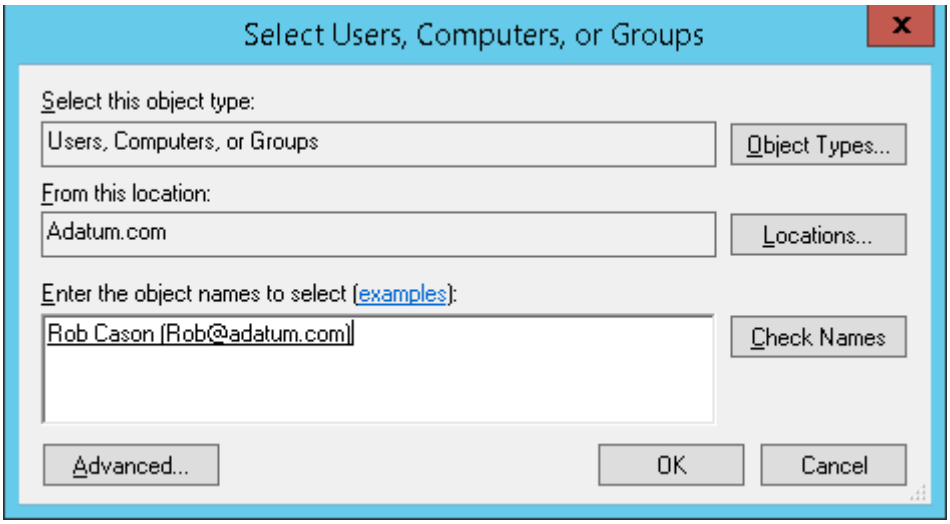

3. Cửa sổ **Profile**, chọn **Fabric Administrator (Delegated Administrator)**, và chọn **Next**.



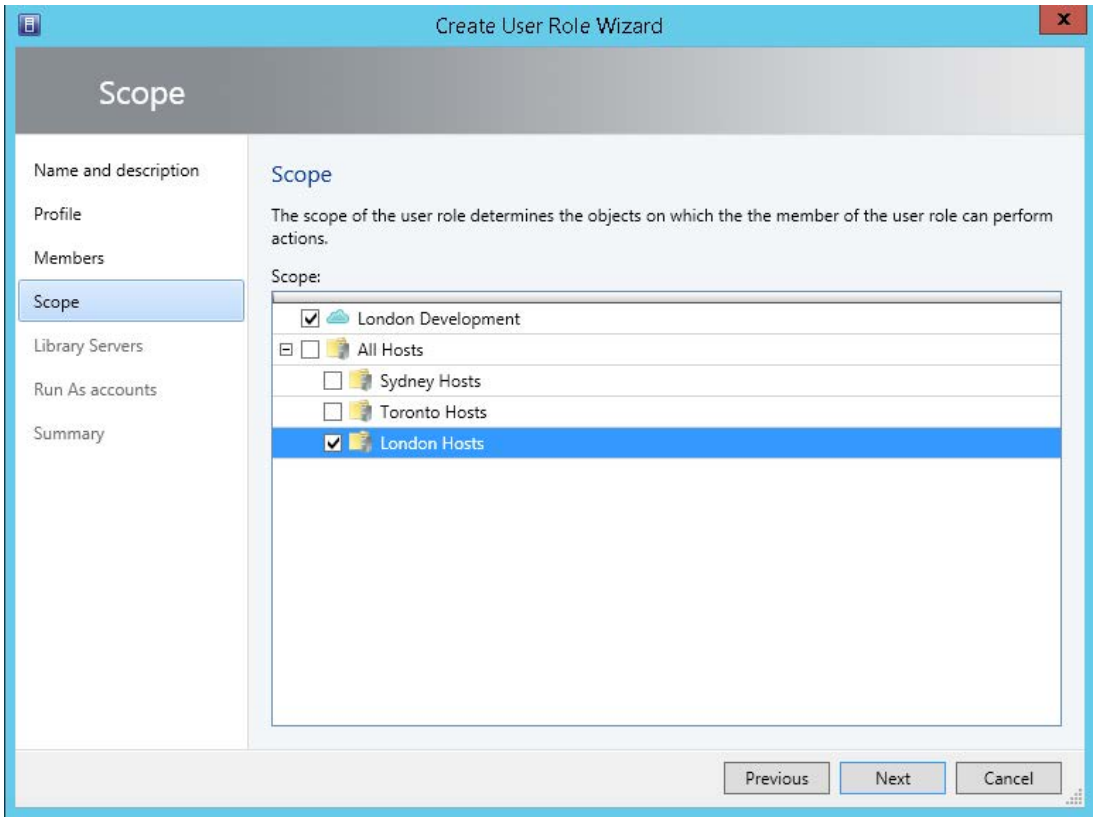
4. Cửa sổ **Members**, chọn **Add**,



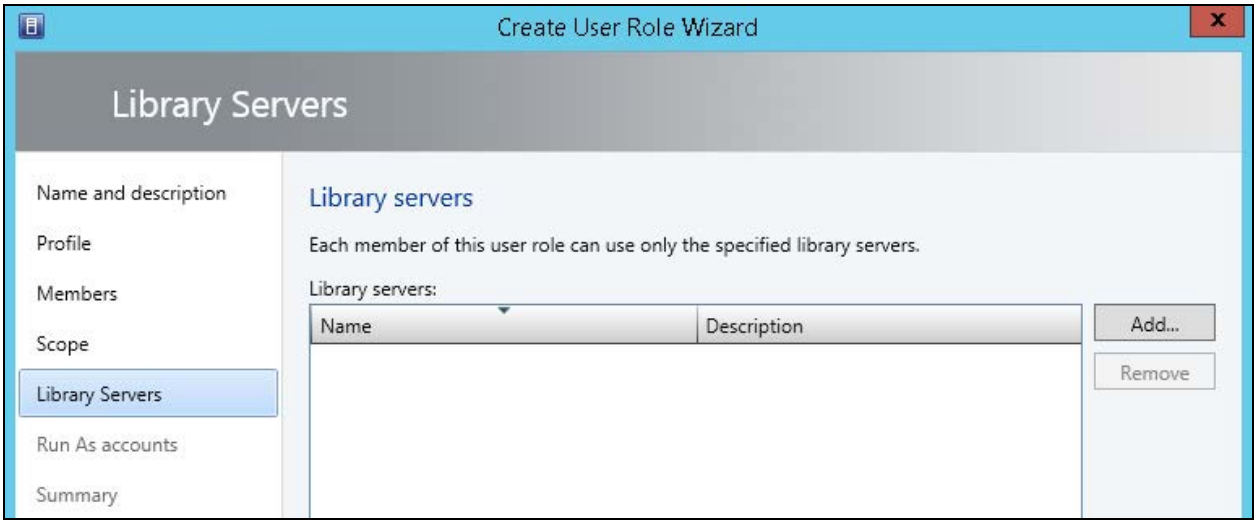

5. Hộp thoại **Select Users**, **Computers**, **or Groups**, nhập **Rob Cason**, chọn **Check Names**, chọn **OK**, và chọn **Next**.



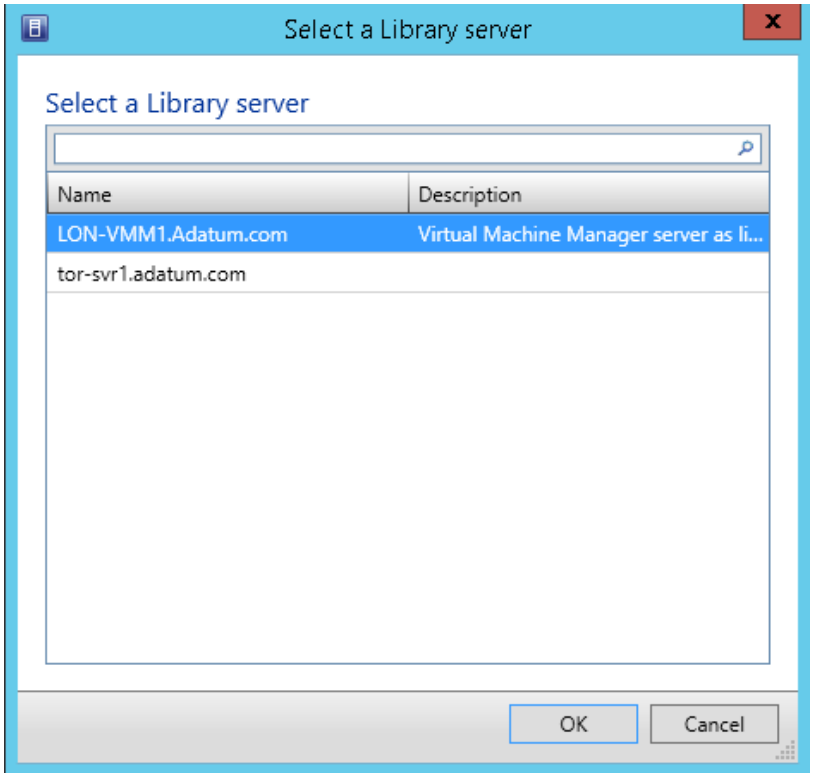
6. Cửa sổ **Scope**, đánh dấu chọn 2 ô **London Development** và **London Hosts**, chọn **Next**.



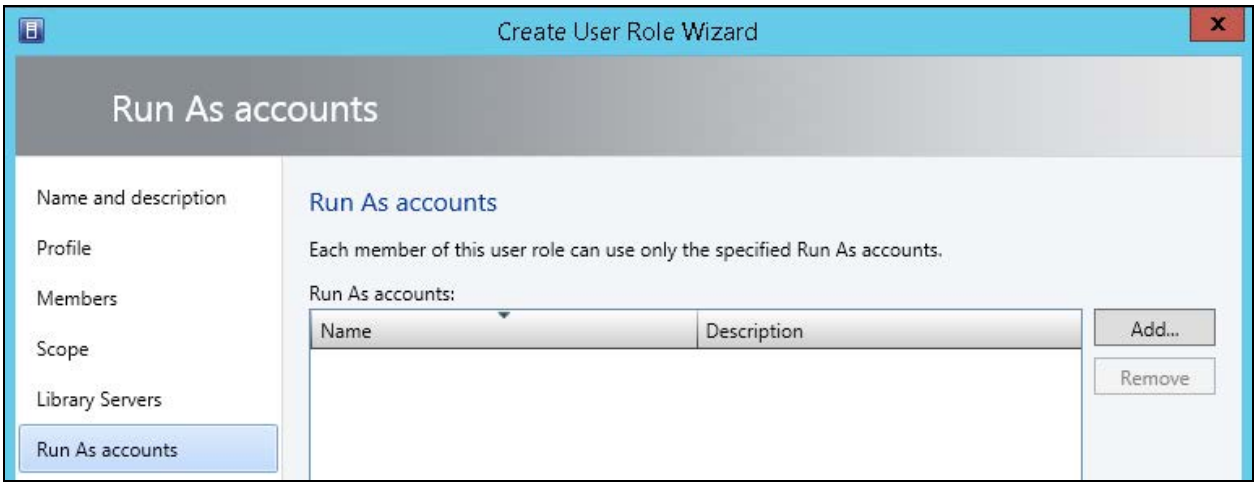

7. Cửa sổ **Library servers**, chọn **Add.**



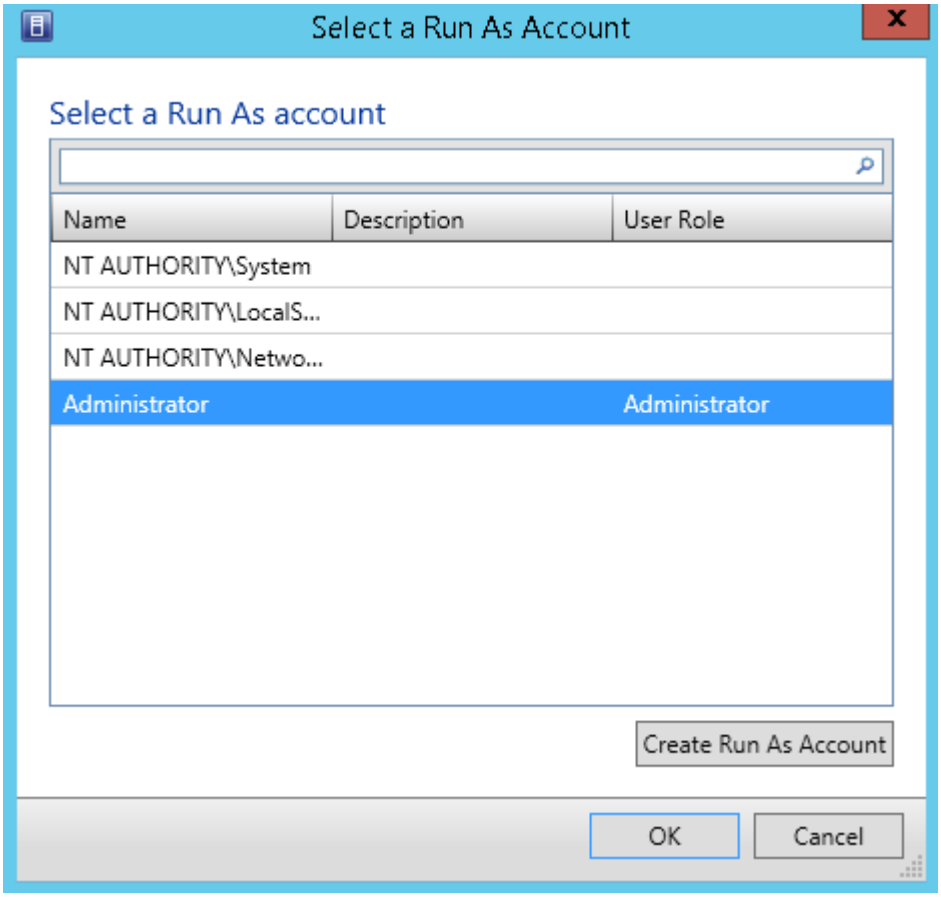
8. Hộp thoại **Select a Library servers,** chọn **LON-VMM1.Adatum.com**, chọn **OK**, và chọn **Next**.




9. Cửa sổ **Run As accounts**, chọn **Add**.



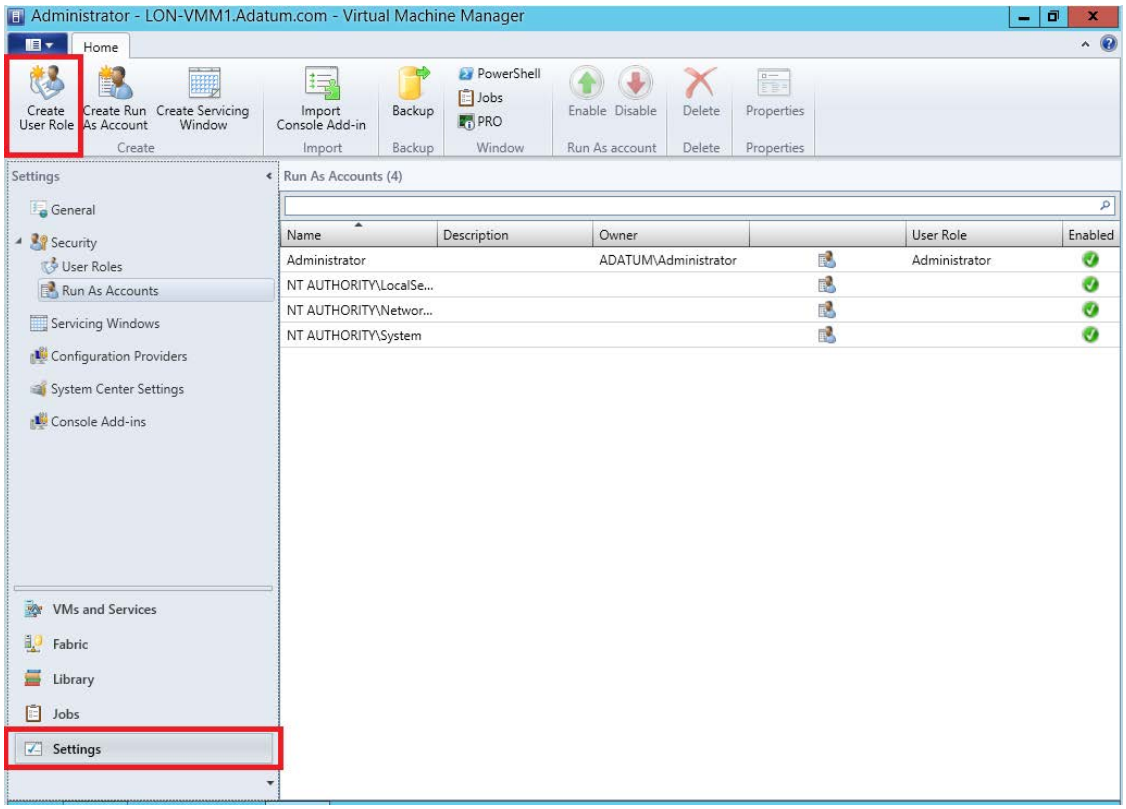
10. Hộp thoại **Select a Run As Accounts**, chọn **Administrator**, chọn **OK**, chọn **Next**, và chọn **Finish**.




11. Kiểm tra và tắt cửa sổ **Jobs**.

## Bước 2: Cấu hình Self-service Administration trong VMM.

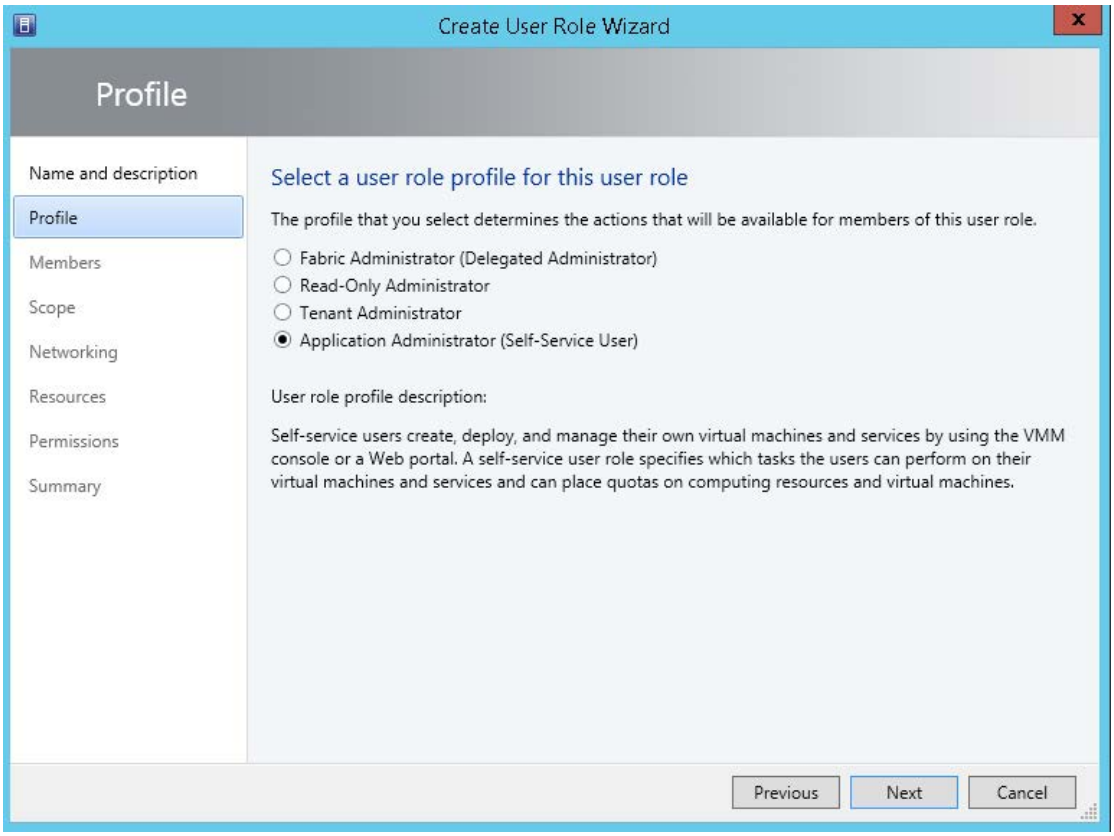
1. Trên máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **Settings**, chọn **Create User Role**.



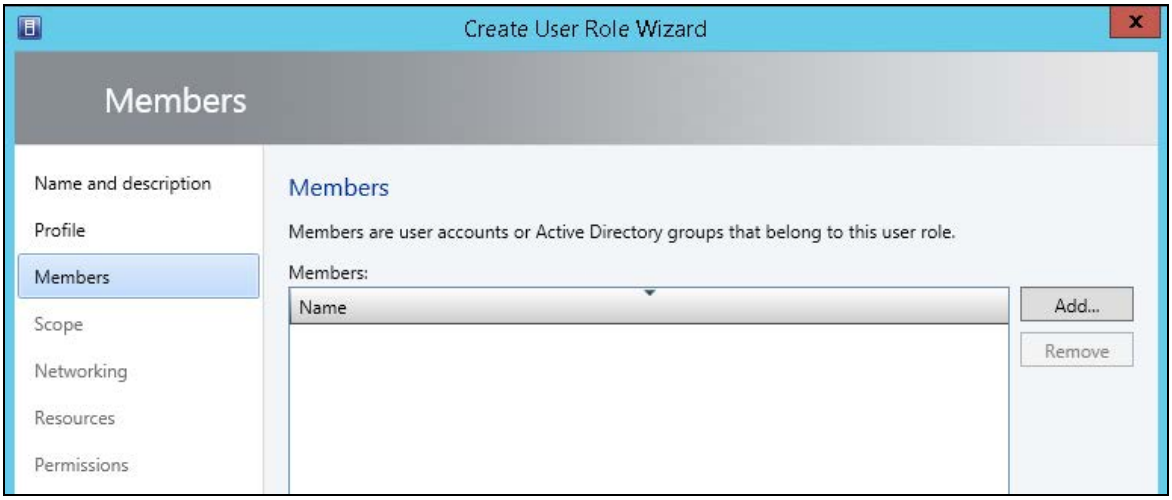

2. Cửa sổ **Name and Description**, trong ô **Name**, nhập **DevContractors**, trong ô **Description**, nhập **Development team contractors**, và chọn **Next**.



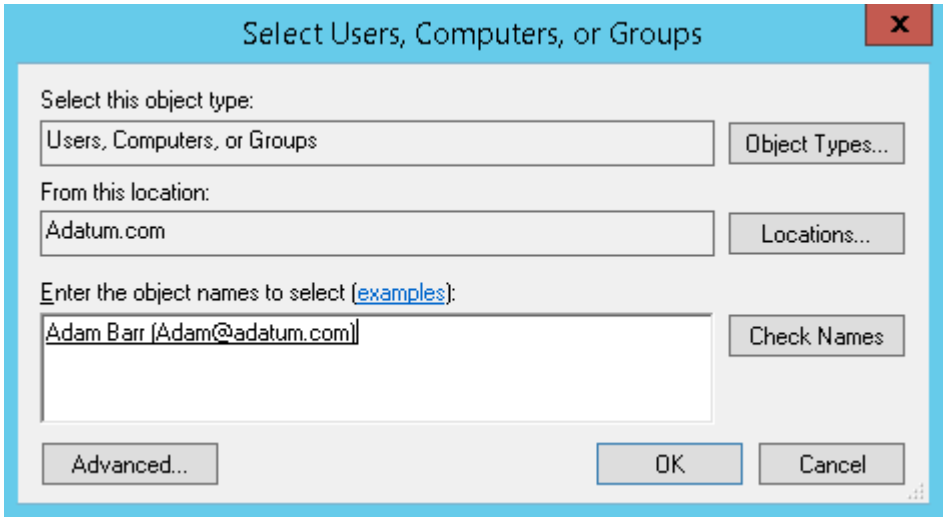
3. Cửa sổ **Profile**, chọn **Application Administrator (Self-Service User)**, và chọn **Next**.



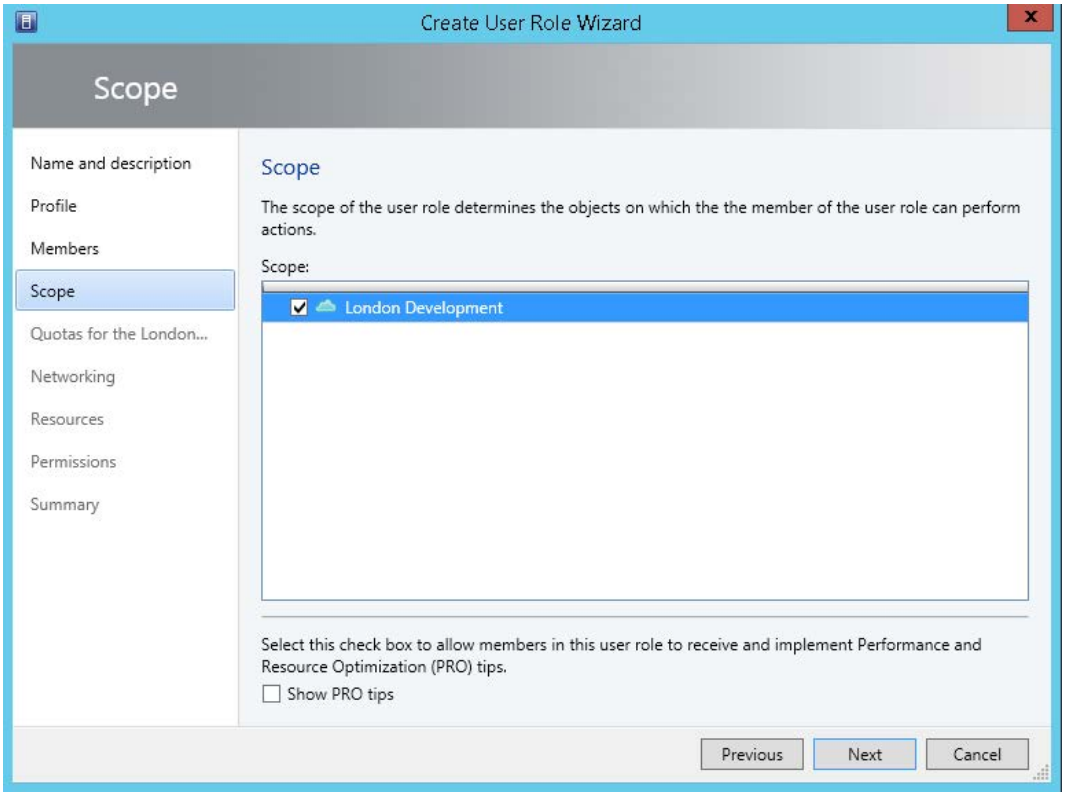

4. Cửa sổ **Members**, chọn **Add**.



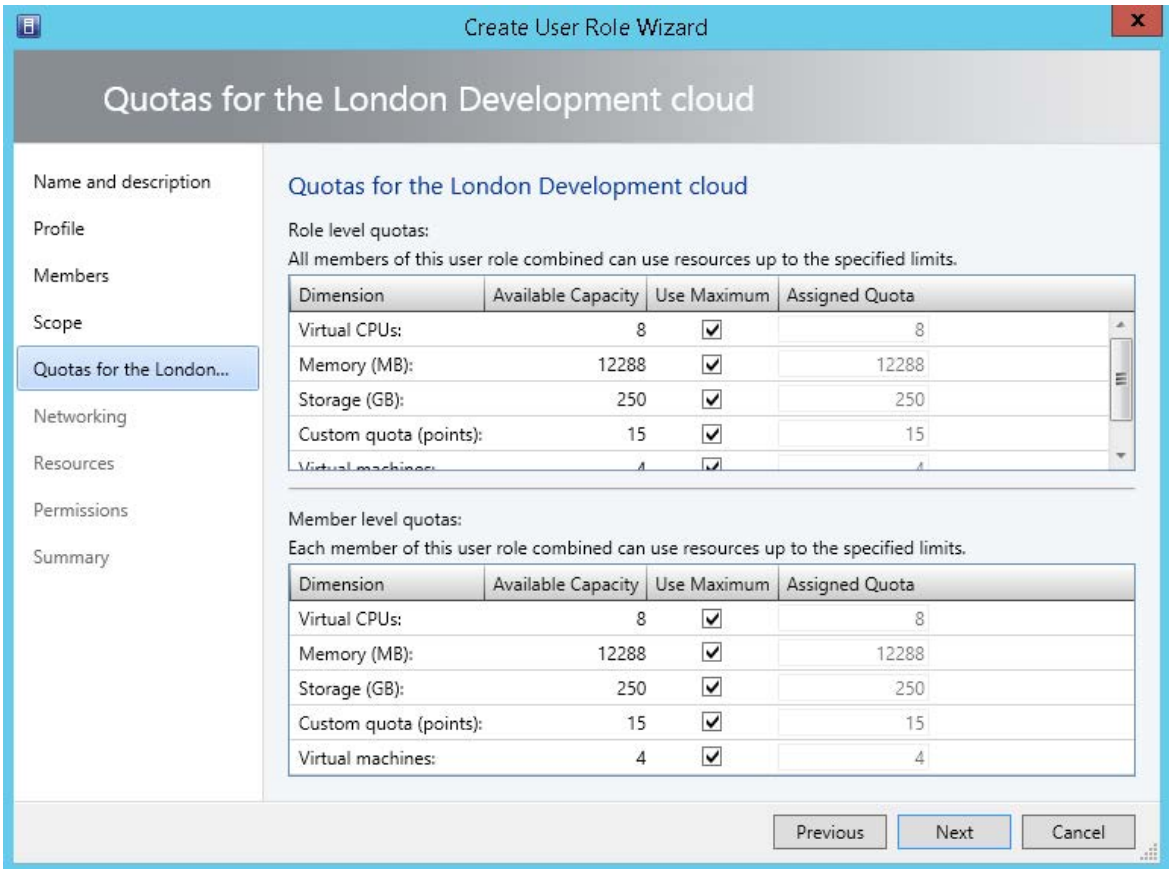
5. Hộp thoại **Select Users, Computers, or Groups,** nhập **Adam**, chọn **Check Names**, chọn **OK**, và chọn **Next**.



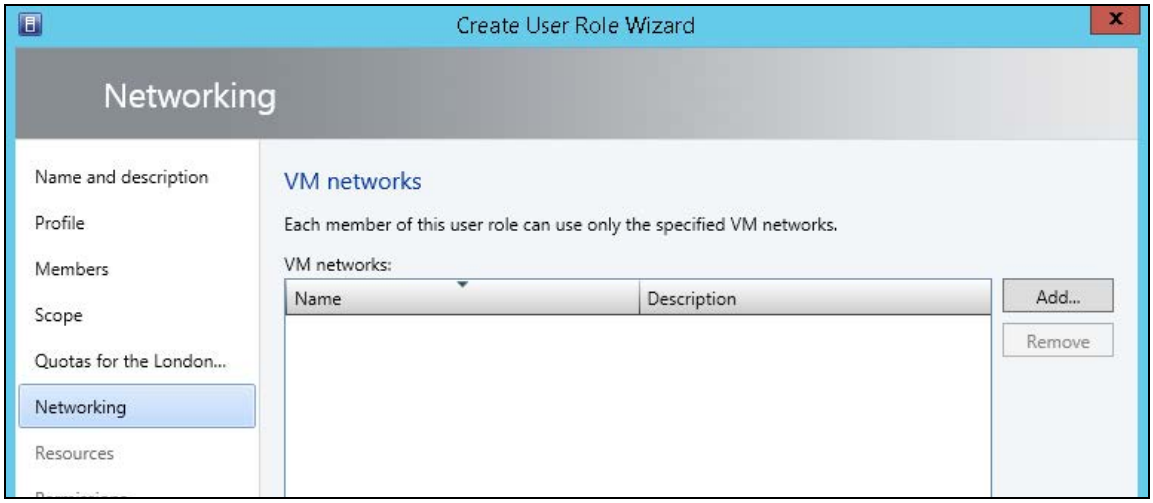

6. Cửa sổ **Scope**, đánh dấu chọn **London Development**, và chọn **Next**.



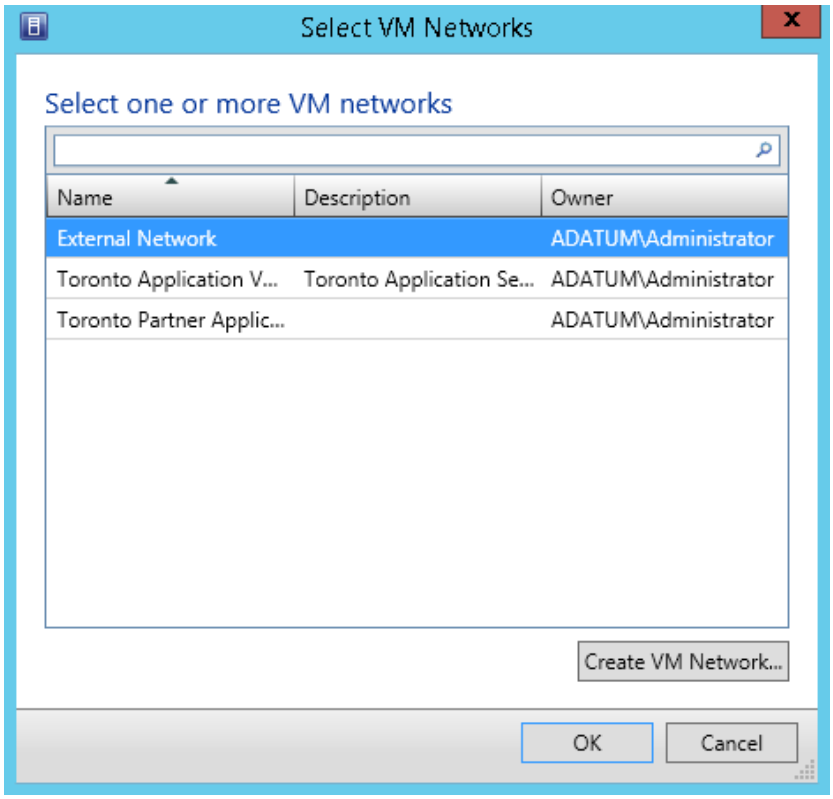
7. Cửa sổ **Quotas for the London Development cloud**, chọn **Next**.



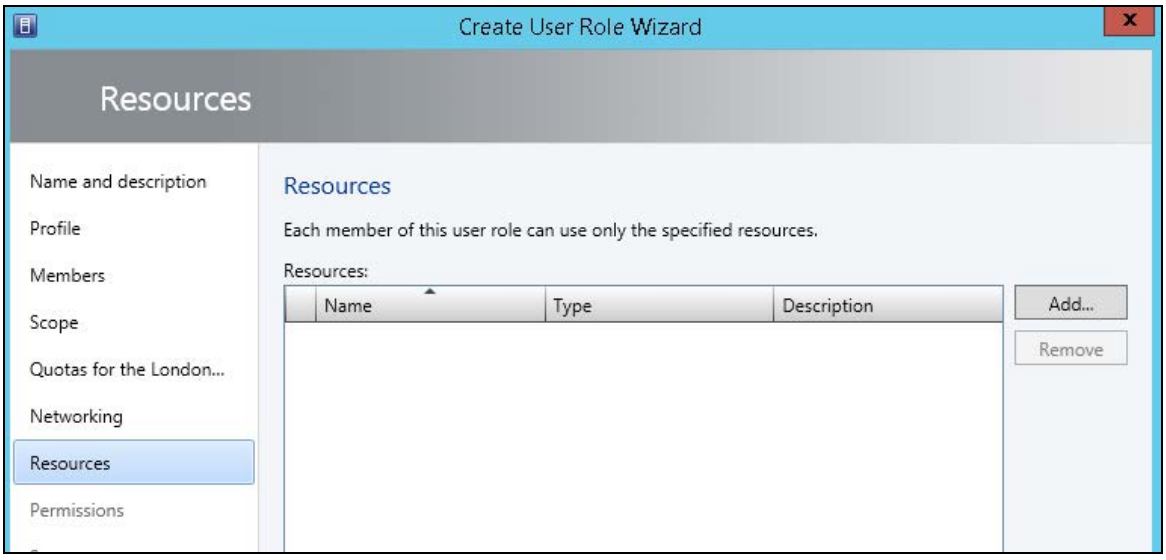

8. Cửa sổ **Networking**, chọn **Add.**



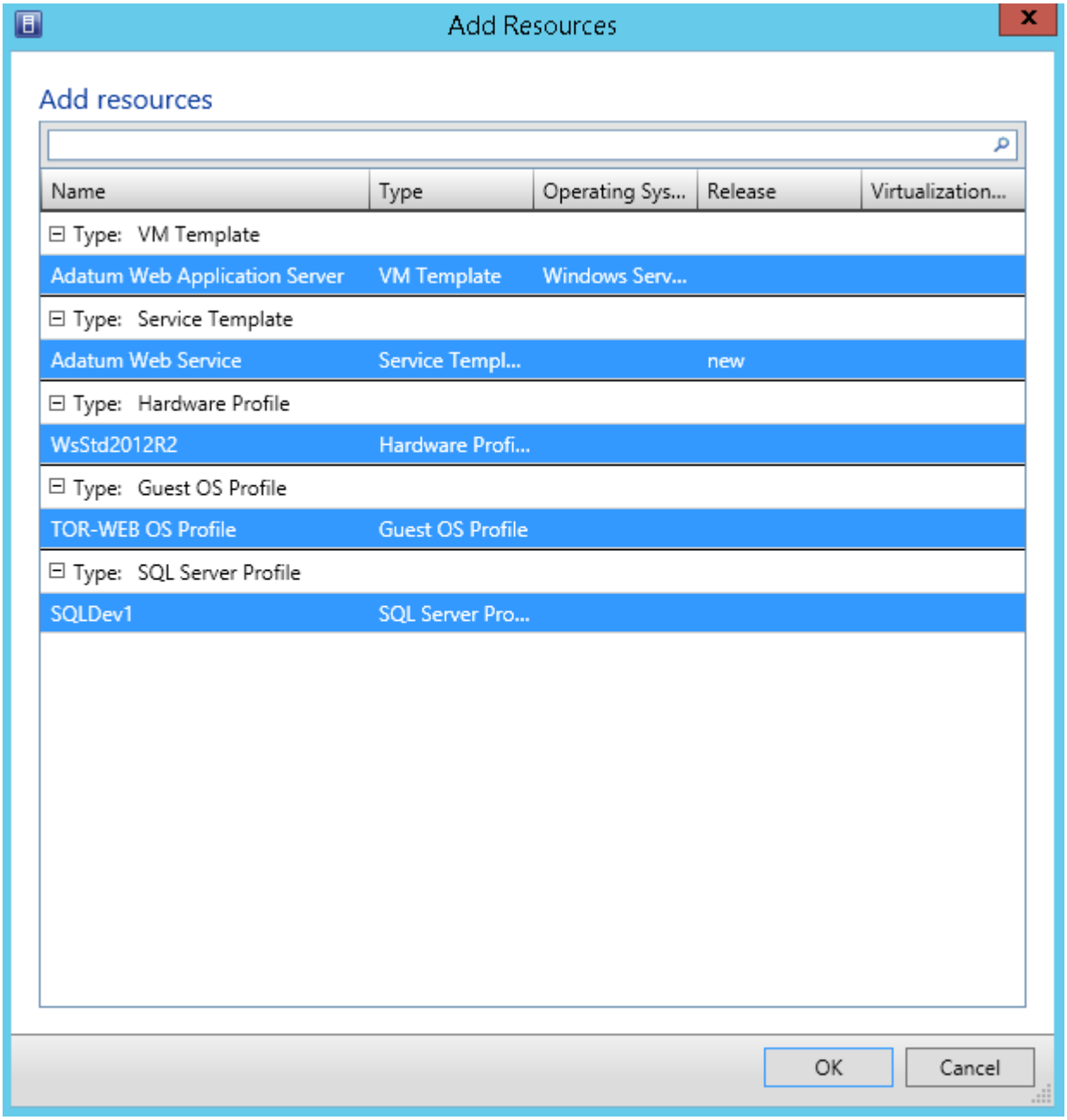
9. Hộp thoại **Select VM Networks**, chọn **External Network**, chọn **OK**, và chọn **Next**.



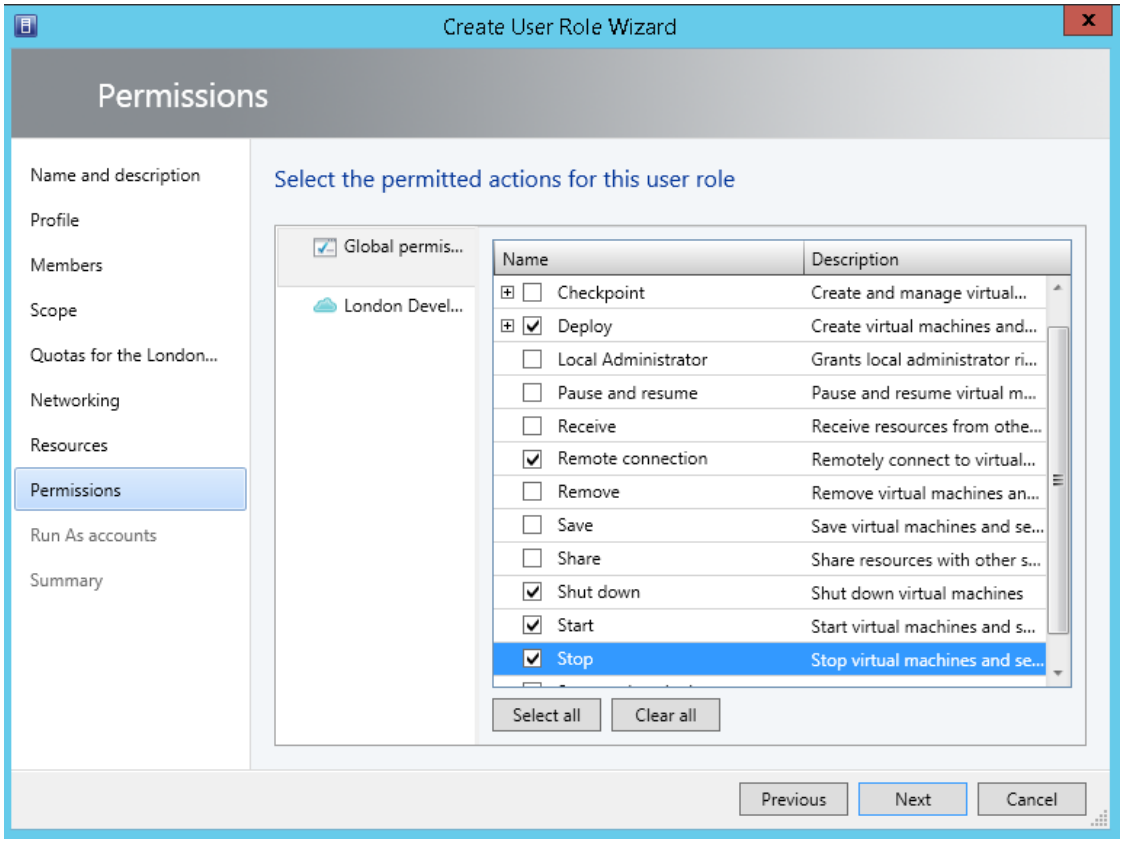

10. Cửa sổ **Resources**, chọn **Add**.



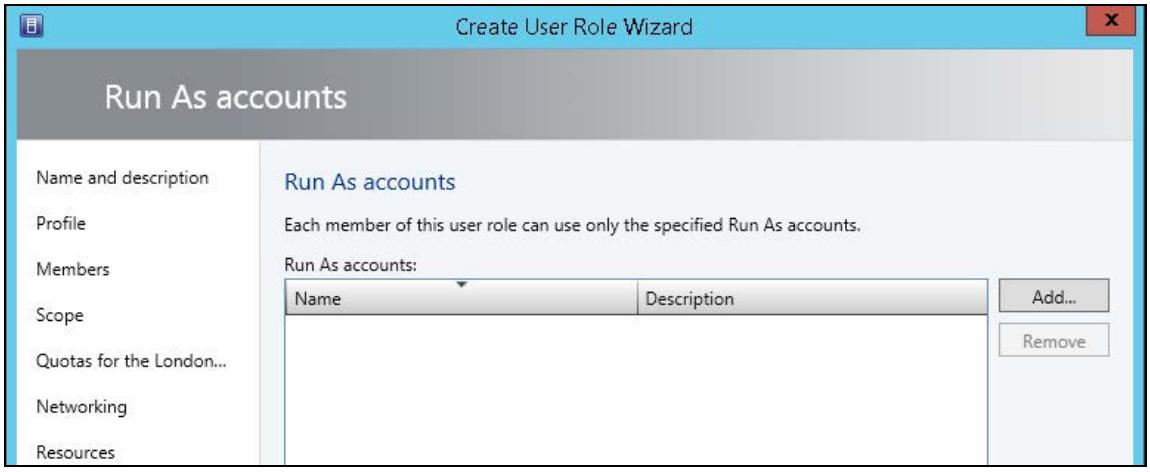
11. Hộp thoại **Add Resources**, giữ phím **Ctrl**, chọn tất cả Template va Profile, chọn **OK**, và chọn **Next**.



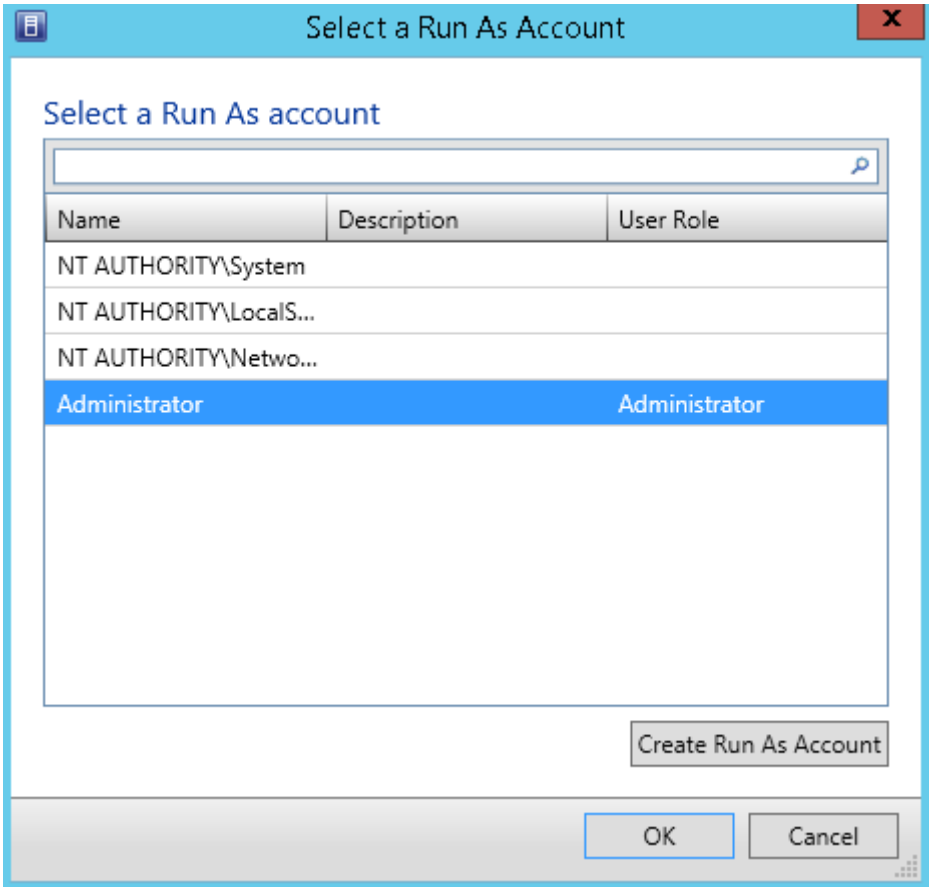
12. Cửa sổ **Permissions**, đánh dấu chọn các ô **Deploy, Remote connection, Shut down, Start, Stop**, và chọn click **Next**.




13. Cửa sổ **Run As accounts**, chọn **Add**.



14. Hộp thoại **Select a Run As accounts,** chọn **Administrator**, chọn **OK**, chọn **Next**, và chọn **Finish.**

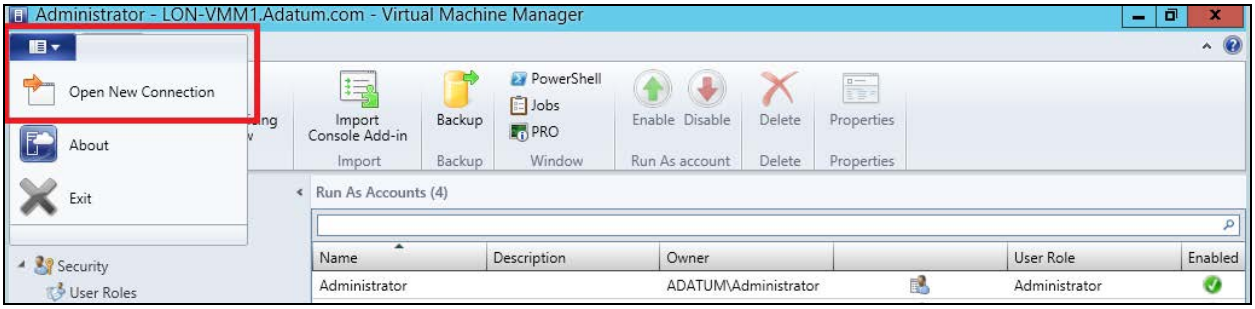



15. Nếu nhận được cảnh báo "**Unable to perform the job because one or more of the selected objects are locked by another job…**" chọn **OK** để bỏ qua cảnh báo.

16. Kiểm tra và tắt cửa sổ **Jobs**.

### Bước 3: Kiểm tra cấu hình bằng VMM.

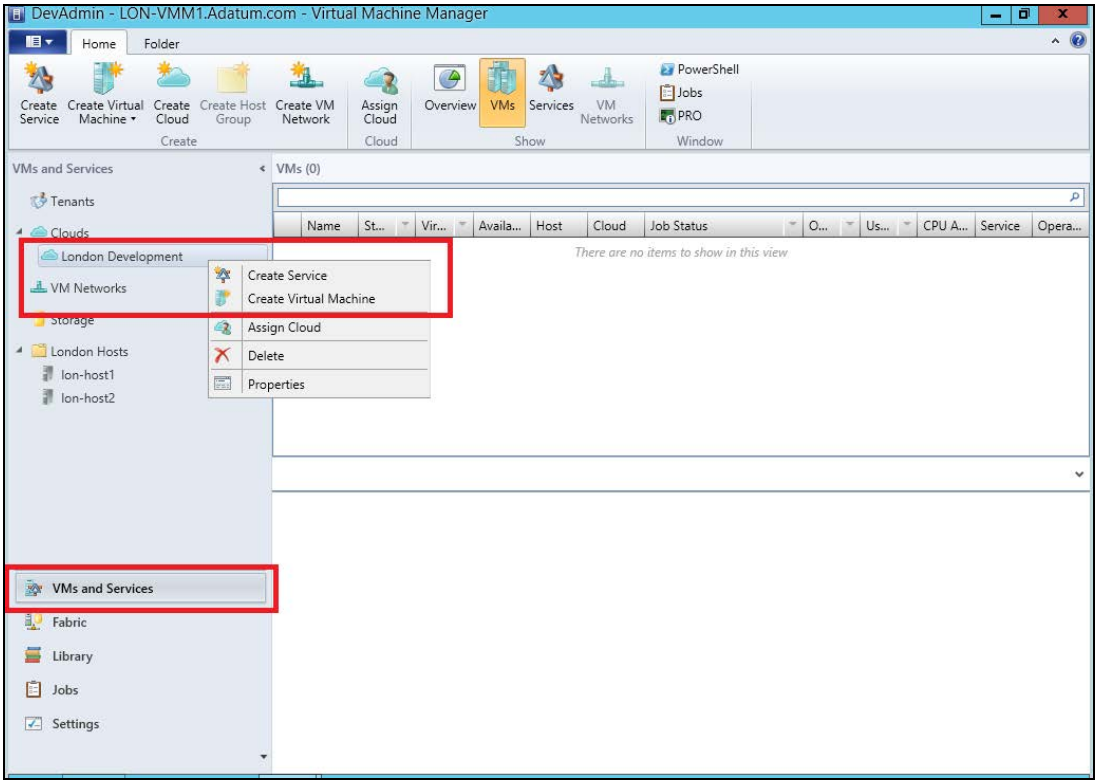
1. Trong cửa sổ **Virtual Machine Manager**, bung menu chính, chọn **Open New Connection**.



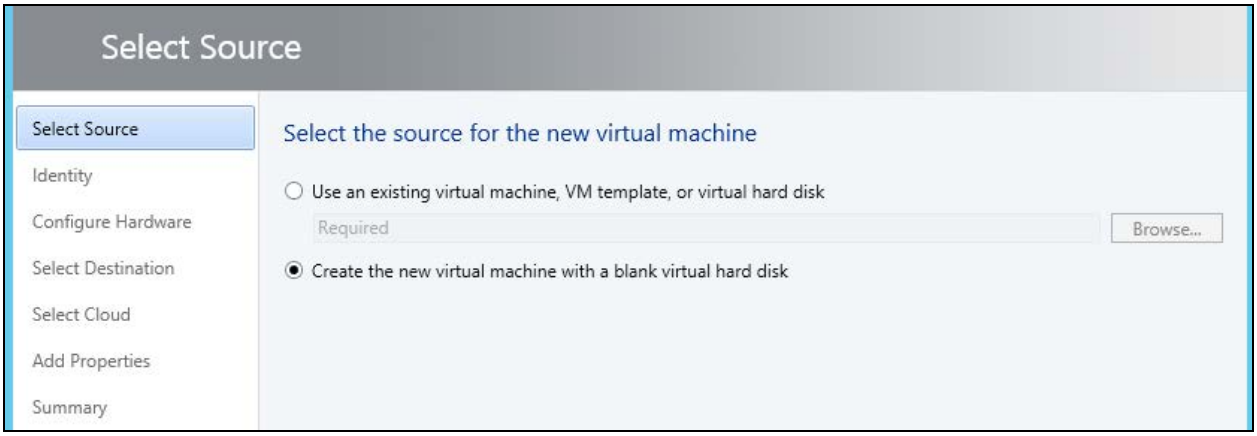

2. Cửa sổ Connect to Server, chọn **Specify credentials**, trong ô **User name**, nhập **Adatum\Rob**, trong ô **Password**, nhập **Pa$$w0rd**, chọn **Connect**



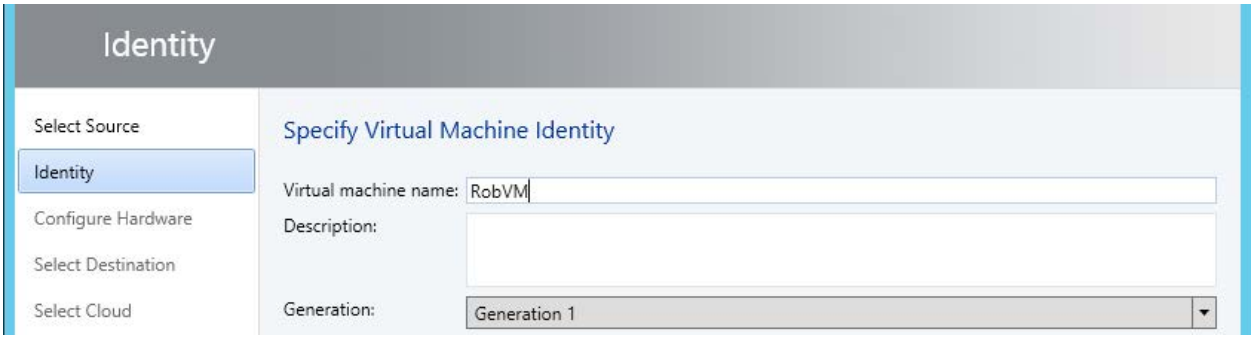
3. Trong cửa sổ **Virtual Machine Manager,** chọn **VMs and Services**, bung **Clouds**, chuột phải **London Development**, chọn **Create Virtual Machine**.



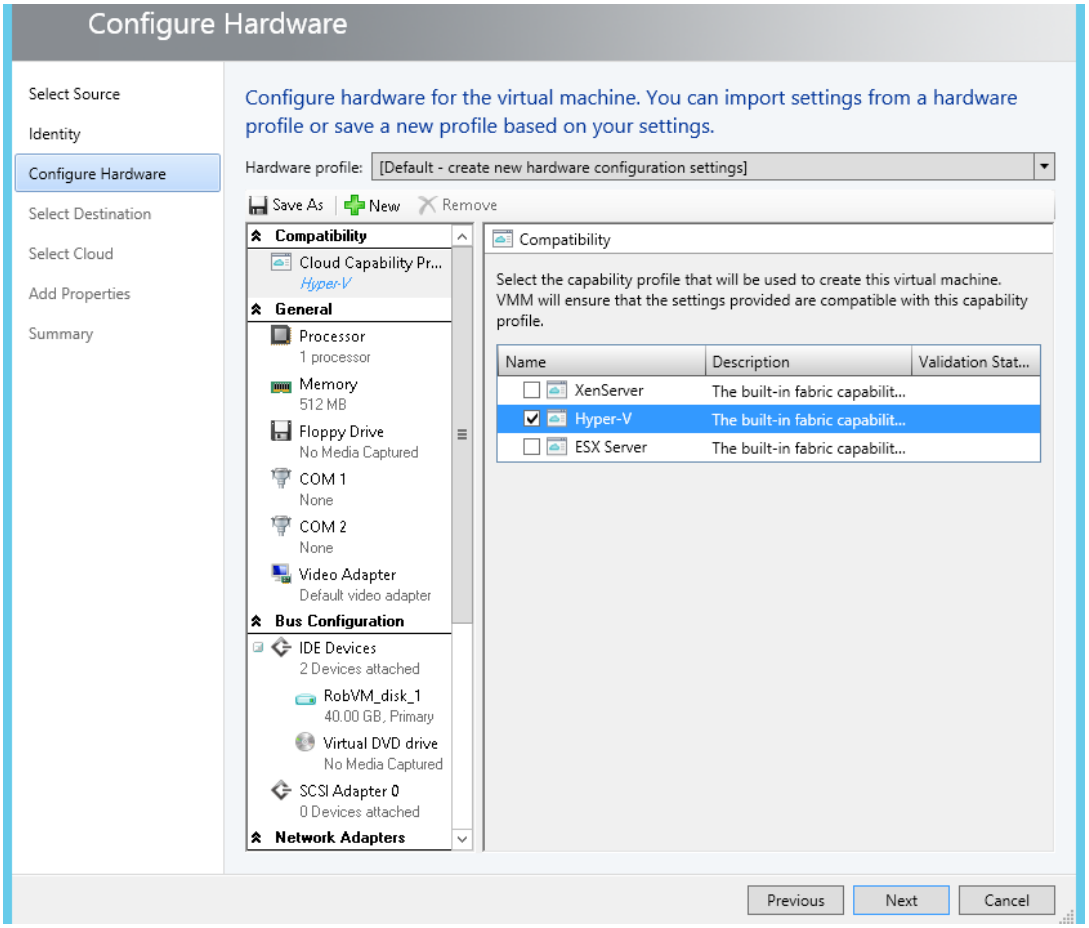

4. Cửa sổ **Select Source**, chọn **Create the new virtual machine with a blank virtual hard disk**, chọn **Next**.



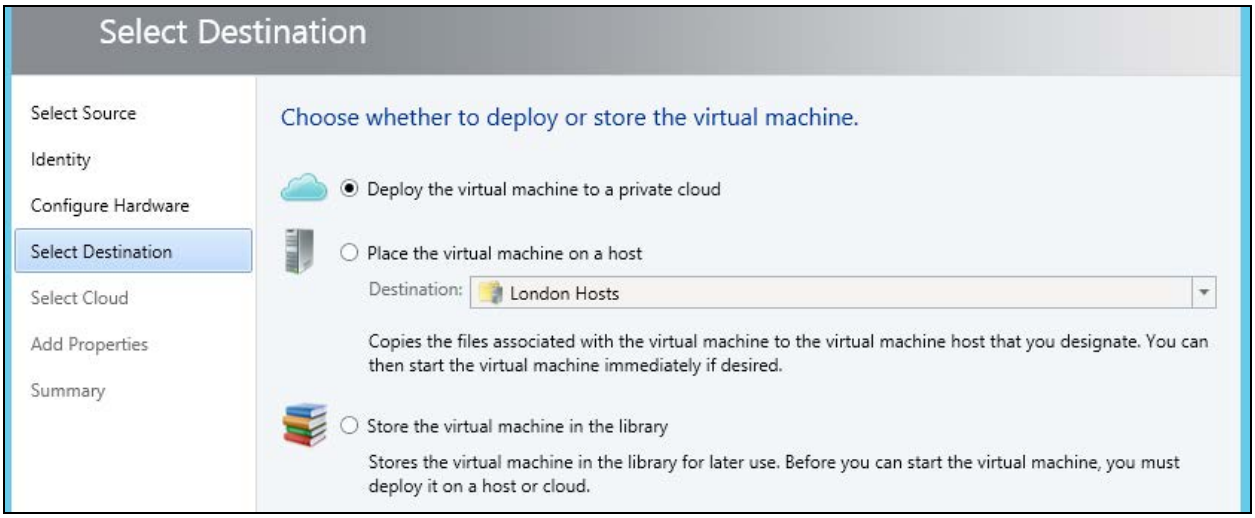
5. Cửa sổ **Specify Virtual Machine Identity**, trong ô **Virtual machine name**, nhập **RobVM**, và chọn **Next**.



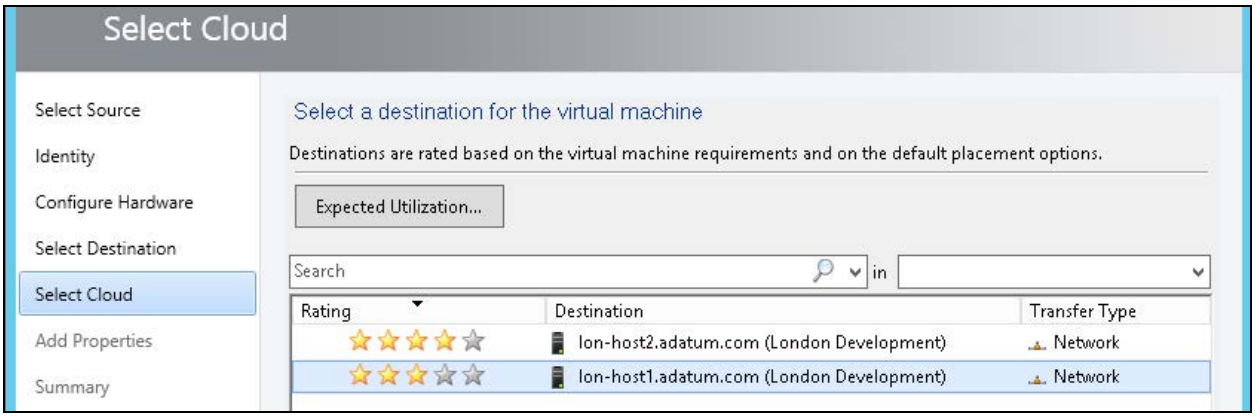

6. Cửa sổ **Configure Hardware**, trong phần **Compatibility**, chọn **Cloud Capability Profile**, đánh dấu chọn **Hyper-V**, và chọn **Next**.



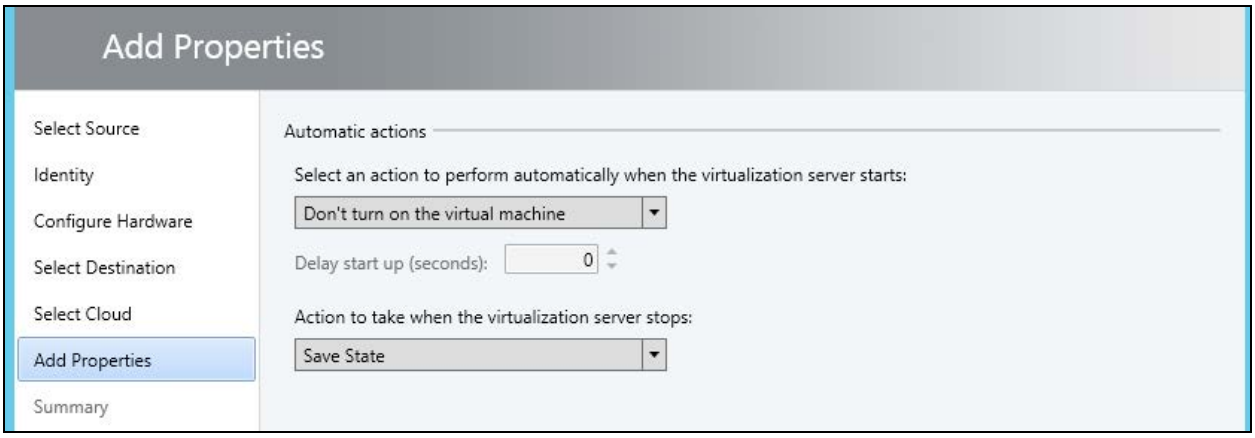
7. Cửa sổ **Select Destination**, chọn **Deploy the virtual machine to a private cloud**, và chọn **Next**.



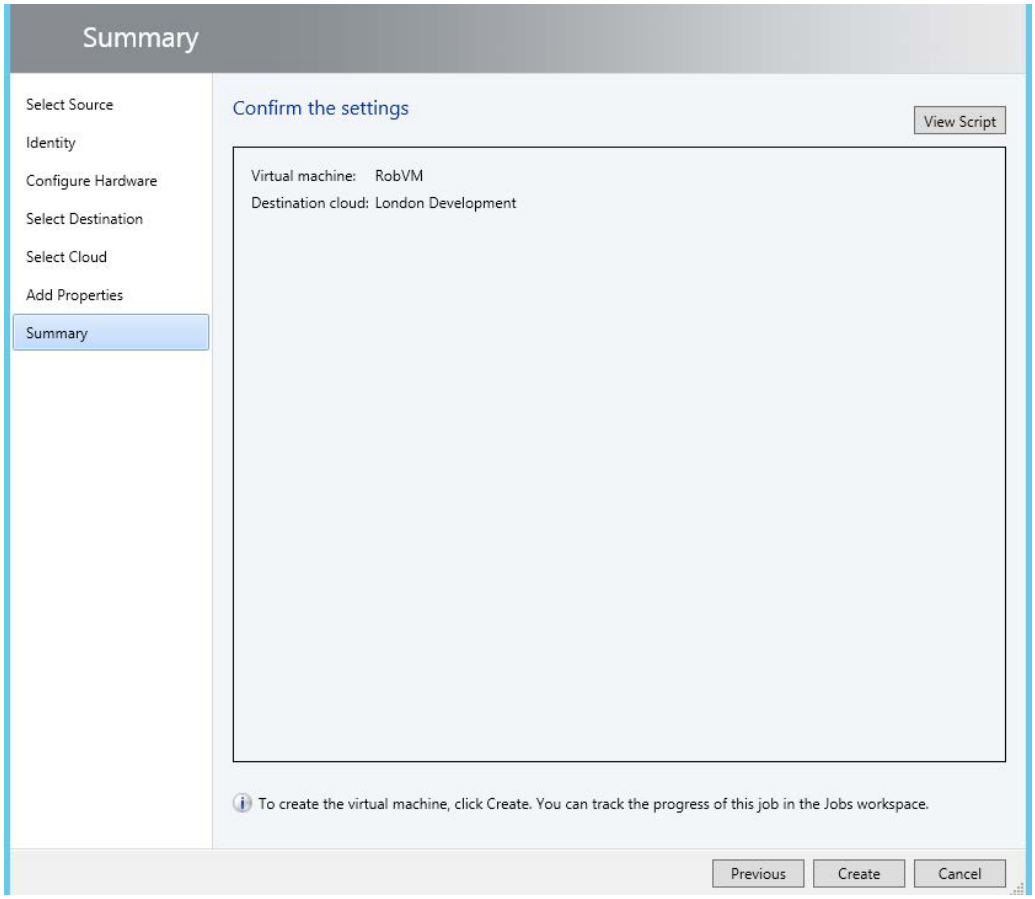

8. Cửa sổ **Select Cloud**, chọn **lon-host1.adatum.com**, và chọn **Next**.



9. Cửa sổ **Add Properties**, chọn **Next**.

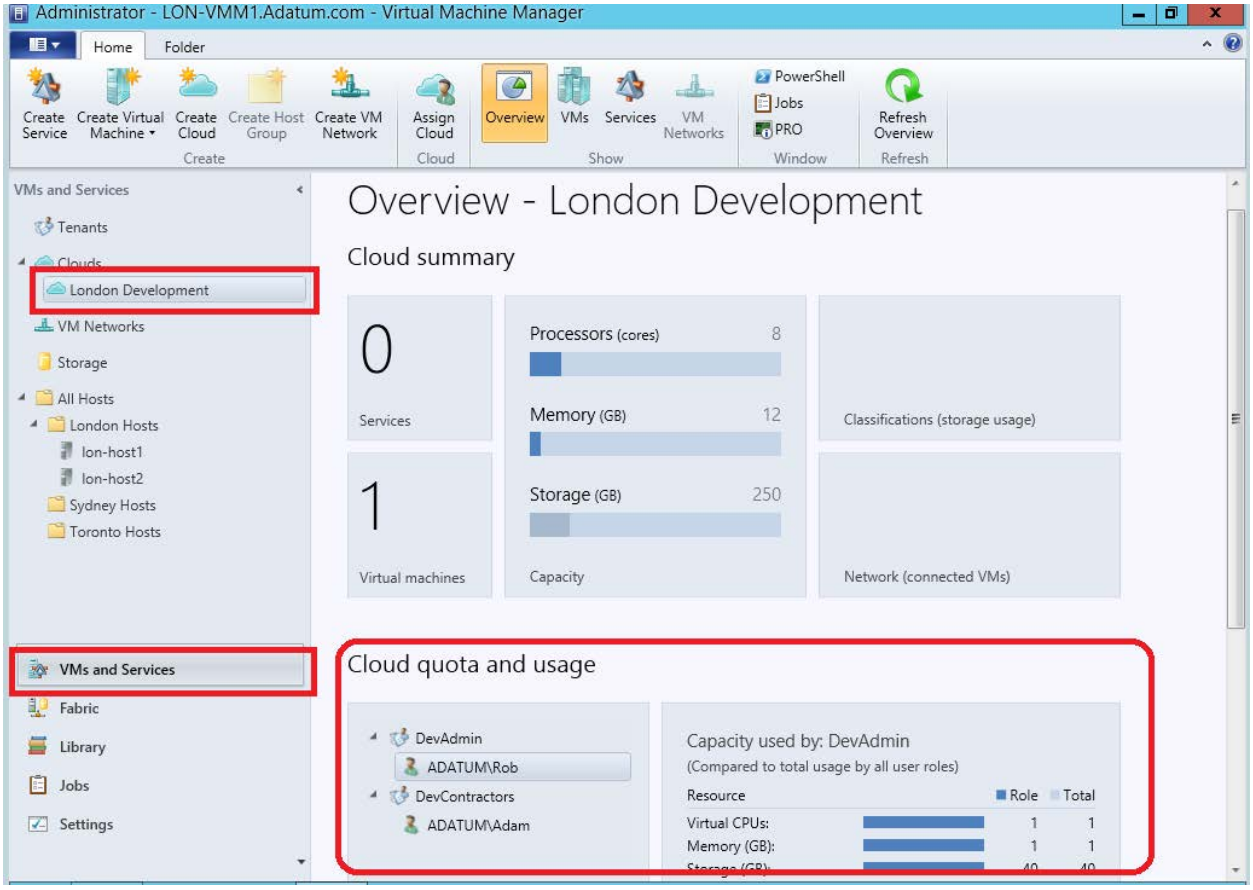



10. Cửa sổ **Summary**, chọn **Create**.



11. Kiểm tra và tắt cửa sổ **Jobs**, tắt cửa sổ **DevAdmin LON-VMM1.Adatum.com Virtual Machine Manager**.

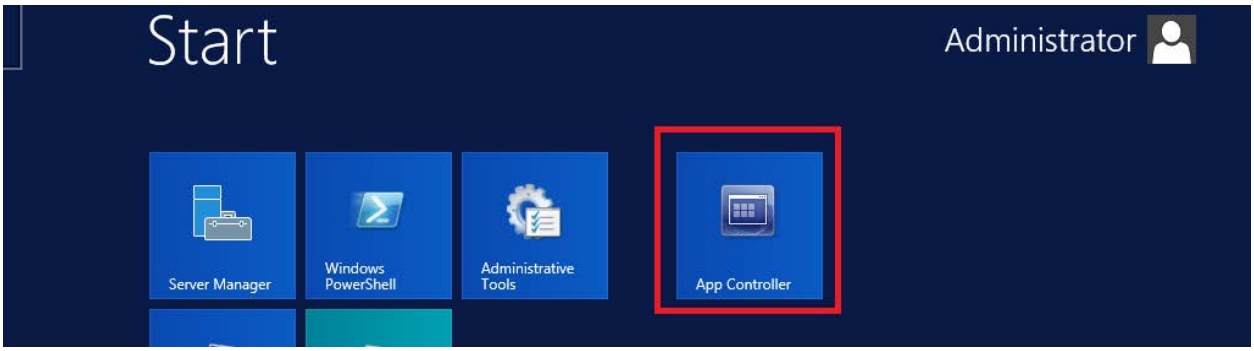
12. Trong cửa sổ **Administrator LON-VMM1.Adatum.com Virtual Machine Manager**, chọn **VMs and Services**, bung **Clouds**, chọn **London Development**, và chọn **Overview**. Kiểm tra quyền của **DevAdmin** và **DevContractors**



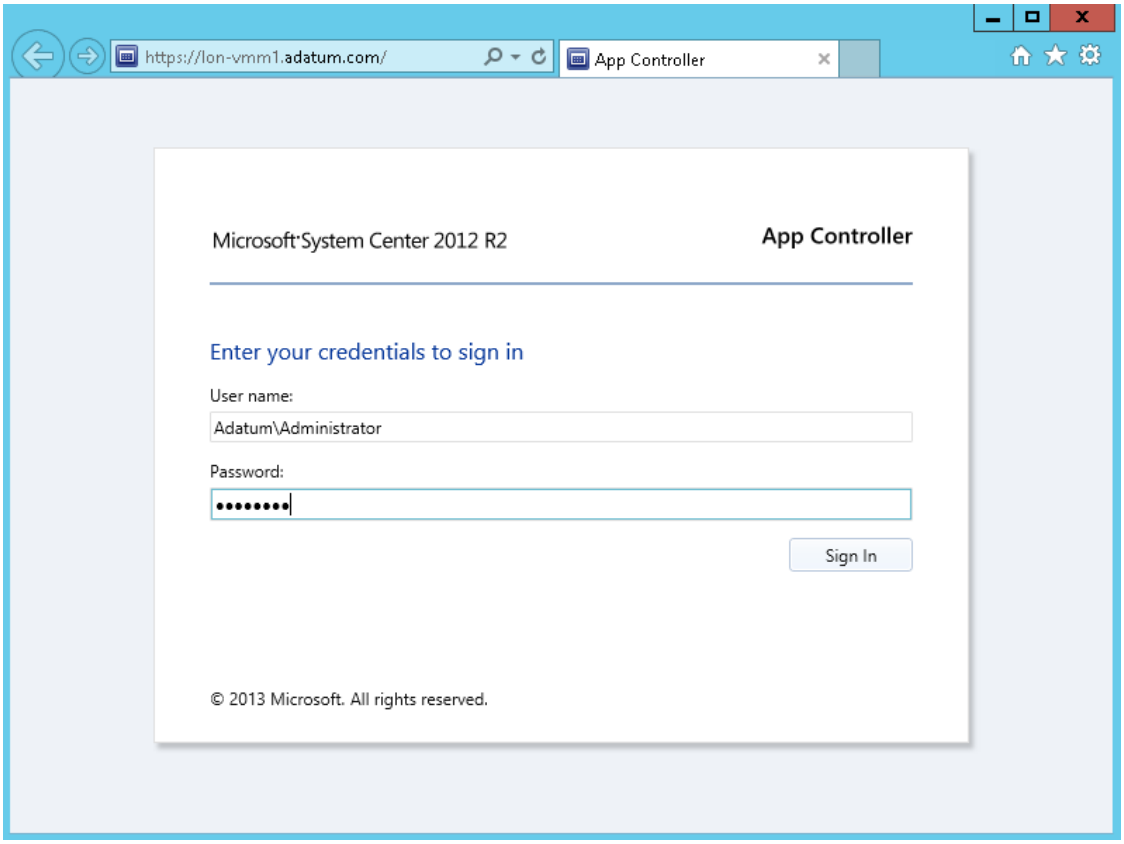
## Bước 4: Kiểm tra cấu hình bằng App Controller.

➢ **Kết nối App Controller đến VMM**

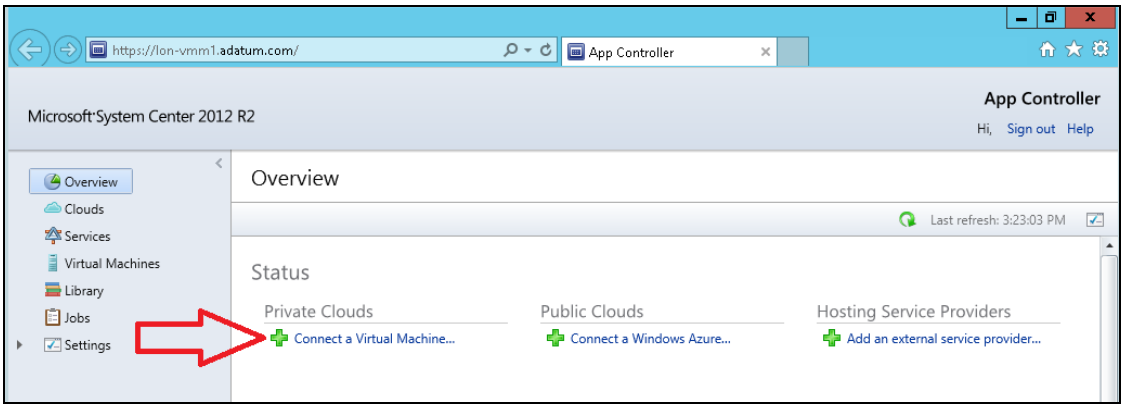
1. Trên máy **LON-VMM1**, bung **Start** menu, mở **App Controller**.



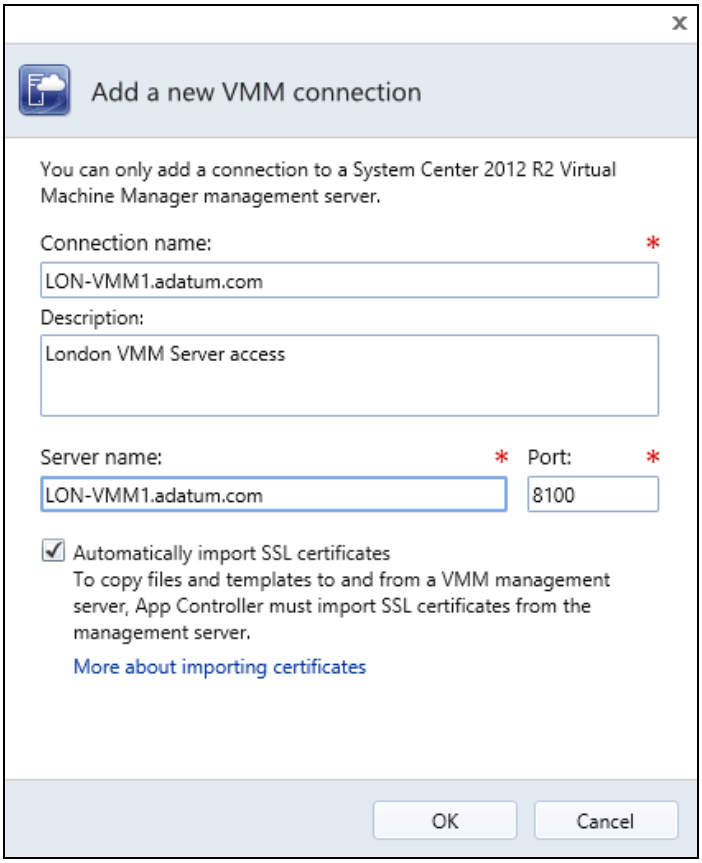

2. Trong cửa sổ **App Controller Credentials**, trong ô **User name**, nhập **Adatum\Administrator**, trong ô **Password**, nhập **Pa$$w0rd**, và chọn **Sign In**.



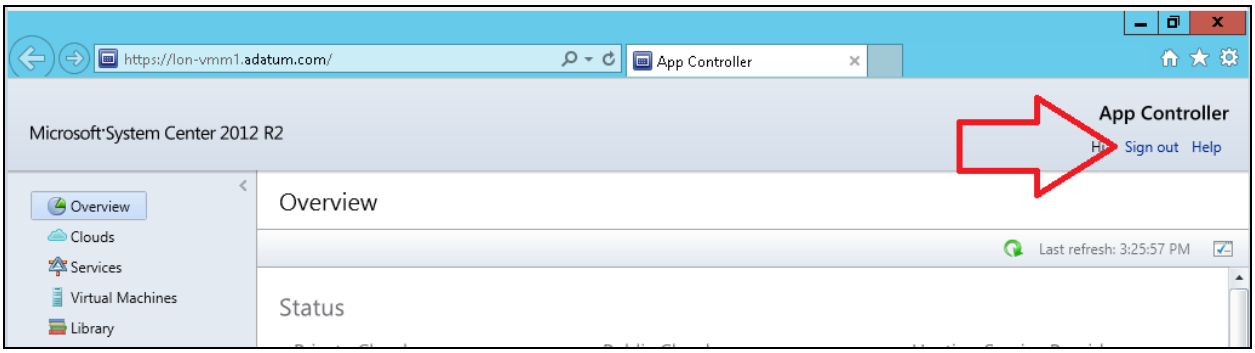
3. Cửa sổ **Overview**, chọn **Connect a Virtual Machine Manager server and clouds**.




4. Cửa sổ **Add a new VMM connection**, trong ô **Connection name**, nhập **LON-VMM1.adatum.com**, trong ô **Description**, nhập **London VMM Server access**, trong ô **Server name**, nhập **LON-VMM1.adatum.com**, và chọn **OK**.

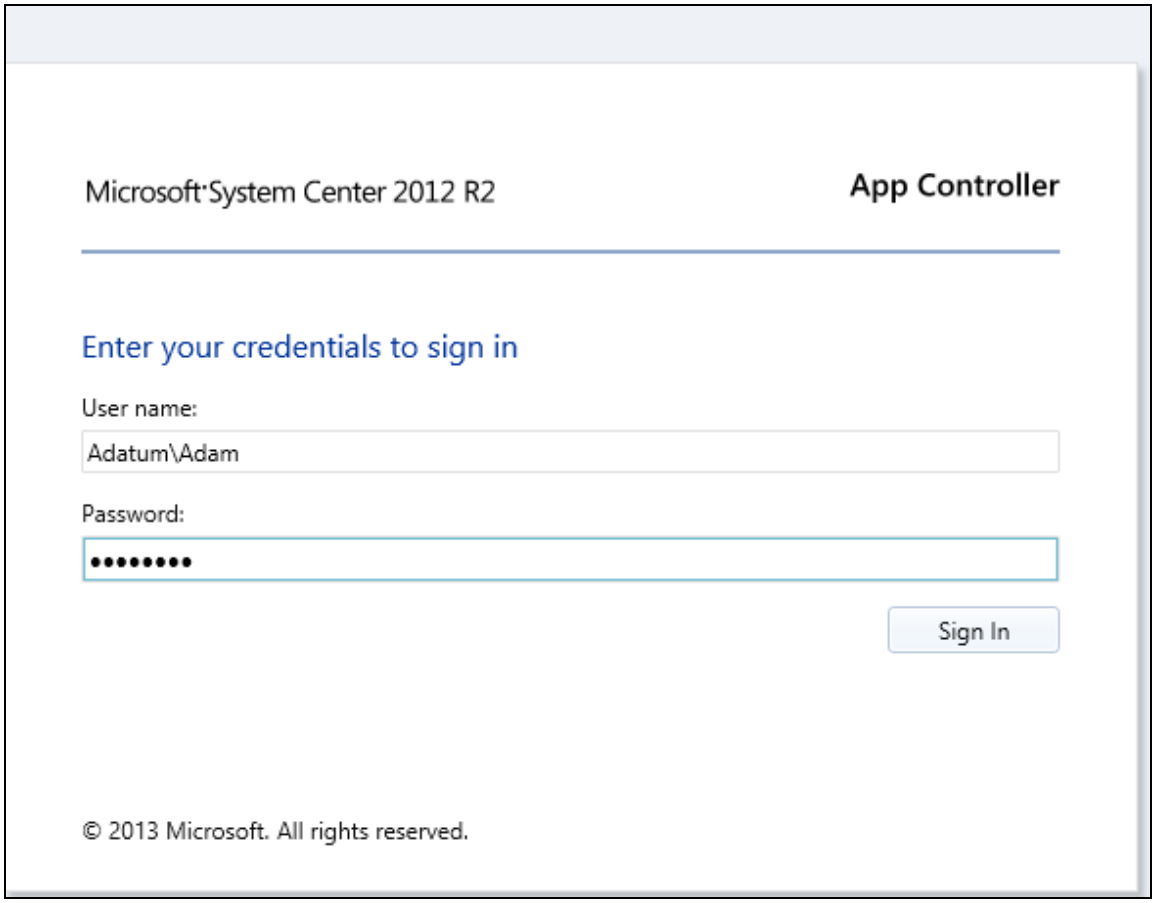


5. Cửa sổ **Overview**, chọn **Sign Out**.

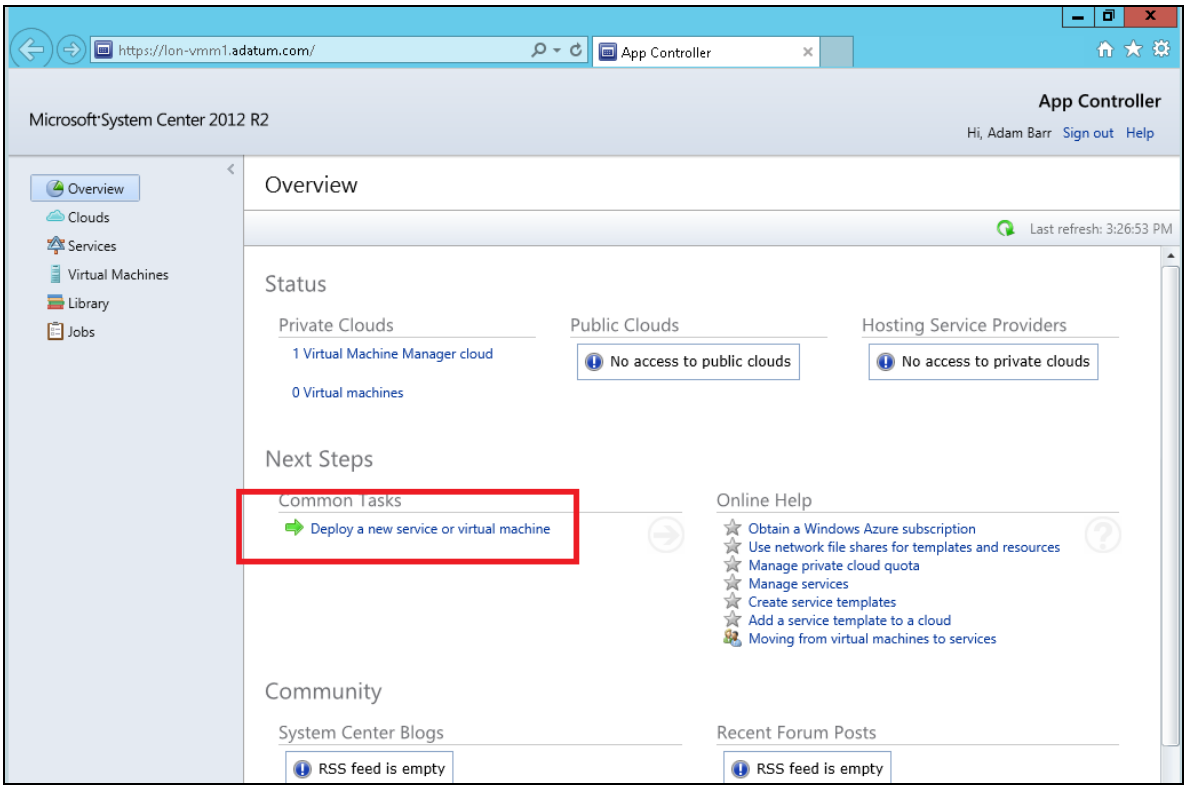



➢ **Kiểm tra Self-service trong App Controller**

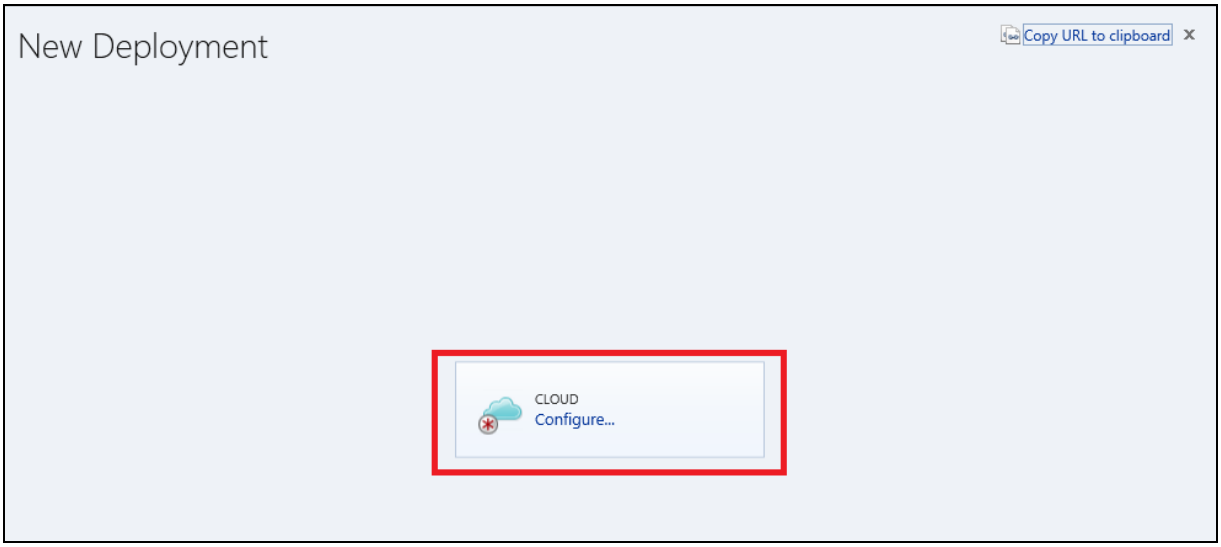
1. Trong cửa sổ **App Controller Credentials**, trong ô **User name**, nhập **Adatum\Adam**, trong ô **Password**, nhập **Pa$$w0rd**, chọn **Sign In**.



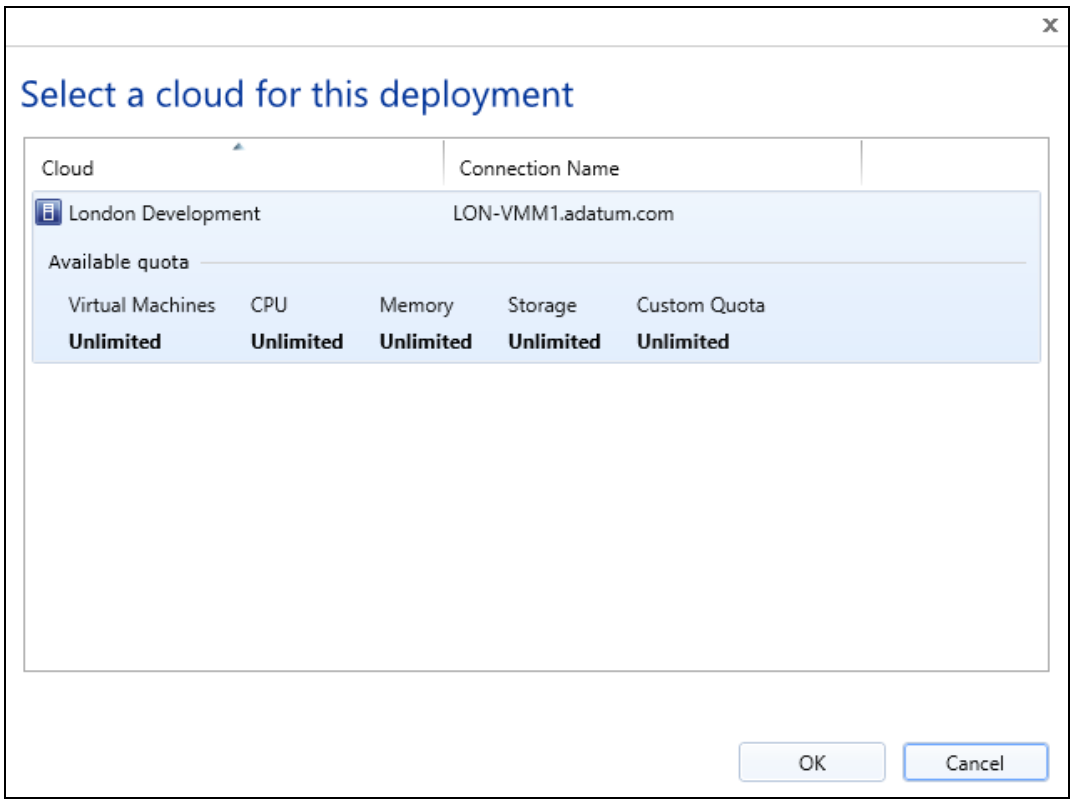
2. Cửa sổ **Overview**, chọn **Deploy a new service or virtual machine**.




3. Cửa sổ **New Deployment**, chọn **Configure**.



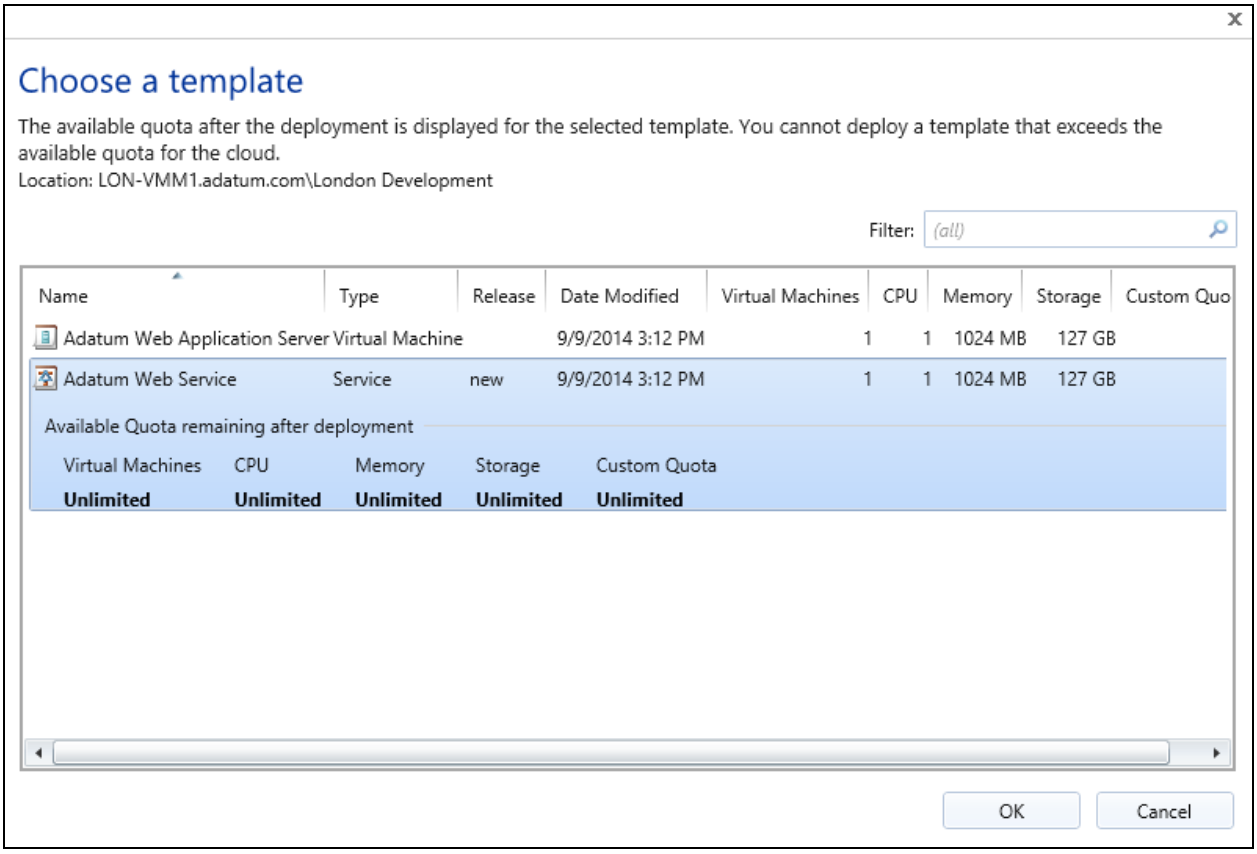
4. Cửa sổ **Select a cloud for this deployment**, chọn **OK.**



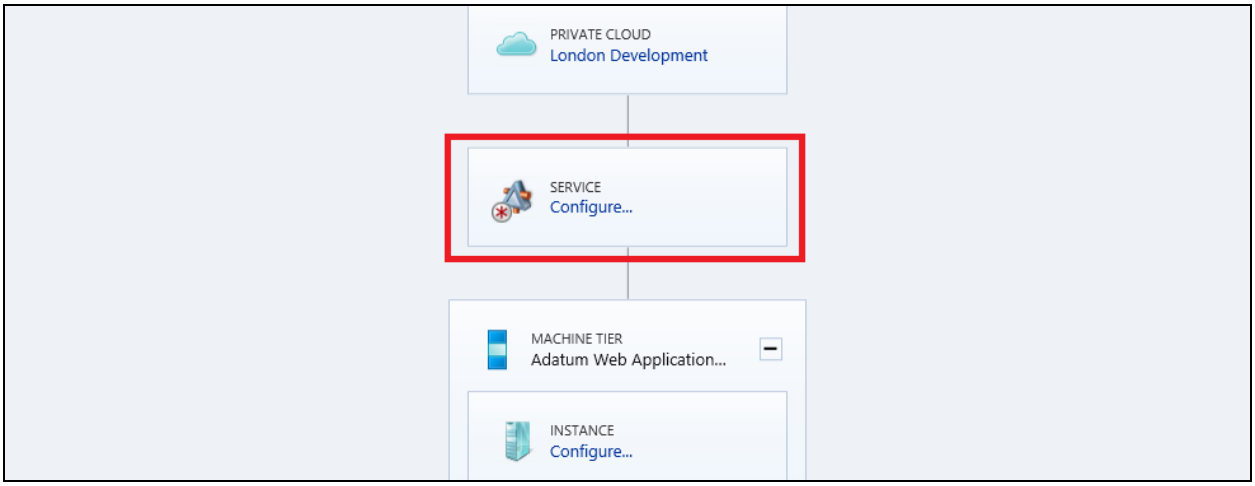

5. Trong mục **Template**, chọn **Select a template**.



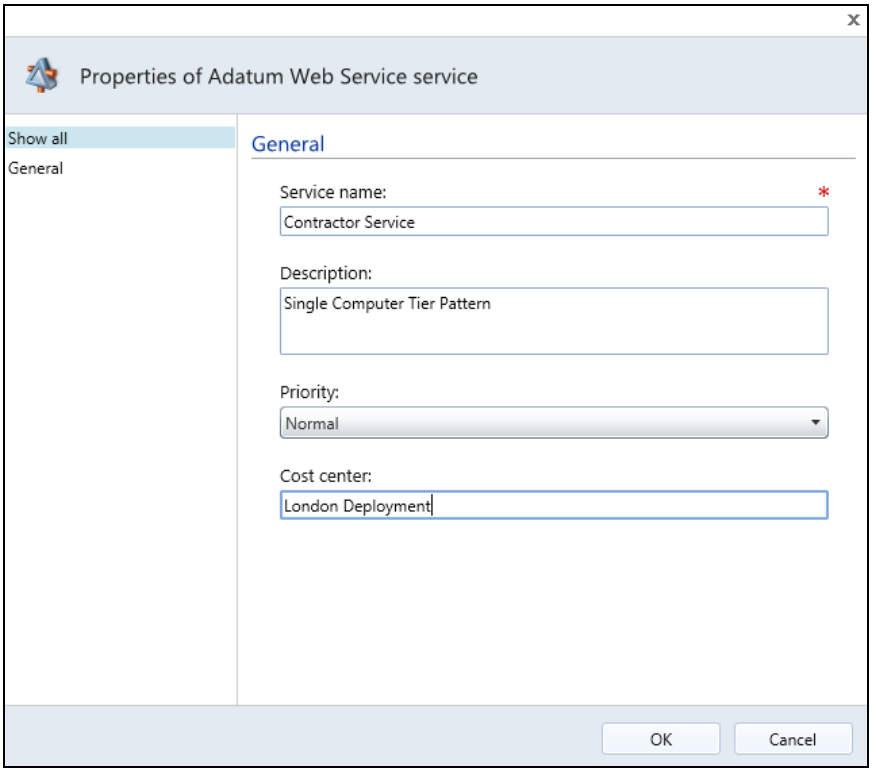
6. Cửa sổ **Choose a template**, chọn **Adatum Web Service**, và chọn **OK**.



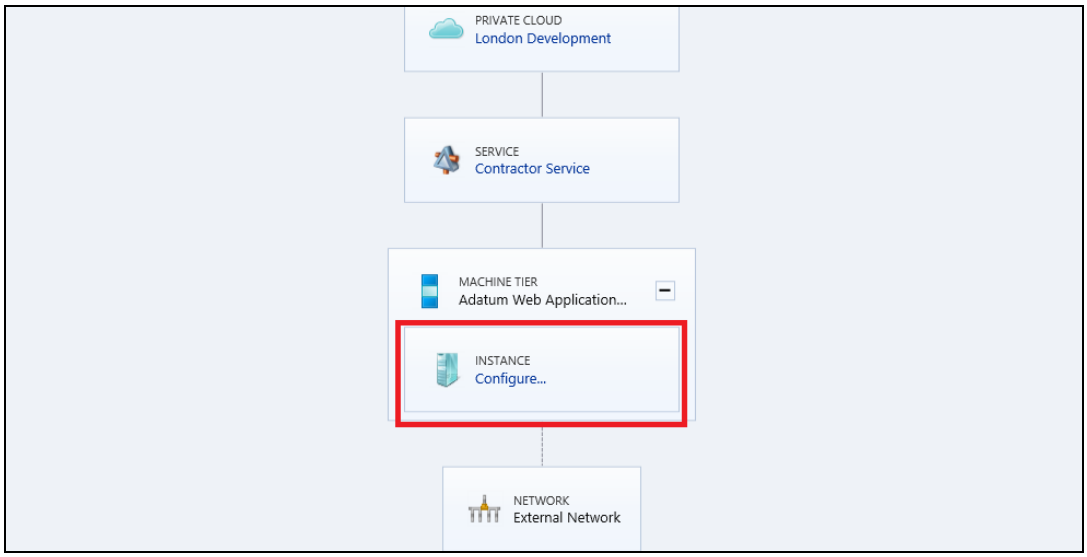

7. Trong mục **SERVICE**, chọn **Configure.**



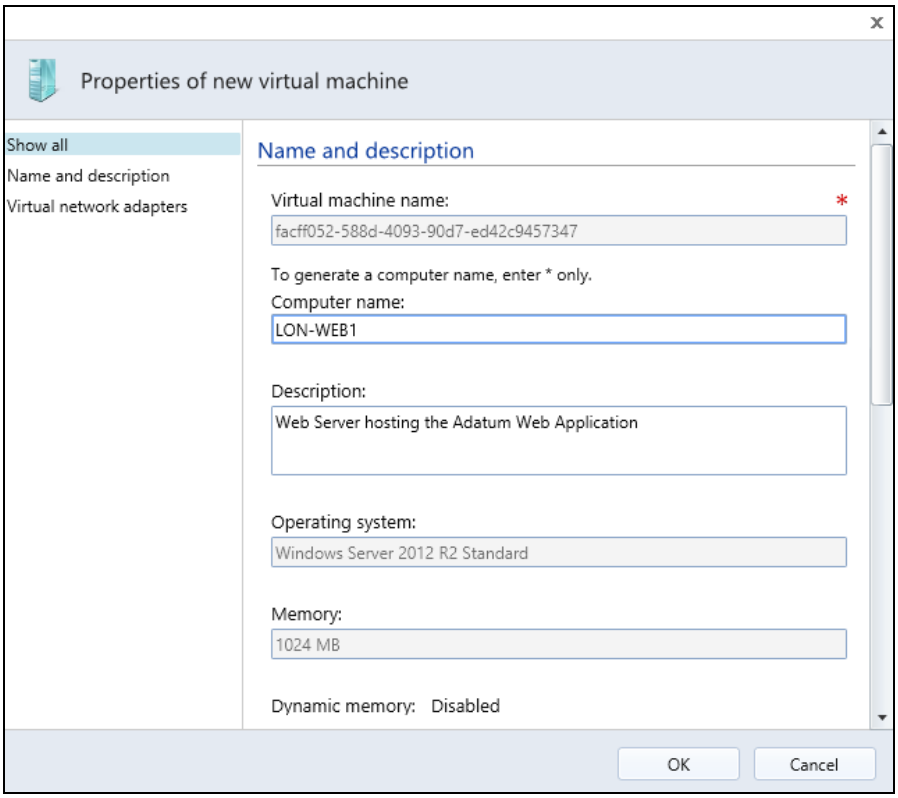
8. Cửa sổ **Properties of Adatum Web Service**, trong ô **Service Name**, nhập **Contractor Service**, trong ô **Cost center**, nhập **London Development**, và chọn **OK**.



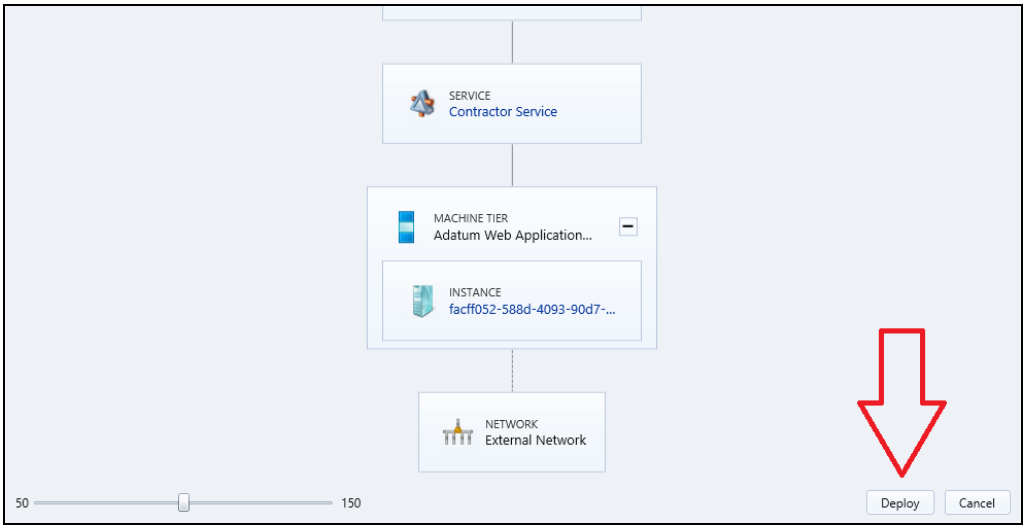

9. Trong mục **INSTANCE**, chọn **Configure**.



10. Cửa sổ **Properties of new virtual machine,** trong ô **Computer Name**, nhập **LON-WEB1**, chọn **OK.**

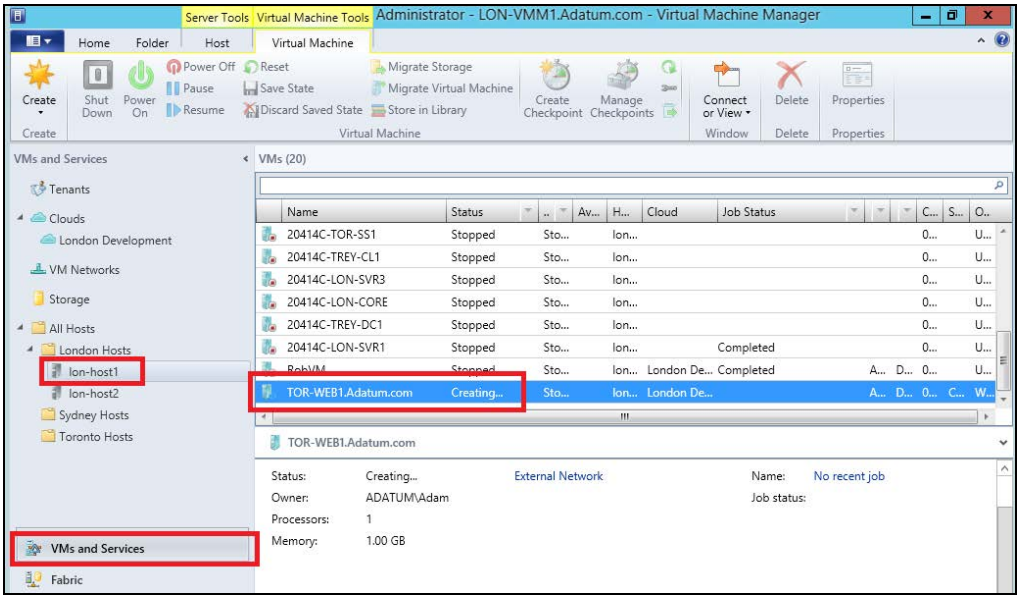



11. Cửa sổ **New Deployment**, chọn **Deploy** để tạo một máy ảo mới.

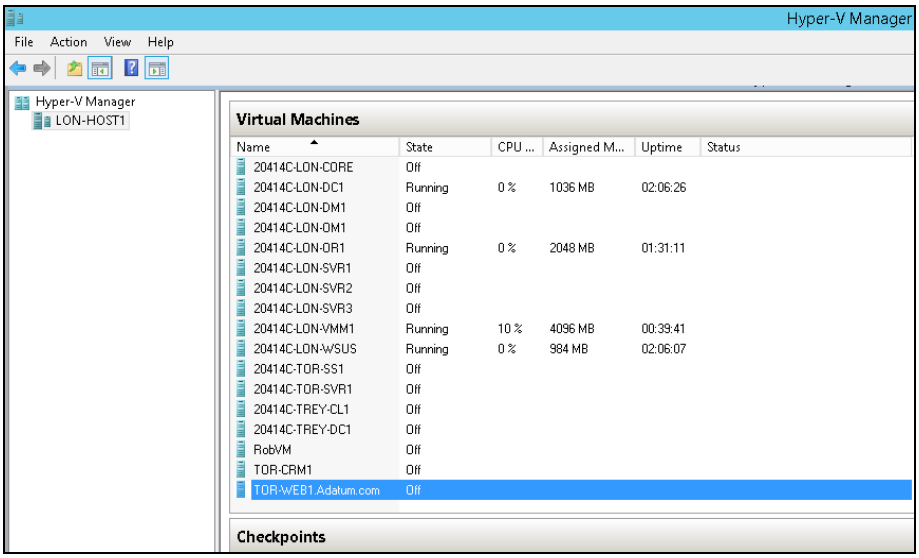


12. Tắt cửa sổ **App Controller**.

13. Trong cửa sổ **VMM**, chọn **VM and Services,** bung **All Hosts**, bung **London Hosts**, chọn **lon-host1,** kiểm tra có máy ảo **TOR-WEB1.Adatum.com** đang được khởi tạo.




14. Sau khoảng 15-20 phút, mở cửa sổ Hyper-V Manager, kiểm tra máy ảo **TOR-WEB1.Adatum.com** được cài đặt thành công (*Chú ý: Trong thời gian chờ đợi, bạn có thể thực hiện bài tập tiếp theo*)



## Bài tập 3: Triển khai chức năng Host Updating trong VMM.

A. Datum đã triển khai VMM để quản lý các Hyper-V Hosts trong trung tâm dữ liệu của mình ở London. Nhóm quản trị của A. Datum đang có kế hoạch sử dụng VMM để quản lý các bản cập nhật mà họ sẽ cài đặt cho các Hyper-V Hosts. Bởi vì Hyper-V Hosts sẽ kiểm soát một số tài nguyên quan trọng trong các máy ảo, nên điều quan trọng là phải cập nhật được các phiên bản sửa lỗi bảo mật và nâng cấp chức năng mới nhất.

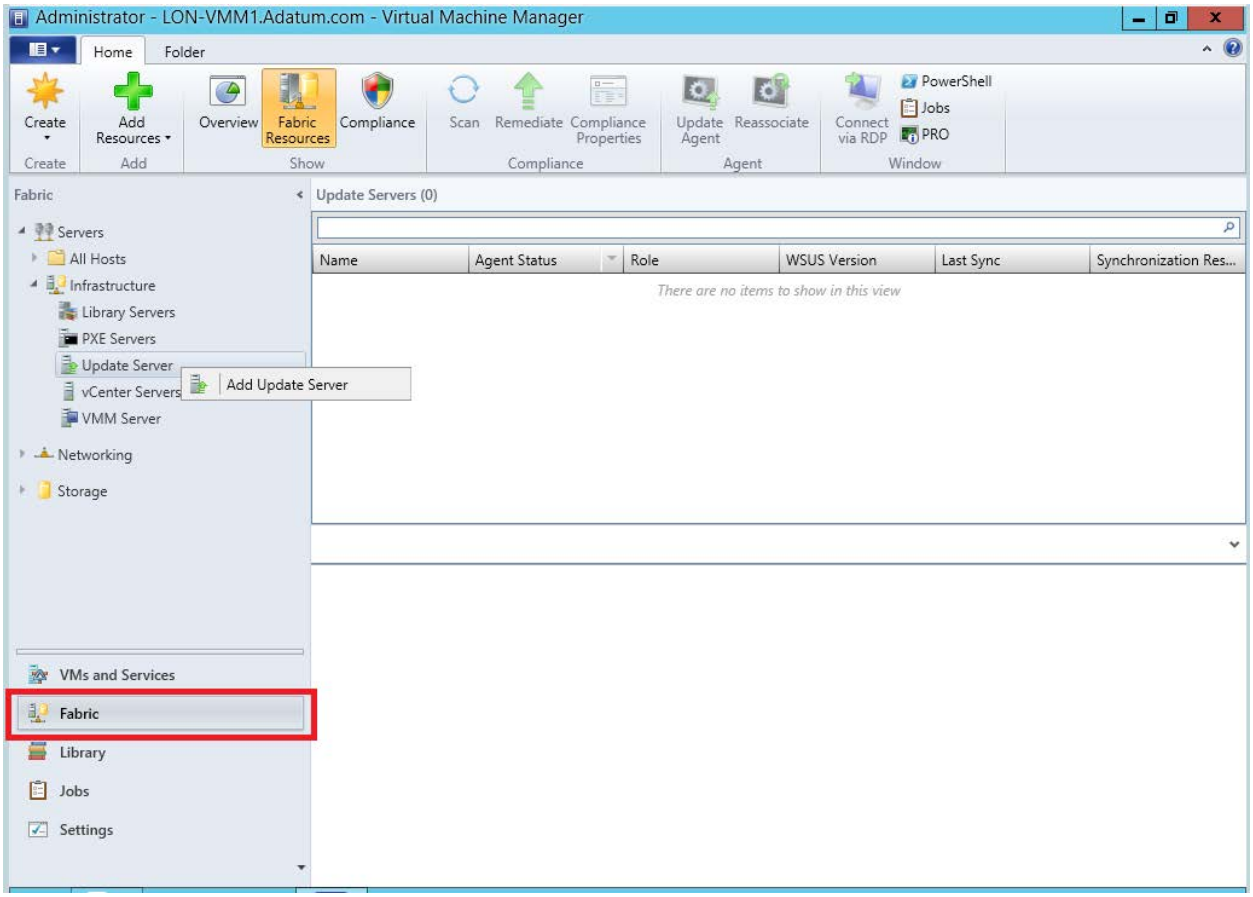
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình cho VMM tích hợp với WSUS.
2. Cấu hình Software Update Baseline trong VMM.
3. Kiểm tra kết quả.

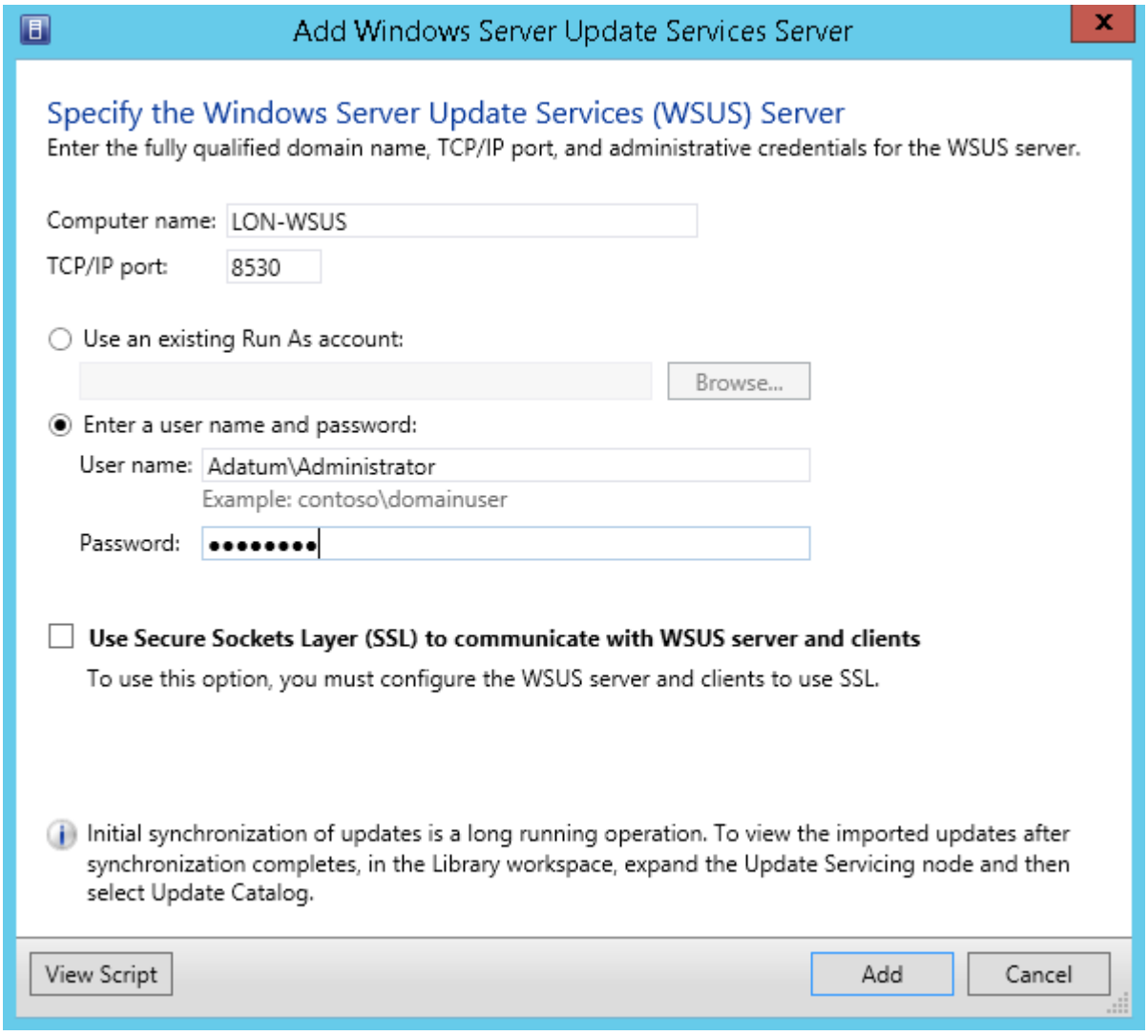
❖ **Thực hiện:**

**Bước 1: Cấu hình cho VMM tích hợp với WSUS.**

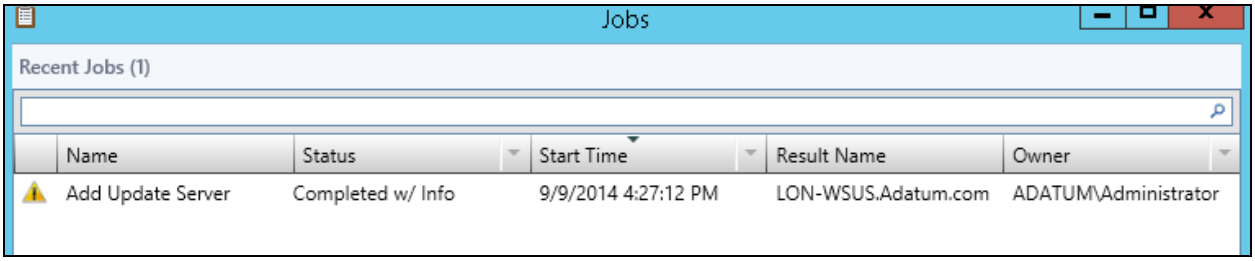
1. Trên máy **LON-VMM1**, trong cửa sổ **Virtual Machine Manager**, chọn **Fabric**, bung **Servers**, bung **Infrastructure**, chuột phải **Update Server**, chọn **Add Update Server**.



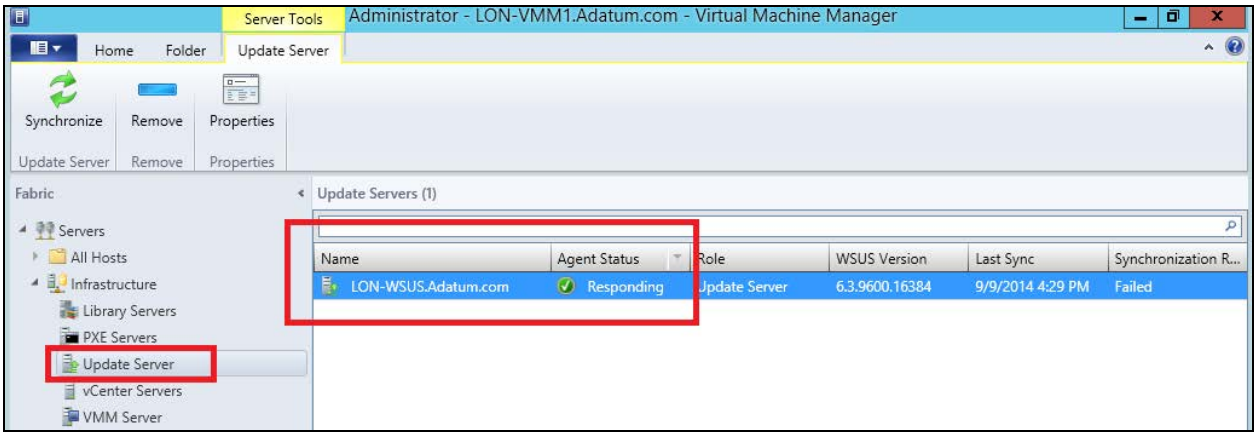
2. Hộp thoại **Add Windows Server Update Services Server**, trong ô **Computer name**, nhập **LON-WSUS**, trong ô **TCP/IP port**, nhập **8530**. Chọn **Enter a user name and password**, trong ô **User name**, nhập **Adatum\Administrator**, trong ô **Password**, nhập **Pa$$w0rd**, và chọn **Add**.



3. Kiểm tra và tắt cửa sổ **Jobs**.

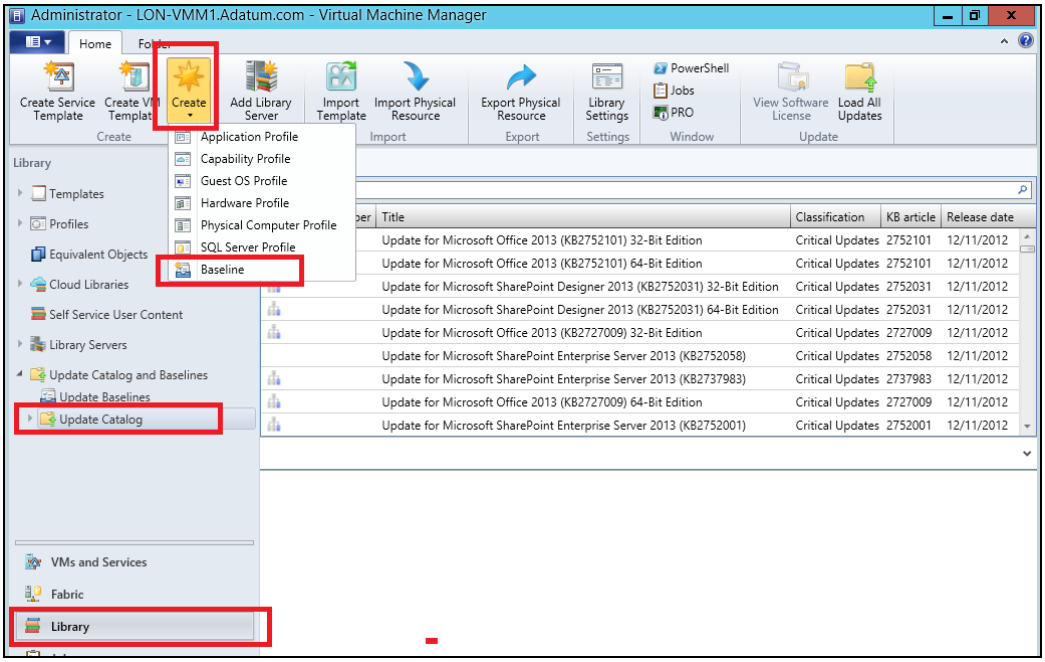



4. Trong **Update Server**, chọn **LON-WSUS.adatum.com** , kiểm tra **Agent Status** là **Responding**.

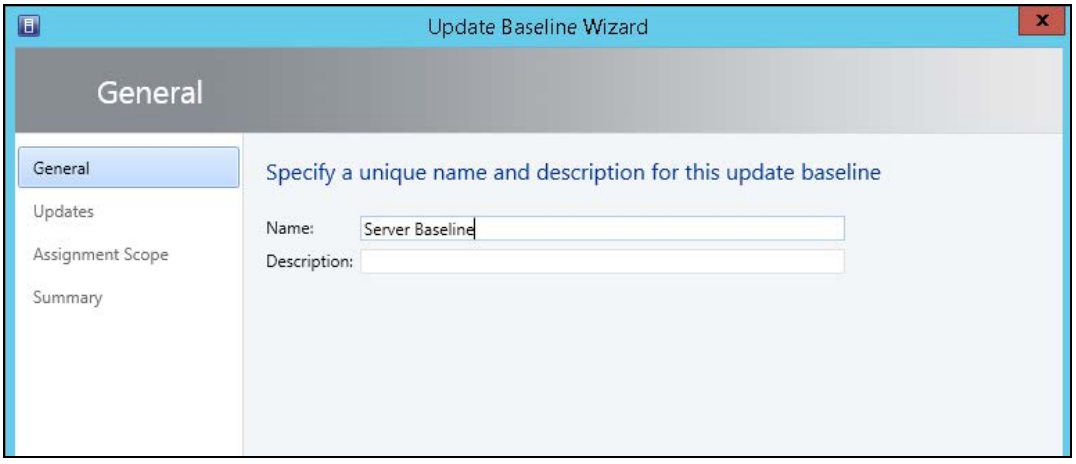


## Bước 2: Cấu hình Software Update Baseline trong VMM.

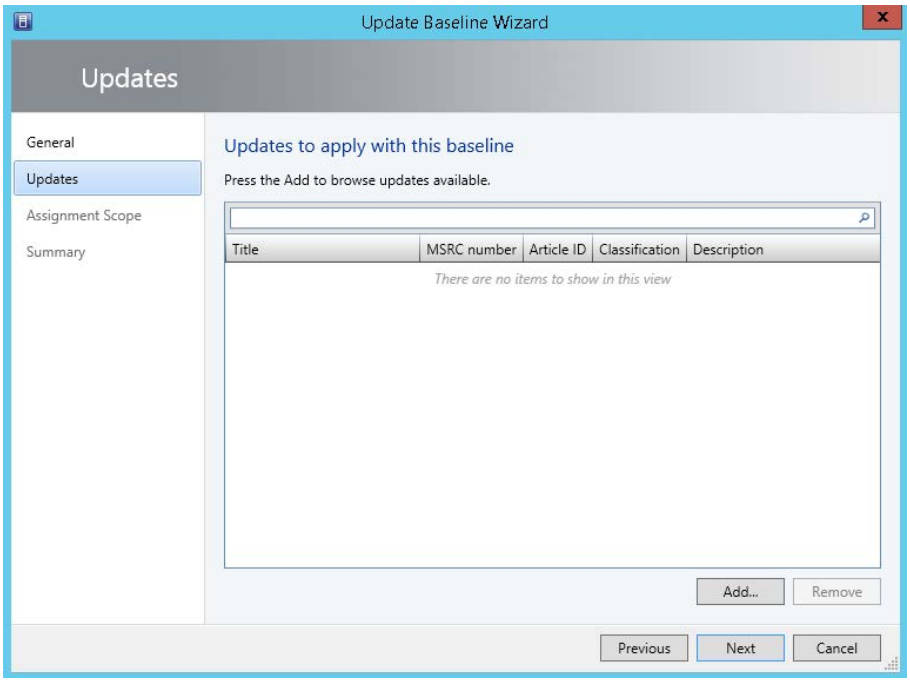
1. Trên máy **LON-VMM1**,trong cửa sổ **Virtual Machine Manager**, chọn **Library**, bung **Update Catalog and Baselines**, chọn **Update Catalog**. (***Chú ý:*** *Kiểm tra có các bản update được đồng bộ từ WSUS Server. Nếu không có, cửa sổ* ***Update Catalog****, chọn* ***Synchronize Update Server***.), bung **Create**, chọn **Baseline**.



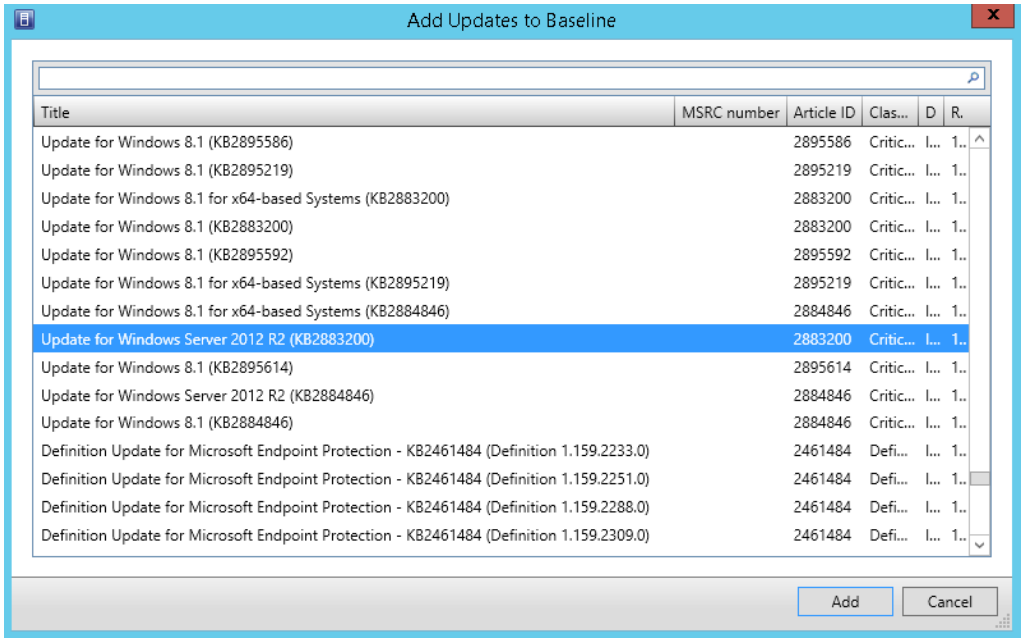

2. Cửa sổ **General**, trong ô **Name**, nhập **Server Baseline**, và chọn **Next**.



3. Cửa sổ **Updates**, chọn **Add**.

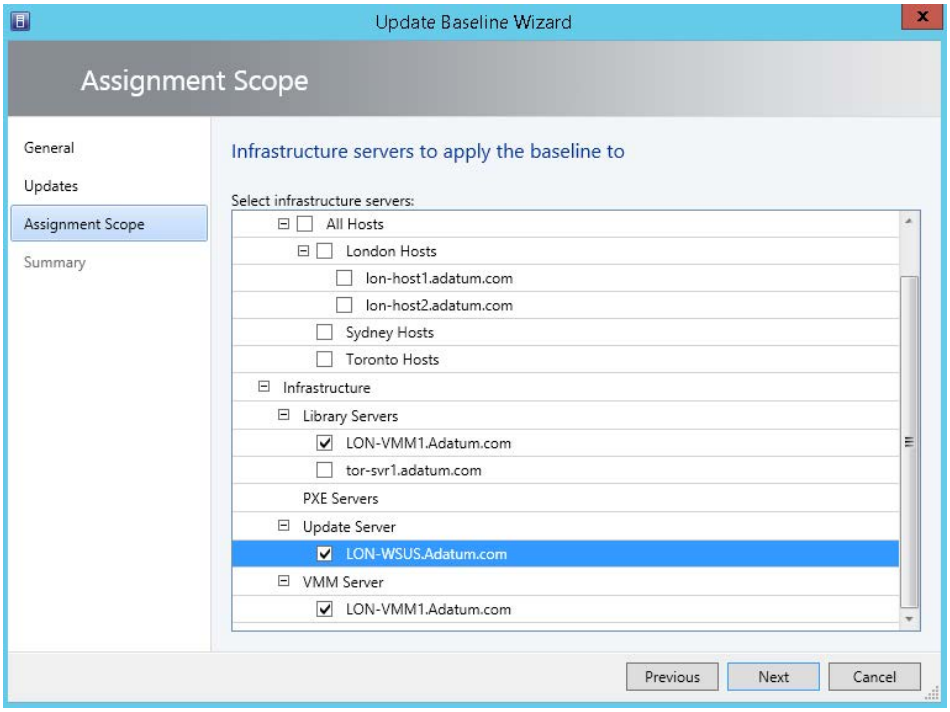



4. Hộp thoại **Add Updates to Baseline**, chọn bản cập nhật **Update for Windows Server 2012 R2 (KB2883200),** chọn **Add**, và chọn **Next**.

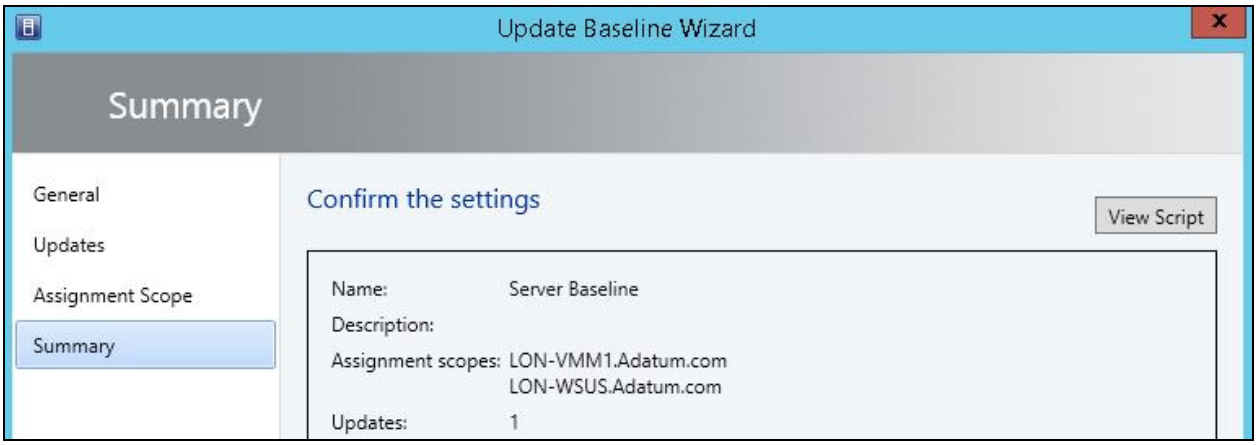


5. Cửa sổ **Assignment Scope**, đánh dấu chọn các mục như bên dưới, và chọn **Next**

- Library Servers: **LON-VMM1.Adatum.com**
- Update Server: **LON-WSUS.Adatum.com**
- VMM Server: **LON-VMM1.Adatum.com**



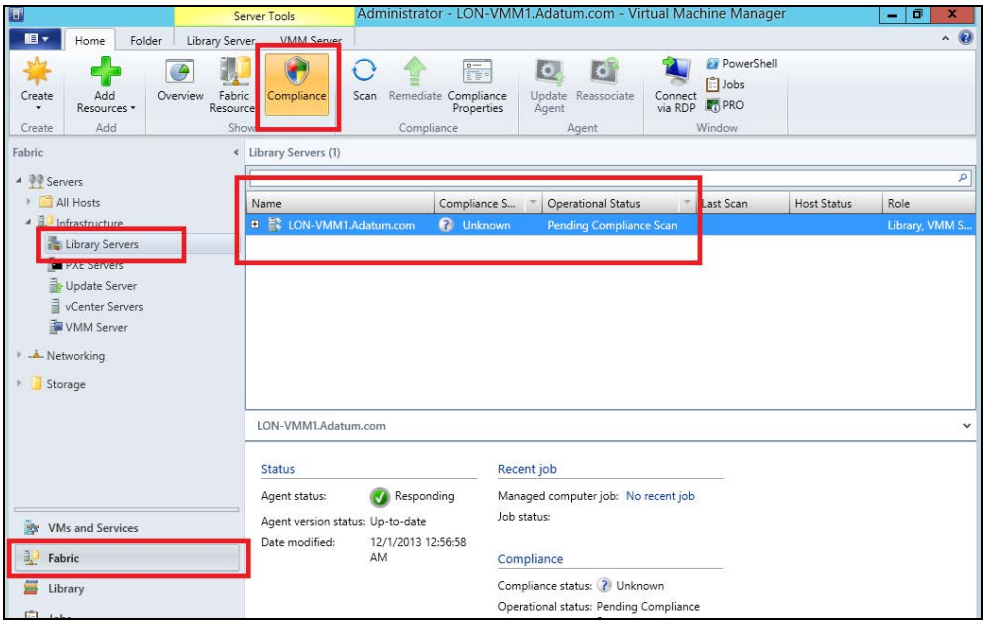

6. Cửa sổ **Summary**, chọn **Finish**.



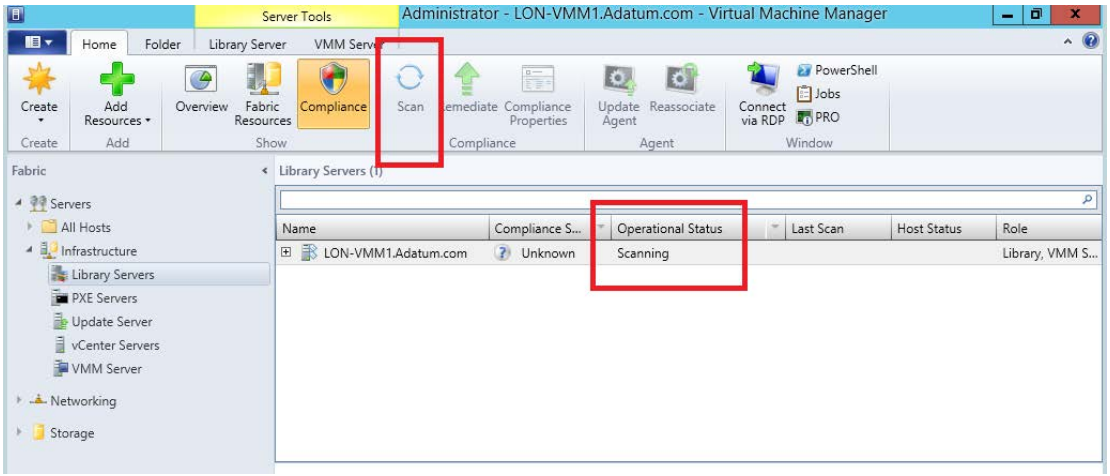

7. Kiểm tra và tắt cửa sổ **Jobs**.

**Bước 3: Kiểm tra kết quả.**

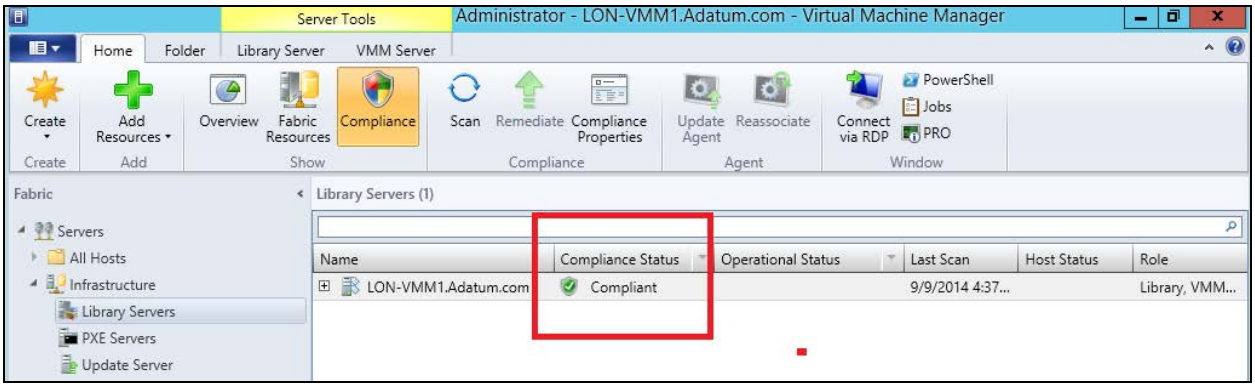
1. Trên máy **LON-VMM1**, trong cửa sổ **VMM**, chọn **Fabric,** bung **Servers**, bung **Infrastructure**, chọn **Library Servers**, chọn **LON-VMM1.Adatum.com** chọn **Compliance**. Kiểm tra cột **Compliance Status** báo **Unknown**, cột **Operational Status** báo **Pending Compliance Scan**.




2. Chọn **LON-VMM1.Adatum.com**, chọn **Scan**, kiểm tra cột **Operational Status** báo **Scanning**.



3. Sau vài phút, kiểm tra cột **Compliance Status** báo **Compliant**.




**Lưu ý:** Nếu cột Compliance Status báo Non-Compliant, thì chuột phải LON-VMM1.Adatum.com, chọn Remediate. Trong cửa sổ Update Remediation, đánh dấu chọn Do not restart servers after remediation, và chọn Remediate.

4. Tắt cửa sổ **Virtual Machine Manager**.

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công chức năng VMM Host Updating**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20414C-LON-VMM1, 20414C-LON-SVR1, 20414C-LON-SVR2, 20414C-LON-WSUS, and 20414C-TOR-SVR1, 20414C-LON-OR1.**

# Bài 5: Thực hiện giám sát hệ thống bằng Sytem Center Operations Manager (SCOM)

## I. Mục tiêu:

- Giám sát server  bằng công cụ sẵn có của Windows Server 2012.
- Giám sát server bằng Operations Manager.
- Cấu hình các thành phần giám sát trong Operations Manager.
- Theo dõi hiệu suất của Server.

## II. Kịch bản:

Sau khi đã hoàn thành việc triển khai cơ sở hạ tầng. Công ty A. Datum muốn thực hiện một chiến lược giám sát hệ thống mạng. A. Datum quyết định sử dụng các công cụ giám sát có sẵn trên Windows Server 2012 cho một số văn phòng chi nhánh. Ngoài ra, A. Datum đã cài đặt System Center Operations Manager ở London để giám sát các máy chủ trong trung tâm dữ liệu.

## III. Yêu cầu tổng quan:

Bạn cần phải thực hiện công việc giám sát các server trong hệ thống bằng công cụ có sẵn trên Windows Server 2012 và sử dụng Operations Manager.

## IV. Mô hình thực hành gồm các máy:

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-OM1**<br>**20414C-LON-SVR1**<br>**20414C-LON-SVR2** |

| | |
|---|---|
| | **20414C-TOR-SVR1**<br>**20414C-TOR-SS1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên lại từ bước 1 đến 3 cho các máy ảo còn lại.

**VI. Thực hành:**

*Thời gian thực hành: 60 phút*

## Bài tập 1: Giám sát server bằng công cụ sẵn có của Windows Server 2012

A. Datum vẫn chưa quyết định triển khai Operations Manager trong trung tâm dữ liệu ở Toronto, vì vậy bạn phải giám sát các server bằng các công cụ sẵn có của Windows Server 2012. A. Datum muốn giám sát nhiều máy chủ bằng một giao diện duy nhất, và thu thập thông tin từ nhiều server ở một vị trí duy nhất.

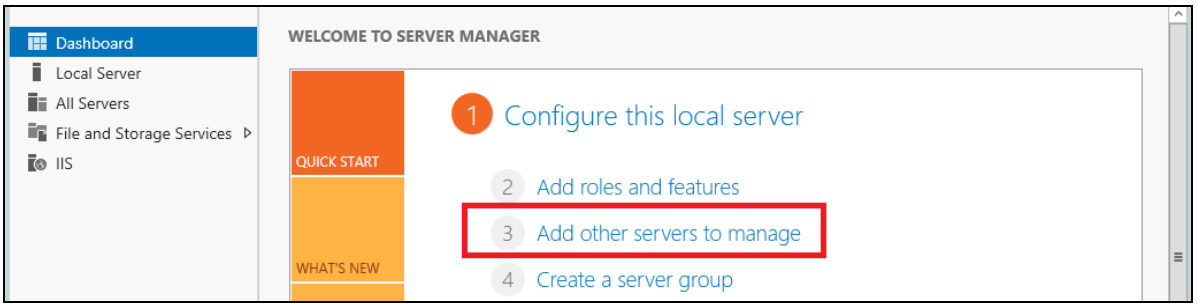
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hinh Server Manager giám sát nhiều Servers.
2. Cấu hình Data Collector Set.
3. Cấu hình Event subscription.

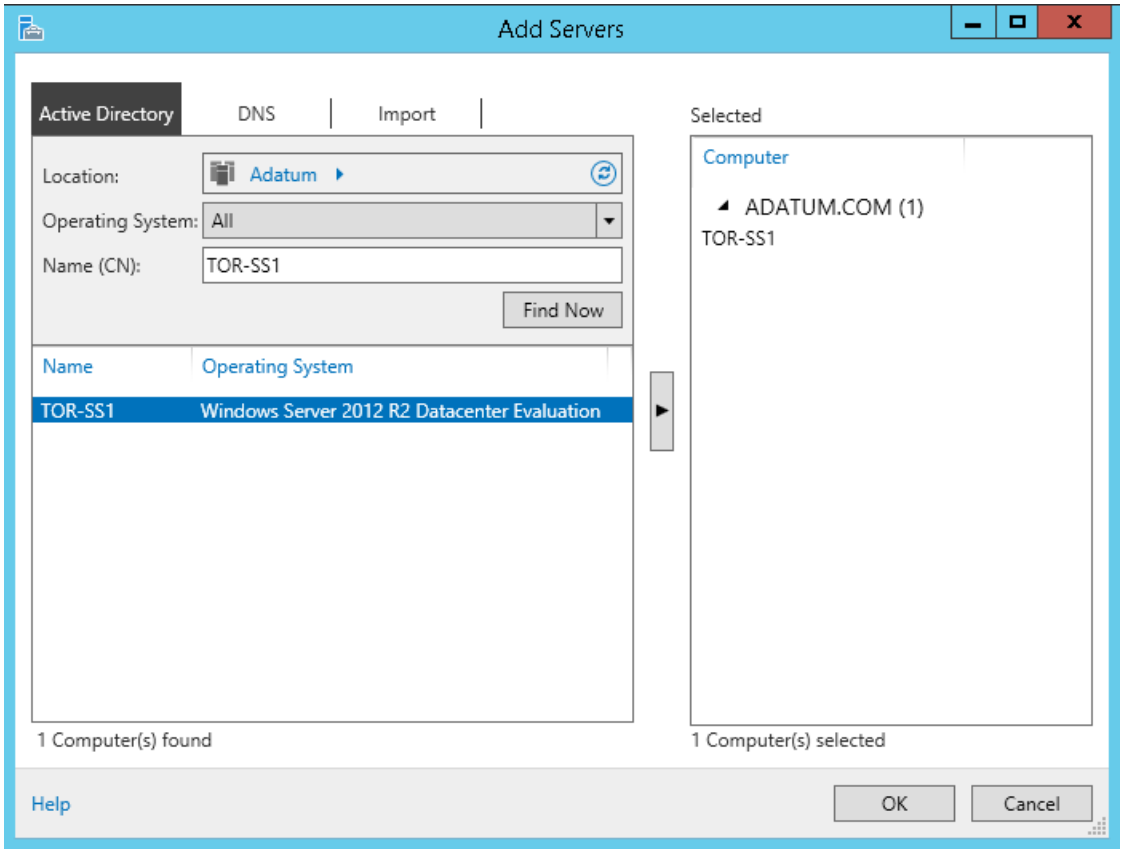
❖ **Thực hiện:**

**Bước 1: Cấu hình Server Manager giám sát nhiều Servers.**

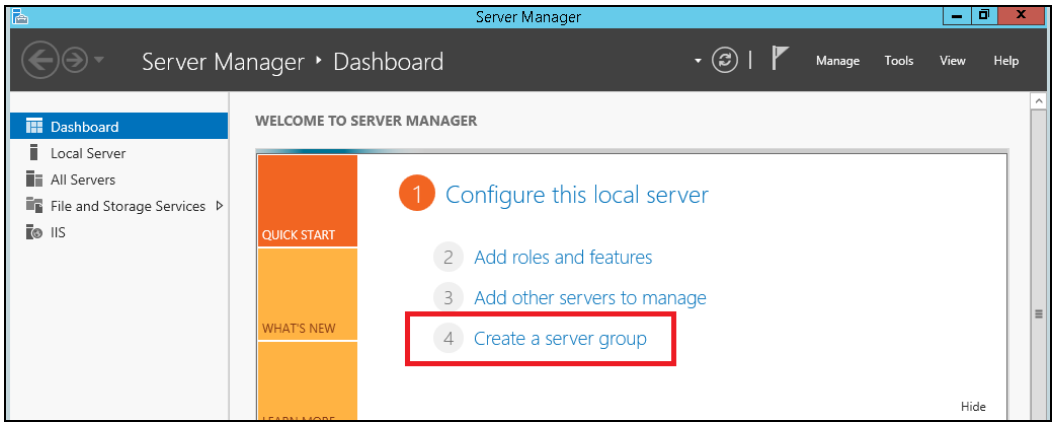
1. Trên máy **TOR-SVR1**, trong cửa sổ **Server Manager**, chọn **Add other servers to manage**.



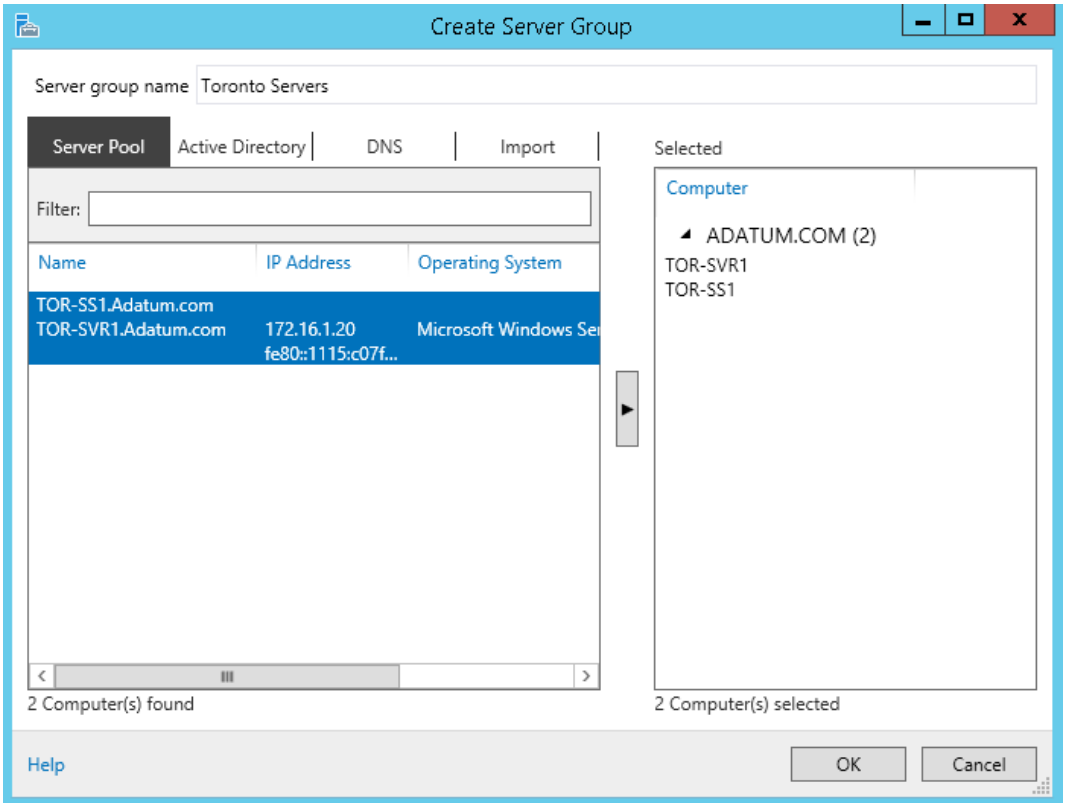

2. Hộp thoại **Add Servers**, trong ô **Name (CN)**, nhập **TOR-SS1**, chọn **Find Now**. Chọn **TOR-SS1**, nhấn biểu tượng mũi tên để add server vào ô **Selected**, chọn **OK**.



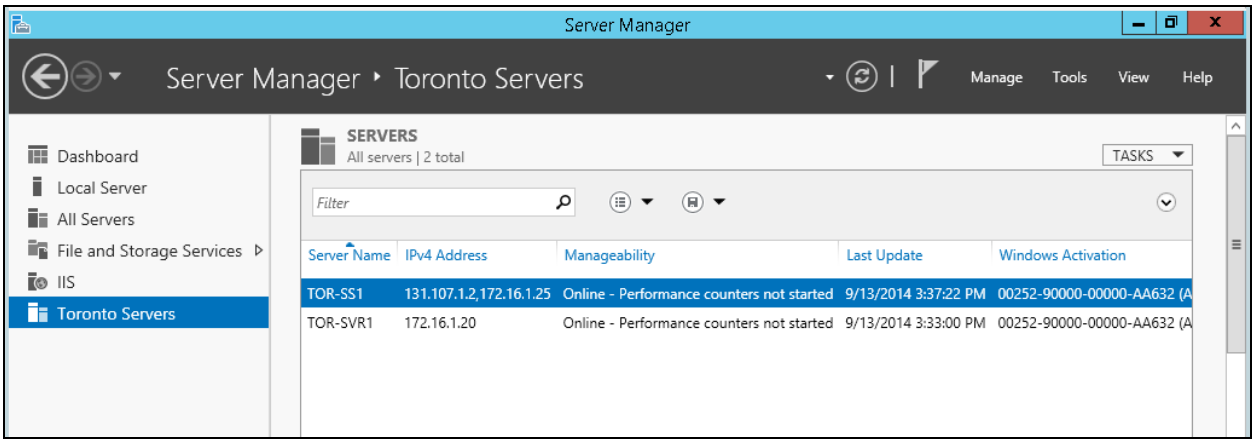
3. Trong cửa sổ **Server Manager**, chọn **Create a server group**.



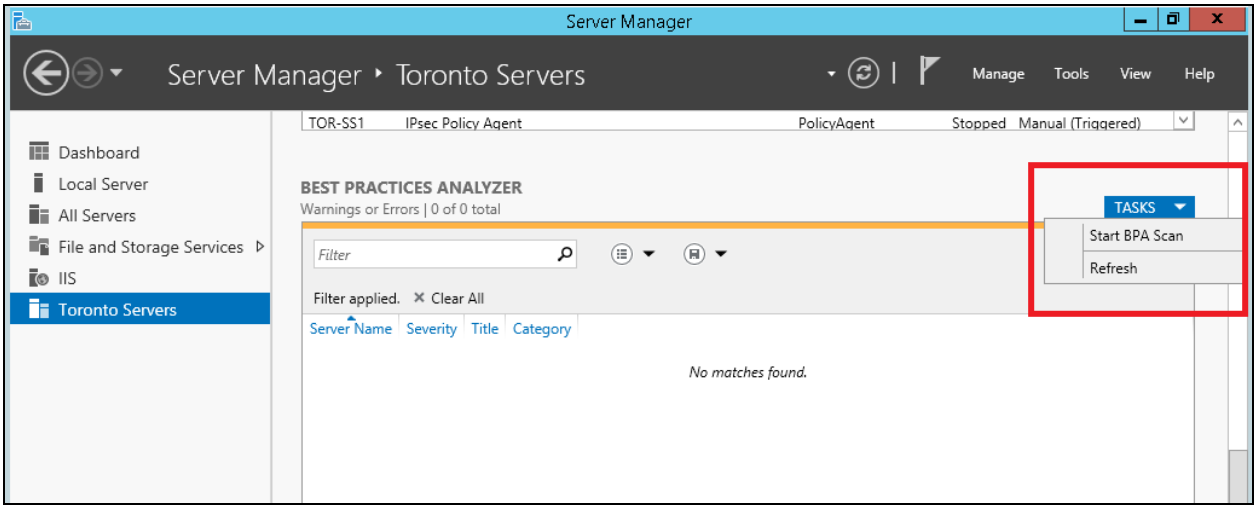

4. Hộp thoại **Create Server Group**, trong ô **Server group name**, nhập **Toronto Servers**. Giữ phím **Ctrl** chọn **TOR-SVR1.Adatum.com** và **TOR-SS1.Adatum.com**. Nhấn biểu tượng mũi tên để add 2 server vào ô **Selected,** chọn **OK**.



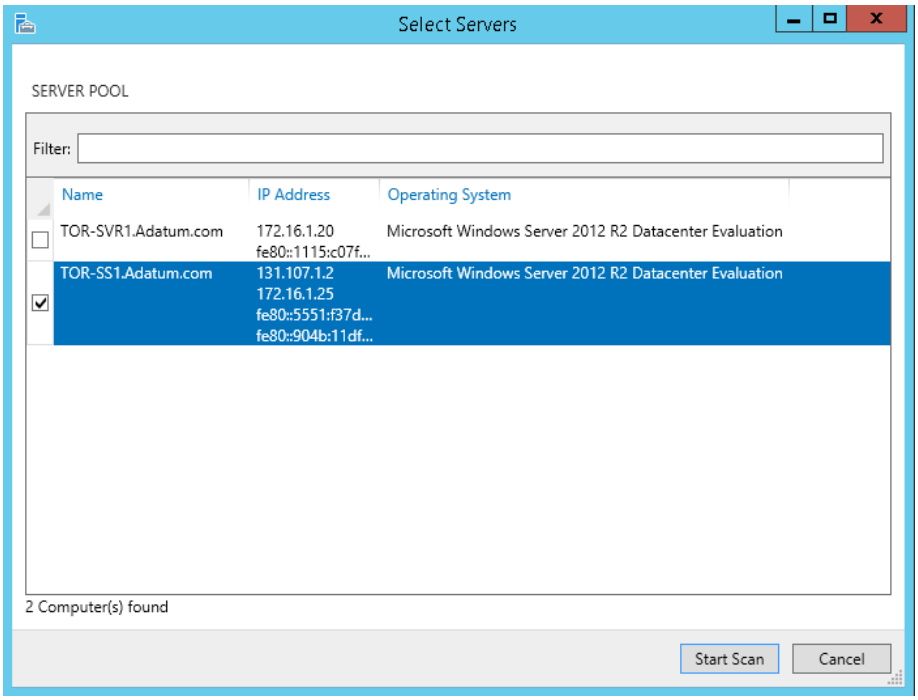
5. Trong **Server Manager**, chọn **Toronto Servers**. Trong phần **SERVERS**, chọn **TOR-SS1**.



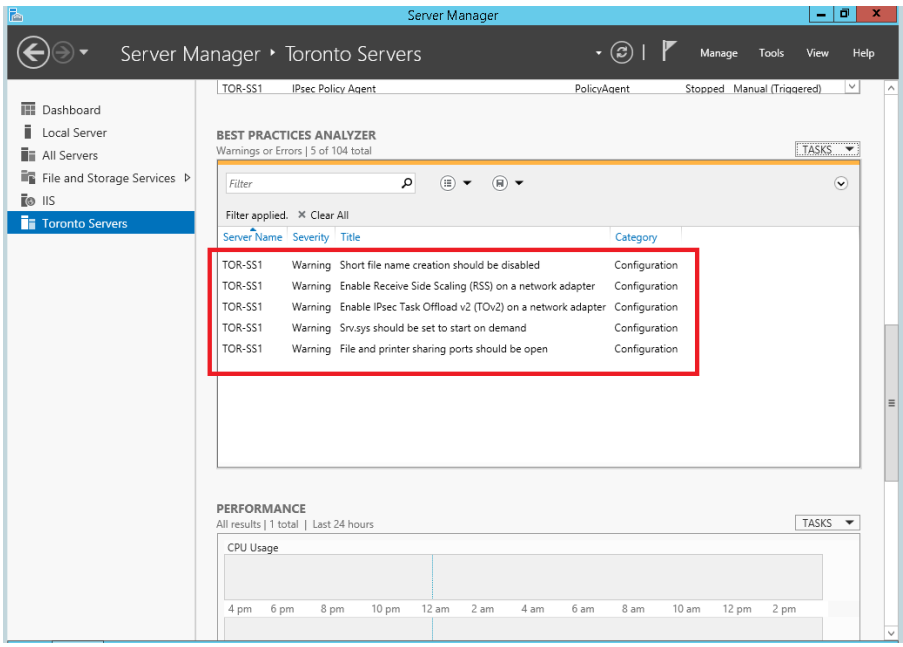

6. Kéo thanh trượt xuống phần **BEST PRACTICES ANALYZER**, bung **TASKS**, chọn **Start BPA Scan**.



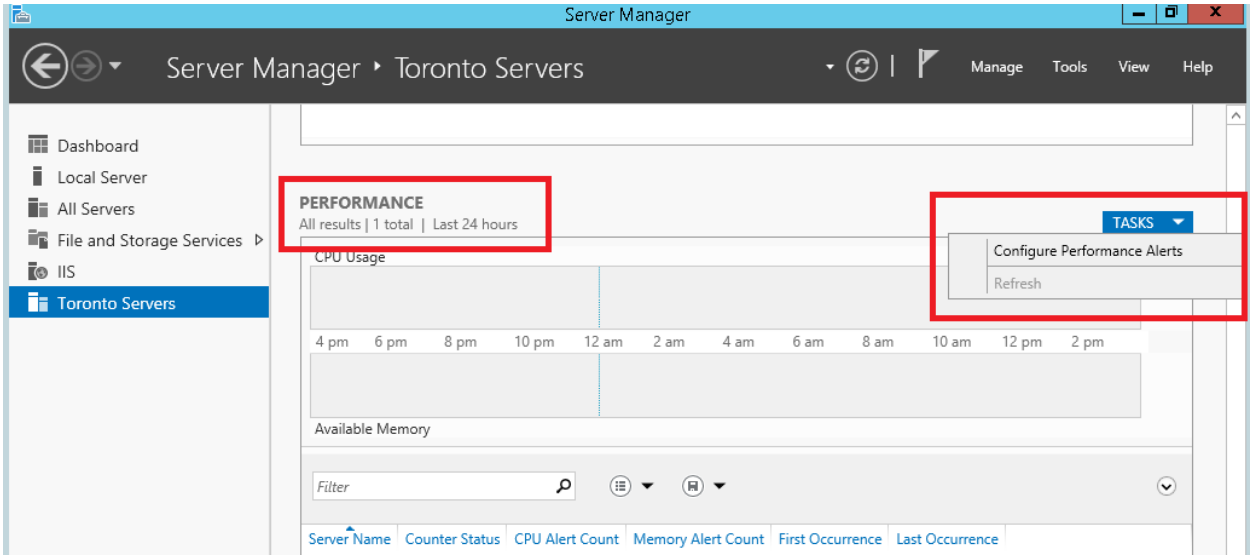
7. Hộp thoại **Select Servers**, chọn **Start Scan**.



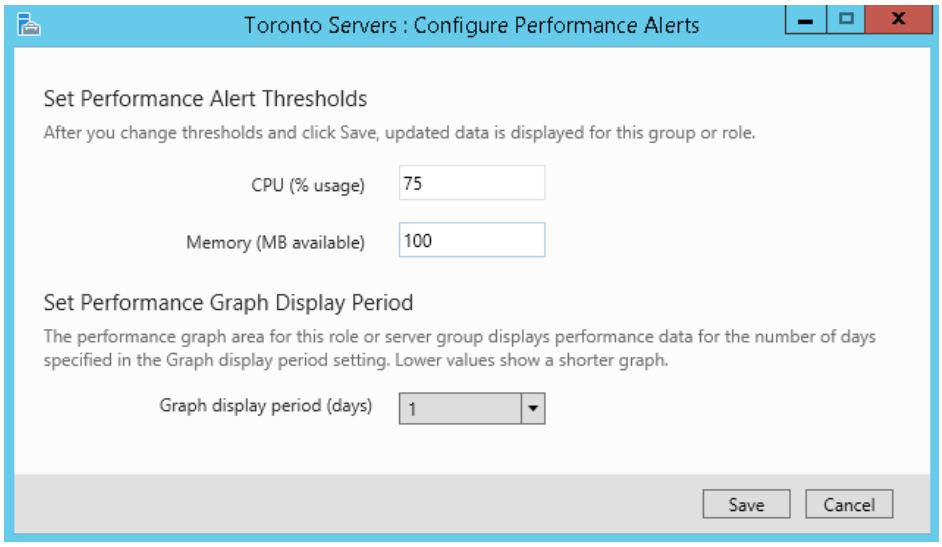

8. Quá trình **Scan** sẽ hoàn tất trong khoảng từ 2 tới 5 phút.



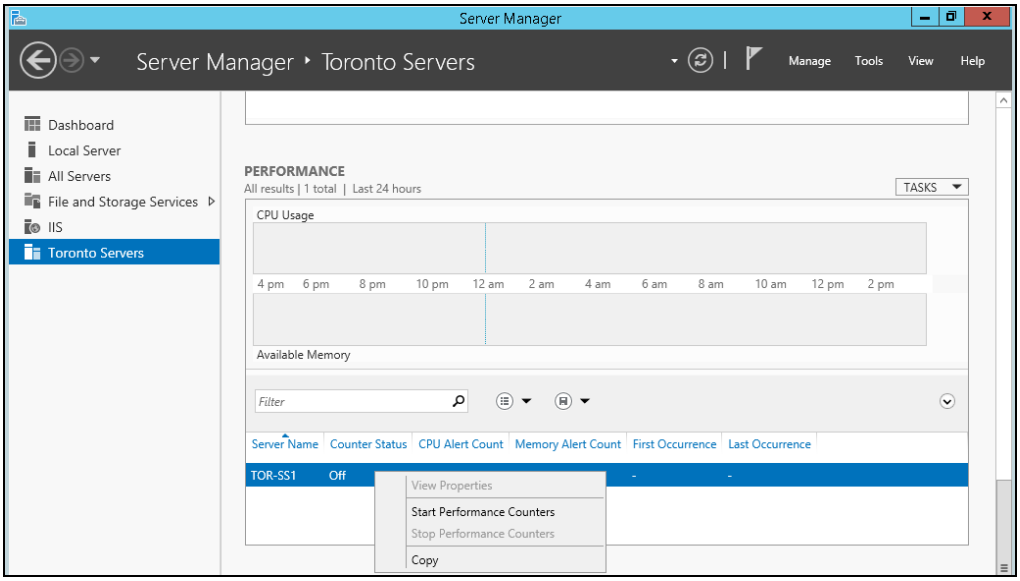
9. Kéo thanh trượt xuống phần **PERFORMANCE**, bung **TASKS**, chọn **Configure Performance Alerts**.




10. Hộp thoại **Toronto Servers: Configure Performance Alerts**, trong ô **CPU (% usage)**, nhập **75**, trong ô **Memory (MB available)**, nhập **100**, và chọn **Save**.

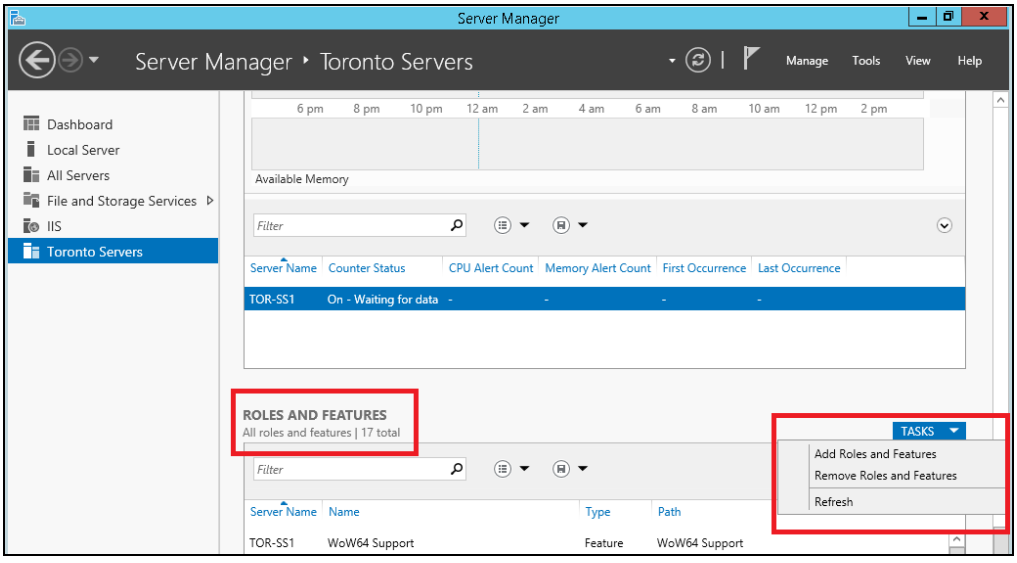


11. Trong phần **PERFORMANCE**, chuột phải **TOR-SS1**, chọn **Start Performance Counters**.

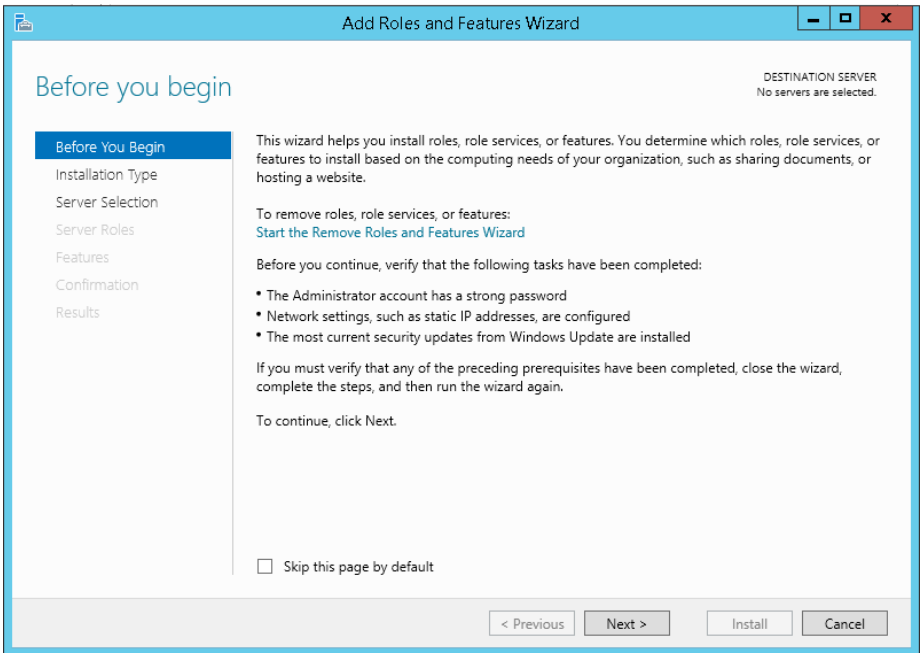



**Chú ý:** Thời gian hoàn tất Performance Counters khoảng 30 phút nên trong thời gian chờ đợi, bạn sẽ làm các bước tiếp theo. Sau khi hoàn thành bài tập, bạn sẽ kiểm tra lại kết quả của bước này.

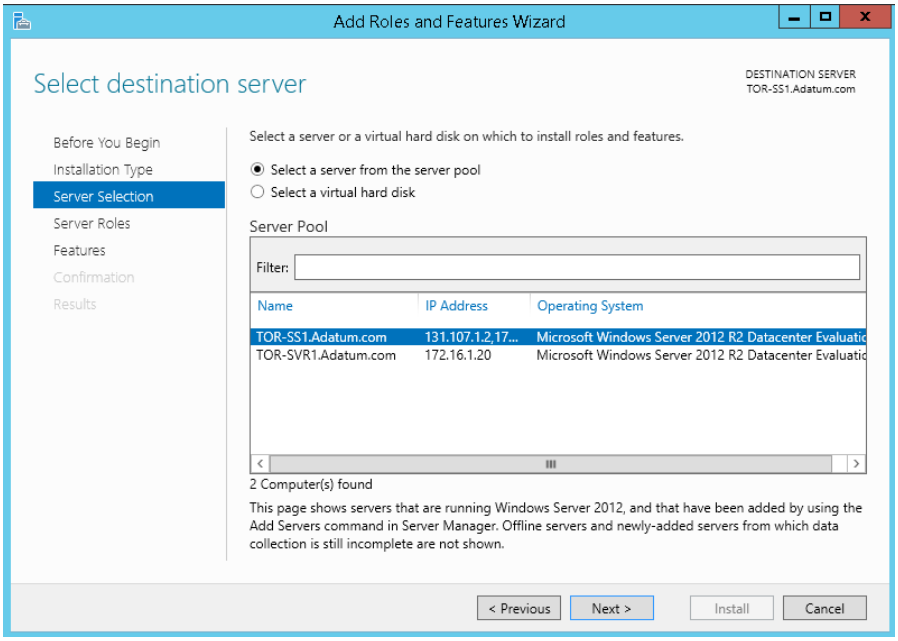
12. Kéo thanh trượt xuống phần **ROLES AND FEATURES**, bung **TASKS**, chọn **Add Roles and Features**.



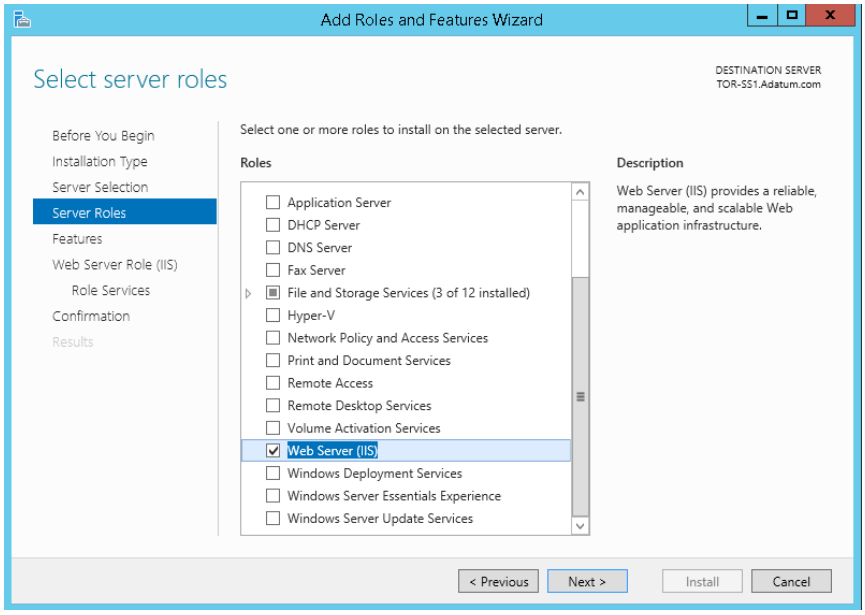
13. Cửa sổ **Before you begin**, chọn **Next** 2 lần.




14. Cửa sổ **Select destination server**, chọn **TOR-SS1.Adatum.com**, và chọn **Next**.

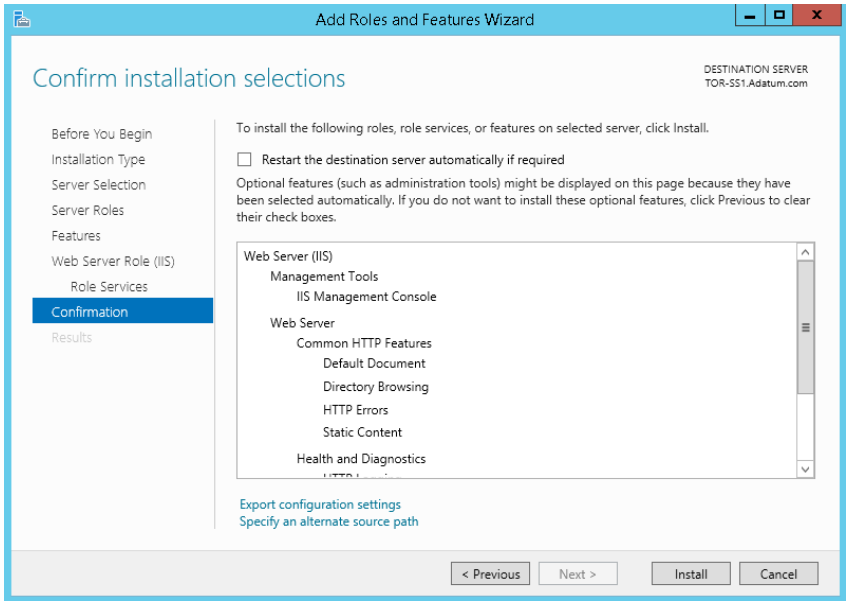


15. Cửa sổ **Select server roles**, đánh dấu chọn **Web Server (IIS)**, chọn **Add Features**, và chọn **Next**.



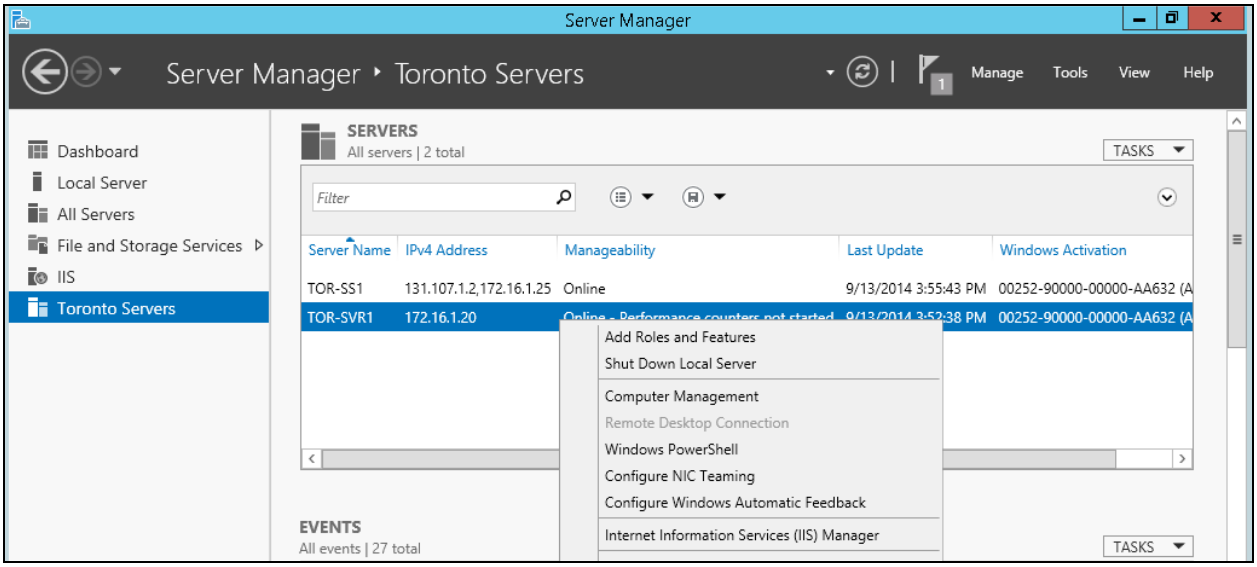

16. Cửa sổ **Select features**, chọn **Next** 3 lần.

17. Cửa sổ **Confirmation installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close.**

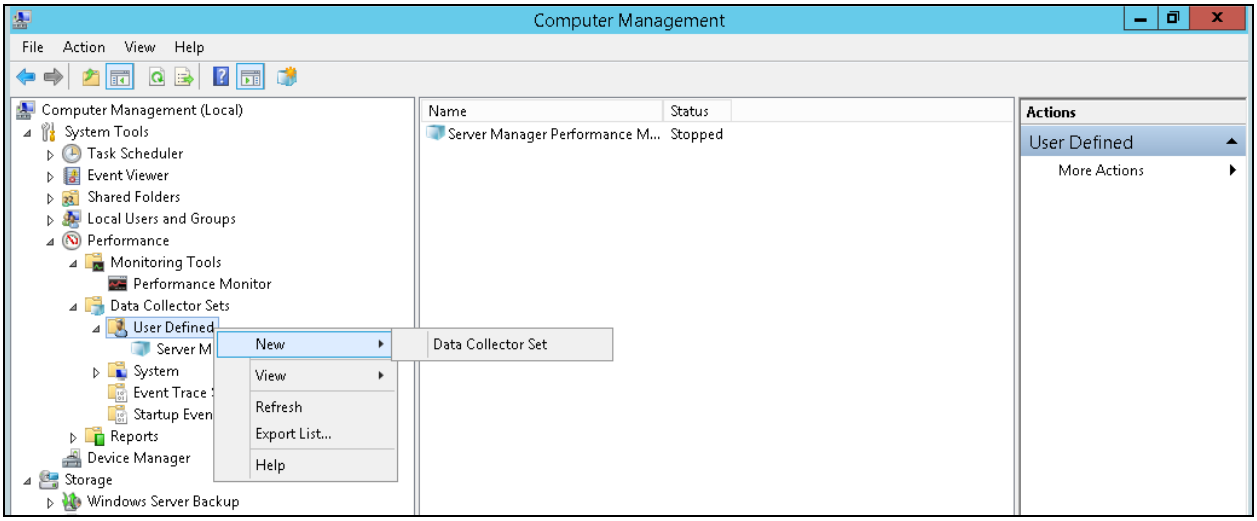


## Bước 2: Cấu hình Data Collector Set.

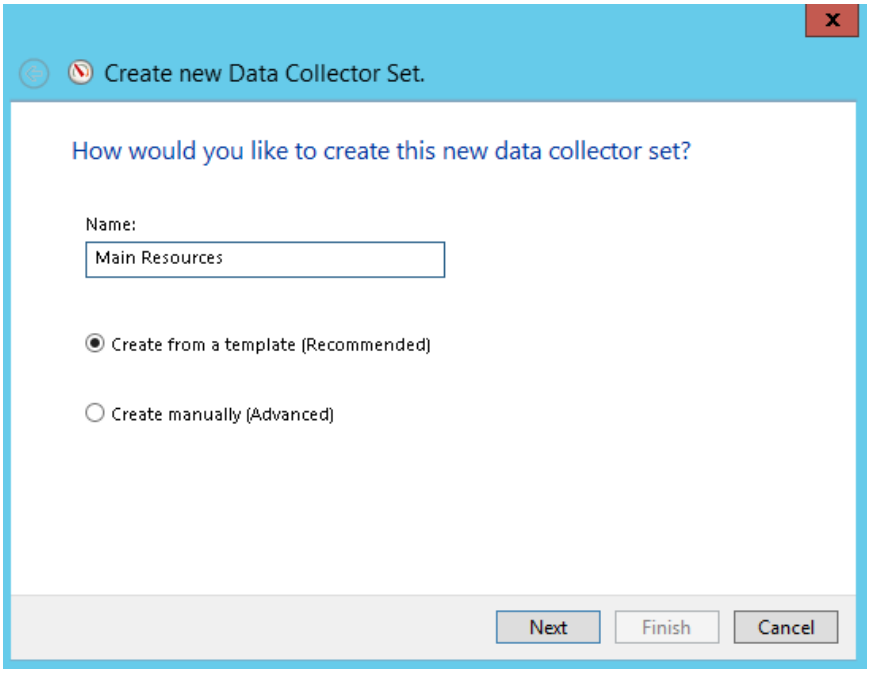
1. Trên máy **TOR-SVR1**, trong cửa sổ **Server Manager**, chọn **Toronto Servers**, trong phần **SERVERS**, chuột phải **TOR-SVR1**, chọn **Computer Management**.



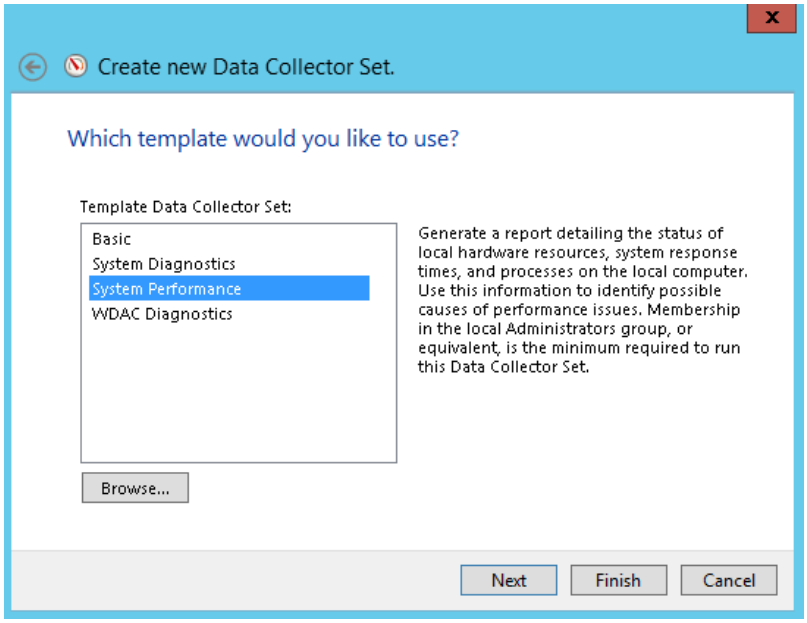

2. Trong cửa sổ **Computer Management**, bung **Performance**, bung **Data Collector Sets**, chuột phải **User Defined**, chọn **Data Collector Set**.



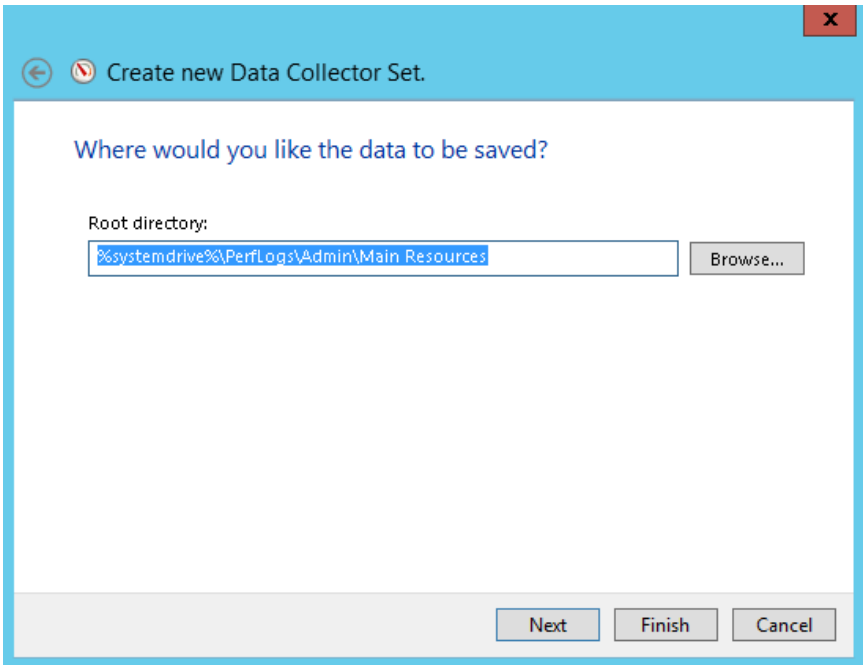
3. Cửa sổ **Create new Data Collector Set**, trong ô **Name**, nhập **Main Resources**, chọn **Next**.



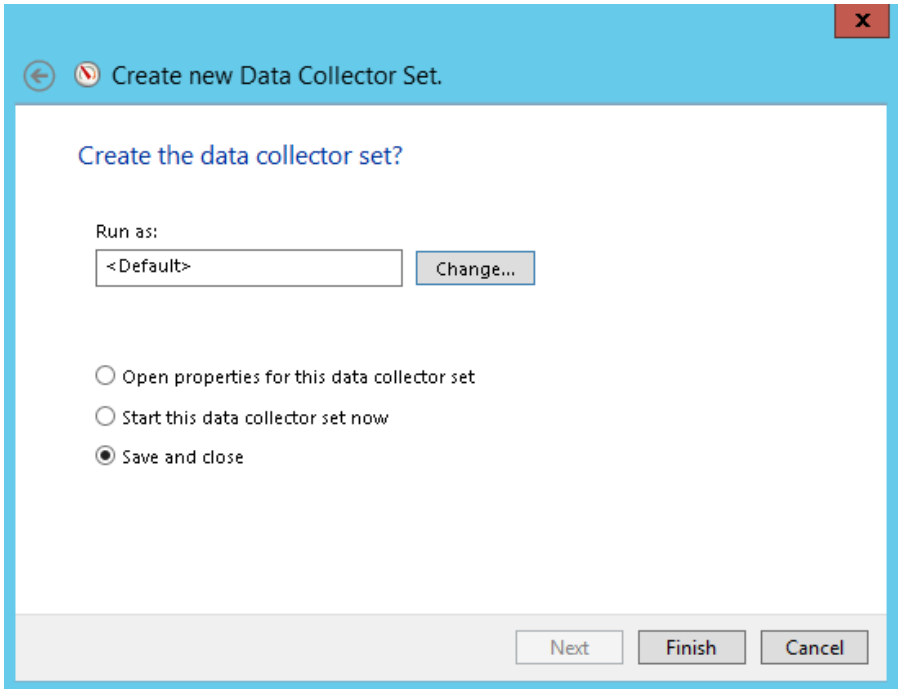

4. Cửa sổ **Which template would you like to use?**, chọn **System Performance**, chọn **Next**.



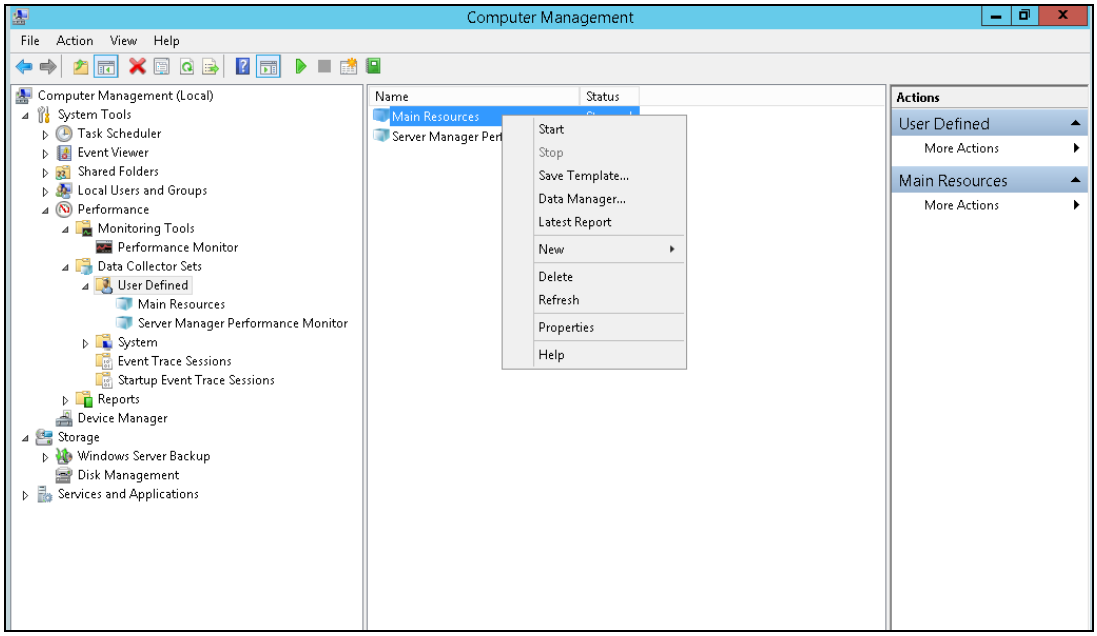
5. Cửa sổ **Where would you like the data to be saved?**, chọn **Next**.



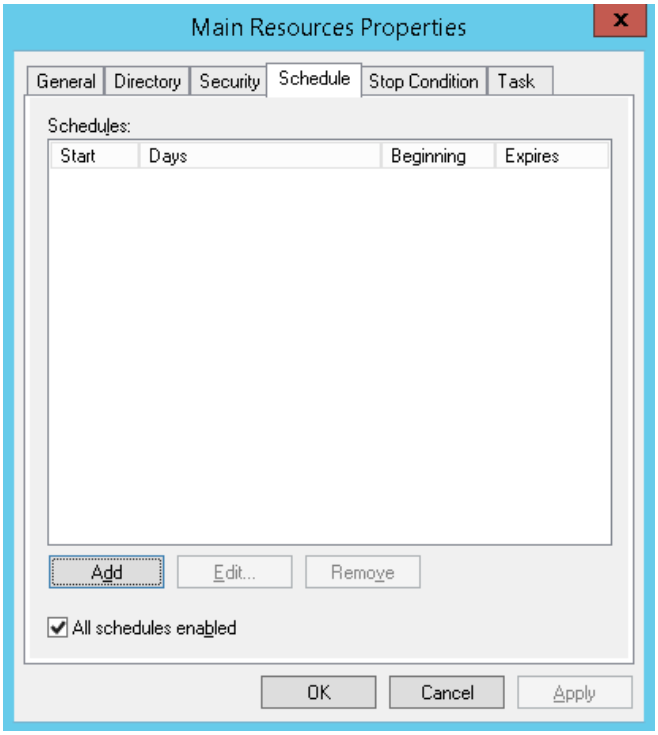

6. Cửa sổ **Create the data collector set**, chọn **Finish**.



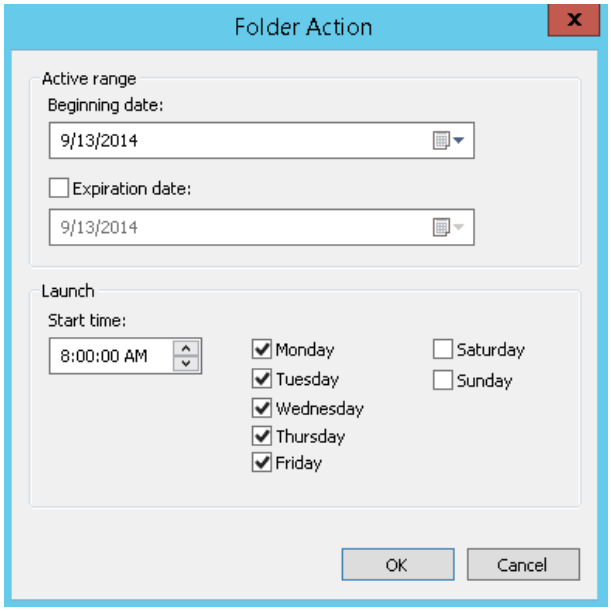
7. Trong mục **User Defined,** chuột phải **Main Resources**, chọn **Properties**.



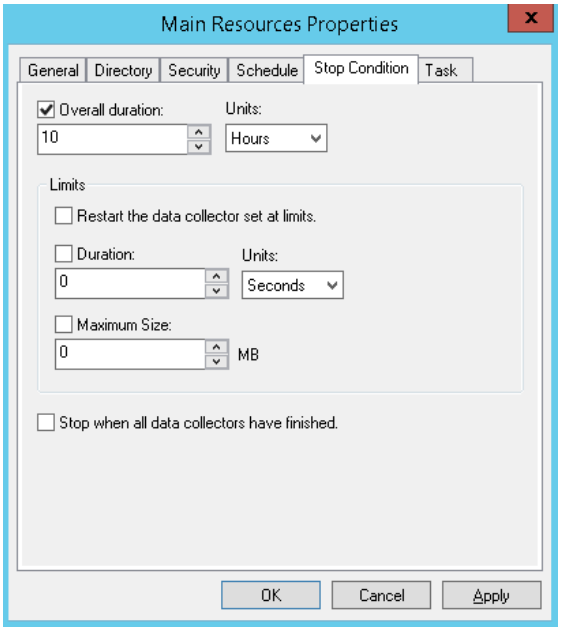

8. Qua tab **Schedule**, chọn **Add**.



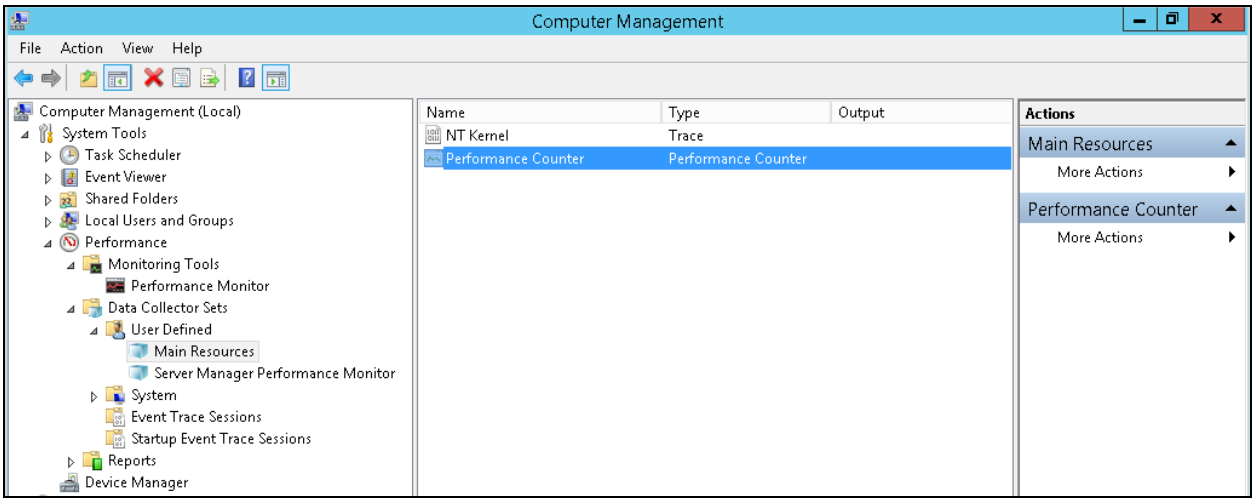
9. Hộp thoại **Folder Action**, trong ô **Start time**, nhập **8:00:00 AM**. Đánh dấu chọn các ngày **Monday, Tuesday, Wednesday, Thursday, Friday,** chọn **OK**.



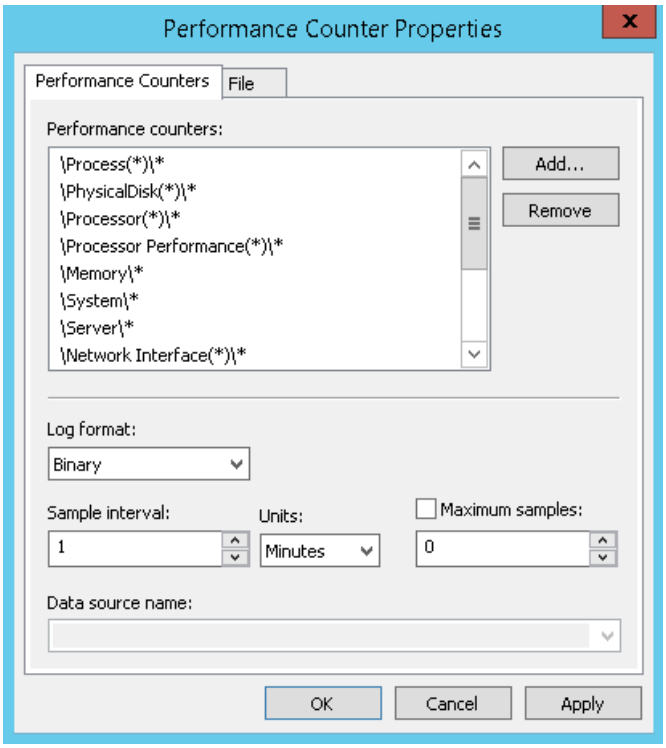

10. Qua tab **Stop Condition**, trong ô **Overall duration**, nhập **10**, bung ô **Units,** chọn **Hours**, và chọn **OK**.



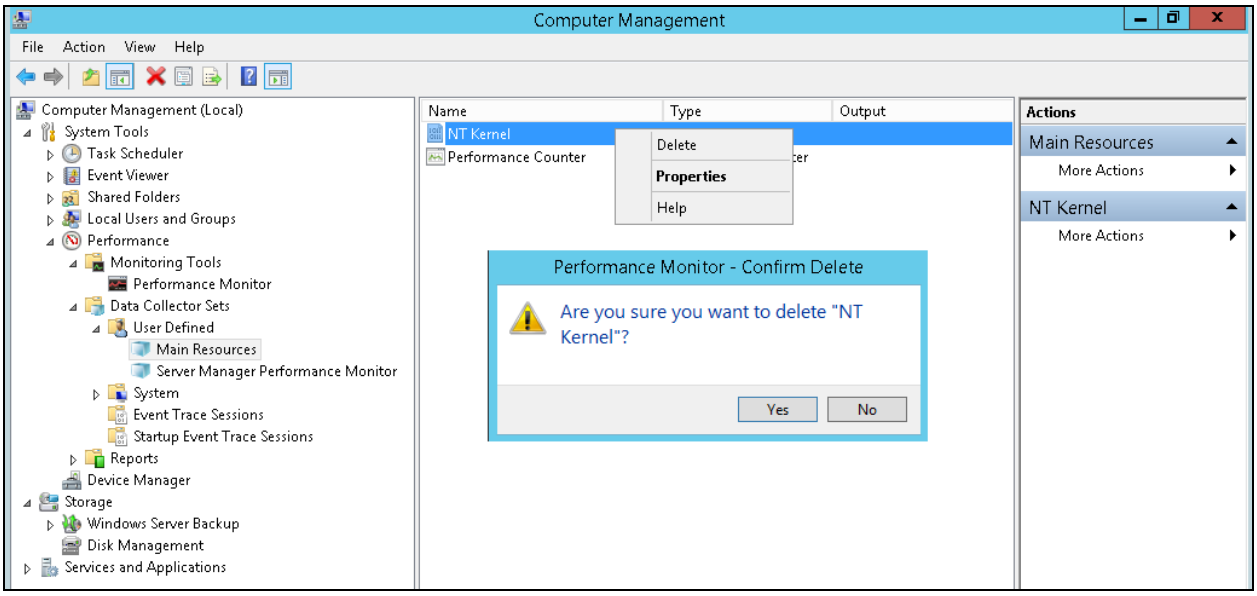
11. Trong cửa sổ **Computer Management,** chọn **Main Resources**, nhấp đôi chuột mở **Performance Counter**.



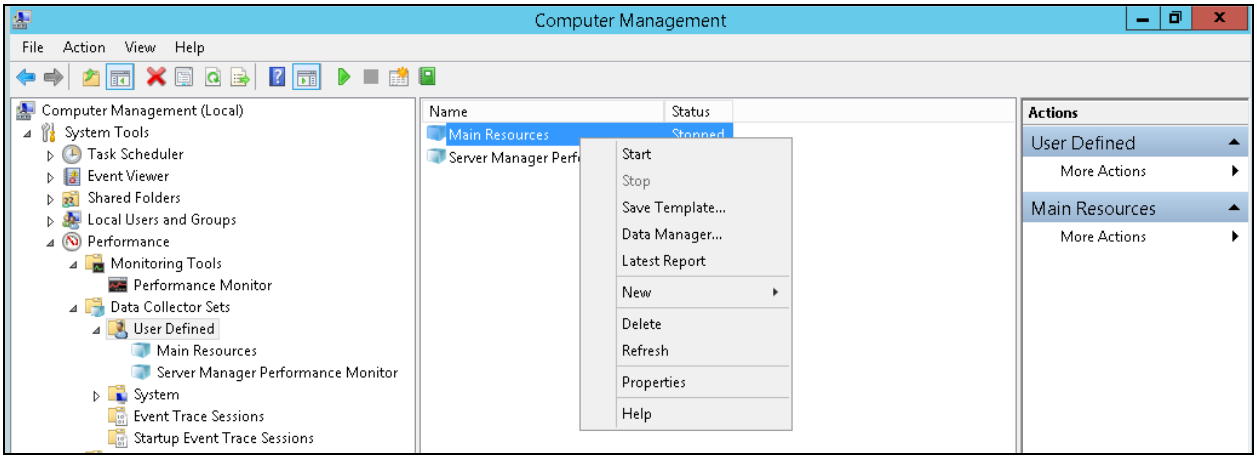

12. Hộp thoại **Performance Counter Properties**, đảm bảo ô **Sample interval**, nhập **1**, ô **Units,** chọn **Minutes**, và chọn **OK**.



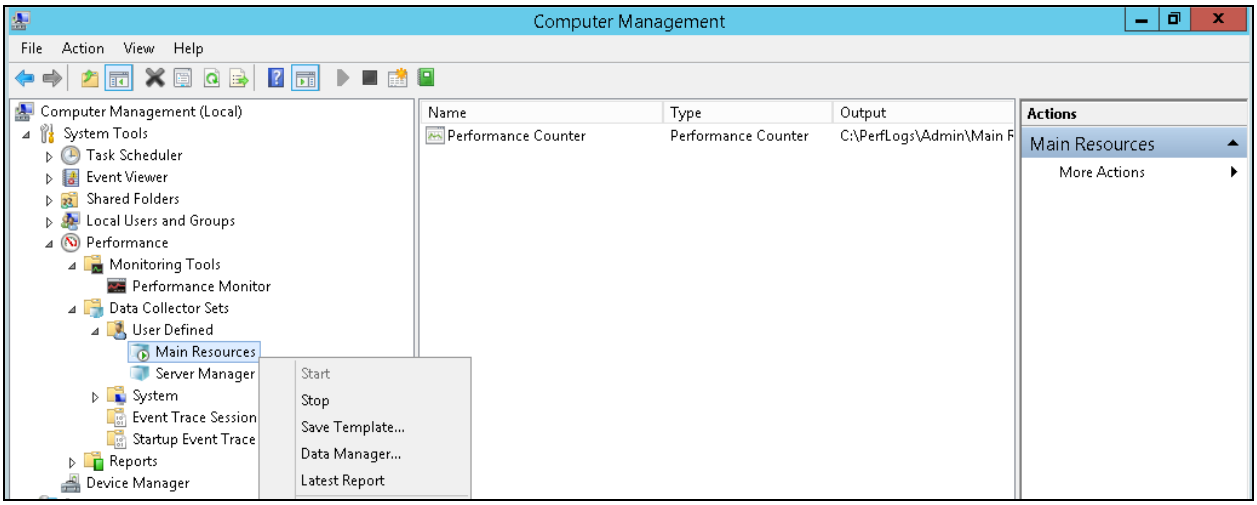
13. Trong mục **Main Resources,** chuột phải **NT Kernel**, chọn **Delete,** và chọn **Yes**.



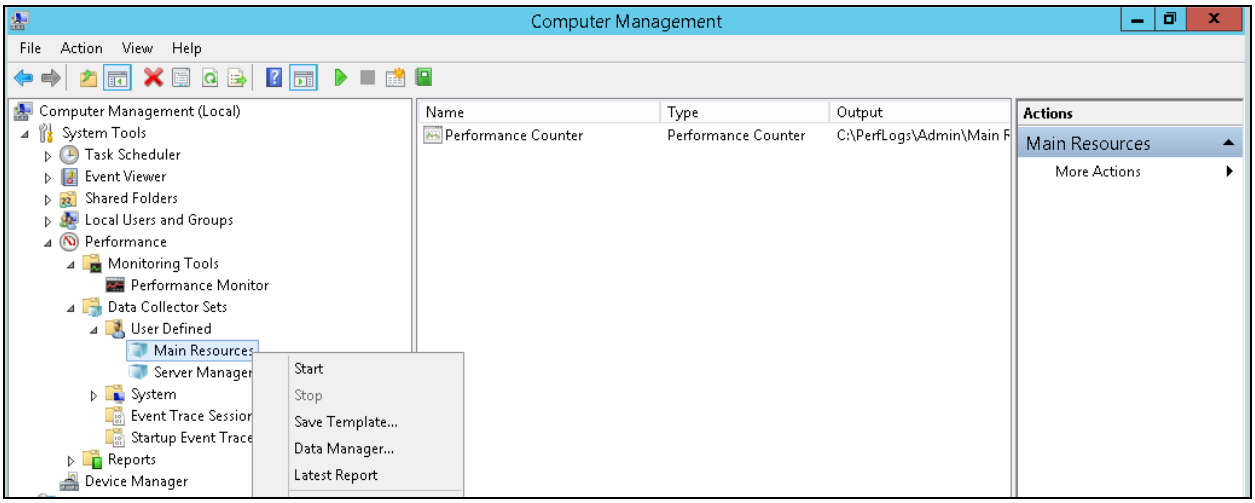

14. Chọn mục **User Defined**, chuột phải **Main Resources**, chọn **Start**.



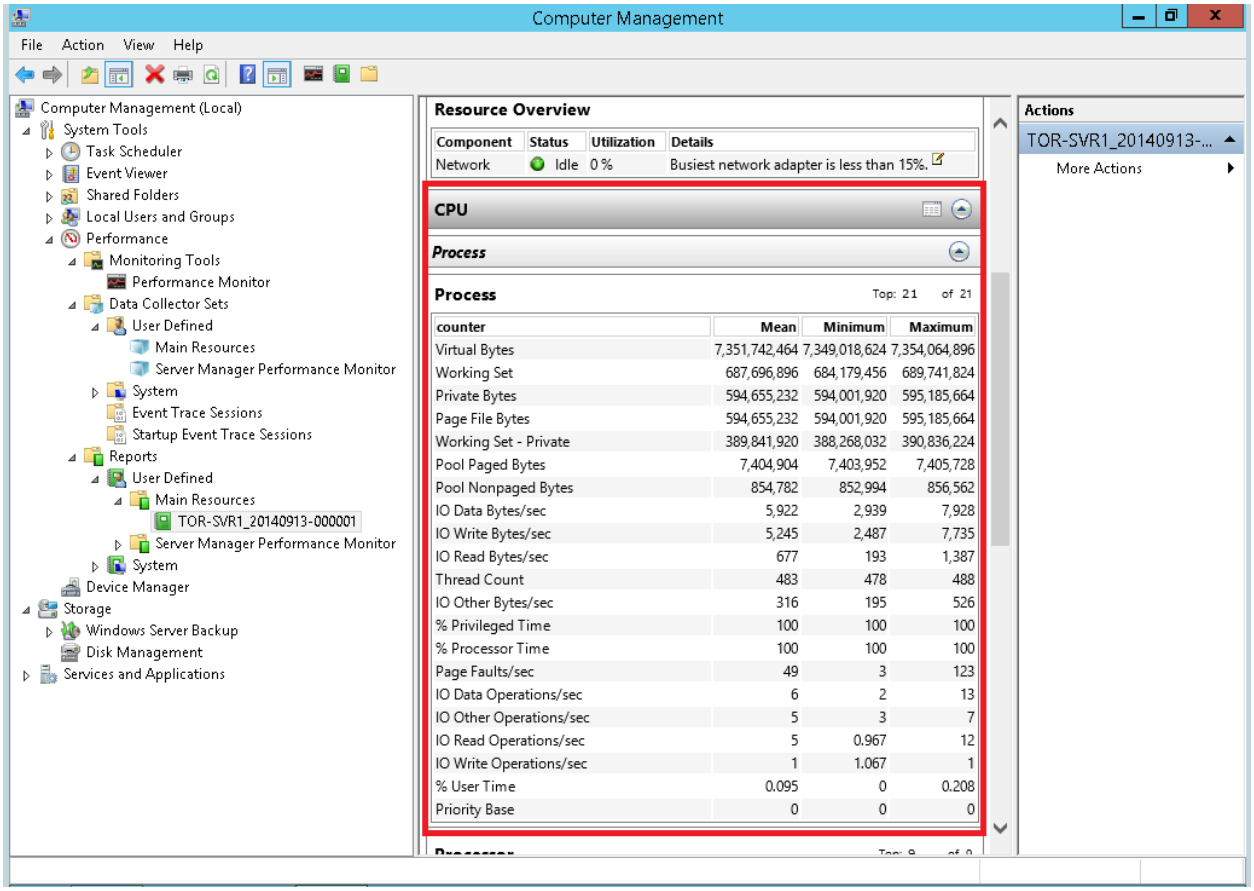
15. Đợi sau 10 phút, chuột phải **Main Resources**, chọn **Stop**.




16. Chuột phải **Main Resources**, chọn **Latest Report**.

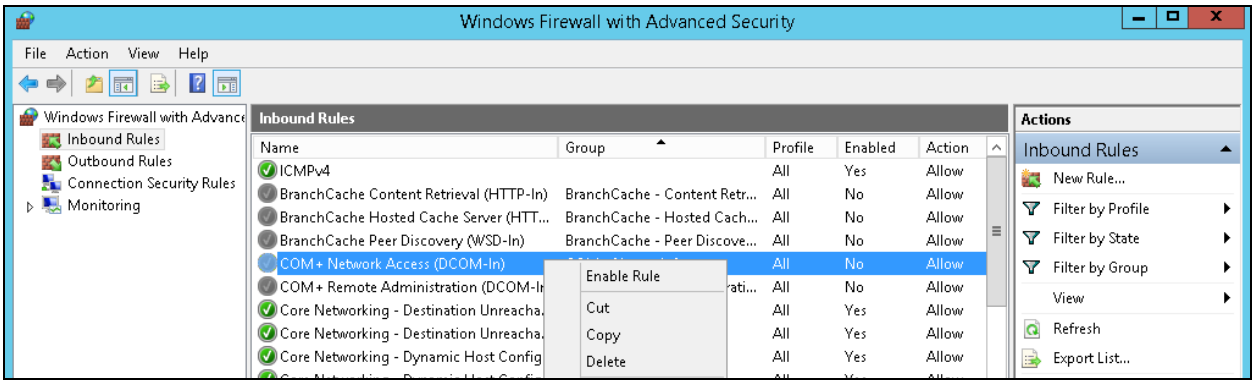


17. Trong **System Performance Report**, chọn **CPU**, chọn **Process**. Kiểm tra thông tin Report. Và tắt **Computer Management**.

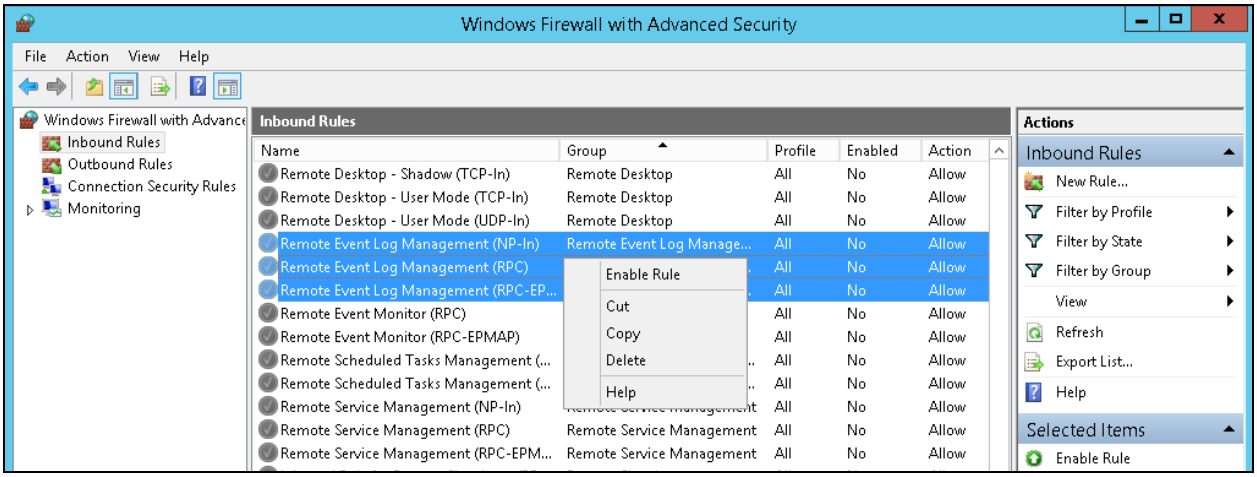


## Bước 3: Cấu hình Event subscription.

1. Trên máy **TOR-SS1**, Trong **Server Manager**, bung menu **Tools**, mở **Windows Firewall with Advanced Security.** Chọn **Inbound Rules**, chuột phải **COM+ Network Access (DCOM-In)**, chọn **Enable Rule**.

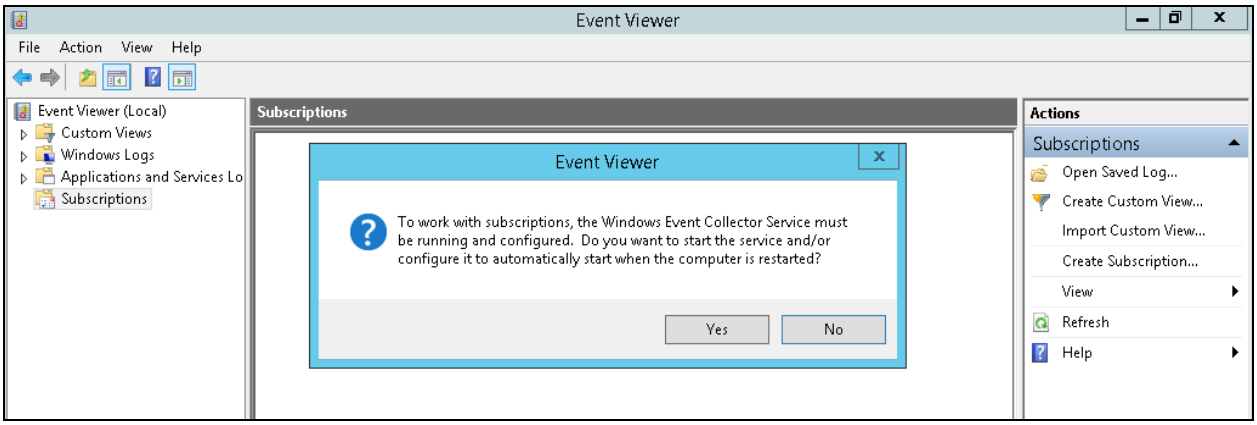



2. Kéo thanh trượt đến các rule có tên **Remote Event Log Management**. Chọn cả 3 rule có tên **Remote Event Log Management,** chuột phải lên 3 rule chọn **Enable Rule**. Tắt **Windows® Firewall with Advanced Security.**

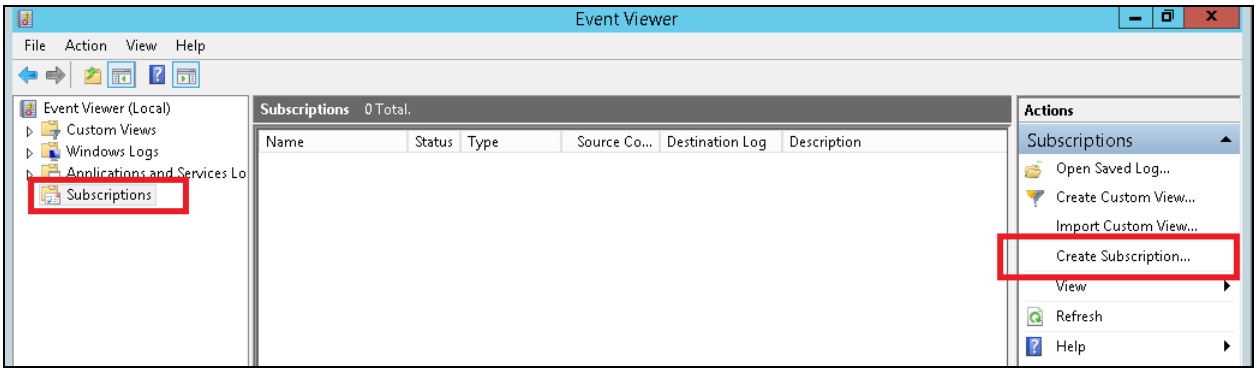



3. Qua máy **TOR-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **Event Viewer**.

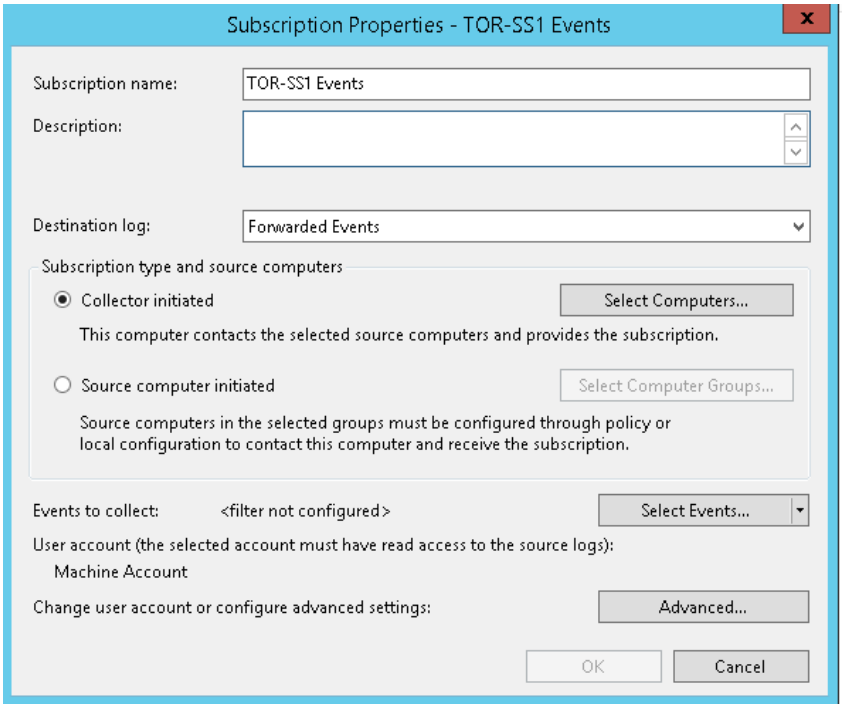
4. Trong cửa sổ **Event Viewer**, chọn **Subscriptions**. Hộp thoại **Event Viewer**, chọn **Yes**.



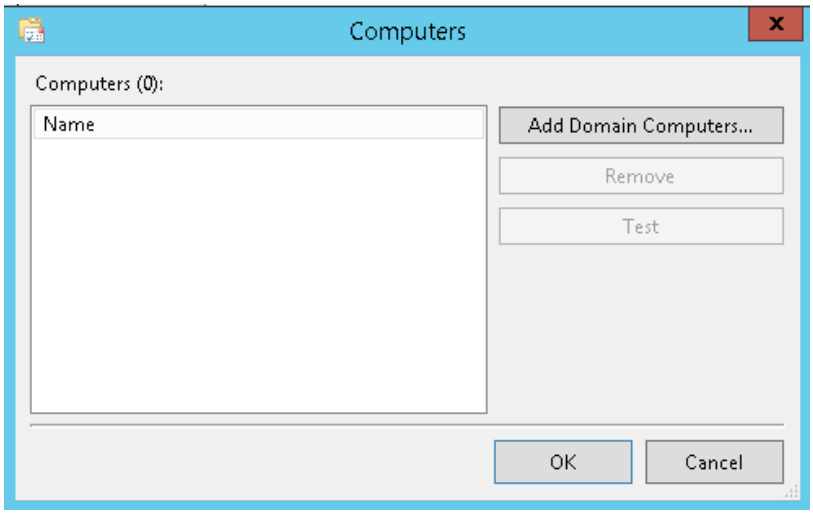

5. Trong cửa sổ **Actions**, chọn **Create Subscription**.



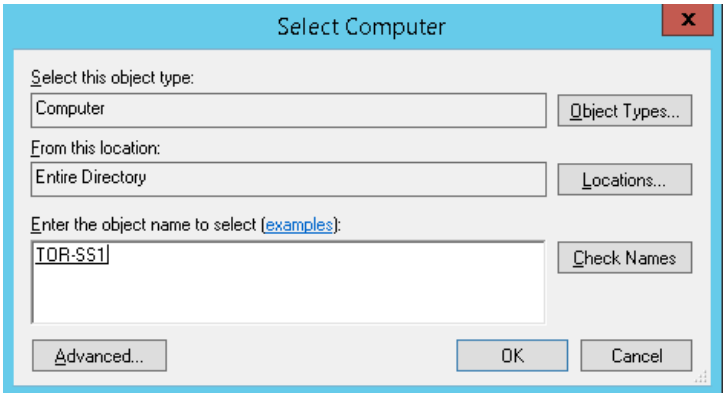
6. Hộp thoại **Subscription Properties**, trong ô **Subscription name**, nhập **TOR-SS1 Events**, chọn **Select Computers**.



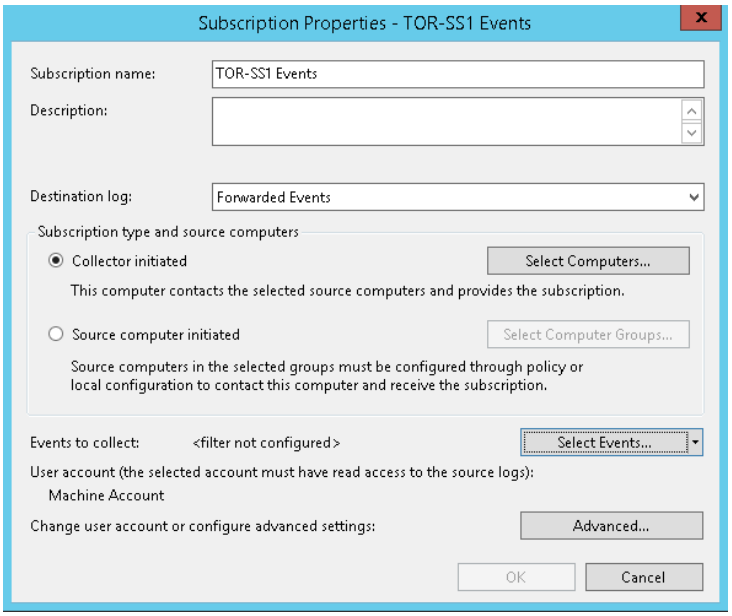

7. Hộp thoại **Computers**, chọn **Add Domain Computers**.



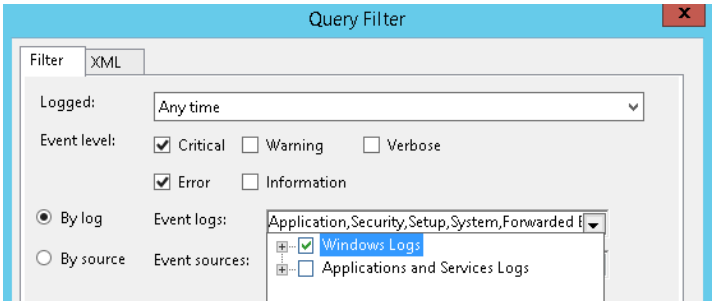
8. Hộp thoại **Select Computer**, trong ô **Enter object name to select**, nhập **TOR-SS1**, chọn **Check Names**, và chọn **OK** 2 lần.



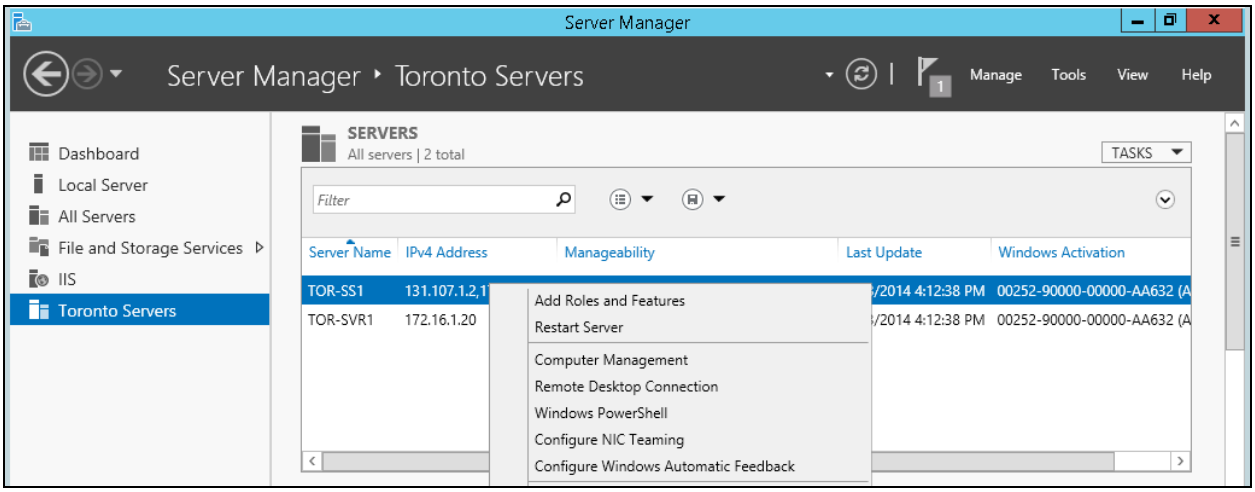

9. Hộp thoại **Subscription Properties,** chọn **Select Events**.



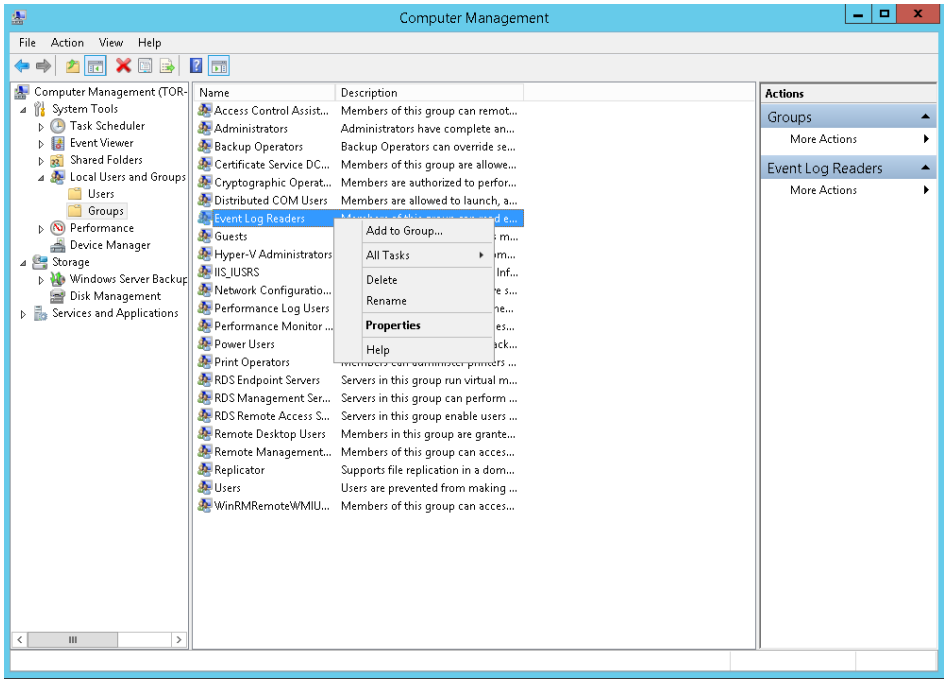
10. Hộp thoại **Query Filter**, đánh dấu chọn cả 2 ô **Critical** và **Error**. Bung **Event logs,** đánh dấu chọn **Windows Logs**, và chọn **OK** 2 lần.



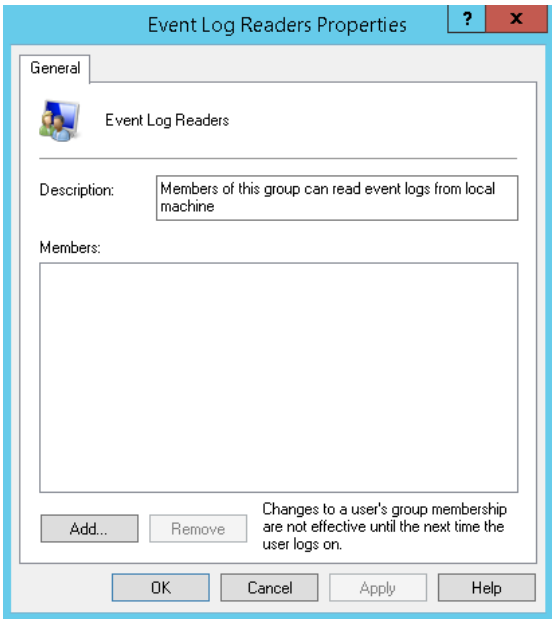

11. Trong cửa sổ **Server Manager**, chọn **Toronto Servers**, chuột phải **TOR-SS1**, chọn **Computer Management**.



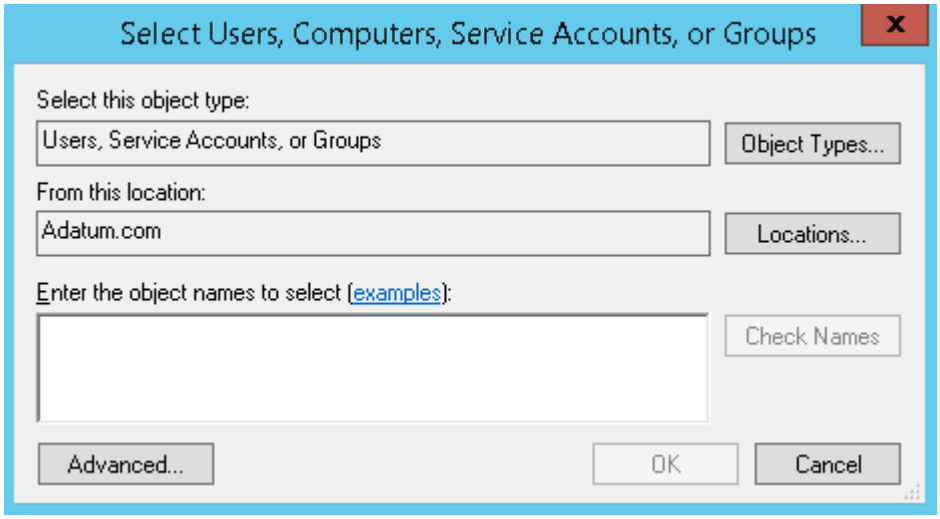
12. Trong cửa sổ **Computer Management**, bung **Local Users and Groups**, chọn **Groups**, chuột phải lên group **Event Log Readers**, chọn **Add to Group**.




13. Hộp thoại **Event Log Readers Properties**, chọn **Add**.

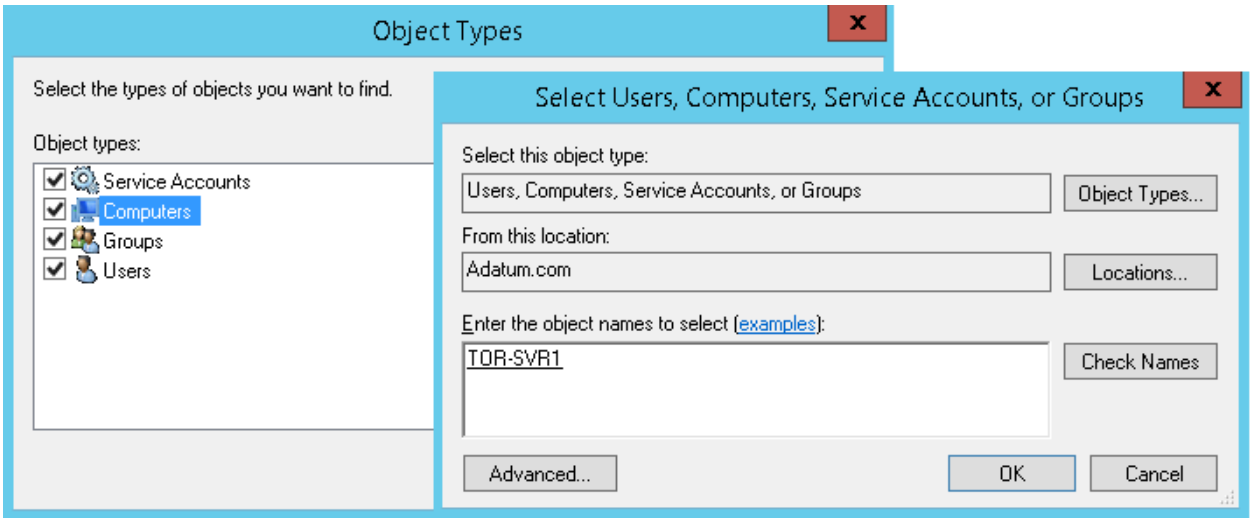


14. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, chọn **Object Types**.

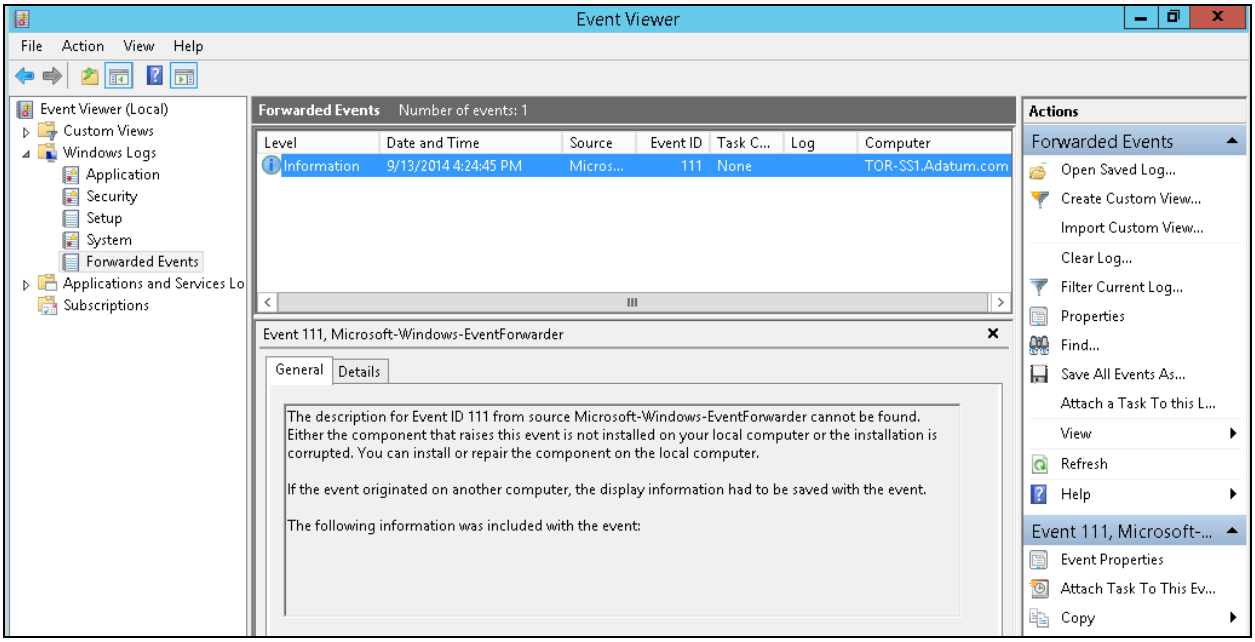



15. Hộp thoại **Object Types**, đánh dấu chọn **Computers**, và chọn **OK**.

16. Trong ô **Enter the object names to select**, nhập **TOR-SVR1**, chọn **Check Names**, và chọn **OK** 2 lần.



17. Qua cửa sổ **Event Viewer**, bung **Windows Logs,** chọn **Forwarded Events**. Sau khoảng 10 phút sẽ nhận được Event Forwarder như trong hình bên dưới.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã giám sát các servers bằng cách sử dụng các công cụ có sẵn trên Windows Server 2012.**

## Bài tập 2: Thực hiện giám sát server bằng Operations Manager

A. Datum đã triển khai một Operations Manager Server trong trung tâm dữ liệu ở London. Bây giờ bạn cần phải triển khai Operations Manager Agent cho các server trong trung tâm dữ liệu ở London.

❖ **Bài thực hành bao gồm các bước:**

1. Triển khai Operations Manager Agent.
2. Cấu hình Agentless Monitoring.

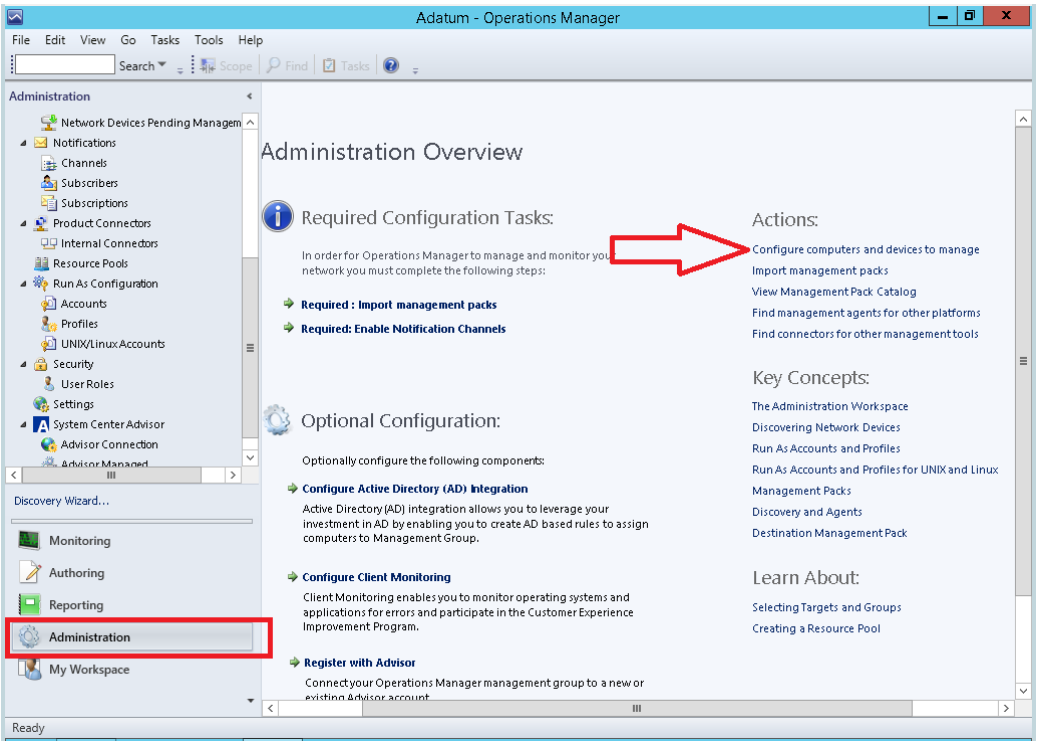
❖ **Thực hiện**

## Bước 1: Triển khai Operations Manager Agent.

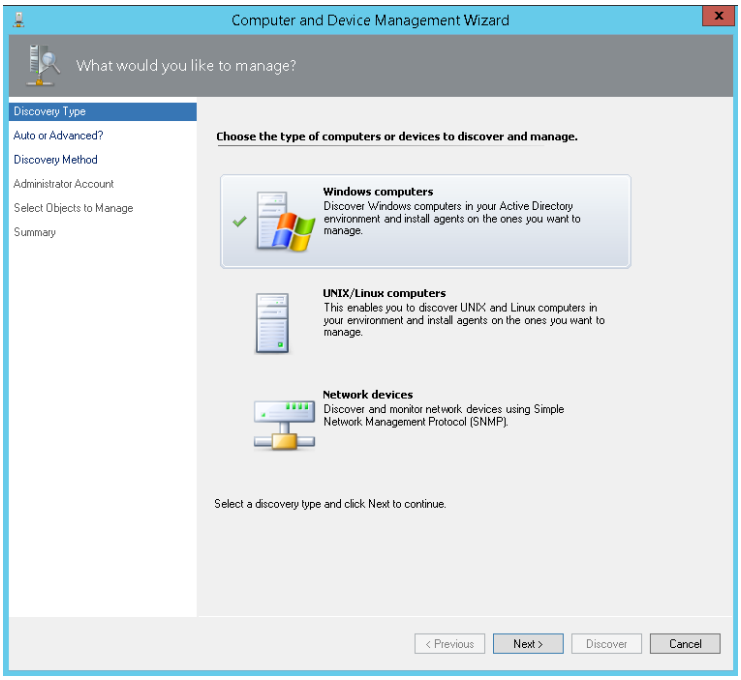
1. Trên máy **LON-OM1**, trên thanh task bar, mở **Operations Manager Console**.



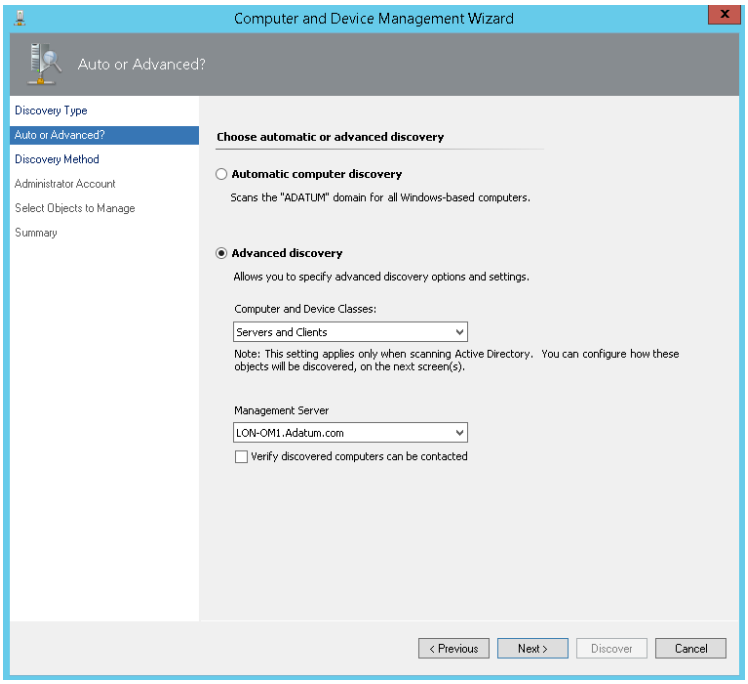

2. Trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Configure computers and devices to manage**.



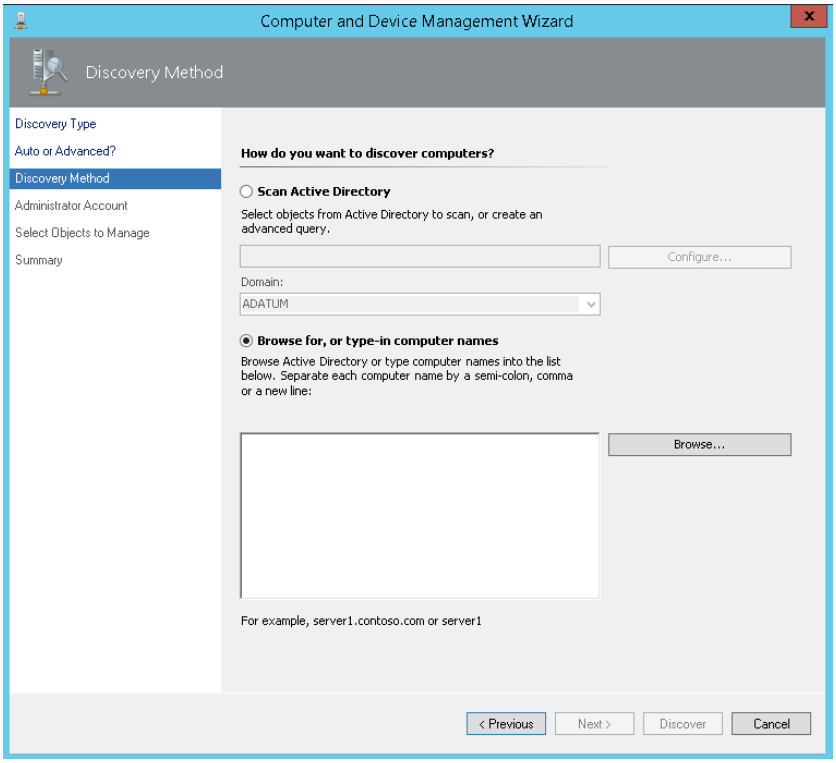
3. Cửa sổ **Discovery Type**, chọn **Windows computers**, chọn **Next**.



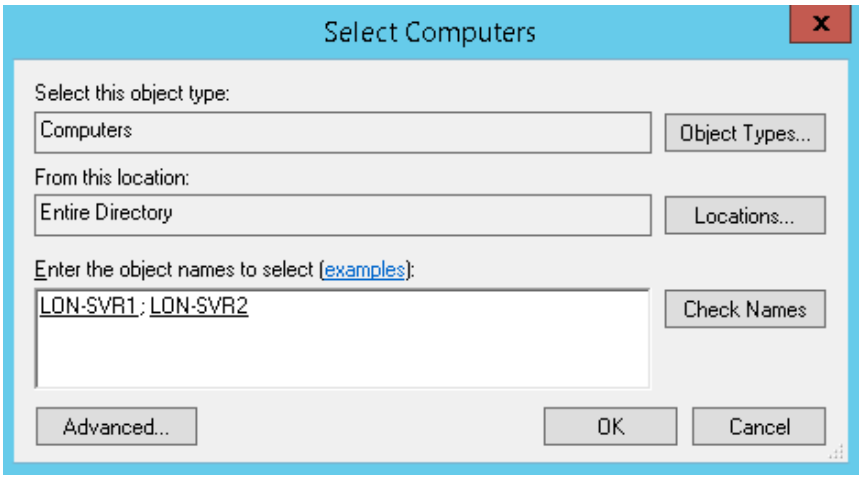

4. Cửa sổ **Auto or Advanced?**, chọn **Advanced discovery**, chọn **Next**.



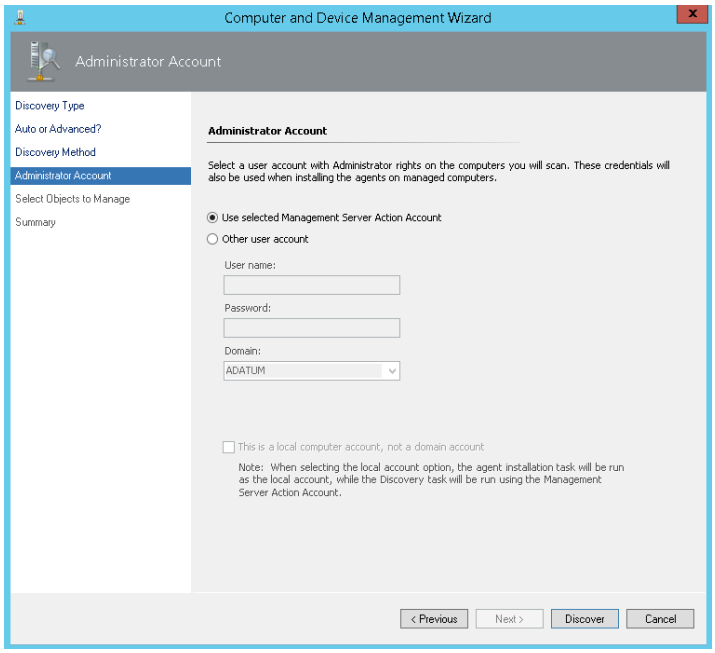
5. Cửa sổ **Discovery Method**, chọn **Browse for, or type-in computer names**, chọn **Browse**.



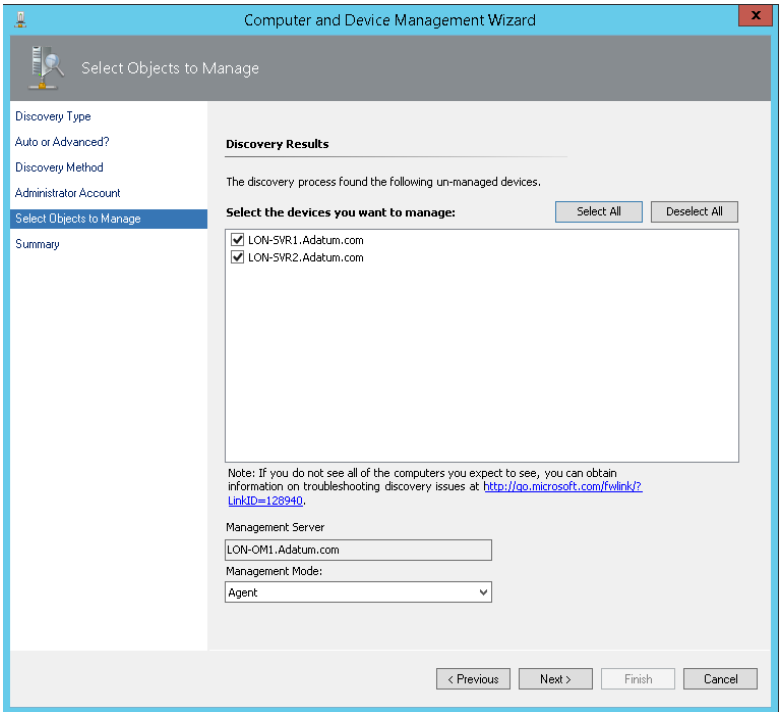

6. Hộp thoại **Select Computers**, nhập **LON-SVR1; LON-SVR2**, chọn **Check Names**, và chọn **Next**.



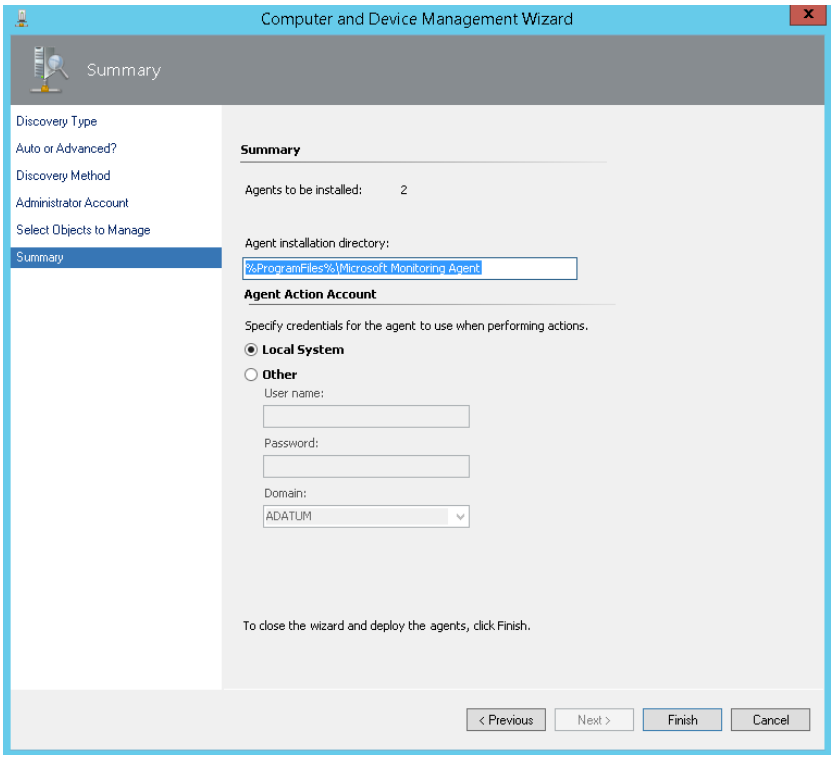
7. Cửa sổ **Administrator Account**, chọn **Discover**.



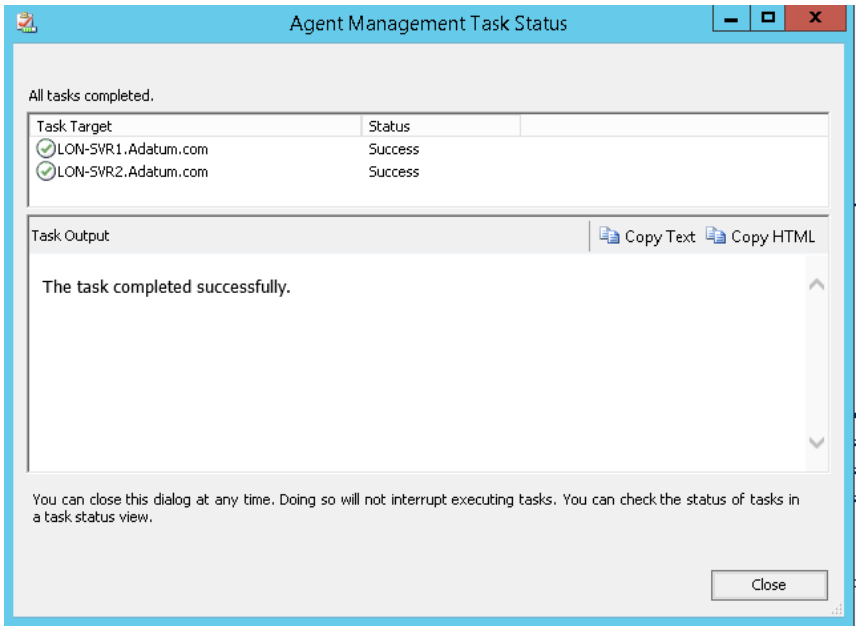

8. Cửa sổ **Select Objects to Manage**, chọn **Select All**, và chọn **Next**.



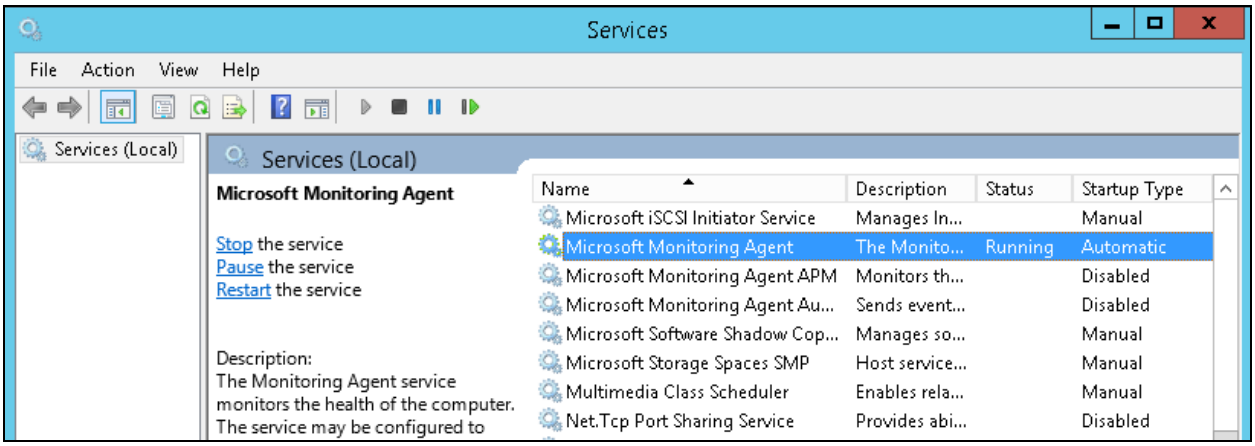
9. Cửa sổ **Summary**, chọn **Finish**.




10. Cửa sổ **Agent Management Task Status**, sau khi cấu hình thành công, chọn **Close**.

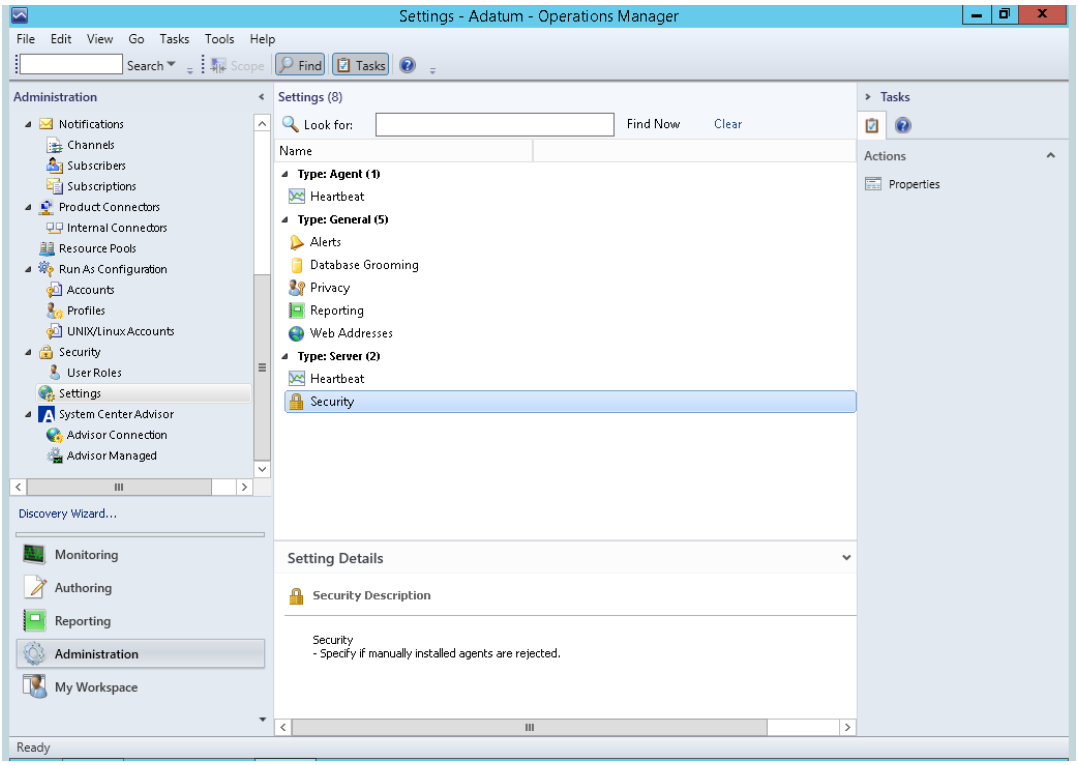


11. Qua máy **LON-SVR1**, trong **Server Manager**, bung menu Tools, mở **Services**. Kiểm tra service **Microsoft Monitoring Agent** đã được start (Status: Running).

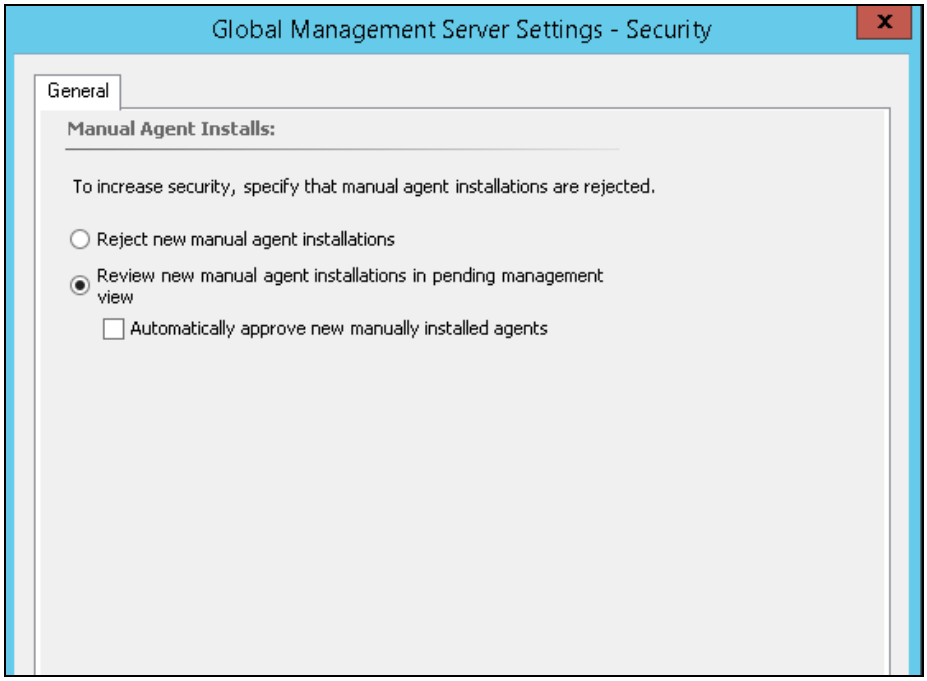



## Bước 2: Cấu hình Agentless Monitoring.

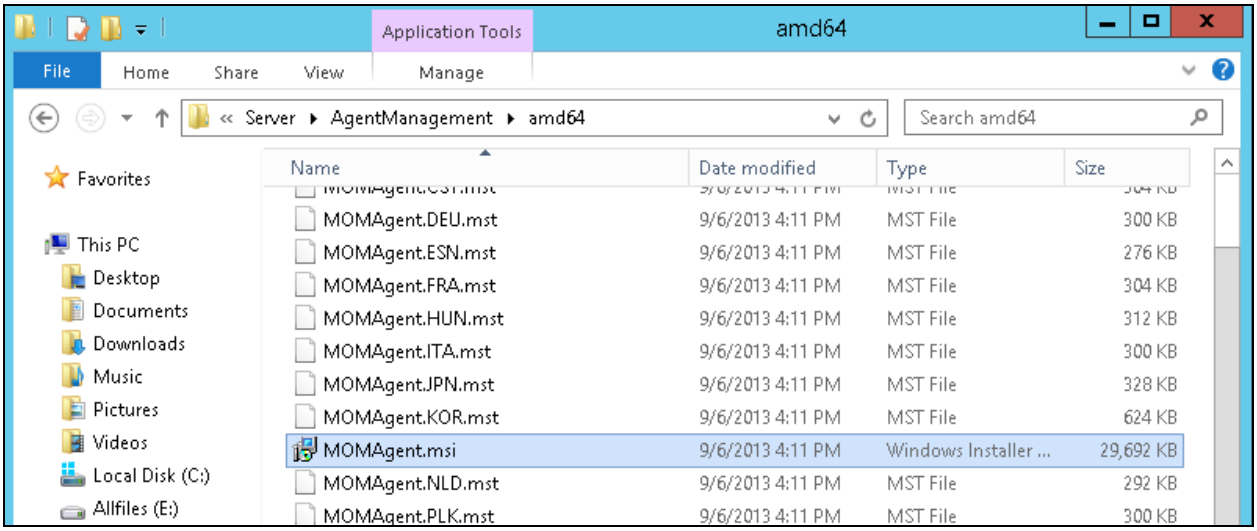
1. Trên máy **LON-OM1**, trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Settings**, nhấp đôi chuột mở mục **Security**.



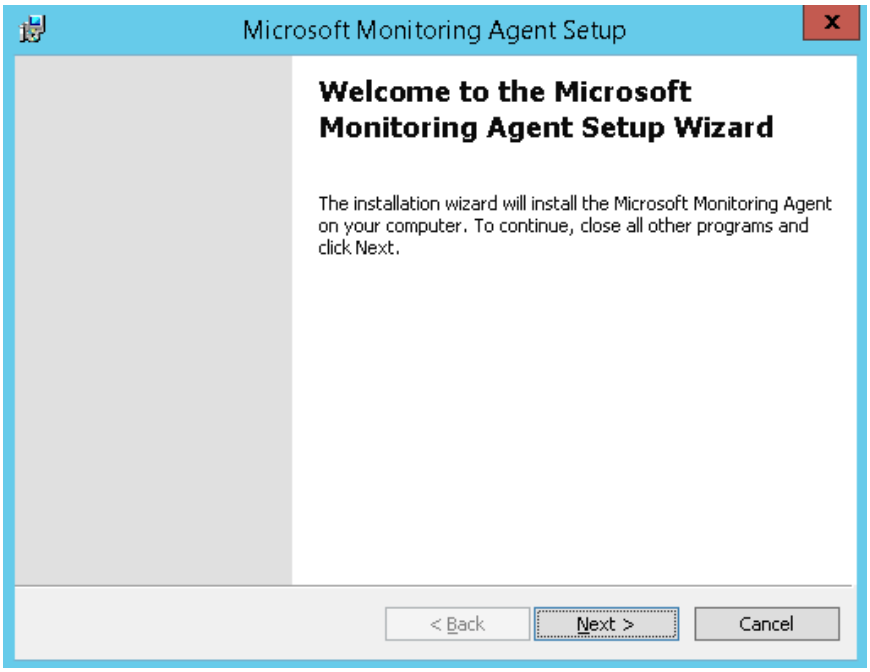
2. Hộp thoại **Global Management Server Settings – Security**, chọn **Review new manual agent installations in pending management view**, và chọn **OK**.




3. Qua máy **LON-DC1**, mở **File Explorer**, truy cập **\\LON-OM1\c$\Program Files\Microsoft System Center 2012 R2\Operations Manager\Server\AgentManagement\amd64**, nhấp đôi chuột lên file **MOMAgent.msi**.



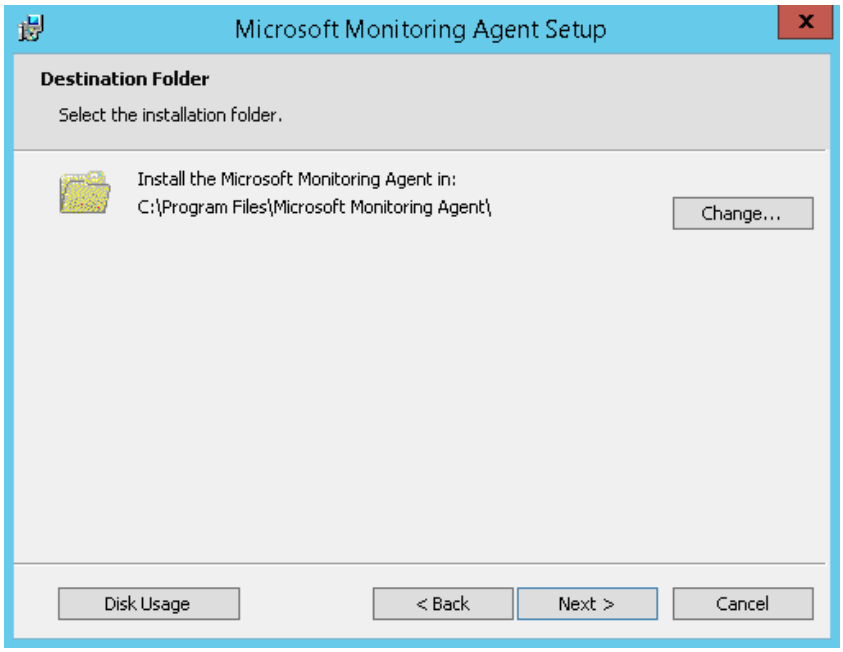
4. Cửa sổ **Microsoft Monitoring Agent Setup**, click **Next**.




5. Cửa sổ **Important Notice**, chọn **I Agree**.



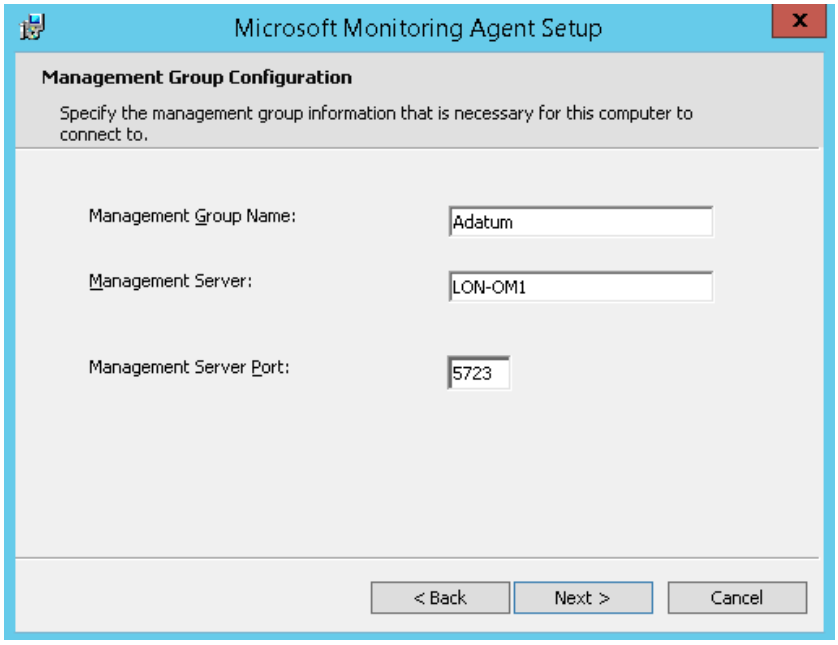
6. Cửa sổ **Destination Folder**, chọn **Next**.



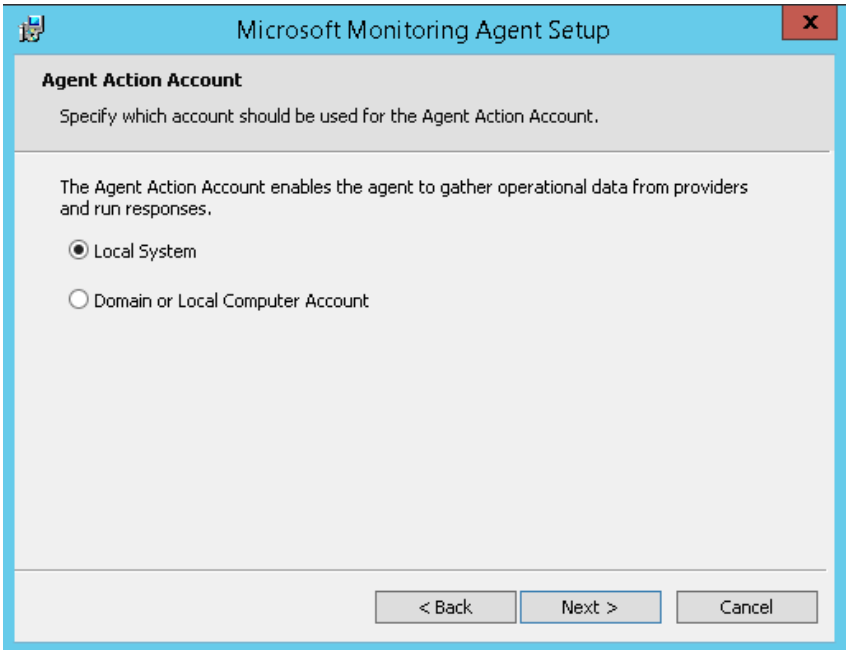

7. Cửa sổ **Agent Setup Options**, chọn **Next**.



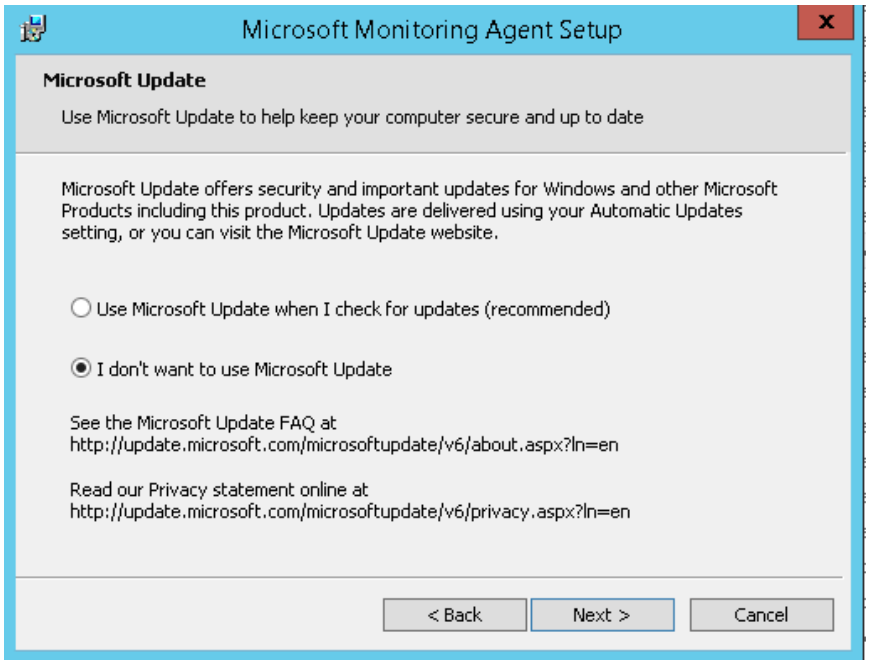
8. Cửa sổ **Management Group Configuration**, trong ô **Management Group Name**, nhập **Adatum**, trong ô **Management Server**, nhập **LON-OM1**, và chọn **Next**.



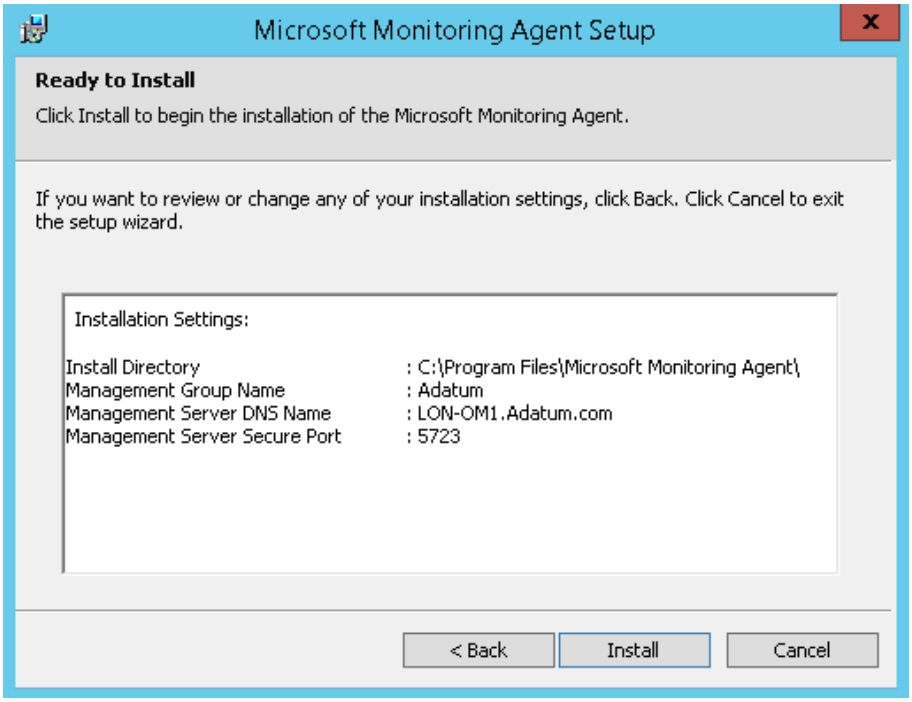

9. Cửa sổ **Agent Action Account**, chọn **Local System**, chọn **Next**.



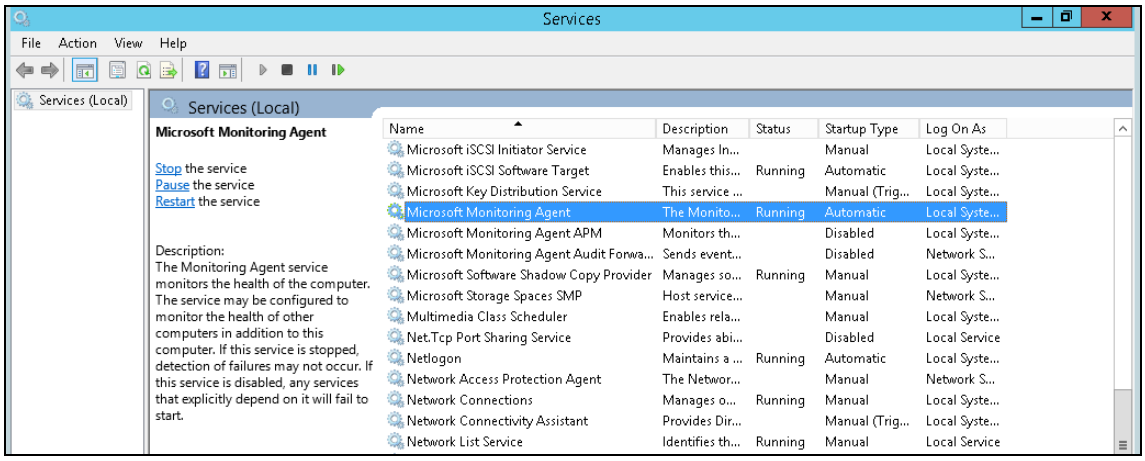
10. Cửa sổ **Microsoft Update,** chọn **Next**.



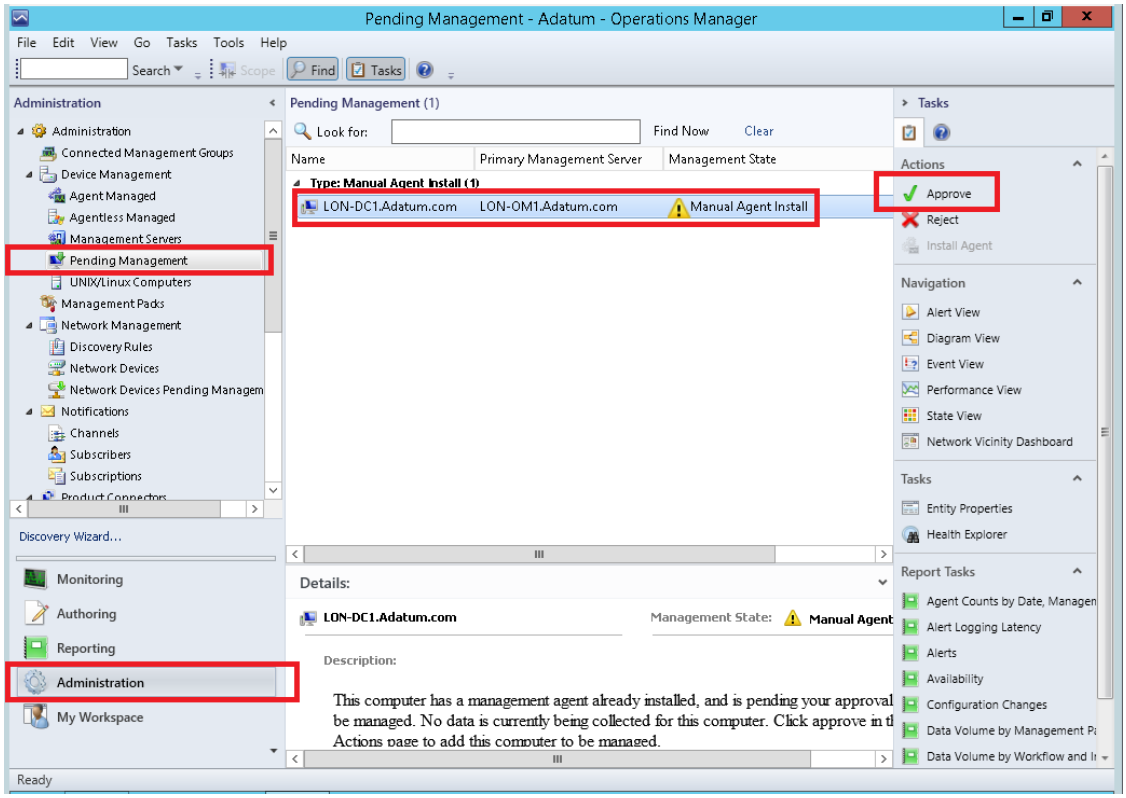

11. Cửa sổ **Ready to Install**, chọn **Install**. Sau khi cài đặt thành công, chọn **Finish**.



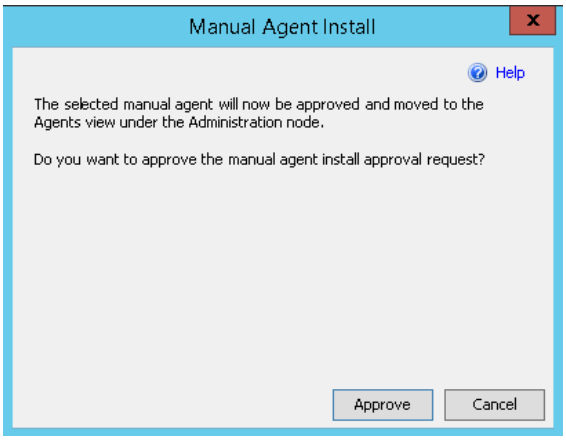
12. Trong **Server Manager**, bung menu Tools, mở **Services**. Kiểm tra service **Microsoft Monitoring Agent** đã được start (Status: Running).




13. Qua máy **LON-OM1**, trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Pending Management**, chọn **LON-DC1.Adatum.com**, chọn **Approve**.

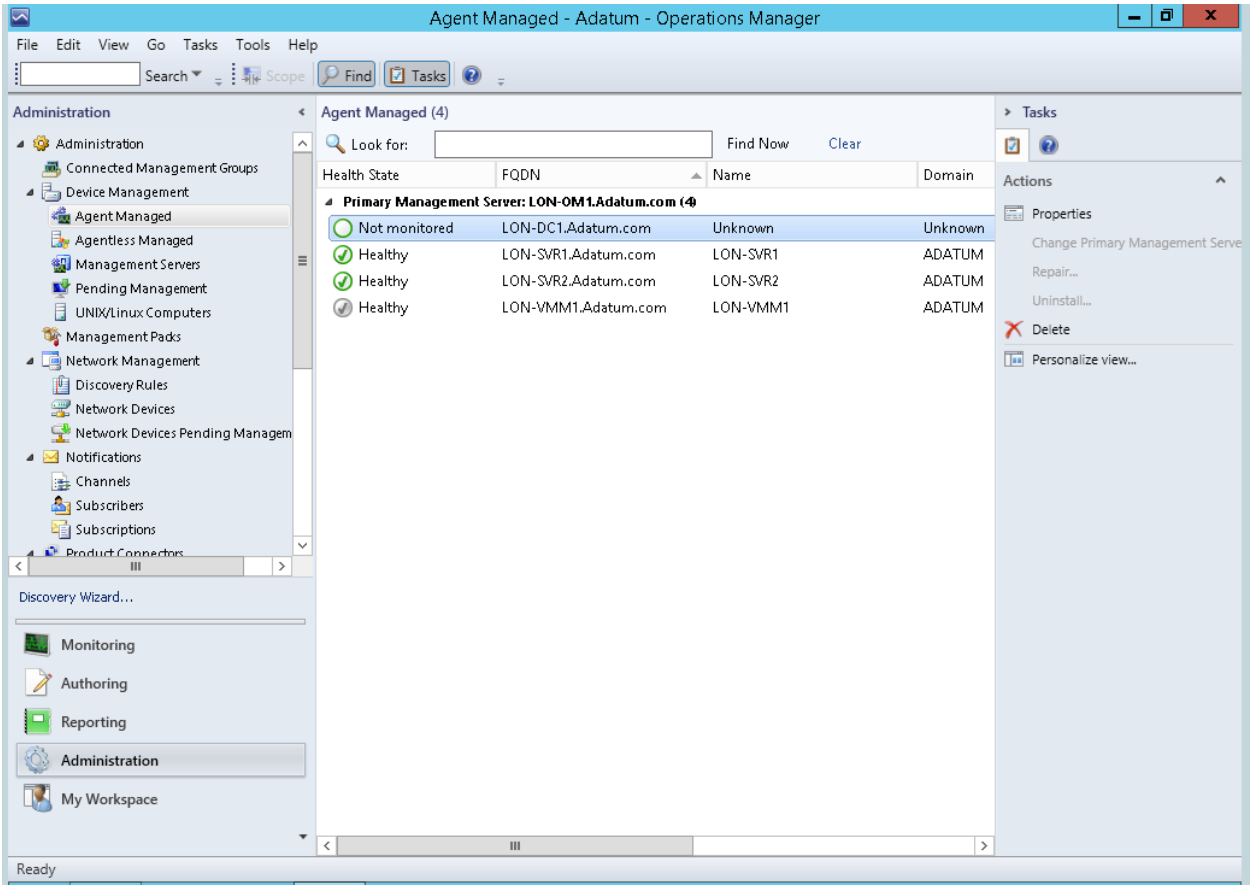


14. Hộp thoại **Manual Agent Install**, chọn **Approve**.




15. Chọn **Administration**, chọn **Agent Managed**. Kiểm tra đã hiển thị máy **LON-DC1**.

**Chú ý:** Sau khoảng 5-10 phút, trạng thái của **LON-DC1** sẽ hiển thị là **Not monitored**.



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai cài đặt thành công Operations Manager Agent cho các Server trong truy tâm dữ liệu ở London.**

## Bài tập 3: Cấu hình các thành phần giám sát trong Operations Manager

Sau khi triển khai Operations Manager Agent thành công, bước tiếp theo bạn sẽ triển khai và cấu hình các thành phần giám sát trong Operations Manager

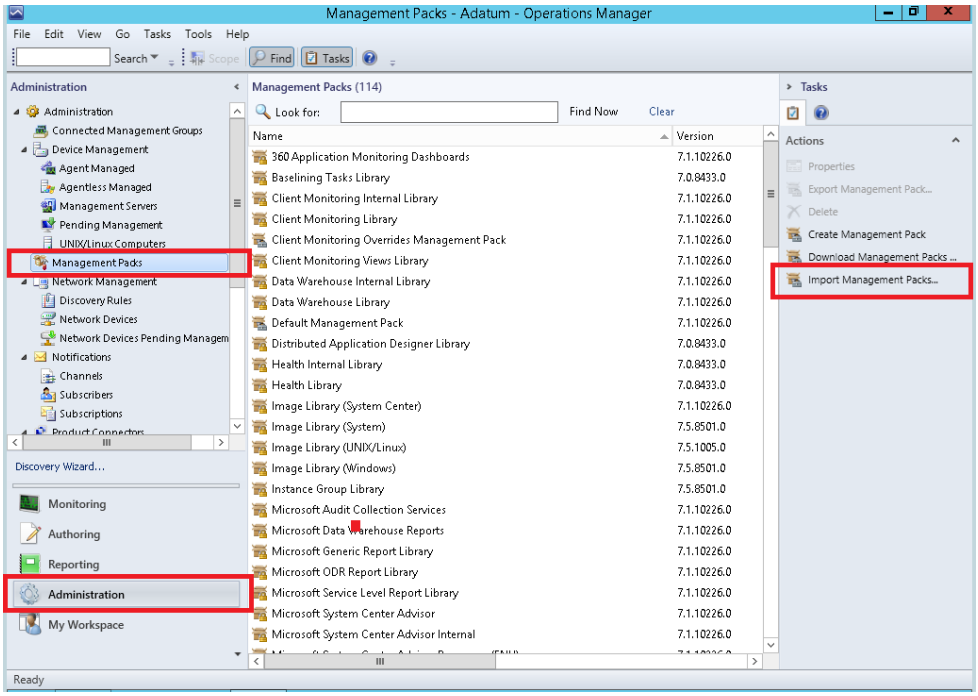
❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt và cấu hình Management Packs.
2. Cấu hình Notifications, Subscribers, và Subscriptions.
3. Giám sát hiệu suất của Server.

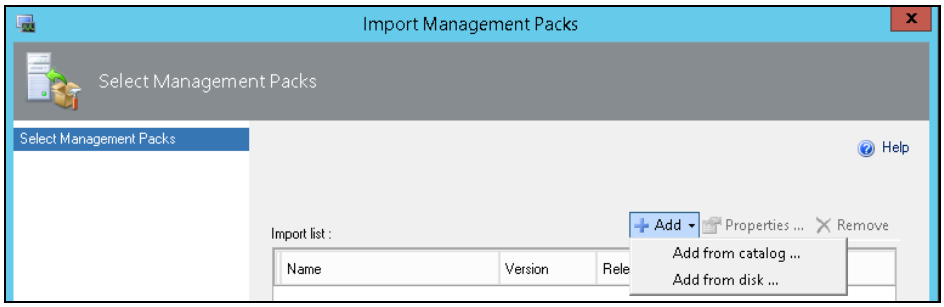
❖ **Thực hiện:**

### Bước 1: Cài đặt và cấu hình Management Packs.

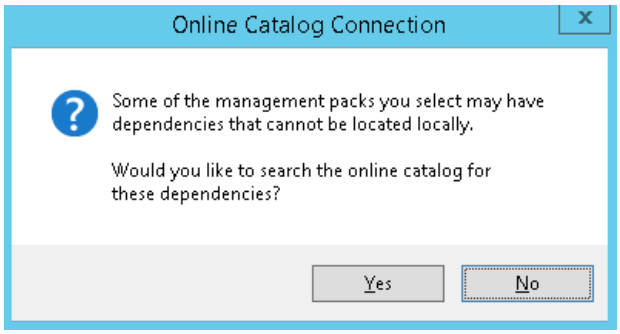
1. Trên máy **LON-OM1**, trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Management Packs**, chọn **Import Management Packs**.



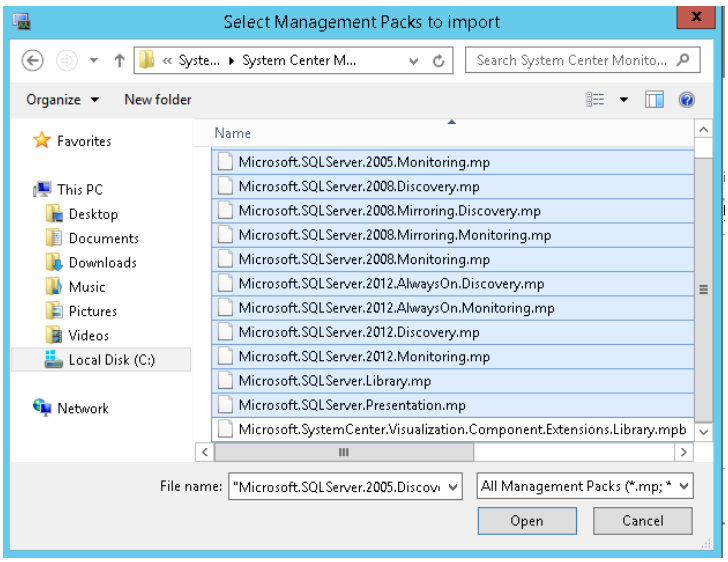
2. Hộp thoại **Import Management Packs**, chọn **Add**, và chọn **Add from disk**.



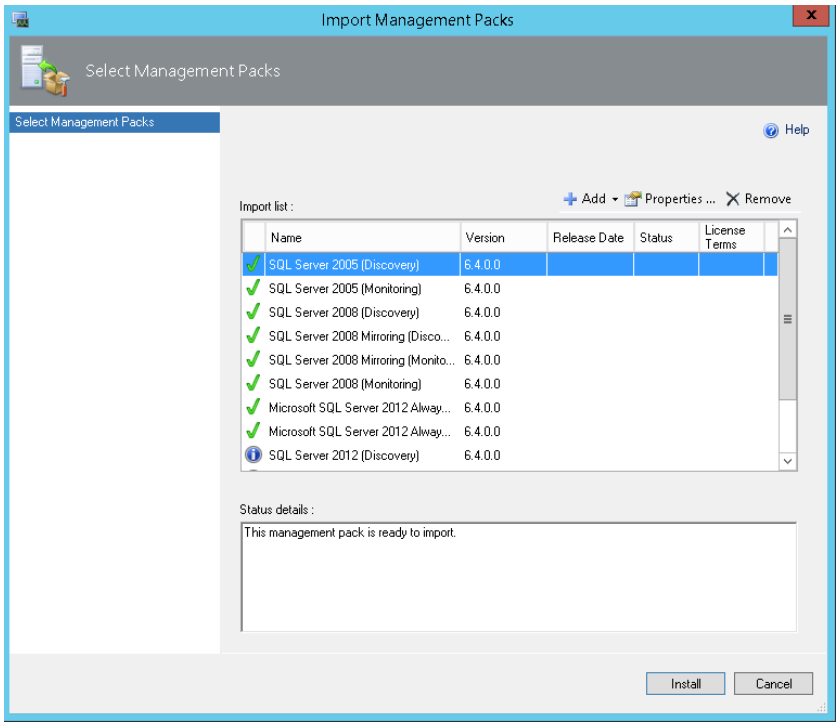

3. Hộp thoại **Online Catalog Connection**, chọn **No**.



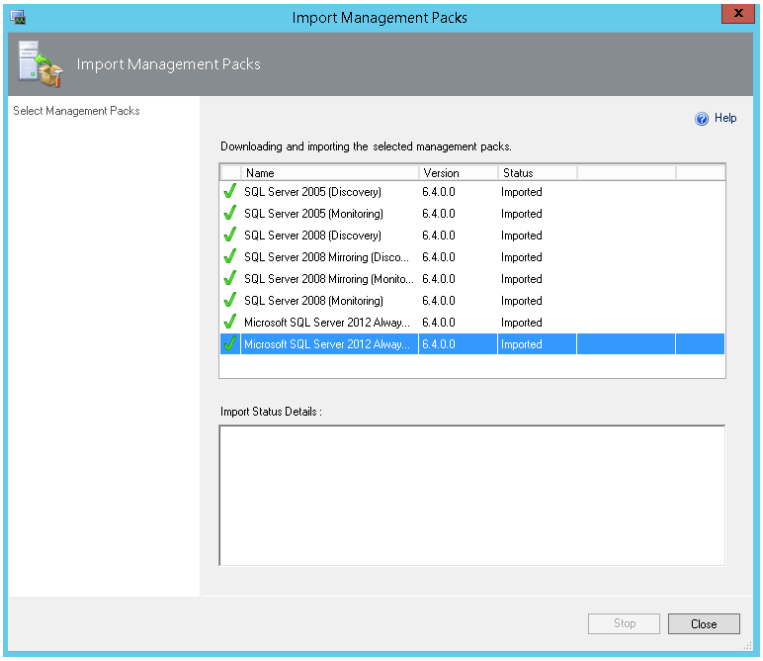

4. Hộp thoại **Select Management Packs to import**, trỏ vào đường dẫn **C:\Program Files (x86)\System Center Management Packs\System Center Monitoring Pack for SQL Server,** chọn tất cả các file có tên "**SQL Server**", và chọn **Open**.



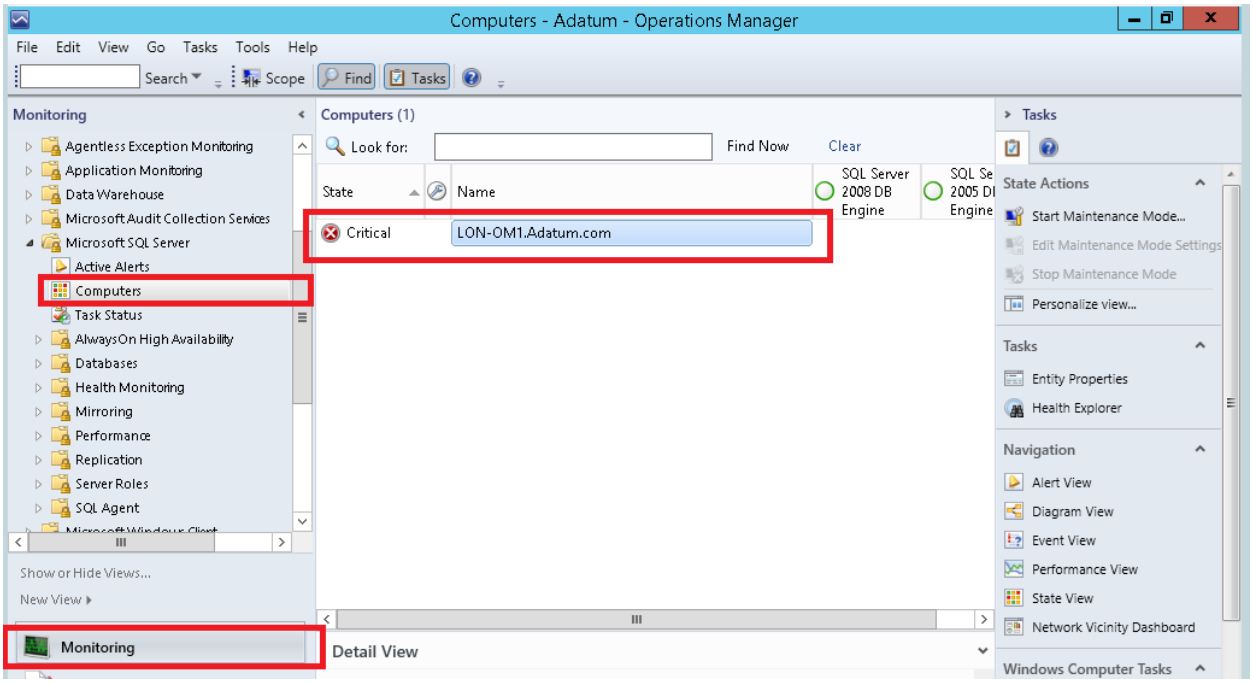
5. Hộp thoại **Select Management Packs**, chọn **Install**.



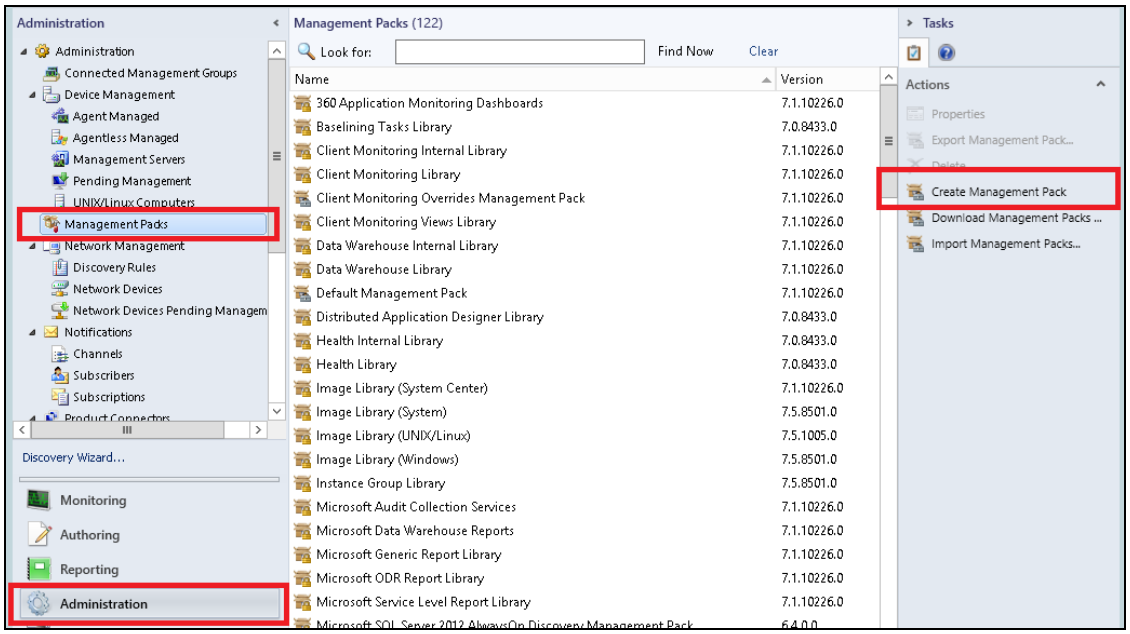

6. Sau khi import thành công, chọn **Close**.



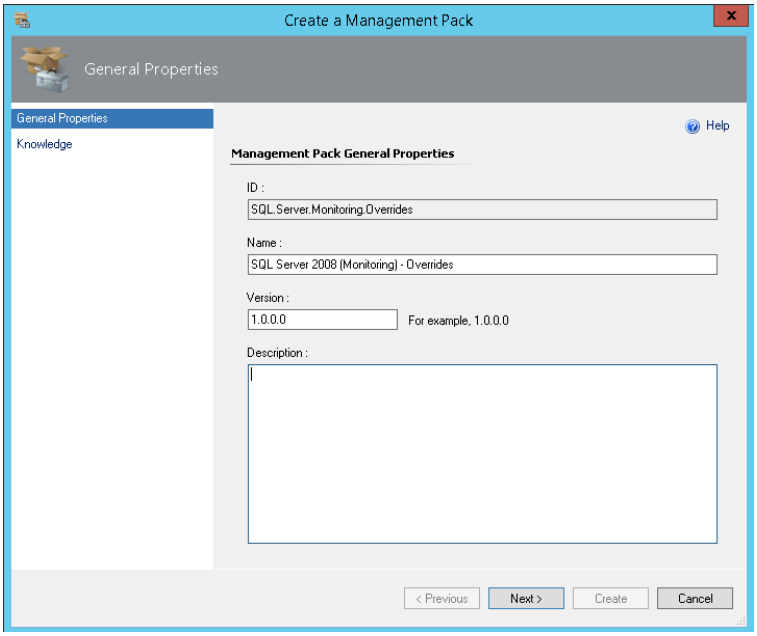
7. Trong cửa sổ **Operations Manager,** chọn **Monitoring**, bung **Microsoft SQL Server**, chọn **Computers**. Kiểm tra có máy **LON-OM1.Adatum.com** (Nếu chưa hiển thị thì đợi vài phút).



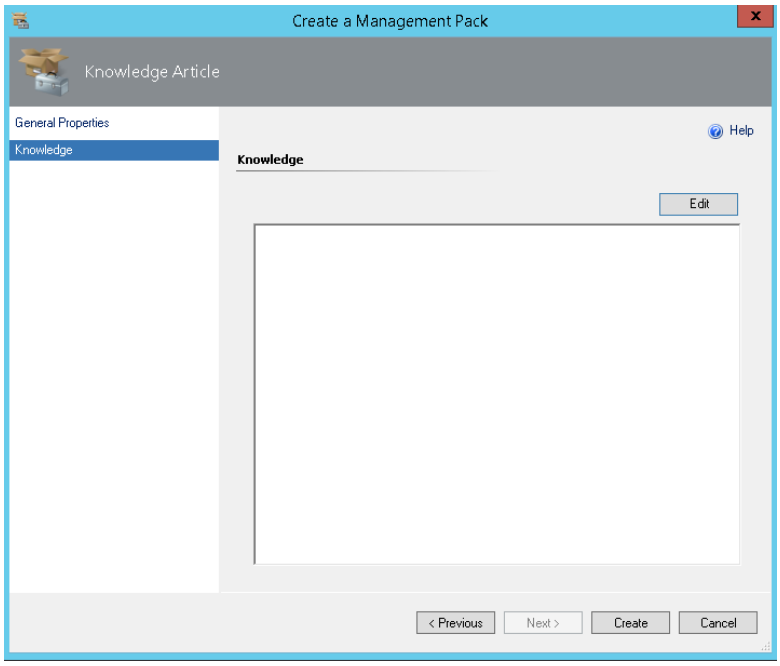
8. Trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Management Packs**, chọn **Create Management Pack**.



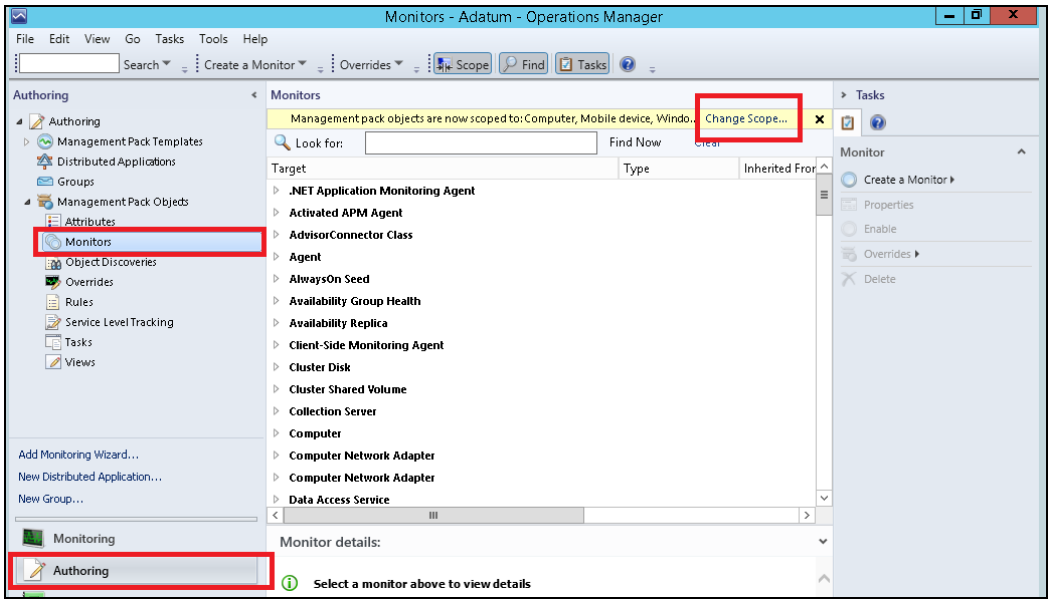

9. Cửa sổ **General Properties**, trong ô **Name**, nhập **SQL Server 2008 (Monitoring) – Overrides**, chọn **Next**.



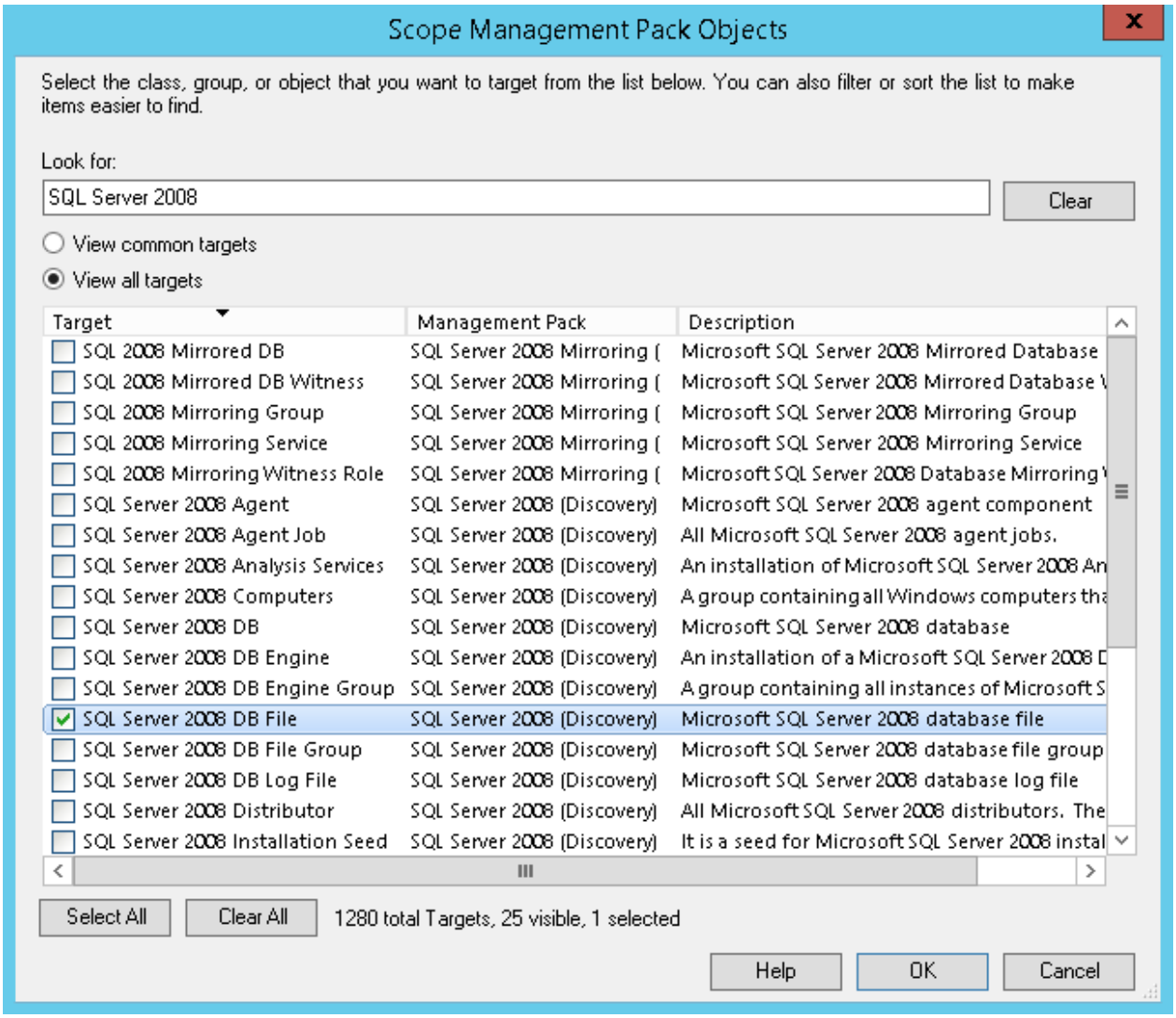
10. Cửa sổ **Knowledge**, chọn **Create**.



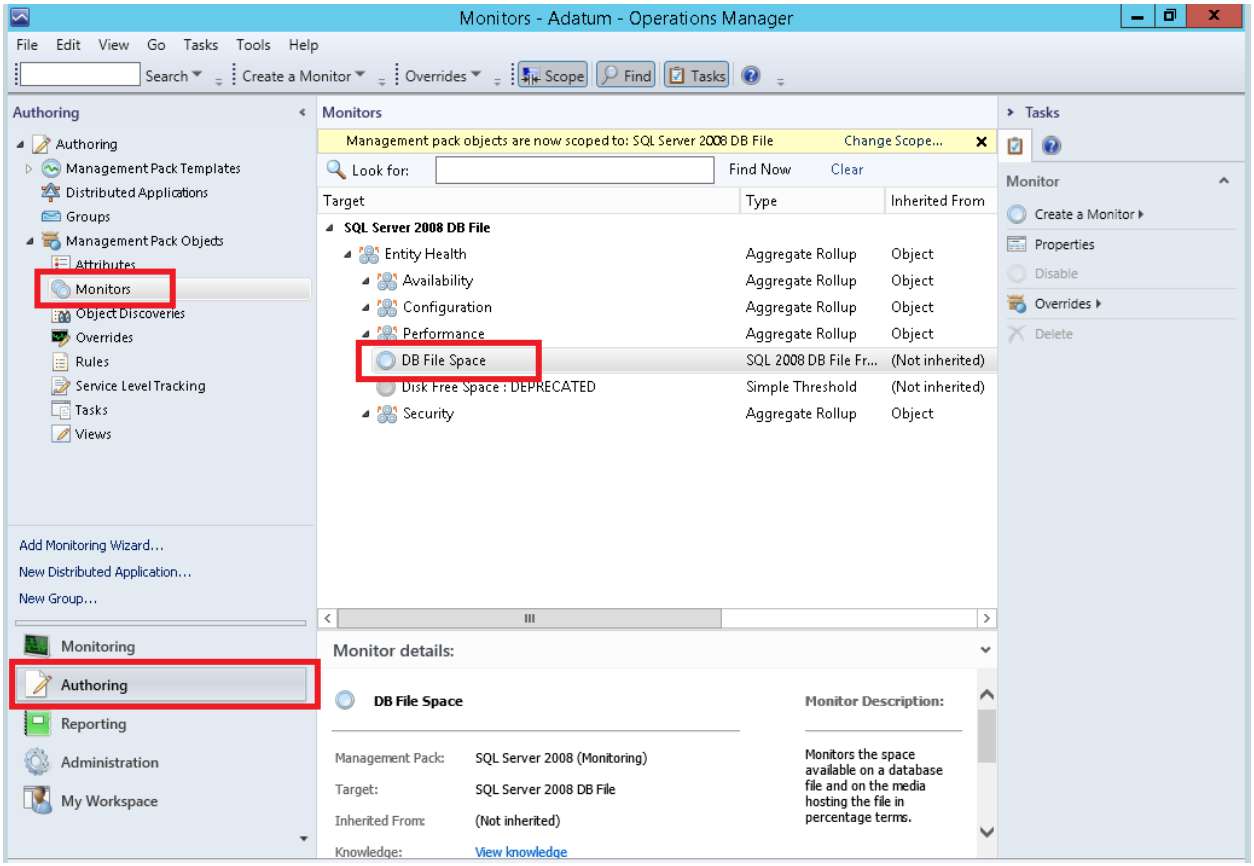

11. Trong cửa sổ **Operations Manager**, chọn **Authoring**, bung **Management Pack Objects**, nhấp đôi chuột vào mục **Monitors**, trong thanh mày vàng, chọn **Change Scope**.



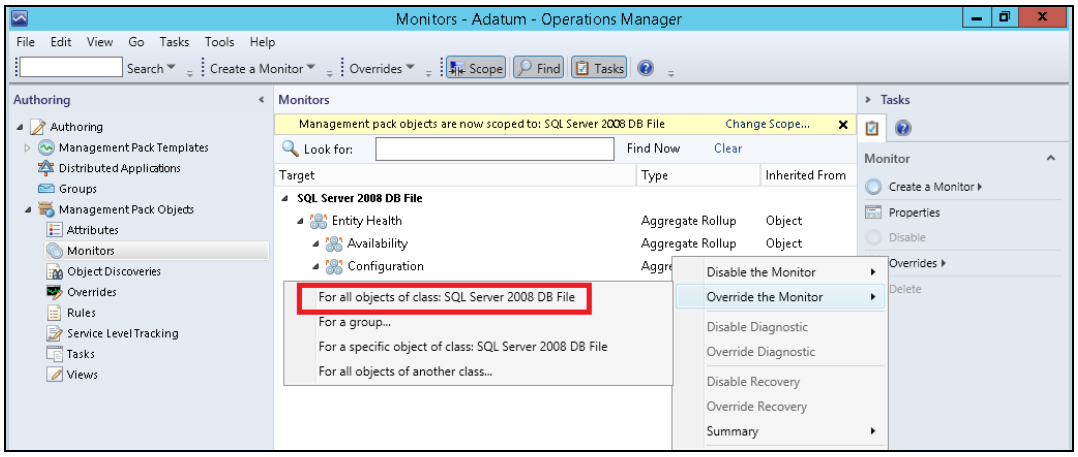
12. Hộp thoại **Scope Management Pack Objects**, chọn **Clear All**, chọn **View all targets**, trong ô **Look for**, nhập **SQL Server 2008**, đánh dấu chọn **SQL Server 2008 DB File**, và chọn **OK**.



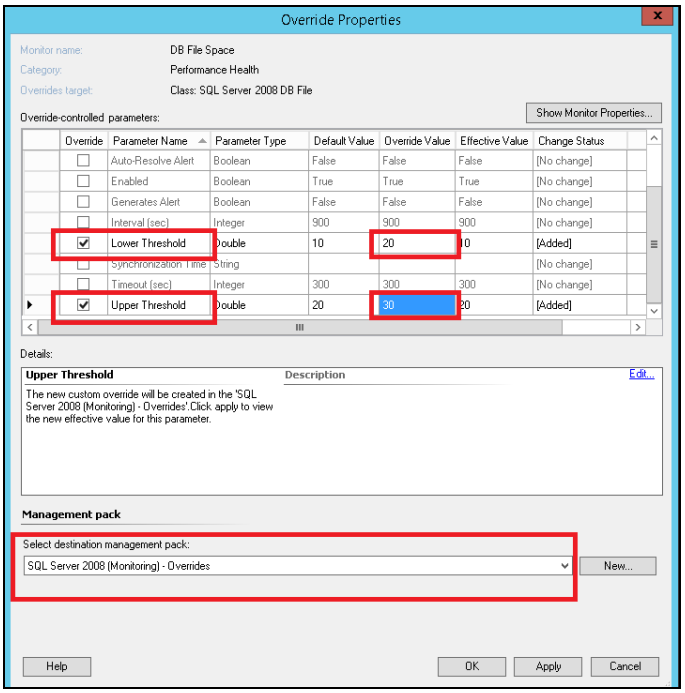
13. Bung **SQL Server 2008 DB File**, bung **Entity Health**, bung **Performance**, chọn **DB File Space**.



14. Trong cs **Tasks**, chọn **Overrides**, chọn **Override the Monitor**, và chọn **For all objects of class: SQL Server 2008 DB File**.



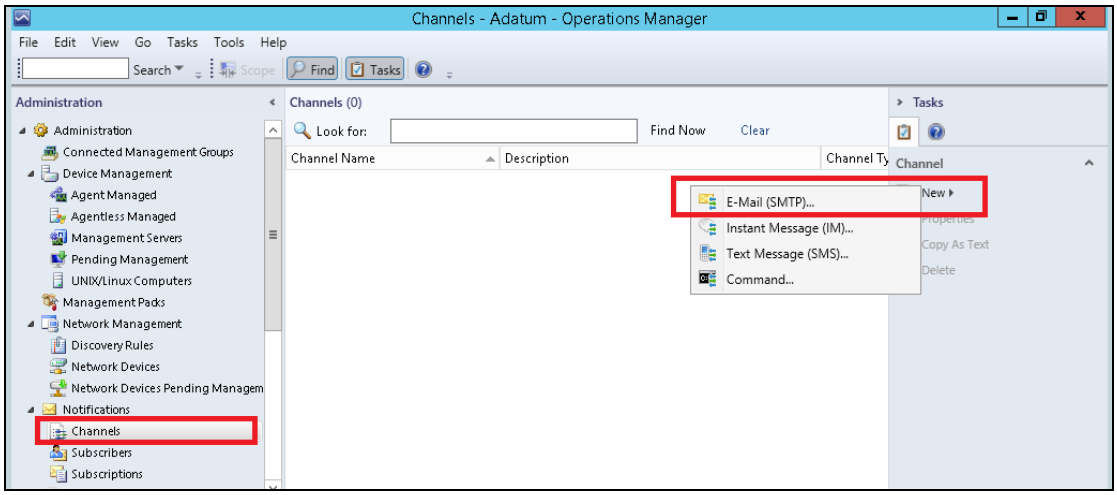

15. Hộp thoại **Overrides Properties**, đánh dấu chọn **Lower Threshold**, chỉnh **Override Value** thành **20**. Đánh dấu chọn **Upper Threshold**, chỉnh **Override Value** thành **30**. Bung ô **Select destination management pack**, chọn **SQL Server 2008 (Monitoring) – Overrides**, và chọn **OK**.



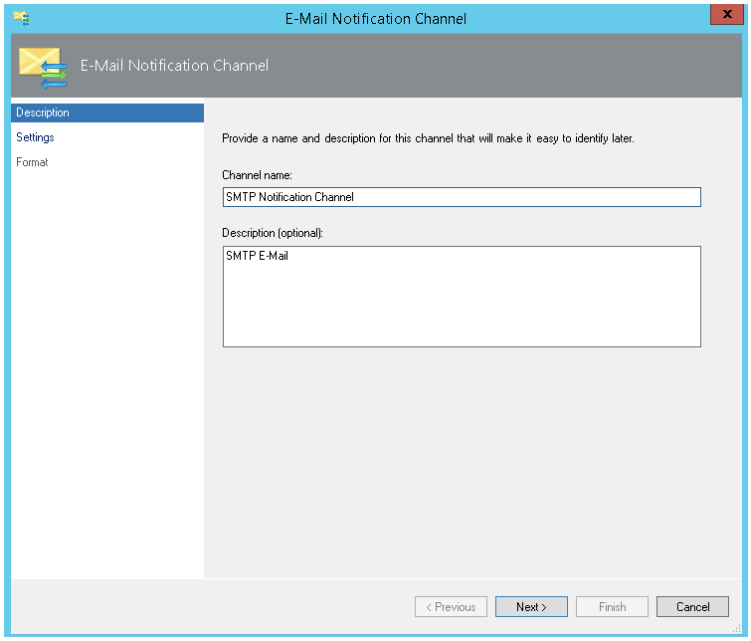
## Bước 2: Cấu hình Notifications, Subscribers, và Subscriptions.

### ➢ Cấu hình Notifications

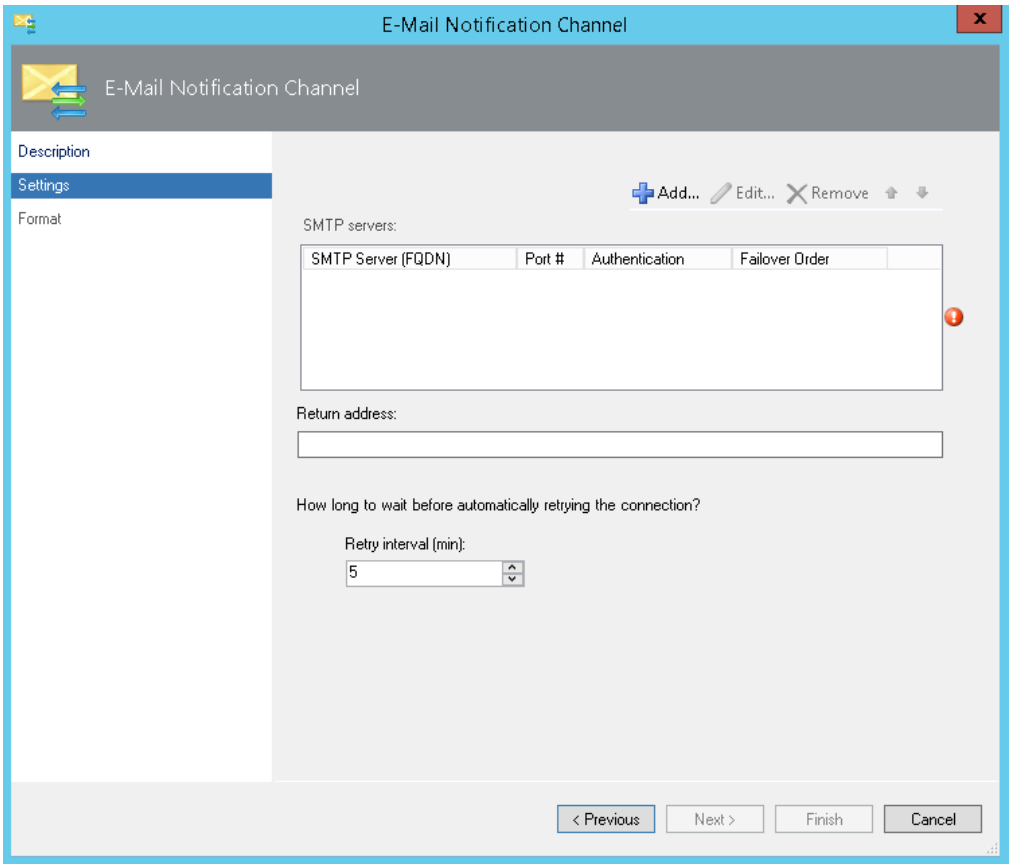
1. Trong cửa sổ **Operations Manager**, chọn **Administration**, bung **Notifications**, chọn **Channels**, chọn **New**, chọn **E-Mail (SMTP)**.



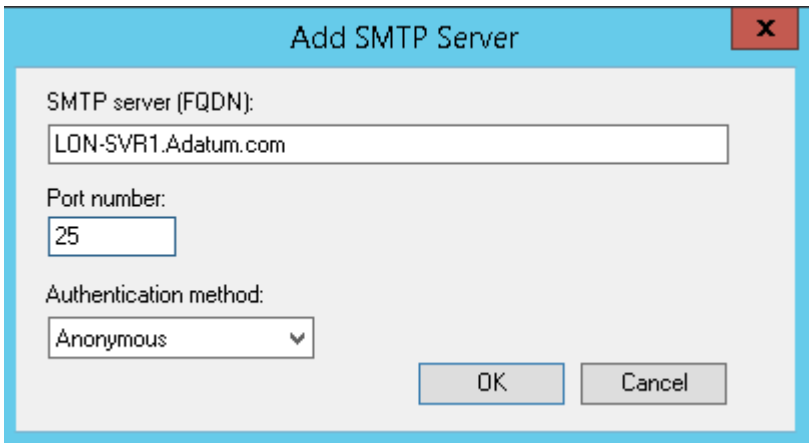

2. Cửa sổ **Description**, trong ô **Channel name**, nhập **SMTP Notification Channel**, và chọn **Next**.



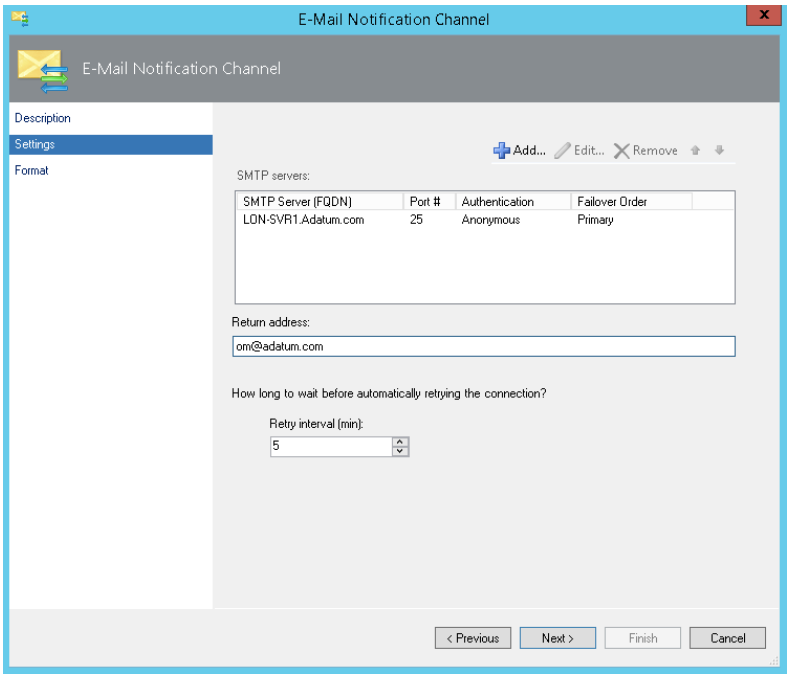
3. Cửa sổ **Settings**, chọn **Add**.



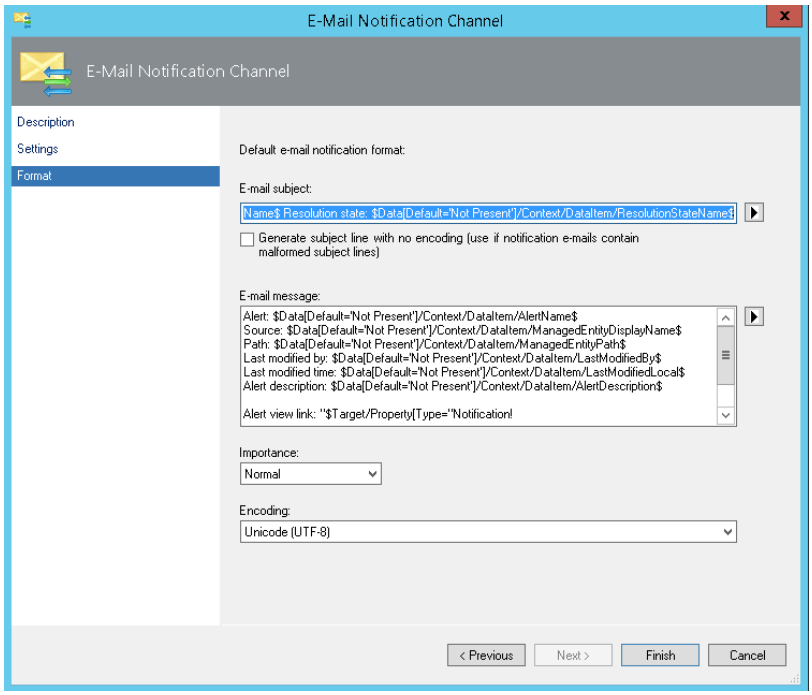

4. Hộp thoại **Add SMTP Server**, trong ô **SMTP server (FQDN)**, nhập **LON-SVR1.Adatum.com**, và chọn **OK**.



5. Cửa sổ **Settings** , trong ô **Return address**, nhập **om@adatum.com**, và chọn **Next**.

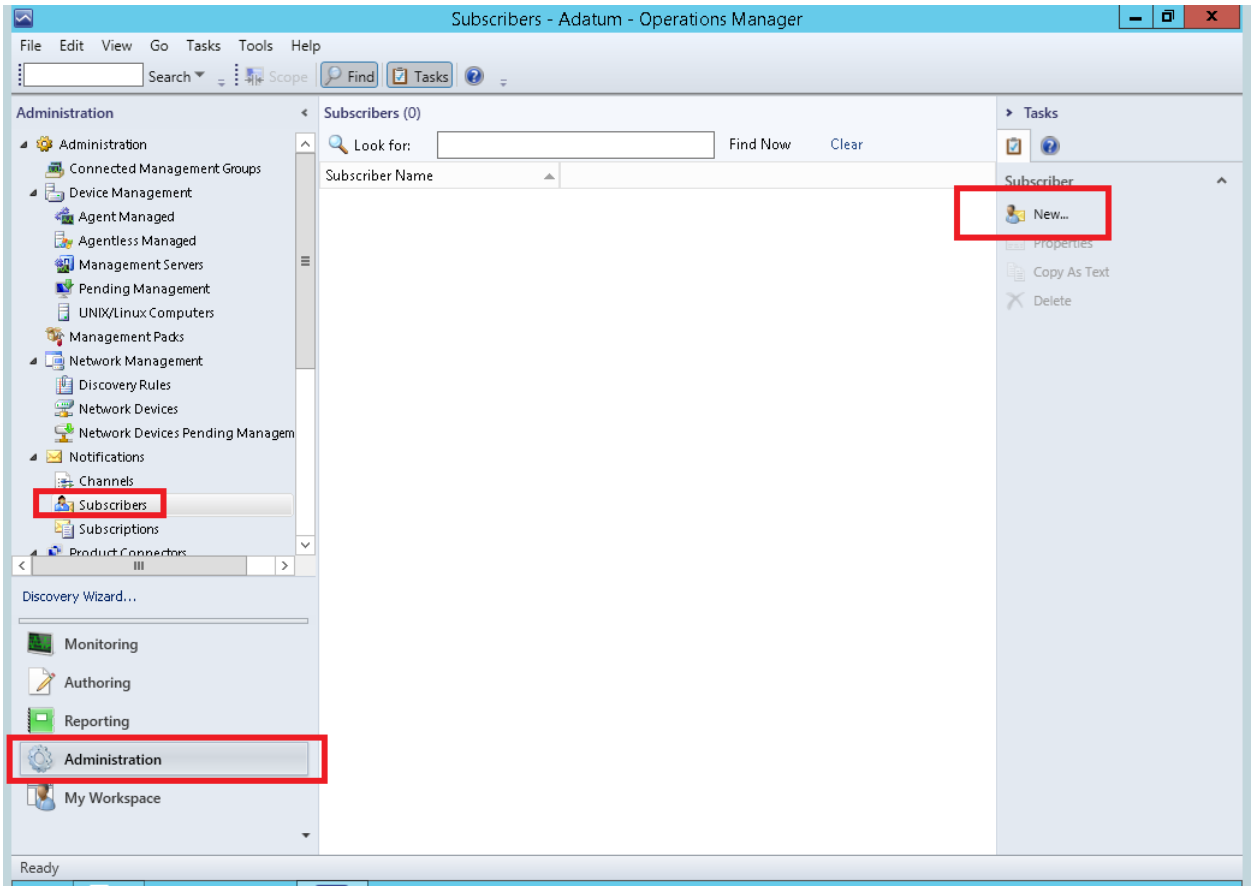



6. Cửa sổ **Format**, chọn **Finish**. Sau khi cấu hình thành công, chọn **Close**.

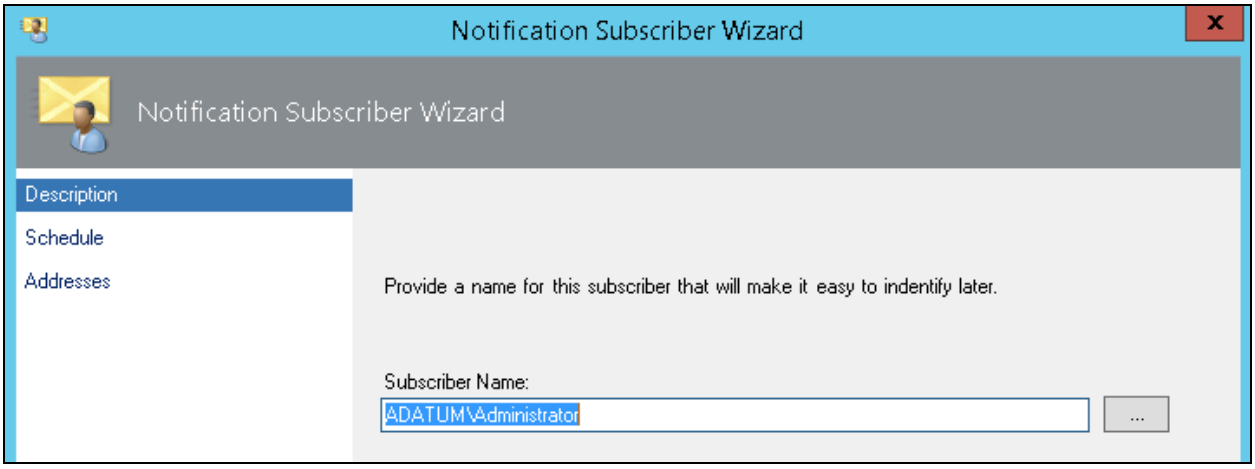


## ➢ Cấu hình Subscribers

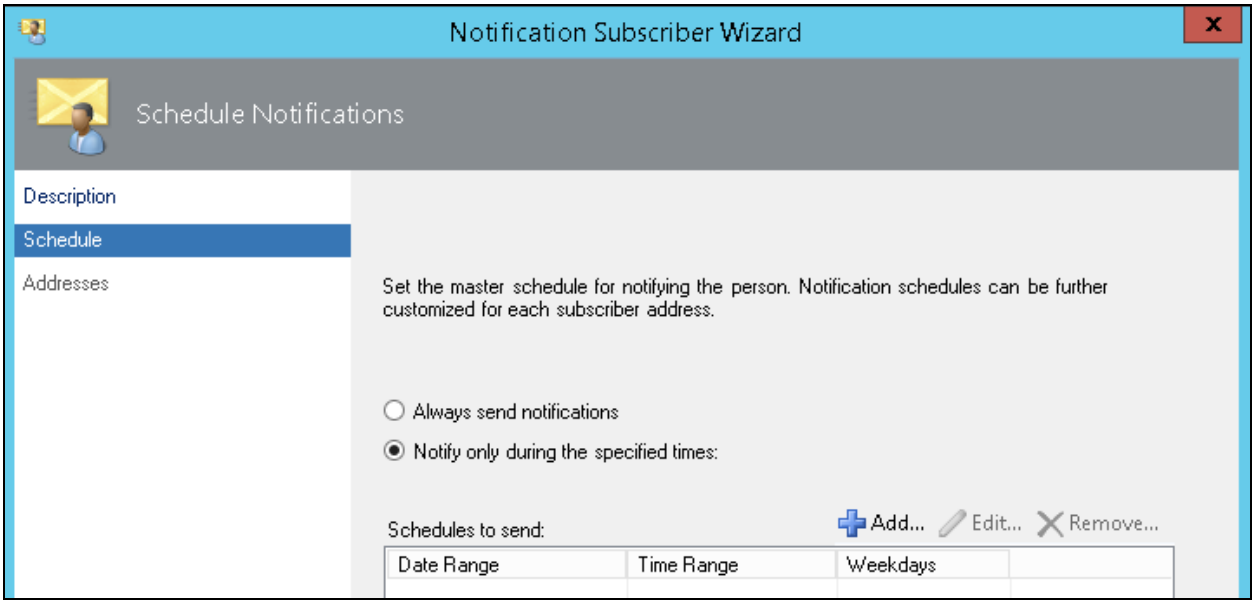
1. Trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Subscribers**, chọn **New**.



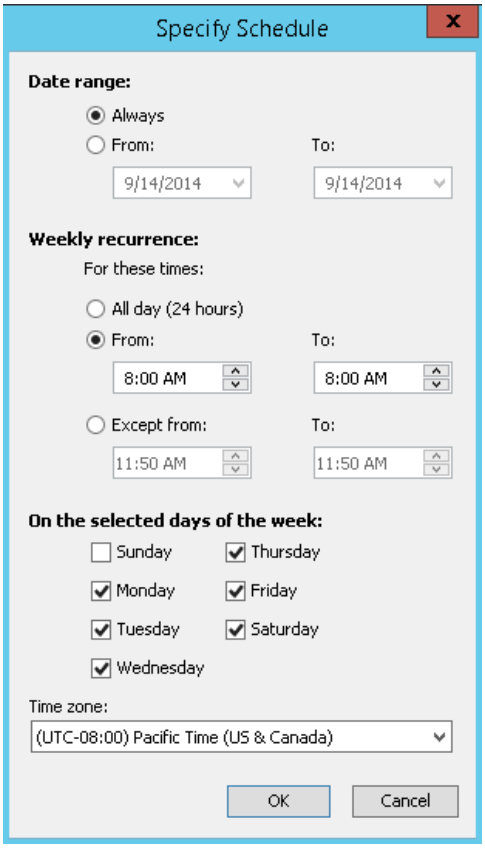
2. Cửa sổ **Description**, trong ô **Subscriber Name**, nhập **ADATUM\Administrator**, chọn **Next**.



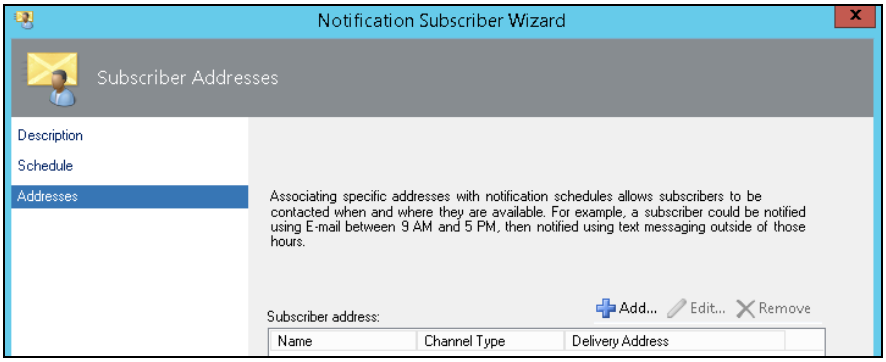

3. Cửa sổ **Schedule**, chọn **Notify only during the specified time**, chọn **Add**.



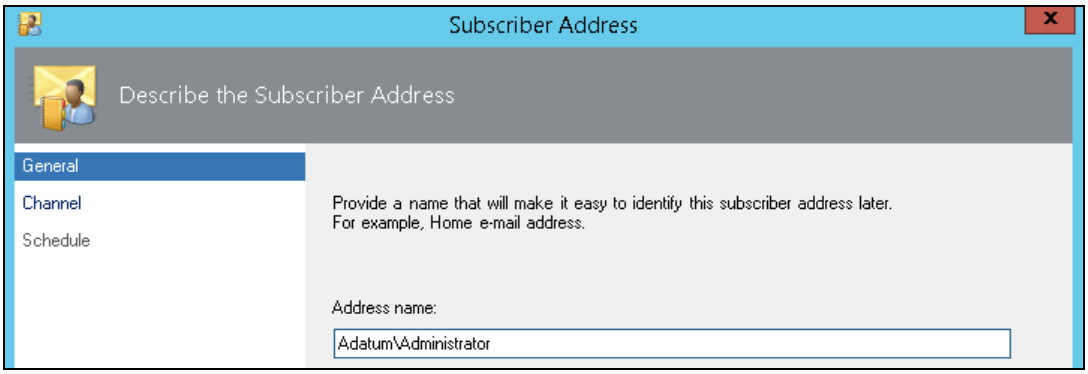
4. Hộp thoại **Specify Schedule**, trong phần **Weekly recurrence**, chọn **From**, thiết lập thời gian từ **8:00 AM** tới **8:00 PM**. Trong phần **On the selected days of the week**, đánh dấu chọn **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, chọn **OK**. Và chọn **Next**.



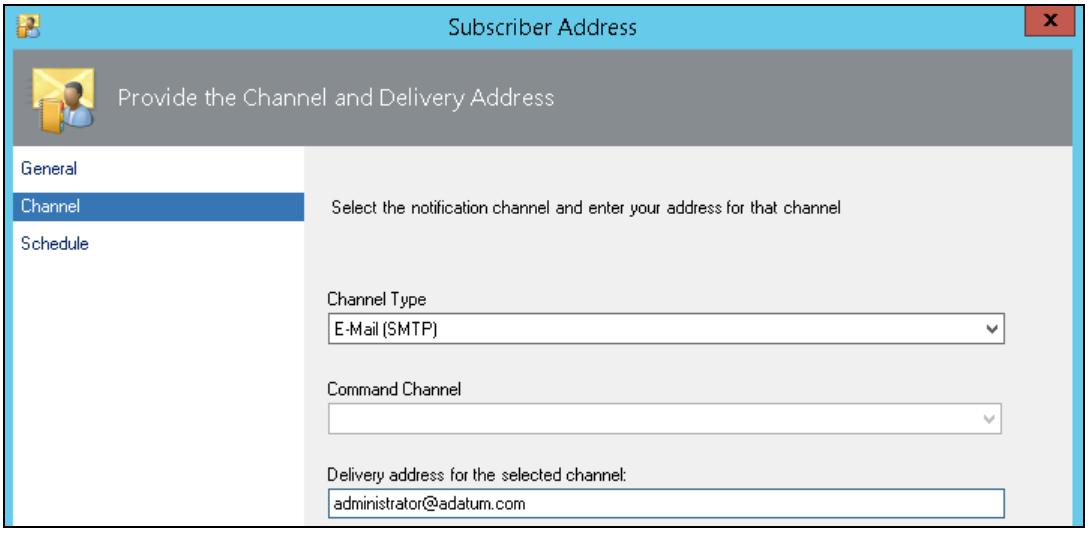

5. Cửa sổ **Addresses**, chọn **Add**.



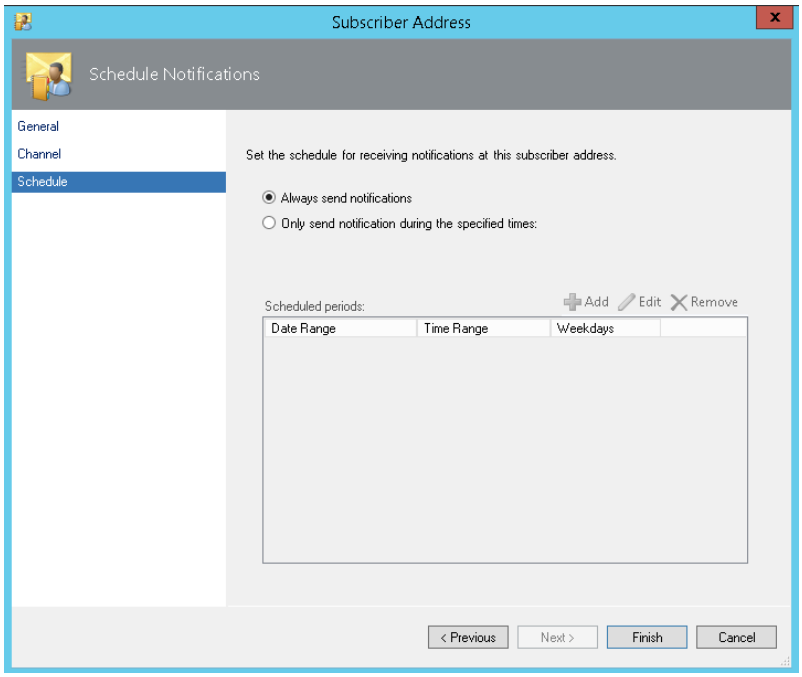
6. Cửa sổ **Describe the Subscriber Address**, trong ô **Address name**, nhập **ADATUM\Administrator**, chọn **Next**.



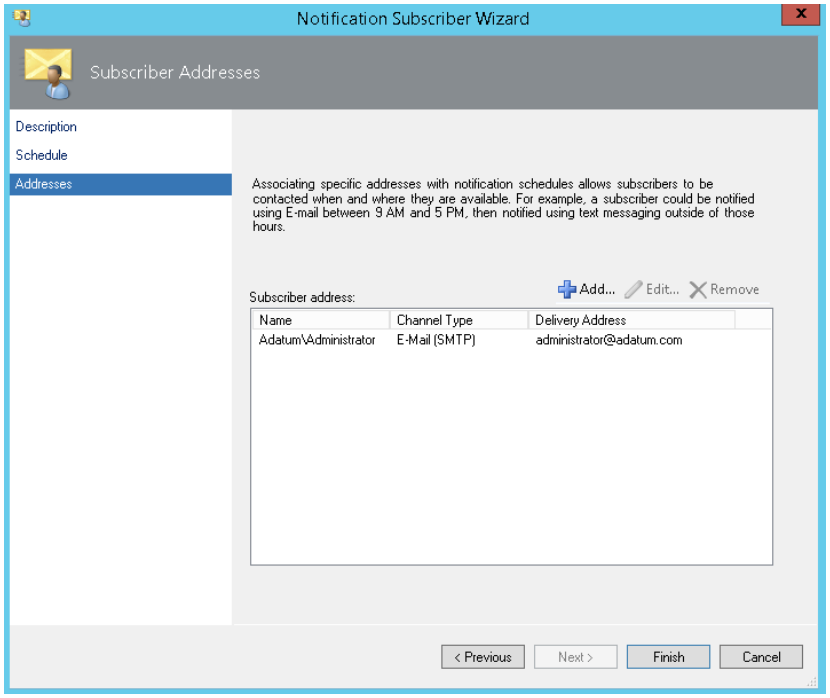

7. Bung ô **Channel Type**, chọn **E-Mail (SMTP)**, trong ô **Delivery address for selected channel**, nhập **administrator@adatum.com**, và chọn **Next**.



8. Cửa sổ **Schedule**, chọn **Finish**.

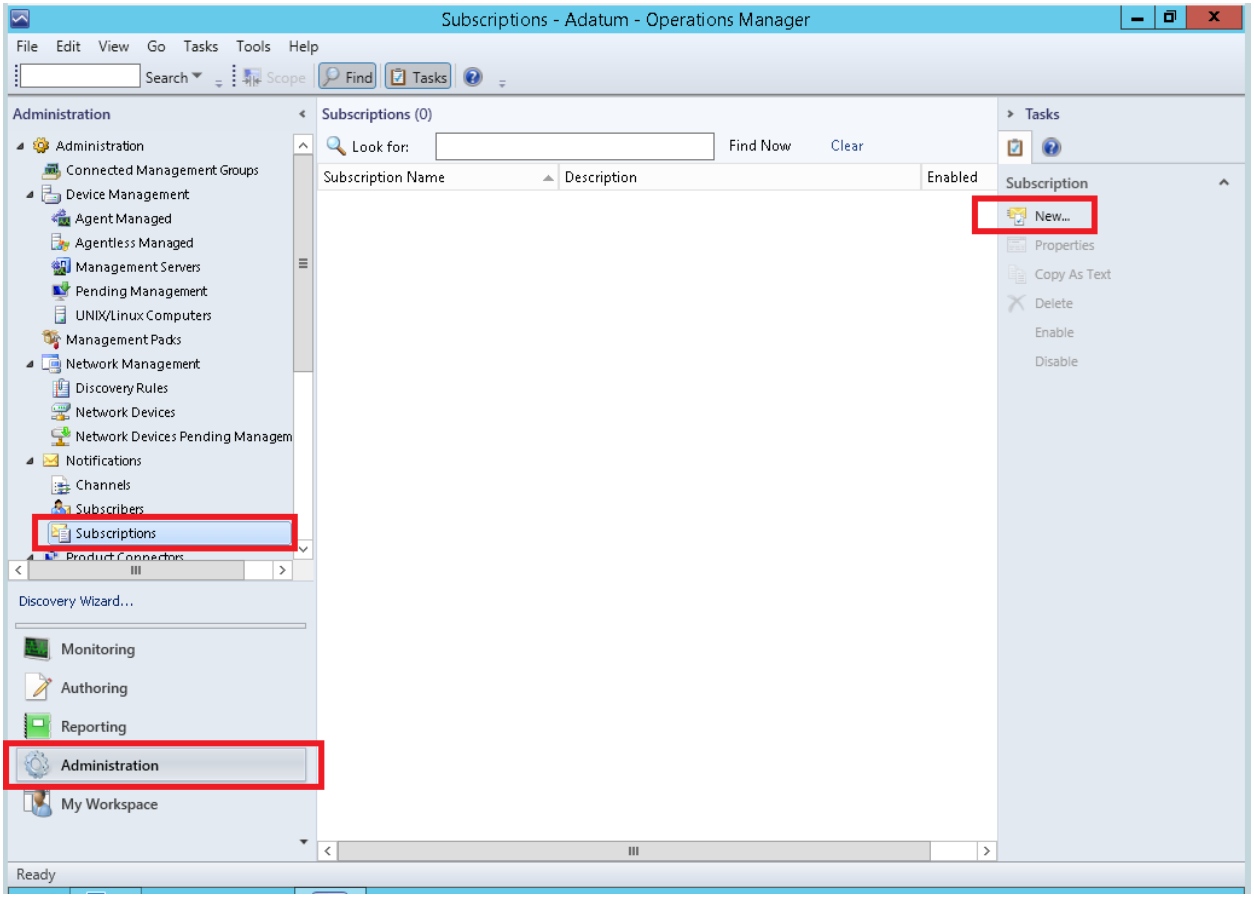



9. Cửa sổ **Addresses**, chọn **Finish**, và chọn **Close**.

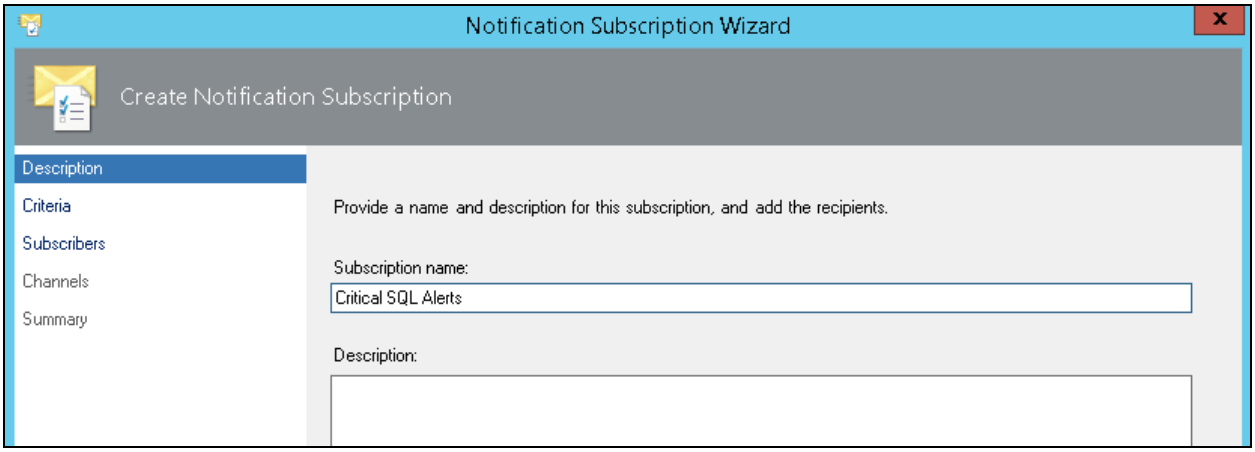


## ➢ Cấu hình Subscriptions

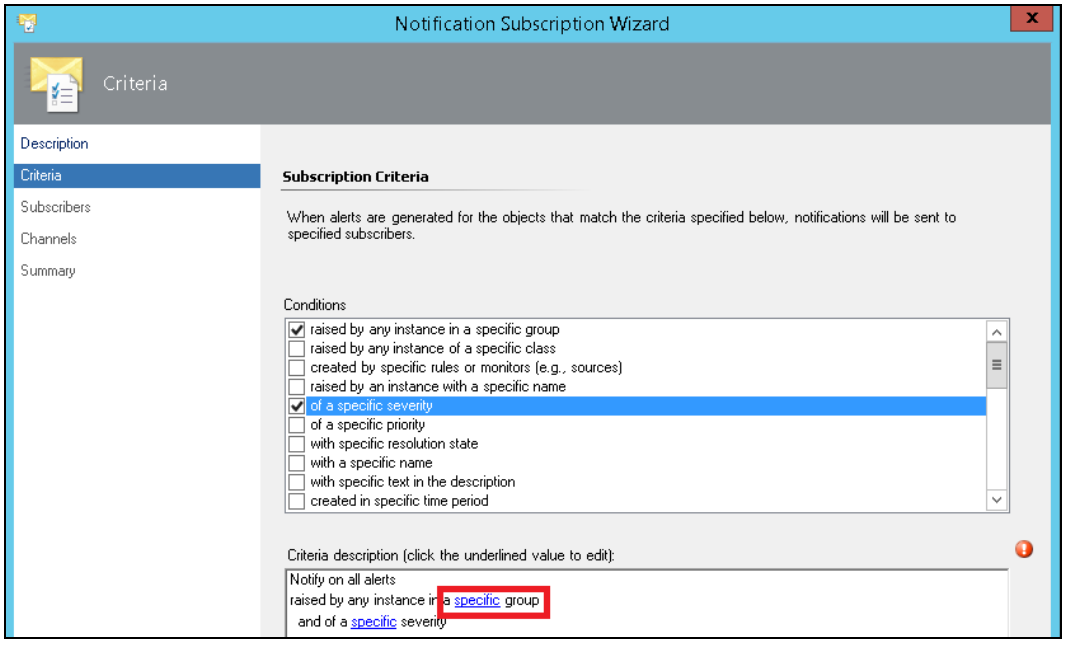
1. Trong cửa sổ **Operations Manager**, chọn **Administration**, chọn **Subscriptions**, chọn **New**.



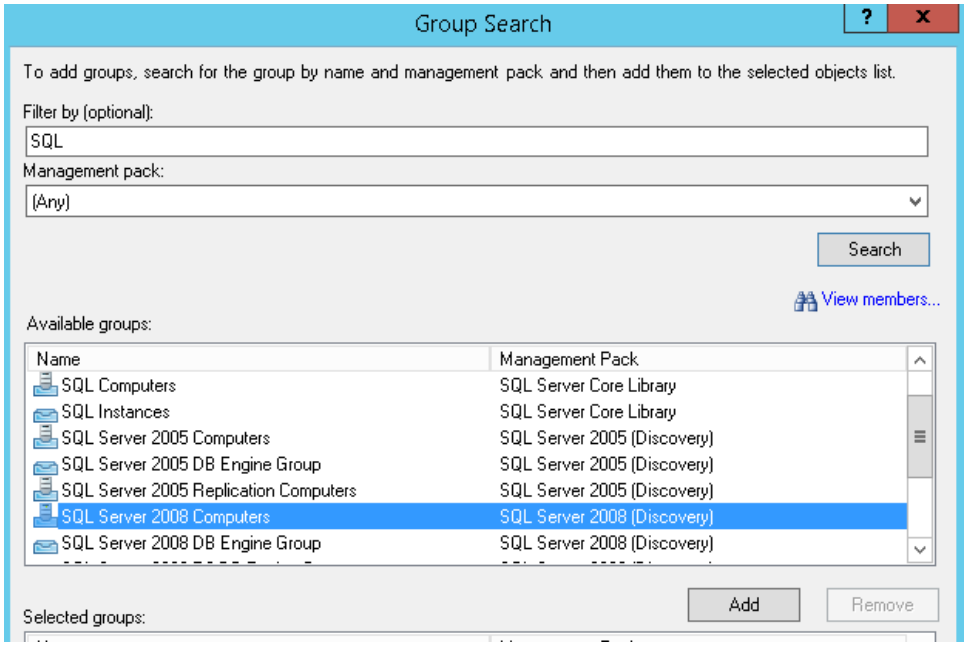
2. Cửa sổ **Create Notification Subscription**, trong ô **Subscription name**, nhập **Critical SQL Alerts**, chọn **Next**.



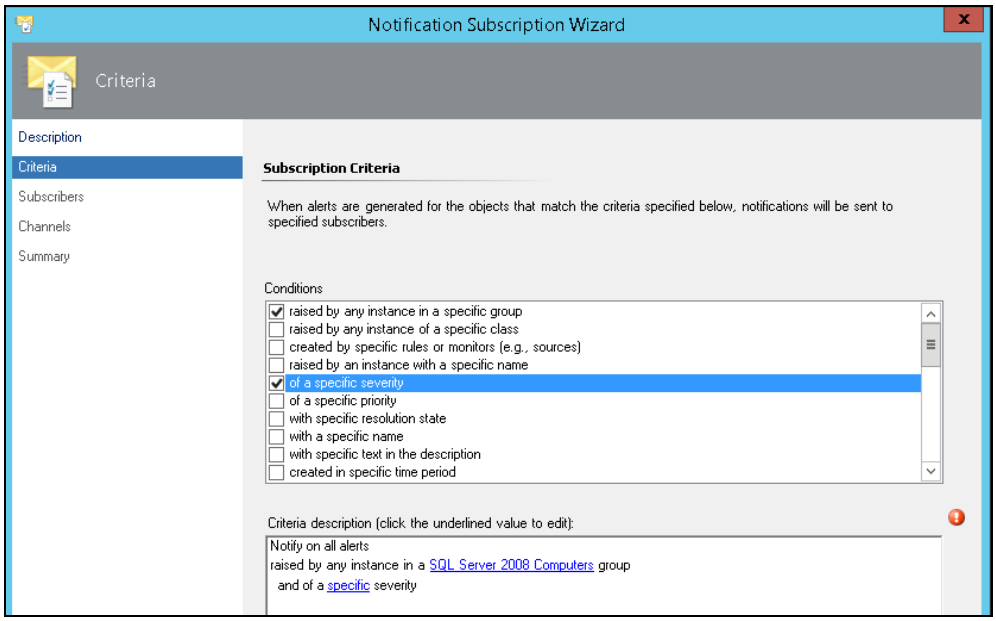

3. Cửa sổ **Criteria**, trong phần **Conditions**, đánh dấu chọn 2 ô **raised by any instance in a specific group**, và **of a specific severity**. Trong phần **Criteria description (click the underlined value to edit)**, chọn **specific** đầu tiên.



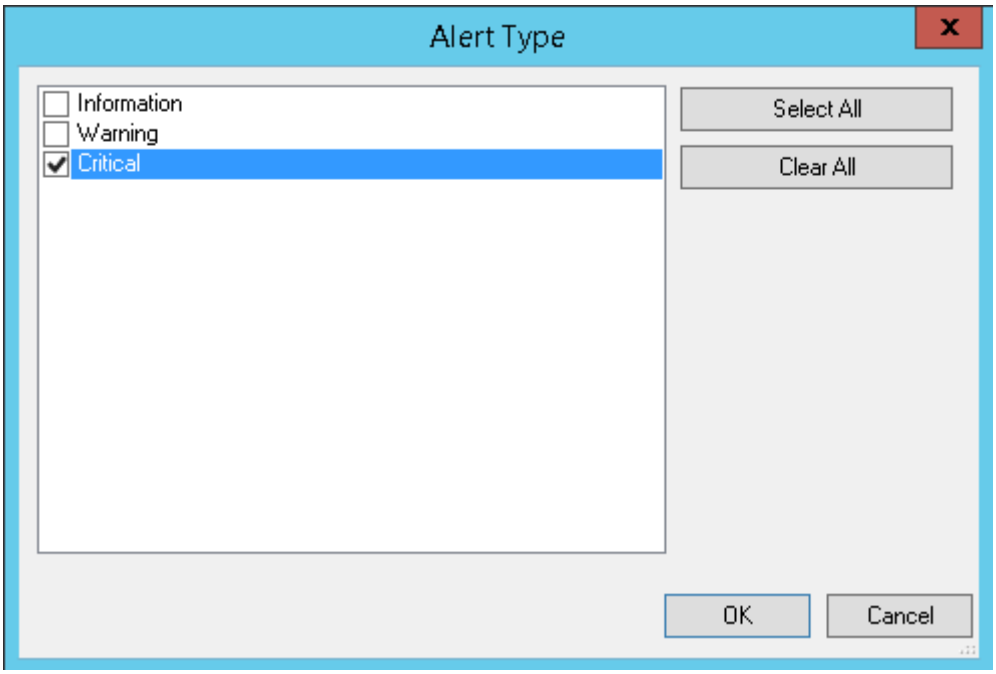
4. Hộp thoại **Group Search**, trong ô **Filter by (optional)**, nhập **SQL**, và chọn **Search**. Trong phần **Available groups**, chọn **SQL Server 2008 Computers**, chọn **Add**, và chọn **OK**.




5. Cửa sổ **Criteria,** trong phần **Criteria description (click the underlined value to edit)**, chọn **specific**.



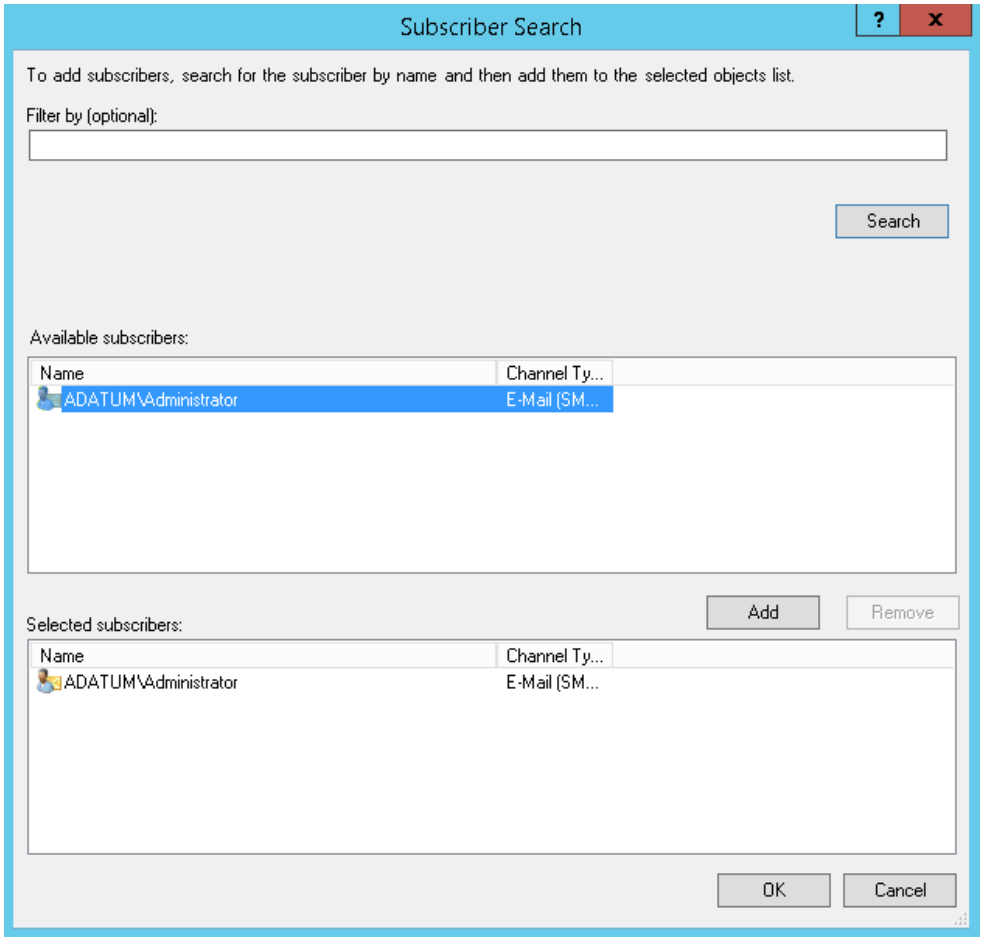
6. Hộp thoại **Alert Type**, đánh dấu chọn **Critical**, chọn **OK**, và chọn **Next**.




7. Cửa sổ **Subscribers**, chọn **Add**.



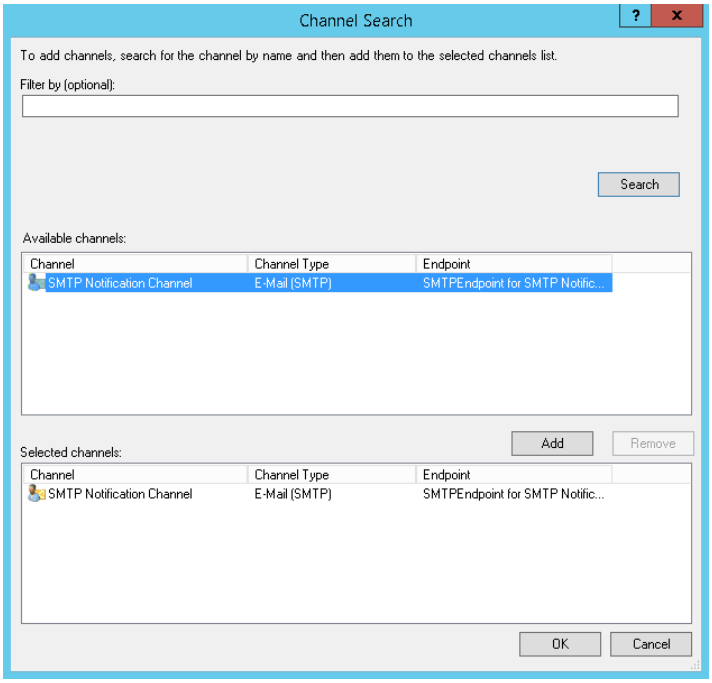
8. Hộp thoại **Subscriber Search**, chọn **Search**, chọn **ADATUM\Administrator**, chọn **Add**, chọn **OK**, và chọn **Next**.



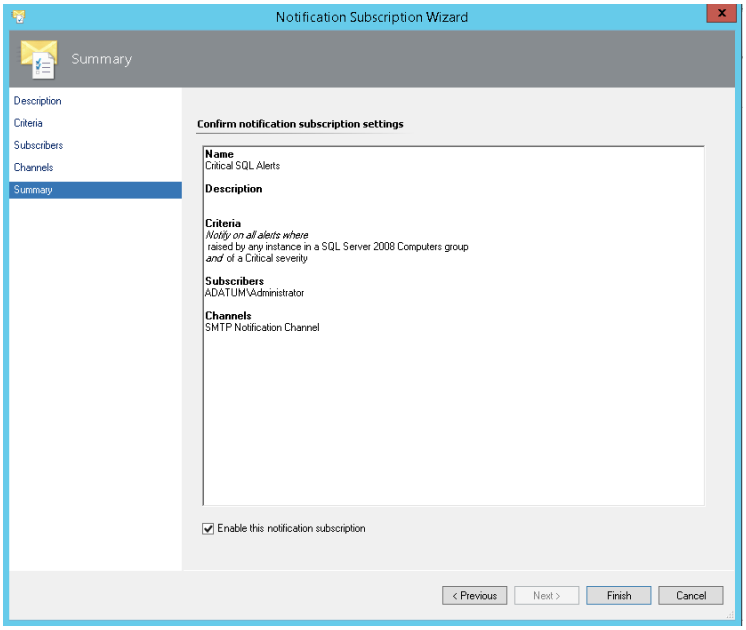

9. Cửa sổ **Channels**, chọn **Add**.



10. Hộp thoại **Channel Search**, chọn **Search**, chọn **SMTP Notification Channel**, chọn **Add**, chọn **OK**, và chọn **Next**.

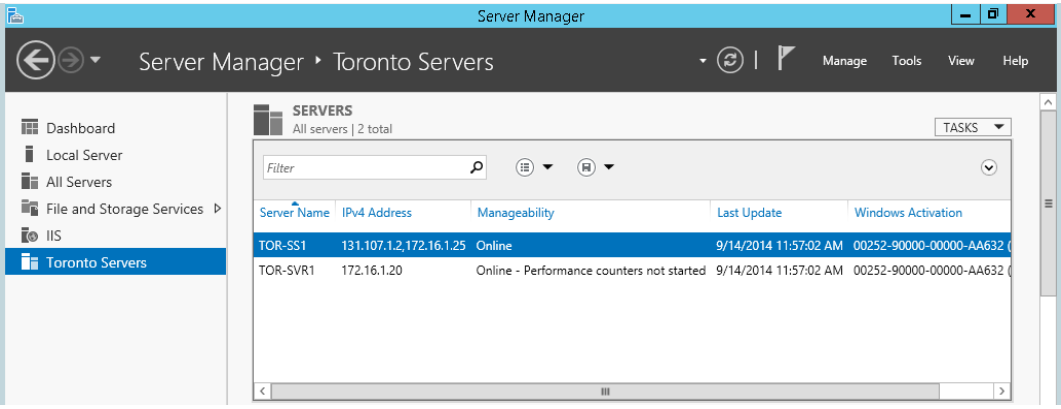



11. Cửa sổ **Summary**, chọn **Finish**, và chọn **Close**.

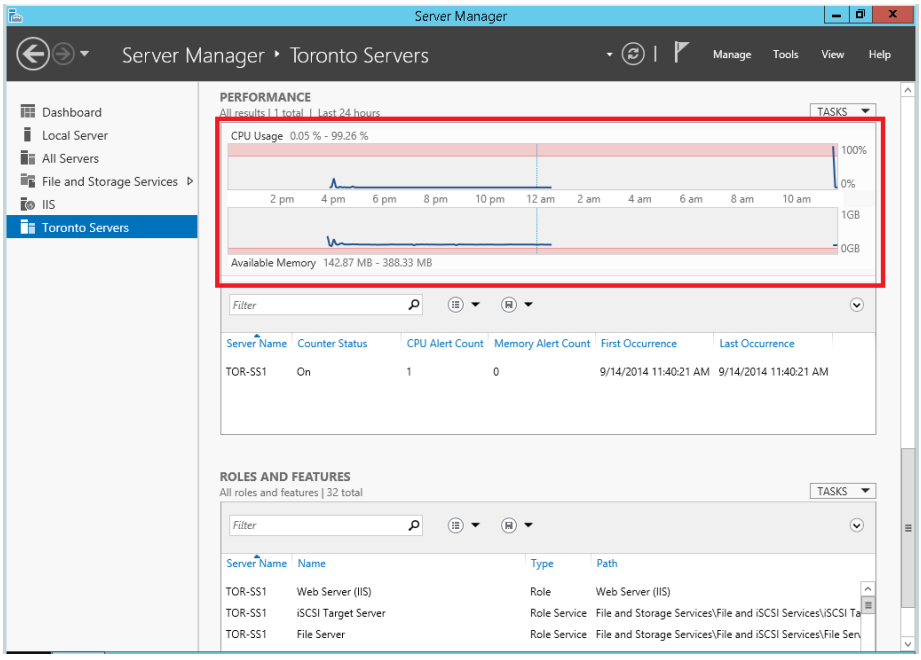


## Bước 3: Giám sát hiệu suất của Server.

1. Qua máy **TOR-SVR1**. Trong **Server Manager**, chọn **Toronto Servers**, trong phần **SERVERS**, chọn **TOR-SS1**.




2. Kéo thanh trượt xuống phần **PERFORMANCE** và xem hiệu suất trong biểu đồ (Nếu chưa có thông tin, đợi khoảng 30 phút rồi kiểm tra lại).




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công các thành phần giám sát trong System Center Operation Manager**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho các máy ảo còn lại.

# Bài 6: Triển khai khả năng sẵn sàng cao (High Availability) cho dữ liệu và ứng dụng.

**I. Mục tiêu:**

- Triển khai giải pháp sẵn sàng cao cho việc lưu trữ dữ liệu.
- Triển khai giải pháp sẵn sàng cao bằng Network Load Balancing (NLB).

**II. Kịch bản:**

Một trong những yêu cầu quan trọng khi triển khai Windows Server 2012 tại công ty A. Datum là phải cung cấp khả năng sẵn sàng cao cho tất cả các dịch vụ mạng và các ứng dụng quan trọng. A. Datum đã xác định dịch vụ File và một số ứng dụng Web là các dịch vụ quan trọng phải có khả năng sẵn sàng cao.

**III. Yêu cầu tổng quan:**

A. Datum yêu cầu khả năng sẵn sàng cao cho dịch vụ File và ứng dụng Web như sau:

- Dù ổ cứng của File Server bị hỏng, người dùng vẫn phải truy cập được dữ liệu của họ trên File Server.
- Dù File Server gặp sự cố bất kỳ, người dùng vẫn phải truy cập được dữ liệu của họ trên File Server.
- Dù Web Server gặp sự cố bất kỳ cũng không ảnh hưởng đến hoạt động của các ứng dụng web.

**IV. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-CL1**<br>**20414C-LON-SVR1**<br>**20414C-LON-SVR2**<br>**20414C-TOR-SVR1**<br>**20414C-TOR-SS1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy thật, khởi động vào **20414C-LON-HOST1**.
2. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiên lại từ bước 2 đến 4 cho các máy ảo còn lại**.**

**VI. Thực hành:**

*Thời gian thực hành: 60 phút*

**Bài tập 1: Triển khai giải pháp sẵn sàng cao cho việc lưu trữ dữ liệu.**

❖ **Bài tập bao gồm các bước:**

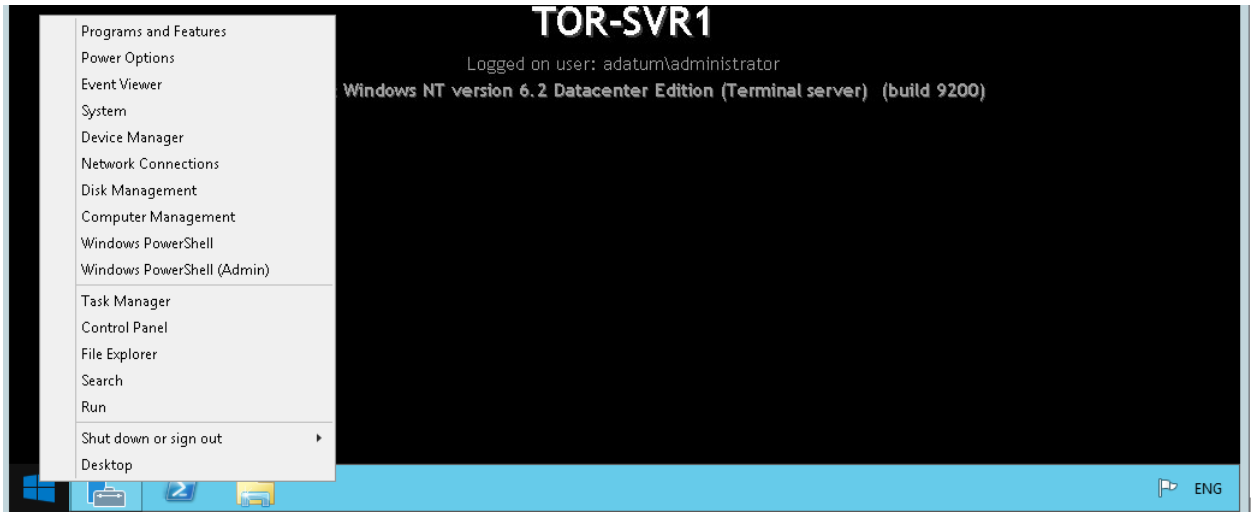
1. Cấu hình NIC Teaming.
2. Cấu hình iSCSI initiators và MPIO.
3. Cấu hình Storage Spaces sử dụng iSCSI targets.
4. Kiểm tra khả năng sẵn sàng cao.

❖ **Thực hiện:**

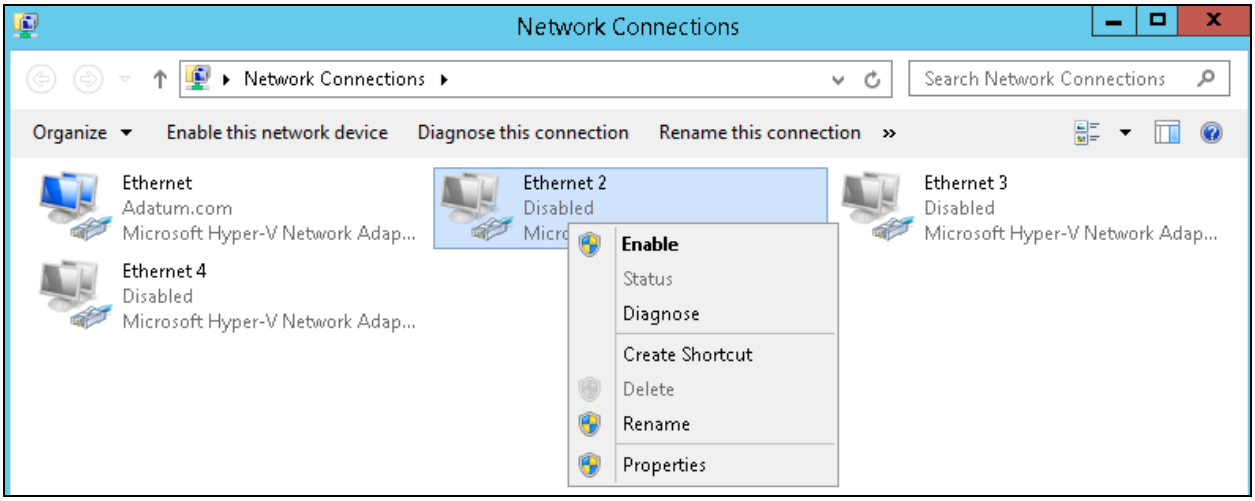
**Bước 1. Cấu hình NIC Teaming.**

1. Sign in vào máy **TOR-SVR1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

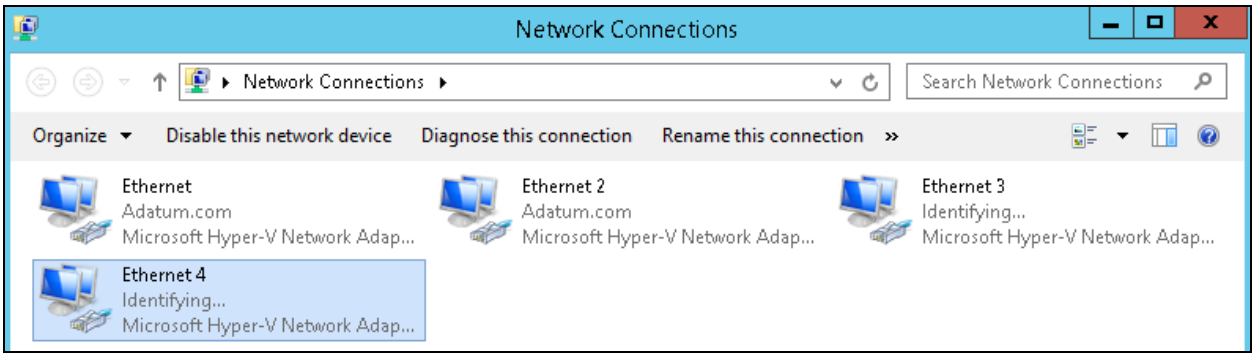
2. Chuột phải lên **Start Menu**, chọn **Network Connections**




3. Trong cửa sổ **Network Connections**, chuột phải **Ethernet 2**, chọn **Enable**.

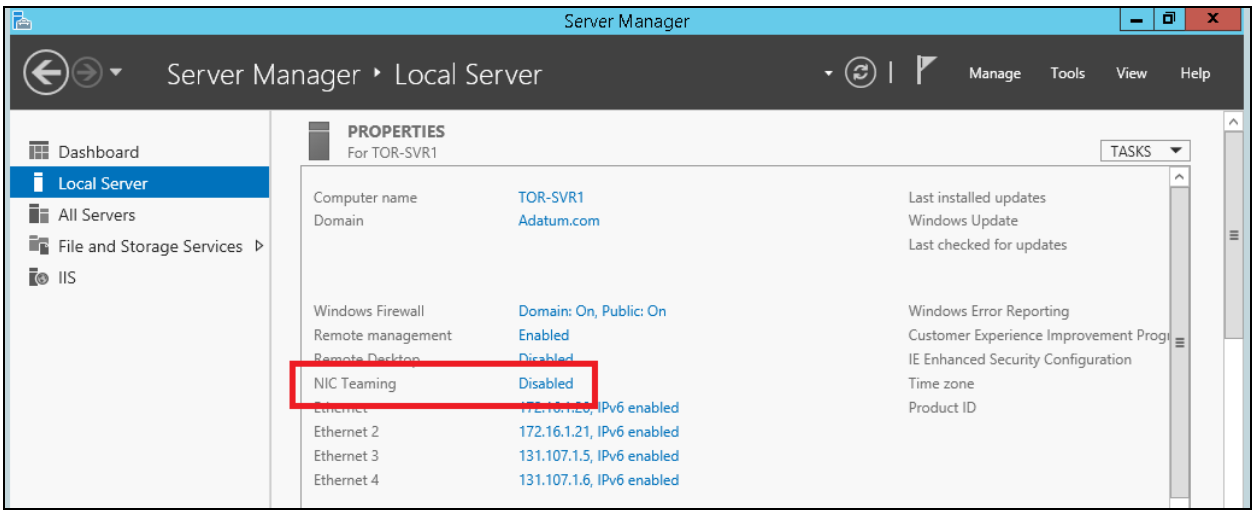


4. Lặp lại bước 3 để enable 2 card **Ethernet 3** và **Ethernet 4**.

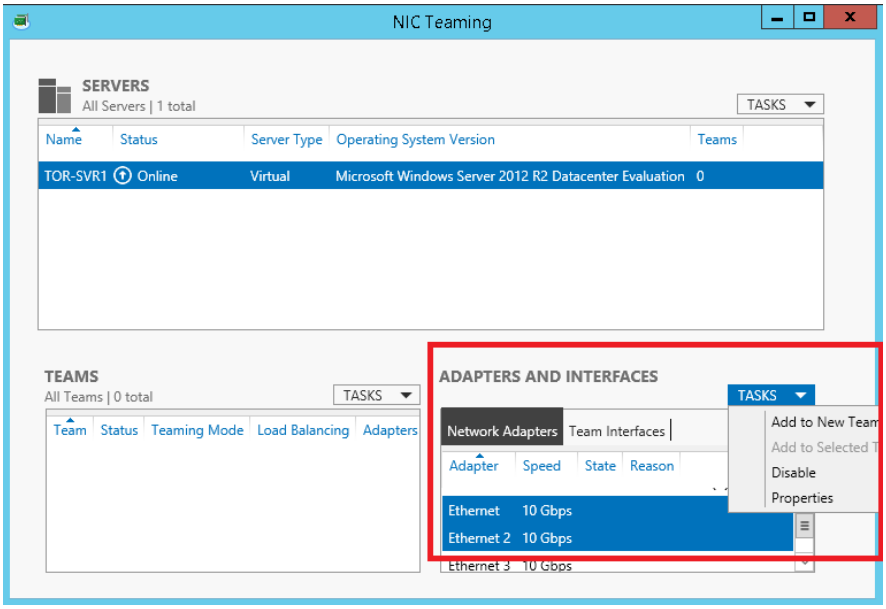



5. Tắt cửa sổ **Network Connections**.

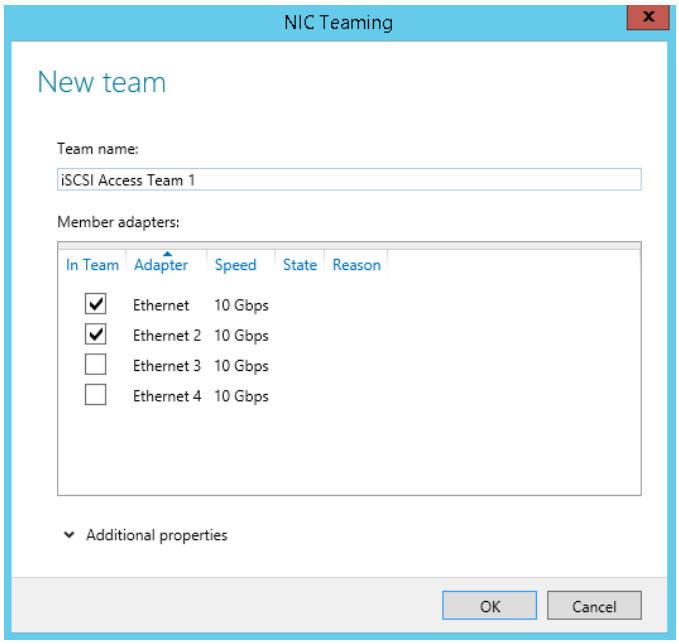
6. Mở **Server Manager**, chọn **Local Server,** trong dòng **NIC Teaming**, chọn **Disabled**.



7. Cửa sổ **NIC Teaming**, trong ô **Adapters and Interfaces**, giữ phím **Ctrl,** chọn 2 card **Ethernet** và **Ethernet 2**. Bung **Tasks**, chọn **Add to New Team**.

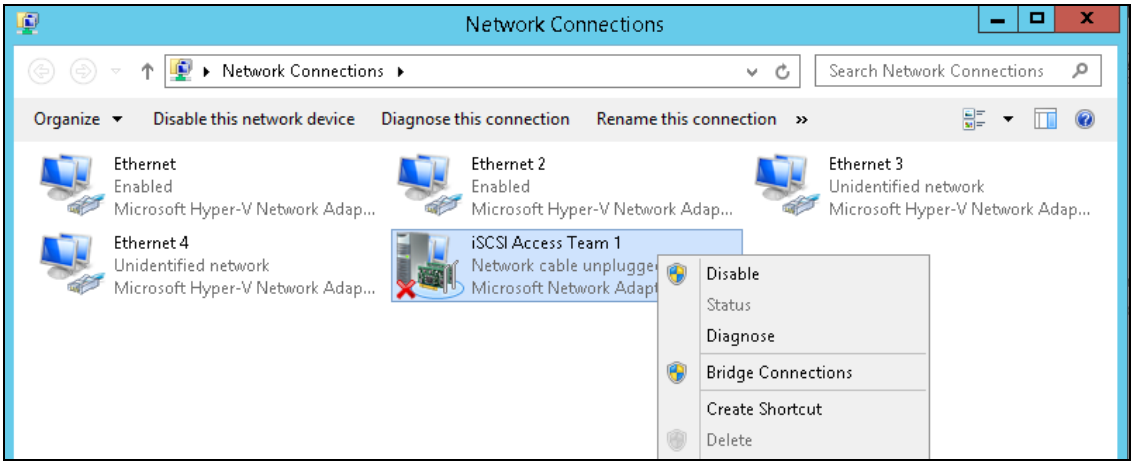



8. Hộp thoại **New team**, trong ô **Team name**, nhập **iSCSI Access Team 1**, chọn **OK**. Tắt cửa sổ **NIC Teaming**.



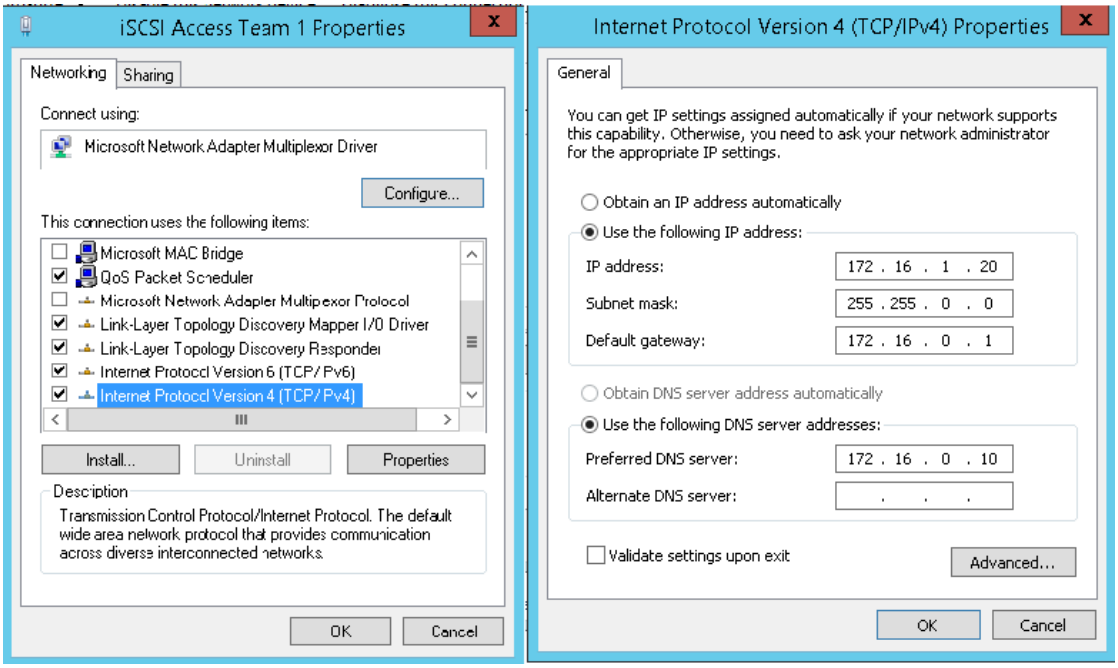
9. Chuột phải lên Start Menu, chọn **Network Connections**

10. Trong cửa sổ **Network Connections**, chuột phải **iSCSI Access Team 1**, chọn **Properties**.

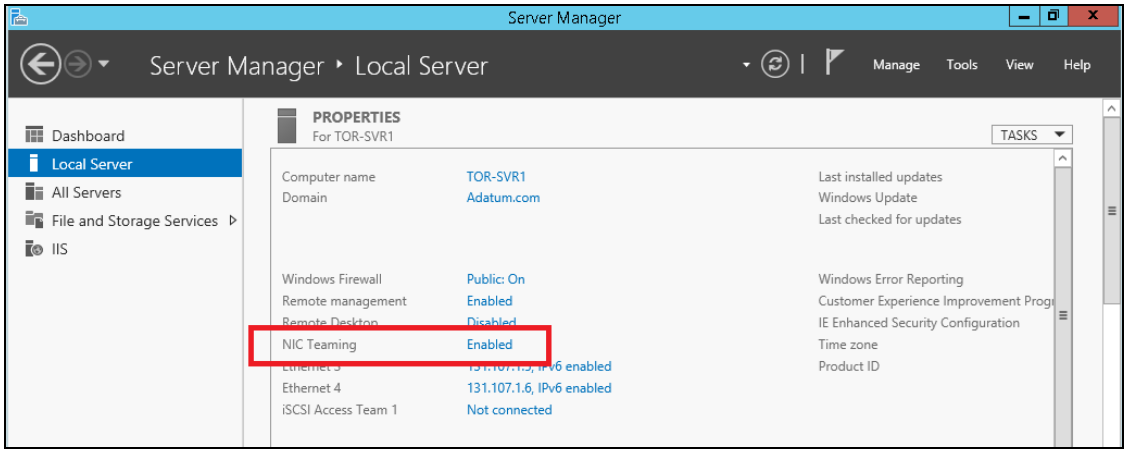



11. Hộp thoại **iSCSI Access Team 1 Properties**, nhấp đôi chuột **Internet Protocol Version 4 (TCP/IPv4)**.

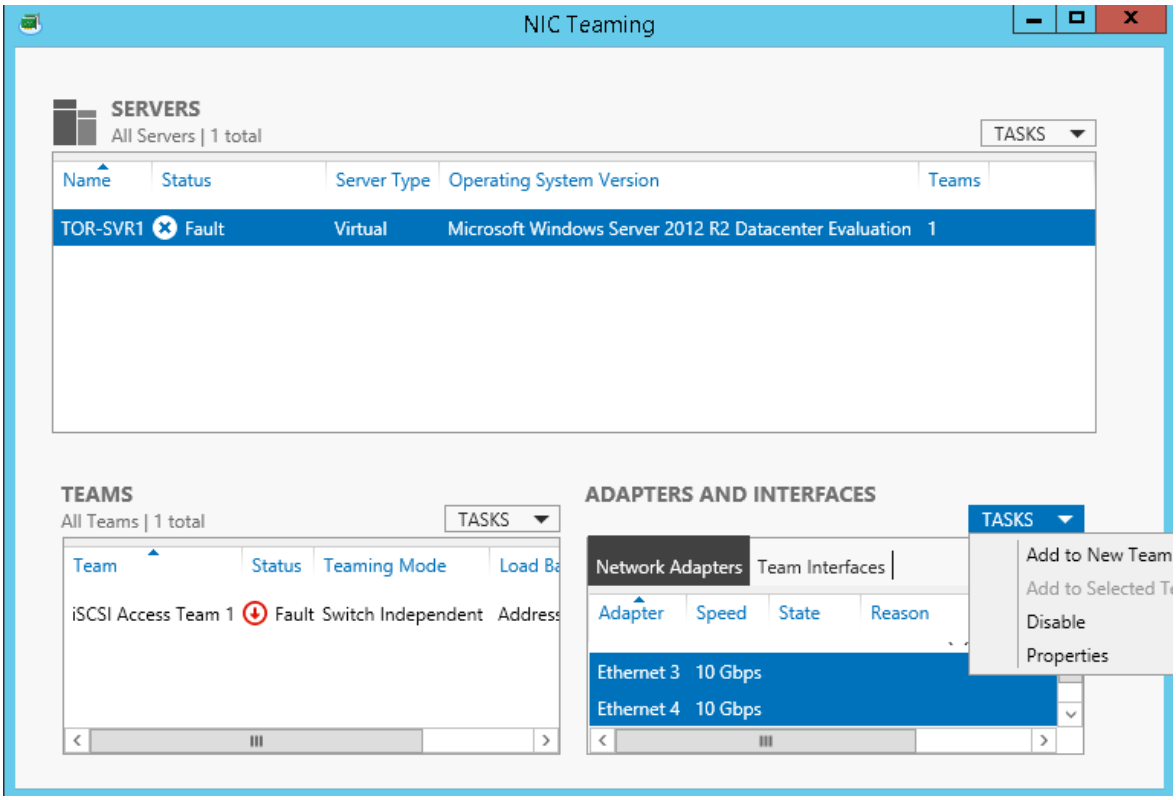
12. Chọn **Use the following IP address**, thiết lập địa chỉ như trong hình và chọn **OK** 2 lần:



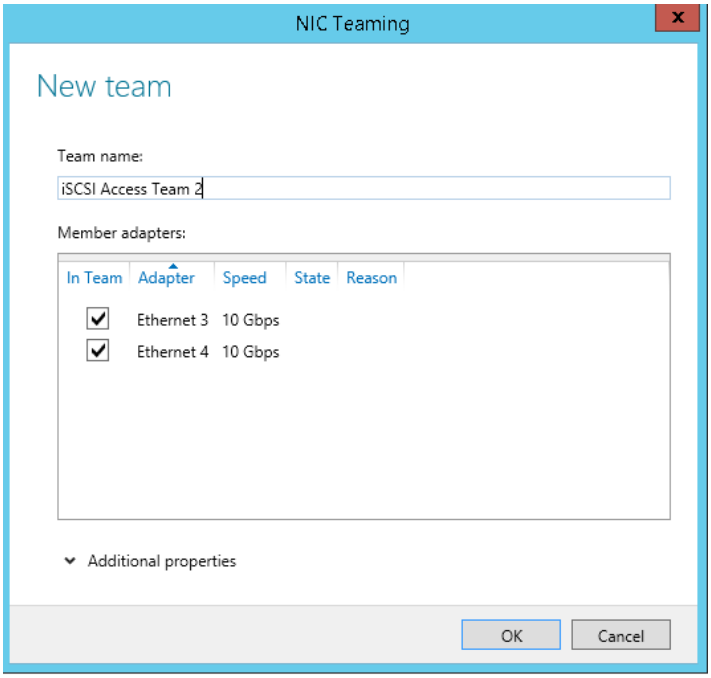
13. Trong cửa sổ **Server Manager**, chọn **Local Server**, trong dòng **NIC Teaming**, chọn **Enabled**.



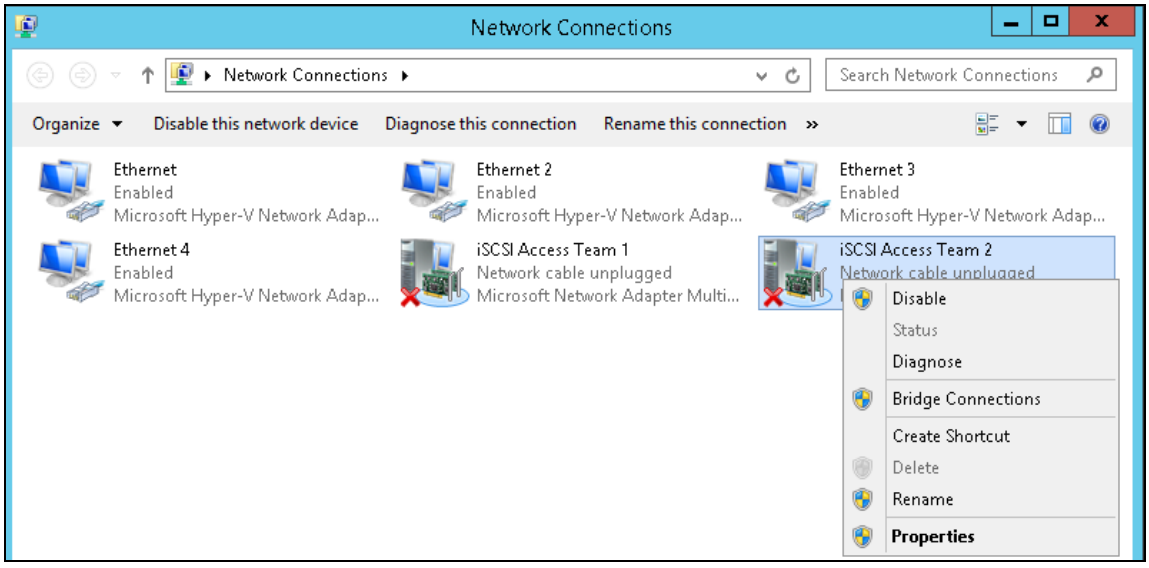

14. Cửa sổ **NIC Teaming**, trong ô **Adapters and Interfaces**, giữ phím **Ctrl,** chọn 2 card **Ethernet 3** và **Ethernet 4**. Bung **Tasks**, chọn **Add to New Team**.



15. Hộp thoại **New team**, trong ô **Team name**, nhập **iSCSI Access Team 2**, chọn **OK**. Tắt cửa sổ **NIC Teaming**

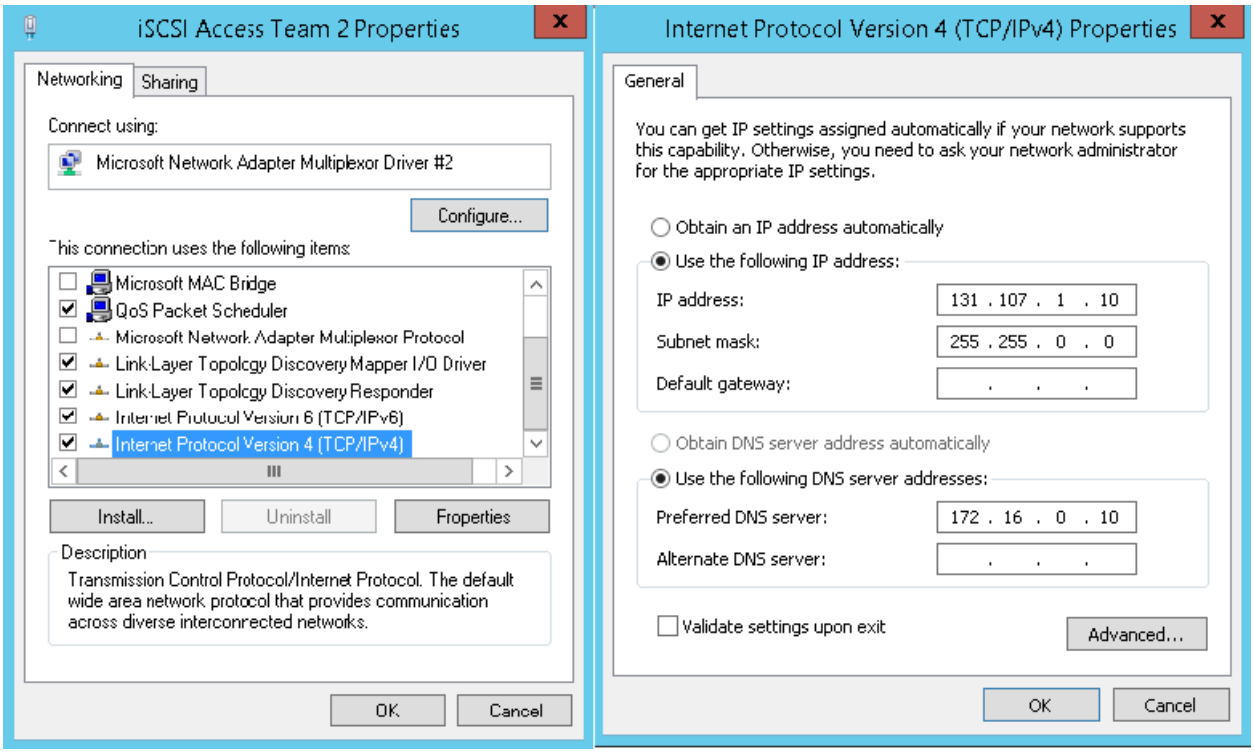



16. Trong cửa sổ **Network Connections**, chuột phải **iSCSI Access Team 2**, chọn **Properties**.



17. Hộp thoại **iSCSI Access Team 2 Properties**, nhấp đôi chuột **Internet Protocol Version 4 (TCP/IPv4)**.

18. Chọn **Use the following IP address**, thiết lập địa chỉ như trong hình và chọn **OK** 2 lần:

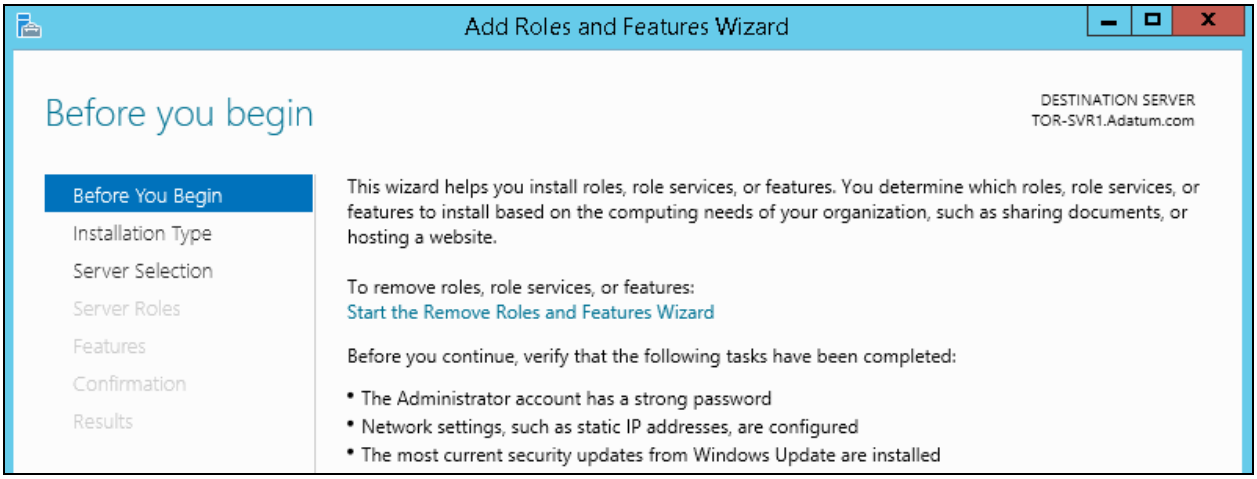



19. Tắt cửa sổ **Network Connections**.

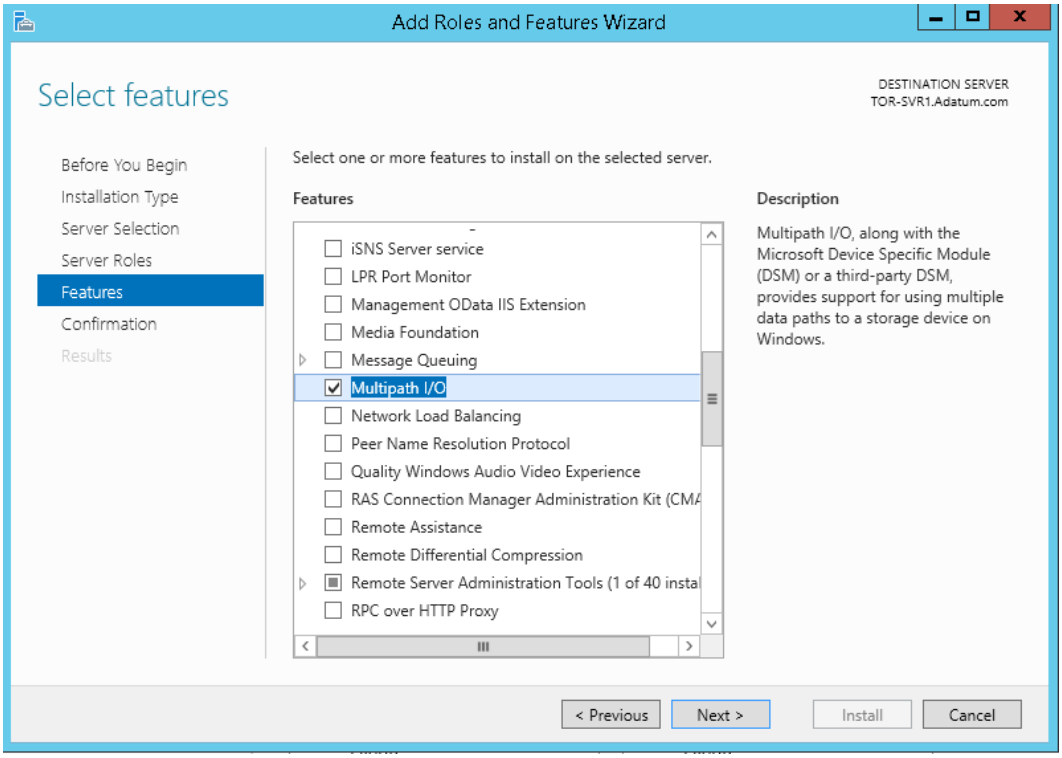
## Bước 2. Cấu hình iSCSI initiators và MPIO.

1. Trên máy **TOR-SVR1**, trong cửa sổ **Server Manager**, chọn **Add roles and features**.

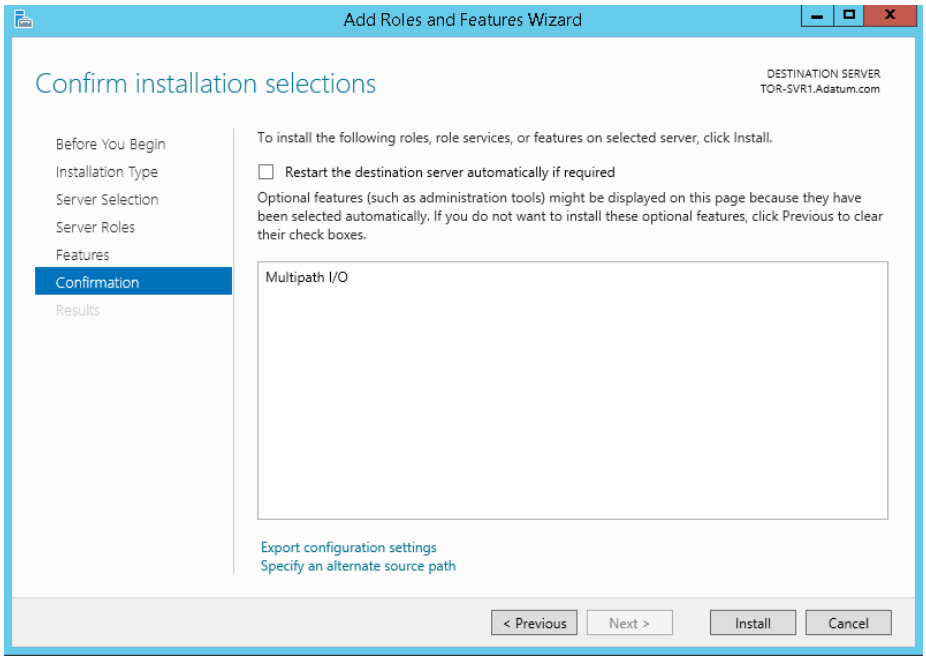
2. Cửa sổ **Before You Begin**, chọn **Next** 4 lần.




3. Cửa sổ **Select features**, đánh dấu chọn **Multipath I/O**, và chọn **Next**.

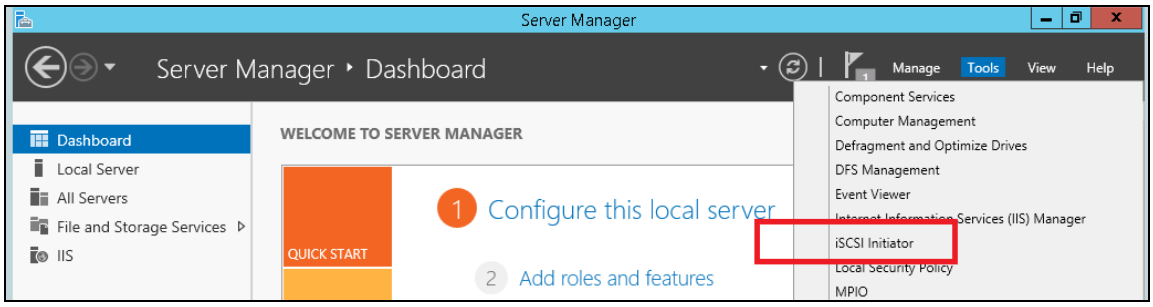


4. Cửa sổ **Confirm installation selections**, chọn **Install**.

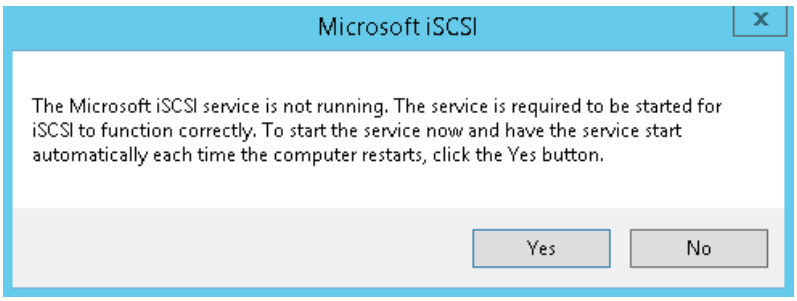



5. Sau khi cài đặt thành công, chọn **Close**.

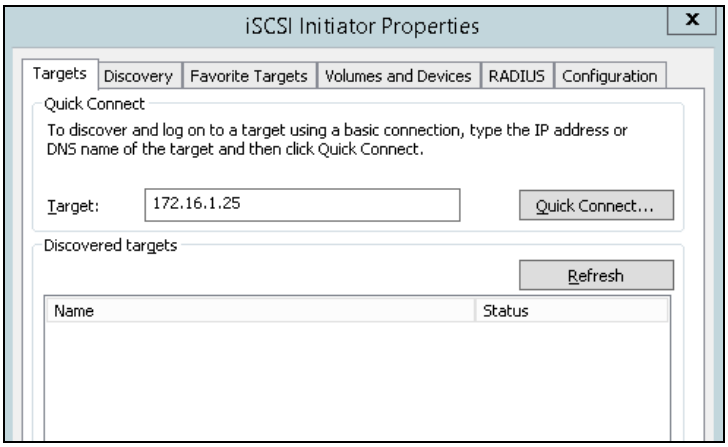
6. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **iSCSI Initiator**.



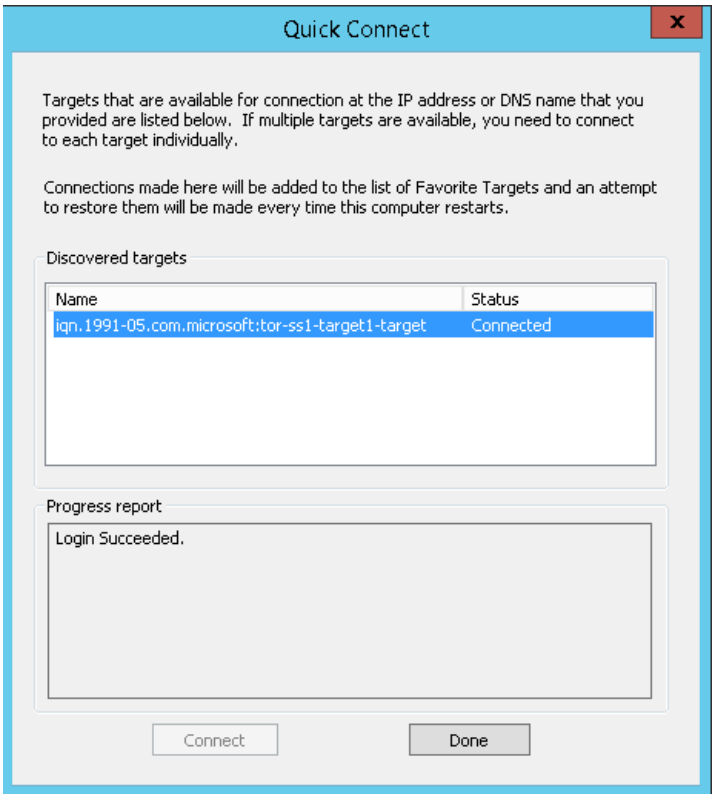

7. Hộp thoại **Microsoft iSCSI**, chọn **Yes**.



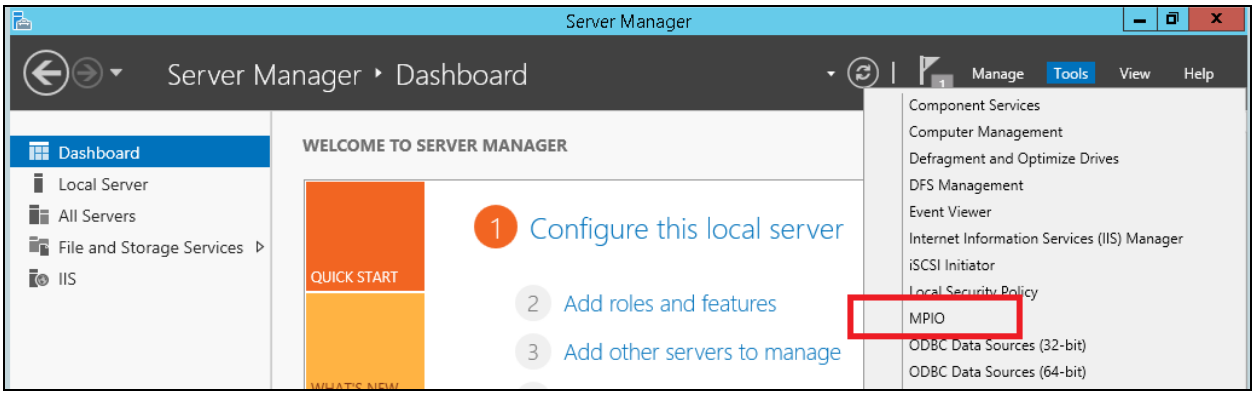
8. Hộp thoại **iSCSI Initiator Properties**, trong tab **Targets**, nhập **172.16.1.25** vào ô **Target**, chọn **Quick Connect**.



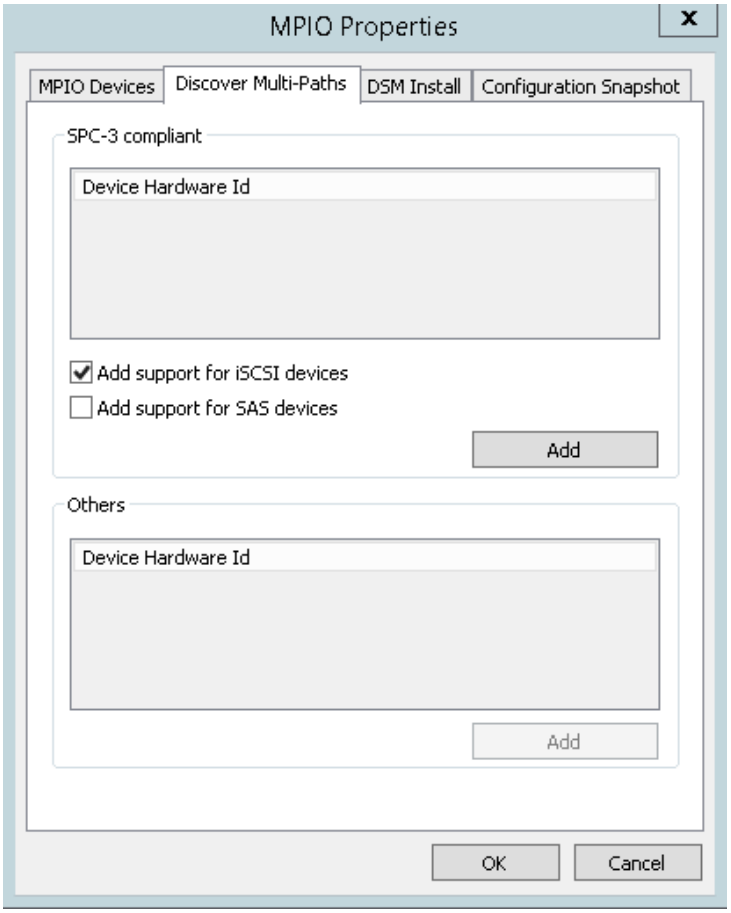

9. Hộp thoại **Quick Connect**, kiểm tra có 1 target đang ở trạng thái Connected, chọn **Done**, chọn **OK.**



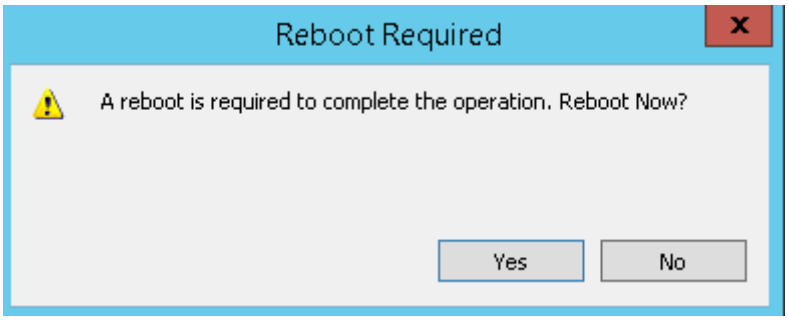
10. Trong **Server Manager**, bung menu **Tools**, mở **MPIO**.




11. Trong hộp thoại **MPIO Properties**, qua tab **Discover Multi-Paths**, đánh dấu chọn **Add support for iSCSI devices**, chọn **Add**.



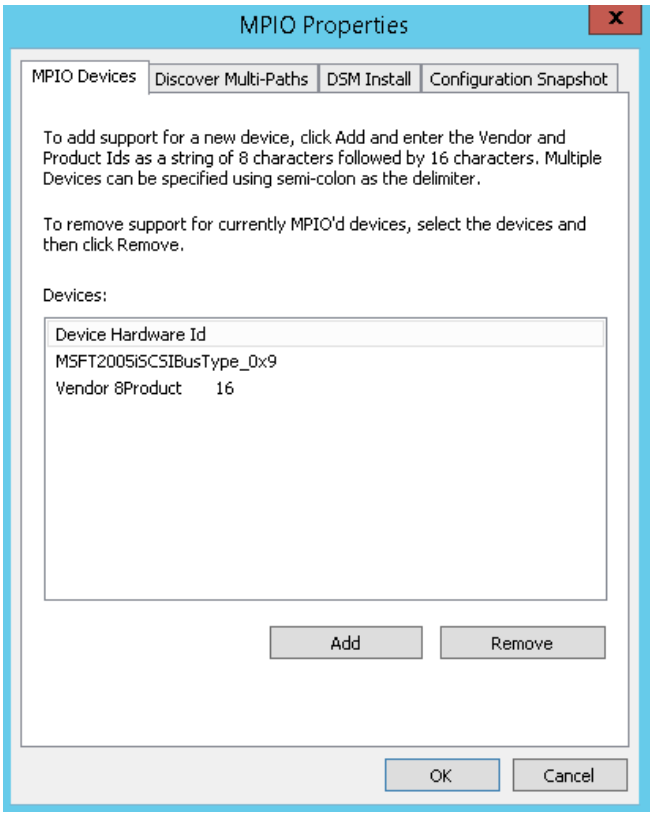
12. Khi nhận được thông báo yêu cầu khởi động lại may, chọn **Yes**.




13. Khi khởi động thành công, sign in vào máy **TOR-SVR1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

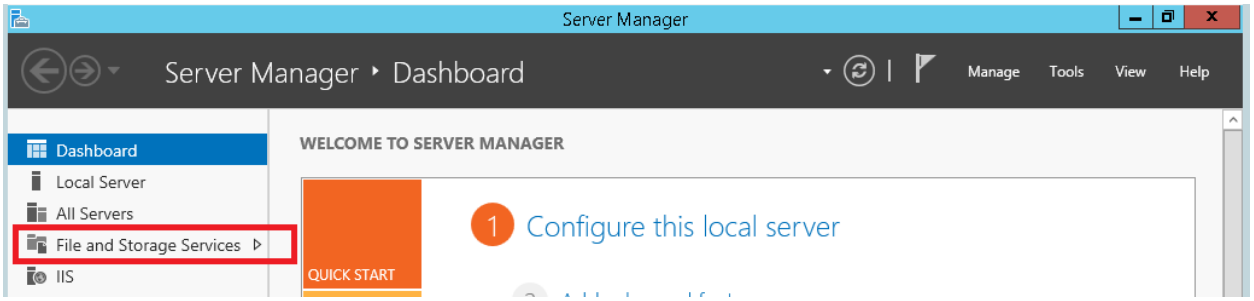
14. Trong **Server Manager**, bung menu **Tools**, mở **MPIO**.

15. Hộp thoại **MPIO Properties**, trong tab **MPIO Devices**, kiểm tra có **Device Hardware ID** là **MSFT2005iSCSIBusType_0x9**. Chọn **OK**

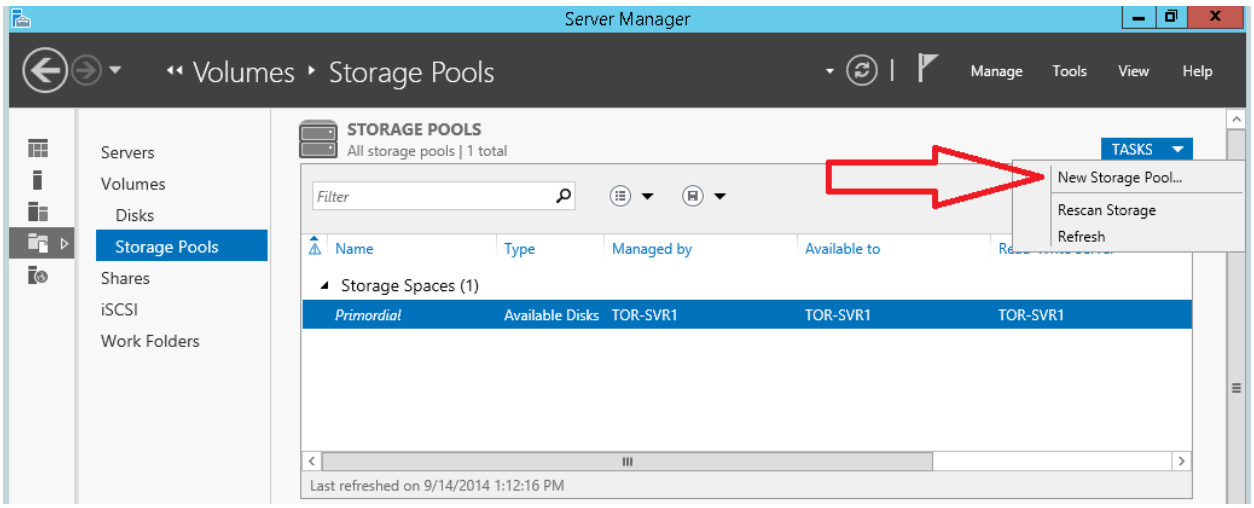


## Bước 3. Cấu hình Storage Spaces sử dụng iSCSI targets.

1. Trên máy **TOR-SVR1**, trong cửa sổ **Server Manager**, chọn **File and Storage Services**.

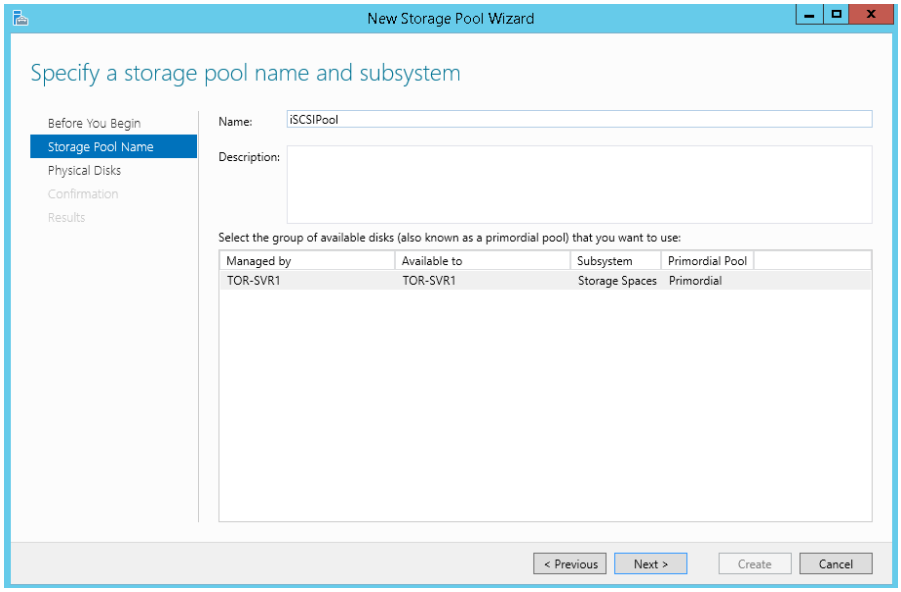



2. Chọn **Storage Pools**, trong phần **STORAGE POOLS**, bung **TASKS**, chọn **New Storage Pool**.

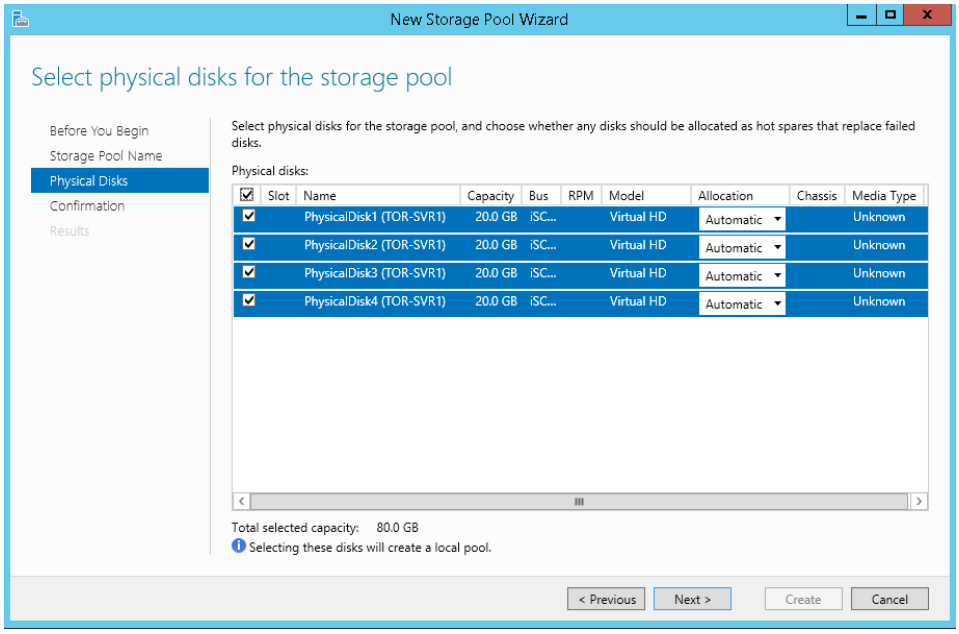



3. Cửa sổ **Before You Begin**, chọn **Next**.

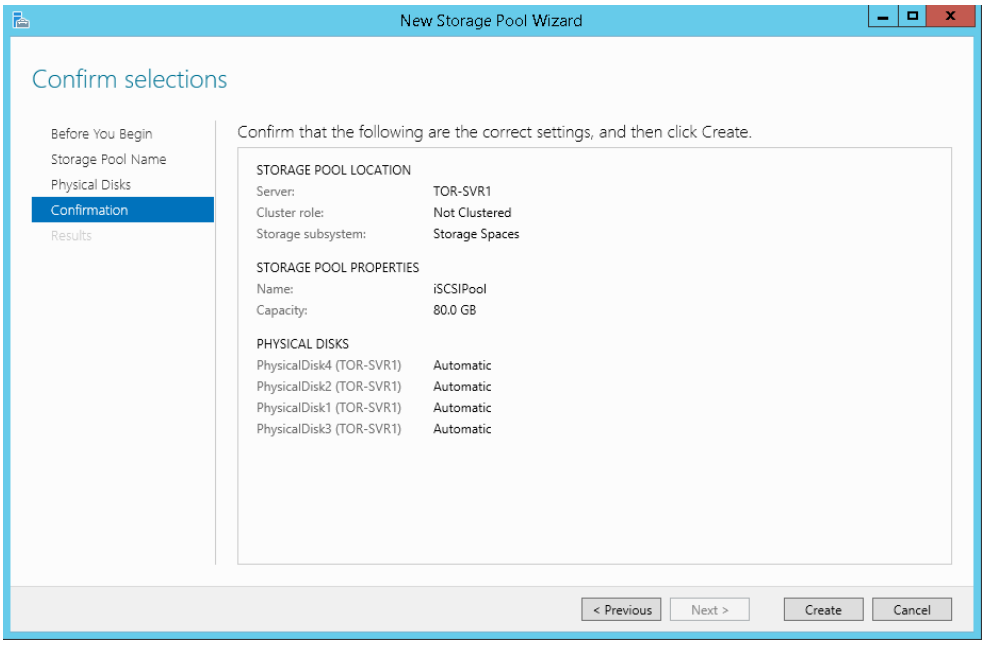
4. Cửa sổ **Specify a storage pool name and subsystem**, trong ô **Name**, nhập **iSCSIPool**, và chọn **Next**.



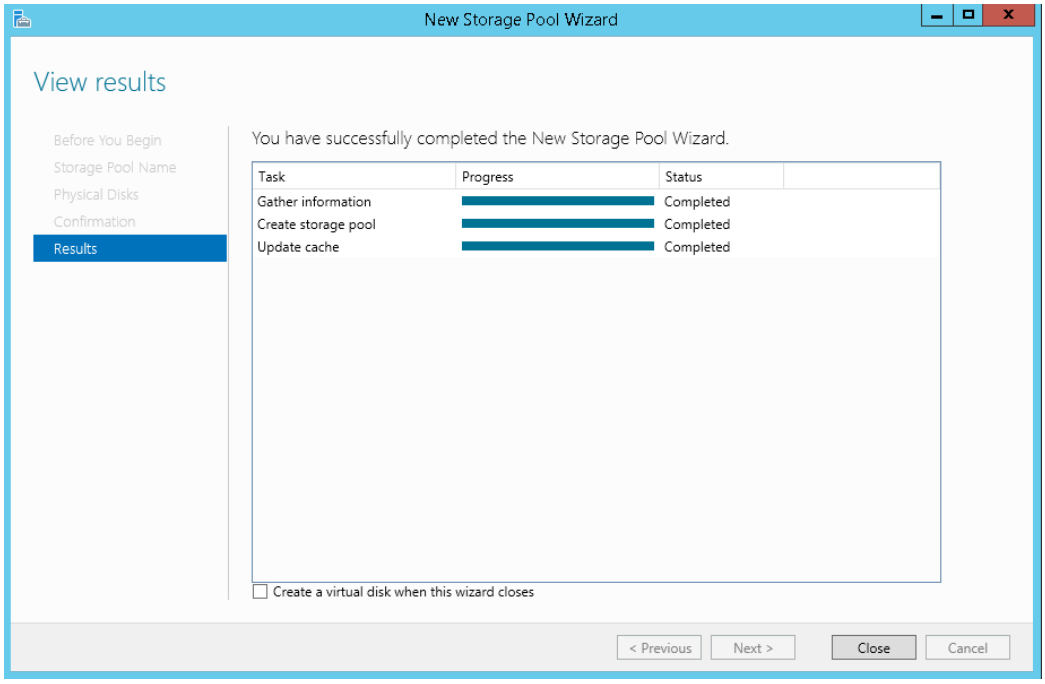

5. Cửa sổ **Select physical disks for the storage pool**, đánh dấu chọn cả 4 **PhysicalDisk**, và chọn **Next**.



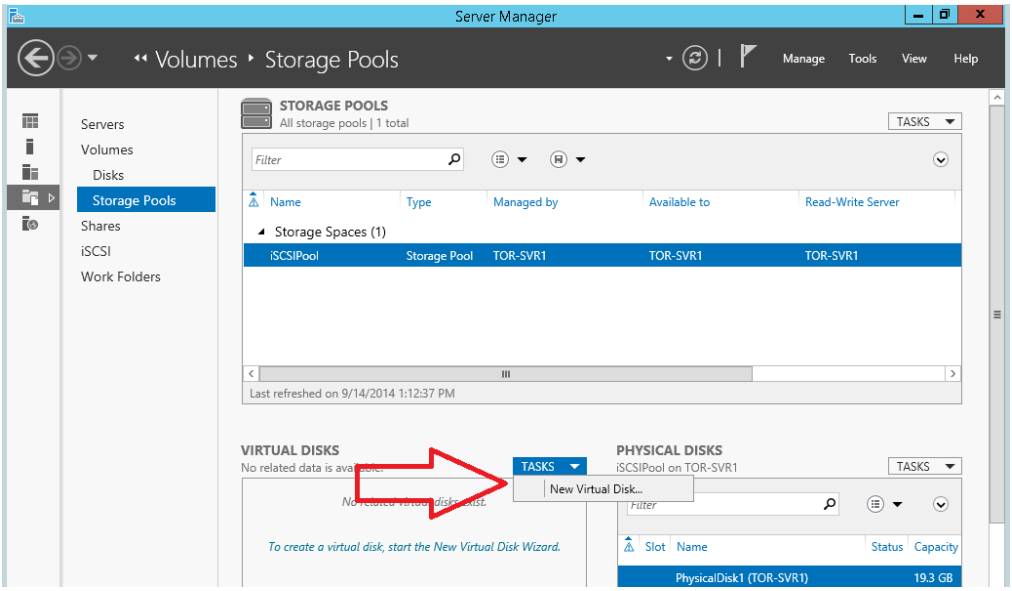
6. Cửa sổ **Confirm selections**, chọn **Create**.




7. Cửa sổ **View results**, kiểm tra tạo thành công, và chọn **Close**.

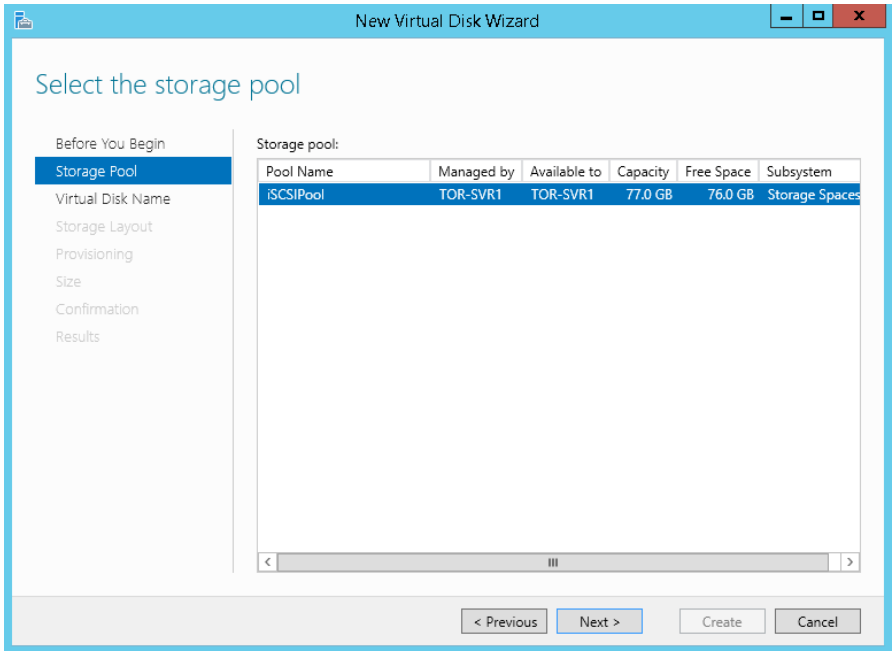


8. Trong phần **STORAGE POOLS,** chọn **iSCSIPool**, trong phần **VIRTUAL DISKS**, bung **TASKS**, chọn **New Virtual Disk**.

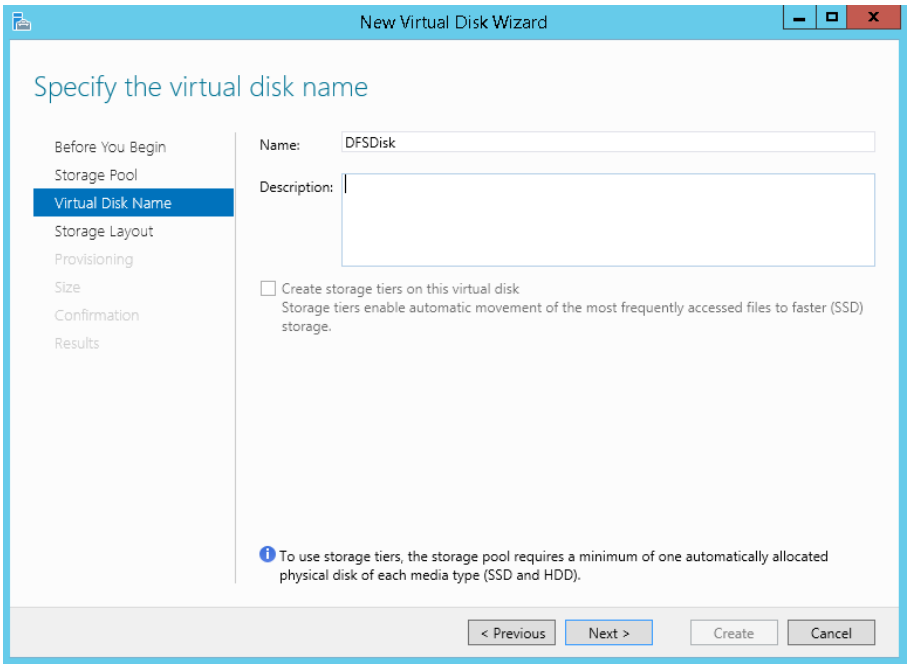



9. Cửa sổ **Before You Begin**, chọn **Next**.

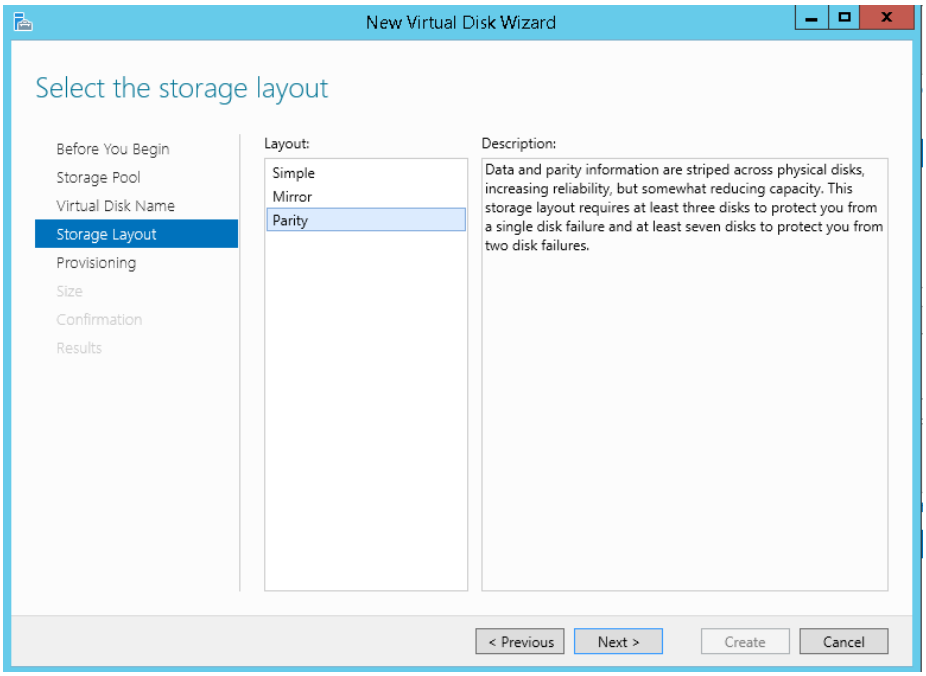
10. Cửa sổ **Select the storage pool**, chọn **iSCSIPool**, và chọn **Next**.



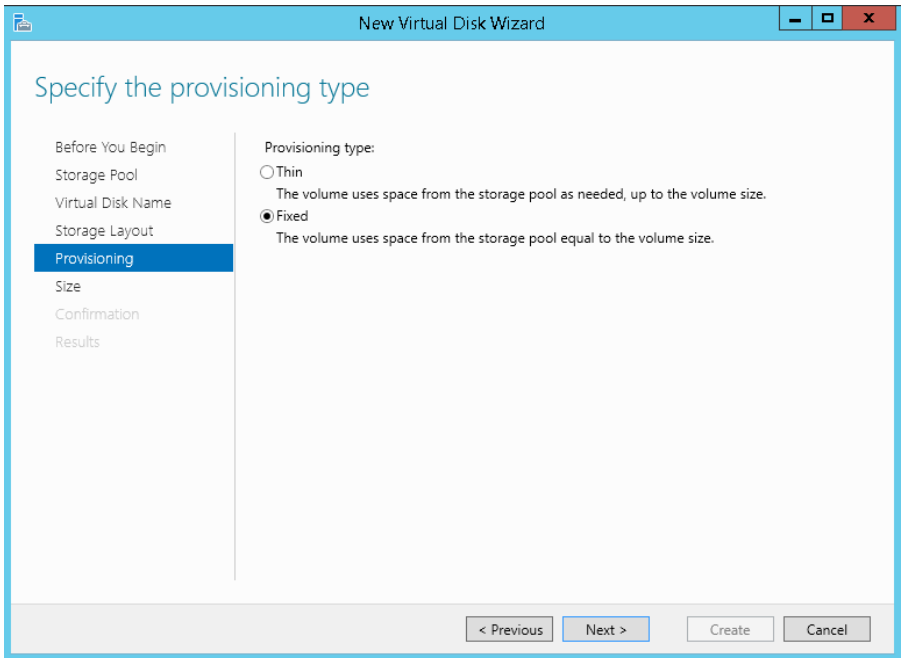
11. Cửa sổ **Specify the virtual disk name**, trong ô **Name**, nhập **DFSDisk**, và chọn **Next**.



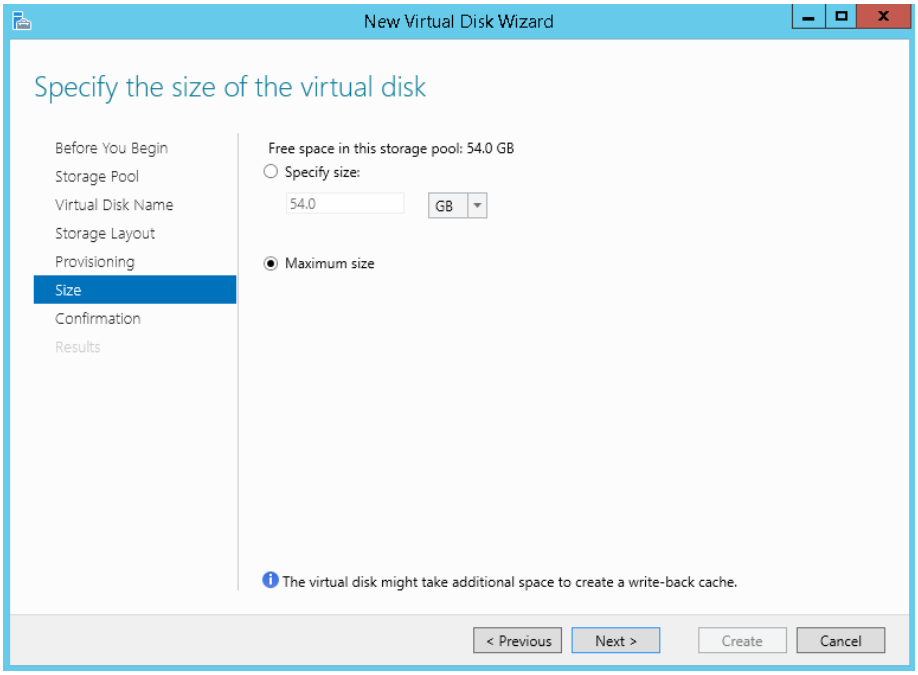

12. Cửa sổ **Select the storage layout**, chọn **Parity**, và chọn **Next**.



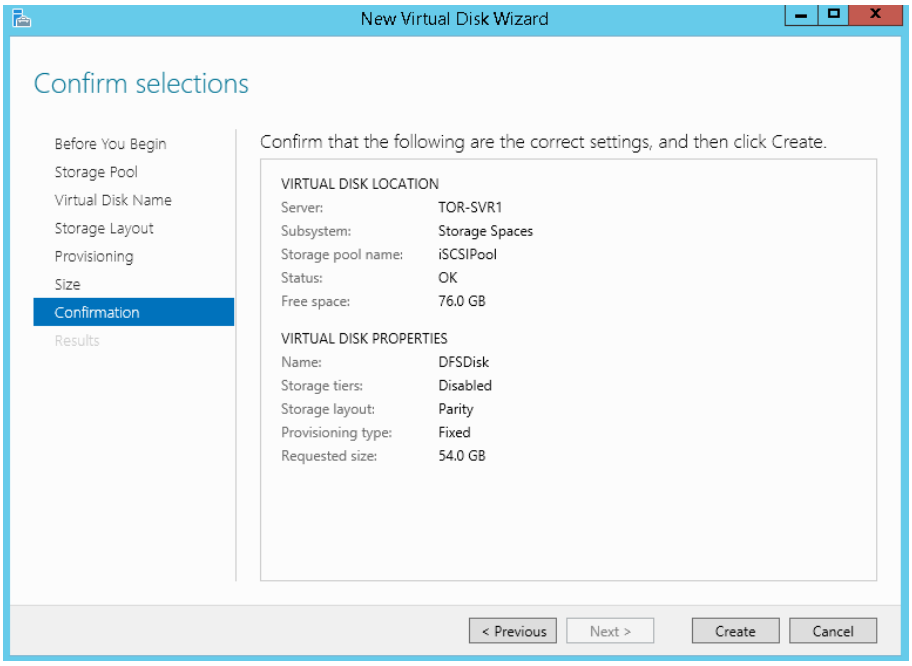
13. Cửa sổ **Specify the provisioning type**, chọn **Fixed**, và chọn **Next**.



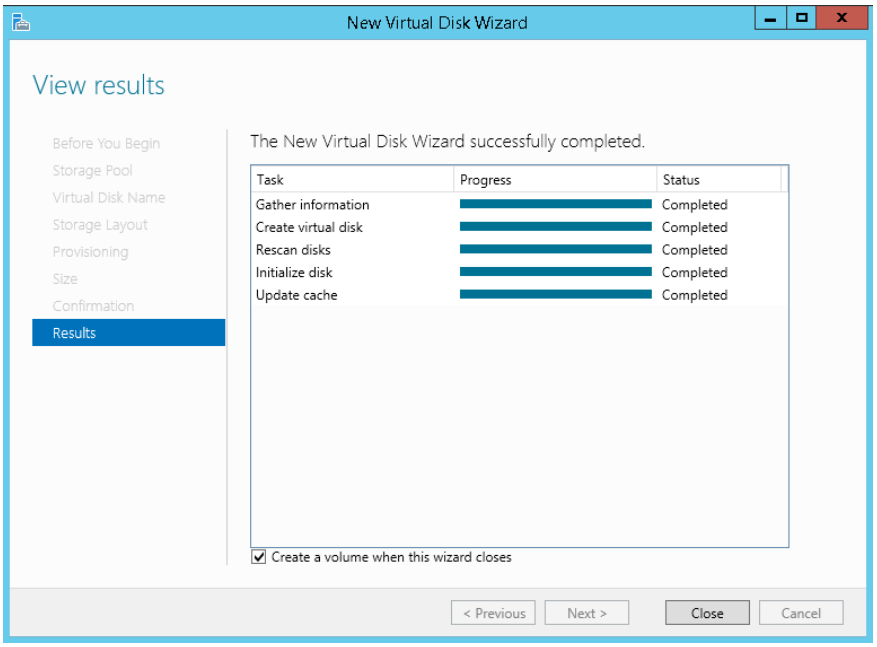

14. Cửa sổ **Specify the size of the virtual disk**, chọn **Maximum size**, và chọn **Next**.



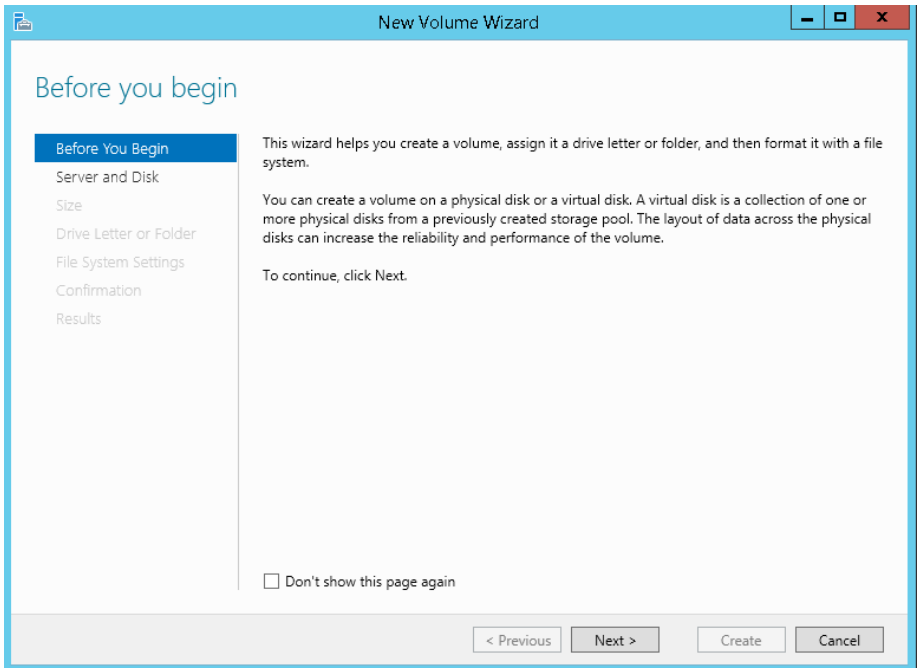
15. Cửa sổ **Confirm selections**, chọn **Create**.



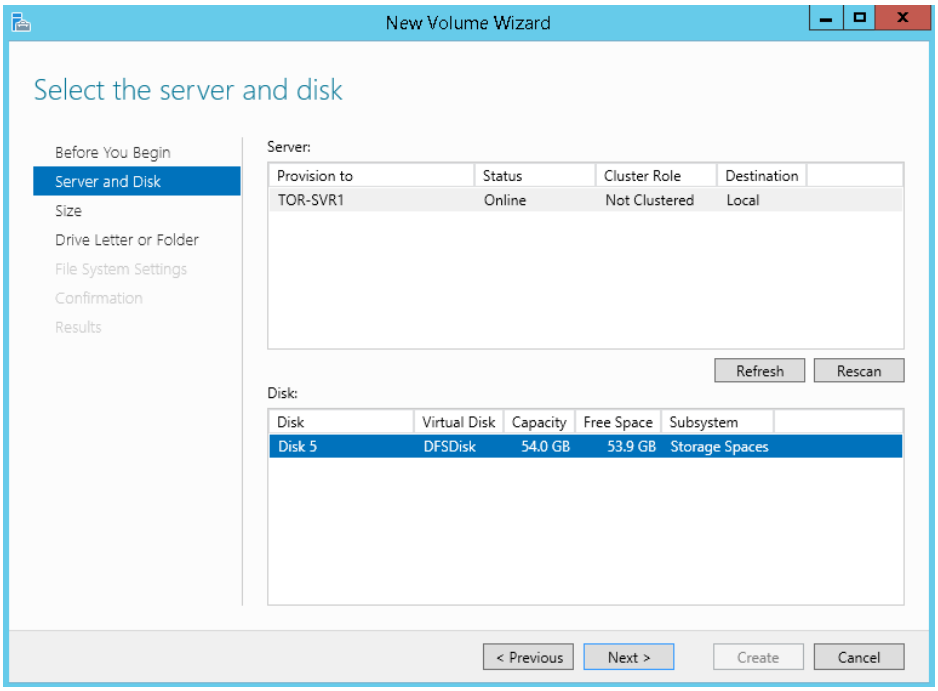

16. Cửa sổ **View results**, sau khi tạo thành công. Kiểm tra có đánh dấu chọn **Create a volume when this wizard closes**, và chọn **Close**.



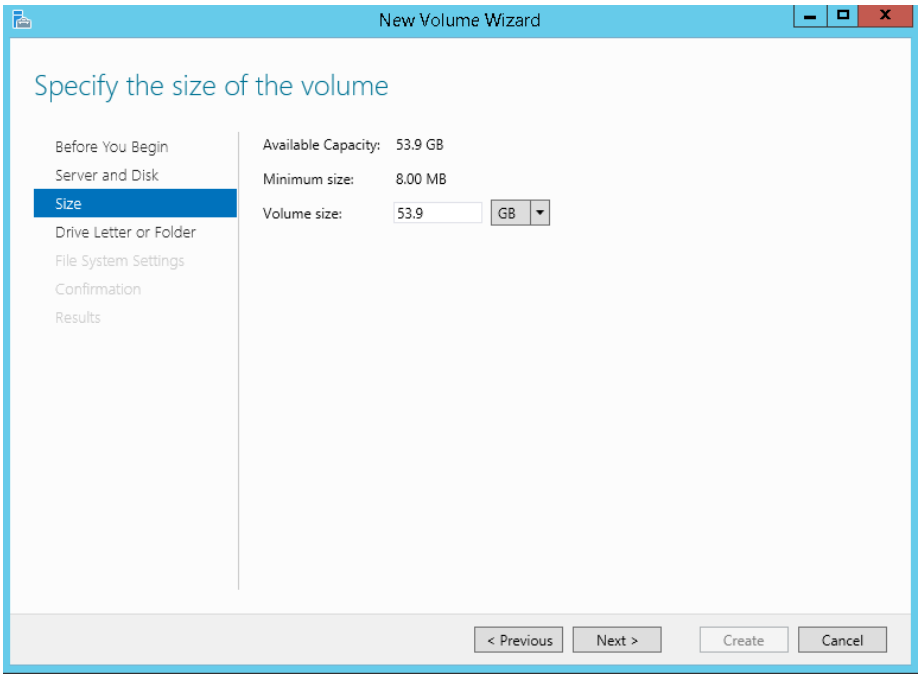
17. Cửa sổ **Before You Begin**, chọn **Next**.



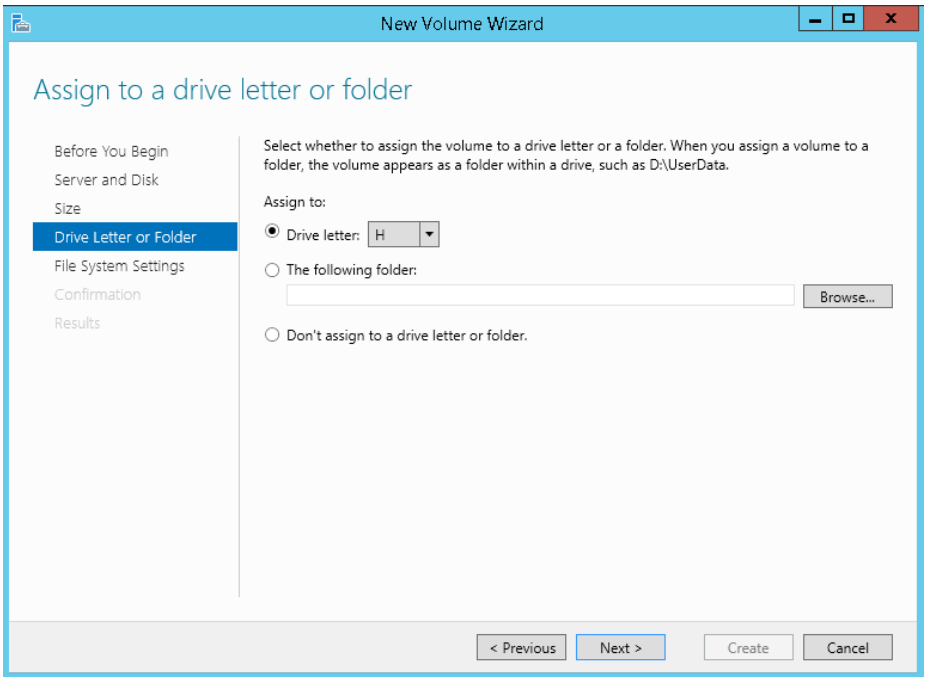

18. Cửa sổ **Select the server and disk**, chọn **DFSDisk**, và chọn **Next**.



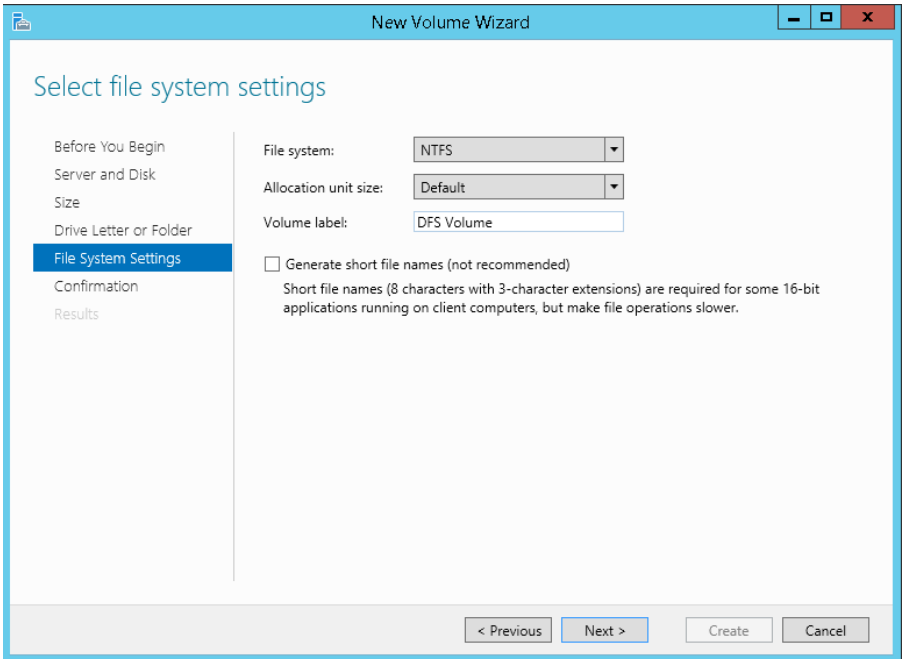
19. Cửa sổ **Specify the size of the volume**, chọn **Next**.



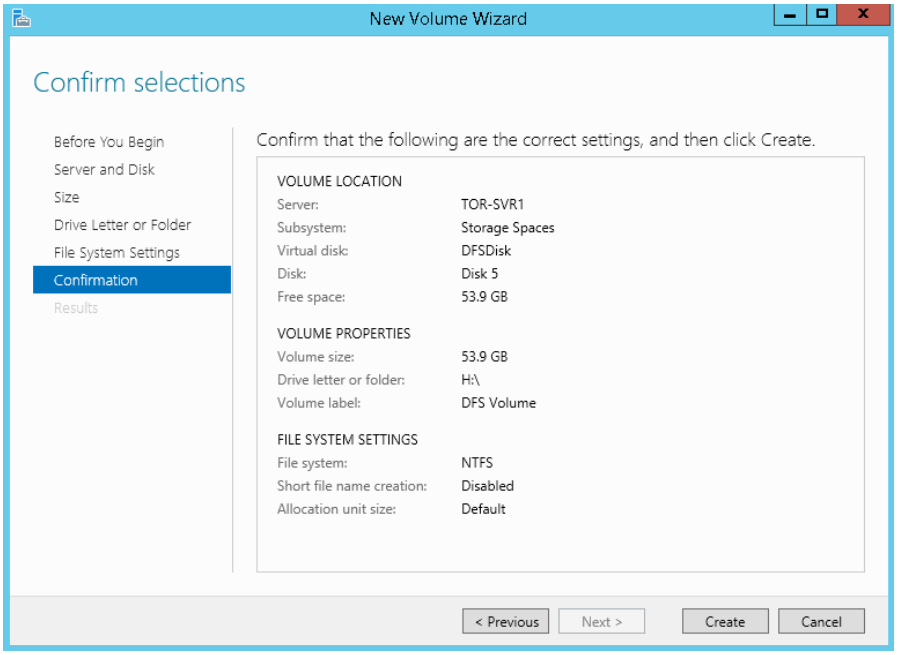

20. Cửa sổ **Assign to a drive letter or folder**, bung ô **Drive letter**, chọn **H**, và chọn **Next**.



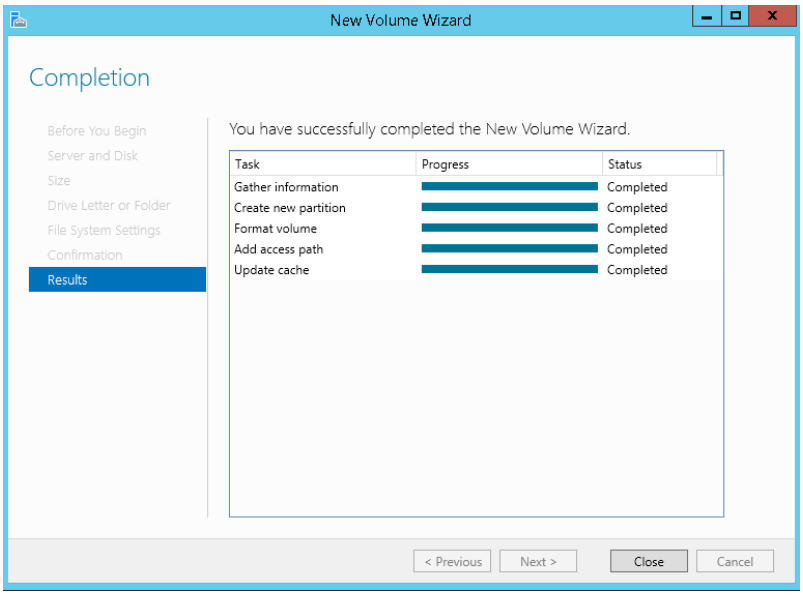
21. Cửa sổ **Select file system settings**, trong ô **Volume label**, nhập **DFS Volume**, và chọn **Next**.




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



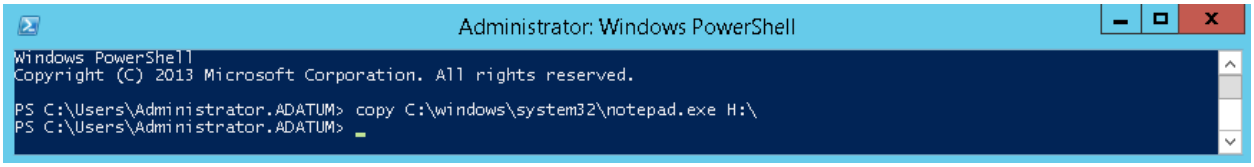
23. Cửa sổ **Completion**, sau khi tạo thành công, chọn **Close**.




## Bước 4. Kiểm tra khả năng sẵn sàng cao.

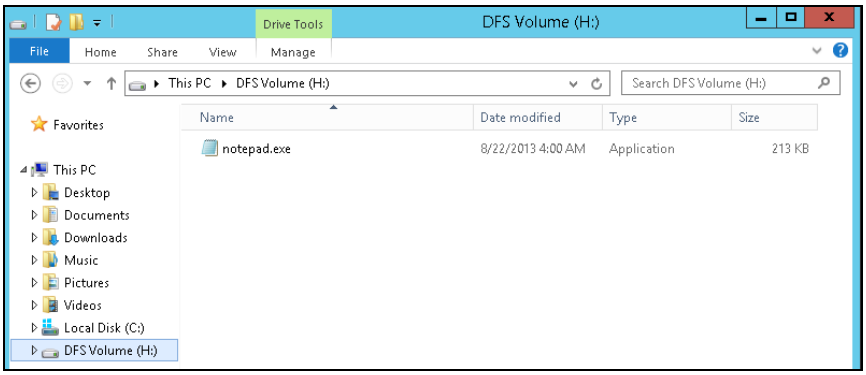
1. Trên máy **TOR-SVR1**, mở **Windows PowerShell**, gõ lệnh:

**Copy C:\windows\system32\notepad.exe H:**



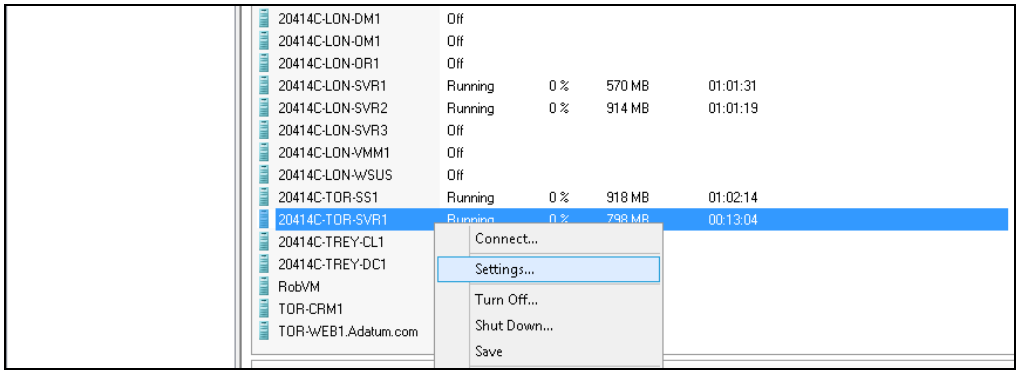

2. Tắt **Windows PowerShell**.

3. Mở **File Explorer,** vào ổ đĩa **DFSVolume (H:)**. Kiểm tra có file **notepad.exe**.

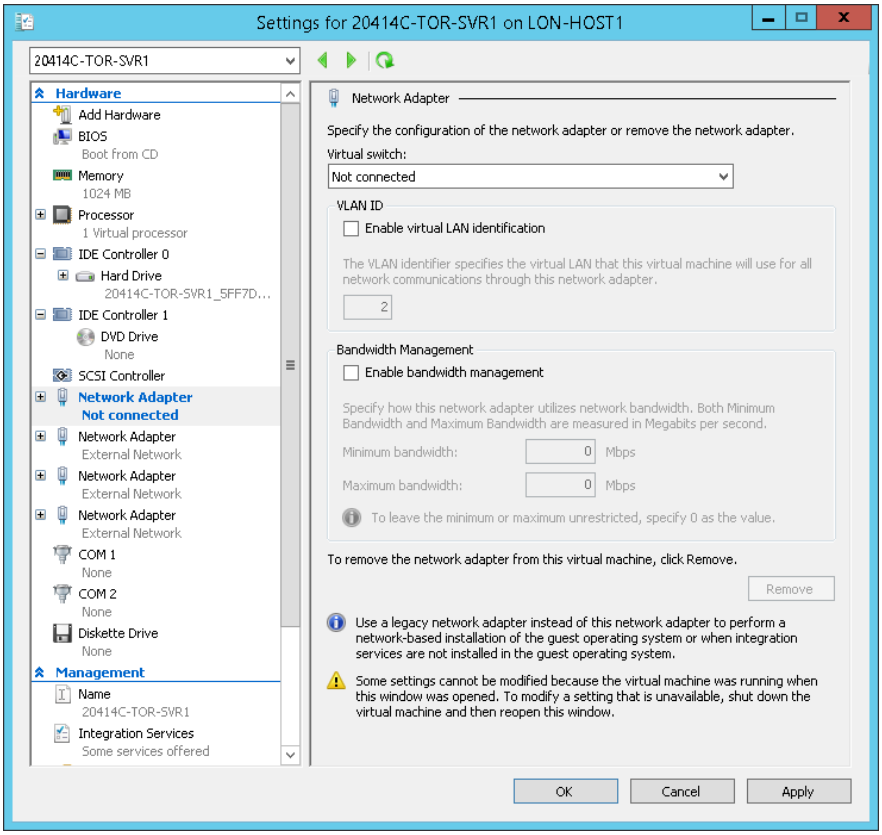


4. Tắt **File Explorer.**

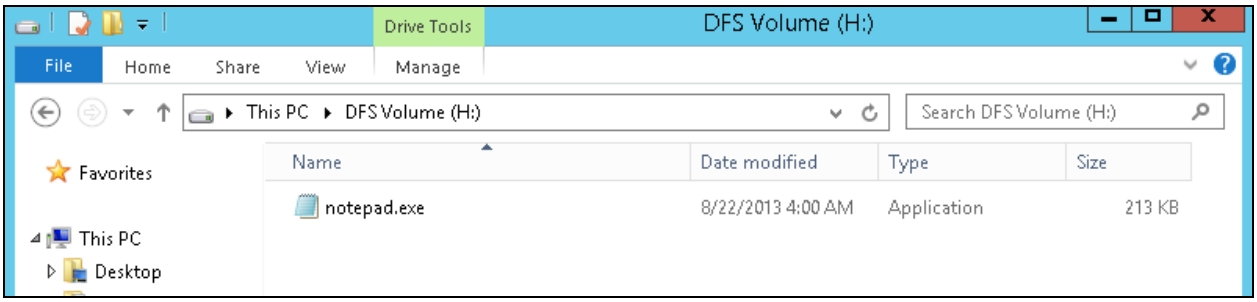
5. Trên máy thật, mở **Hyper-V Manager**, chuột phải máy ảo **20414C-TOR-SVR1**, chọn **Settings**.



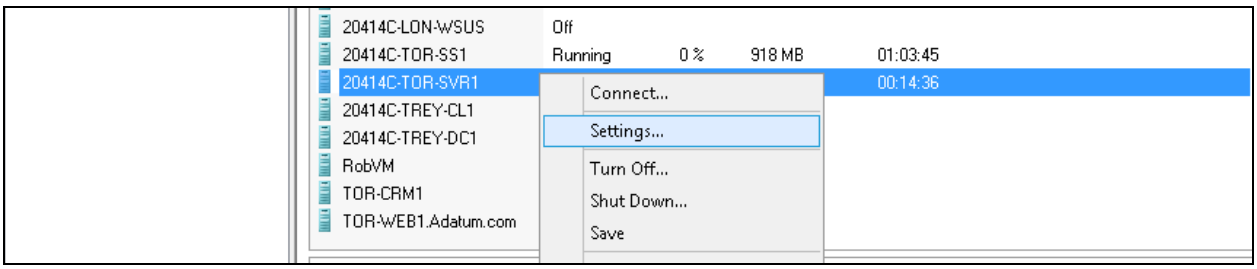

6. Hộp thoại **Settings for 20414C-TOR-SVR1**, chọn mục **Network Adapter** đầu tiên. Bung ô **Virtual Switch**, chọn **Not connected**, và chọn **OK**.



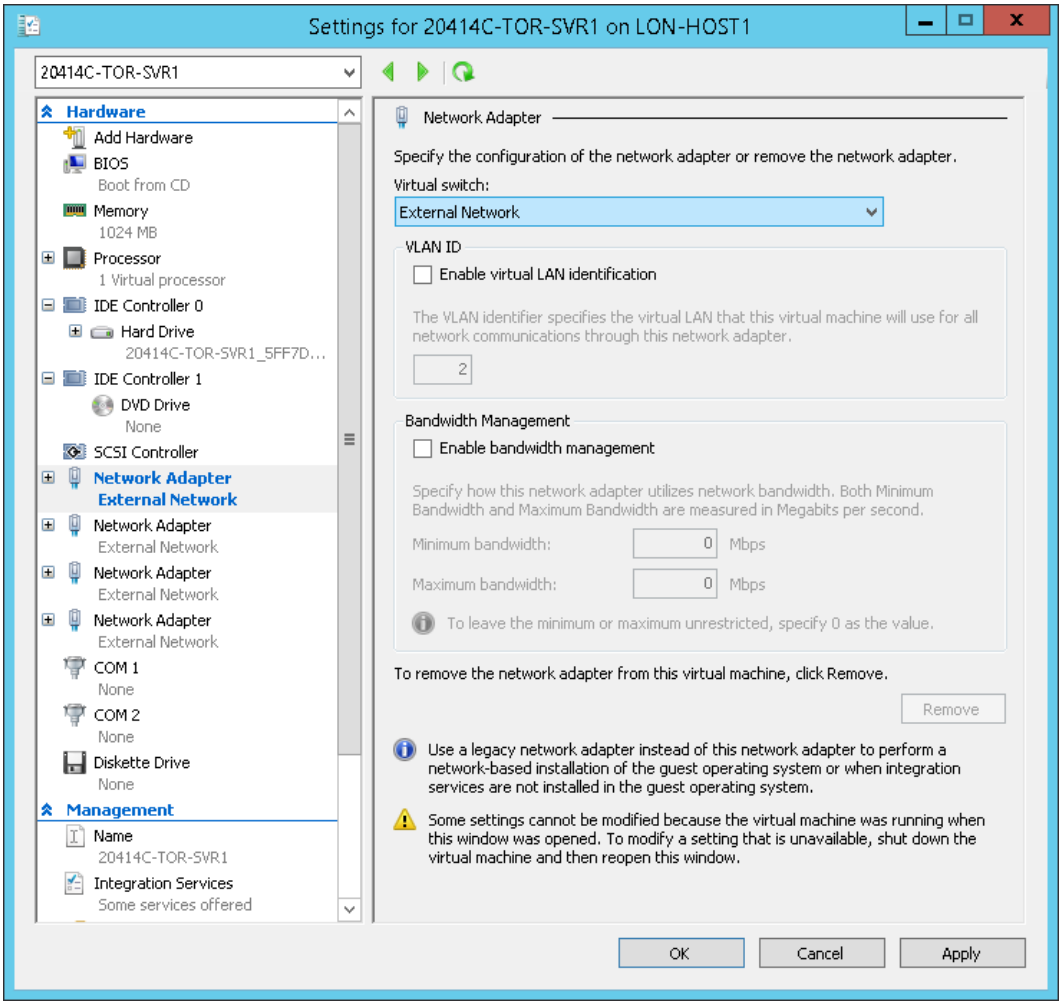
7. Trên **TOR-SVR1**, mở **File Explorer**, chọn **DFSVolume (H:)**. Kiểm tra vẫn còn file **notepad.exe** dù máy **TOR-SVR1** không còn kết nối vào hệ thống.




8. Trên máy thật, mở **Hyper-V Manager**, chuột phải máy ảo **20414C-TOR-SVR1**, chọn **Settings**.



9. Hộp thoại **Settings for 20414C-TOR-SVR1**, chọn mục **Network Adapter** đầu tiên. Bung ô **Virtual Switch**, chọn **External Network**, và chọn **OK**.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công giải pháp sẵn sàng cao cho việc lưu trữ dữ liệu.**

## Bài tập 2: Triển khai giải pháp sẵn sàng cao sử dụng Network Load Balancing (NLB).

❖ **Bài tập bao gồm các bước:**

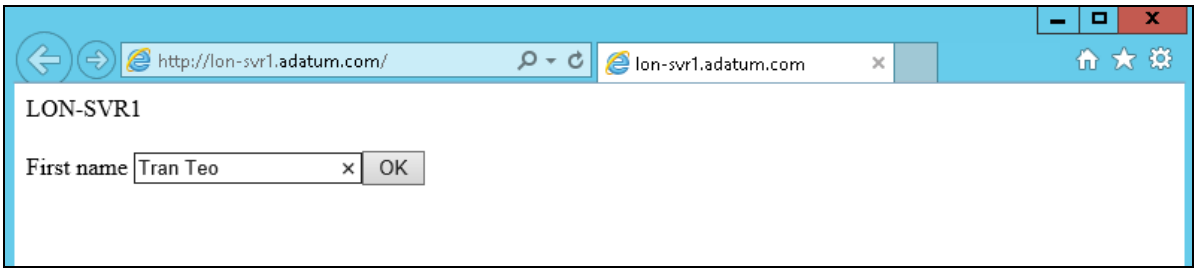
1. Cấu hình NLB cluster
2. Cấu hình các Web Servers sử dụng highly availability storage
3. Kiểm tra kết quả

❖ **Thực hiện:**

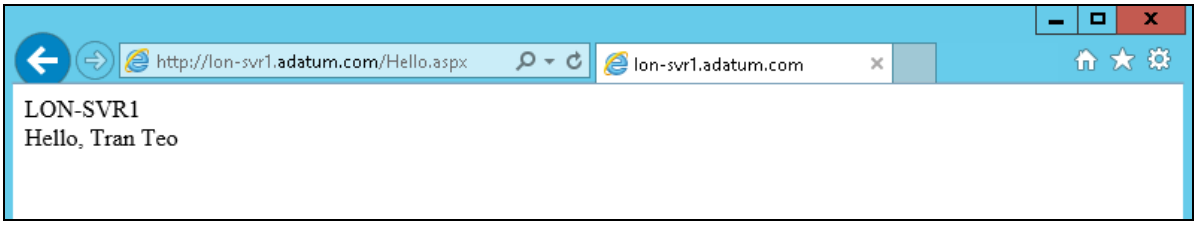
### Bước 1. Cấu hình NLB cluster

1. Sign in vào máy **LON-DC1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

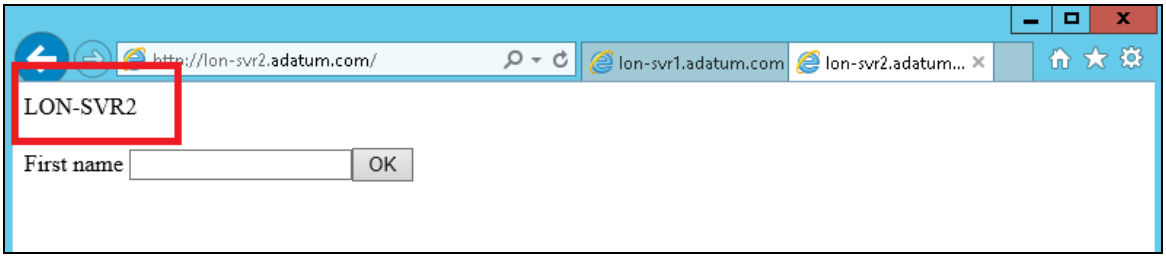
2. Mở **Internet Explorer**, truy cập **http://LON-SVR1.adatum.com**. Trong ô **First name**, nhập tên của bạn vào và chọn **OK**




3. Kiểm tra tin nhắn hiển thị với tên của bạn.

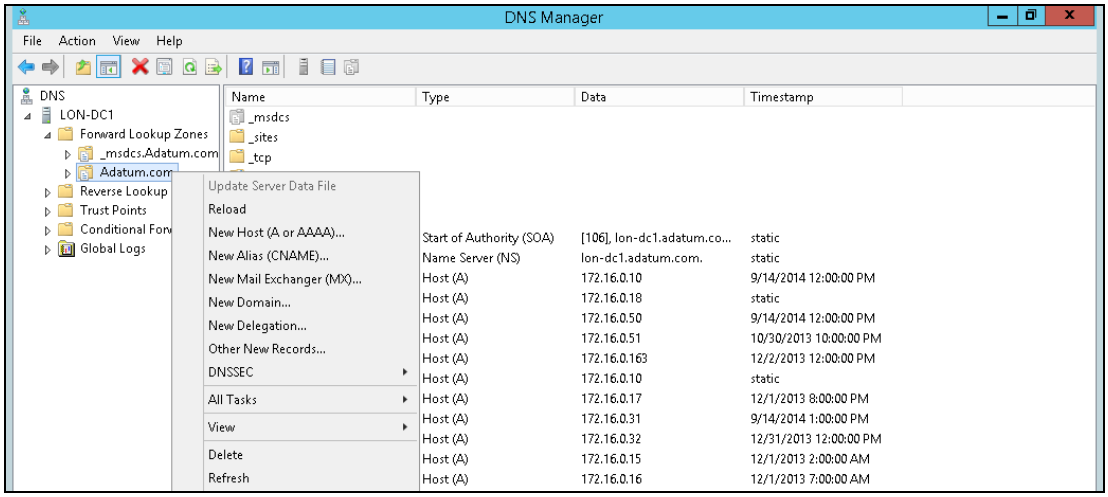



4. Mở **Internet Explorer**, truy cập **http://LON-SVR2.adatum.com.** Kiểm tra tên của server sẽ hiển thị ở phía trên cùng của trang.

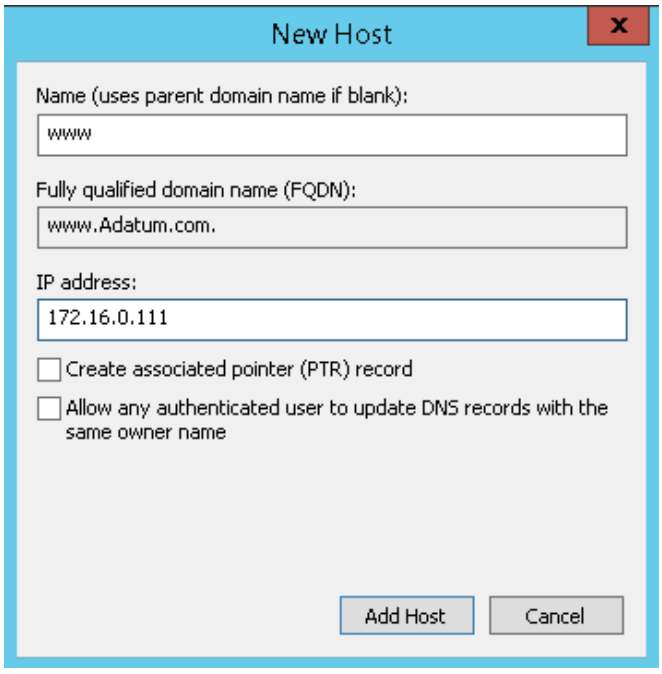


5. Trong **Server Manager,** bung **Tools**, mở **DNS**.

6. Trong cửa sổ **DNS Manager**, bung **LON-DC1**, bung **Forward Lookup Zones**, chuột phải **Adatum.com**, chọn **New Host (A or AAAA)**.



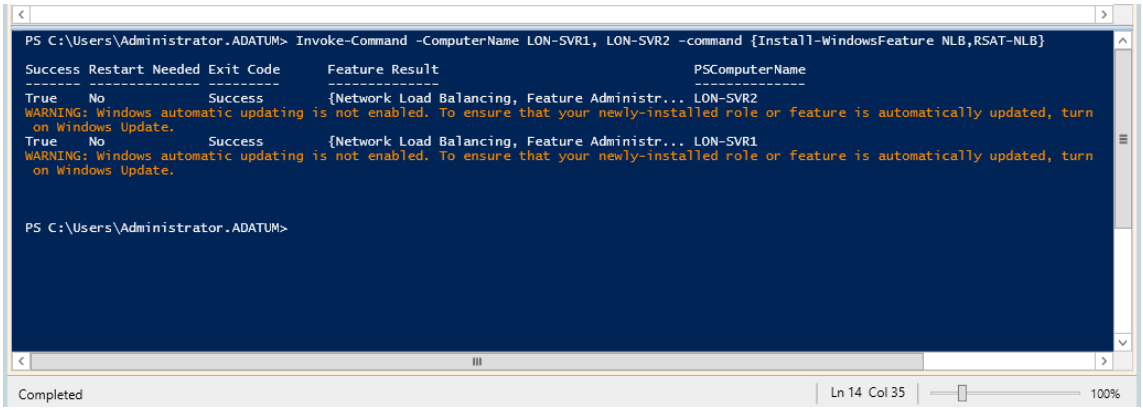

7. Hộp thoại **New Host**, trong ô **Name**, nhập **www**, trong ô **IP Address text**, nhập **172.16.0.111**, chọn **Add Host**, chọn **OK**, và chọn **Done**.



8. Qua máy **LON-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **Windows PowerShell ISE**.

9. Trong cửa sổ **Windows PowerShell Integrated Scripting Environment (ISE)**, gõ lệnh:

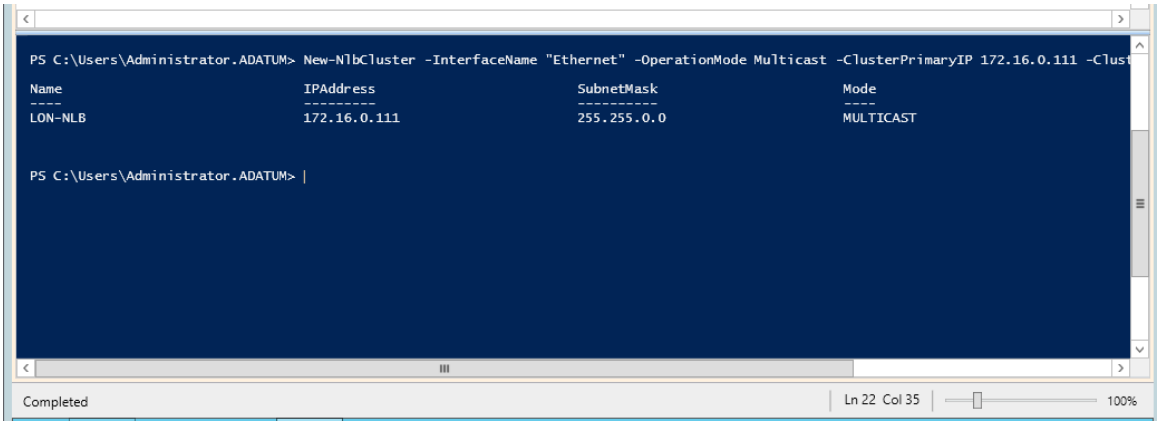
**Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature NLB,RSAT-NLB}**




**Chú ý:** Lệnh này để cài đặt feature **Network Load Balancing (NLB)** cho 2 máy **LON-SVR1** và **LON-SVR2**

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

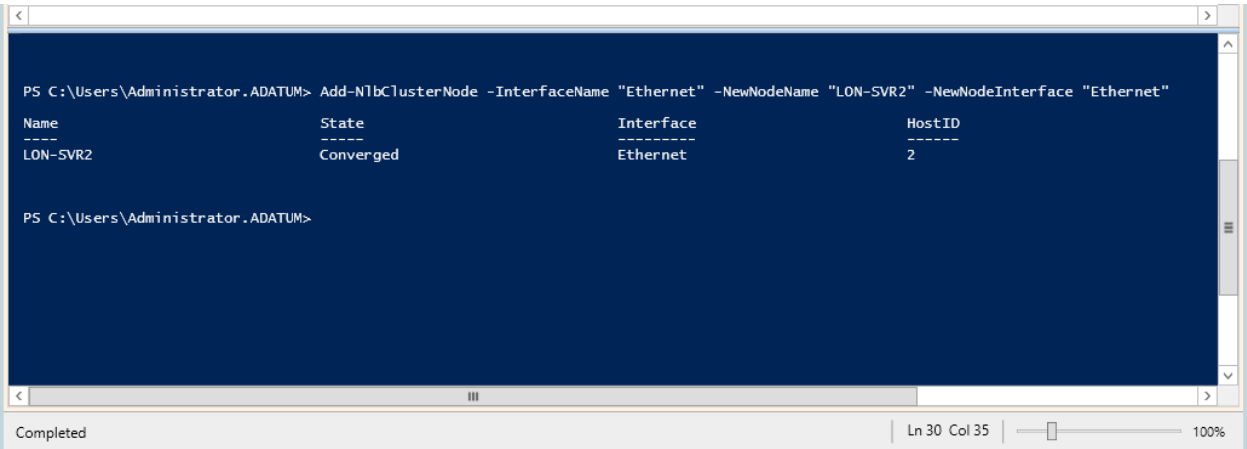
**New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP 172.16.0.111 -ClusterName LON-NLB**




**Chú ý:** Lệnh này để tạo NLB Cluster tên **LON-NLB** có Virtual IP **172.16.0.111**

11. Trong cửa sổ **Windows PowerShell ISE**, gõ lệnh:

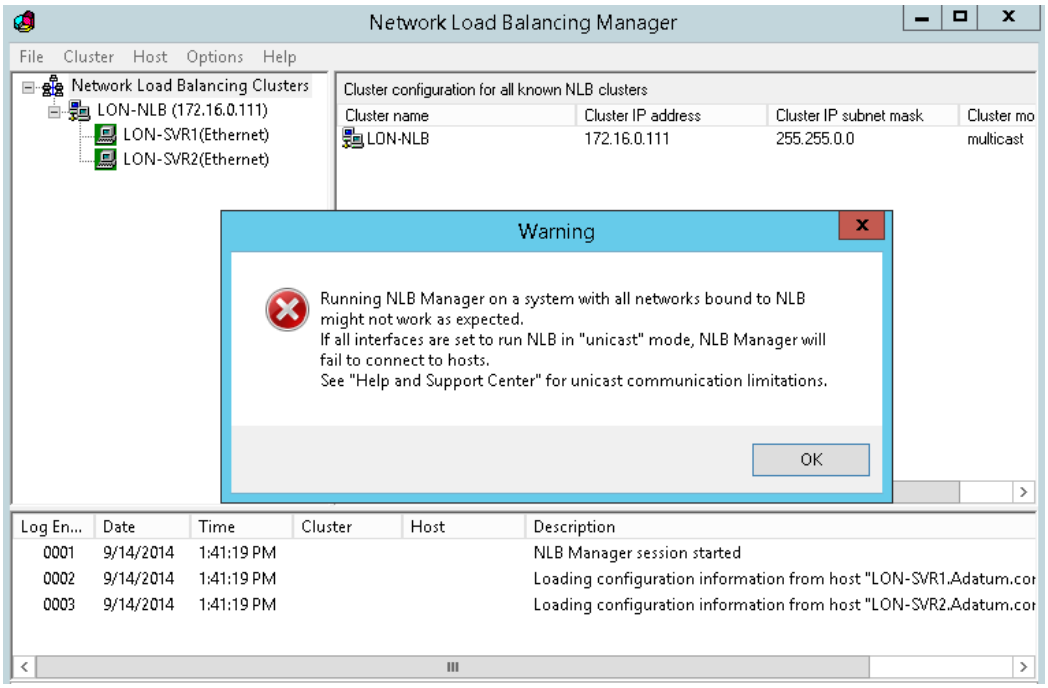
**Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -NewNodeInterface "Ethernet"**



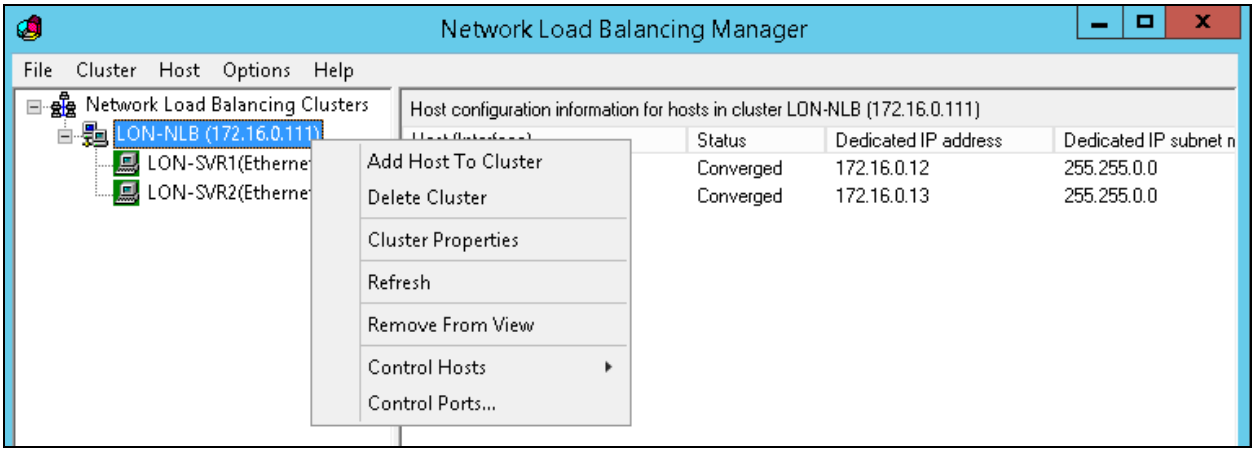

**Chú ý:** Lệnh này để add máy **LON-SVR2** vào cluster **LON-NLB**

12. Trong **Server Manager**, bung menu **Tools**, mở **Network Load Balancing Manager**

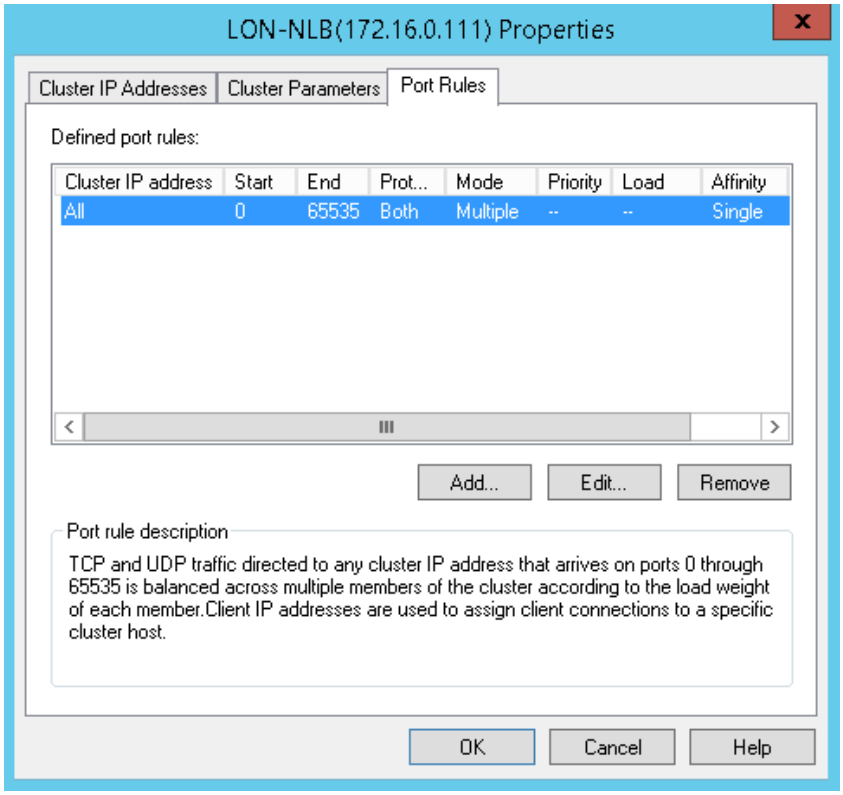
13. Hộp thoại cảnh báo, chọn **OK**.



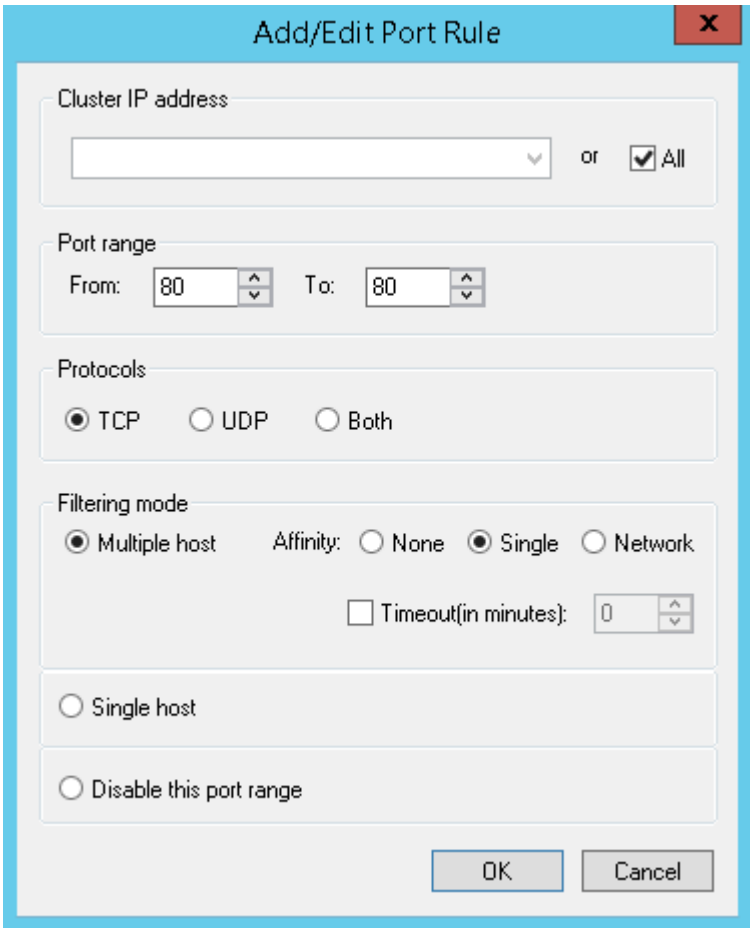
14. Trong cửa sổ **Network Load Balancing Manager**, chuột phải **LON-NLB**, chọn **Cluster Properties**.




15. Hộp thoại **Cluster Properties**, qua tab **Port Rules**, chọn rule **All**, chọn **Remove**. Sau đó chọn **Add**.



16. Hộp thoại **Add/Edit Port Rule**, nhập thông tin như hình bên dưới, và chọn **OK** 2 lần:

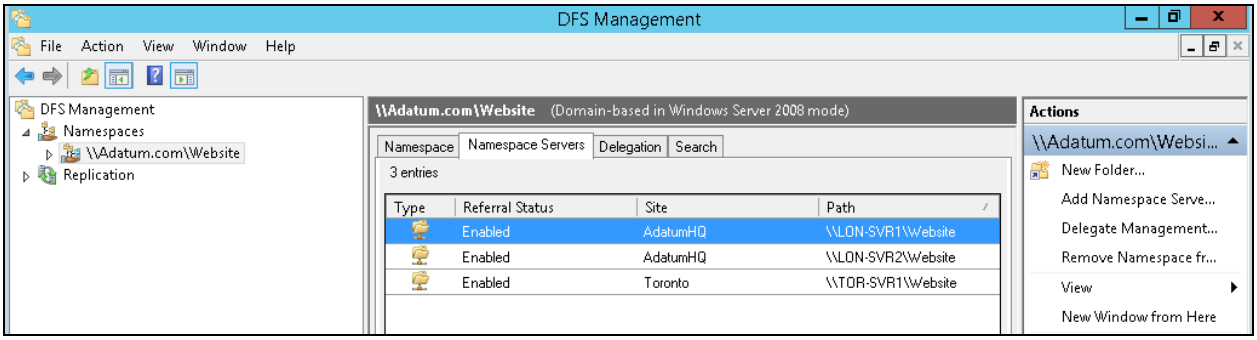


## Bước 2. Cấu hình các Web Servers sử dụng highly availability storage

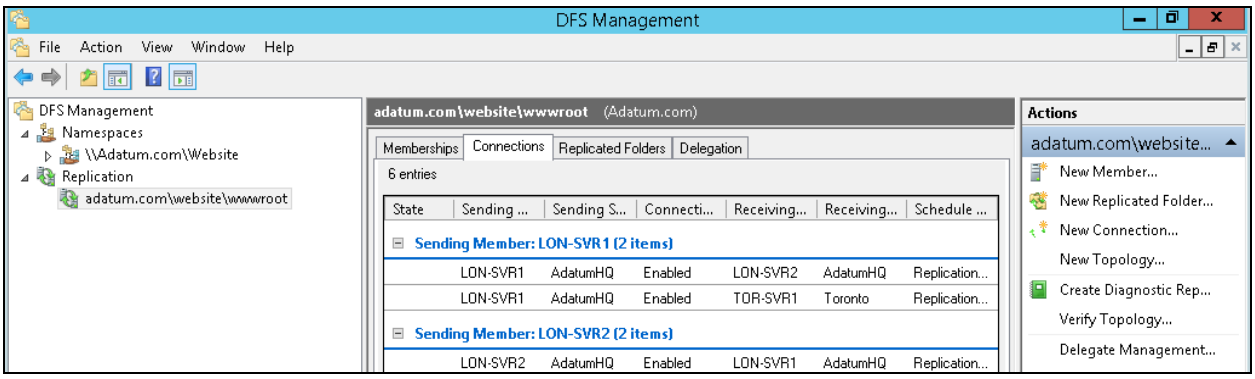
1. Qua máy **LON-SVR1**.

2. Trong **Server Manager**, bung menu **Tools**, mở **DFS Management**.

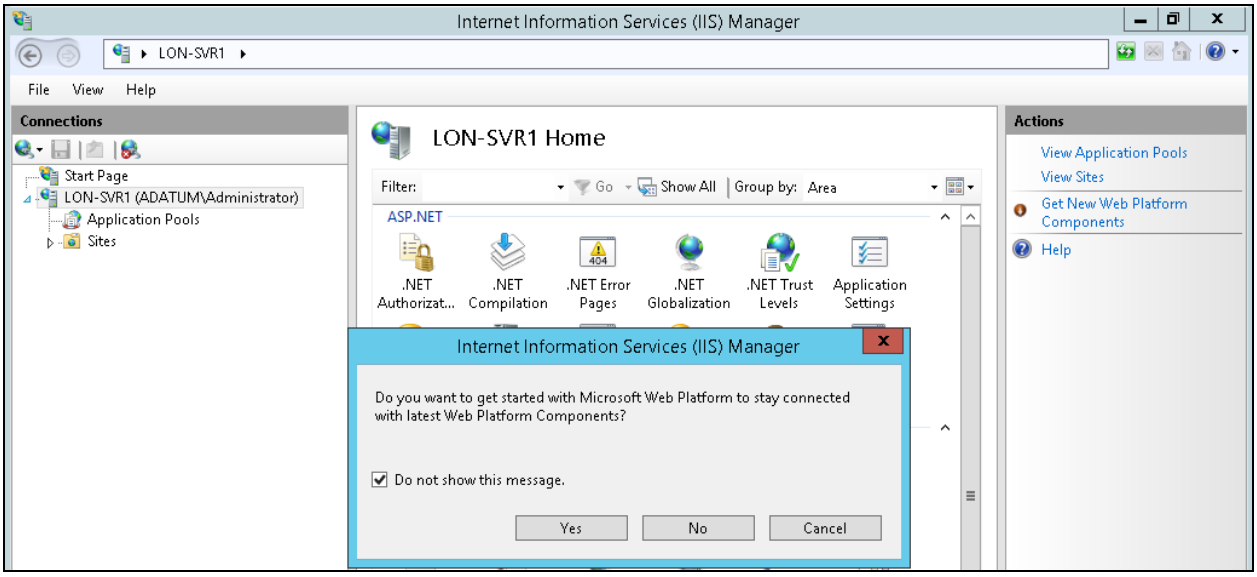
3. Trong cửa sổ **DFS Management**, bung **Namespaces**, chọn **\\Adatum.com\Website**, qua tab **Namespace Servers**. Kiểm tra có 3 server: **LON-SVR1, LON-SVR2, TOR-SVR1**



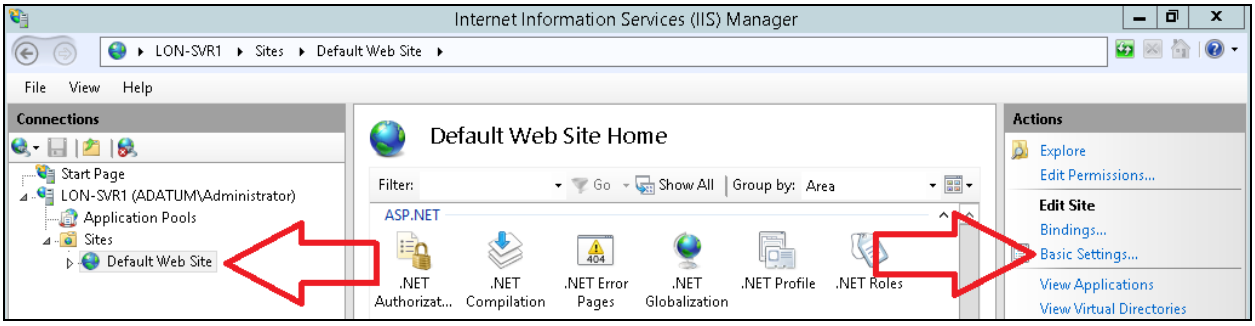

4. Bung **Replication**, chọn **adatum.com\website\wwwroot**, qua tab **Connections**. Kiểm tra mỗi máy chủ đang đồng bộ với hai máy chủ khác. Tắt cửa sổ **DFS Management**.



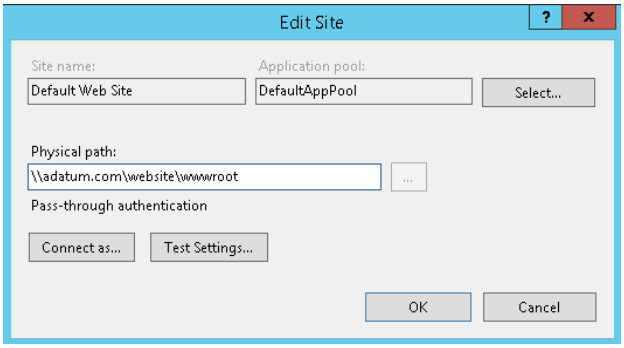
5. Trong **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**. Hộp thoại thông báo, đánh dấu chọn **Do not show this message**, và chọn **Yes**.



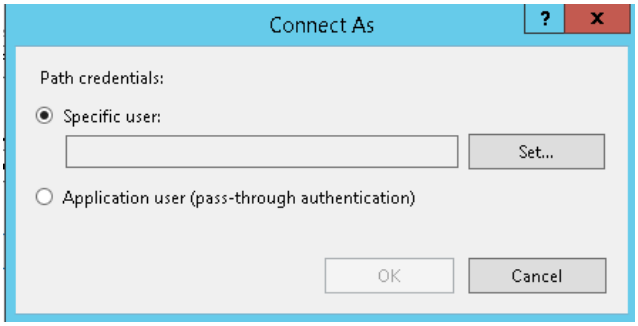

6. Bung **LON-SVR1**, bung **Sites**, chọn **Default Web Site**. Trong cửa sổ **Actions**, chọn **Basic Settings**.



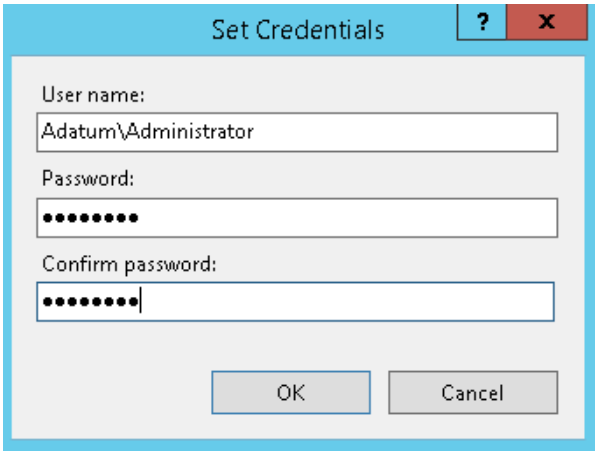
7. Hộp thoại **Edit Site**, trong ô **Physical path**, nhập **\\adatum.com\website\wwwroot**, chọn **Connect as**.




8. Hộp thoại **Connect as**, chọn **Specific user**, và chọn **Set**.




9. Hộp thoại **Set Credentials**, nhập **Adatum\administrator** vào ô **User name**, nhập **Pa$$w0rd** vào ô **Password** và **Confirm password**. Chọn **OK** 3 lần, và tắt Internet Information Services (IIS) Manager.

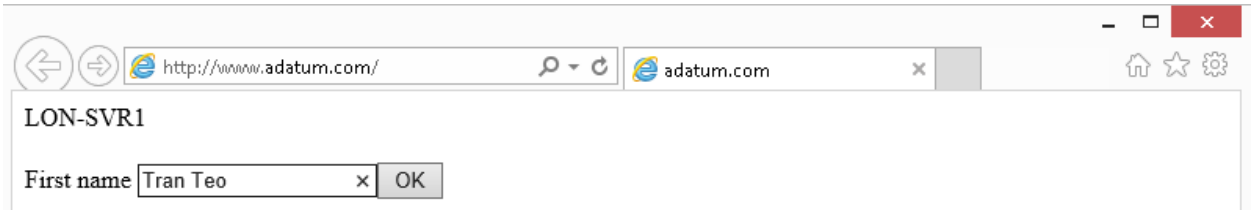


10. Lặp lại từ bước 5 tới bước 9 cho máy **LON-SVR2**.

**Bước 3. Kiểm tra kết quả**

1. Qua máy **LON-CL1**.

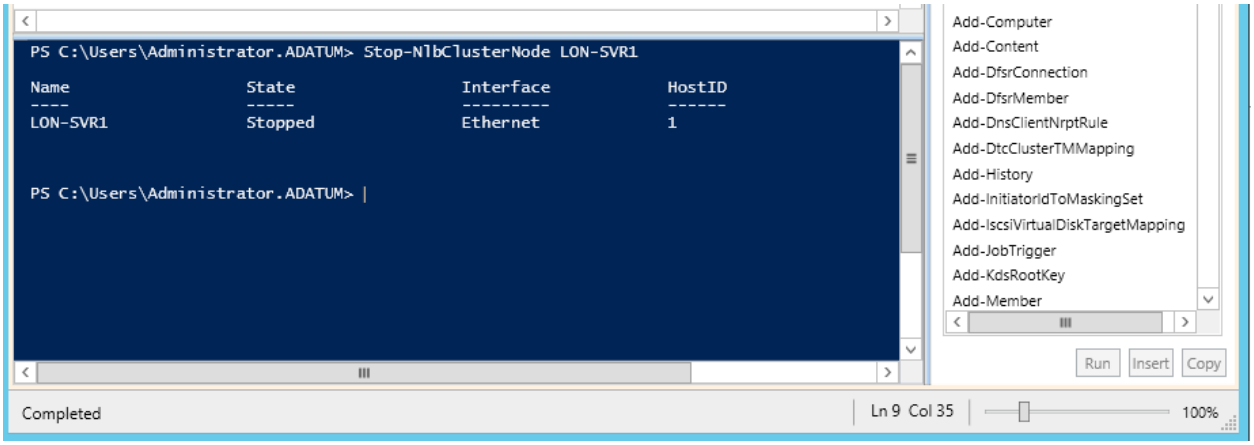
2. Mở **Internet Explorer**, truy cập **http://www.adatum.com**. Lưu ý tên của server đang truy cập sẽ hiển thị ở phía trên cùng của trang. Nhấn phím **F5** 20 lần. Lưu ý tên máy chủ không thay đổi.




3. Qua máy **LON-SVR1**.

4. Trong **Server Manager**, bung menu **Tools**, mở **Windows PowerShell ISE**, gõ lệnh:

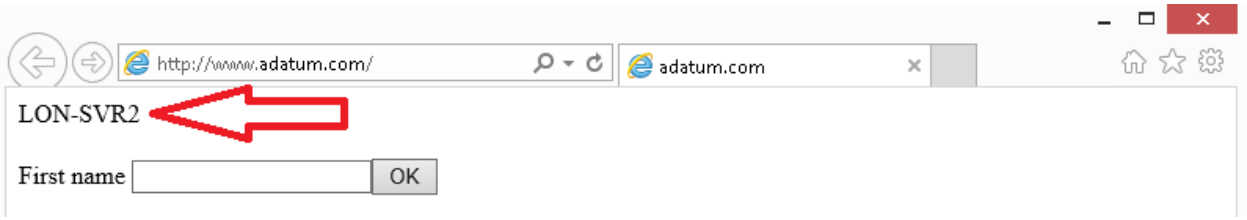
**Stop-NlbClusterNode *servername***




**Lưu ý:** Thế ***servername*** là tên của máy chủ mà bạn kết nối trong các bước trên. (vd: **LON-SVR1**)

5. Qua máy **LON-CL1.**

6. Mở **Internet Explorer**, truy cập **http://www.adatum.com**. Kiểm tra bạn đang kết nối với một web server khác (vd: LON-SVR2).




7. Qua máy **LON-SVR1**.

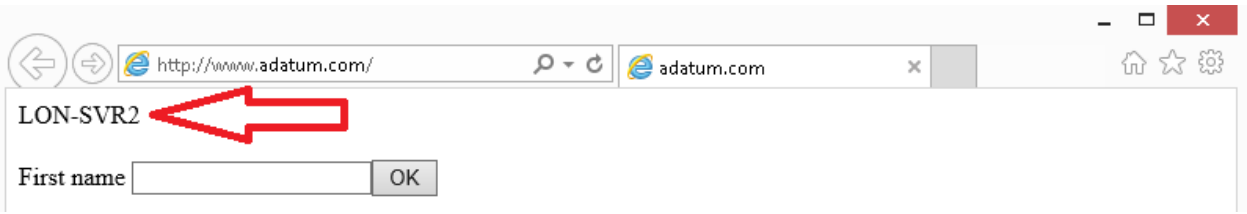
8. Mở **Windows PowerShell ISE** , gõ lệnh:

**Start-NlbClusterNode *servername***

**Lưu ý:** Thế ***servername*** là tên của máy chủ mà bạn kết nối trong các bước trên. (vd: **LON-SVR1**)

9. Qua máy **LON-CL1**.

10. Trong cửa sổ **Internet Explorer,** nhấn phím **F5**. Kiểm tra tên server không thay đổi.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công giải pháp sẵn sàng cao cho hệ thống Web bằng công nghệ Network Load Balancing (NLB).**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20414C-LON-CL1, 20414C-LON-SVR1, 20414C-LON-SVR2, 20414C-TOR-SVR1, 20414C-TOR-SS1.**

# Bài 7: Triển khai khả năng sẵn sàng cao cho hệ thống ảo hóa bằng công nghệ Failover Clustering

**I. Mục tiêu:**

- Triển khai Failover Cluster.
- Cấu hình Scale-Out File Server.
- Cấu hình Cluster-Aware Updating (CAU).
- Triển khai khả năng sẵn sàng cao cho hệ thống ảo hóa.

**II. Kịch bản và các yêu cầu tổng quan:**

Một trong những yêu cầu quan trọng cho triển khai Windows Server 2012 tại công ty A. Datum là tất cả các dịch vụ, ứng dụng và máy chủ phải có khả năng sẵn sàng cao. A. Datum đã cấu hình khả năng sẵn sàng cao cho vấn đề lưu trữ dữ liệu và các ứng dụng web. Bây giờ tổ chức muốn cung cấp khả năng sẵn sàng cao cho các máy chủ và các ứng dụng không thể sử dụng giải pháp Network Load Balancing (NLB).

A. Datum đã quyết định sử dụng giải pháp Failover Clustering để hỗ trợ khả năng sẵn sàng cao cho các dịch vụ này. Bạn phải lập kế hoạch và thực hiện giải pháp Failover Clustering để giải quyết các yêu cầu tại A. Datum. Ngoài ra, A. Datum muốn sử dụng tính năng sẵn sàng cao mới trong Windows Server 2012 là Scale-Out File Server, và thực hiện các thủ tục tự động cập nhật cho các node trong cluster bằng chức năng Cluster-Aware Updating (CAU).

Để giám sát hệ thống, A. Datum đã triển khai Microsoft System Center Operations Manager 2012, bây giờ họ muốn tích hợp sản phẩm này với Microsoft System Center VMM 2012 để quản lý môi trường ảo hóa và Hyper-V hosts.

**III. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1** (Máy thật)<br>**20414C-LON-DC1**<br>**20414C-LON-OM1**<br>**20414C-LON-SVR1**<br>**20414C-LON-SVR2**<br>**20414C-LON-VMM1**<br>**20414C-LON-HOST2** (Máy thật) |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**IV. Chuẩn bị:**

Bài thực hành gồm 2 máy thật, 1 máy khởi động **20414C-LON-HOST1** và 1 máy khởi động **20414C-LON-HOST2**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên lại từ bước 1 đến 3 cho các máy ảo còn lại.

**V. Thực hành:**

*Thời gian thực hành: 100 phút*

**Bài tập 1: Triển khai Failover Cluster.**

Bước đầu tiên trong việc triển khai Failover Clustering cho các ứng dụng và các máy ảo là tạo Failover Cluster. Bạn phải cấu hình một Failover Cluster có 2 node. A. Datum đã có iSCSI Storage để lưu trữ cho Failover Cluster. Ngoài ra, bạn có hai server vật lý làm Hyper-V hosts trong Cluster.

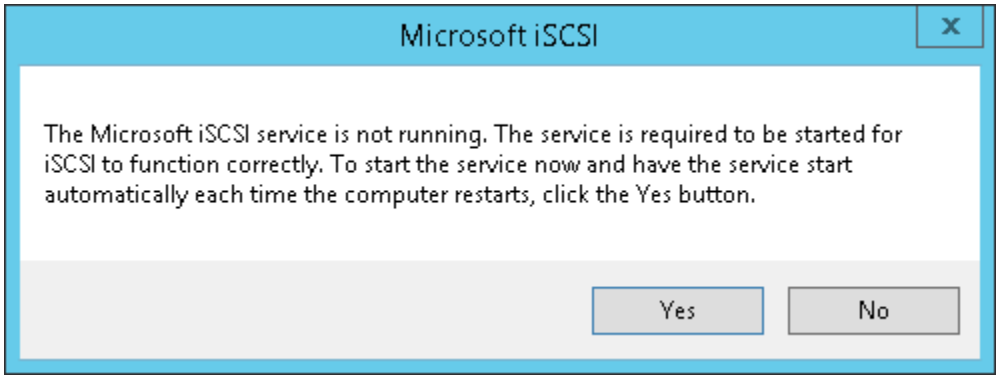
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình cho 2 Server vật lý kết nối tới iSCSI Targets.
2. Cài đặt và cấu hình Failover Clustering trên 2 Server vật lý
3. Cấu hình Cluster
4. Xác nhận cấu hình Cluster

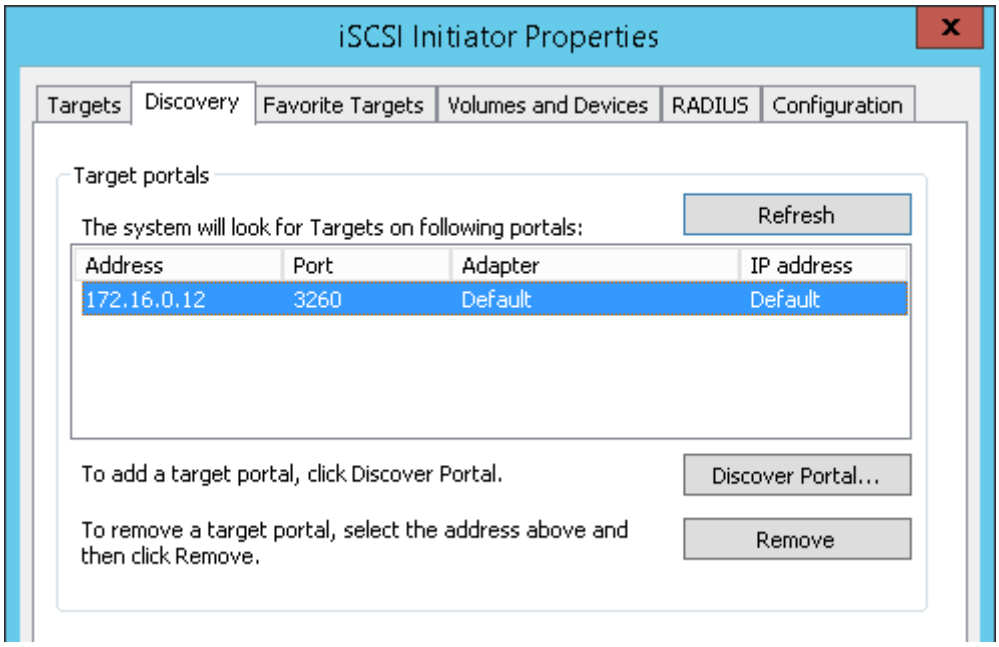
❖ **Thực hiện:**

**Bước 1. Cấu hình cho 2 Server vật lý kết nối tới iSCSI Targets.**

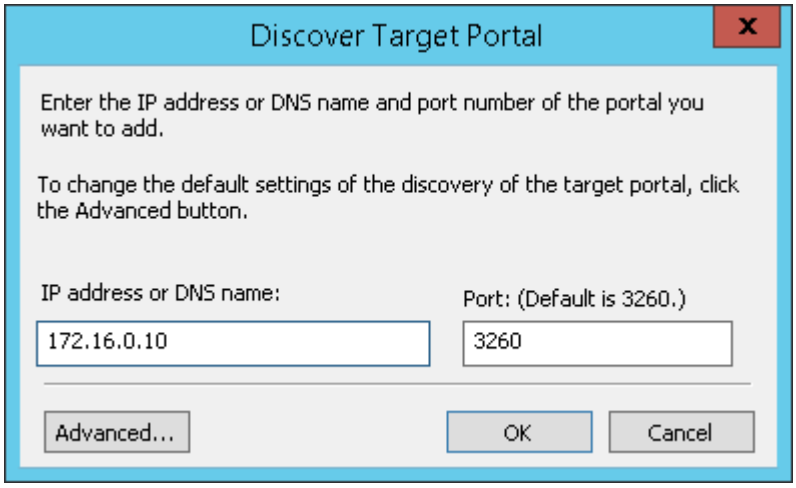
1. Trên máy **LON-HOST1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **iSCSI Initiator**, hộp thoại **Microsoft iSCSI**, chọn **Yes**.



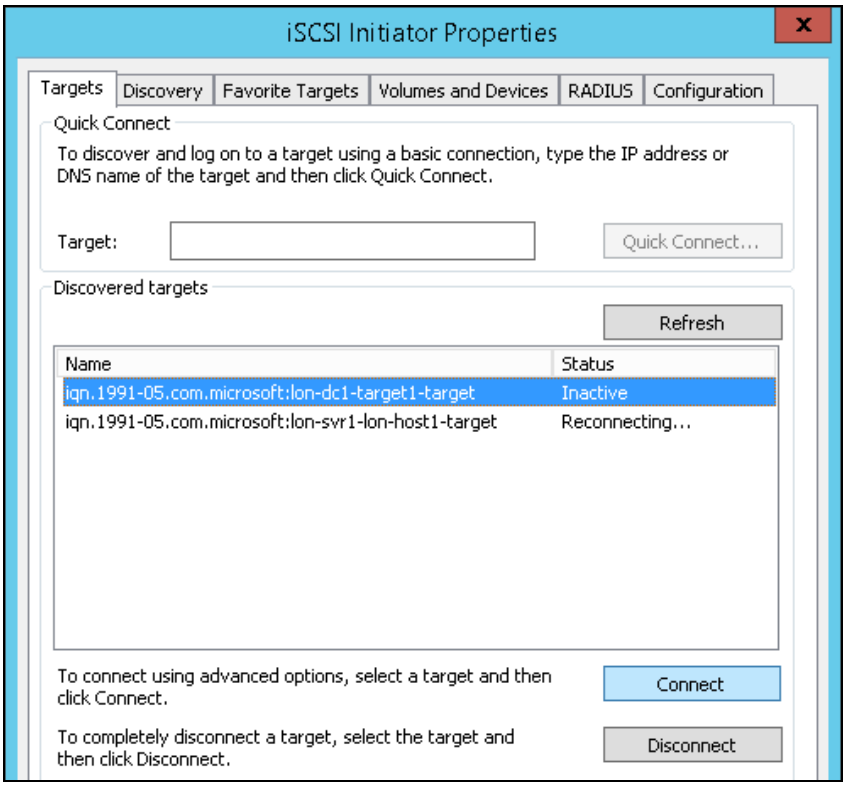
2. Hộp thoại **iSCSI Initiator,** qua tab **Discovery**, chọn **Discover Portal…**



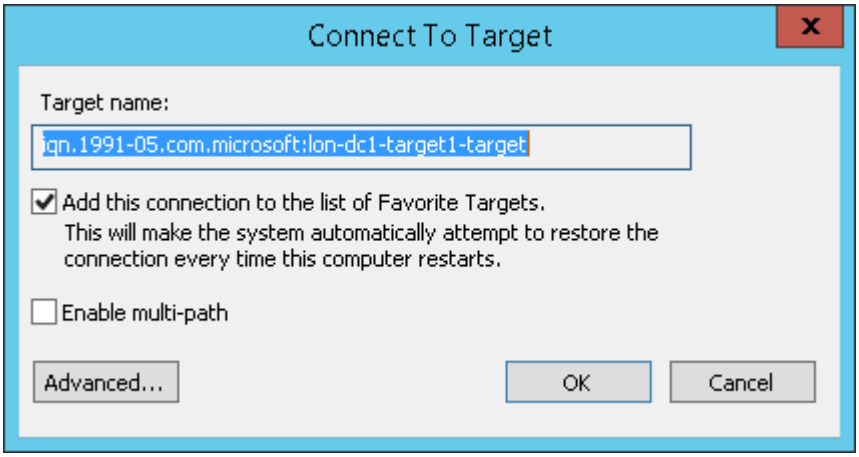

3. Trong ô **IP address or DNS name**, nhập **172.16.0.10**, và chọn **OK**.



4. Hộp thoại **iSCSI Initiator,** qua tab **Targets**, chọn **Refresh**, trong ô **Targets**, chọn **iqn.1991-05.com.microsoft:lon-dc1- target1-target**, và chọn **Connect**.

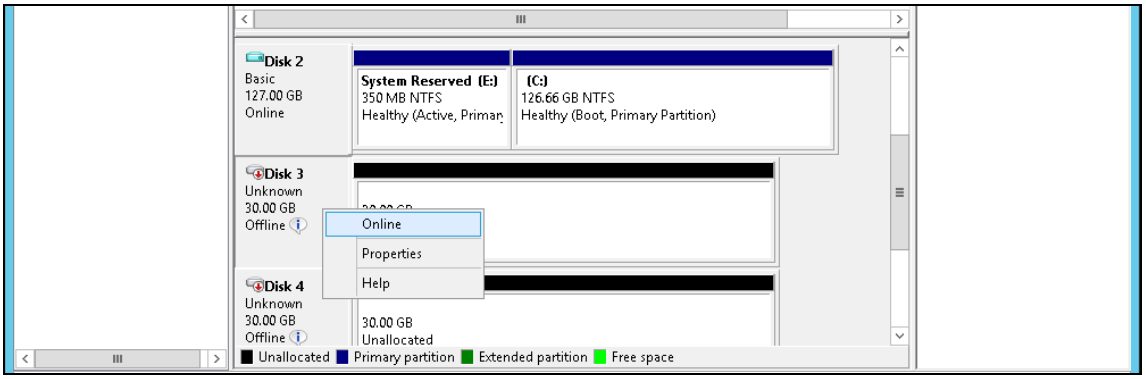



5. Hộp thoại **Connect To Target**, đánh dấu chọn **Add this connection to the list of Favorite Targets**, và chọn **OK** 2 lần.

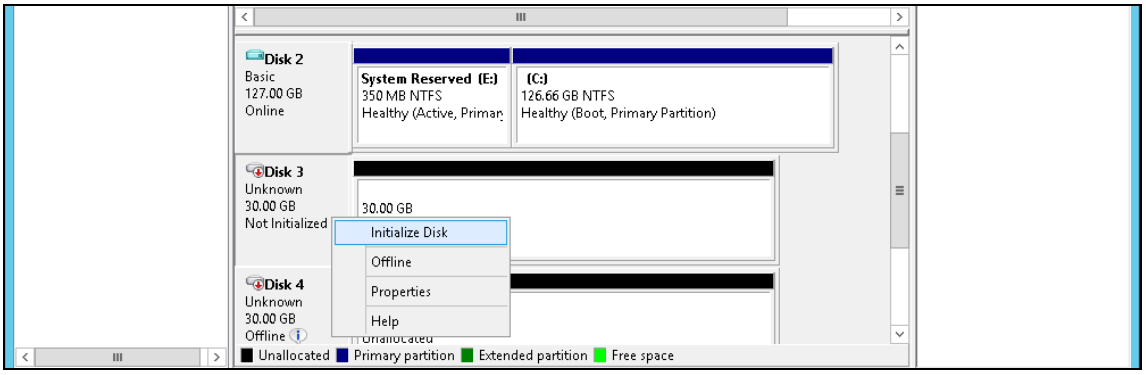


6. Lặp lại từ bước 1 đến 5 trên máy **LON-HOST2**

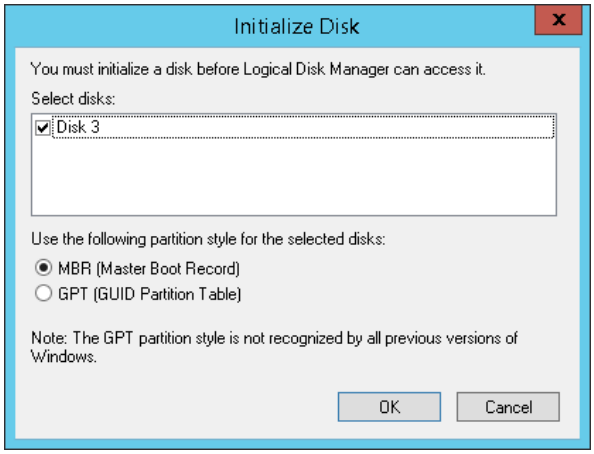
7. Trên máy **LON-HOST2**, trong **Server Manager**, bung menu **Tools**, mở **Computer Management**. Bung **Storage**, chọn **Disk Management**, chuột phải **Disk 3**, chọn **Online**.



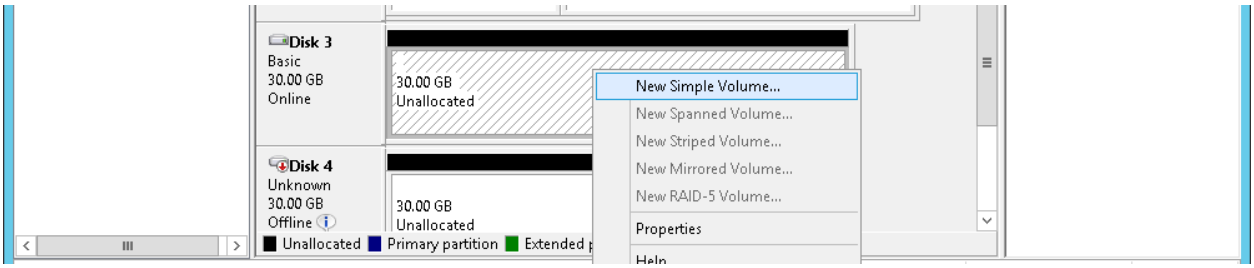

8. Chuột phải **Disk 3**, chọn **Initialize Disk**.




9. Hộp thoại **Initialize Disk**, chọn **OK**.

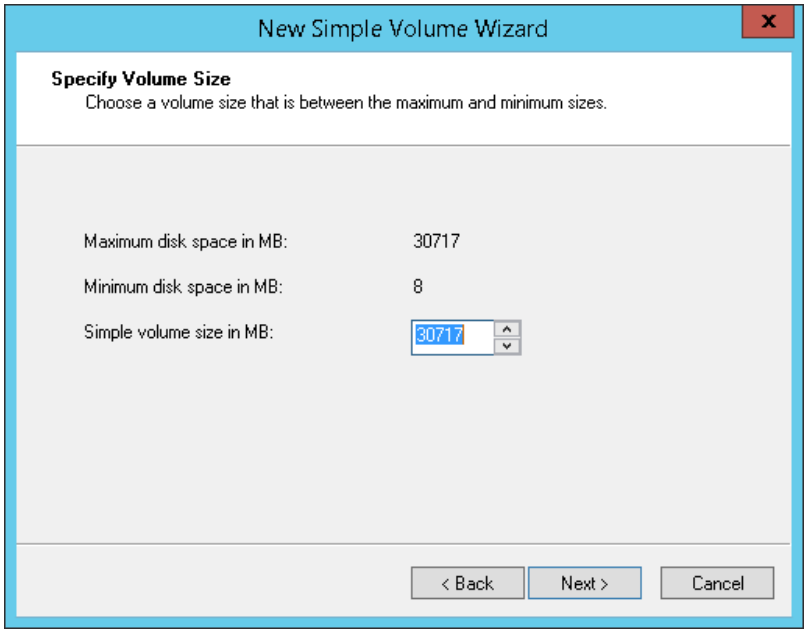


10. Chuột phải lên phần **Unallocated** của **Disk 3**, chọn **New Simple Volume**.



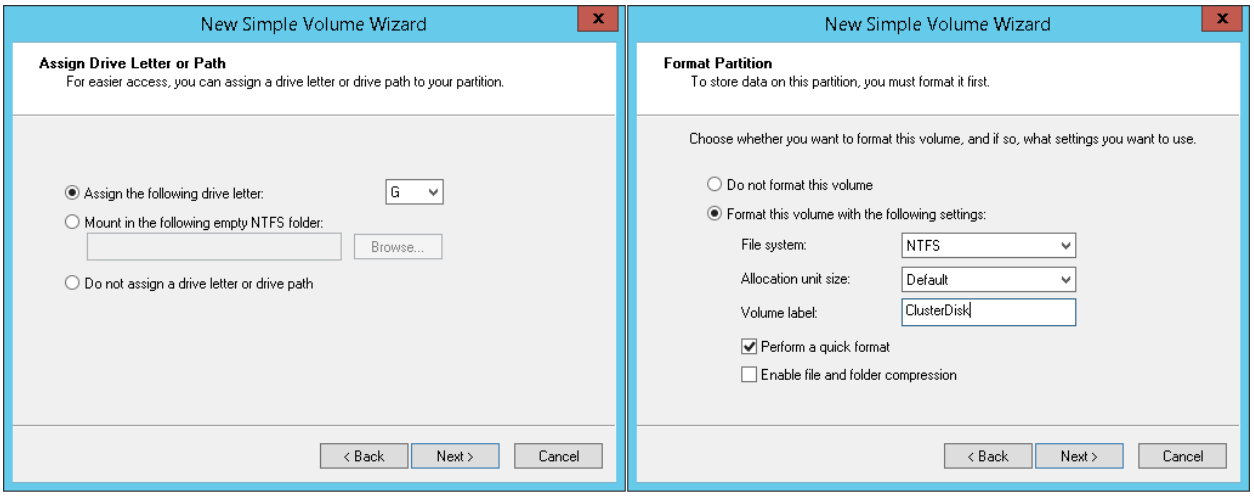

11. Cửa sổ **Welcome**, chọn **Next**.

12. Cửa sổ **Specify Volume Size**, chọn **Next**.

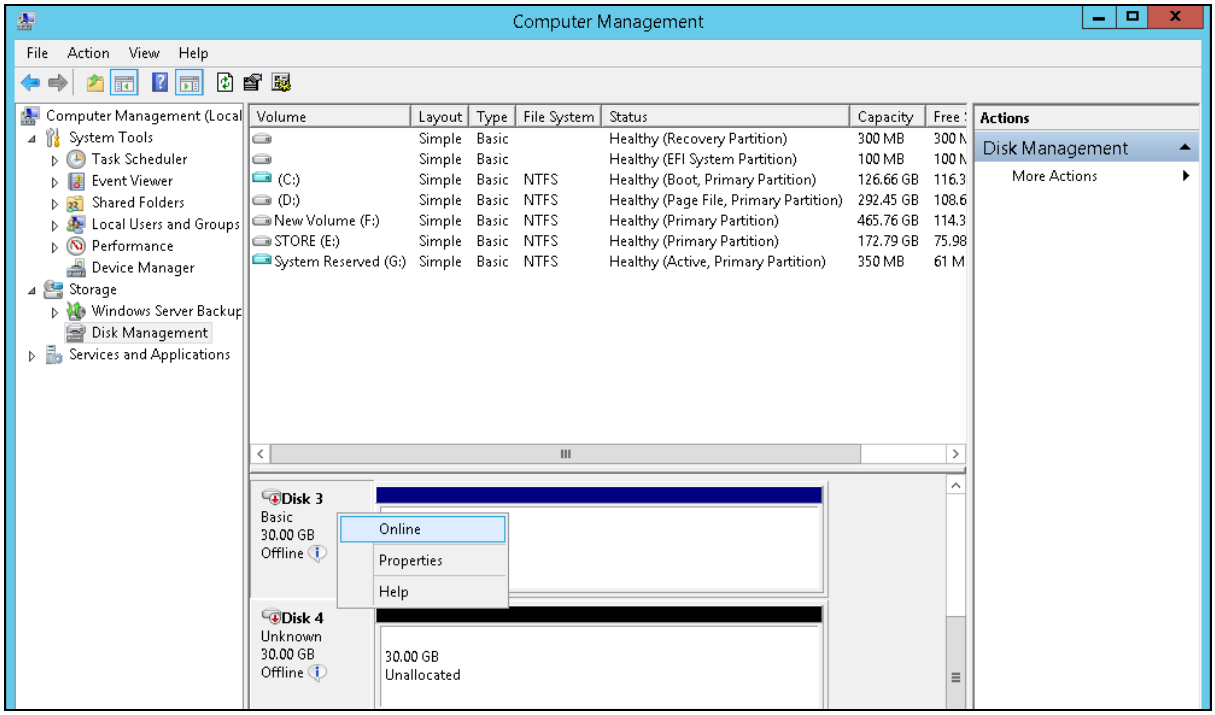


13. Cửa sổ **Assign Drive Letter or Path**, chọn **Next**.

14. Cửa sổ **Format Partition**, trong ô **Volume label**, nhập **ClusterDisk**, chọn **Next**, và chọn **Finish**. (Nếu có hộp thoại yêu cầu format, chọn **Cancel)**.



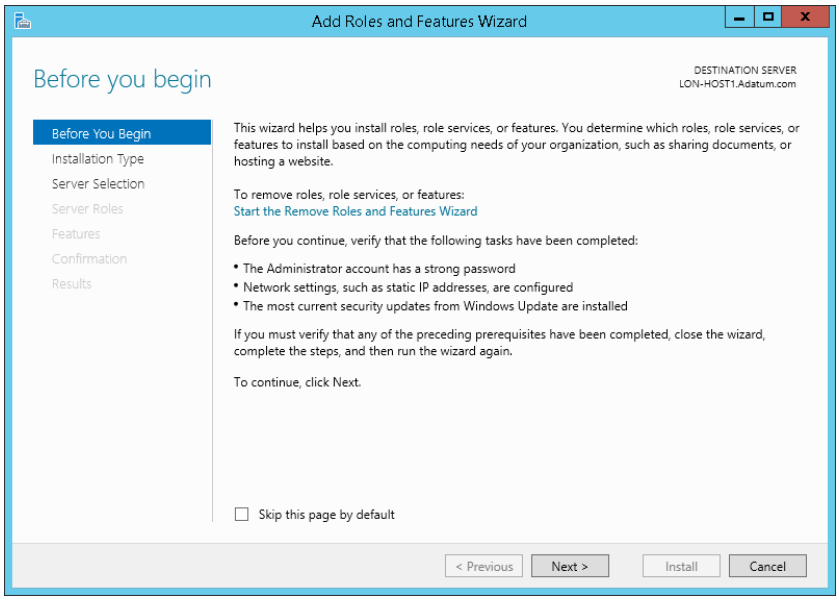

15. Qua máy **LON-HOST1,** trong **Server Manager**, bung menu **Tools**, mở **Computer Management**. Bung **Storage**, chọn **Disk Management**, chuột phải **Disk 3**, chọn **Online**.



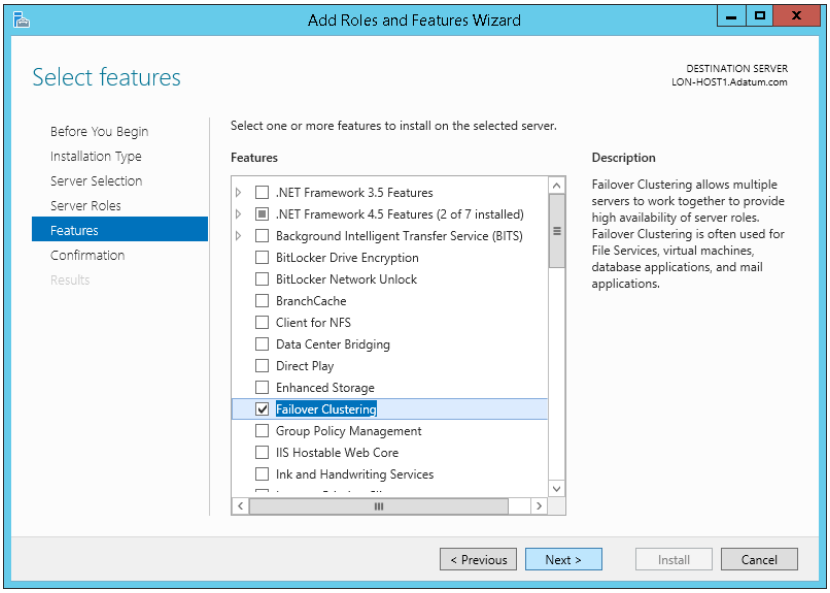
## Bước 2. Cài đặt và cấu hình Failover Clustering trên 2 Server vật lý

1. Trên máy **LON-HOST1**, trong cửa sổ **Server Manager,** chọn **Add roles and features**.

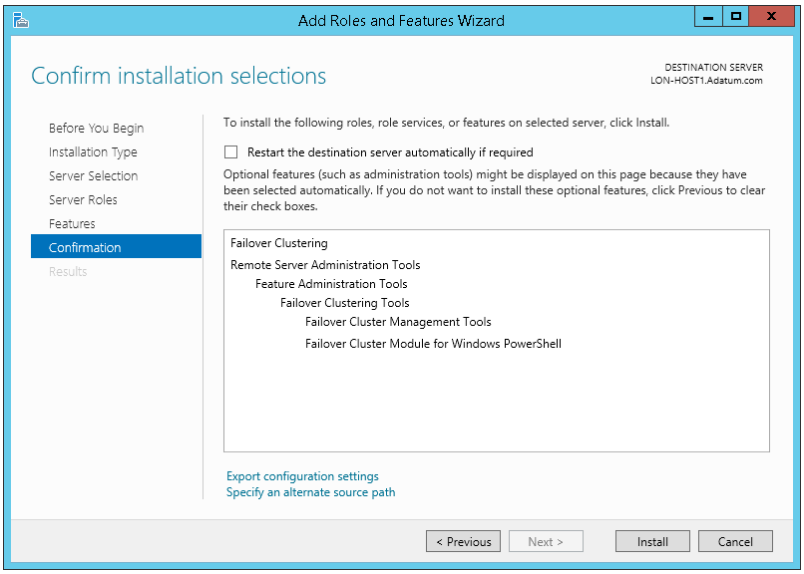
2. Cửa sổ **Before You Begin**, chọn **Next** 4 lần.




3. Cửa sổ **Select features**, đánh dấu chọn **Failover Clustering**, chọn **Add Features**, và chọn **Next**.



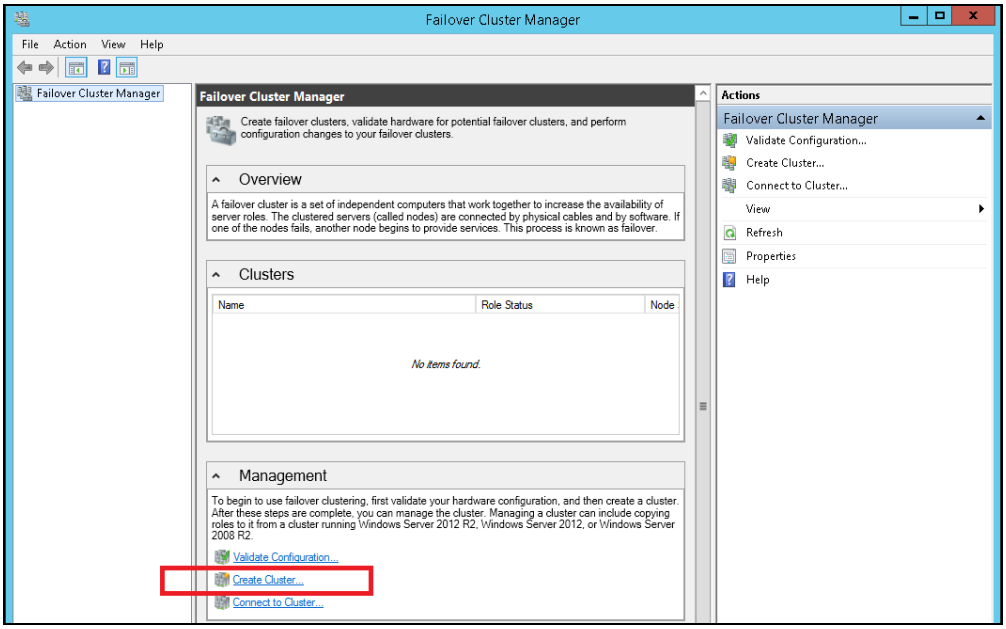
4. Cửa sổ **Confirm installation selections**, chọn **Install**.



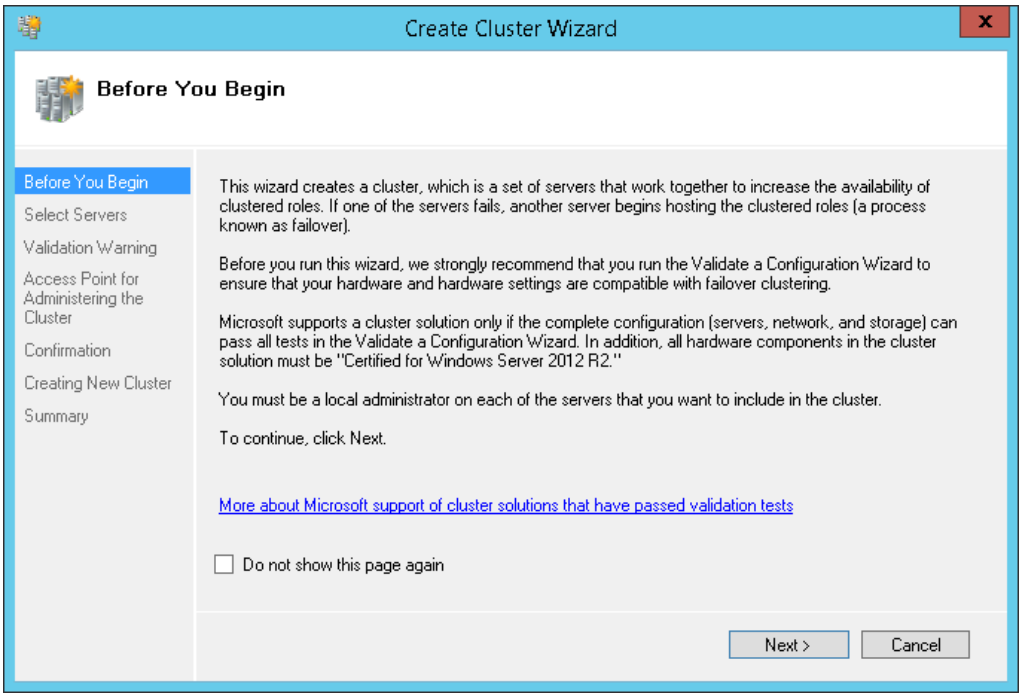

5. Sau khi cài đặt thành công, chọn **Close**.

6. Lặp lại từ bước 1 đến 5 trên máy **LON-HOST2**.

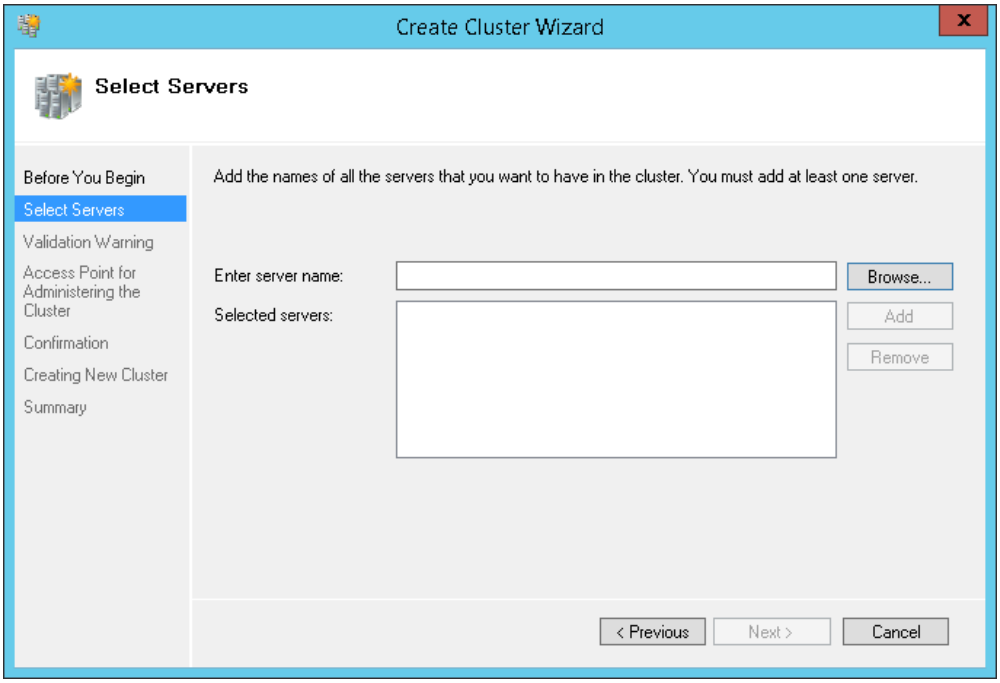
7. Trên máy **LON-HOST1**, trong **Server Manager**, bung menu **Tools**, mở **Failover Cluster Manager**. Trong phần **Management**, chọn **Create Cluster**.



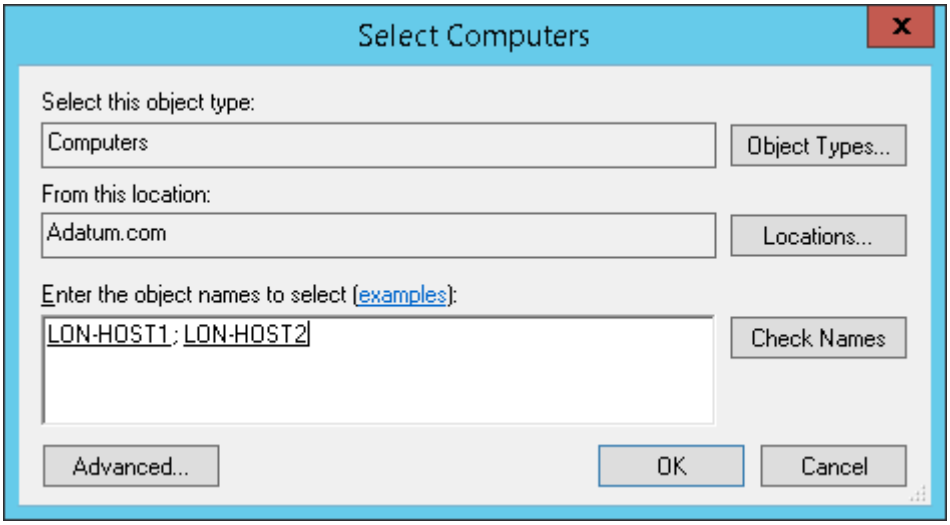
8. Cửa sổ **Before You Begin**, chọn **Next**.



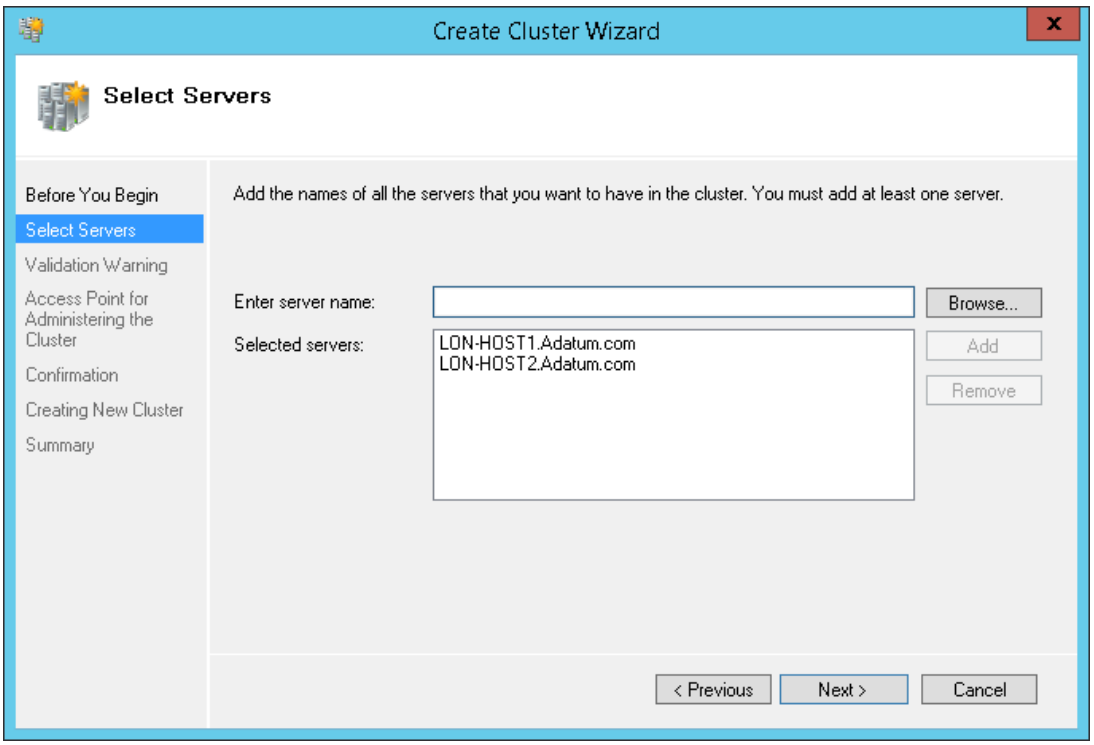

9. Cửa sổ **Select Server**, chọn **Browse**...



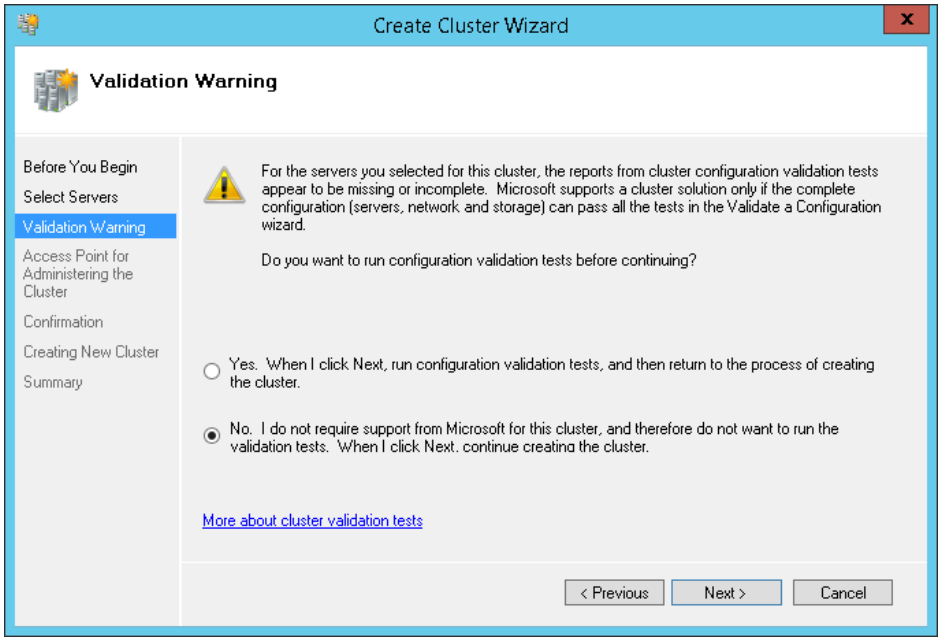
10. Hộp thoại **Seclect Computer**, nhập **LON-HOST1;LON-HOST2**, chọn **Check Names**, và chọn **OK.**



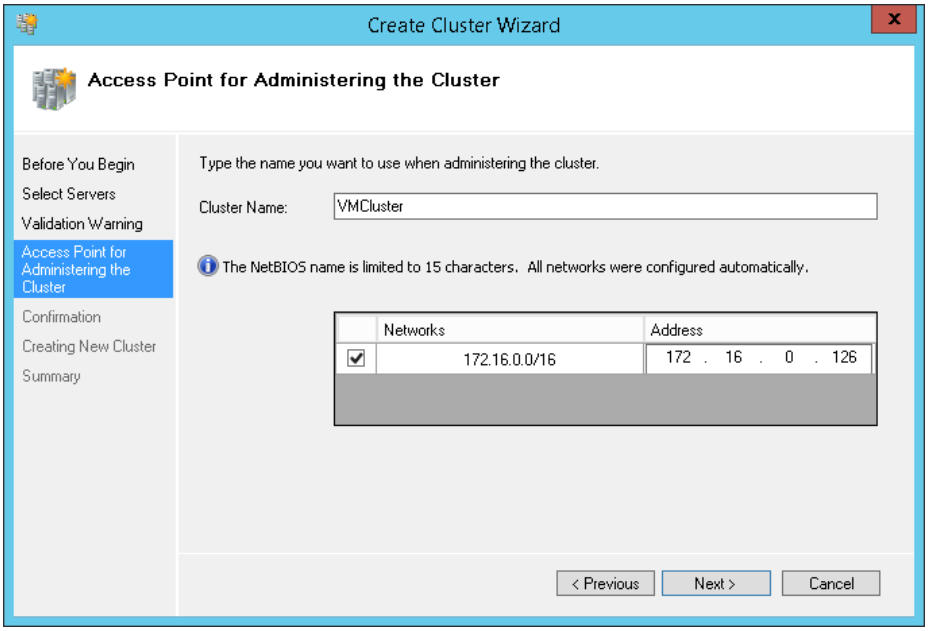

11. Cửa sổ **Select Server**, kiểm tra có 2 máy **LON-HOST1.adatum.com** và L**ON-HOST2.adatum.com**, chọn Next



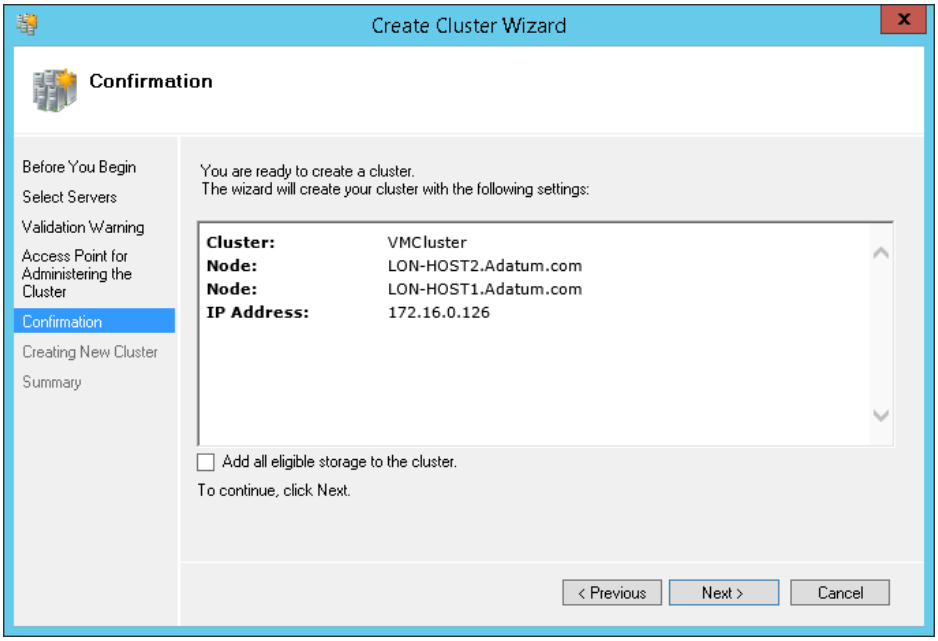
12. Cửa sổ **Validation Warning**, chọn **No, I do not require support from Microsoft for this cluster**, và chọn **Next**.



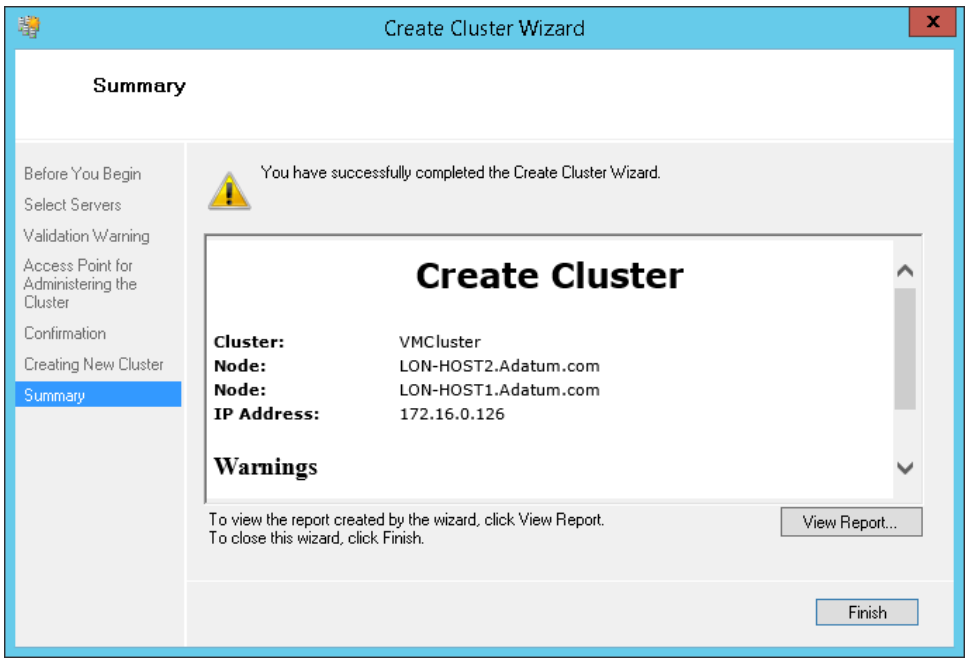

13. Cửa sổ **Access Point for Administering the Cluster**, trong ô **Cluster Name**, nhập **VMCluster**. Trong ô **Address**, nhập **172.16.0.126**, chọn **Next**.



14. Cửa sổ **Confirmation**, bỏ dấu chọn **Add all eligible storage to the cluster**, và chọn **Next**.

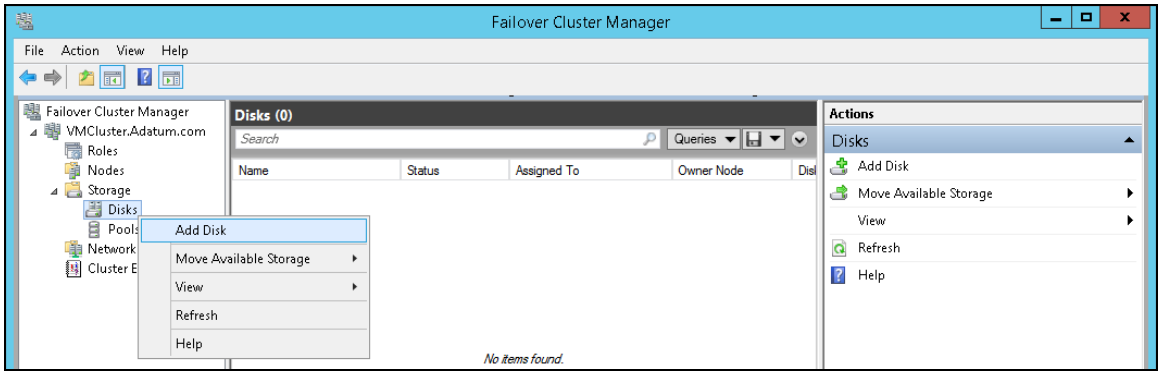



15. Cửa sổ **Create Cluster Wizard Summary**, chọn **Finish**.

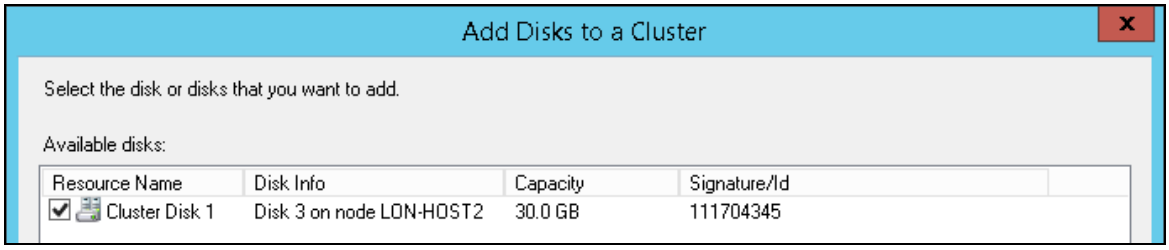


## Bước 3. Cấu hình Cluster

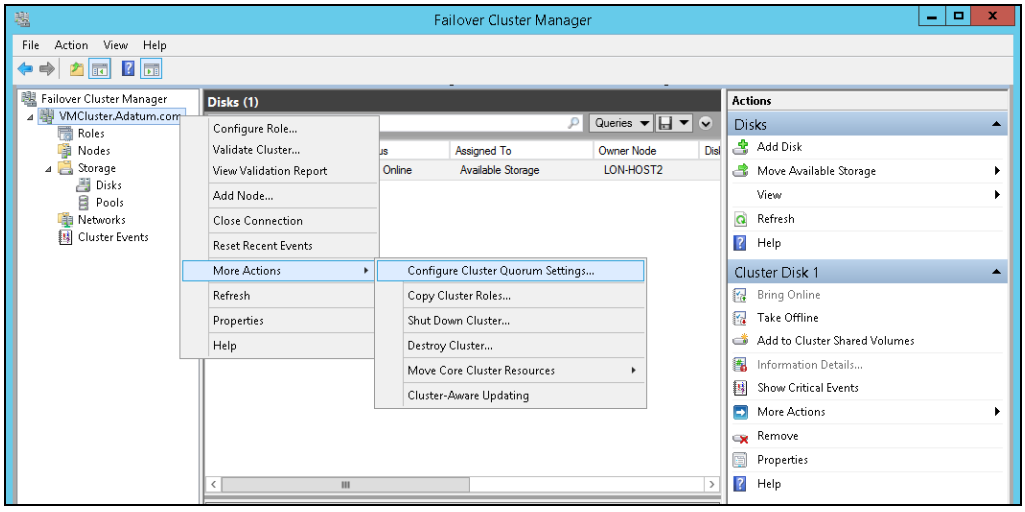
1. Trên máy **LON-HOST1**,trong cửa sổ **Failover Cluster Manager**, bung **VMCluster.Adatum.com**, bung **Storage**, chuột phải **Disks**, chọn **Add Disk**.



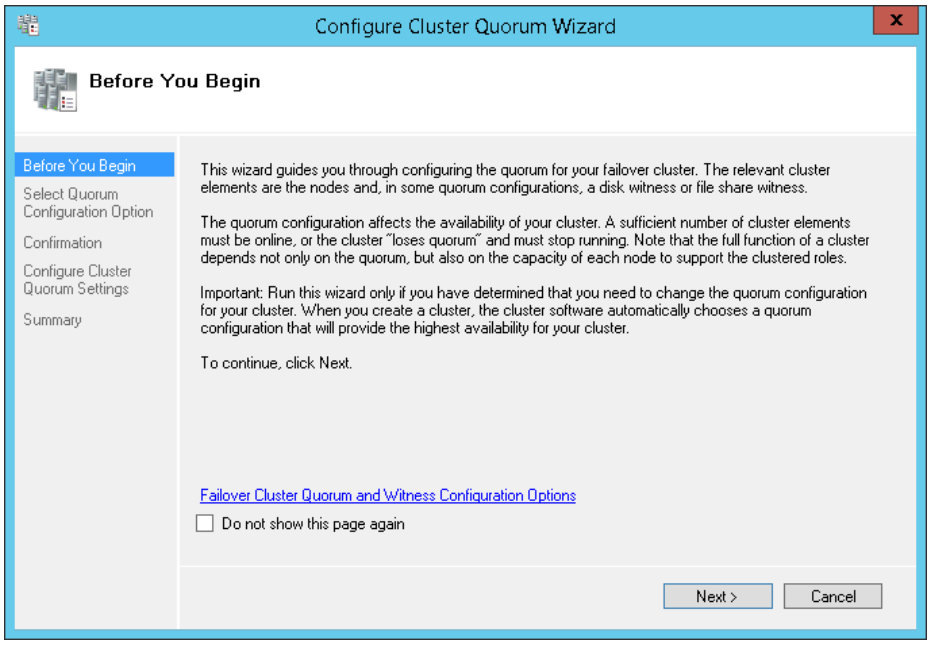

2. Hộp thoại **Add Disks to a Cluster**, kiểm tra đánh dấu chọn **Cluster Disk 1**, và chọn **OK**.



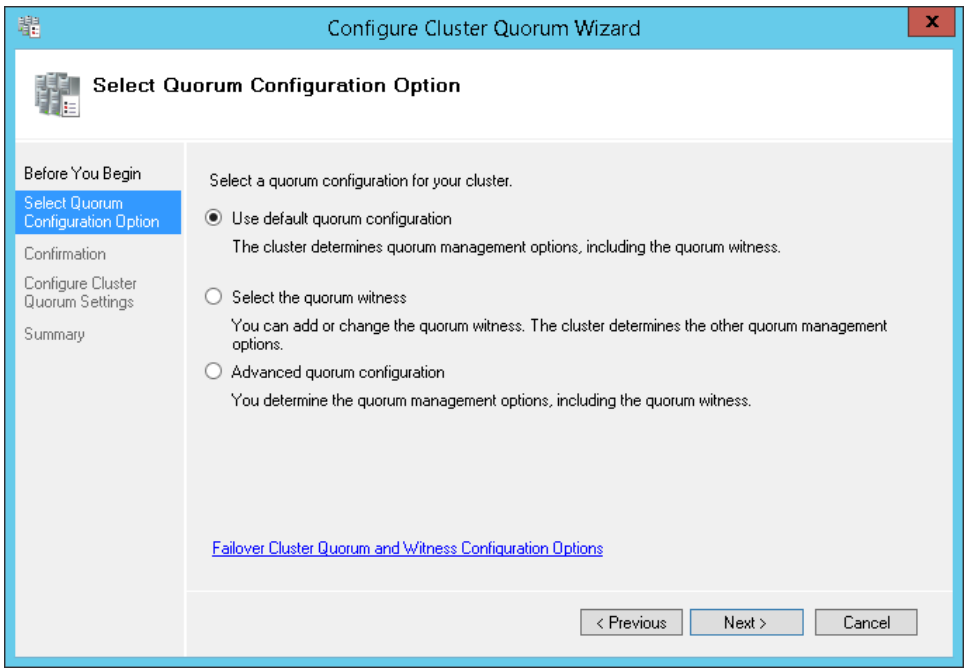

3. Trong cửa sổ **Failover Cluster Manager,** chuột phải **VMCluster.Adatum.com**, bung **More Actions**, chọn **Configure Cluster Quorum Settings.**



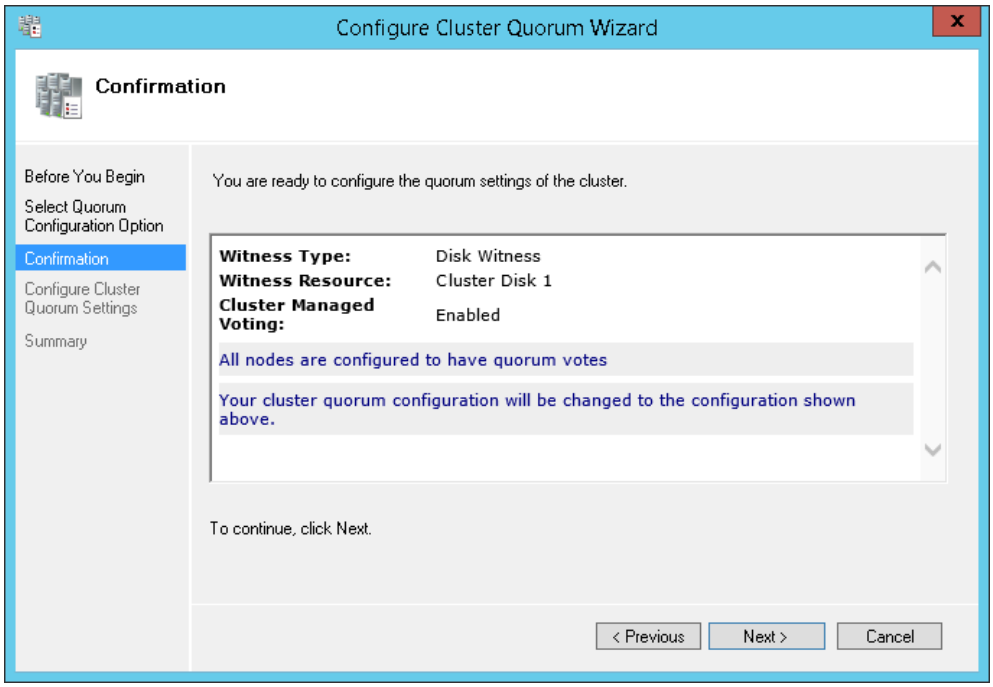
4. Cửa sổ **Before You Begin**, chọn **Next**.




5. Cửa sổ **Select Quorum Configuration Option**, chọn **Use default quorum configuration**, chọn **Next**.



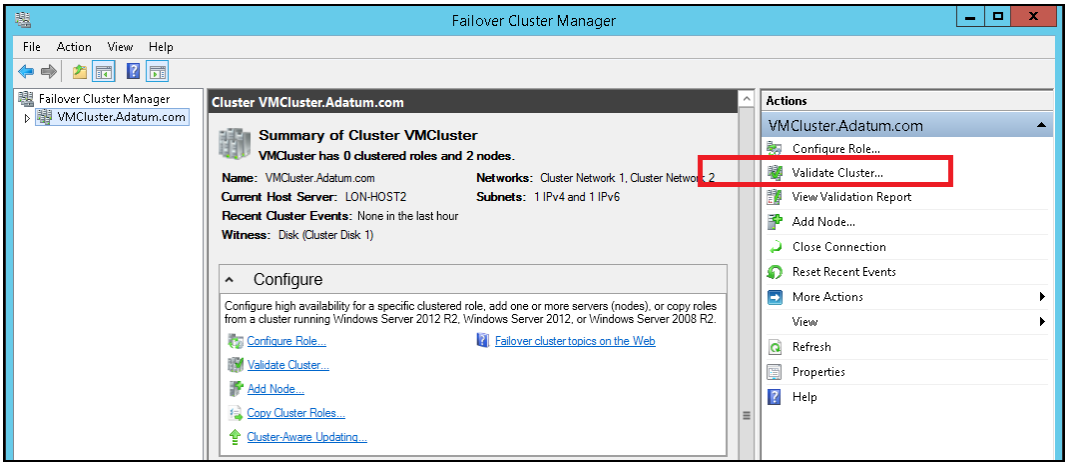
6. Cửa sổ **Confirmation**, chọn **Next**, và chọn **Finish**.



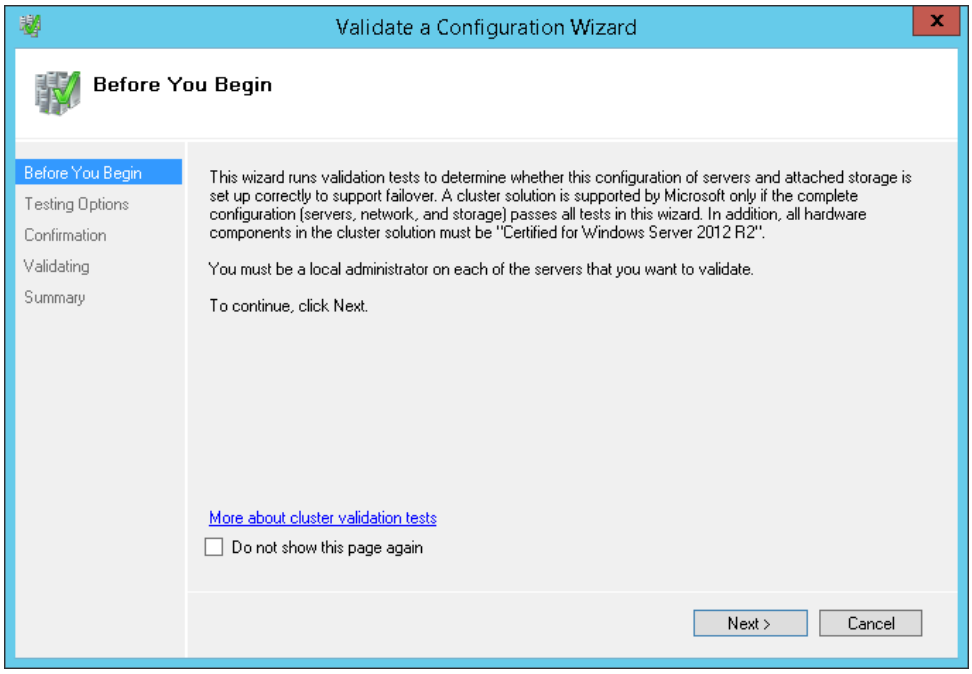

## Bước 4. Xác nhận cấu hình Cluster

1. Qua máy **LON-HOST2**, trong **Server Manager**, bung menu **Tools**, mở **Failover Cluster Manager**.

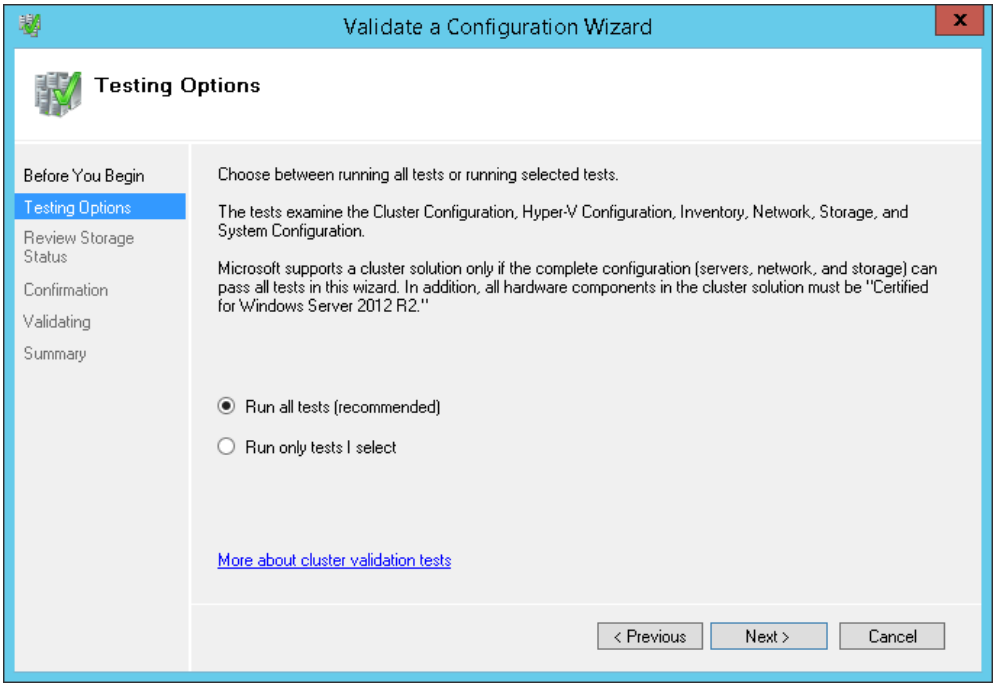
2. Trong cửa sổ **Failover Cluster Manager**, chọn **VMCluster.Adatum.com.** Cửa sổ **Actions**, chọn **Validate Cluster**.



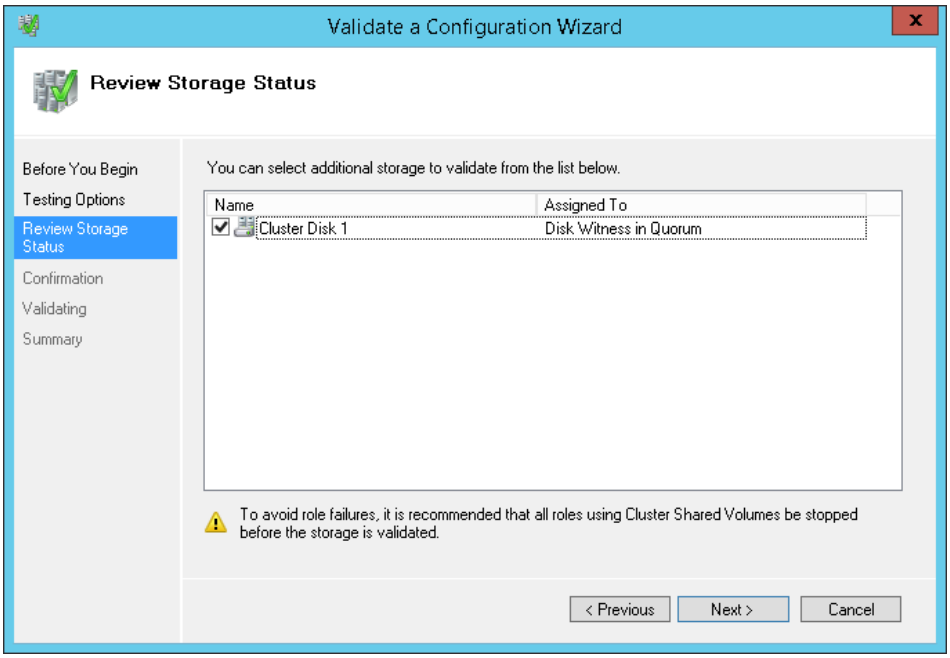
3. Cửa sổ **Before You Begin**, chọn **Next**.



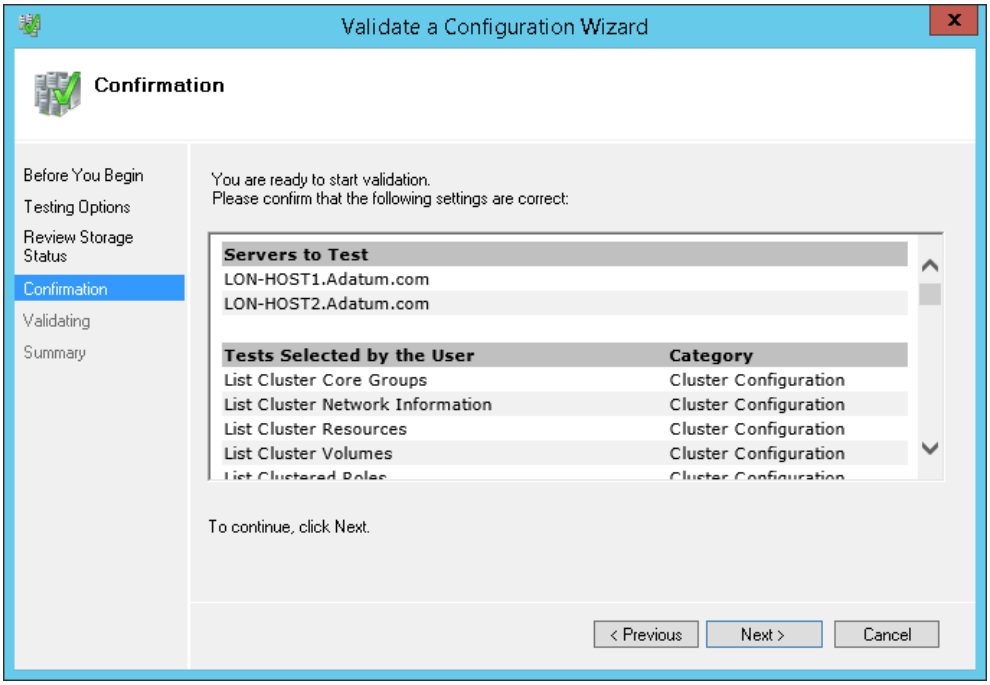

4. Cửa sổ **Testing Options**, chọn **Run all tests (recommended)**, và chọn **Next**.



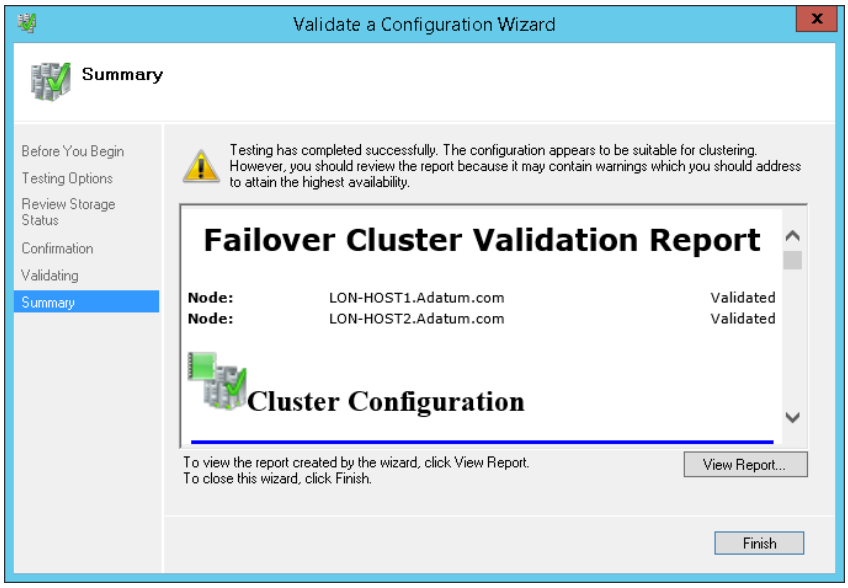
5. Cửa sổ **Review Storage Status**, chọn **Cluster Disk 1**, và chọn **Next**.



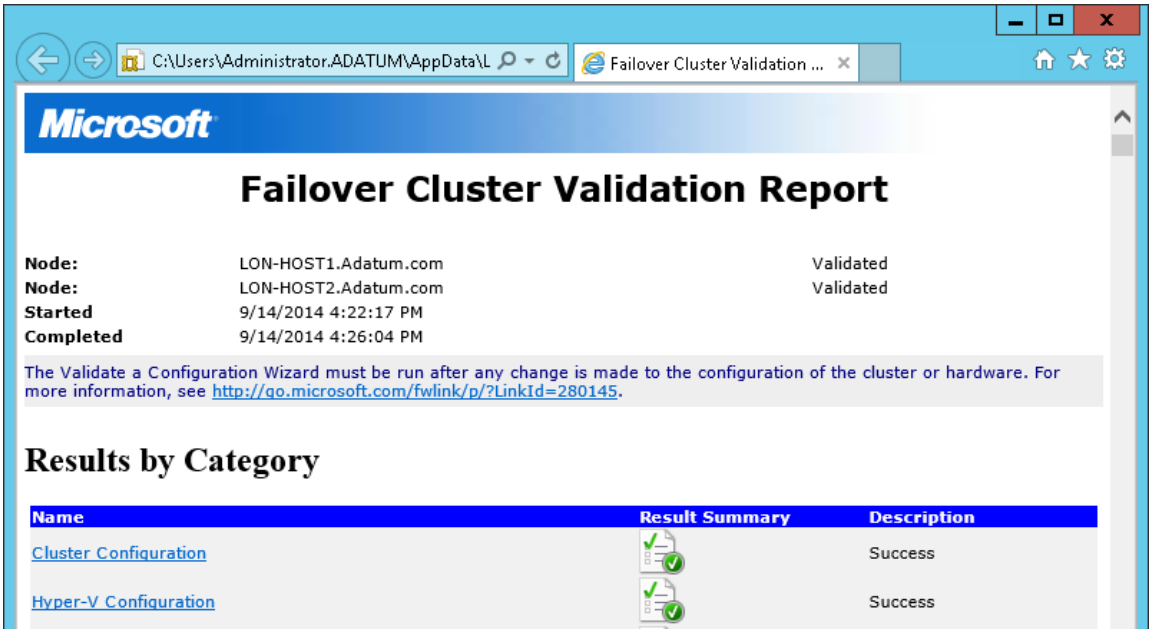

6. Cửa sổ **Confirmation**, chọn **Next**.



7. Cửa sổ **Summary**, đợi sau khi quá trình kiểm tra hoàn tất, chọn **View Report**.




8. Xem xét báo cáo, có một số cảnh báo, nhưng không có bất kỳ lỗi nào.




9. Tắt **Internet Explorer**, và chọn **Finish**.

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã tạo Failover Cluster thành công.**

## Bài tập 2: Cấu hình Scale-Out File Server.

Bạn đã hoàn thành cấu hình lưu trữ sẵn sàng cao cho dịch vụ file. Tiếp theo bạn sẽ kích hoạt khả năng sẵn sàng cao cho các File Server bằng cách cấu hình cho các File Server làm thành viên của một Scale-Out File Server, và bạn sẽ sử dụng làm nơi lưu trữ các máy ảo Hyper-V.

❖ **Bài thực hành bao gồm các bước:**

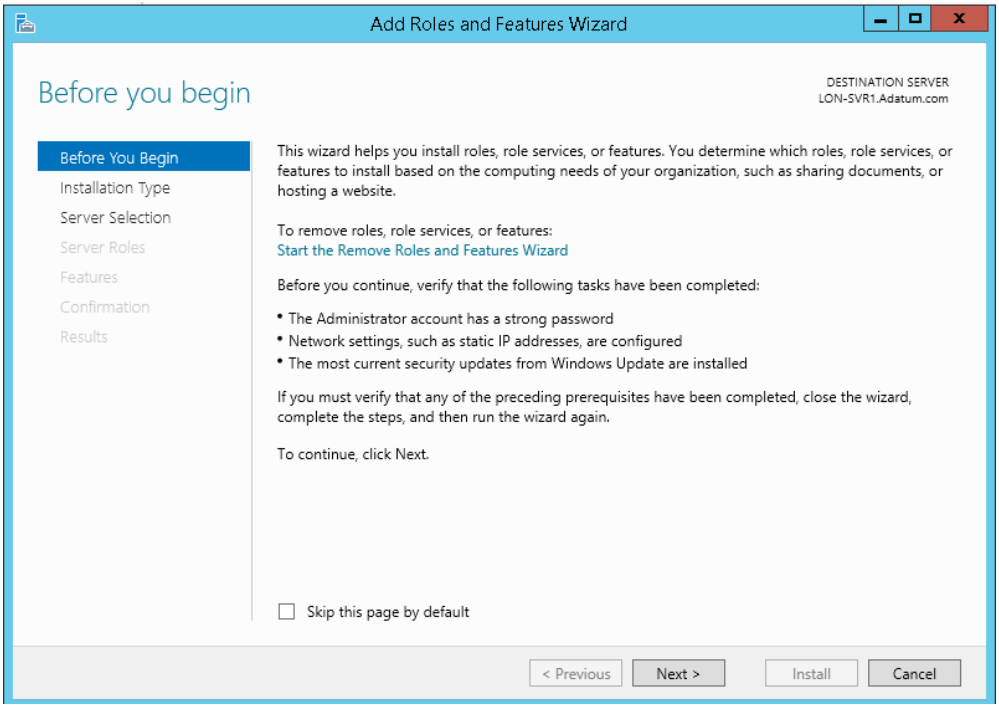
1. Cài đặt File Server role và Failover Clustering trên LON-SVR1 và LON-SVR2
2. Cấu hình cho LON-SVR1 và LON-SVR2 kết nối tới iSCSI Target.
3. Cấu hình Scale-Out File Server
4. Tạo File Share

❖ **Thực hiện:**

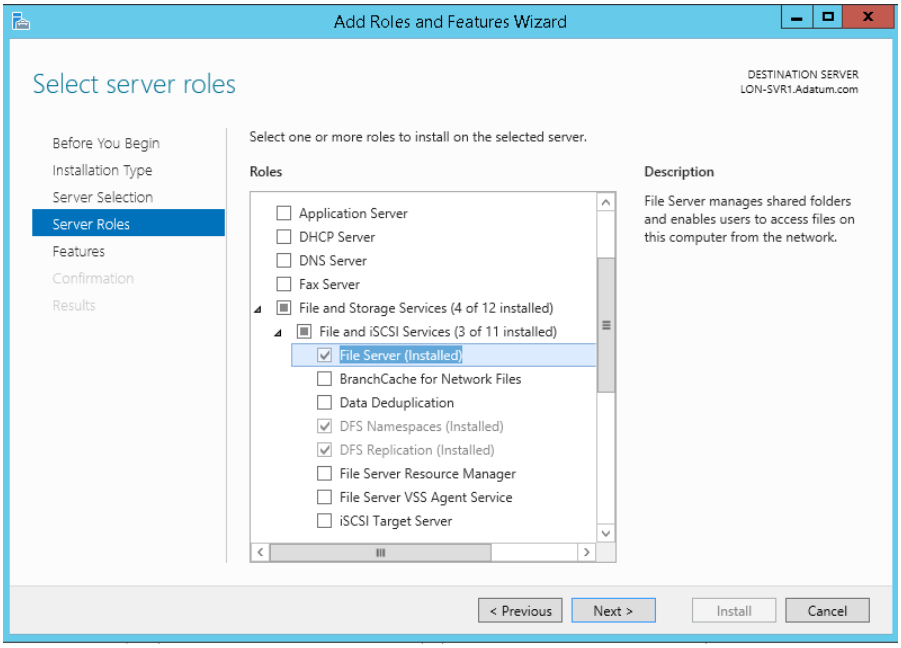
### Bước 1. Cài đặt File Server role và Failover Clustering trên LON-SVR1 và LON-SVR2

1. Trên máy **LON-SVR1**, trong **Server Manager**, chọn **Add roles and features**.

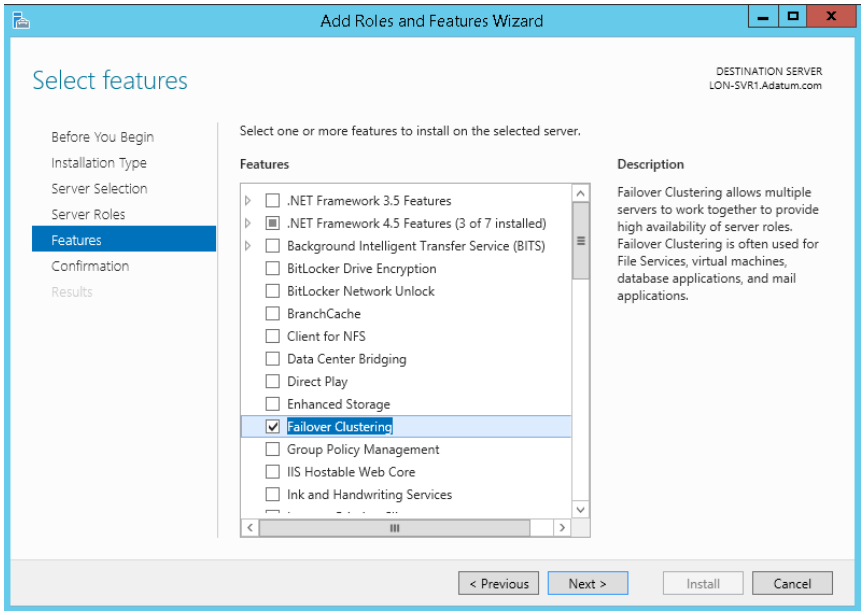
2. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.



3. Cửa sổ **Select server roles**, bung **File and Storage Services (Installed)**, bung **File and iSCSI Services (Installed)**, kiểm tra có đánh dấu chọn **File Server**, chọn **Next**.




4. Cửa sổ **Select features**, đánh dấu chọn **Failover Clustering**, chọn **Add Features**, và chọn **Next**.

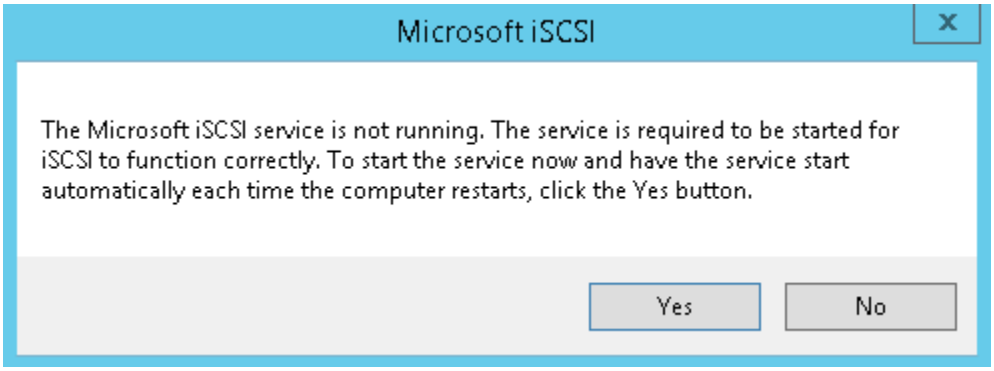


5. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.

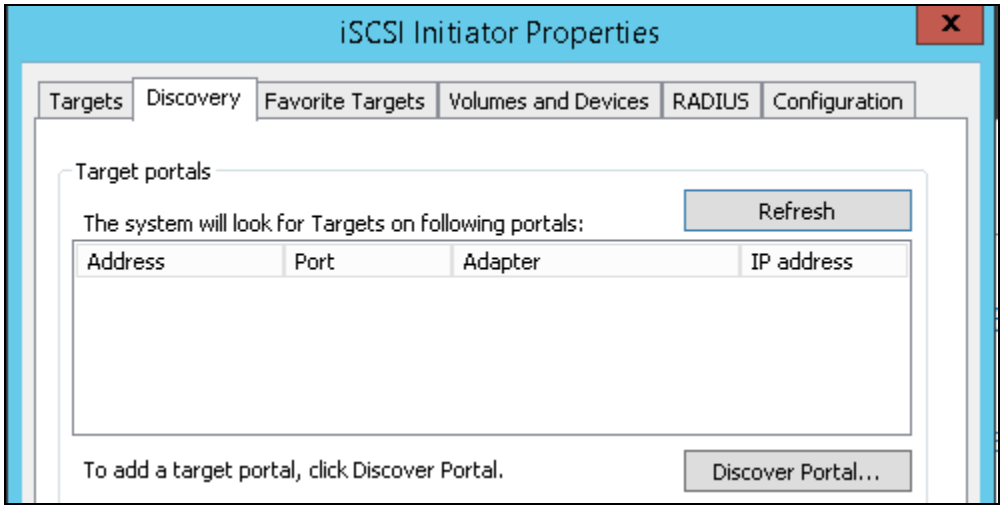
6. Lặp lại từ bước 1 đến 6 cho máy **LON-SVR2**.

**Bước 2. Cấu hình cho LON-SVR1 và LON-SVR2 kết nối tới iSCSI Target.**

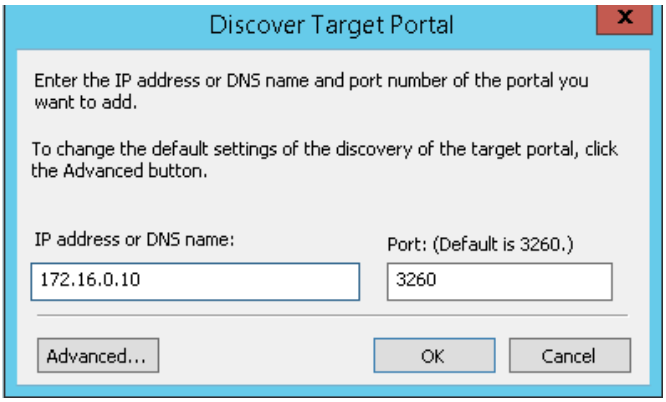
1. Trên máy **LON-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **iSCSI Initiator**. Hộp thoại **Microsoft iSCSI**, chọn **Yes**.



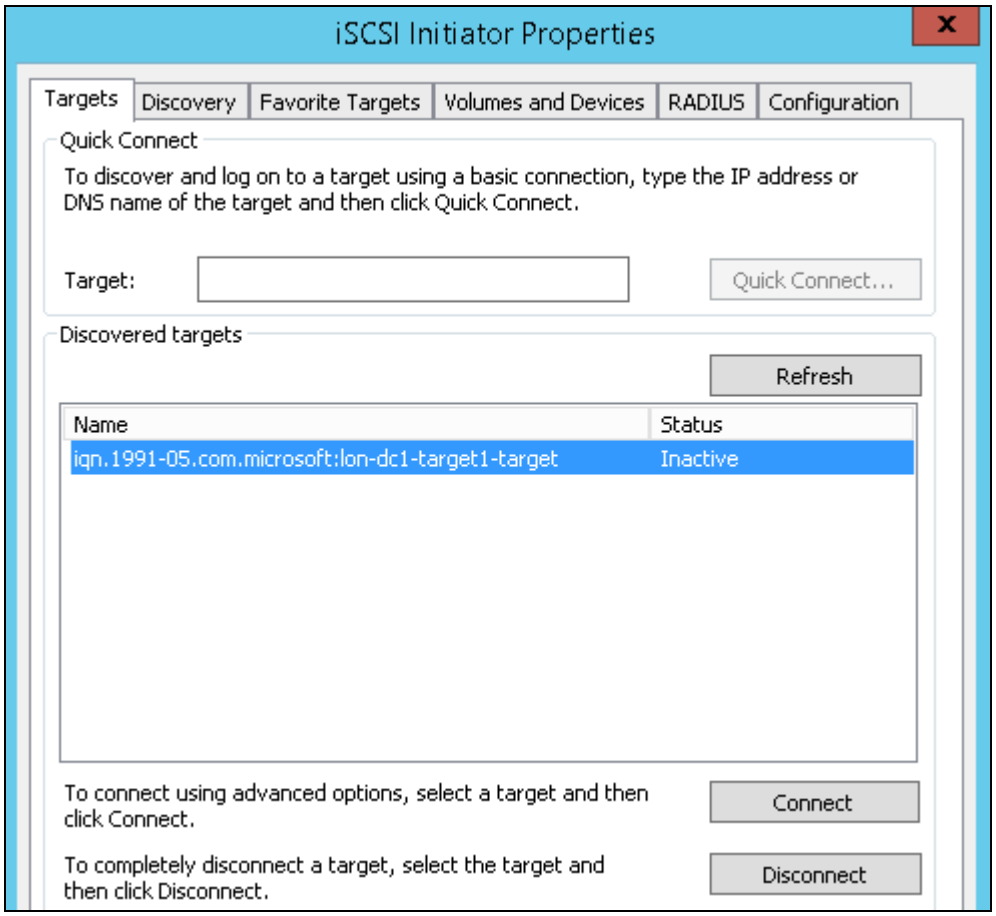

2. Hộp thoại **iSCSI Initiator,** qua tab **Discovery**.



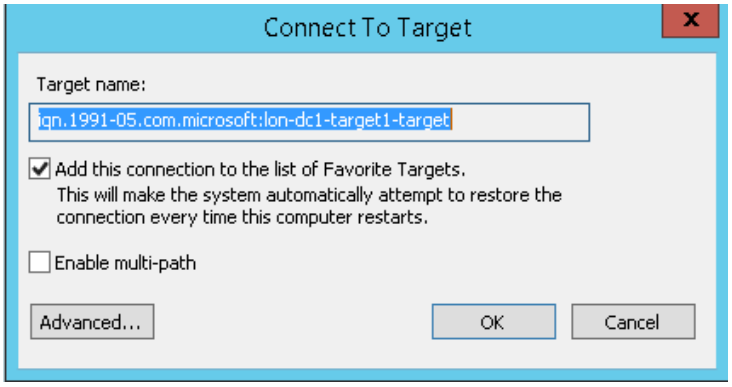
3. Chọn **Discover Portal**, trong ô **IP address or DNS name**, nhập **172.16.0.10**, và chọn **OK**.




4. Qua tab **Targets**, chọn **iqn.1991-05.com.microsoft:lon-dc1-target1-target**, chọn **Connect**.



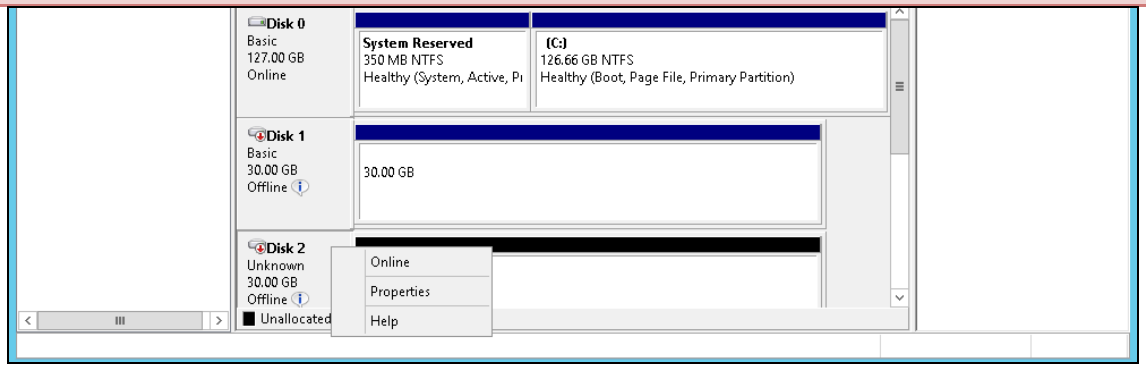
5. Hộp thoại **Connect To Target,** đánh dấu chọn **Add this connection to the list of Favorite Targets**, và chọn **OK** 2 lần.



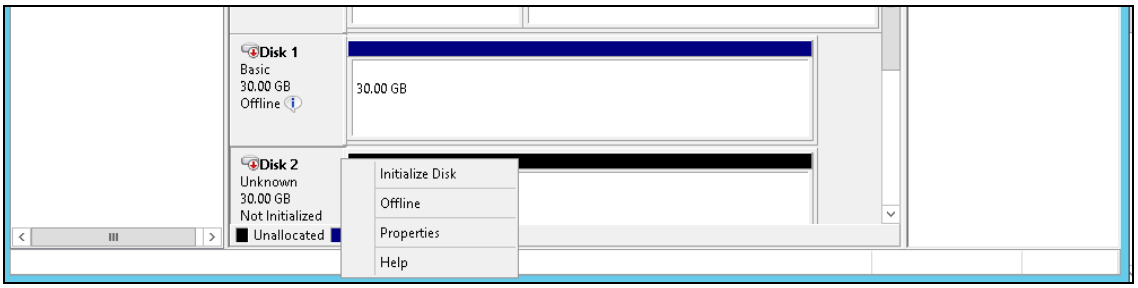

6. Lặp lại từ bước 1 đến 4 cho máy **LON-SVR2**.

7. Trên máy **LON-SVR2**, trong **Server Manager**, bung menu **Tools**, mở **Computer Management**, bung **Storage**, chọn **Disk Management**, chuột phải **Disk 2**, chọn **Online**.

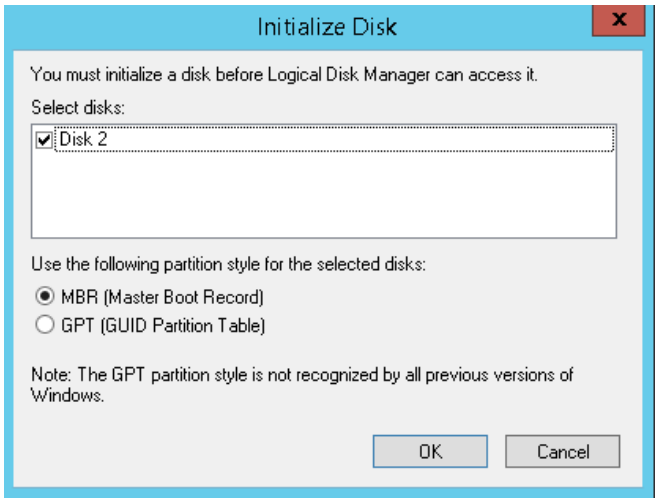
**Lưu ý:** Không chọn **Disk 1**, vì **Disk 1**là đĩa cứng đã được sử dụng trong bài tập trước.



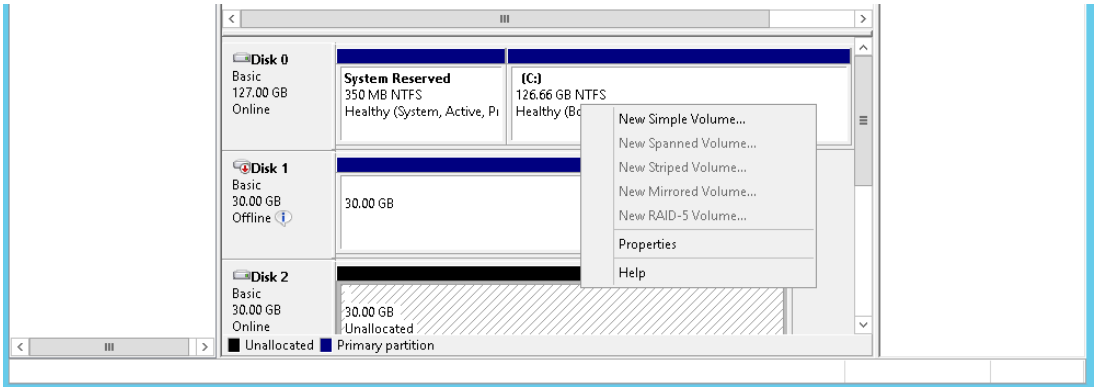

8. Chuột phải **Disk 2**, chọn **Initialize Disk**.



9. Hộp thoại **Initialize Disk**, chọn **OK**.

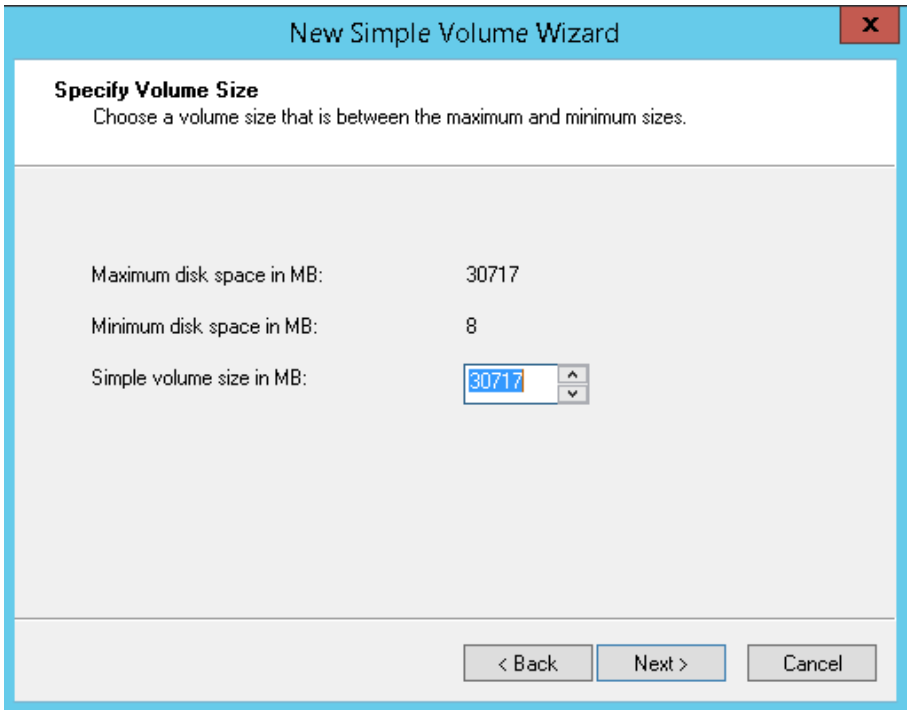



10. Chuột phải lên phần Unallocated của **Disk 2**, chọn **New Simple Volume**.

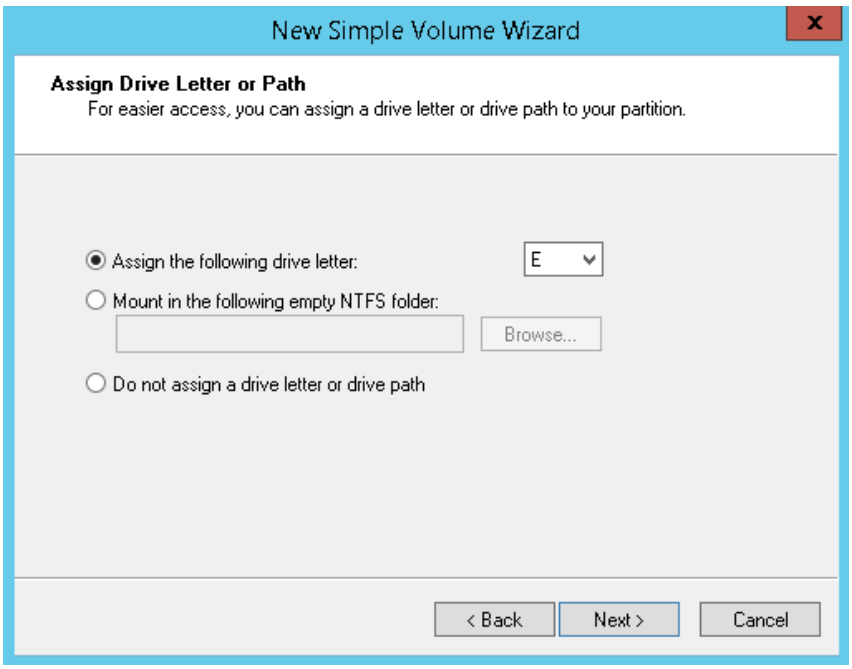



11. Cửa sổ **Welcome**, chọn **Next**.

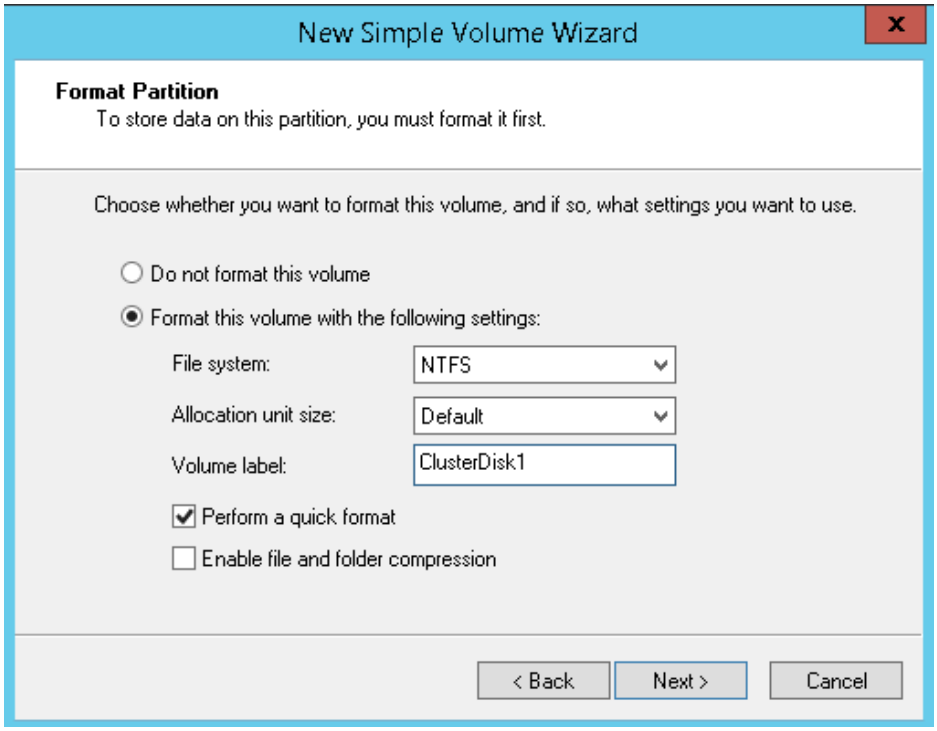
12. Cửa sổ **Specify Volume Size**, chọn **Next**.




13. Cửa sổ **Assign Drive Letter or Path**, chọn **Next**.

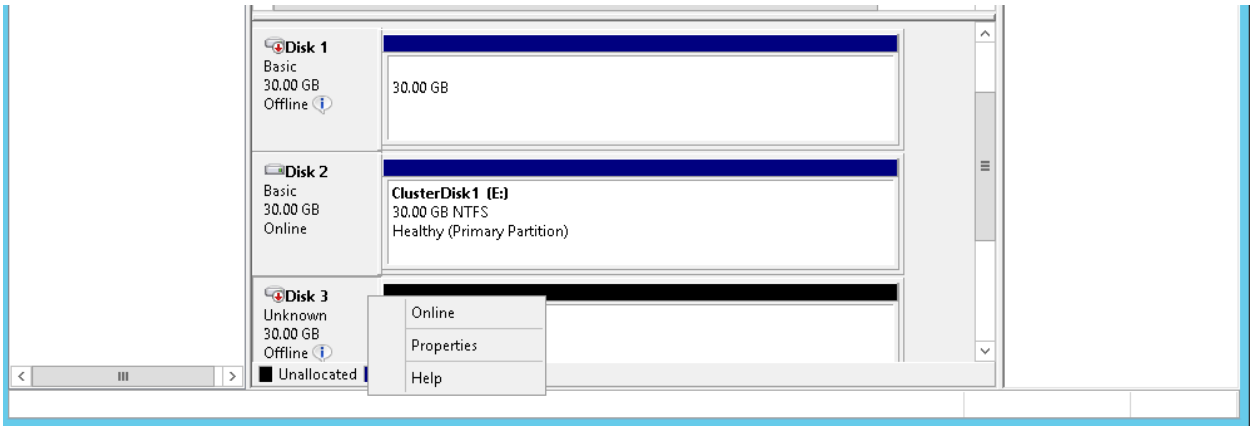


14. Cửa sổ **Format Partition**, trong ô **Volume label**, nhập **ClusterDisk1**, chọn **Next**, và chọn **Finish**.

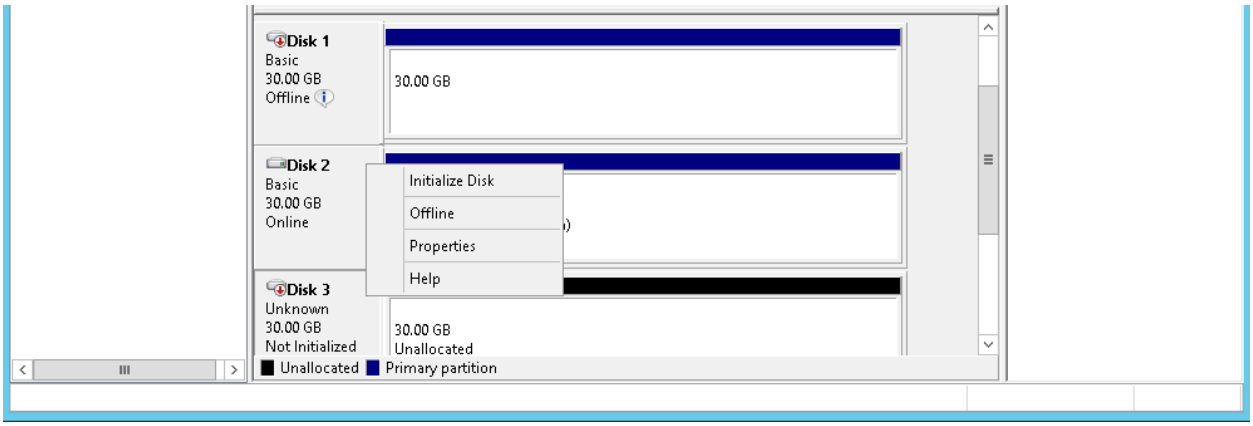



15. Nếu xuất hiện hộp thoại yêu cầu format, chọn **Cancel**.

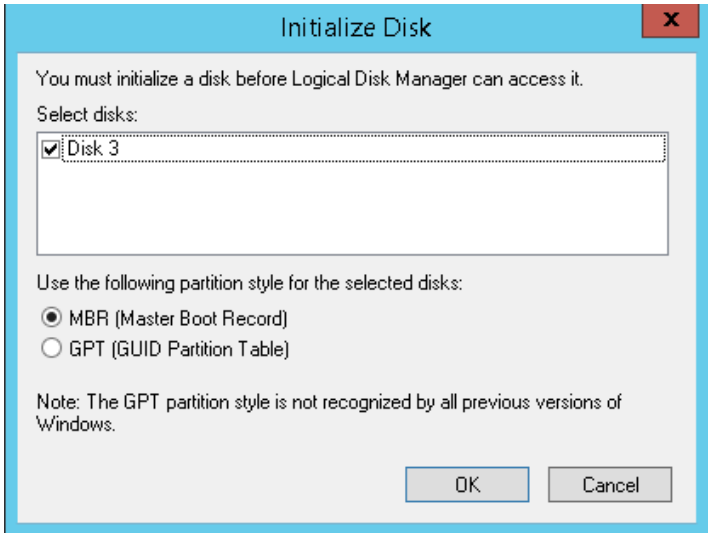
16. Chuột phải **Disk 3**, chọn **Online**.



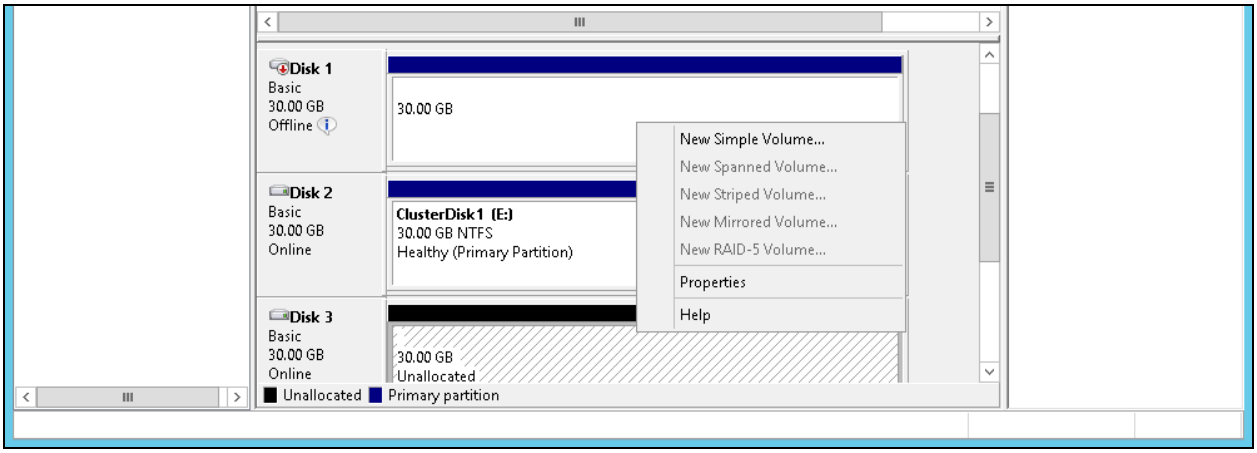
17. Chuột phải **Disk 3**, chọn **Initialize Disk**.




18. Hộp thoại **Initialize Disk**, chọn **OK**.

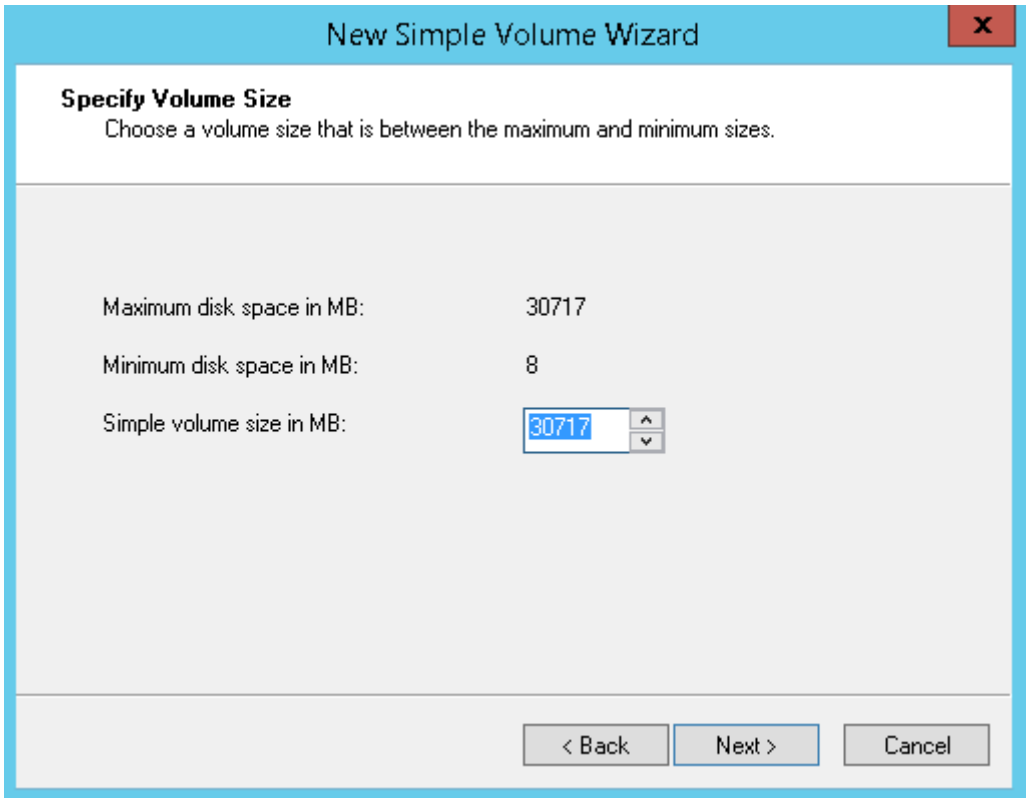


19. Chuột phải lên phần Unallocated của **Disk 3**, chọn **New Simple Volume**.

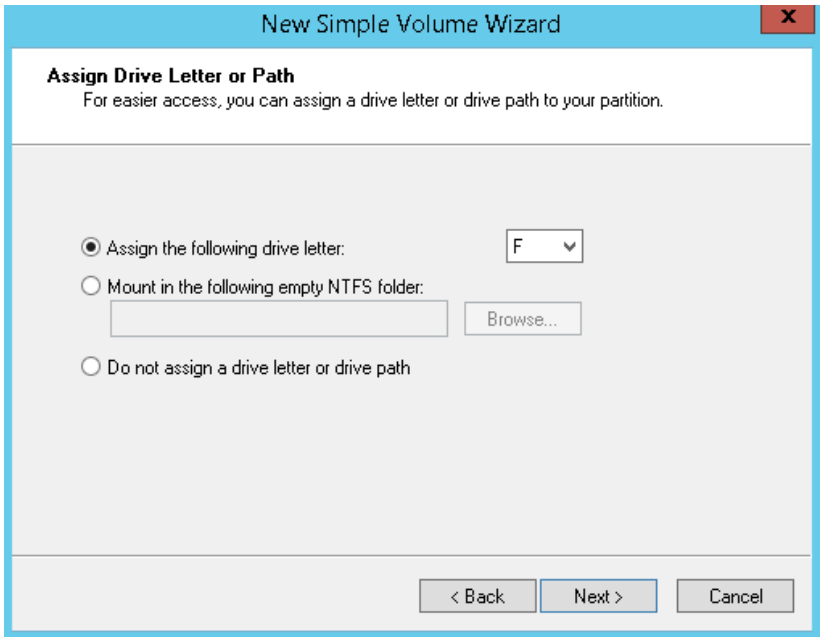



20. Cửa sổ **Welcome**, chọn **Next**.

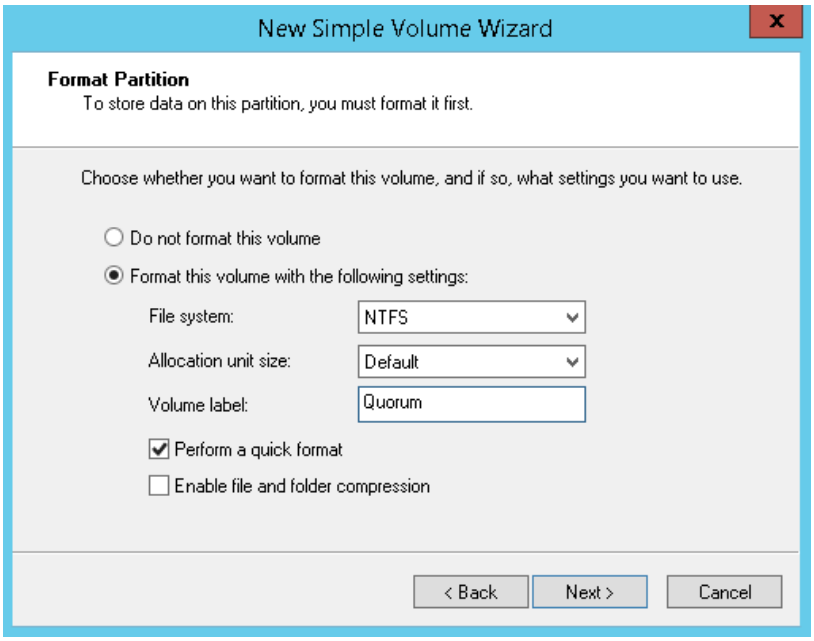
21. Cửa sổ **Specify Volume Size**, chọn **Next**.



22. Cửa sổ **Assign Drive Letter or Path**, chọn **Next**.



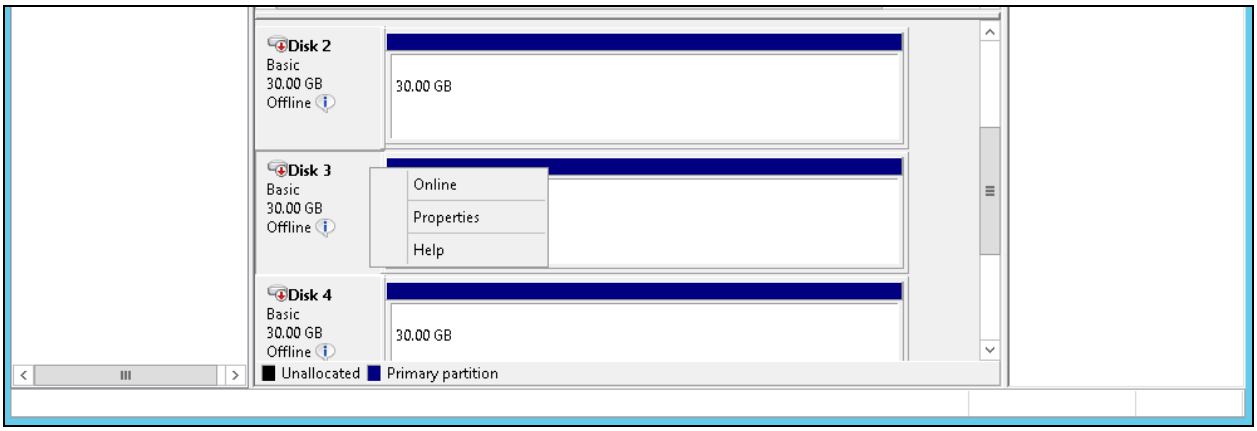

23. Cửa sổ **Format Partition**, trong ô **Volume label**, nhập **Quorum,** chọn **Next**, và chọn **Finish**.



24. Nếu xuất hiện hộp thoại yêu cầu format, chọn **Cancel**.

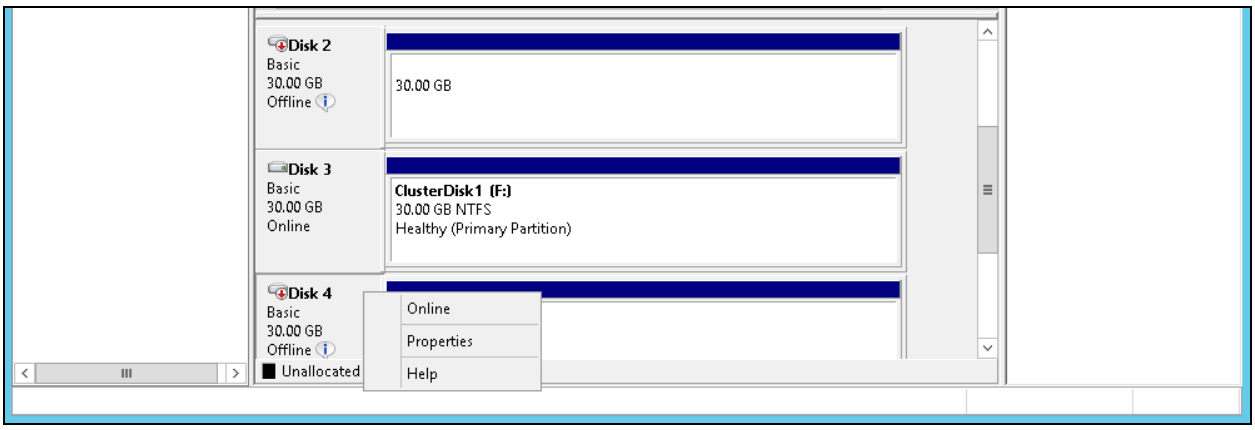
25. Tắt **Computer Management**.

26. Qua máy **LON-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **Computer Management**, bung **Storage**, chọn **Disk Management**, chuột phải **Disk 3**, chọn **Online**.



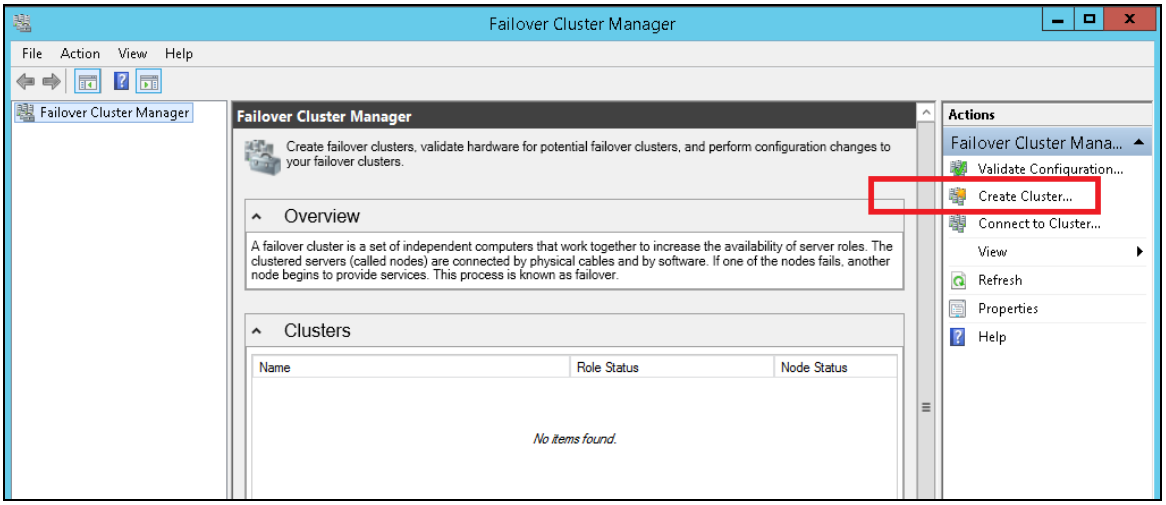

**Lưu ý:** Đảm bảo bạn không chọn **Disk 2,** vì nó là đĩa đã được sử dụng trong bài trước. Trên máy **LON-SVR1** có gắn sẵn 2 ổ cứng, nên 3 ổ cứng của iSCSI Target bắt đầu từ **Disk 2.** Còn trên **LON-SVR2** thì 3 ổ cứng của iSCSI Target bắt đầu từ **Disk 1.**

27. Chuột phải **Disk 4**, chọn **Online.** Tắt Computer Management.

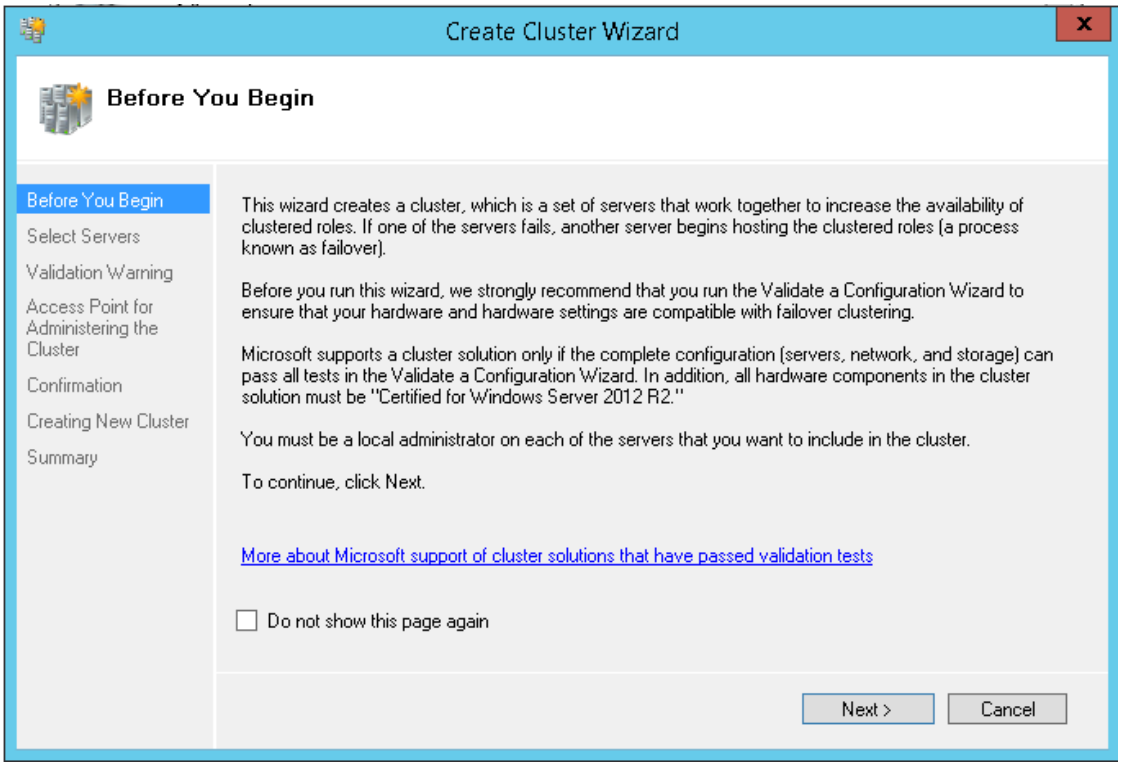


## Bước 3. Cấu hình Scale-Out File Server

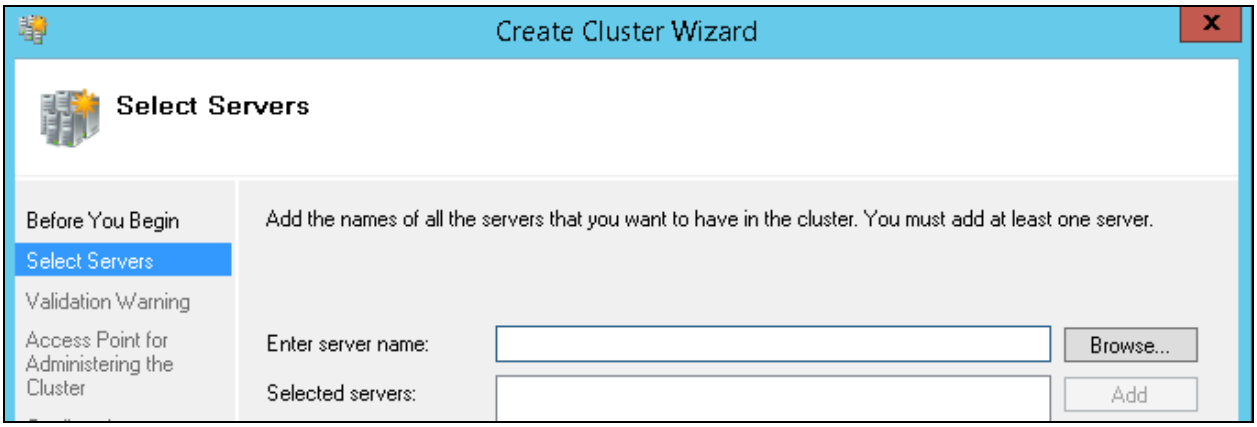
1. Trên máy **LON-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **Failover Cluster Manager**, trong phần **Management**, chọn **Create Cluster**.



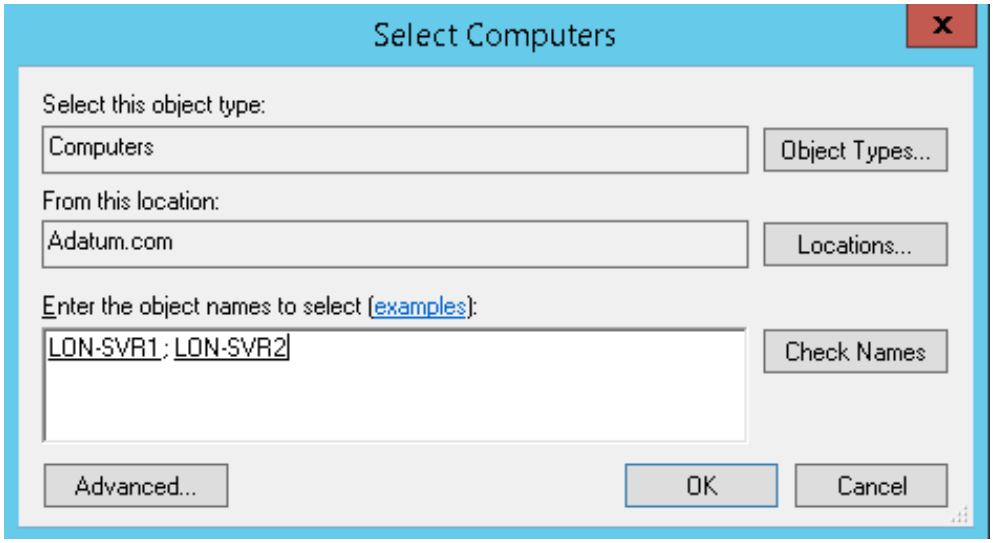

2. Cửa sổ **Before You Begin**, chọn **Next**.



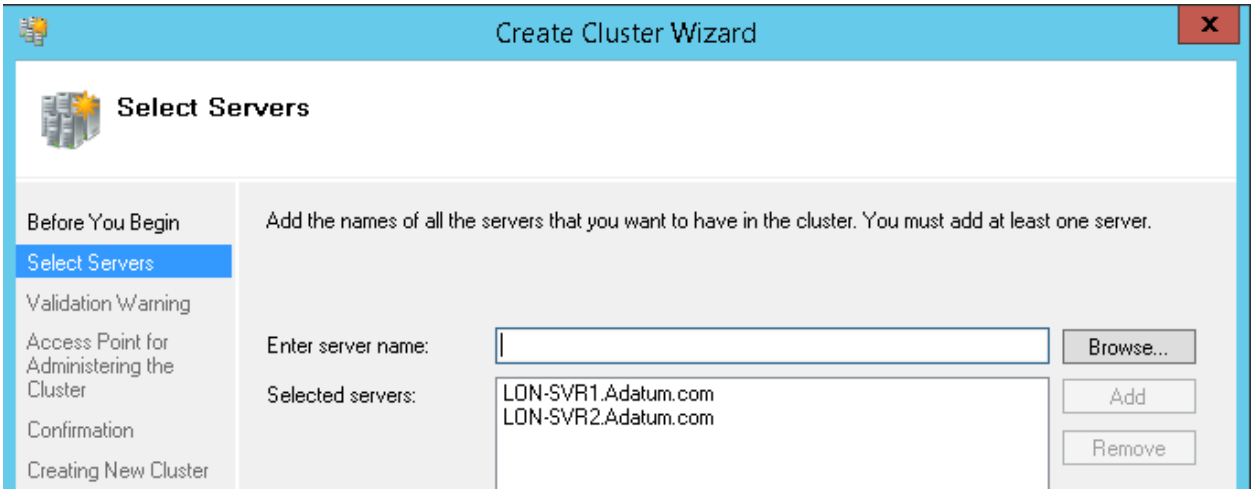
3. Cửa sổ **Select Servers**, chọn **Browse...**



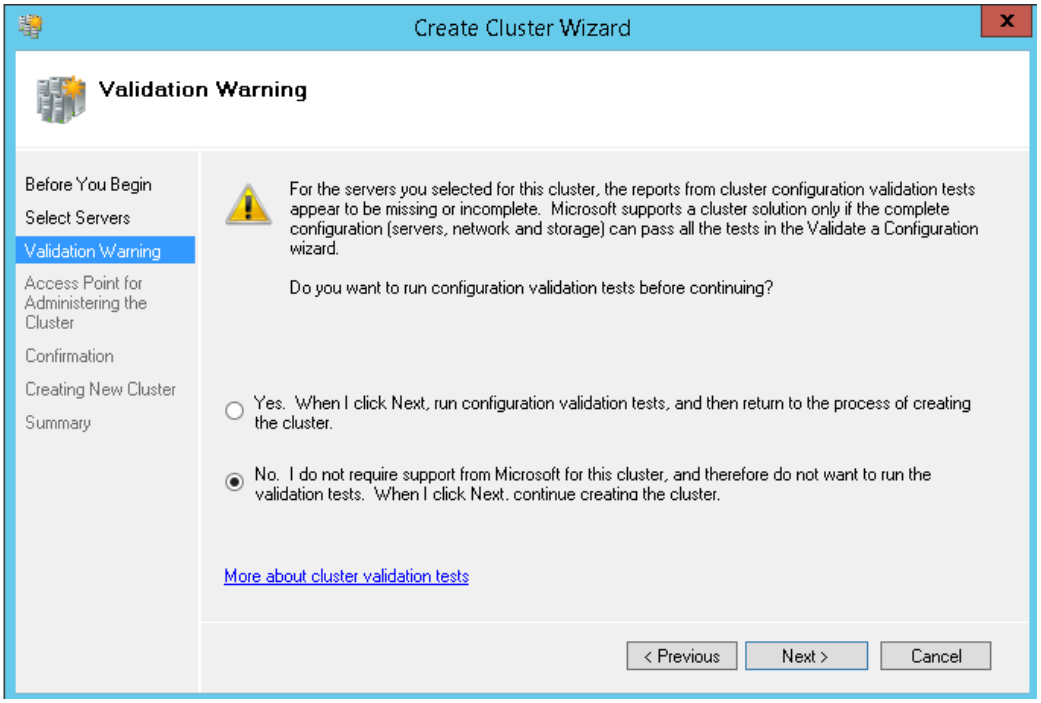

4. Hộp thoại **Select Computers**, nhập **LON-SVR1**; **LON-SVR2**, chọn **Check Names**, và chọn **OK**.



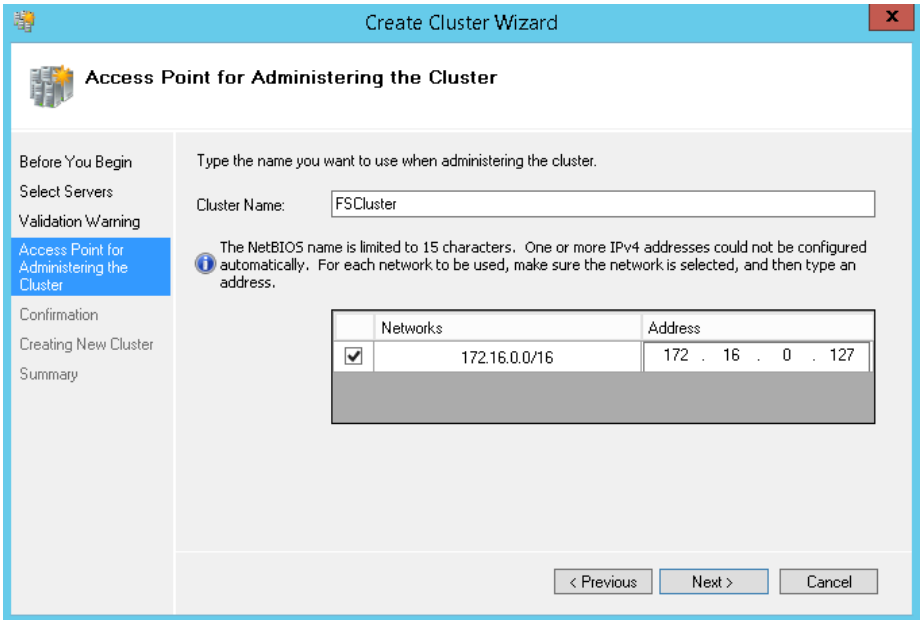
5. Cửa sổ **Select Servers**, kiểm tra có 2 máy **LON-SVR1.adatum.com** và **LON-SVR2.adatum.com** , chọn **Next**.



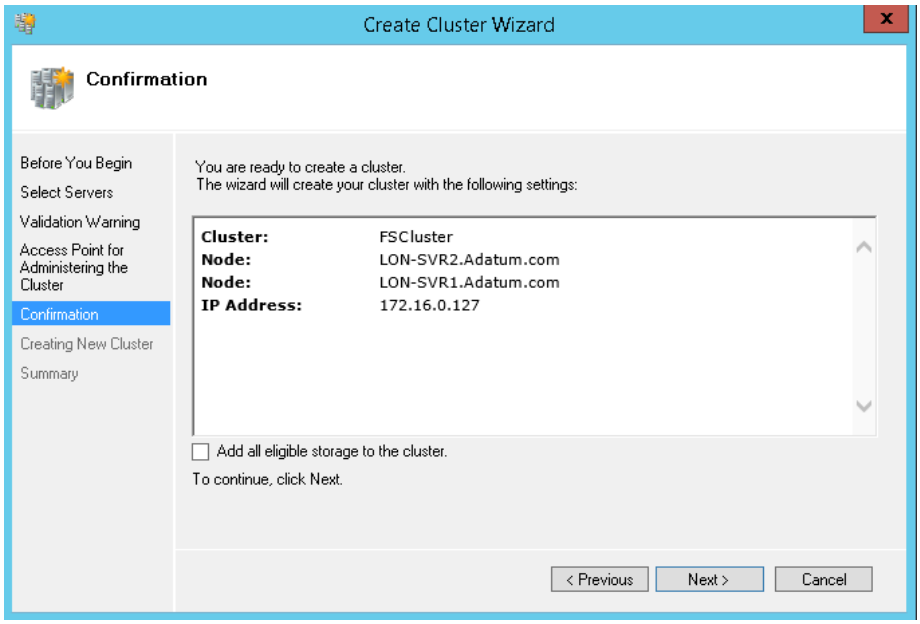

6. Cửa sổ **Validation Warning**, chọn **No, I do not require support from Microsoft for this cluster**, và chọn **Next**.



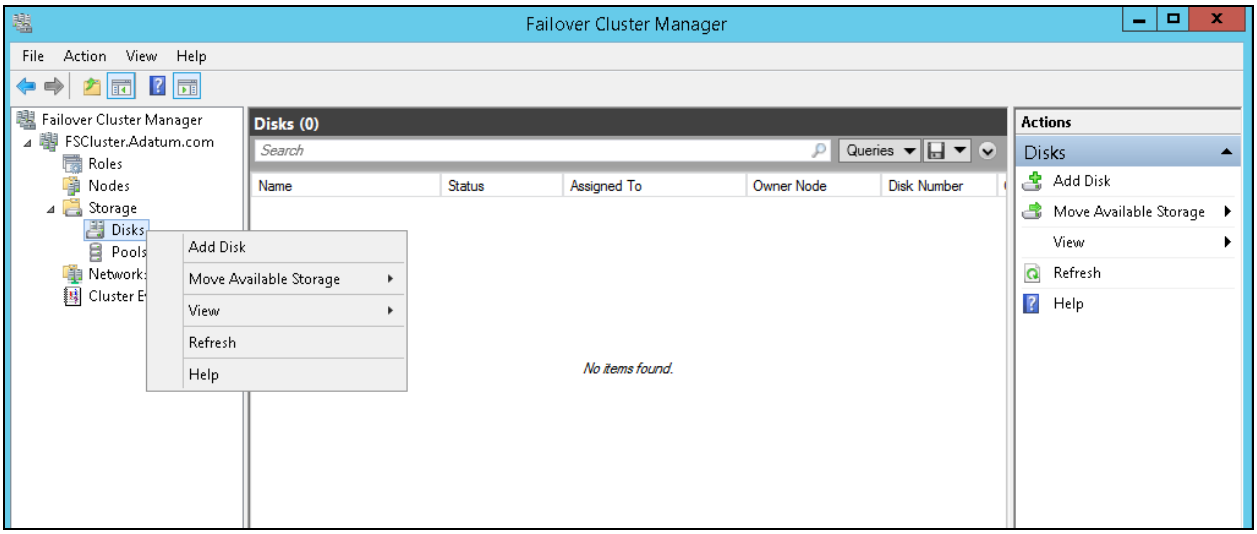
7. Cửa sổ **Access Point for Administering the Cluster**, trong ô **Cluster Name**, nhập **FSCluster**, trong ô **Address**, nhập **172.16.0.127**, và chọn **Next**.



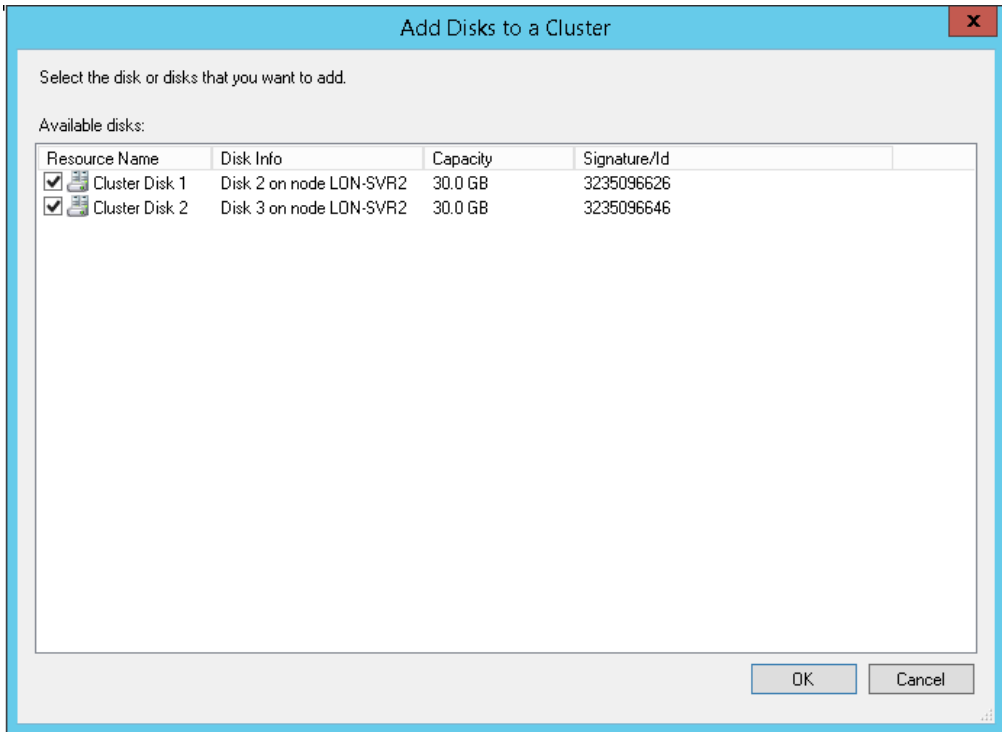

8. Cửa sổ **Confirmation**, bỏ dấu chọn **Add all eligible storage to the cluster**, chọn **Next**, và chọn **Finish**.



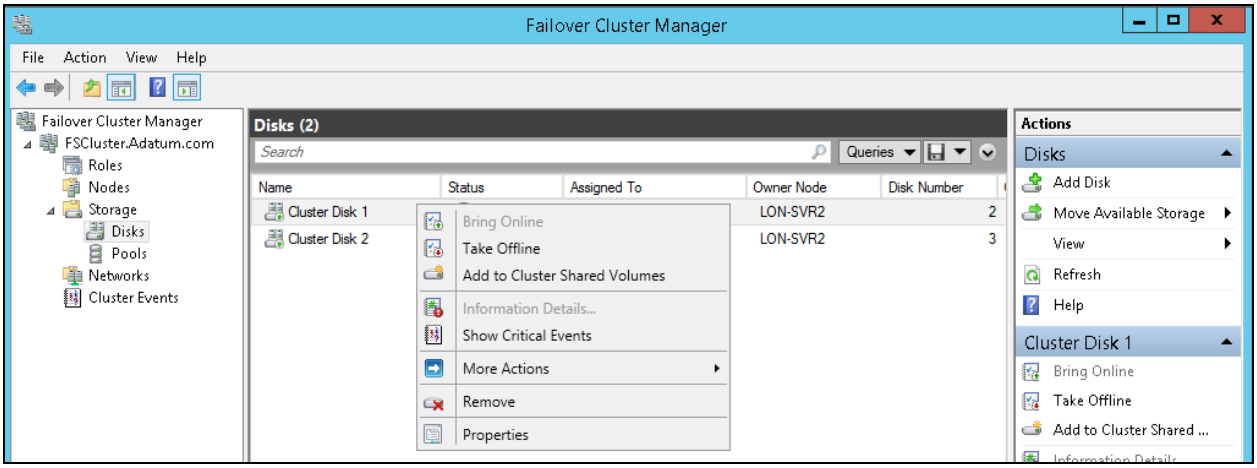
9. Trong cửa sổ **Failover Cluster Manager**, bung **FSCluster.Adatum.com**, bung **Storage**, chuột phải **Disks**, chọn **Add Disk**.



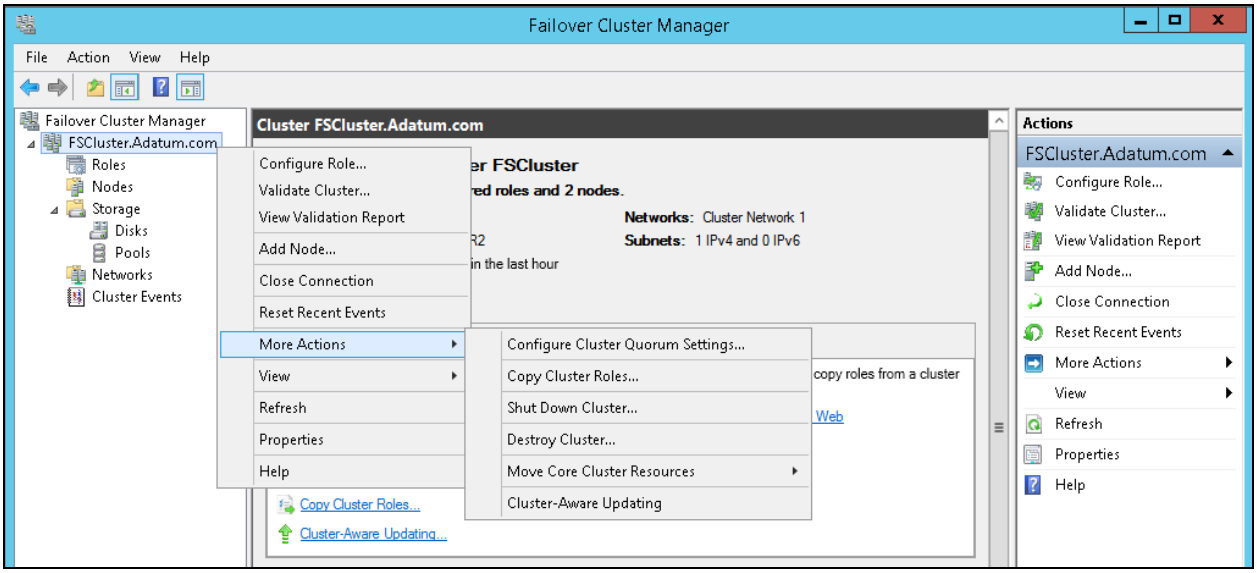

10. Hộp thoại **Add Disks to a Cluster**, kiểm tra có đánh dấu chọn **Cluster Disk 1** và **Cluster Disk 2**, chọn **OK**.



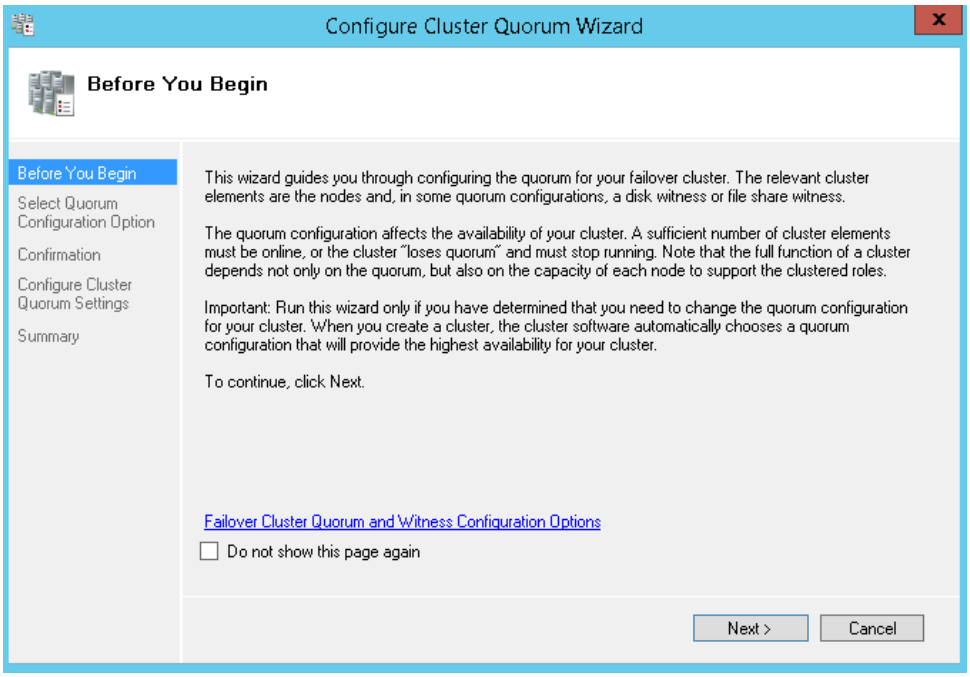
11. Kiểm tra 2 đĩa **Cluster Disk 1** và **Cluster Disk 2** đã hiển thị trong cửa sổ **Failover Cluster Manager**. Chuột phải **Cluster Disk 1**, chọn **Add to Cluster Shared Volumes.**



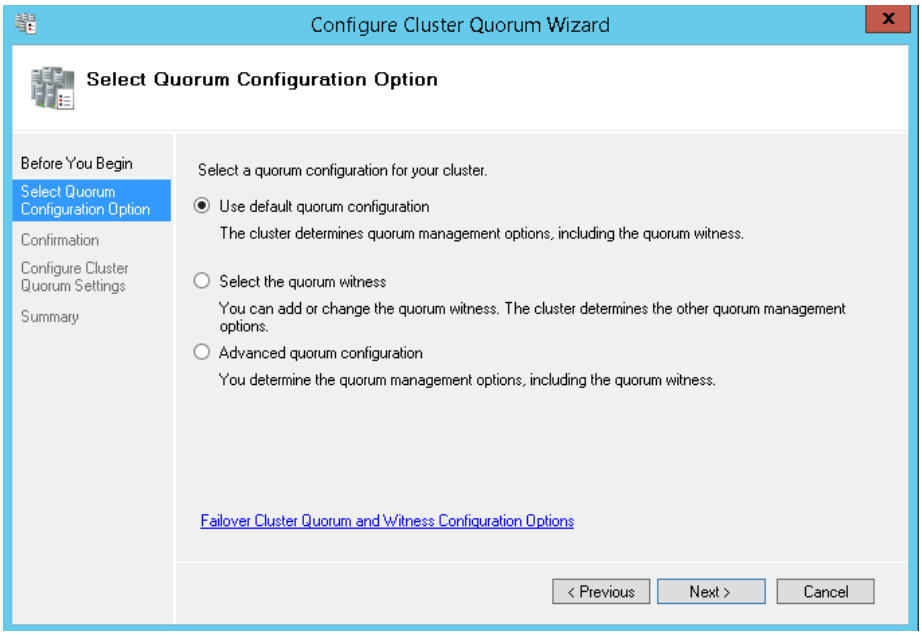

12. Trong cửa sổ **Failover Cluster Manager,** chuột phải **FSCluster.Adatum.com**, bung **More Actions**, chọn **Configure Cluster Quorum Settings**.



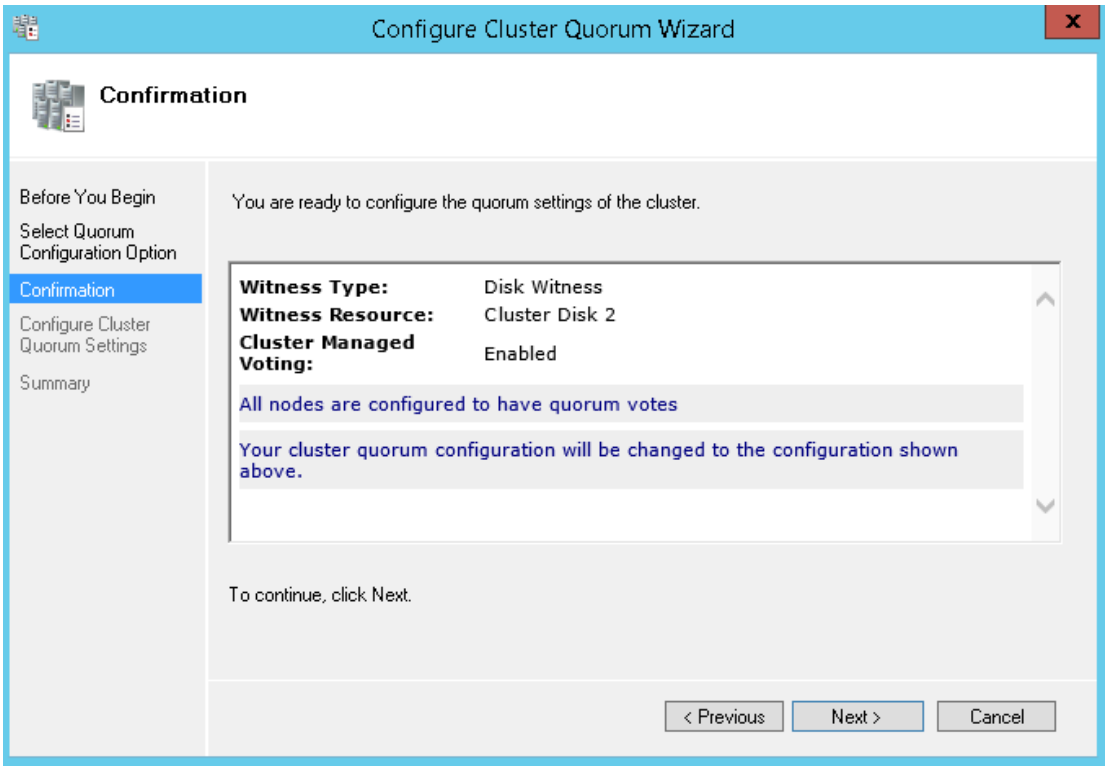
13. Cửa sổ **Before You Begin**, chọn **Next**.



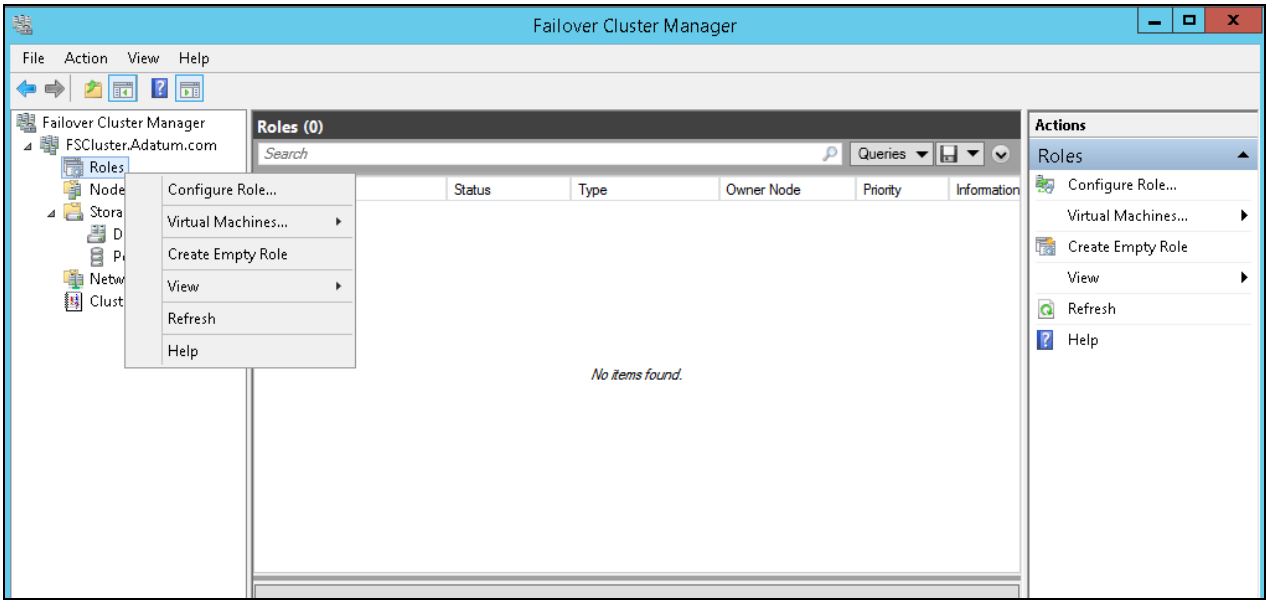

14. Cửa sổ **Select Quorum Configuration Option**, chọn **Use default quorum configuration**, và chọn **Next**.



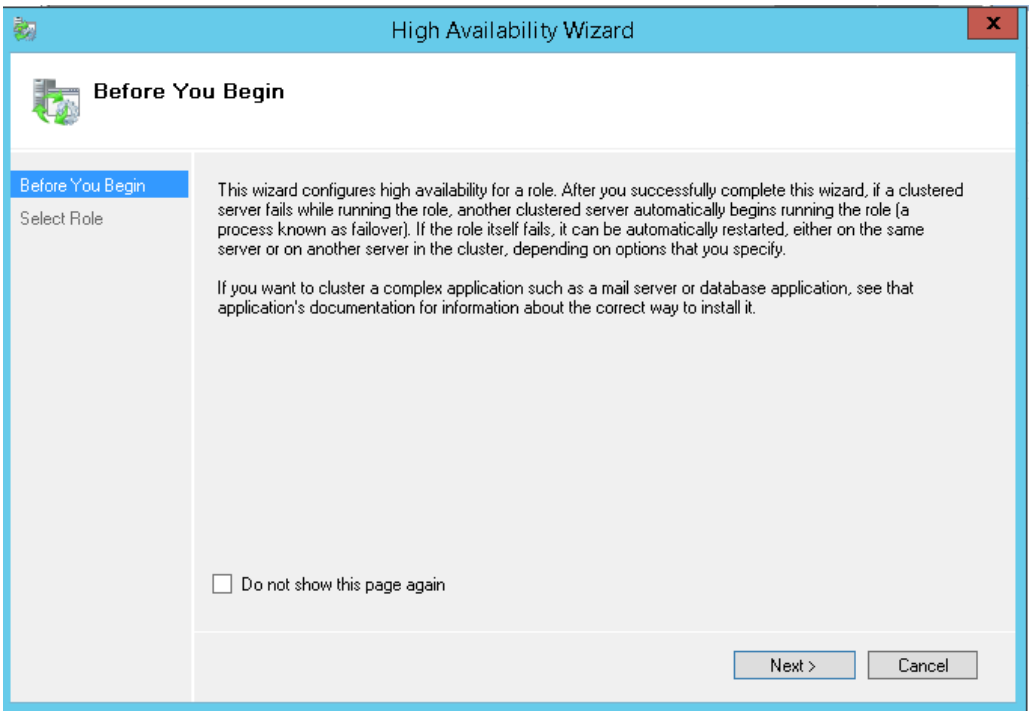
15. Cửa sổ **Confirmation**, chọn **Next**, và chọn **Finish**.



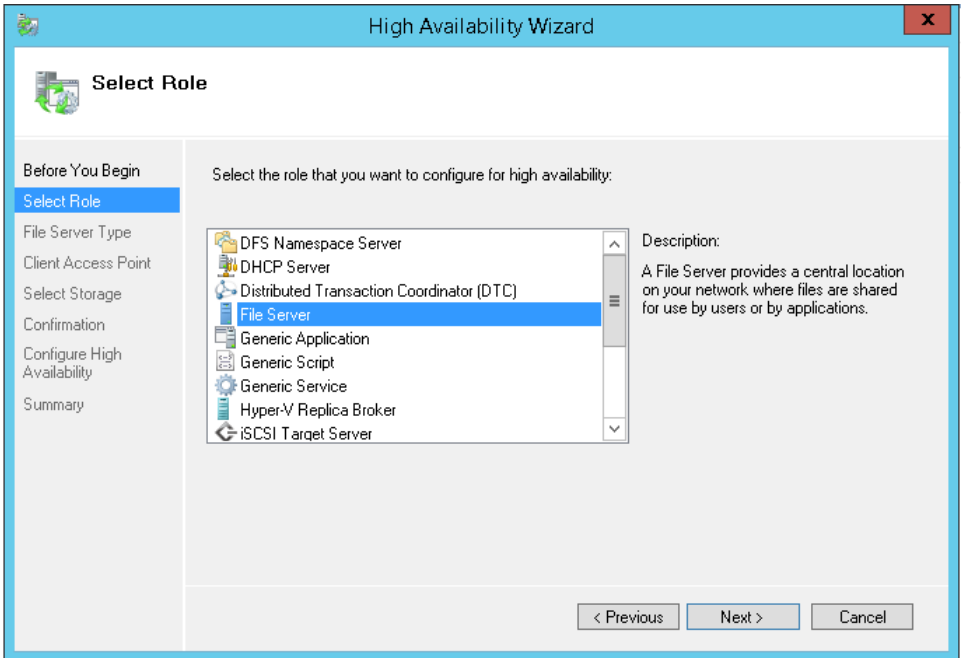

16. Bung **FSCluster.Adatum.com,** chuột phải **Roles**, chọn **Configure Role**.



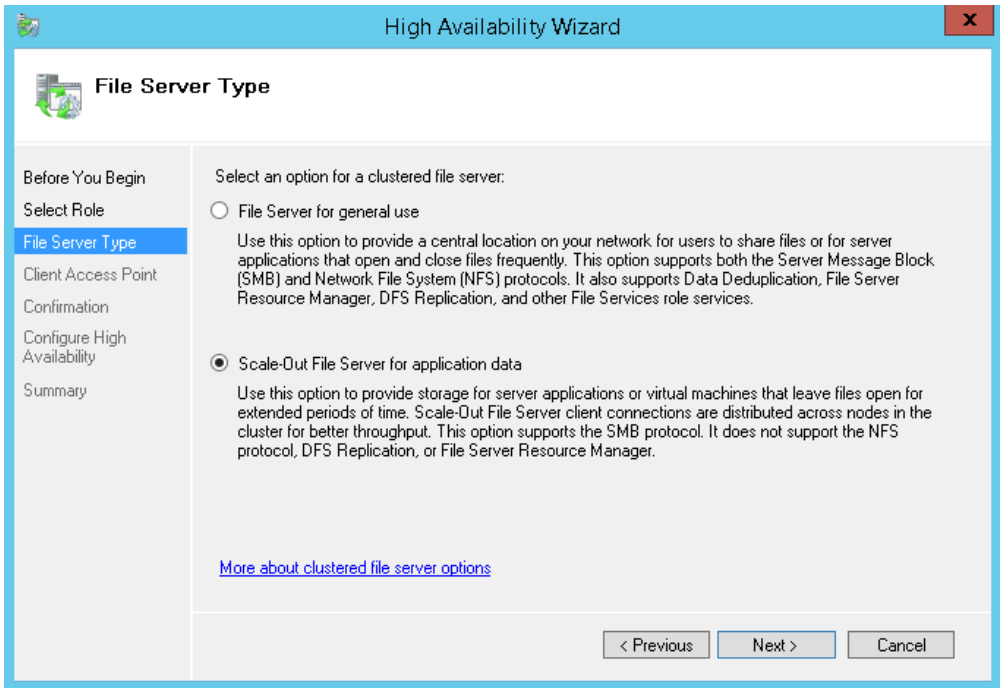
17. Cửa sổ **Before You Begin**, chọn **Next**.



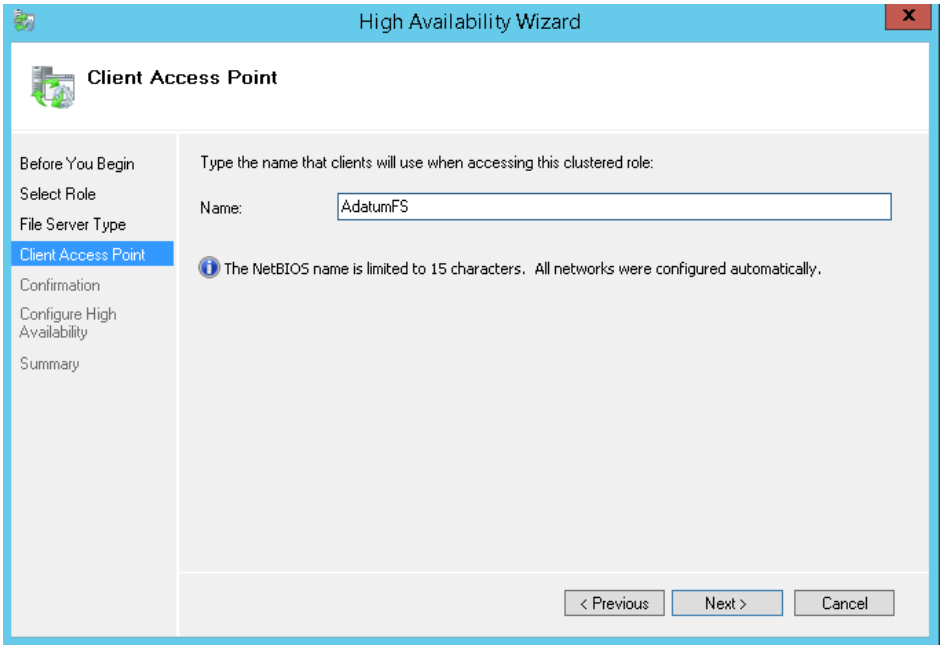

18. Cửa sổ **Select Role**, chọn **File Server**, chọn **Next**.



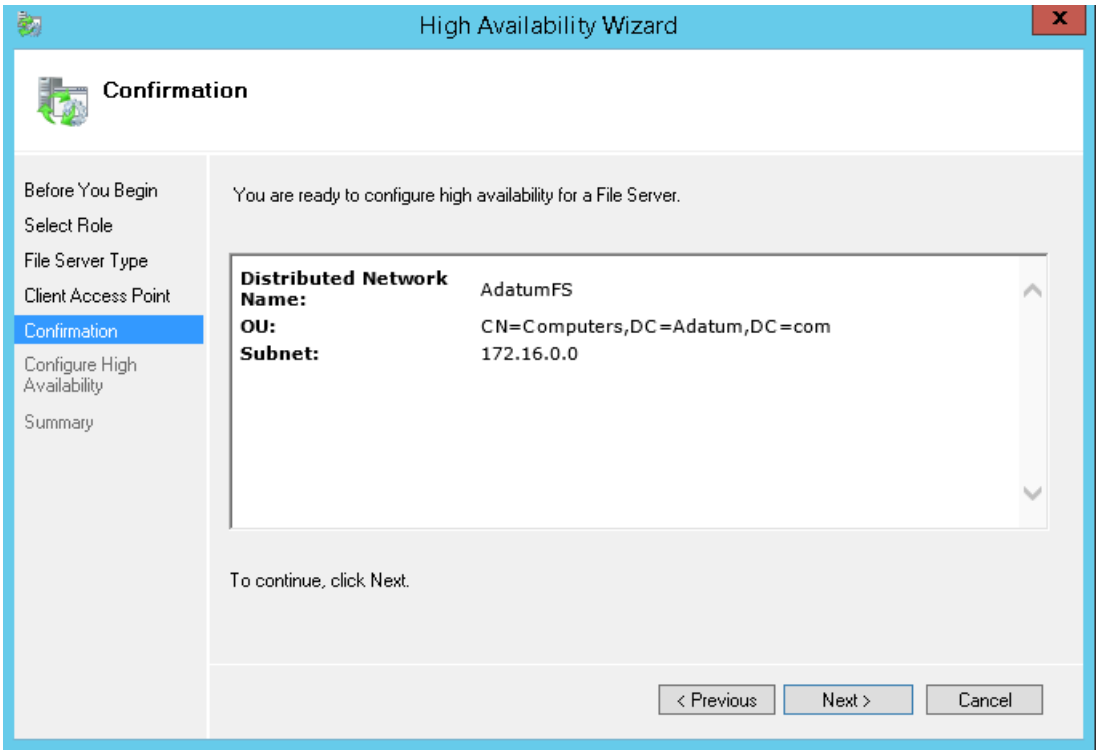
19. Cửa sổ **File Server Type**, chọn **Scale-Out File Server for application data**, chọn **Next**.




20. Cửa sổ **Client Access Point**, trong ô **Name**, nhập **AdatumFS**, chọn **Next**.

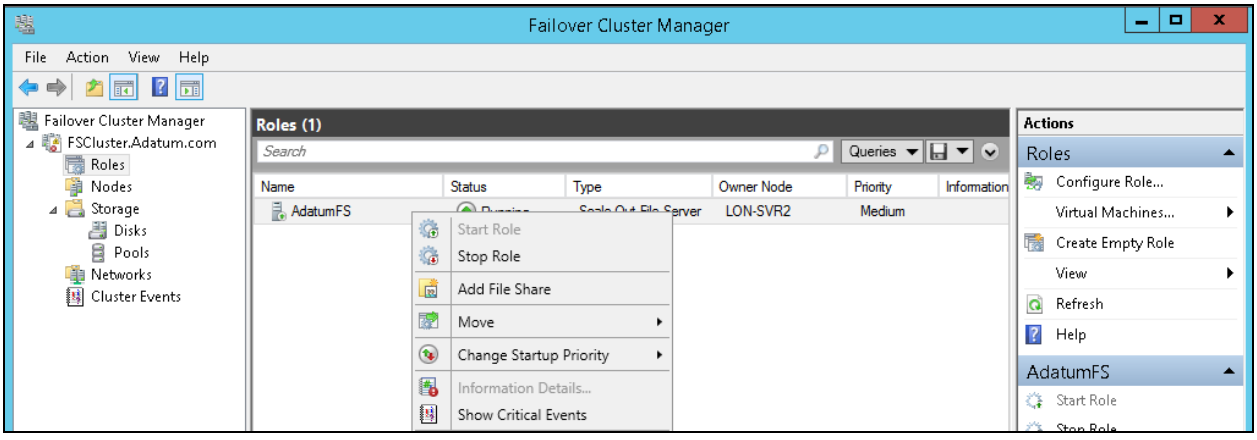


21. Cửa sổ **Confirmation**, chọn **Next**, và chọn **Finish**.

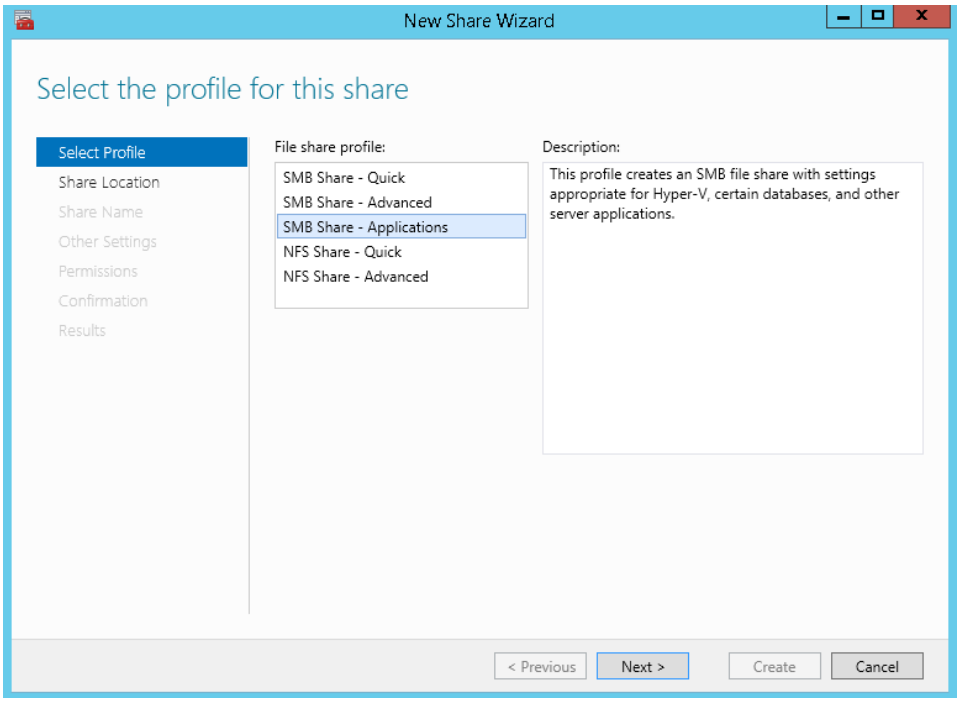



## Bước 4. Tạo File Share

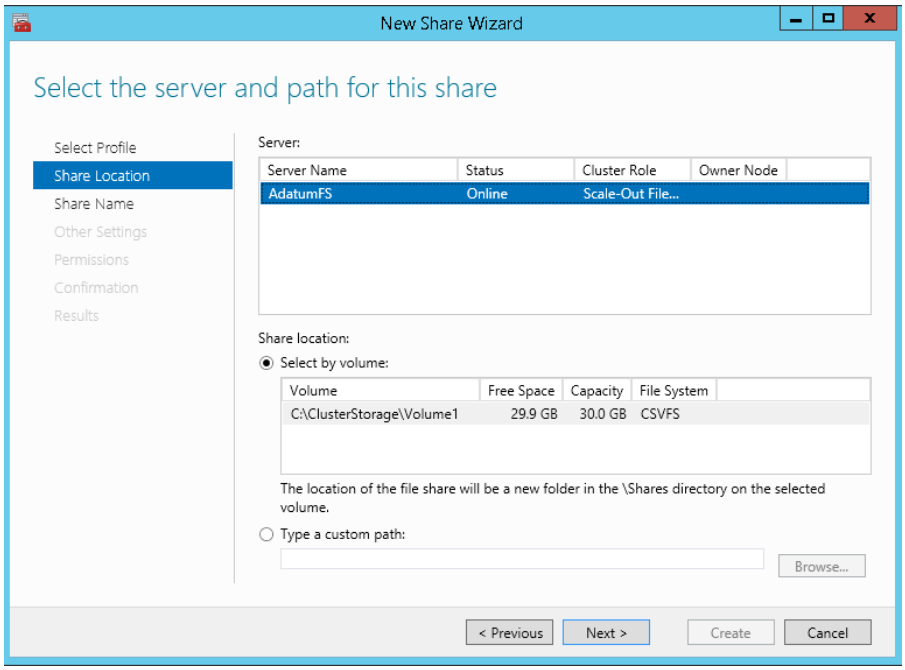
1. Trên máy **LON-SVR1**, trong cửa sổ **Failover Cluster Manager**, chọn **Roles**, chuột phải **AdatumFS**, chọn A**dd File Share.** (Nếu nhận được thông báo **Client Access Point is not ready**, thì bạn thực hiện lại bước này và các bước tiếp theo trên máy **LON-SVR2**.)



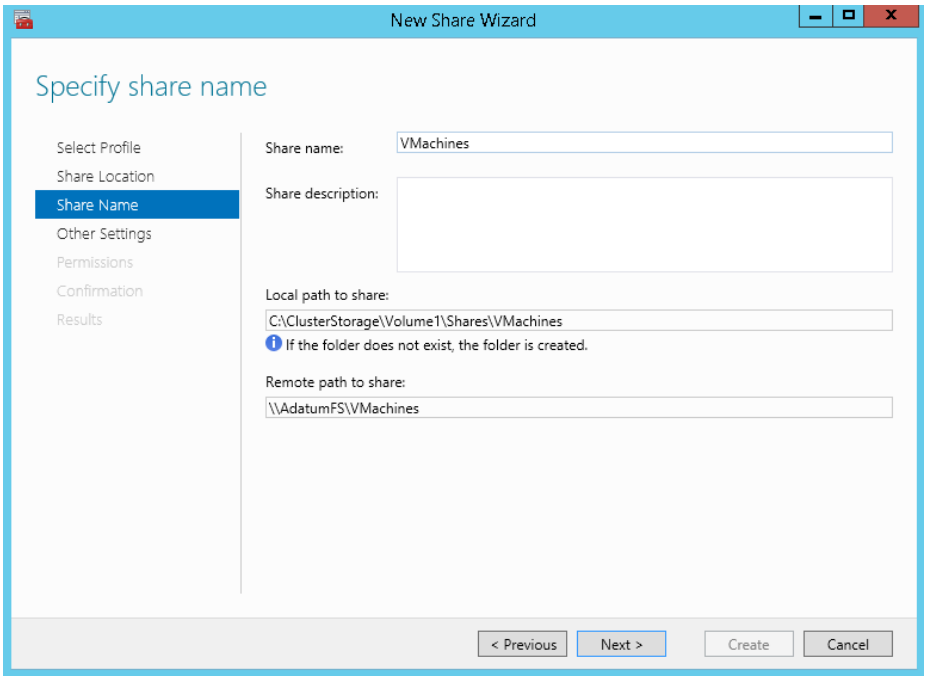
2. Cửa sổ **Select the profile for this share**, chọn **SMB Share- Applications**, và chọn **Next**.



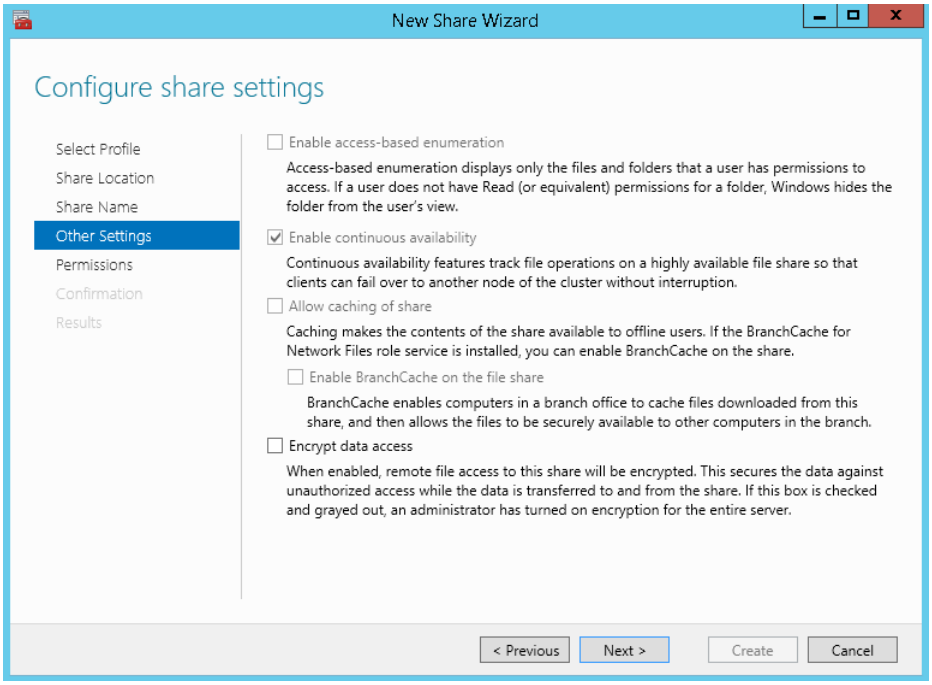

3. Cửa sổ **Select the server and path for this share**, chọn **Select by volume**, và chọn **Next**.



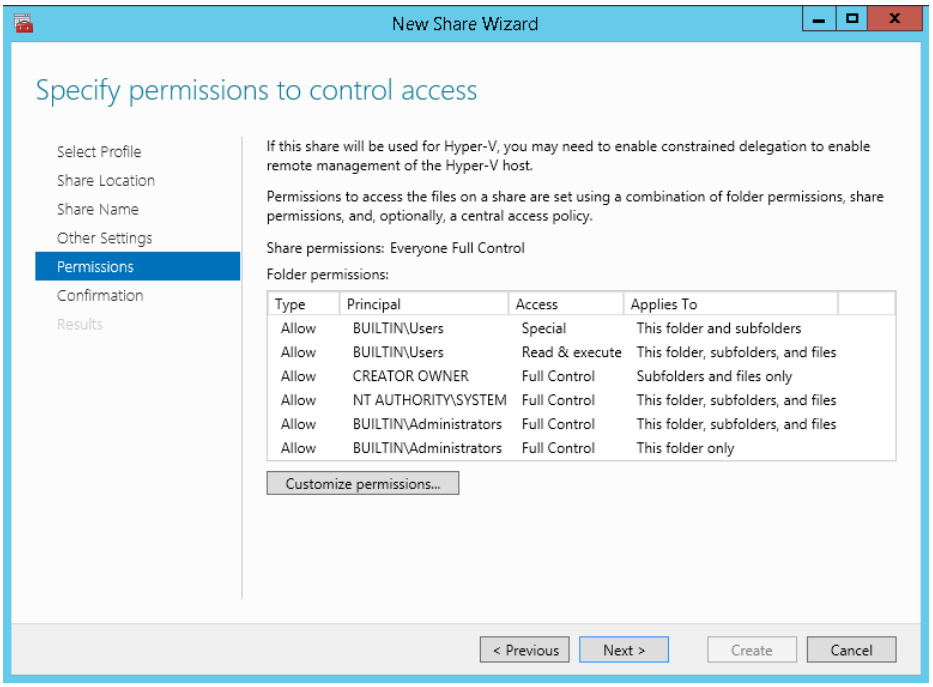
4. Cửa sổ **Specify share name**, trong ô **Share name**, nhập **VMachines**, và chọn **Next**.



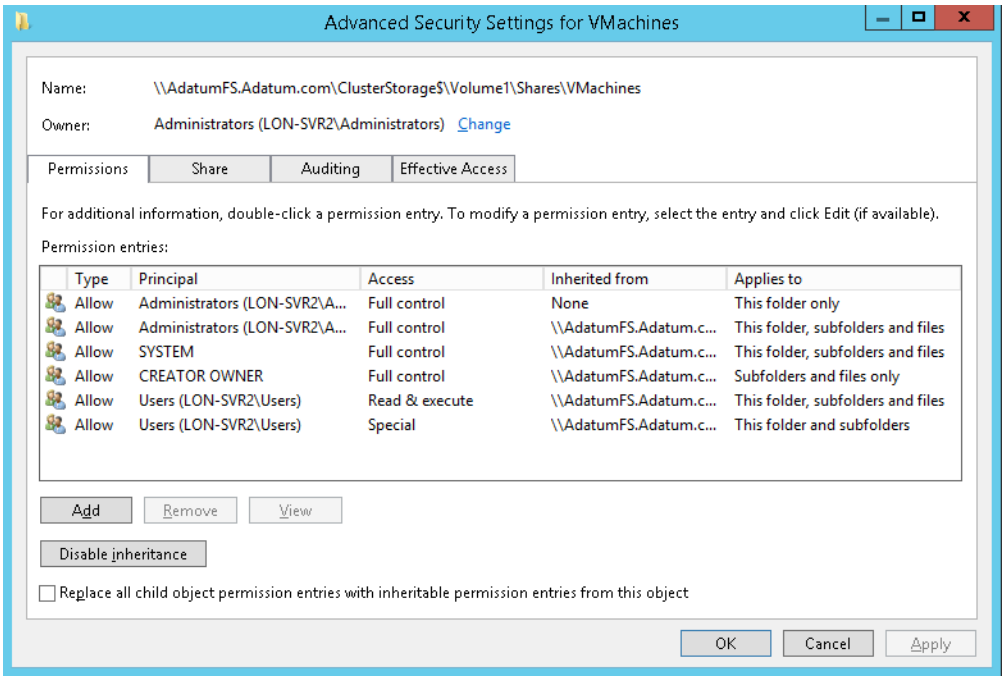

5. Cửa sổ **Configure share settings**, chọn **Next**.



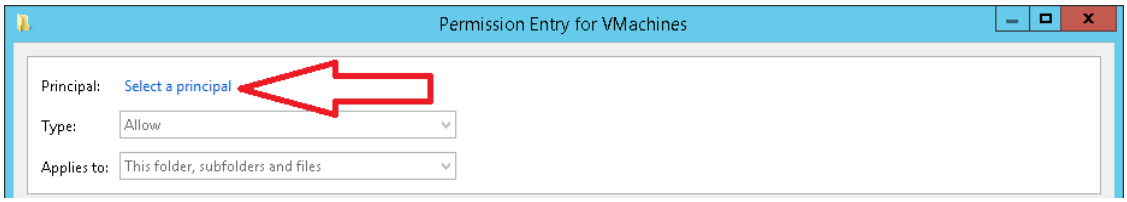
6. Cửa sổ **Specify permissions to control access**, chọn **Customize permissions**.



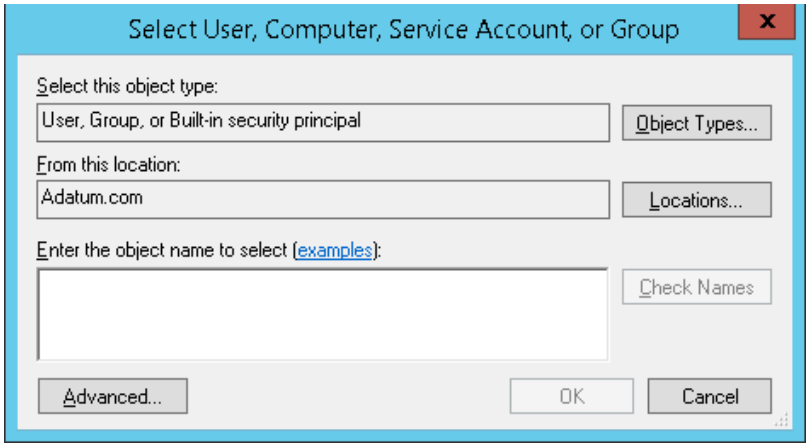

7. Cửa sổ **Advanced Security Settings for VMachines**, chọn **Add**.



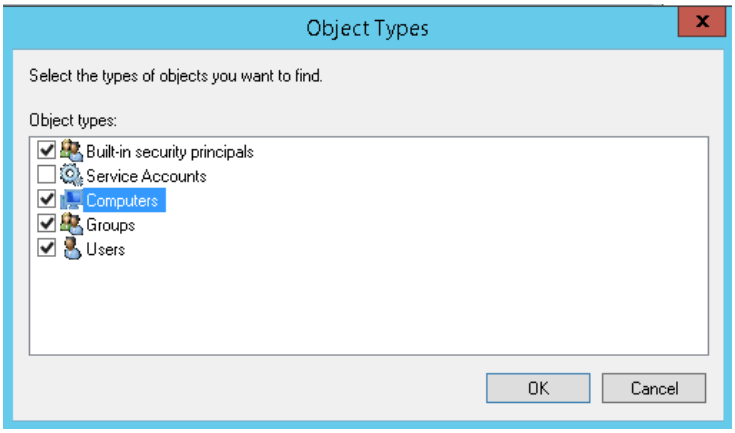
8. Cửa sổ **Permission Entry for VMachines**, chọn **Select a principal**.



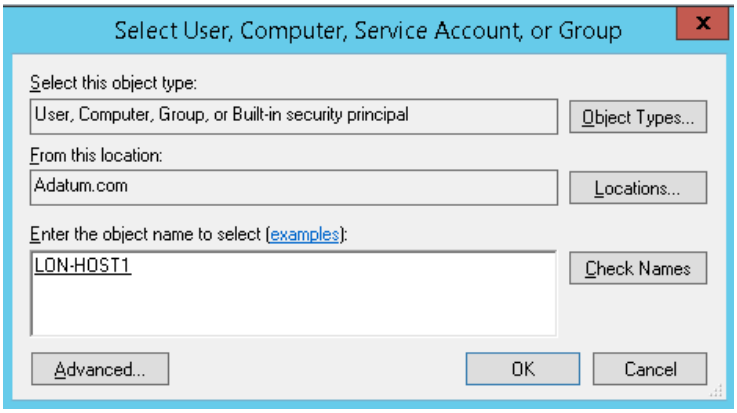

9. Hộp thoại **Select User, Computer, Service Account, or Group**, chọn **Object Types**.



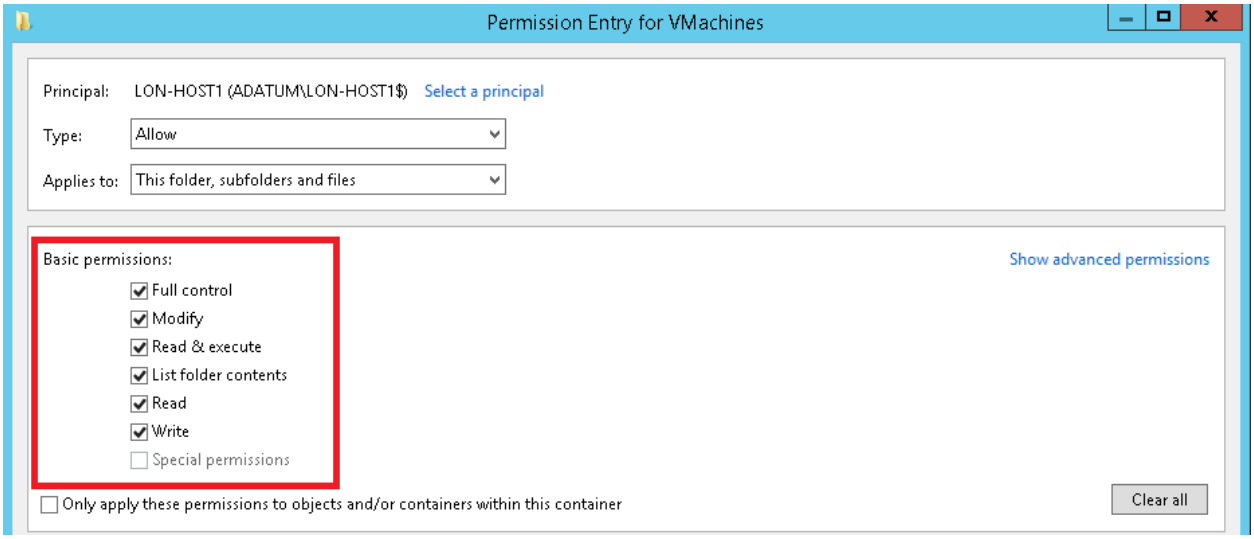

10. Hộp thoại **Object Types**, đánh dấu chọn **Computers**, và chọn **OK**.



11. Hộp thoại **Select User, Computer, Service Account, or Group**, nhập **LON-HOST1**, chọn **Check Names**, và chọn **OK**.



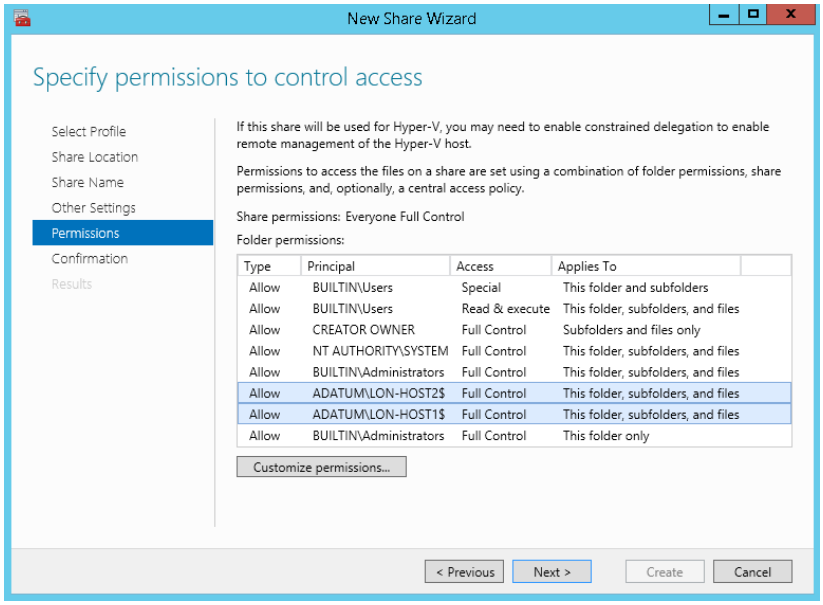

12. Trong phần **Basic Permissions**, đánh dấu chọn **Full Control**, và chọn **OK**.



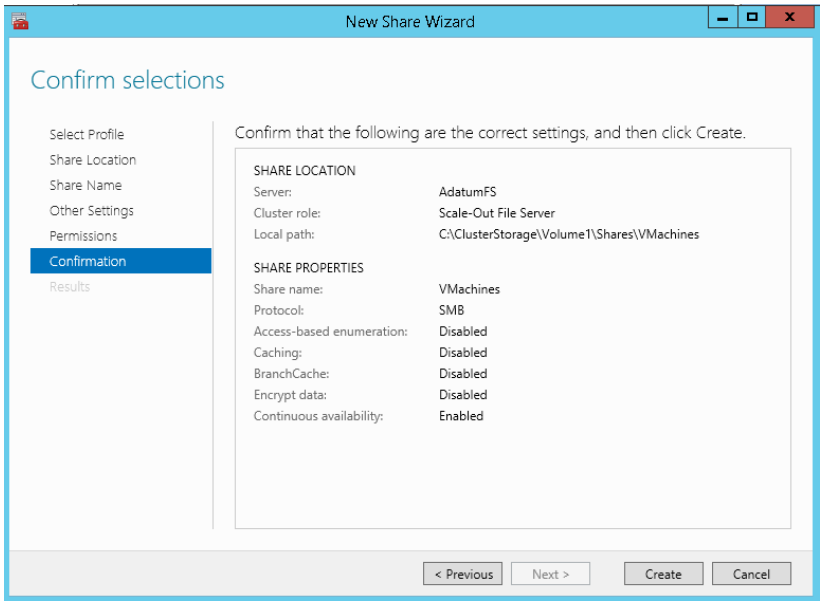

13. Lặp lại từ bước 7 đến 12 để cấp quyền **Full control** cho máy **LON-HOST2**.

14. Chọn **OK** để tắt cửa sổ **Advanced Security Settings for VMachines**.

15. Cửa sổ **Specify permissions to control access**, đảm bảo **ADATUM\LON-HOST1$** và **ADATUM\LON-HOST2$** có quyền Full Control, và chọn **Next**.




16. Cửa sổ **Confirm selections**, chọn **Create**, và chọn **Close**.



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công High Availability cho File Server**

## Bài tập 3: Cấu hình Cluster-Aware Updating (CAU).

Bây giờ, bạn sẽ cần phải cấu hình và kích hoạt tính năng CAU để cập nhật cho tất cả các host trong cùng một Failover Cluster.

❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình CAU
2. Cập nhật Failover Cluster

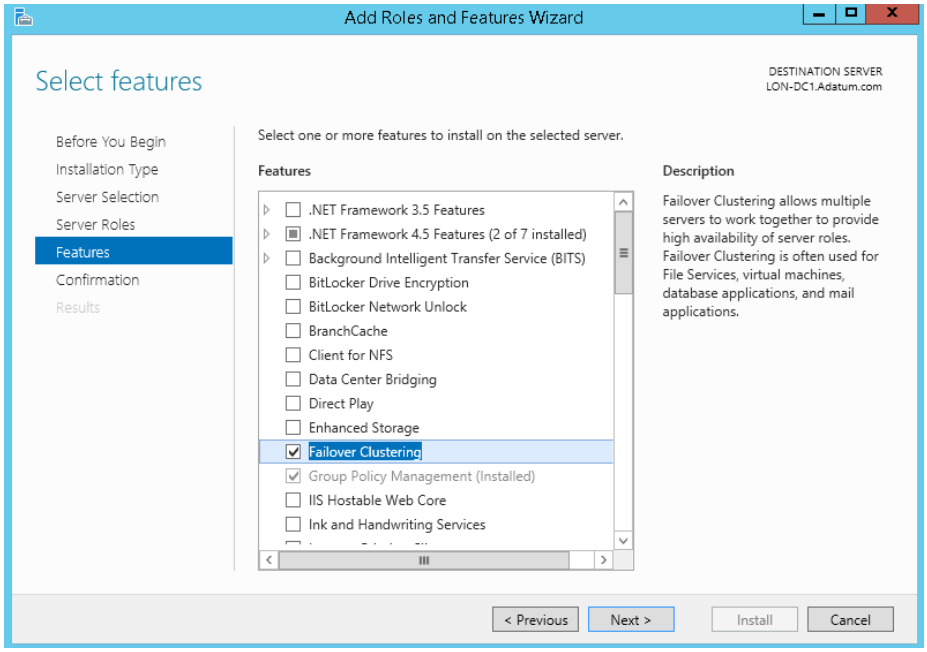
❖ **Thực hiện:**

### Bước 1. Cấu hình CAU

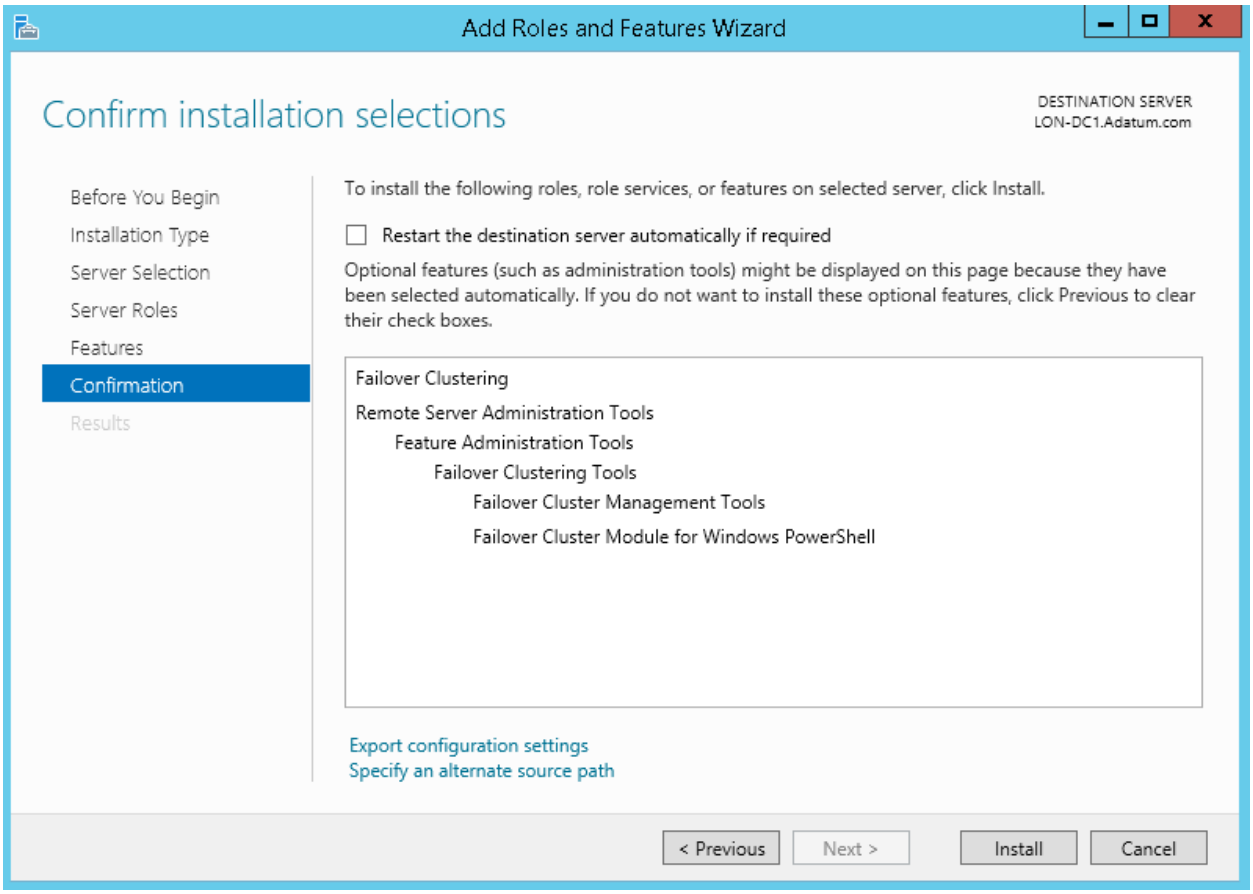
1. Trên máy **LON-DC1**, trong cửa sổ **Server Manager**, chọn **Add roles and features**.

2. Cửa sổ **Before You Begin**, chọn **Next** 4 lần.

3. Cửa sổ **Select features**, đánh dấu chọn **Failover Clustering**, chọn **Add Features**, và chọn **Next**.



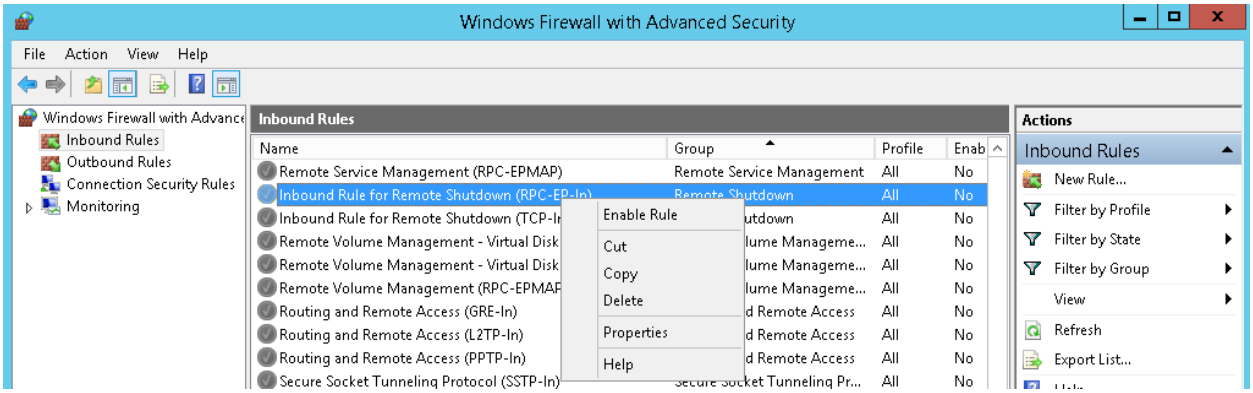
4. Cửa sổ **Confirm installation selections**, chọn **Install**.



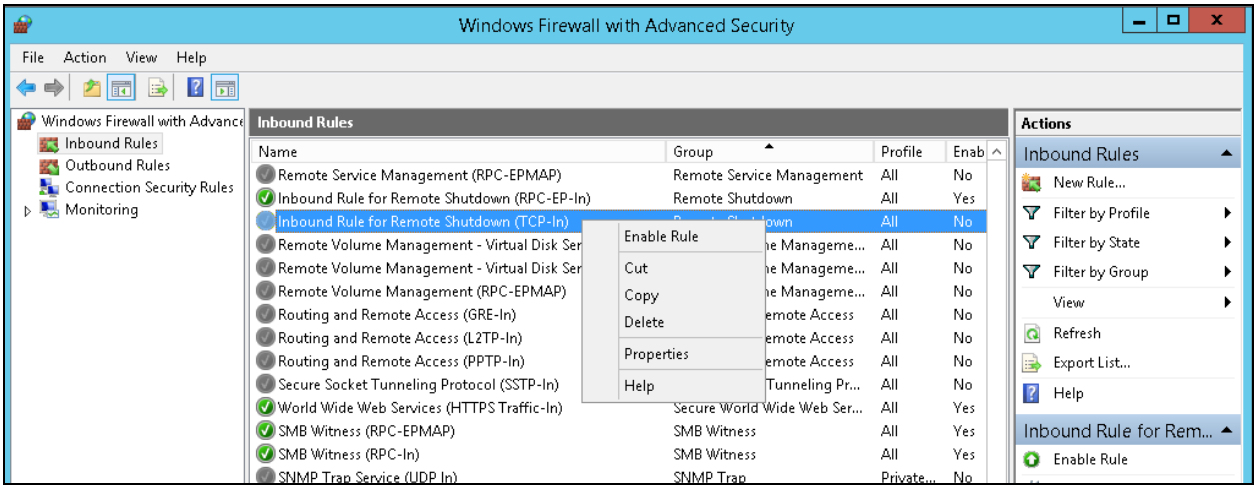

5. Sau khi cài đặt thành công, chọn **Close**.

6. Qua máy **LON-SVR1**, trong **Server Manager**, bung menu **Tools**, mở **Windows Firewall with Advanced Security**.

7. Cửa sổ **Windows Firewall with Advanced Security**, chọn **Inbound Rules**, chuột phải lên rule **Inbound Rule for Remote Shutdown (RPC-EP-In)**, chọn **Enable Rule**.




8. Chuột phải lên rule **Inbound Rule for Remote Shutdown (TCP-In)**, chọn **Enable Rule**.

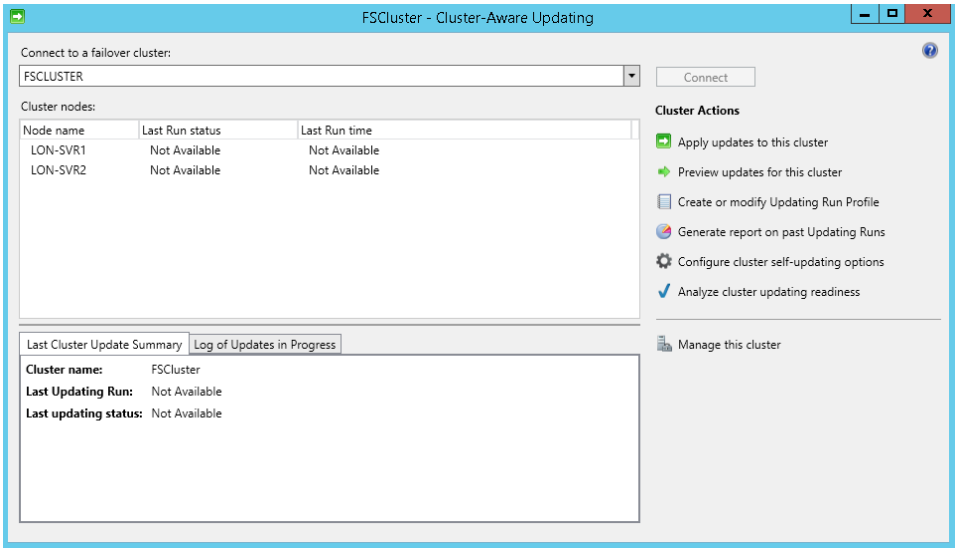



9. Tắt **Windows Firewall with Advanced Security**.

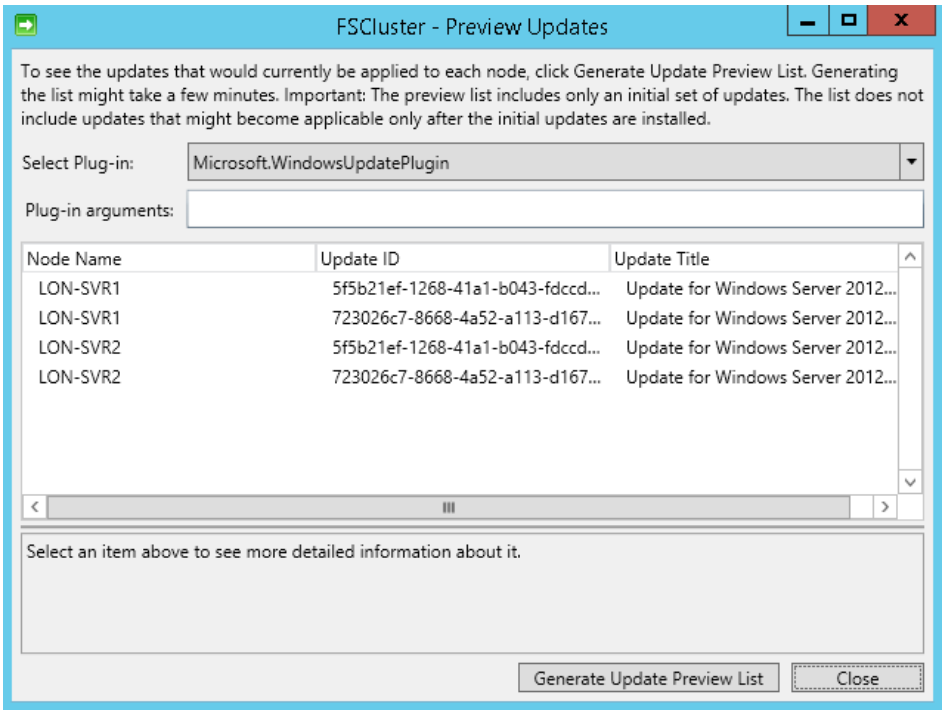
10. Qua máy **LON-SVR2**, Lặp lại từ bước 6 đến bước 9.

11. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Cluster-Aware Updating**.

12. Cửa sổ **Cluster-Aware Updating**, bung ô **Connect to a failover cluster**, chọn **FSCLUSTER**, chọn **Connect**, và chọn **Preview updates for this cluster**.

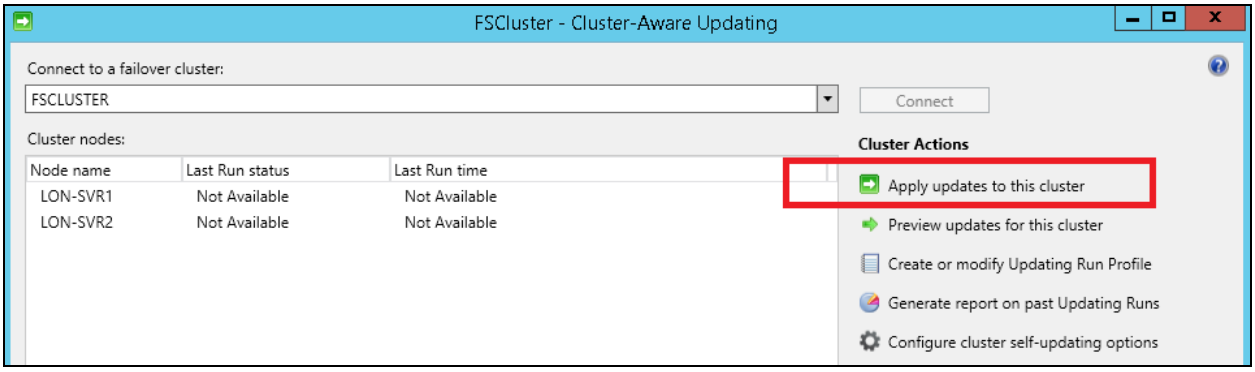



13. Cửa sổ **FSCLUSTER-Preview Updates**, chọn **Generate Update Preview List**. Sau vài phút, cập nhật sẽ xuất hiện trong danh sách. Xem xét cập nhật và sau đó chọn **Close**.

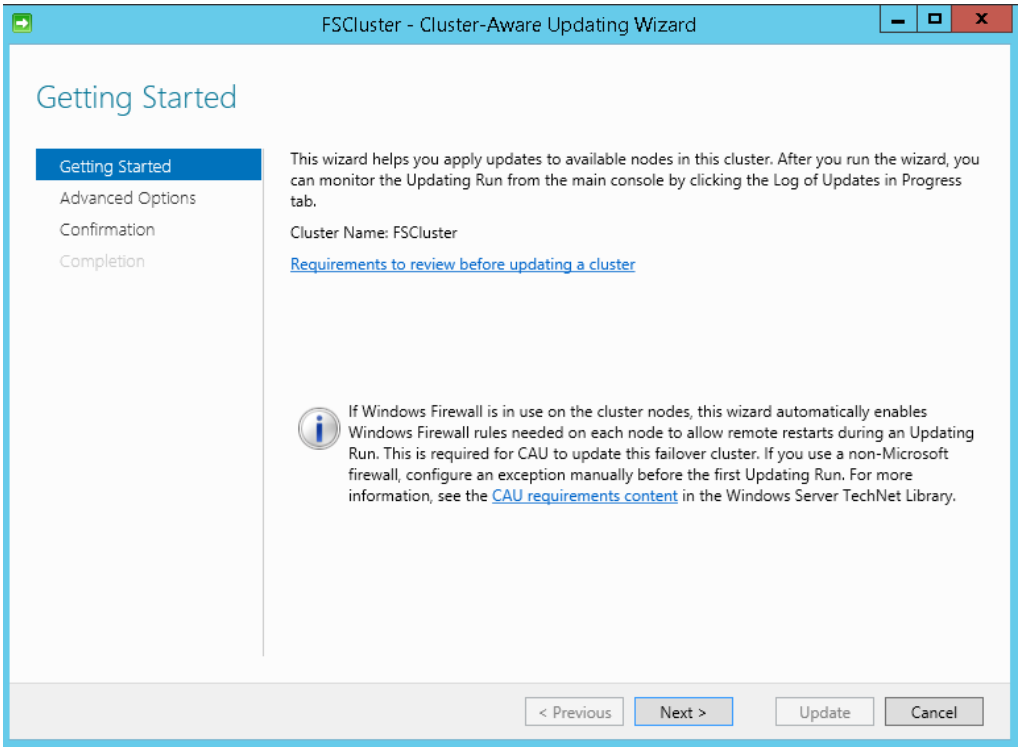


## Bước 2. Cập nhật Failover Cluster

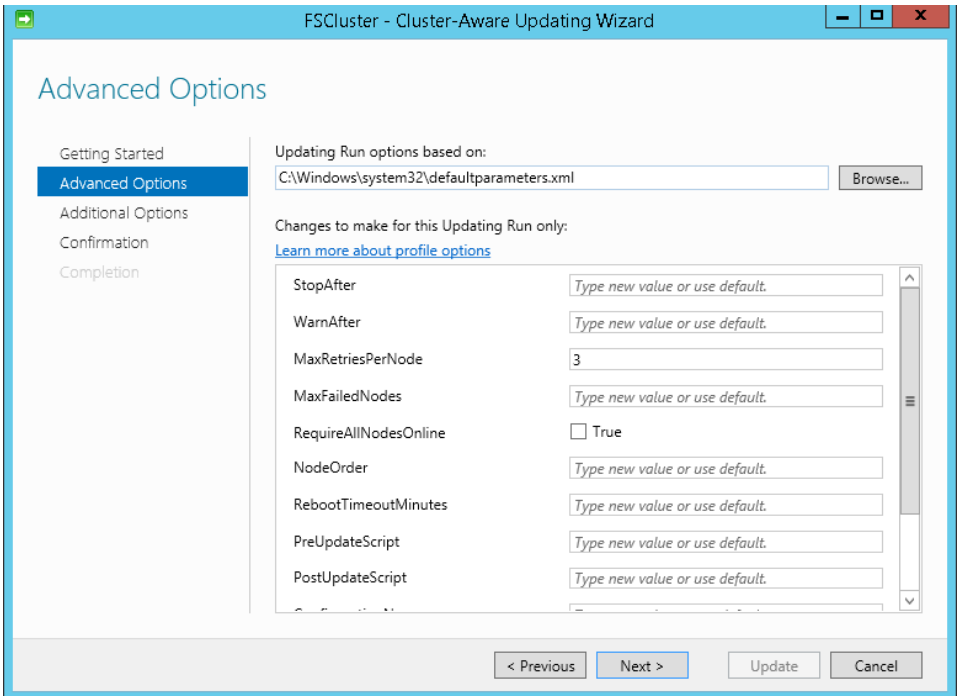
1. Trên **LON-DC1**, trong cửa sổ **Cluster-Aware Updating**, chọn **Apply updates to this cluster**.



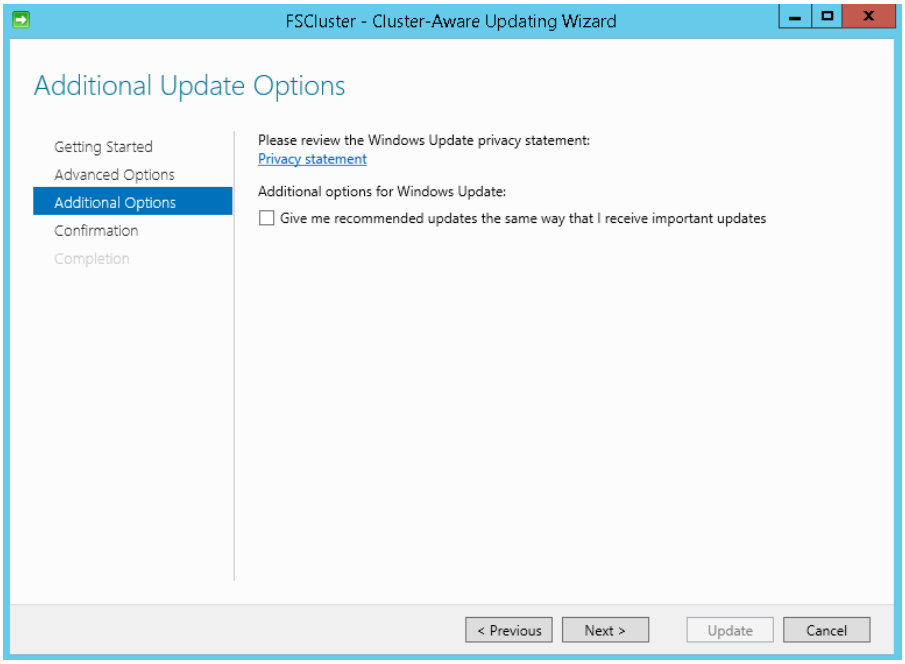

2. Cửa sổ **Getting Started**, chọn **Next**.



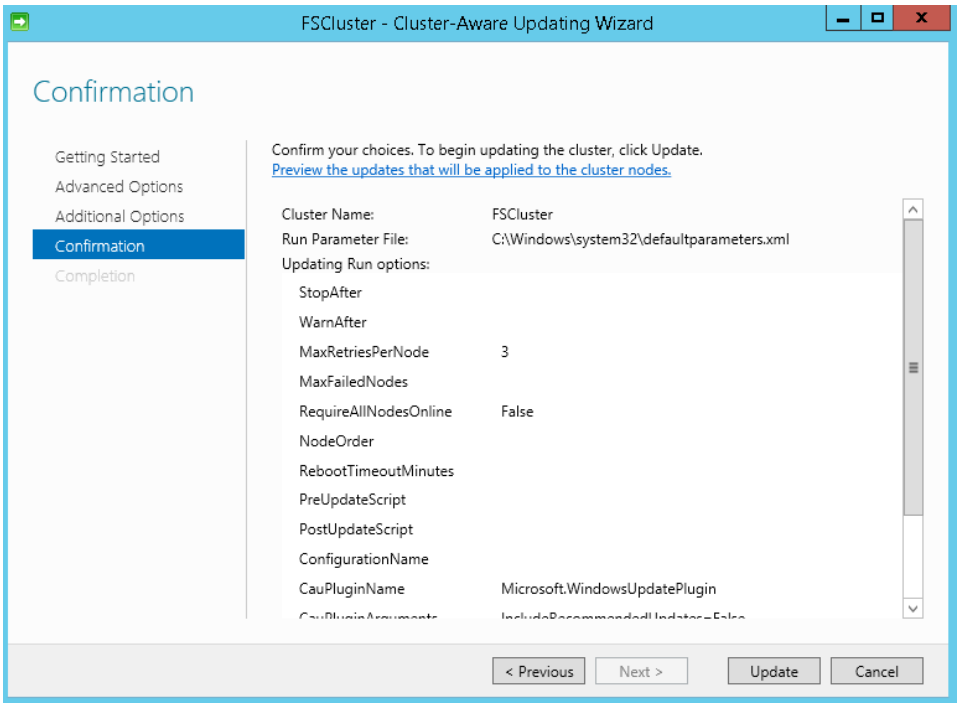
3. Cửa sổ **Advanced Options**, chọn **Next**.



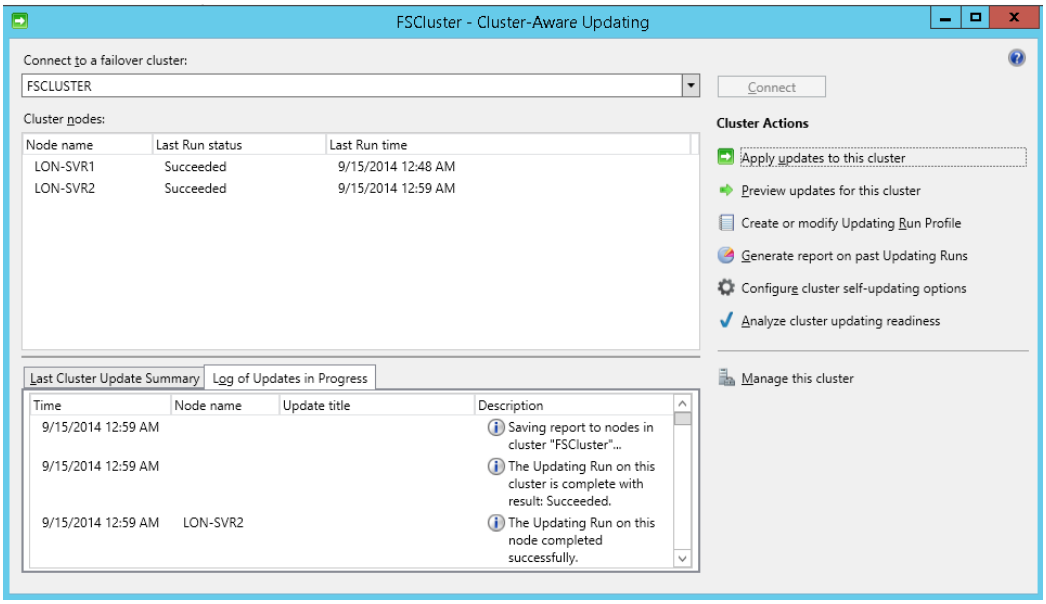

4. Cửa sổ **Additional Update Options**, chọn **Next**.



5. Cửa sổ **Confirmation**, chọn **Update**, và chọn **Close**.

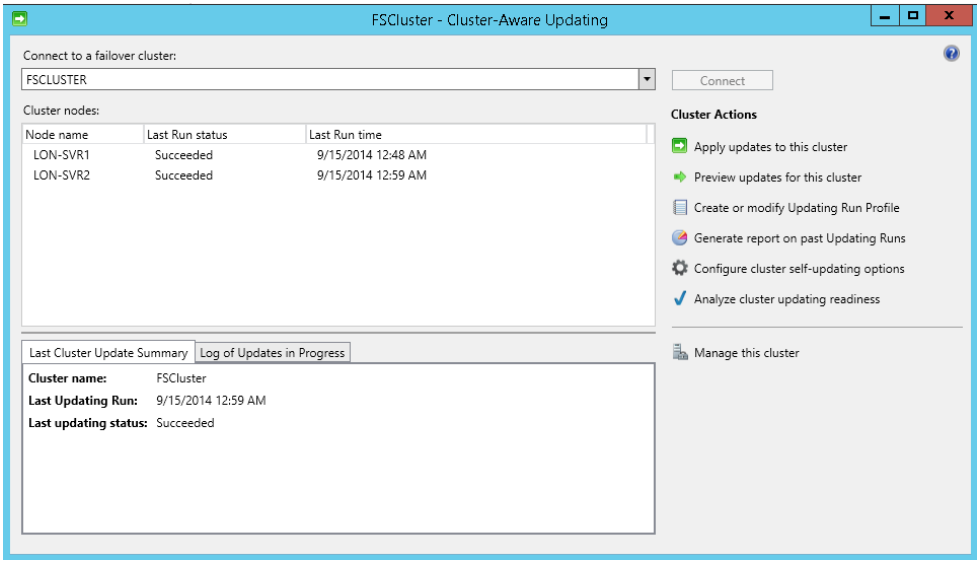



6. Trong cửa sổ **Cluster Nodes**, bạn có thể xem xét tiến độ cập nhật. đợi đến khi cột **Last Run status** báo **Succeeded**.

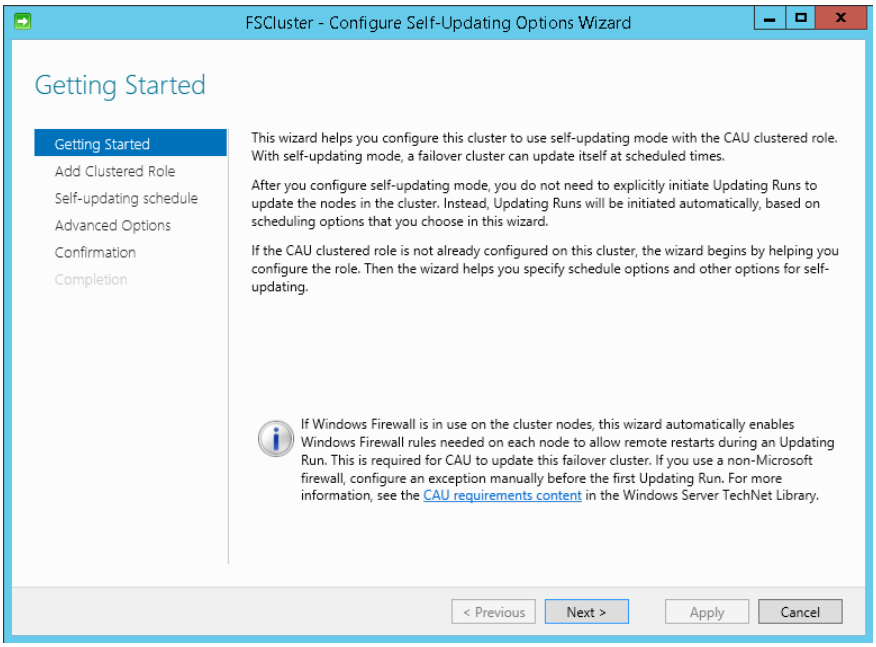


8. Qua máy **LON-SVR1** trong **Server Manager**, bung menu **Tools**, mở **Cluster-Aware Updating**.

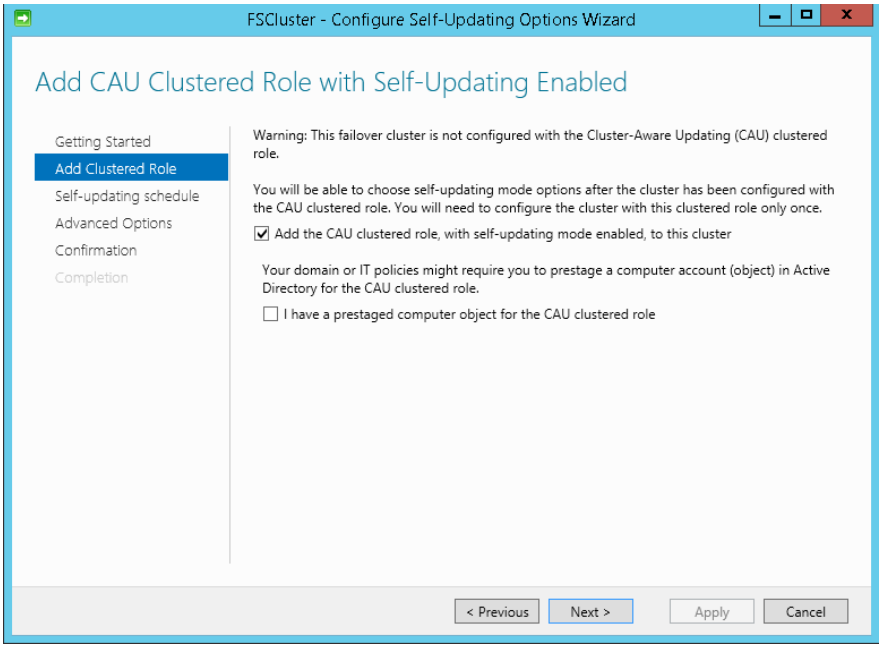
9. Cửa sổ **Cluster-Aware Updating**, bung ô **Connect to a failover cluster**, chọn **FSCLUSTER**, chọn **Connect**, chọn **Configure cluster self-updating options**.



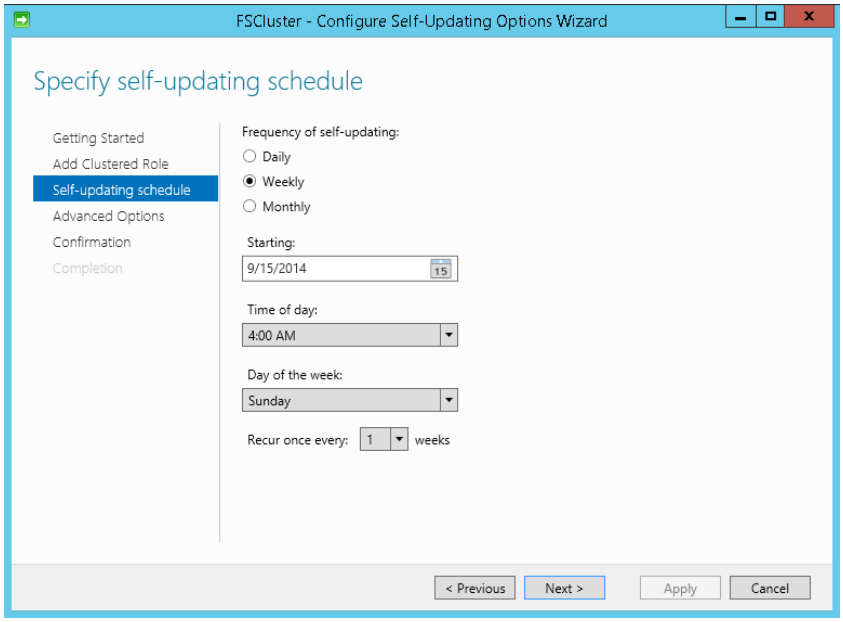

10. Cửa sổ **Getting Started**, chọn **Next**.



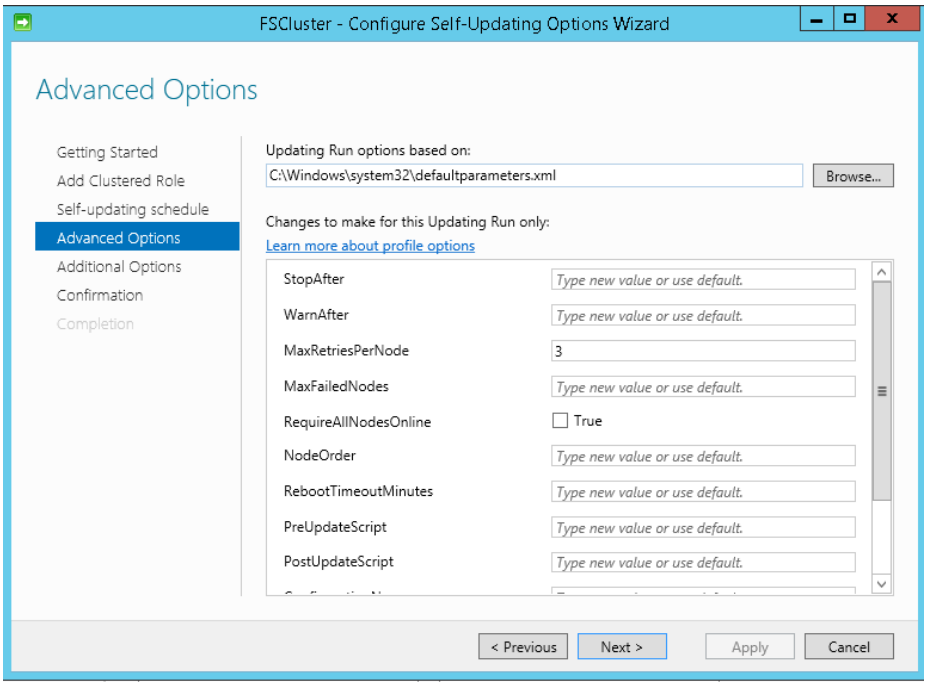
11. Cửa sổ **Add CAU Clustered Role with Self-Updating Enabled**, đánh dấu chọn **Add the CAU clustered role, with self-updating mode enabled, to this cluster**, và chọn **Next**.



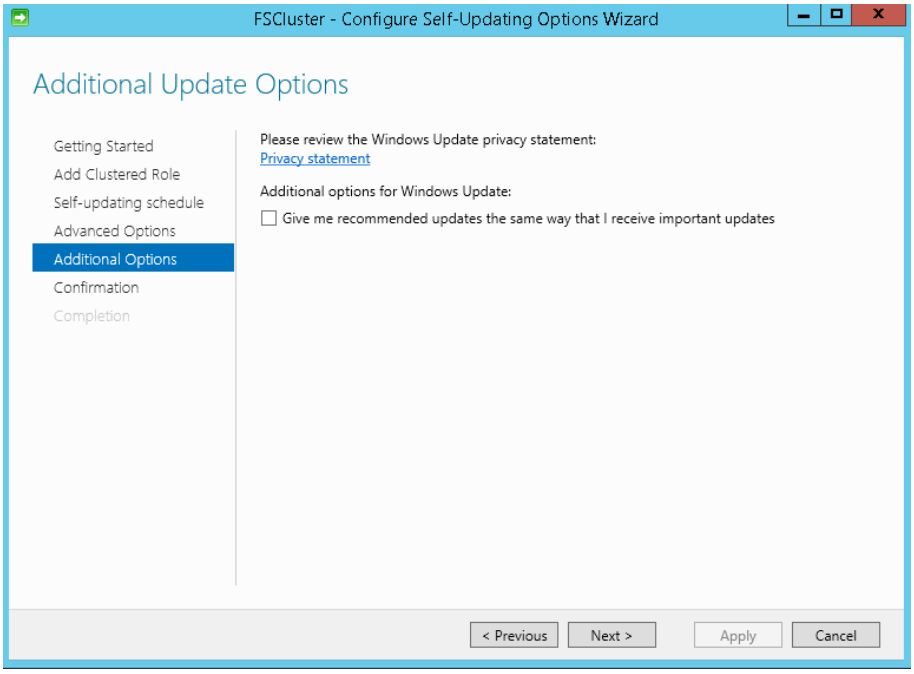

12. Cửa sổ **Specify self-updating schedule**, chọn **Weekly**, bung ô **Time of day**, chọn **4:00 AM**, bung ô **Day of the week**, chọn **Sunday**, và chọn **Next**.



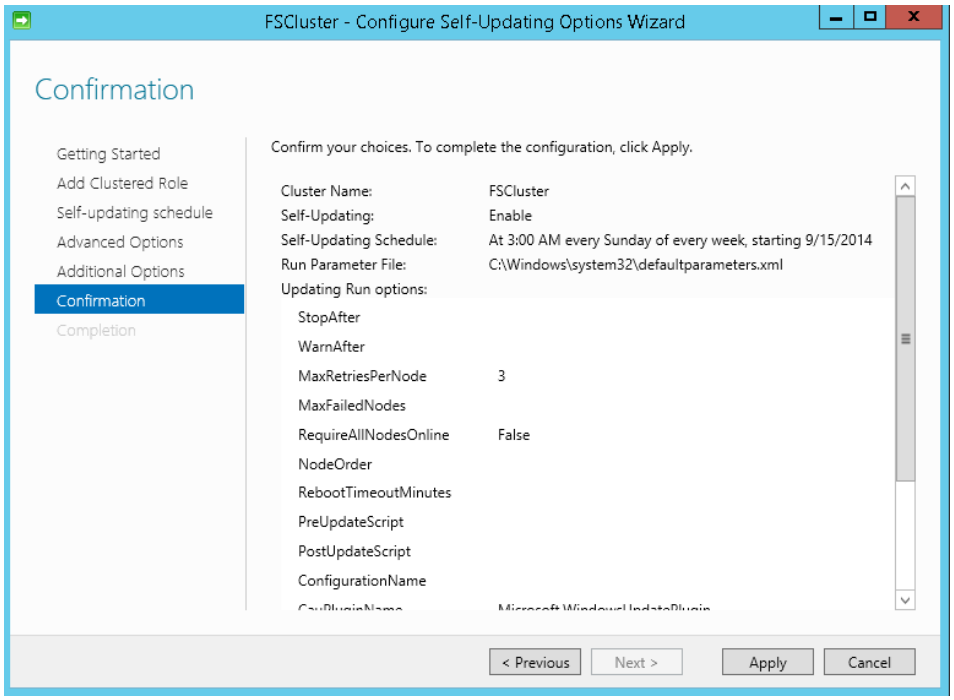
13. Cửa sổ **Advanced Options**, chọn **Next**.



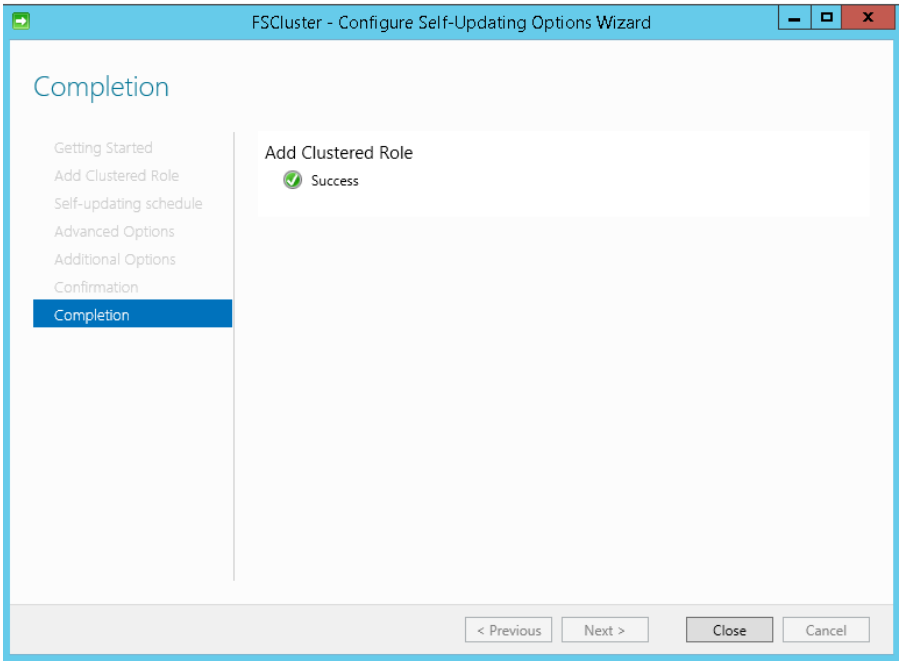

14. Cửa sổ **Additional Update Options**, chọn **Next**.



15. Cửa sổ **Confirmation**, chọn **Apply**.




16. Cửa sổ **Completion**, kiểm tra thông báo **Success**, chọn **Close**.



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công chức năng Cluster-Aware Updating (CAU).**

## Bài tập 4: Triển khai khả năng sẵn sàng cao cho hệ thống ảo hóa.

Tiếp theo, bạn sẽ cấu hình Failover Clustering để hỗ trợ khả năng sẵn sàng cao cho máy ảo có sẵn.

❖ **Bài thực hành bao gồm các bước:**

1. Chuyển file .vhd vào nơi lưu trữ
2. Cấu hình máy Hyper-V sử dụng Scale-Out File Server cluster
3. Cấu hình cho máy ảo hỗ trợ sẵn sàng cao
4. Thực hiện Live Migration
5. Kiểm tra khả năng sẵn sàng cao trong trường hợp gặp sự cố

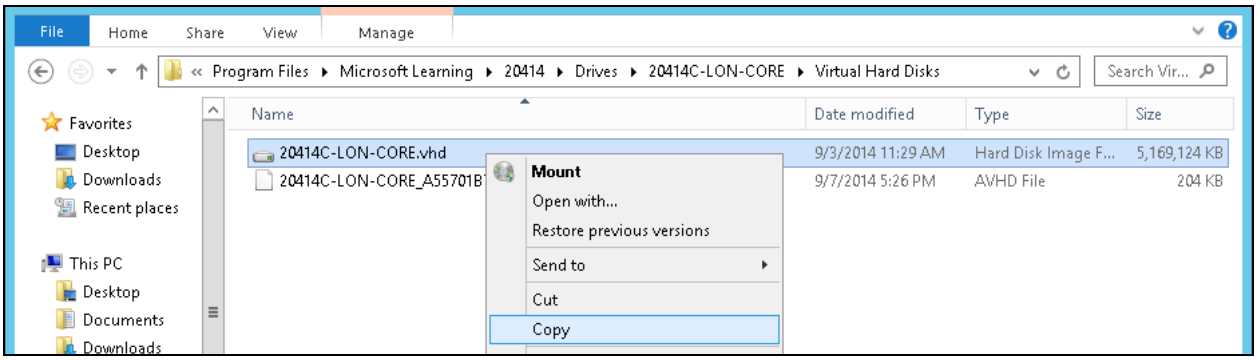
❖ **Thực hiện:**

### Bước 1. Chuyển file .vhd vào nơi lưu trữ

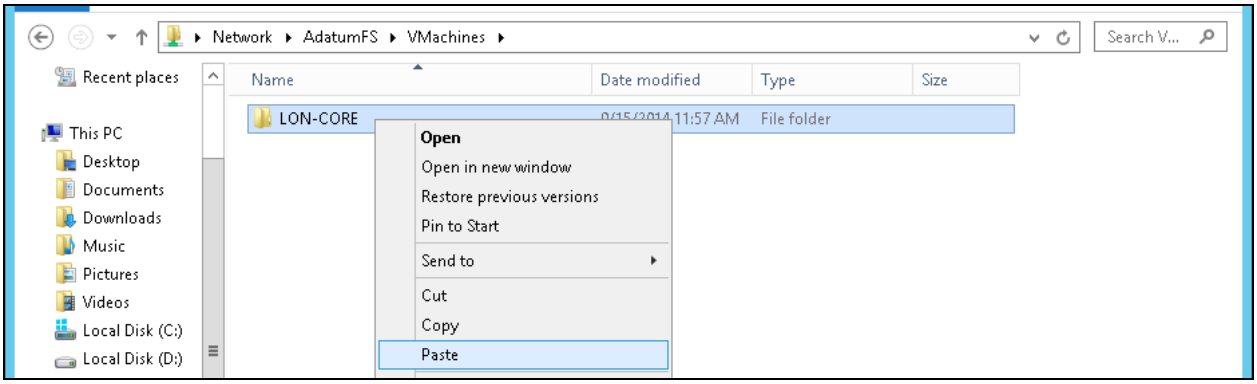
1. Trên máy **LON-HOST1** (máy thật).

2. Mở **File Explorer,** vào đường dẫn **E:\Program Files\Microsoft Learning\20414\Drives\20414C-LON-CORE\Virtual Hard Disks**. (Lưu ý: E: là ổ đĩa chứa máy ảo, ký tự ổ đĩa có thể khác nhau dựa vào cấu hình của mỗi máy.

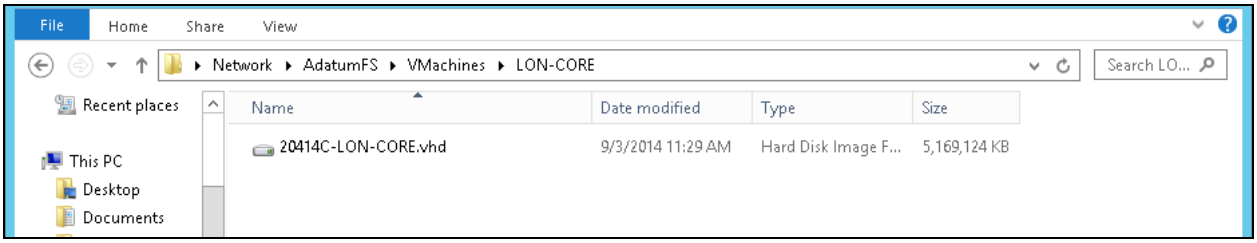
3. Chuột phải lên file **20414C-LON-CORE.vhd**, chọn **Copy**.



4. Trong **File Explorer**, truy cập **\\AdatumFS\VMachines**, tạo folder mới đặt tên **LON-CORE**, chuột phải folder **LON-CORE**, chọn **Paste**.

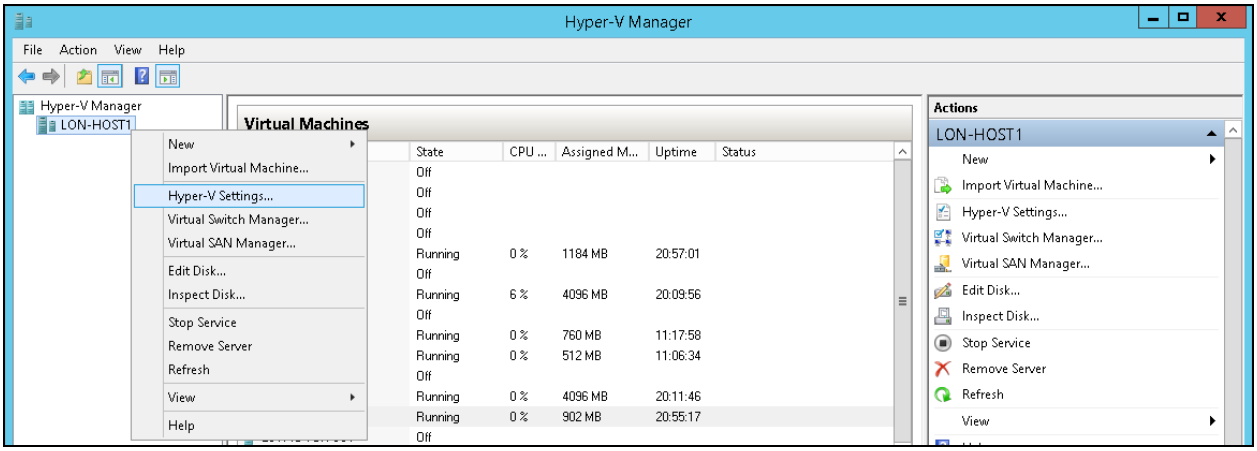



5. Chờ một vài phút cho đến khi chép file VHD thành công. Kiểm tra trong folder **LON-CORE** có file**20414C-LON-CORE.vhd**

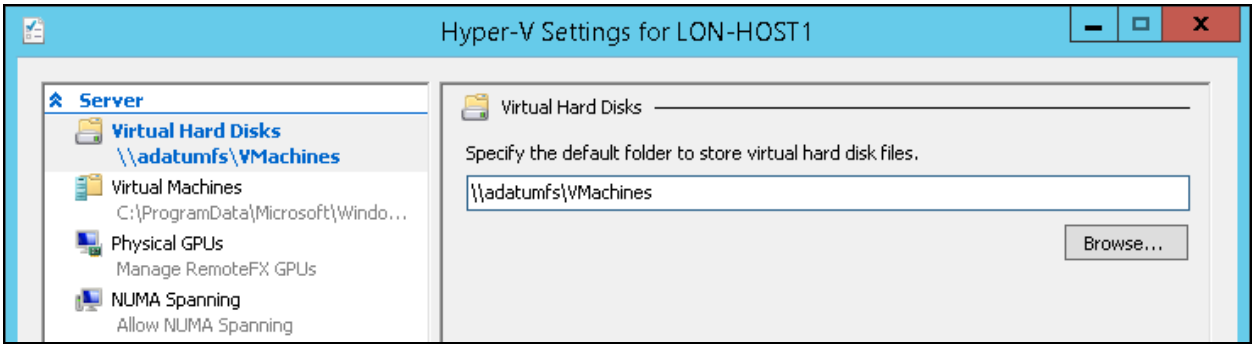



## Bước 2. Cấu hình máy Hyper-V sử dụng Scale-Out File Server cluster

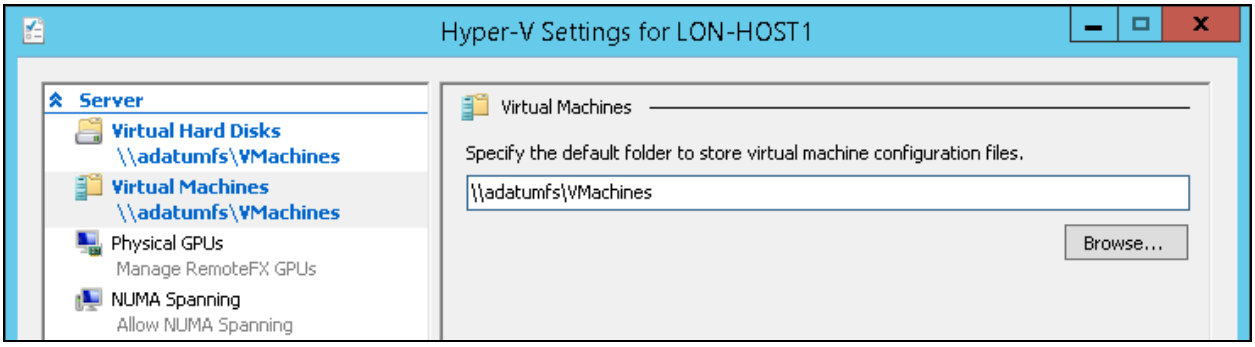
1. Trên máy **LON-HOST1** (máy thật), mở **Hyper-V Manager**, chuột phải **LON-HOST1,** chọn **Hyper-V Settings**.



2. Cửa sổ **Hyper-V Settings for LON-HOST1**, chọn **Virtual Hard Disks**, sửa đường dẫn thành **\\adatumfs\VMachines**




3. Chọn **Virtual Machines**, sửa đường dẫn thành **\\adatumfs\VMachines,** chọn **OK**.

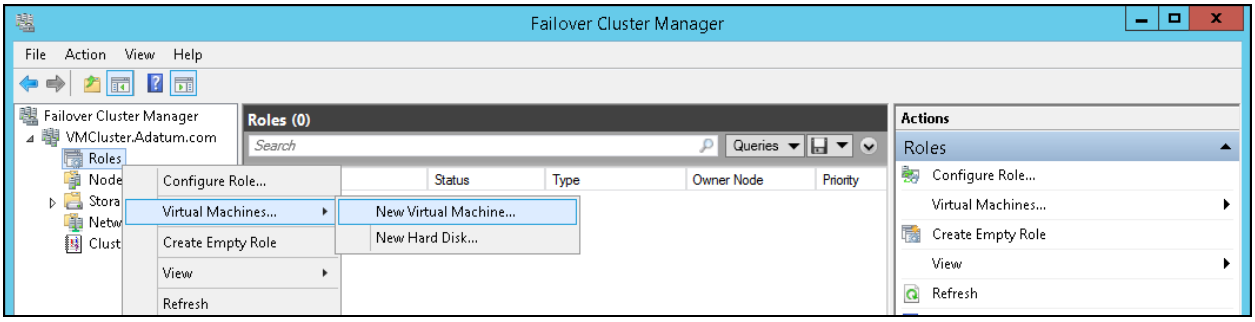



4. Lặp lại từ bước 1 đến 3 cho máy **LON-HOST2** (máy thật).

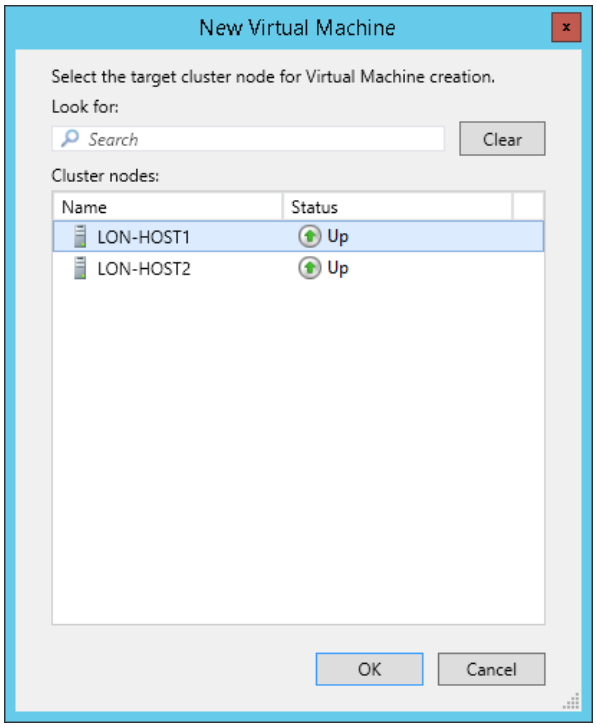
## Bước 3. Cấu hình cho máy ảo hỗ trợ sẵn sàng cao

1. Trên máy **LON-HOST1** (máy thật).

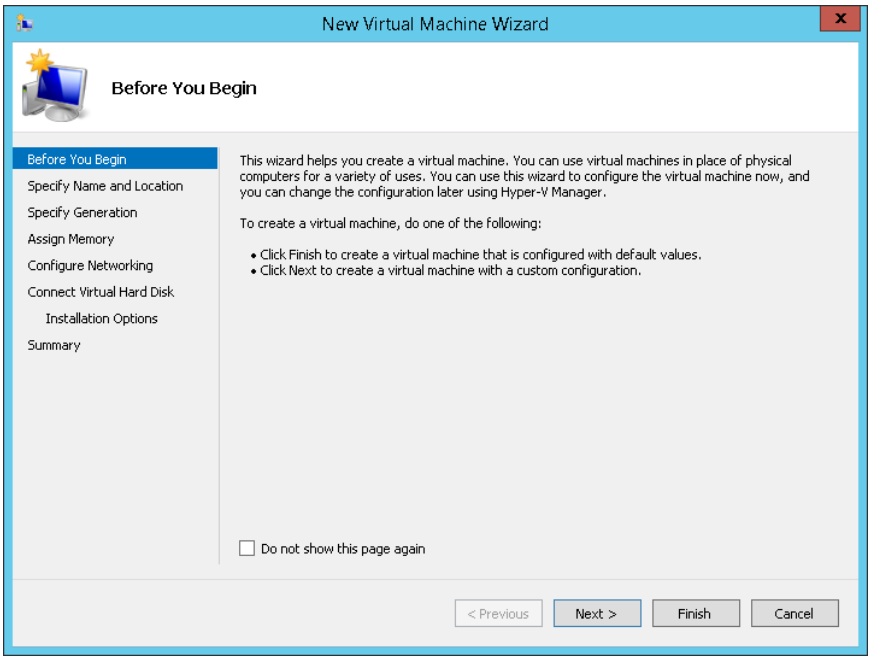
2. Mở **Failover Cluster Manager,** bung **VMCluster.Adatum.com**, chuột phải **Roles**, bung **Virtual Machines**, chọn **New Virtual Machine**.



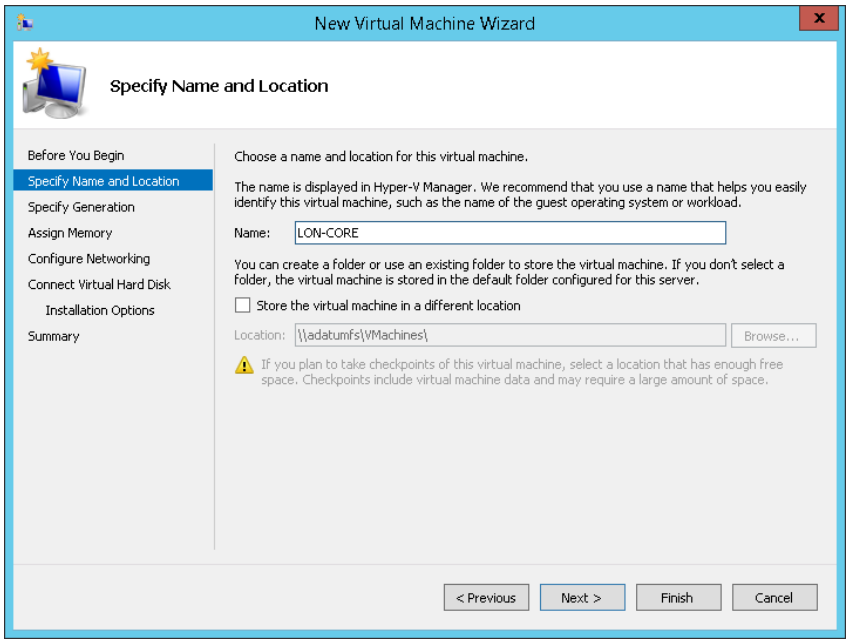
3. Hộp thoại **New Virtual Machine**, chọn **LON-HOST1**, và chọn **OK**.



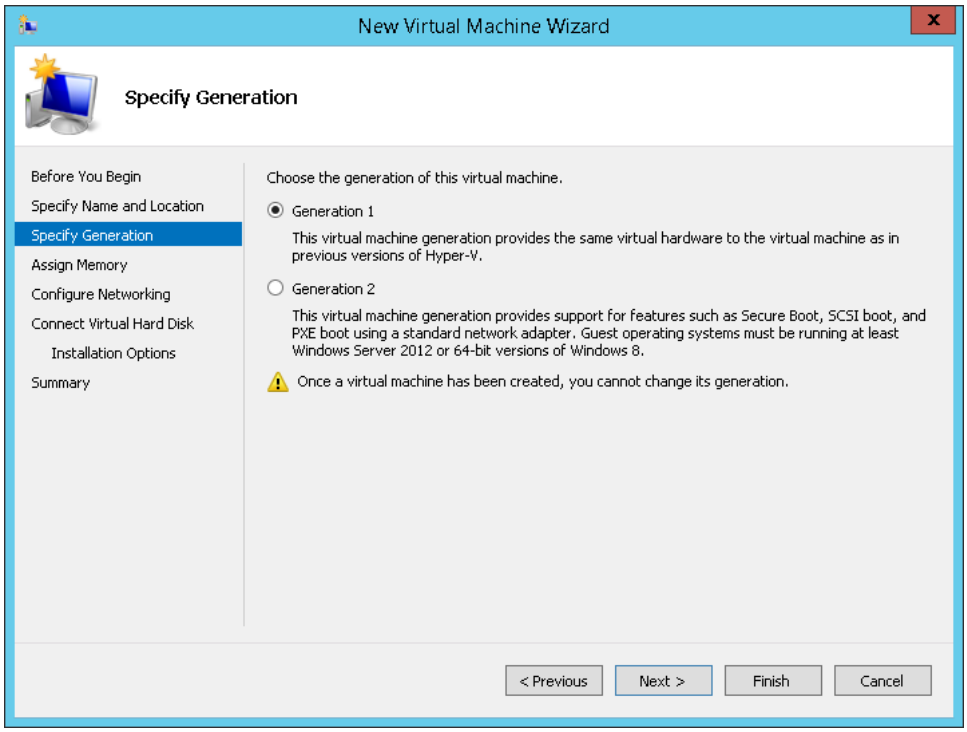

4. Cửa sổ **Before You Begin**, chọn **Next**.



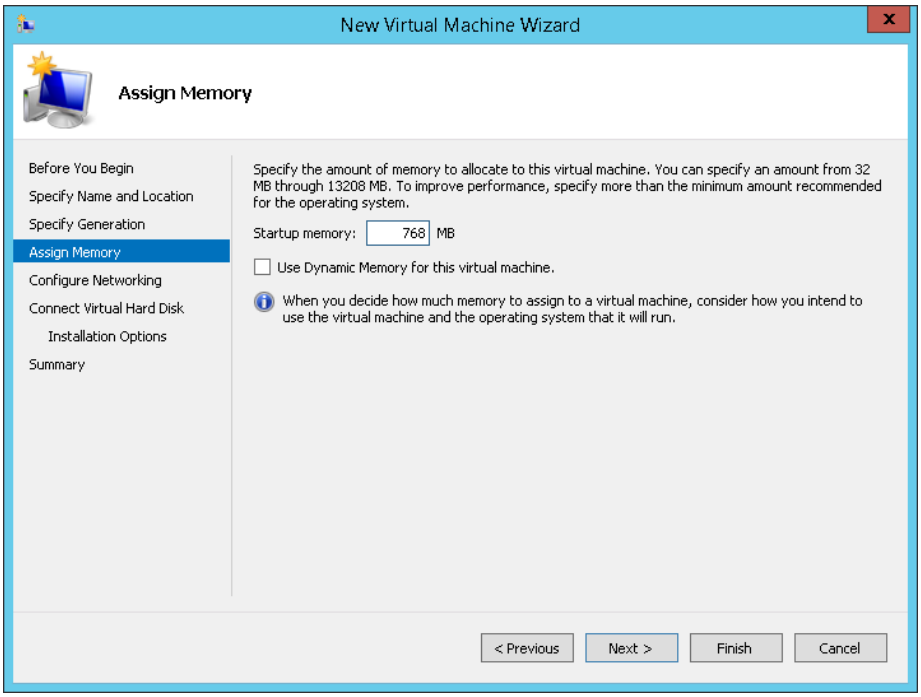
5. Cửa sổ **Specify Name and Location**, nhập **LON-CORE** vào ô **Name**, chọn **Next**.



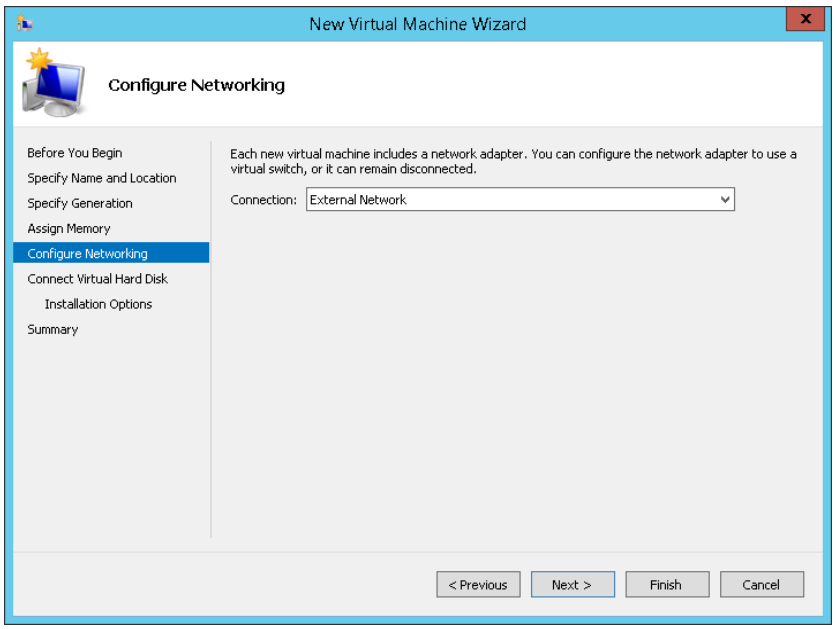

6. Cửa sổ **Specify Generation**, chọn **Generation 1**, và chọn **Next**.



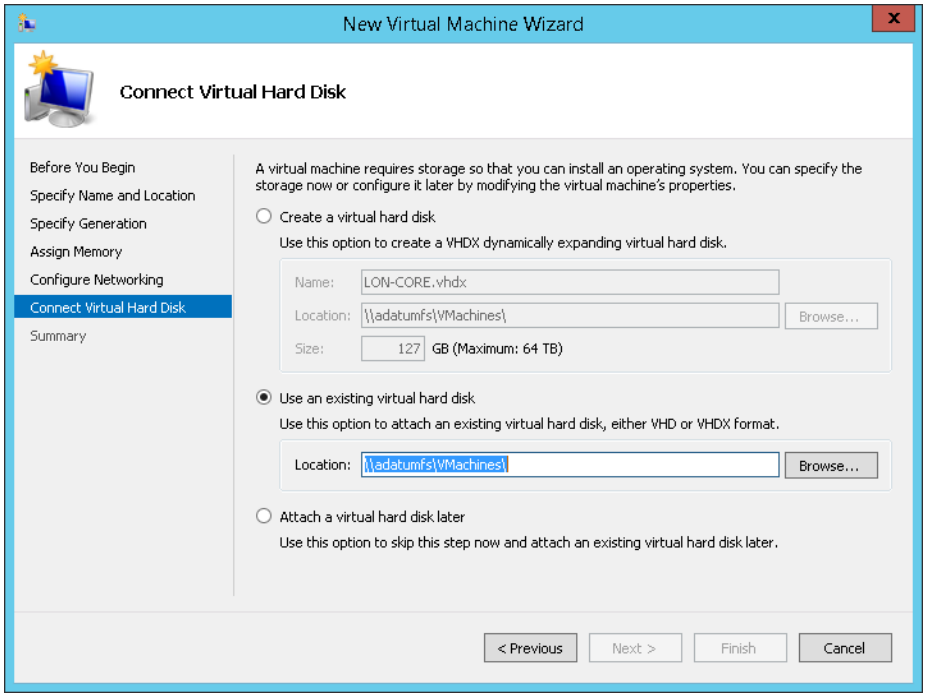
7. Cửa sổ **Assign Memory**, nhập **768** vào ô **Startup memory**, chọn **Next**.



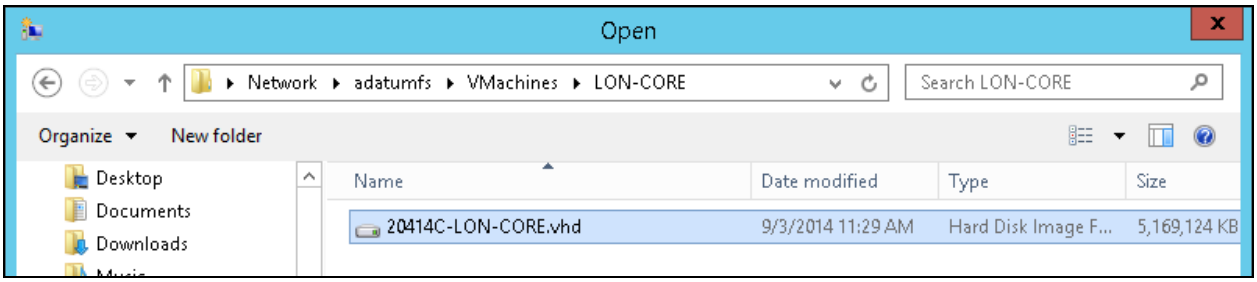

8. Cửa sổ **Configure Networking**, bung ô **Connection** chọn **External Network**, và chọn **Next**.



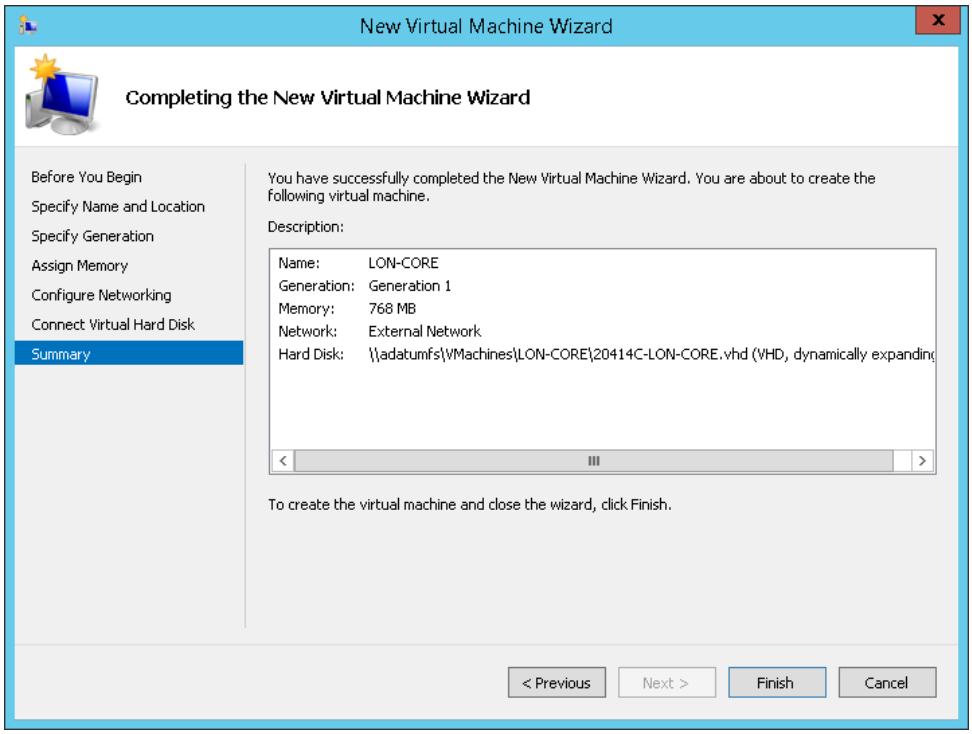
9. Cửa sổ **Connect Virtual Hard Disk**, chọn **Use an existing virtual hard disk**, chọn **Browse**.



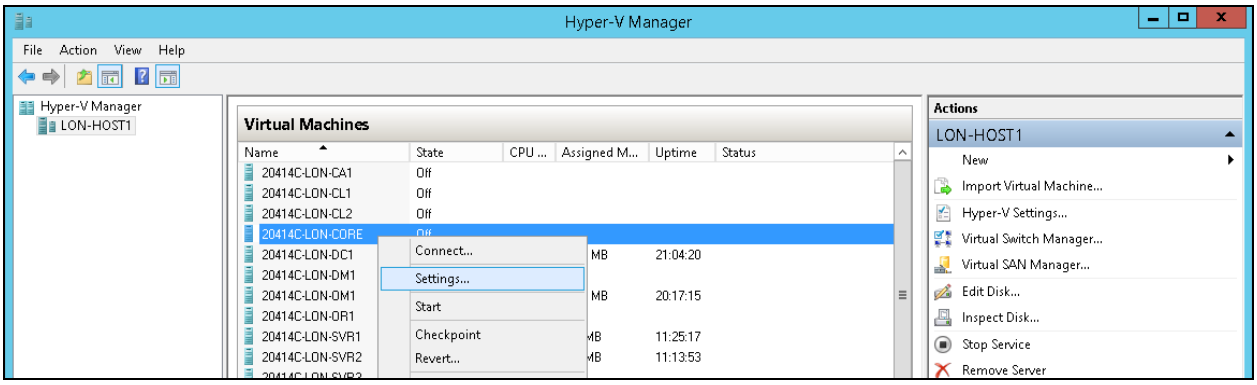

10. Hộp thoại **Open**, mở folder **LON-CORE**, chọn file **20414C-LON-CORE.vhd**, chọn **Open**, và chọn **Next**.



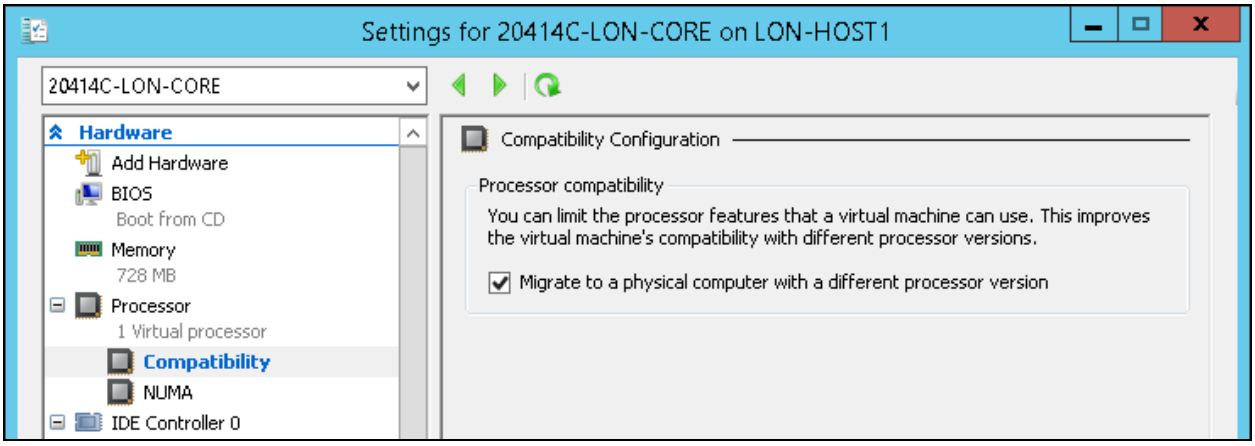
11. Cửa sổ **Completing the New Virtual Machine Wizard**, chọn **Finish** 2 lần



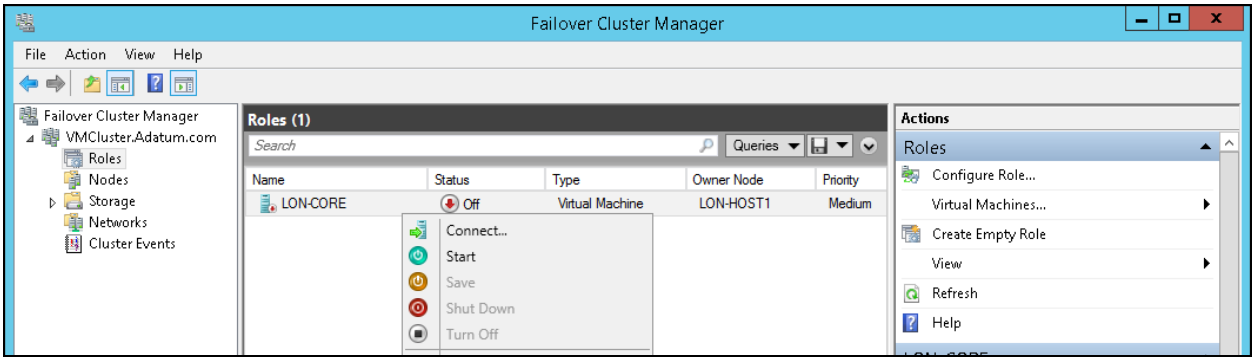

12. Trong cửa sổ **Hyper-V Manager**, chuột phải lên máy ảo **LON-CORE**, chọn **Settings**.



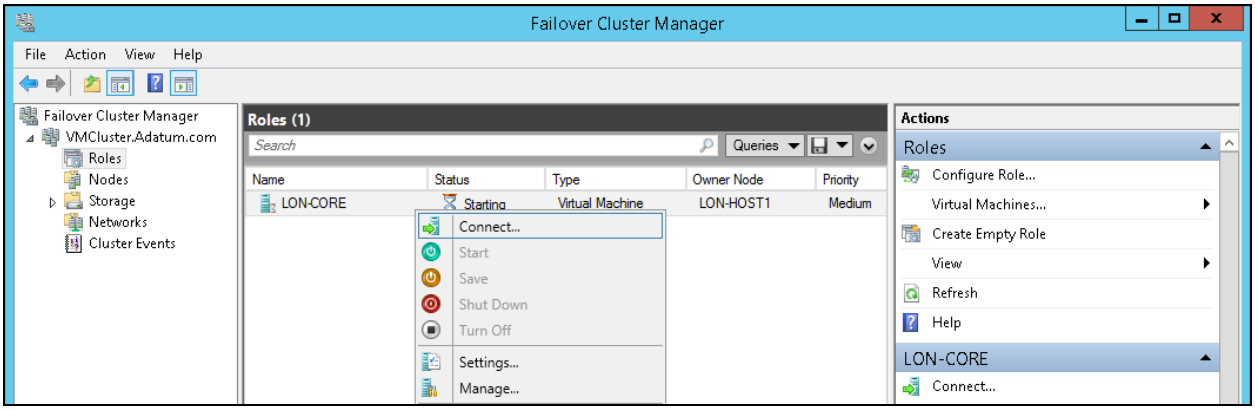
13. Cửa sổ **Settings for LON-CORE on LON-HOST1**, bung **Processor**, chọn **Compatibility**, đánh dấu chọn **Migrate to a physical computer with a different processor version**, và chọn **OK**.




14. Qua cửa sổ **Failover Cluster Manager**, chọn **Roles**, chuột phải lên máy ảo **LON-CORE**, chọn **Start**. Kiểm tra máy ảo khởi động thành công.



15. Chuột phải lên máy ảo **LON-CORE**, chọn **Connect**, sign in vào máy **LON-CORE** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

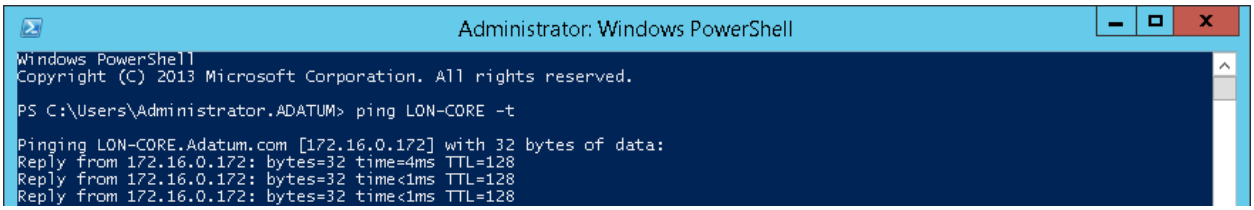



## Bước 4. Thực hiện Live Migration

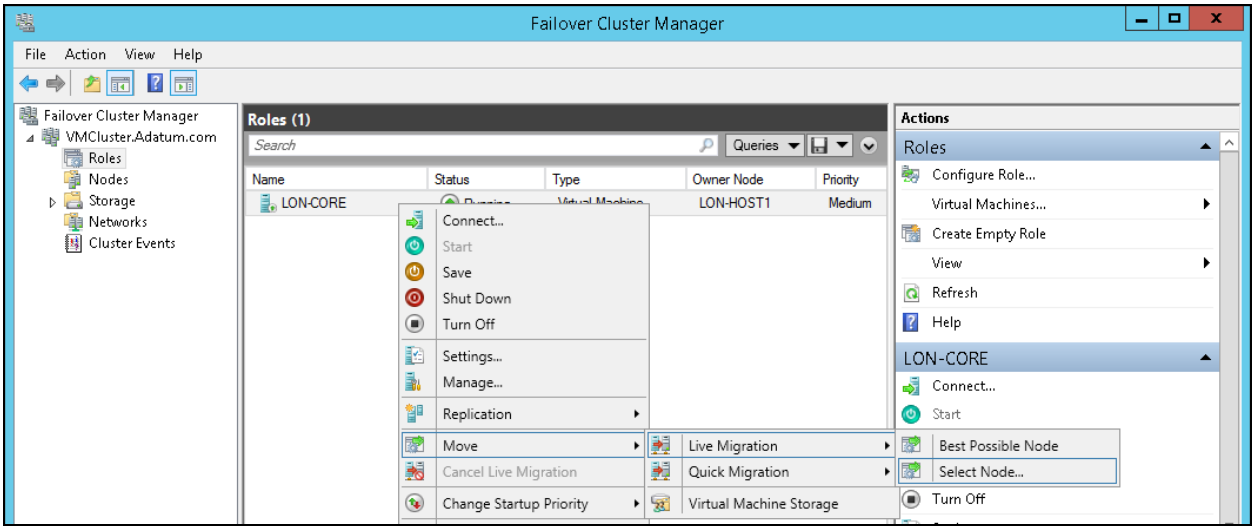
1. Trên máy **LON-HOST2**.

2. Mở **Windows PowerShell**, gõ lệnh:**ping lon-core –t**

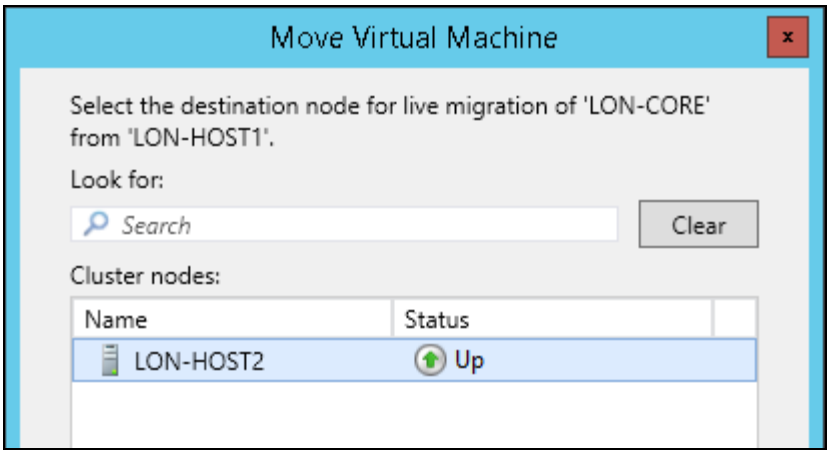
Kiểm tra ping máy LON-CORE thành công.



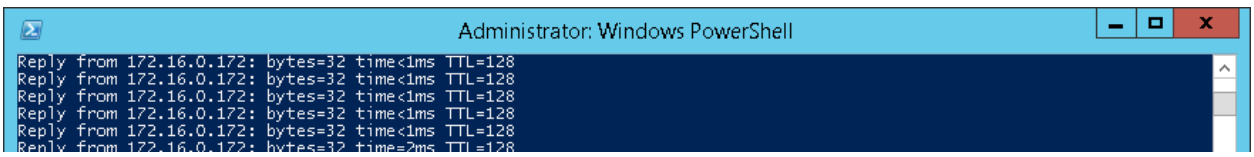
3. Mở **Failover Cluster Manager**, bung **VMCluster.Adatum.com**, chọn **Roles**, chuột phải máy ảo **20414C-LON-CORE**, bung **Move**, chọn **Live Migration**, chọn **Select Node**.




4. Hộp thoại **Move Virtual Machine**, chọn **LON-HOST2**, và chọn **OK**.



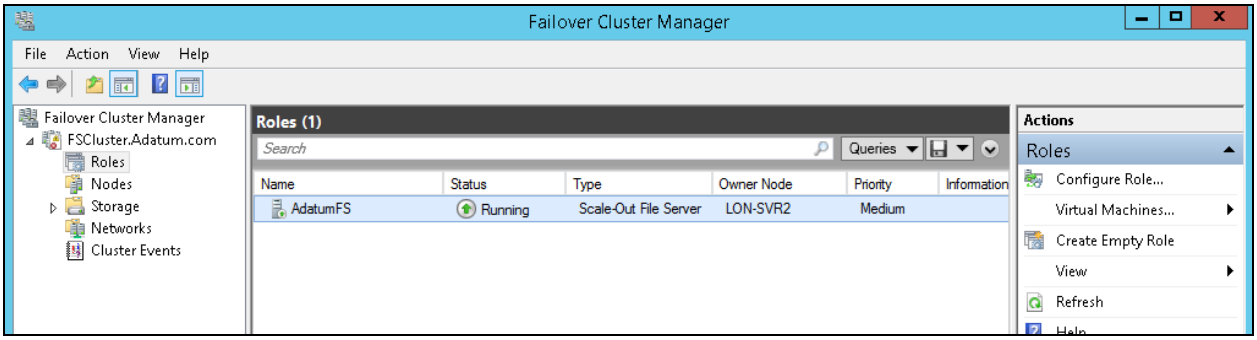

5. Quay lại cửa sổ **Windows PowerShell**, kiểm tra có thể rớt 1 đến 2 gói tin.



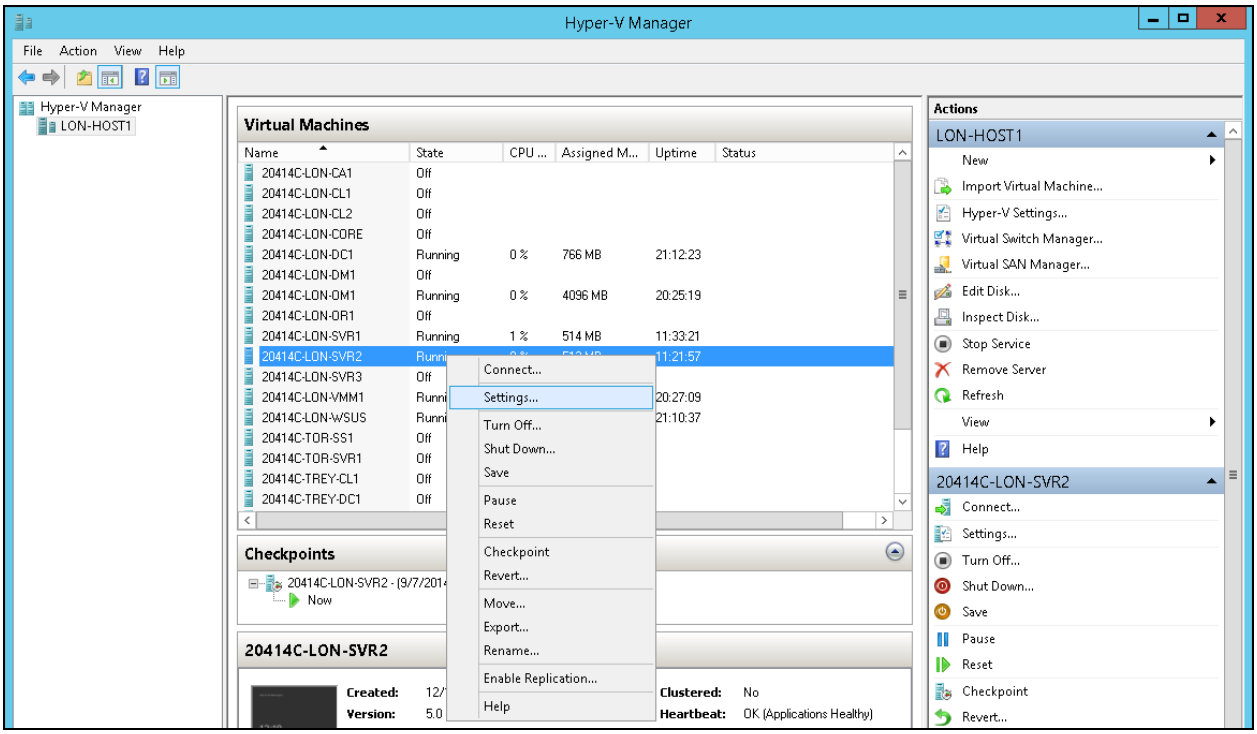

## Bước 5. Kiểm tra khả năng sẵn sàng cao trong trường hợp gặp sự cố

1. Trên máy **LON-SVR1**.

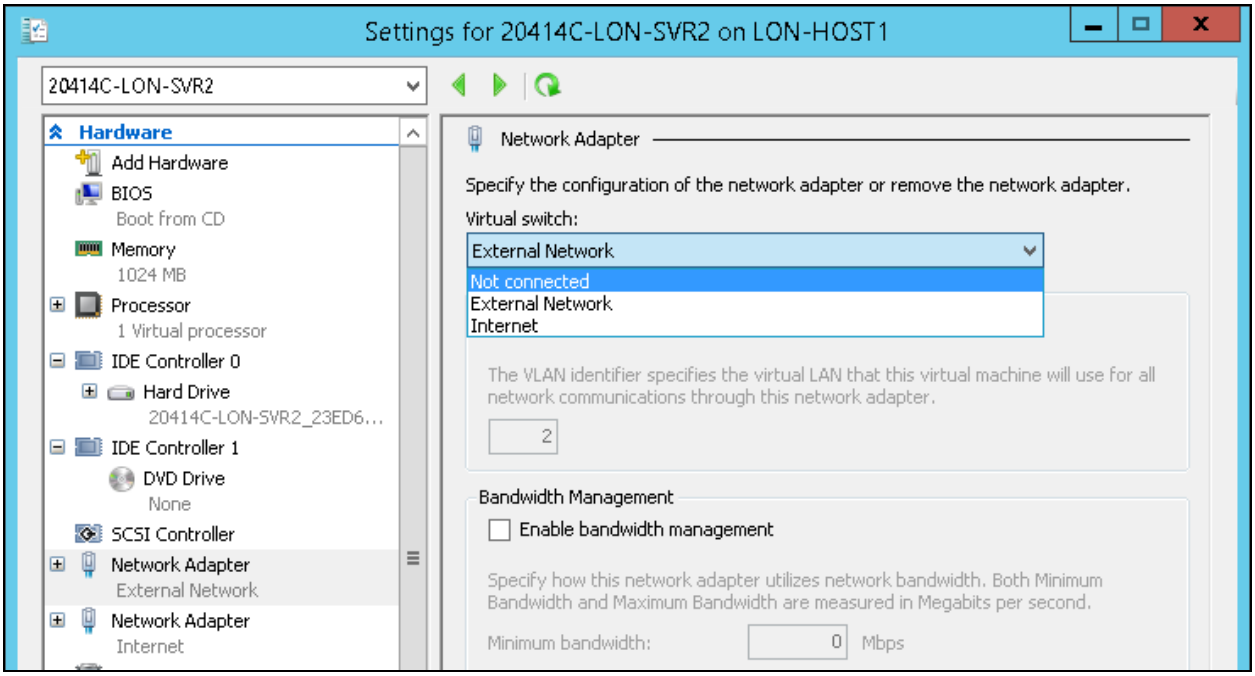
2. Mở **Failover Cluster Manager,** bung **FSCluster.Adatum.com**, chọn **Roles**. Kiểm tra **AdatumFS** đang có trạng thái **Running**, cột **Owner Node** đang là **LON-SVR2**.



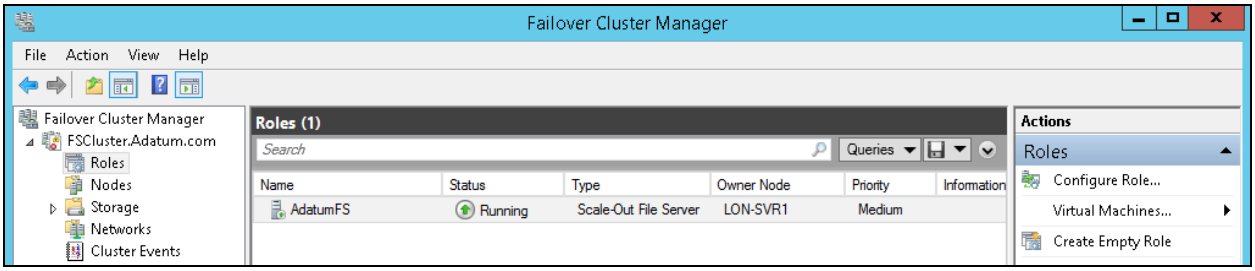

3. Qua máy **LON-HOST1**(Máy thật), mở **Hyper-V Manager**, chuột phải máy ảo **LON-SVR2**, chọn **Settings**.



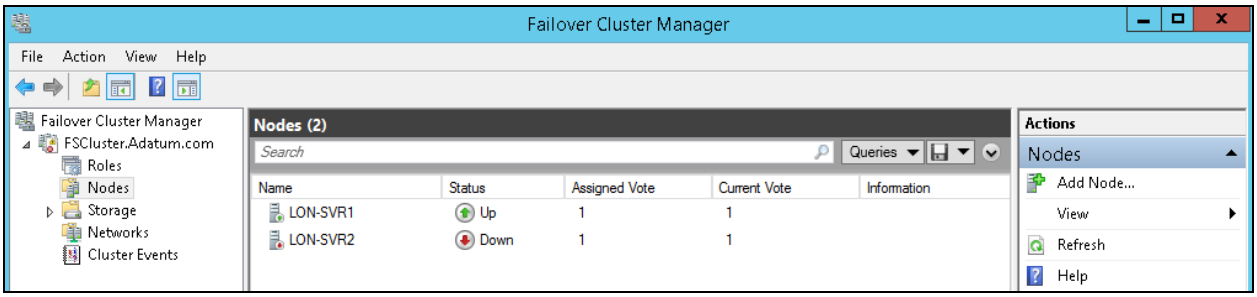
4. Cửa sổ **Setting**, chọn **Network Adapter** (External Network), bung ô **Virtual Switch**, chọn **Not Connected**, và chọn **OK**.



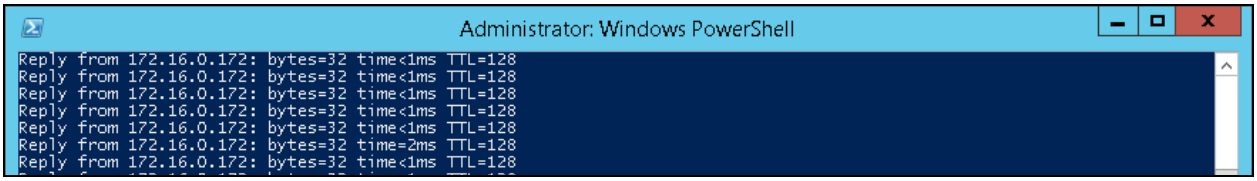

5. Qua máy **LON-SVR1,** mở **Failover Cluster Manager, chọn Roles.** Refesh lại giao diện. Kiểm tra **AdatumFS** đang có trạng thái **Running**, và cột **Owner Node** chuyển thành **LON-SVR1**.



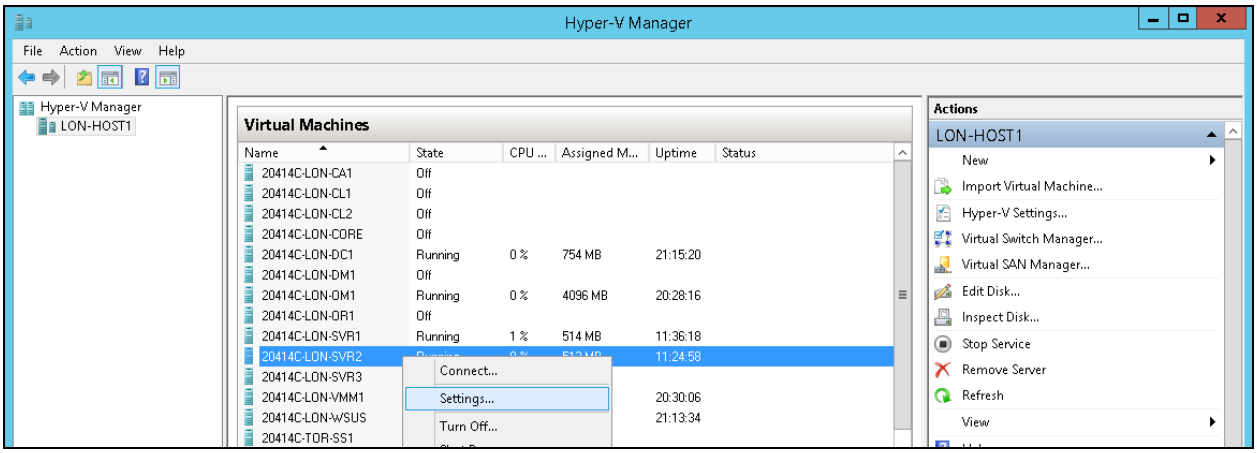
6. Qua mục **Nodes**, kiểm tra **LON-SVR2** đang có trạng thái là **Down**.



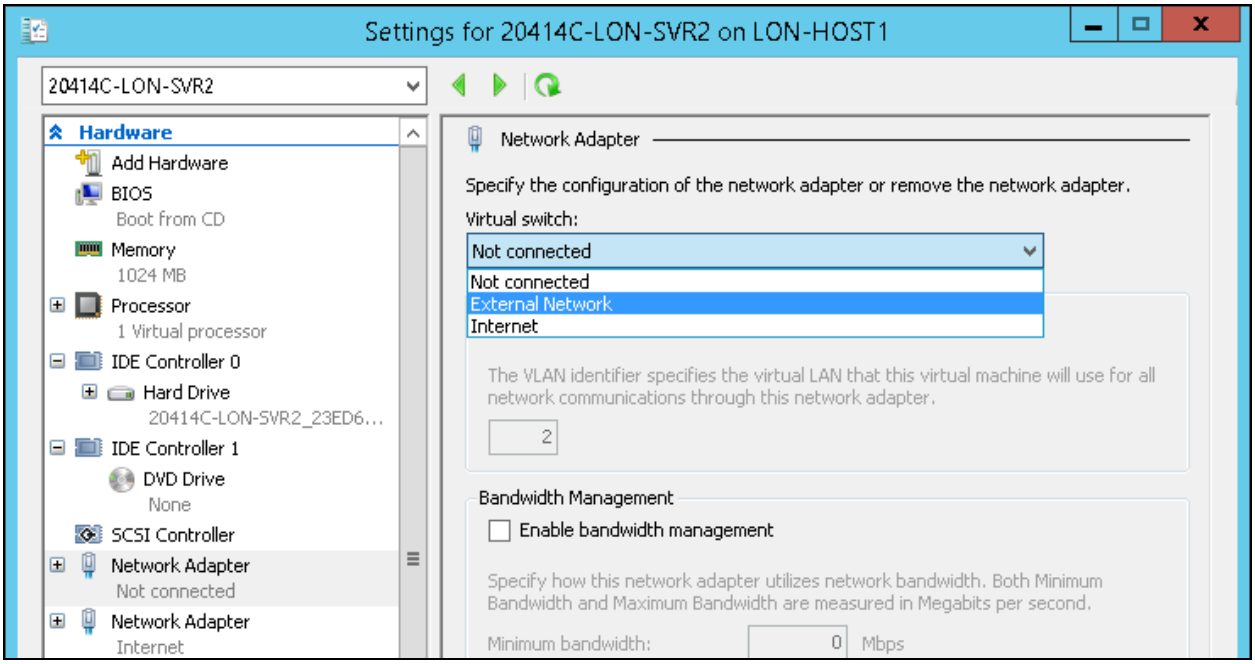

7. Qua máy **LON-HOST2**, trong **Windows PowerShell,** kiểm tra vẫn ping máy **LON-CORE** thành công.



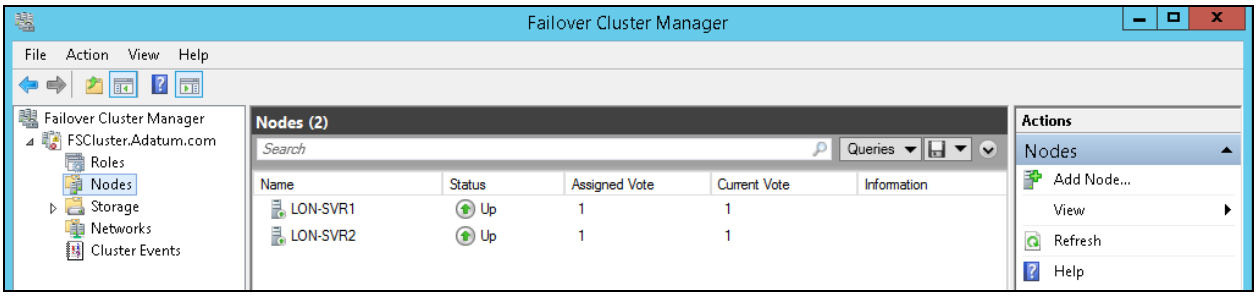

8. Qua máy **LON-HOST1**, mở **Hyper-V Manager**, chuột phải máy ảo **LON-SVR2,** chọn **Settings**.



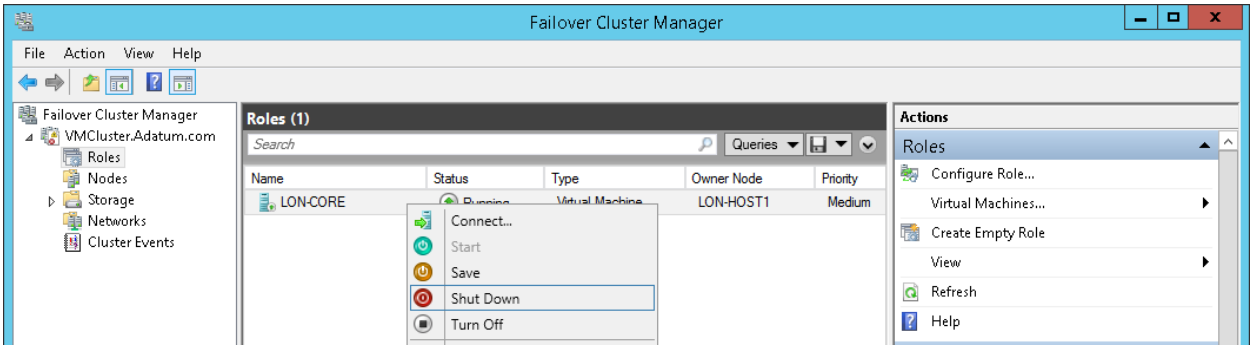
9. Cửa sổ **Settings,** chọn **Network Adapter** (Not connected), bung **Virtual switch**, chọn **External Network**, và chọn **OK**.




10. Qua máy LON-SVR1, mở **Failover Cluster Manager**, vào mục **Nodes,** Refesh lại giao diện. Kiểm tra 2 node đang có trạng thái **Up**.



11. Trong cửa sổ **Failover Cluster Manager**, qua mục **Roles**, chuột phải **LON-CORE**, chọn **Shut Down**.




12. Trên máy **LON-HOST1** và **LON-HOST2**, tắt **Failover Cluster Manager**.

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công khả năng chịu lỗi cho hê thống ảo hóa.**

**VI. Chuẩn bị cho bài tiếp theo:**

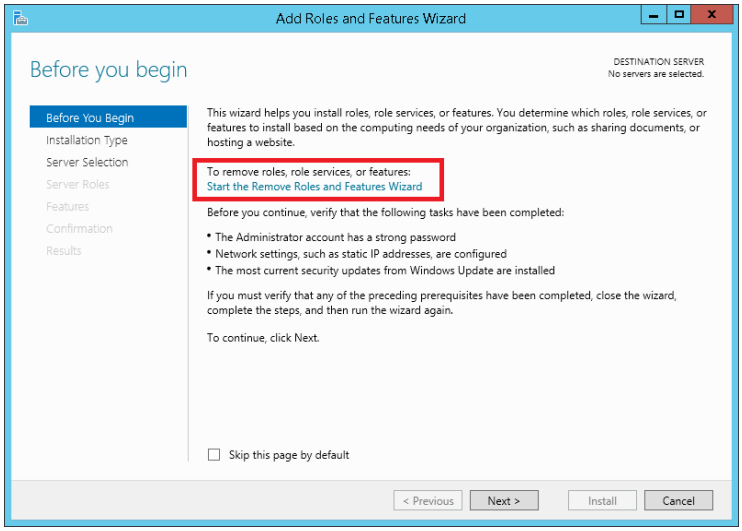
Sau khi hoàn thành bài thực hành, để phục hồi các máy ảo về trạng thái ban đầu, các bạn thực hiện các bước sau:

1. Trên máy **LON-HOST1**, mở công cụ **Hyper-V Manager.**
2. Nhấn chuột phải lên máy ảo **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho các máy ảo còn lại.

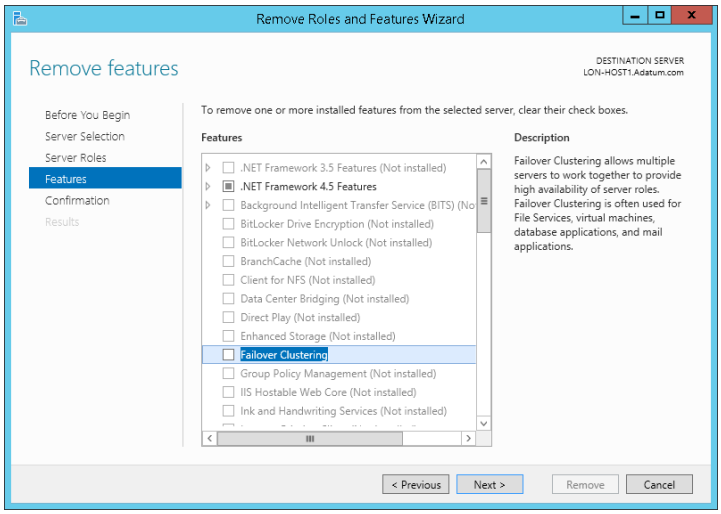
5. Gỡ bỏ feature **Failover Clustering** trên máy **LON-HOST1** và **LON-HOST2.** Thực hiện các bước sau cho cả 2 máy **LON-HOST1** và **LON-HOST2**:

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

b. Cửa sổ **Before you begin**, chọn **Start the Remove Roles and Features Wizard**, chọn **Next** 4 lần.




c. Cửa sổ **Remove features**, bỏ dấu chọn **Failover Clustering**, chọn **Next**, chọn **Remove**




d. Sau khi remove thành công, khởi động lại máy.

# Bài 8: Sao lưu và phục hồi dữ liệu bằng Sytem Center Data Protection Manager (DPM)

**I. Mục tiêu:**

- Cấu hình DPM.
- Sao lưu và phục hồi dữ liệu bằng DPM.

**II. Kịch bản:**

Là một phần của chiến lược ảo hóa, công ty A. Datum đã chuyển đổi hầu hết các server vật lý thành máy ảo và triển khai server ảo mới. A. Datum cần phát triển một chiến lược để sao lưu dữ liệu để đảm bảo an toàn cho các dữ liệu quan trọng trong hệ thống.

**III. Yêu cầu tổng quan:**

Bạn cần phải cấu hình DPM để sao lưu và phục hồi các dữ liệu quan trọng trong hệ thống.

**IV. Mô hình thực hành:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-SVR1**<br>**20414C-LON-DM1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy **20414C-LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên lại từ bước 1 đến 3 cho các máy ảo còn lại.

**VI. Thực hành:**

*Thời gian thực hành: 45 phút*

## Bài tập 1: Cấu hình DPM

A. Datum đã triển khai một DPM Server trong trung tâm dữ liệu ở London. Bạn phải cấu hình các thành phần cần thiết của DPM sao lưu và khôi phục dữ liệu.

❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Storage Pool trong DPM.
2. Triển khai DPM Protection Agents.
3. Cấu hình Protection Groups.

❖ **Thực hiện:**

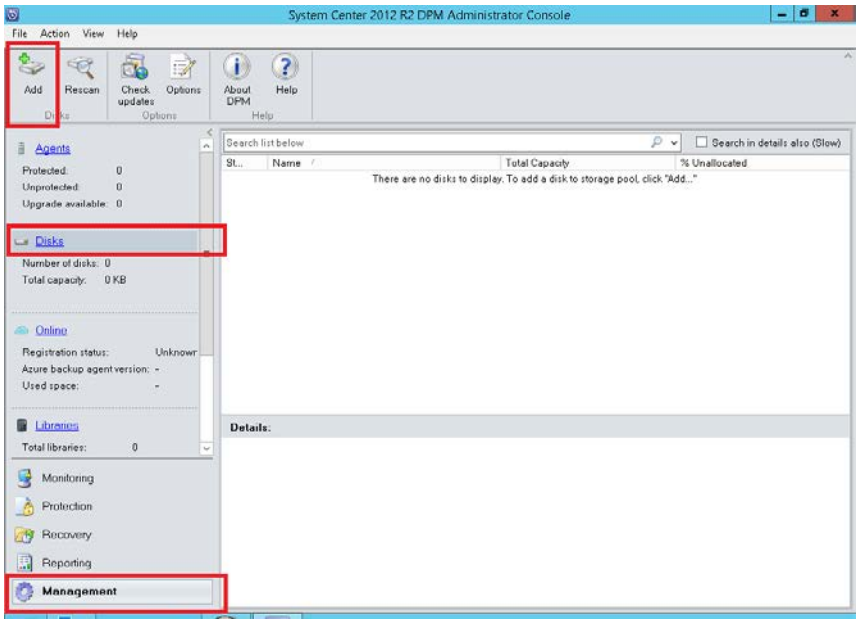
**Bước 1: Cấu hình Storage Pool trong DPM.**

1. Trên máy **LON-DM1**.

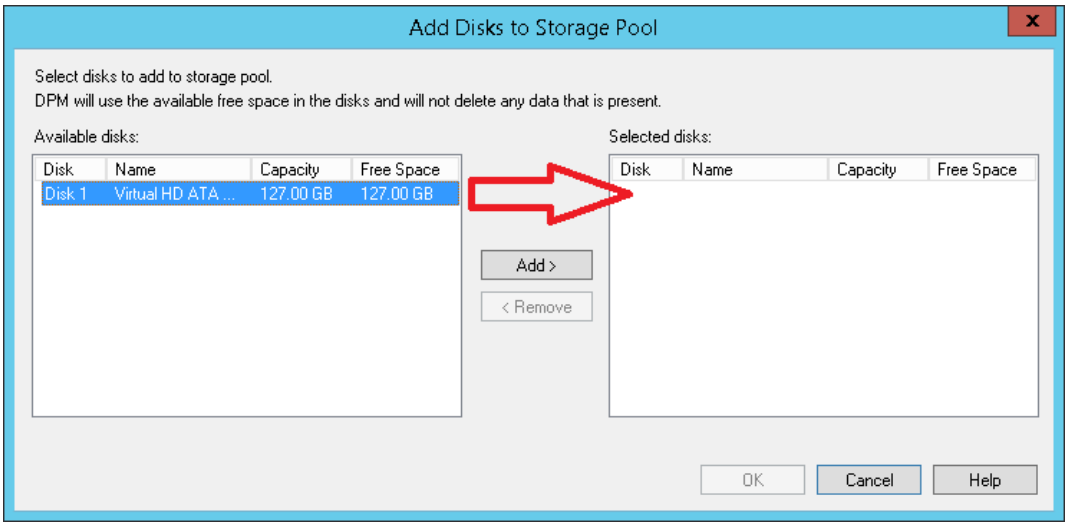
2. Trên desktop, mở **Microsoft System Center 2012 R2 Data Protection Manager**.



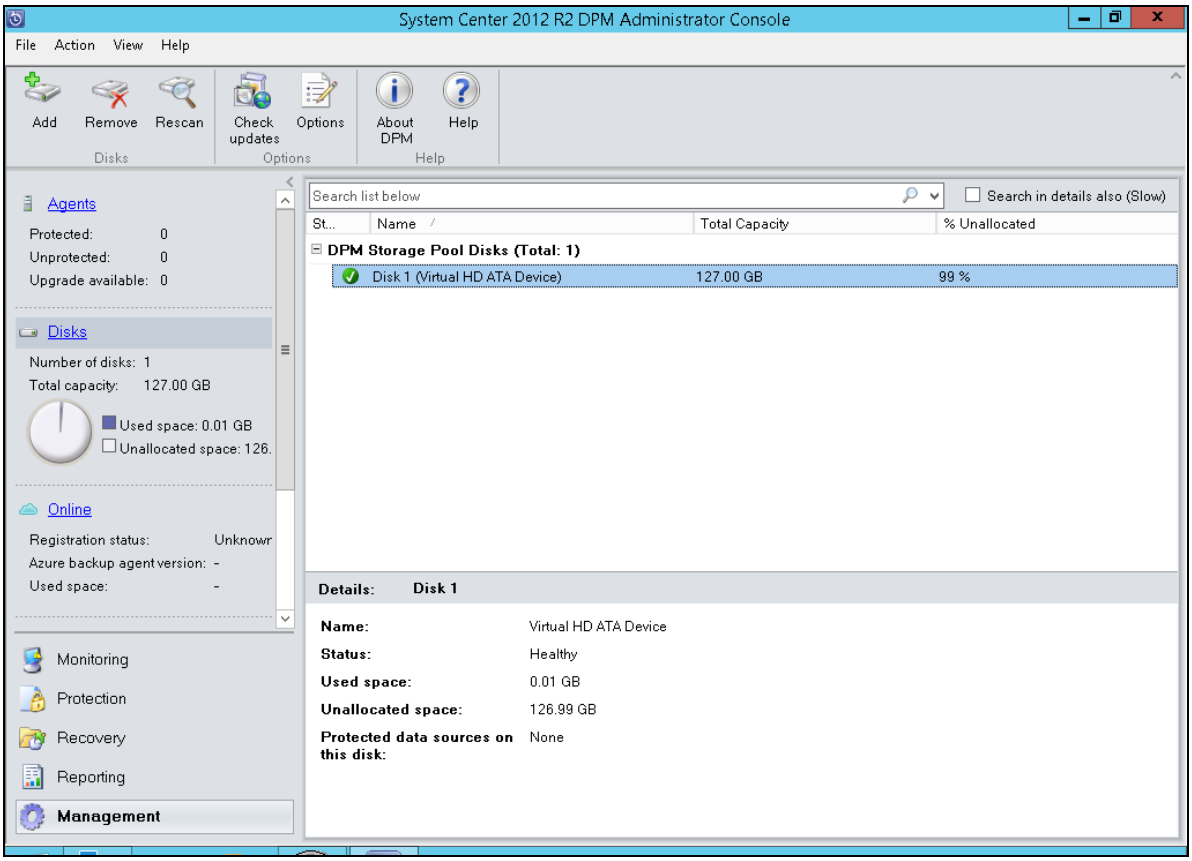

3. Trong cửa sổ **System Center 2012 R2 DPM Administrator Console**, chọn **Management**, chọn **Disks**, chọn **Add**.



4. Cửa sổ **Add Disks to Storage Pool**, chọn **Disk1**, chọn **Add**, và chọn **OK**.

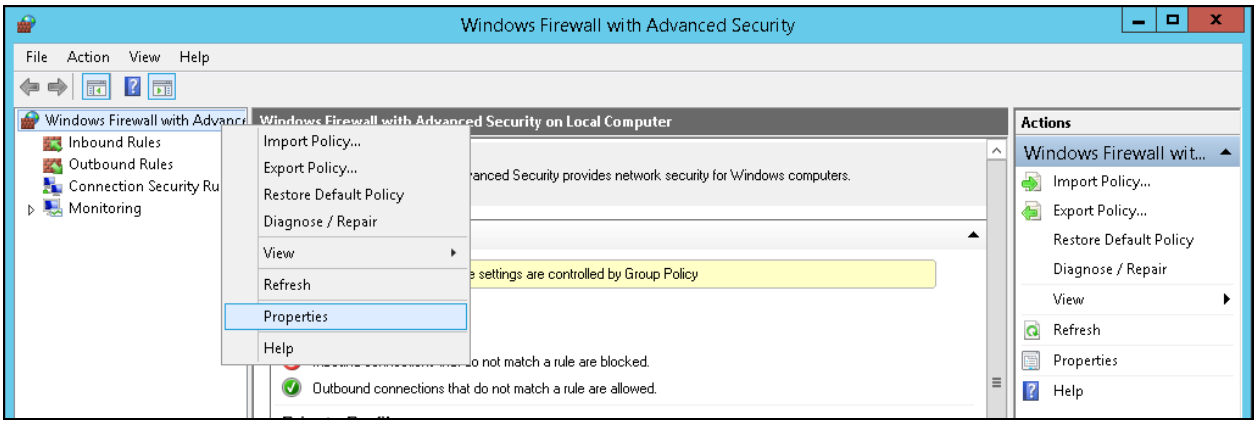



5. Kiểm tra trong mục **DPM Storage Pool** đã hiển thị **Disk1 (Virtual HD ATA Device)**.

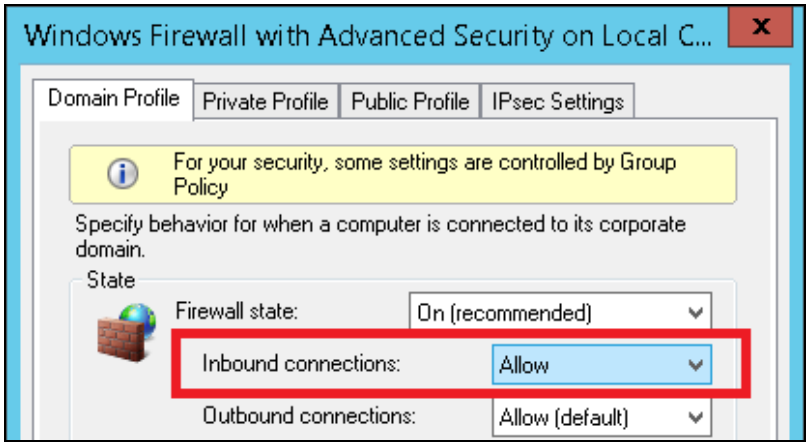


## Bước 2: Triển khai DPM Protection Agents.

1. Qua máy **LON-SVR1,** trong **Server Manager**, bung menu **Tools**, mở **Windows Firewall with Advanced Security**, **Windows Firewall with Advanced Security on Local Computer**, chọn **Properties**.

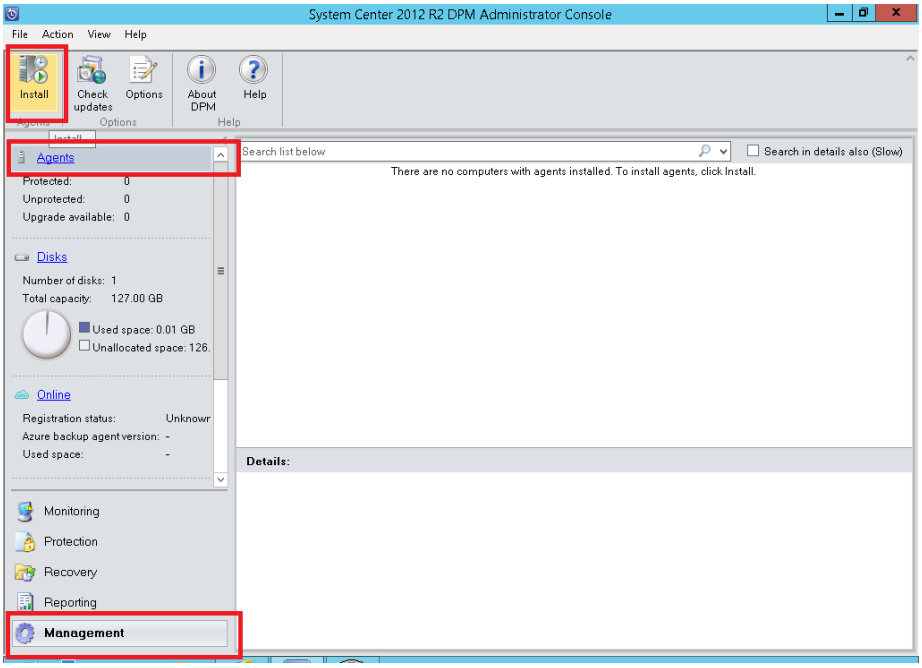



2. Trong hộp thoại **Windows Firewall with Advanced Security on Local Computer**, bung ô **Inbound connections**, chọn **Allow**, và chọn **OK**.

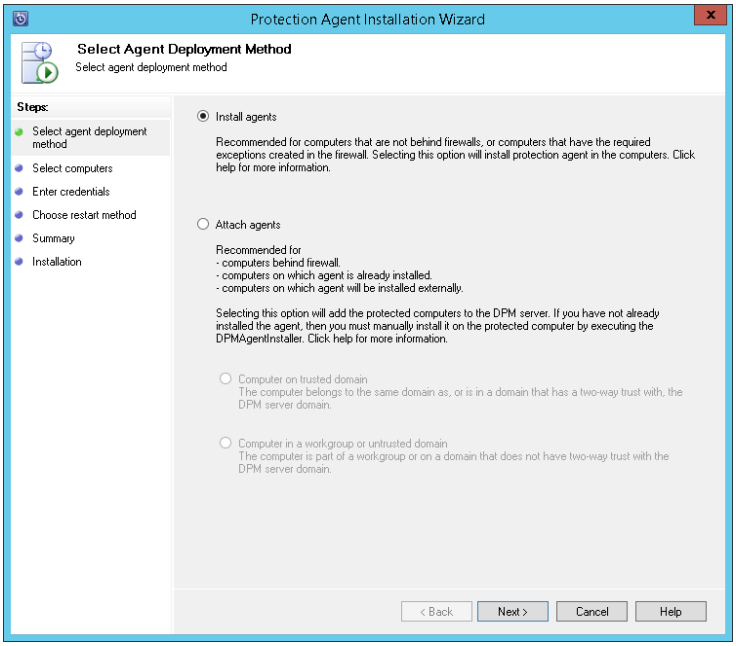



3. Tắt cửa sổ **Windows Firewall with Advanced Security**.

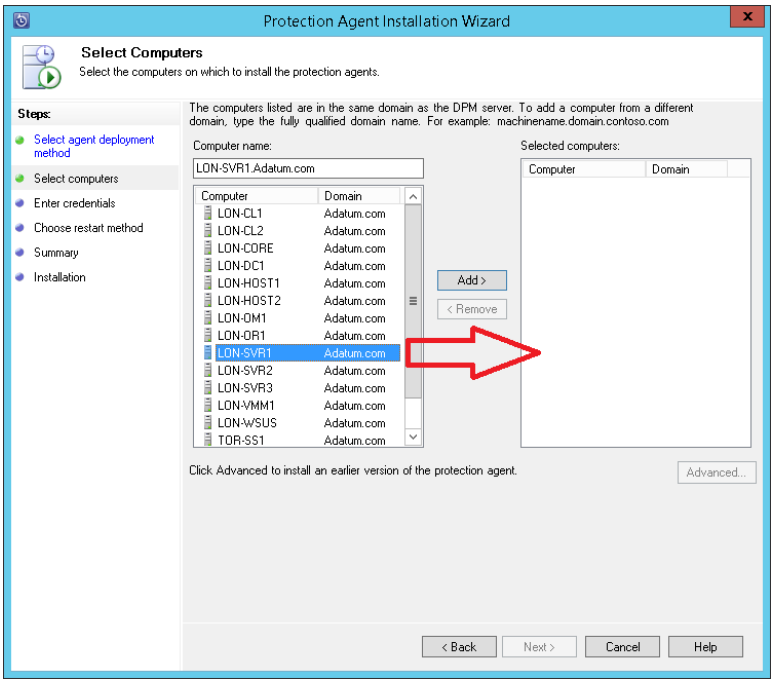
4. Qua máy **LON-DM1**, trong cửa sổ **DPM Administrator Console**, chọn **Management**, chọn **Agents**, chọn **Install**.



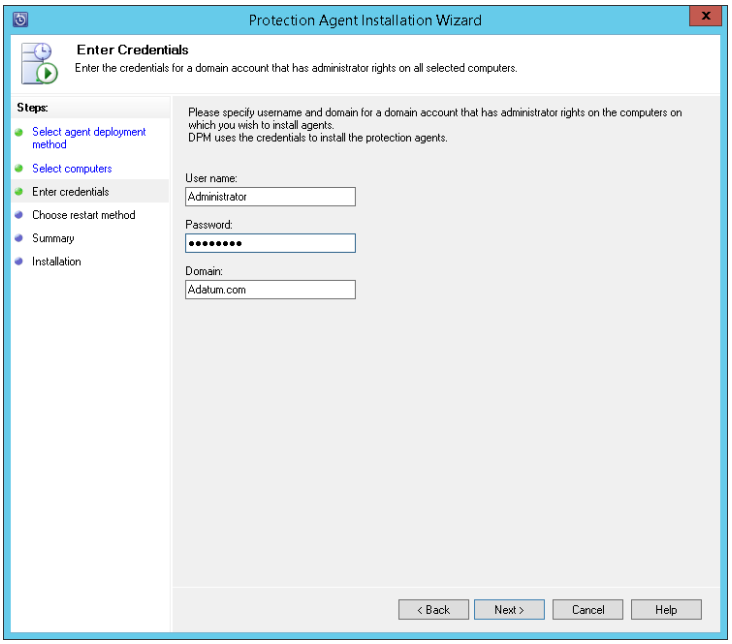

5. Cửa sổ **Select Agent Deployment Method**, chọn **Install agents**, và chọn **Next**.



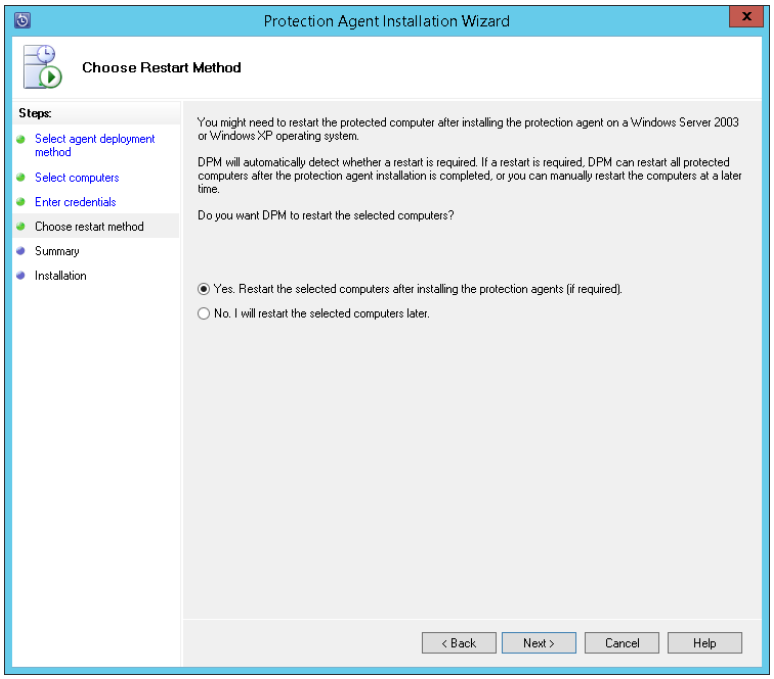
6. Cửa sổ **Select Computers**, chọn **LON-SVR1**, chọn **Add**, và chọn **Next**.



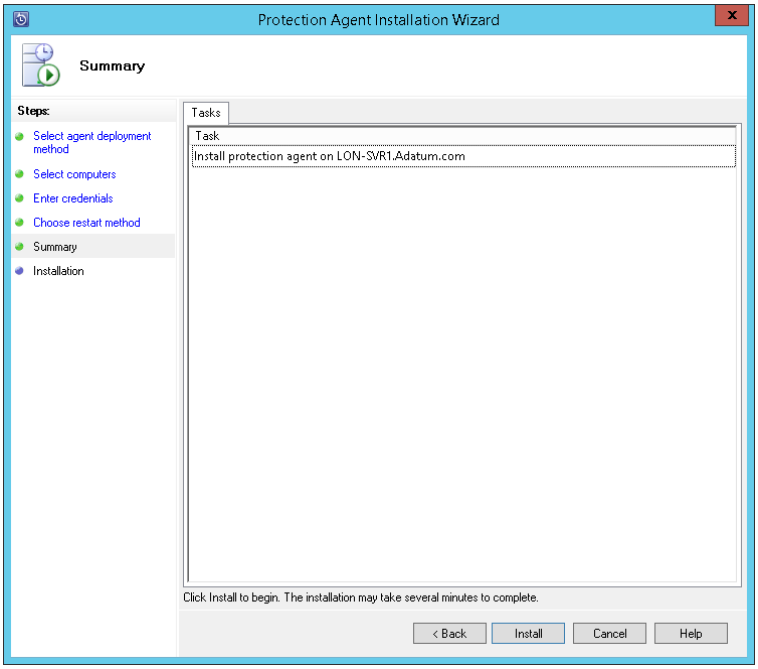

7. Cửa sổ **Enter Credentials**, trong ô **User name**, nhập **Administrator**, trong ô **Password**, nhập **Pa$$w0rd**, và chọn **Next**.



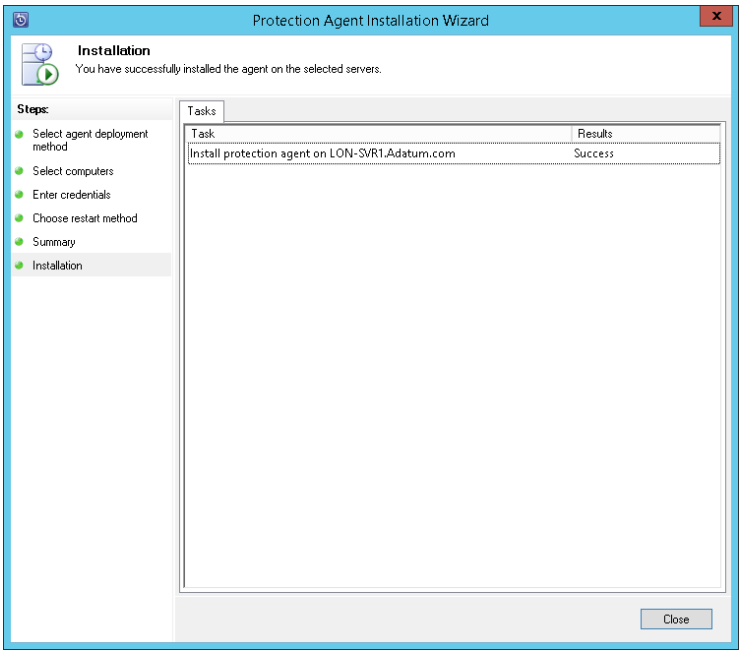
8. Cửa sổ **Choose Restart Method**, chọn **Yes**, và chọn **Next**.




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

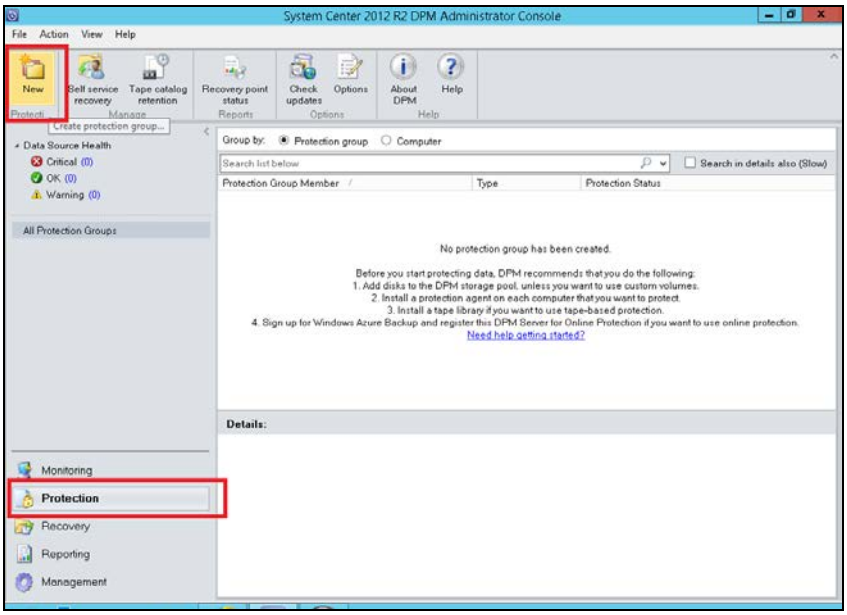


10. Sau khi cài đặt thành công, chọn **Close**

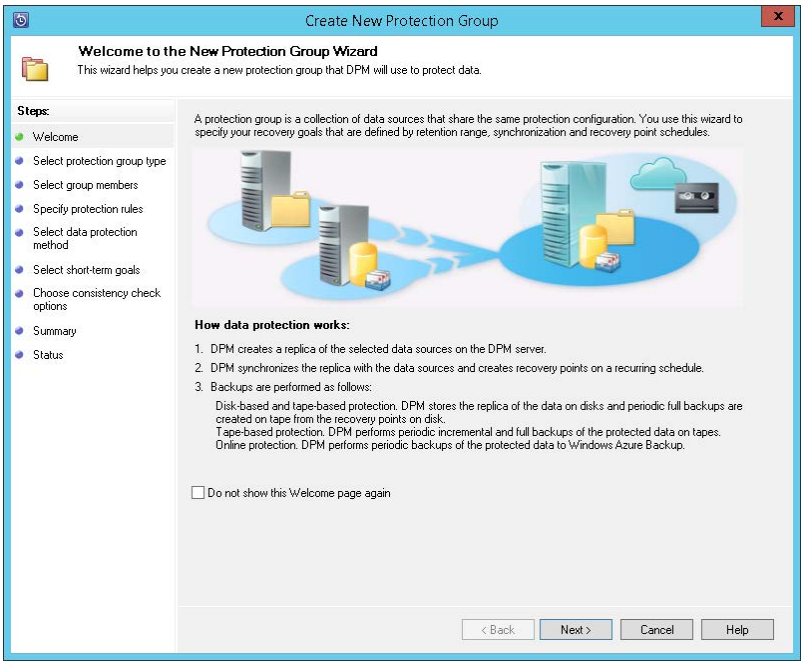



## Bước 3: Cấu hình Protection Groups.

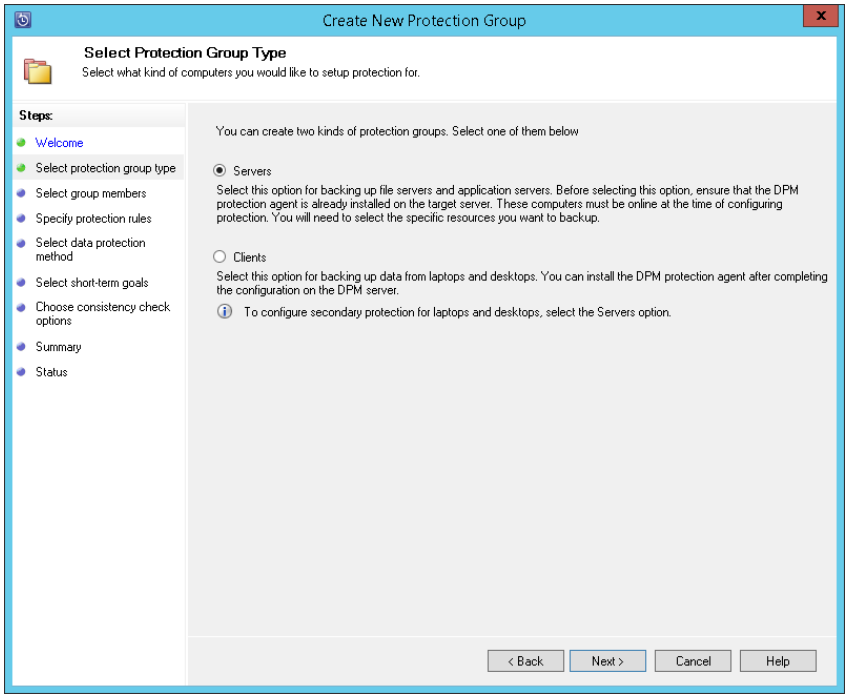
1. Trên máy **LON-DM1**, trong cửa sổ **DPM Administrator Console**, chọn **Protection,** chọn **New**.



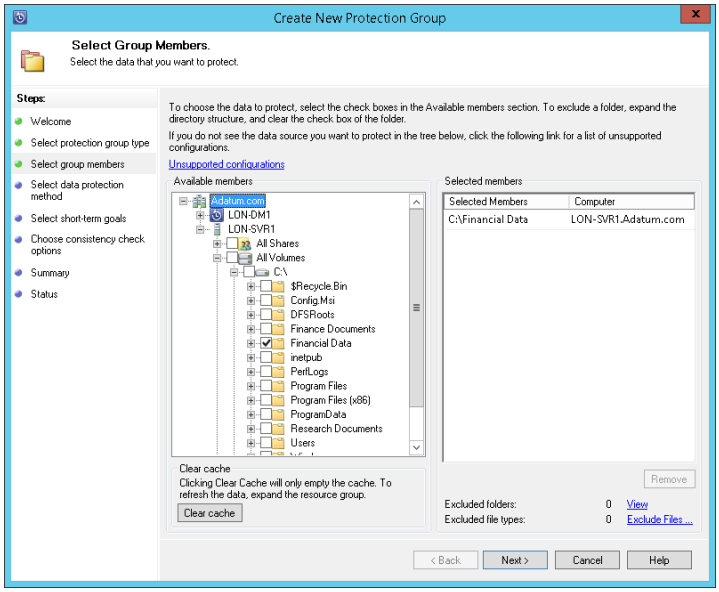
2. Cửa sổ **Welcome to the New Protection Group Wizard**, chọn **Next**.



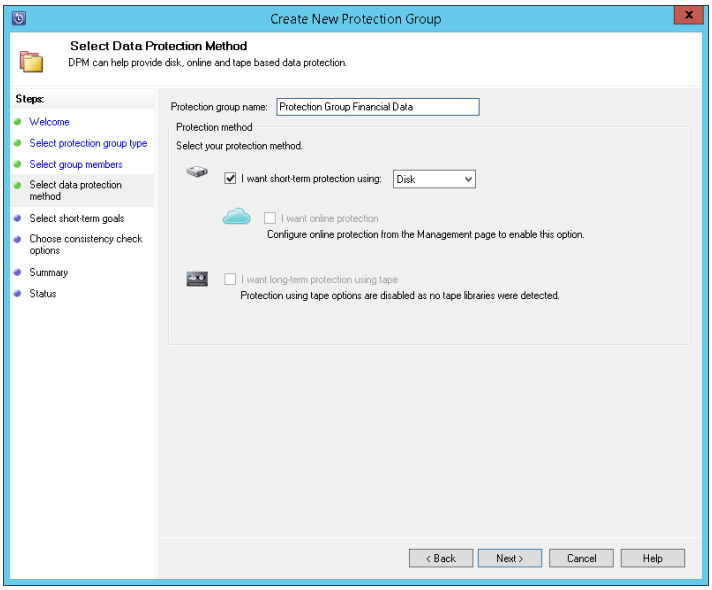

3. Cửa sổ **Select Protection Group Type**, chọn **Servers**, và chọn **Next**.



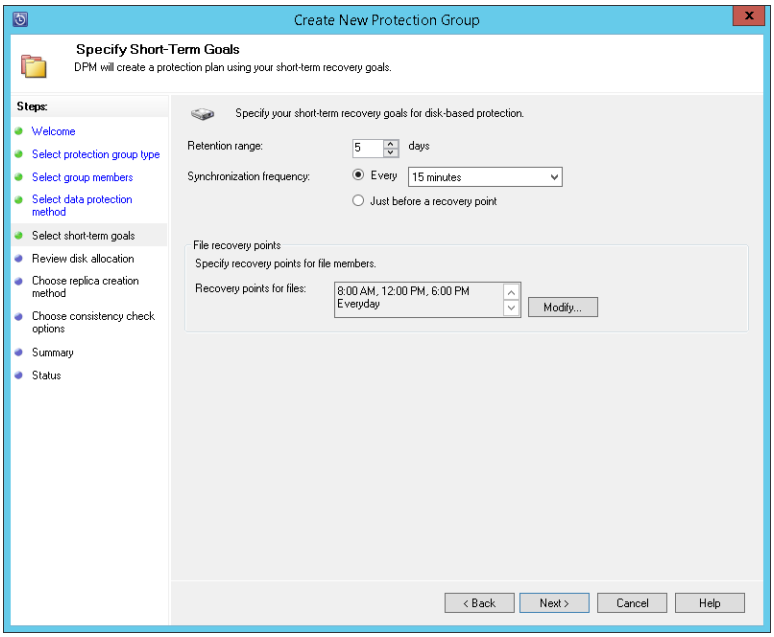
4. Cửa sổ **Select Group Members**, bung **LON-SVR1**, bung **All Volumes**, bung **C:**, đánh dấu chọn **Financial Data**, chọn **OK**, và chọn **Next**.



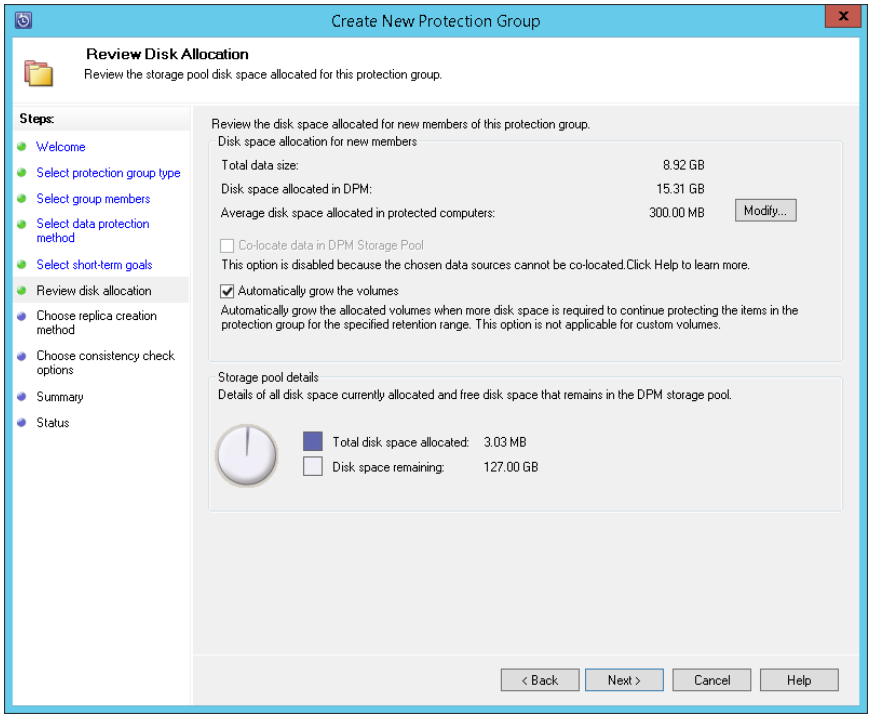

5. Cửa sổ **Select Data Protection Method**, trong ô **Protection group name**, nhập **Protection Group Financial Data**, đảm bảo có đánh dấu chọn **I want short-term protection using Disk**, chọn **Next**.



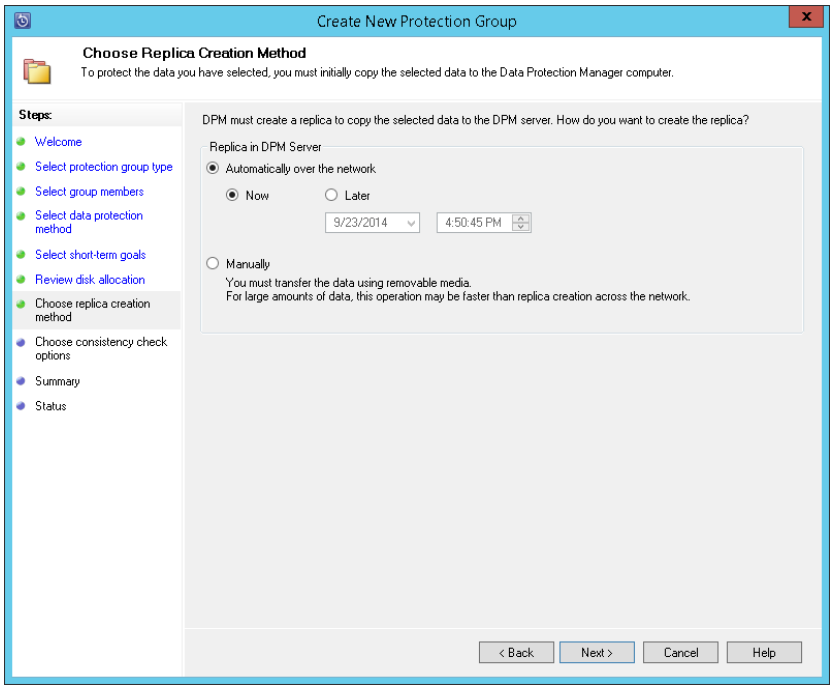
6. Cửa sổ **Specify Short-Term Goals**, chọn **Next**.



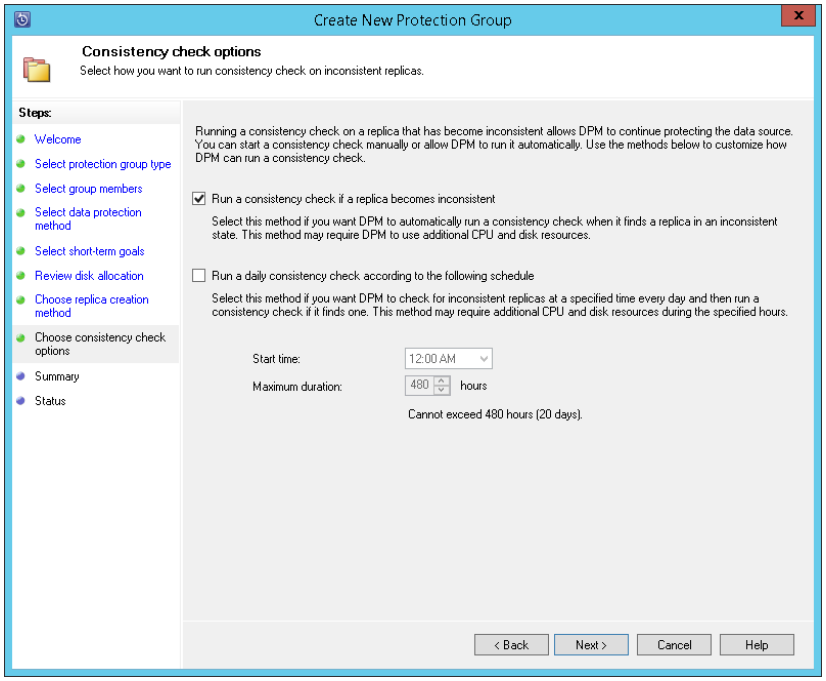

7. Cửa sổ **Review Disk Allocation**, chọn **Next**.



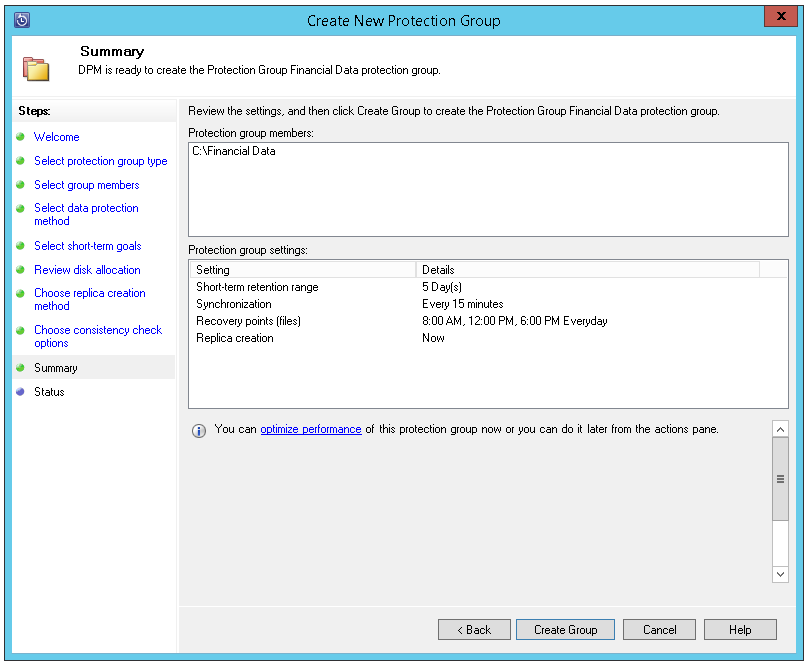
8. Cửa sổ **Choose Replica Creation Method**, chọn **Next**.



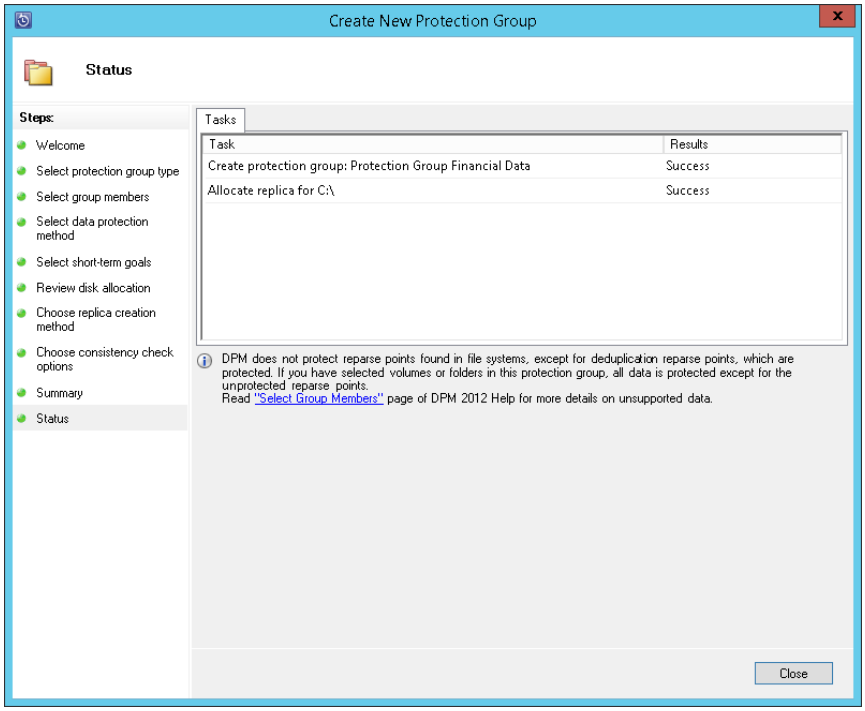

9. Cửa sổ **Consistency check options**, chọn **Next**.



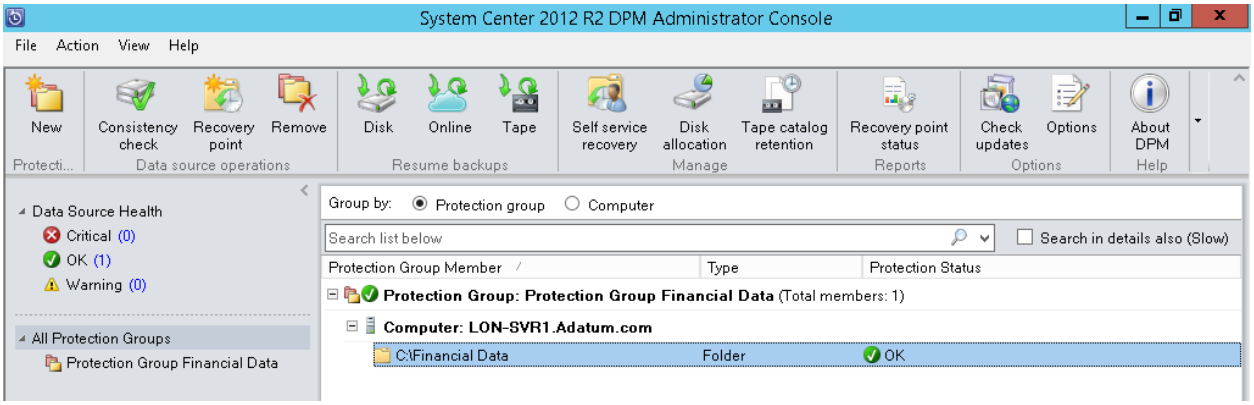
10. Cửa sổ **Summary**, chọn **Create Group**.




11. Cửa sổ **Status**, kiểm tra cột **Results** báo **Success**, chọn **Close**.



12. Trong cửa sổ **DPM Administrator Console, kiểm tra có Protection Group Financial Data.** (Đợi đến khi có biểu tượng dấu chọn màu xanh)




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã tạo được Storage Pool là Disk1. Ngoài ra bạn đã triển khai cài đặt DPM Protection Agents cho LON-SVR1 và tạo Protection groups để hỗ trợ việc sao lưu và phục hồi folder Financial Data.**

## Bài tập 2: Sao lưu và phục hồi dữ liệu bằng DPM.

Các máy ảo tại A. Datum lưu trữ nhiều dữ liệu quan trọng của công ty. yêu cầu quan trọng là bạn phải đảm bảo an toàn cho các dữ liệu này. Vì vậy, bạn cần phải cấu hình DPM để sao lưu và khôi phục các dữ liệu quan trọng.

❖ **Bài thực hành bao gồm các bước:**

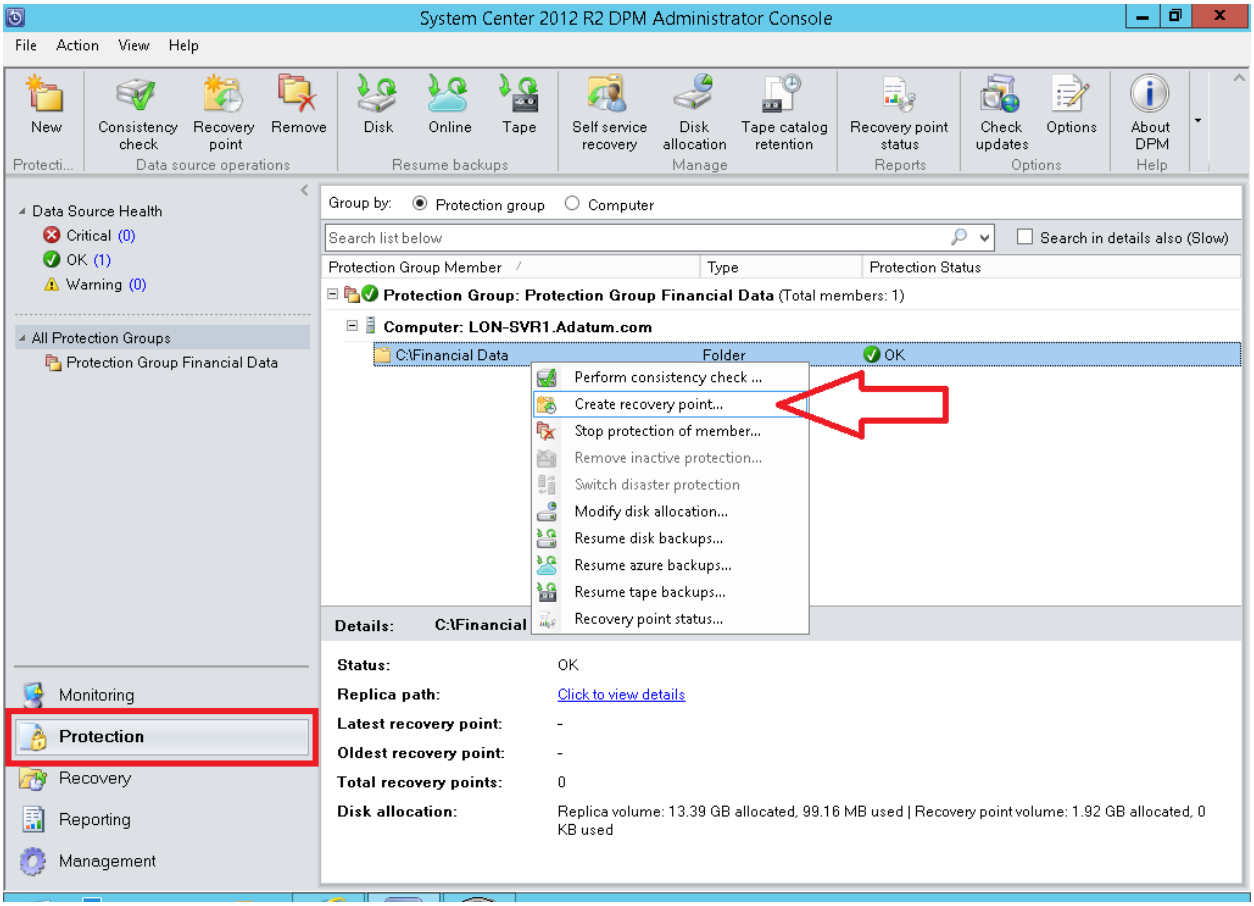
1. Back up dữ liệu.
2. Xóa dữ liệu.
3. Phục hồi dữ liệu.

❖ **Thực hiện:**

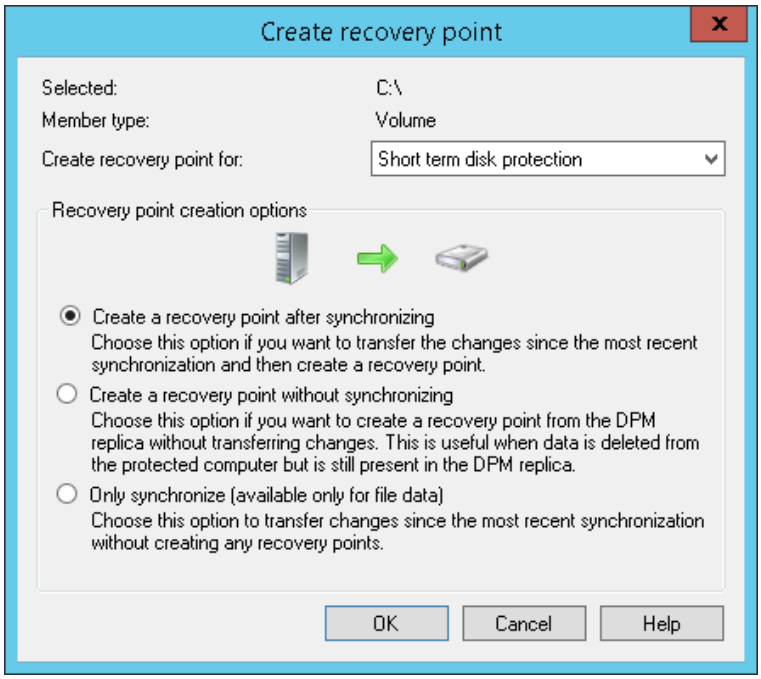
**Bước 1. Back up dữ liệu.**

1. Trên máy **LON-DM1**, trong cửa sổ **DPM Administrator Console**, chọn **Protection,** bung **Protection Group Financial Data** (đảm bảo đang có biểu tượng dấu chọn màu xanh).

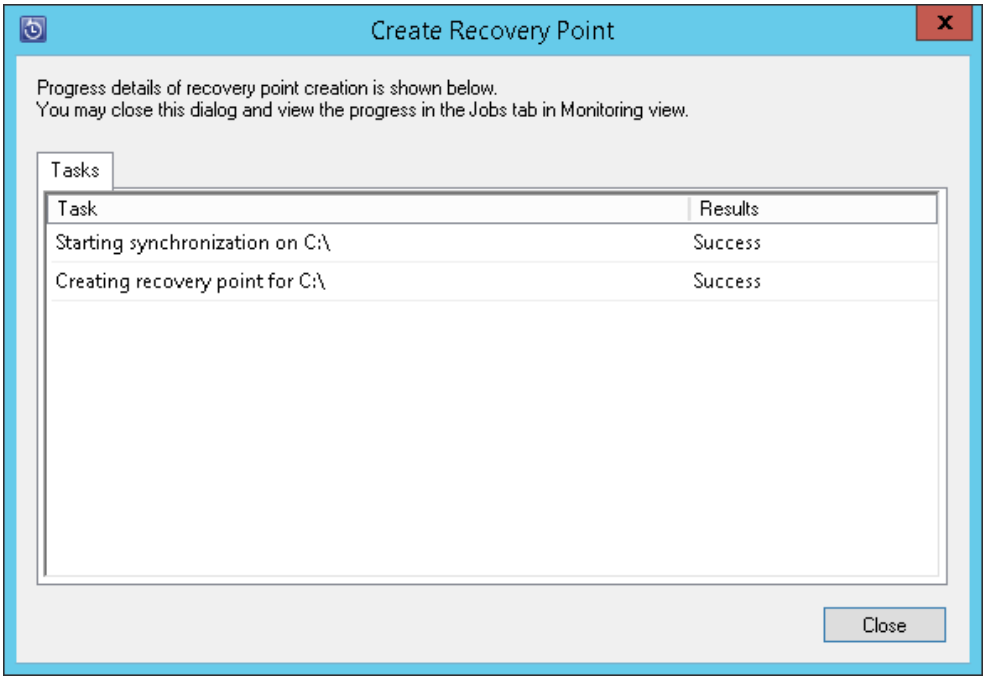
Chuột phải **C:\Financial Data**, chọn **Create recovery point**.



2. Hộp thoại **Create recovery point**, chọn **OK**.



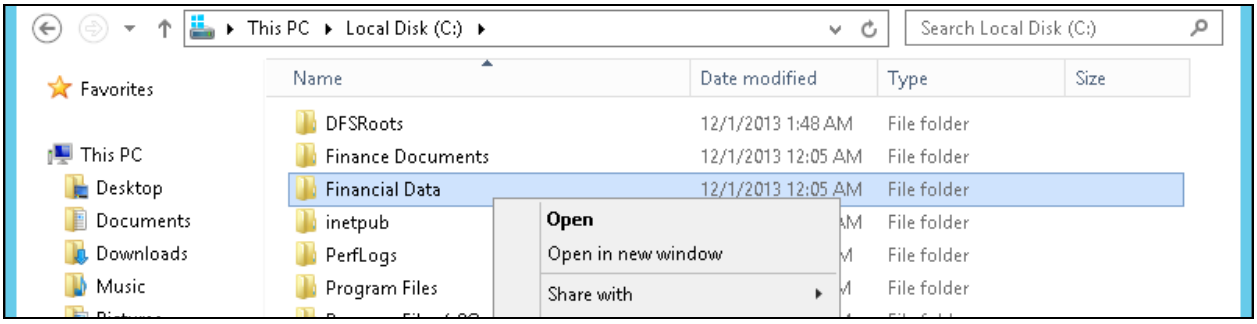

3. Cửa sổ **Create Recovery Point**, kiểm tra cột **Results** báo **Success**, chọn **Close**.



**Bước 2. Xóa dữ liệu.** (Giả lập dữ liệu bị mất)

1. Qua máy **LON-SVR1**.

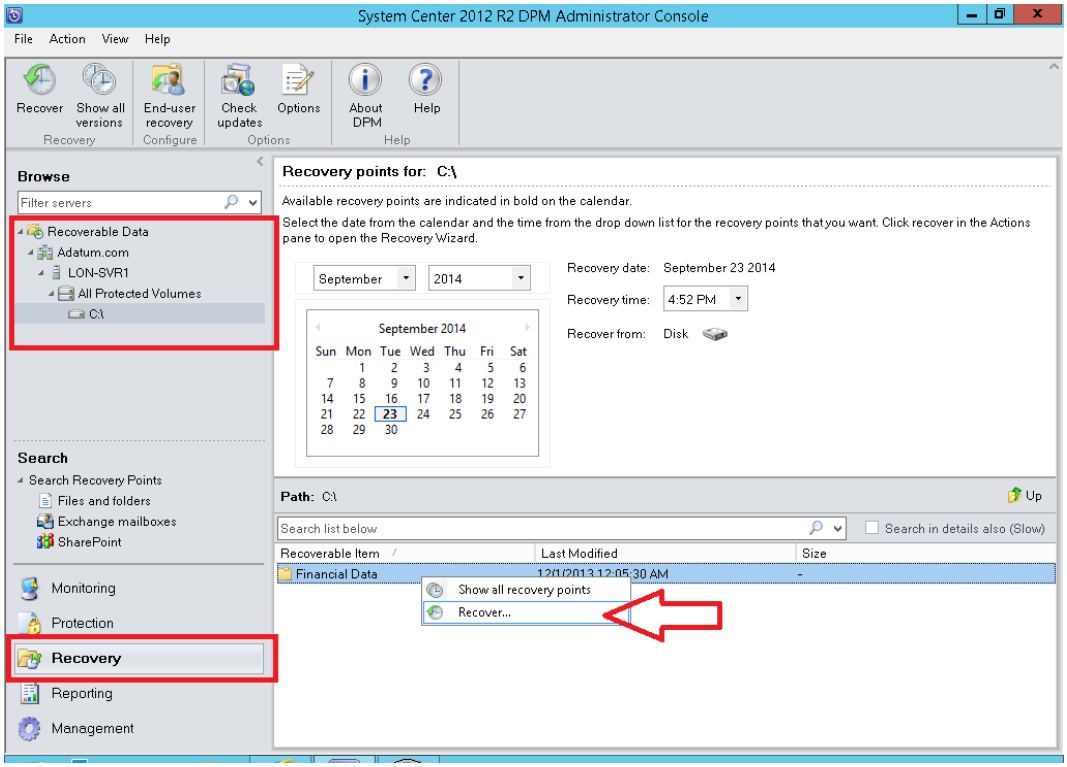
2. Mở **File Explorer**, vào ổ **Local Disk (C:)**, xóa folder **Financial Data**



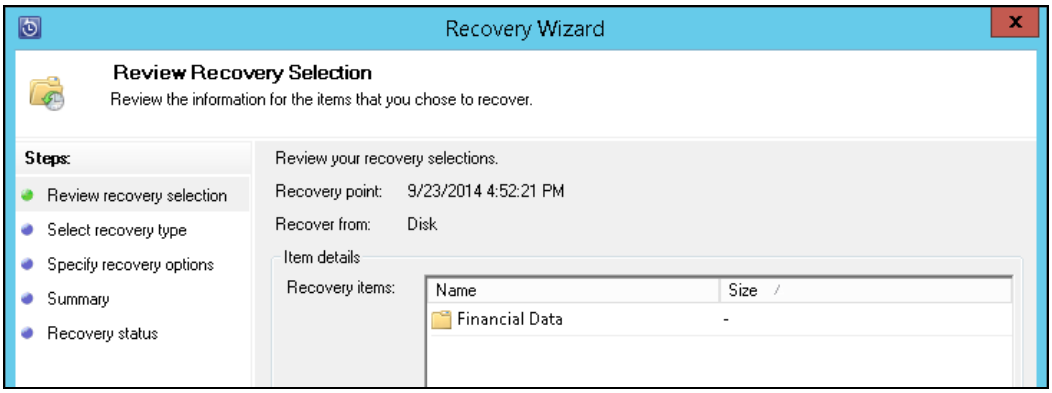

**Bước 3. Phục hồi dữ liệu**

1. Qua máy **LON-DM1**.

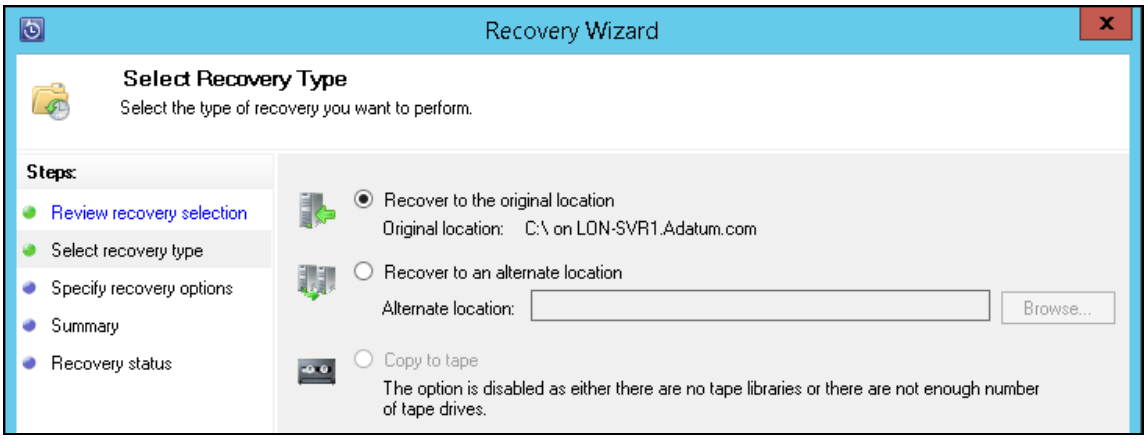
2. Trong cửa sổ **DPM Administrator Console**, chọn **Recovery**, bung **LON-SVR1**, bung **All Protected Volumes**, chọn **C:**. Chuột phải **Financial Data**, chọn **Recover**.



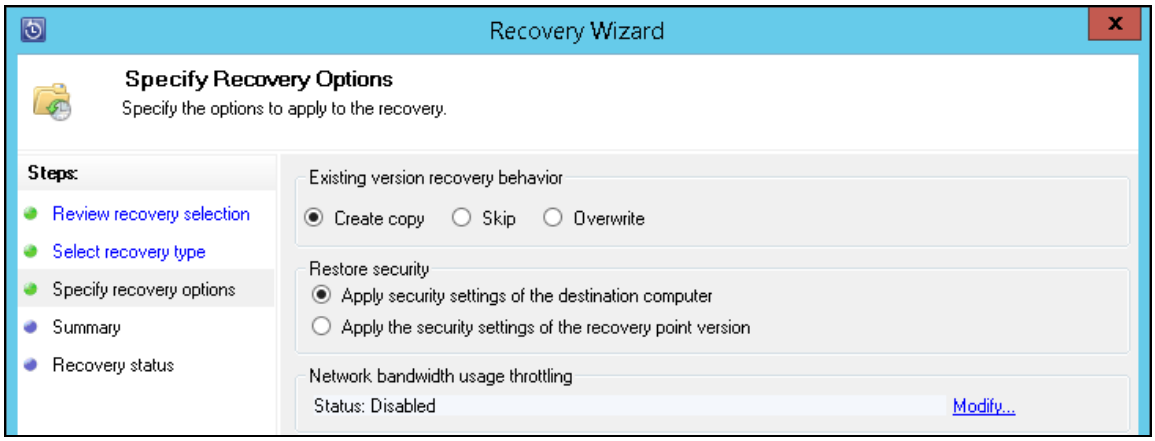
3. Cửa sổ **Review Recovery Selection**, chọn **Next**.



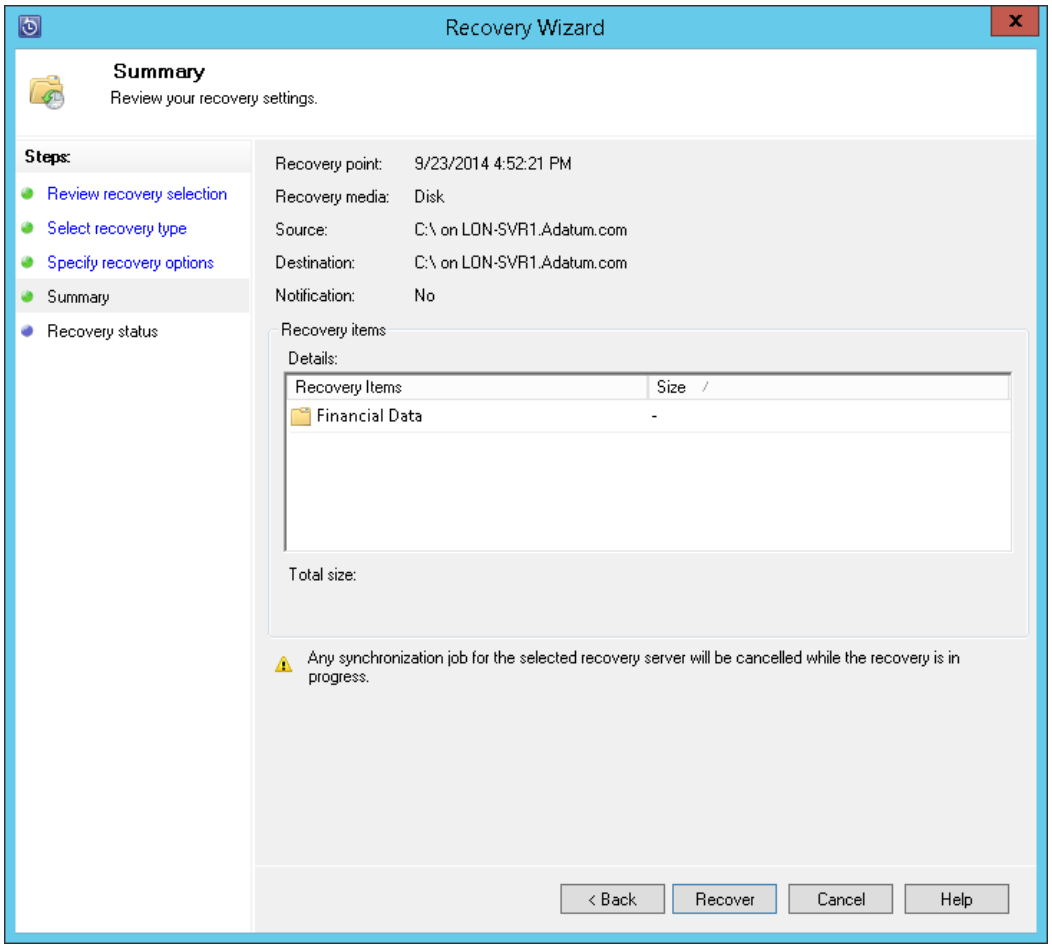

4. Cửa sổ **Select Recovery Type**, chọn **Recover to the original location**, và chọn **Next**.



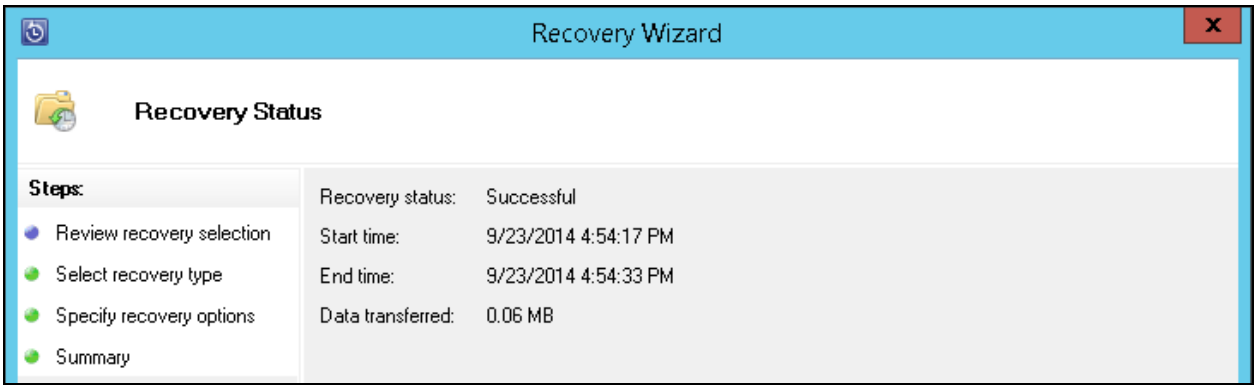

5. Cửa sổ **Specify Recovery Options**, chọn **Next**.



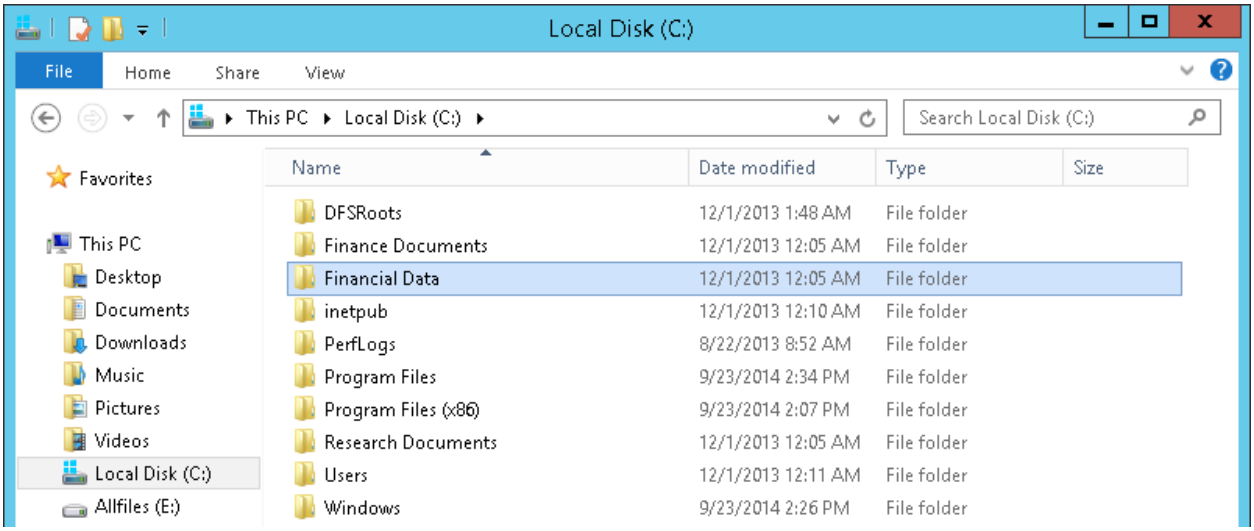
6. Cửa sổ **Summary**, chọn **Recover**.




7. Cửa sổ **Recovery Status**, kiểm tra **Recovery status** báo **Successful**, chọn **Close**.



8. Qua máy **LON-SVR1**, mở **File Explorer**, vào ổ **Local Disk (C:)**. Kiểm tra đã khôi phục thành công folder **Financial Data**.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã sử dụng DPM để sao lưu folder Financial Data, sau đó giả lập folder Financial Data bị mất và sử dụng DPM để khôi phục folder Financial Data.**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20414C-LON-SVR1, 20414C-LON-DM1**

# Bài 9: Triển khai Active Directory Certificate Services (AD CS)

**I. Mục tiêu:**

- Lập kế hoạch triển khai AD CS.
- Triển khai cơ sở hạ tầng CA.
- Tạo và phát hành Certificate mẫu (Certificate Templates).
- Cấu hình chức năng tự động phân phối và thu hồi Certificate.

**II. Kịch bản:**

Hệ thống mạng của công ty A. Datum đã mở rộng, do đó họ có yêu cầu về vấn đề bảo mật. Bộ phận an ninh tại A. Datum muốn cho phép truy cập an toàn vào các trang web quan trọng và cung cấp các tính năng bảo mật như sử dụng thẻ thông minh (Smart Card) và các tính năng DirectAccess của Windows 7 và Windows 8. Để giải quyết những yêu cầu bảo mật này, A. Datum đã quyết định ứng dụng phương pháp mã hóa Public Key Infrastructure (PKI) bằng cách sử dụng dịch vụ AD CS trong Windows Server 2012 R2.

**III. Yêu cầu tổng quan:**

Bộ phận an ninh tại A. Datum cung cấp các yêu cầu cho việc triển khai AD CS như sau:

- Root CA tại A. Datum phải hoàn toàn bị cô lập từ mọi lúc mọi nơi.
- Hệ thống CA phải có khả năng sẵn sàng cao.
- A. Datum có một số ứng dụng yêu cầu xác nhận người dùng bằng certificate. Ngoài ra, bộ phận quản lý phải sử dụng thẻ thông minh (Smart Card) để đăng nhập vào hệ thống.
- A. Datum có một số Web Server chạy ứng dụng cho các clients bên ngoài truy cập. Thông tin liên lạc giữa Web Server và Clients phải được bảo vệ bằng SSL. Bạn nên cấu hình SSL Certificate hết hạn sau ba năm sử dụng.

- A. Datum đang có kế hoạch triển khai DirectAccess để tất cả người sử dụng với máy tính xách tay có thể kết nối với mạng nội bộ mà không cần sử dụng một mạng riêng ảo (VPN). Phải đảm bảo rằng tất cả các máy tính chạy hệ điều hành Windows 7 có một Computer Certificate và các máy tính xách tay phải được cấp DirectAccess Certificate. A. Datum muốn Certificate của mỗi máy tính có hiệu lực trong sáu tháng.
- Tình trạng thu hồi cho tất cả các giấy chứng nhận phải có sẵn cho tất cả các máy tính kết nối với mạng nội bộ ở London, Toronto, và Sydney. A. Datum muốn giảm thiểu lưu lượng mạng cần thiết để lấy các thông tin thu hồi chứng chỉ.
- Các thông tin thu hồi certificate đối với certificate đã cấp cho các DirectAccess Server phải có sẵn để các máy Clients truy cập từ Internet. Tất cả DirectAccess Clients sẽ kết nối với trung tâm dữ liệu ở London. Web Server ở London có địa chỉ truy cập là www.adatum.com.

**IV. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-SVR1**<br>**20414C-LON-CA1**<br>**20414C-LON-CL1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy thật, khởi động vào **20414C-LON-HOST1**.
2. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.

4. Logon vào máy **20414C-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 **20414C-LON-SVR1, 20414C-LON-CA1,** và **20414C-LON-CL1.** Không logon cho tới khi có yêu cầu**.**

**VI. Thực hành:**

## Bài tập 1: Triển khai cơ sở hạ tầng CA.

Bước đầu tiên trong việc triển khai AD CS tại A. Datum là triển khai cơ sở hạ tầng CA. Để tuân thủ các yêu cầu bảo mật là không cho phép truy cập Root CA, trước tiên bạn phải triển Stand-Alone Root CA. Sau đó, bạn sẽ triển khai một Subordinate Enterprise CA để cấp phát certificate.

❖ **Bài tập này bao gồm các bước:**

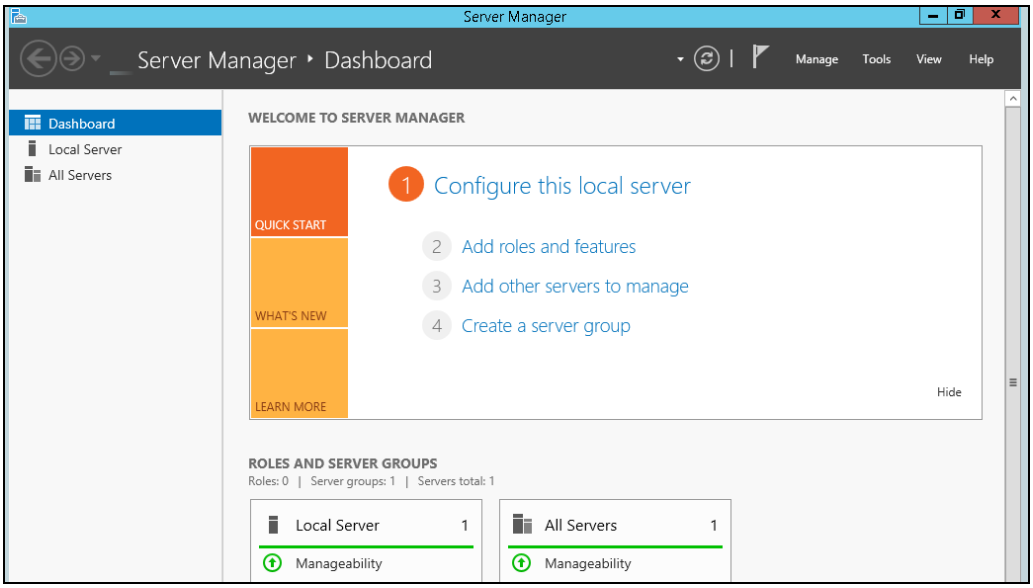
1. Cài đặt và cấu hình Stand-alone Root CA.
2. Cấu hình Certificate Revocation cho Subordinate CA
3. Công bố Root CA certificate trong domain
4. Cài đặt và cấu hình Subordinate Enterprise CA
5. Cấu hình Subordinate trust

❖ **Thực hiện:**

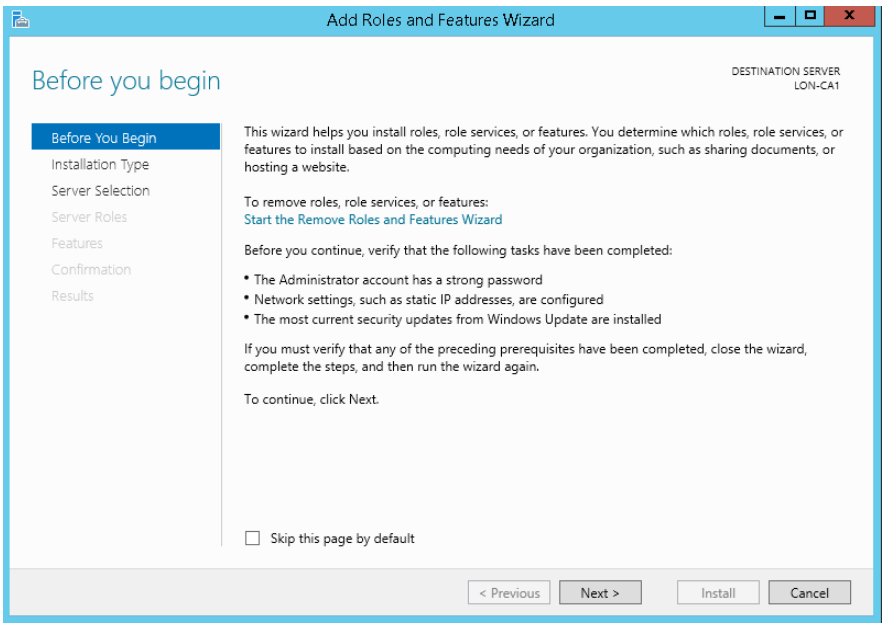
**Bước 1. Cài đặt và cấu hình Stand-alone Root CA.**

1. Sign in máy **LON-CA1** bằng **Administrator** với password **Pa$$w0rd**.

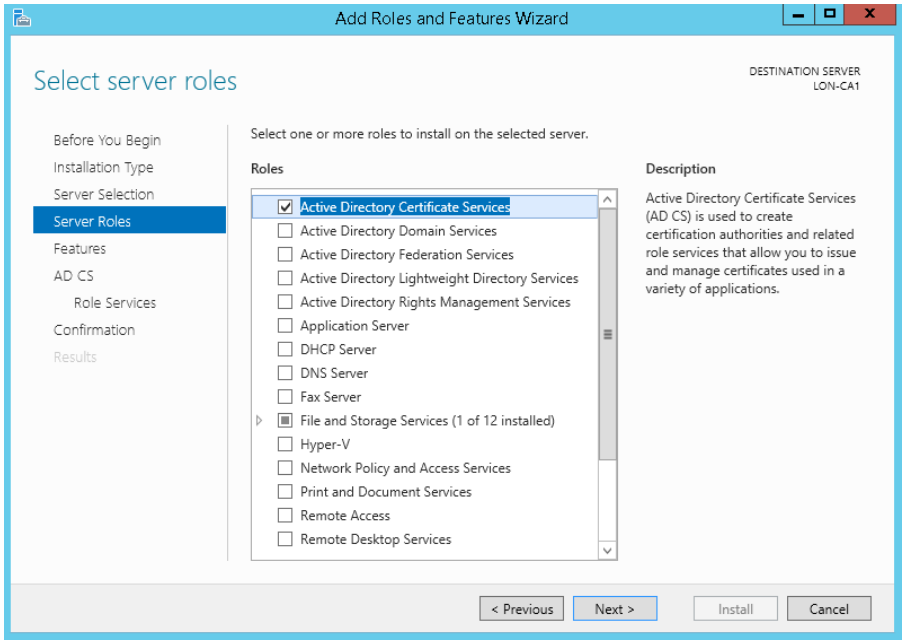
2. Trong cửa sổ **Server Manager**, chọn **Add roles and features**.



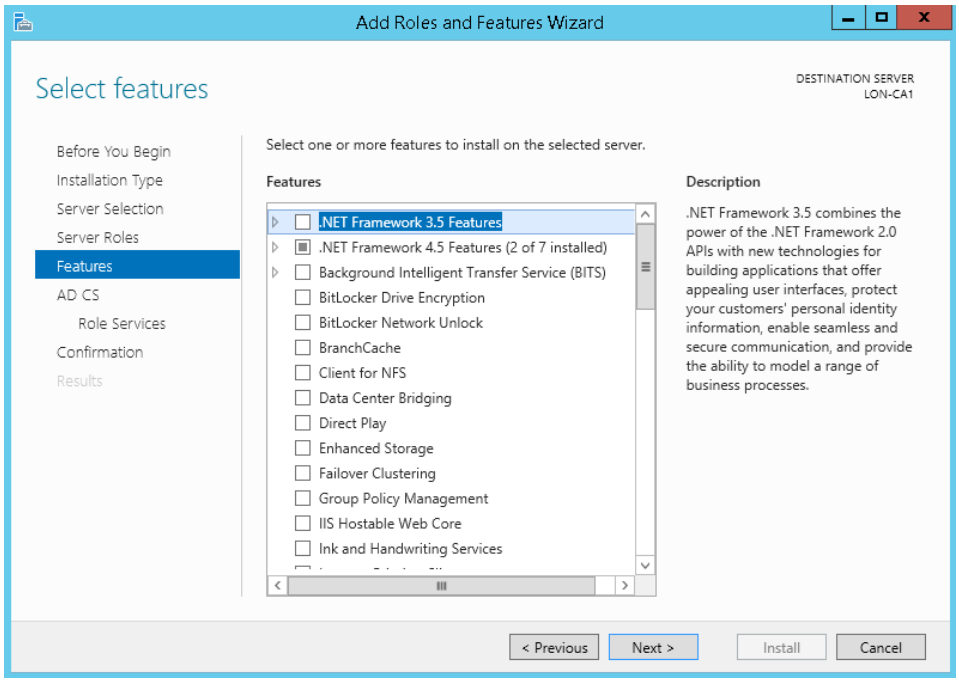

3. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.



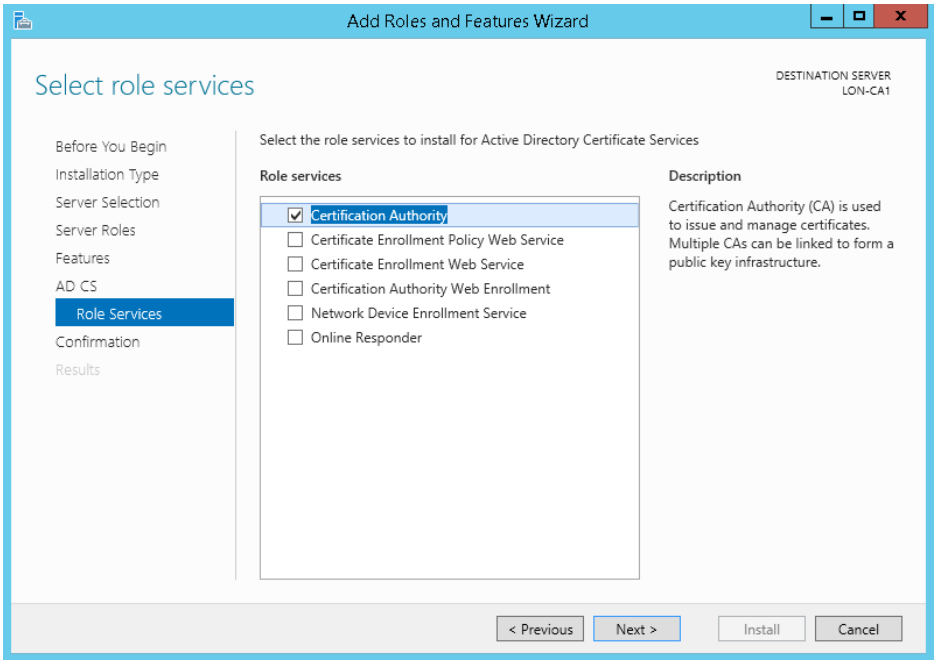
4. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Certificate Services**. Hộp thoại **Add Roles and Features Wizard**, chọn **Add Features**, và chọn **Next**.



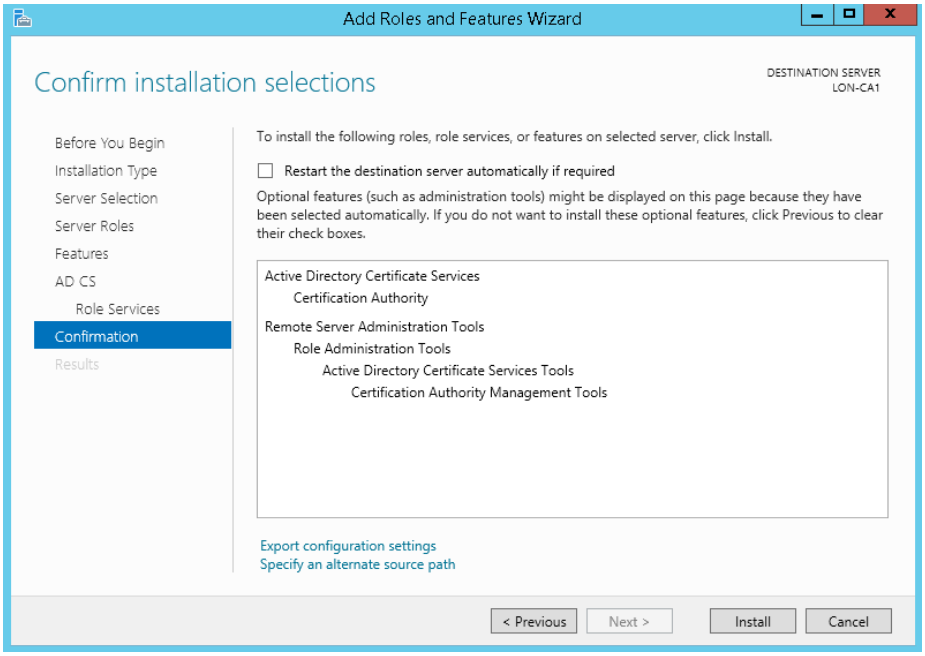

5. Cửa sổ **Select features**, chọn **Next** 2 lần.



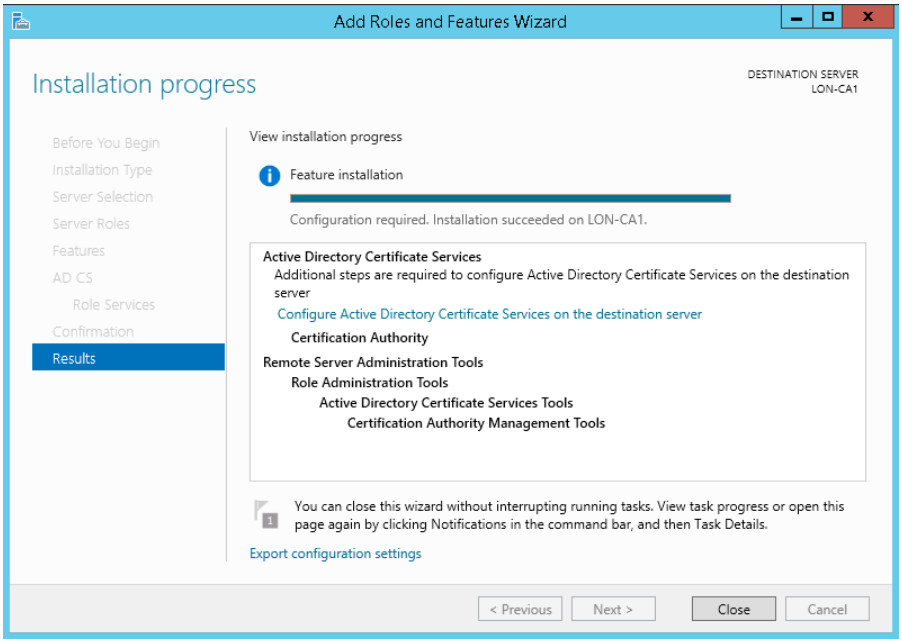
6. Cửa sổ **Select role services**, đảm bảo có đánh dấu chọn **Certification Authority**, chọn **Next**.



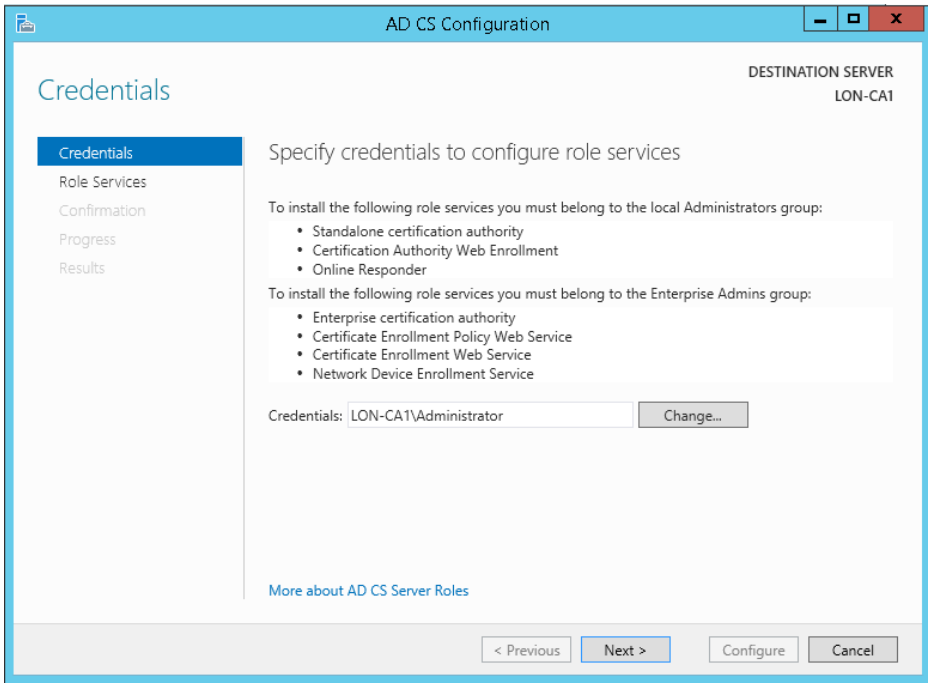

7. Cửa sổ **Confirm installation selections**, chọn **Install**.



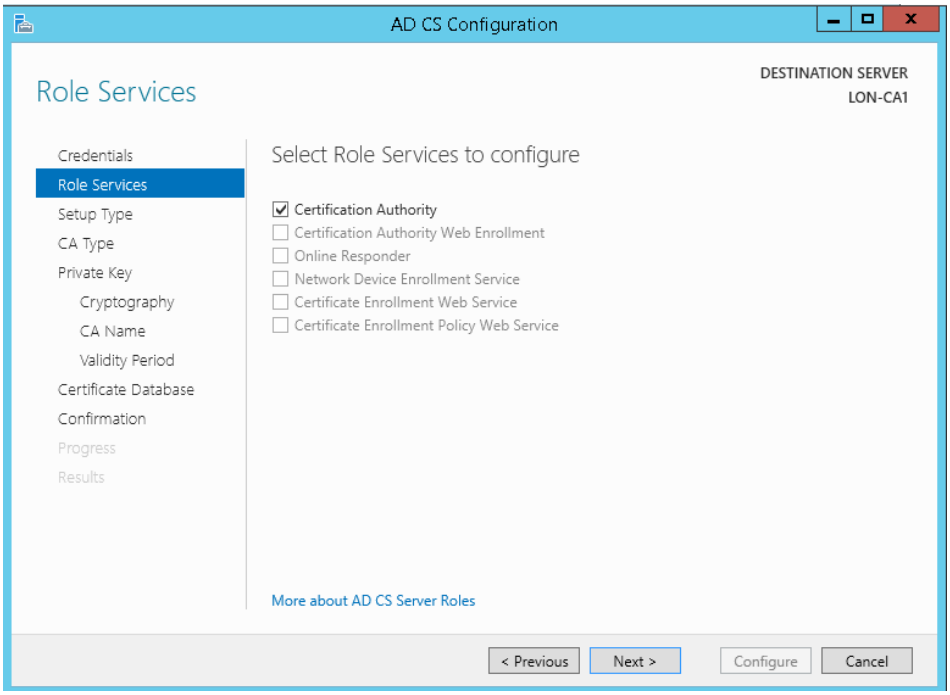
8. Cửa sổ **Installation progress**, sau khi cài đặt thành công, chọn **Configure Active Directory Certificate Services on the destination server**.



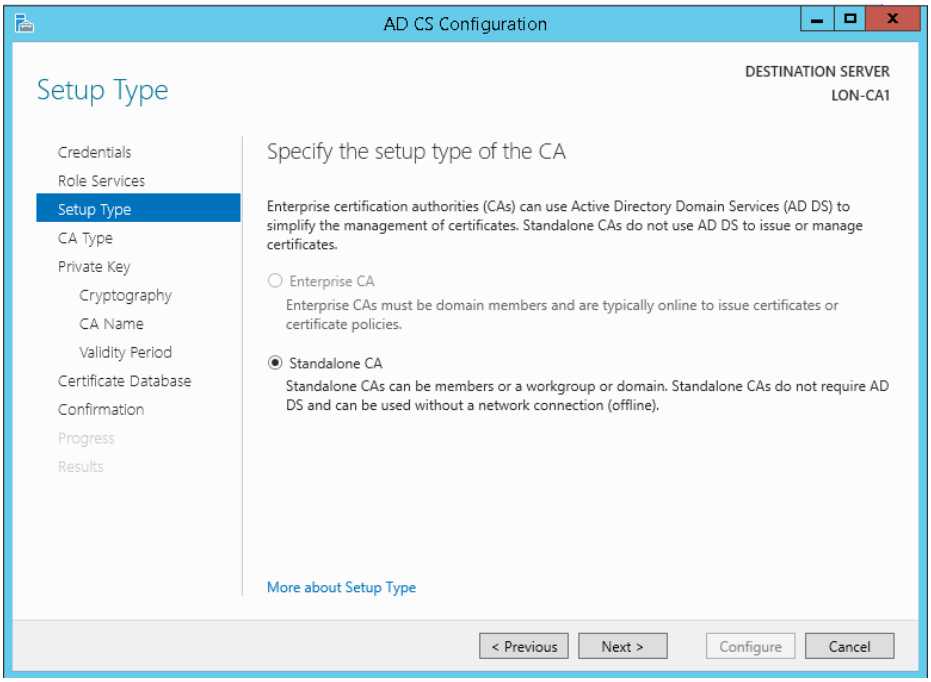

9. Cửa sổ **Credentials**, chọn **Next**.



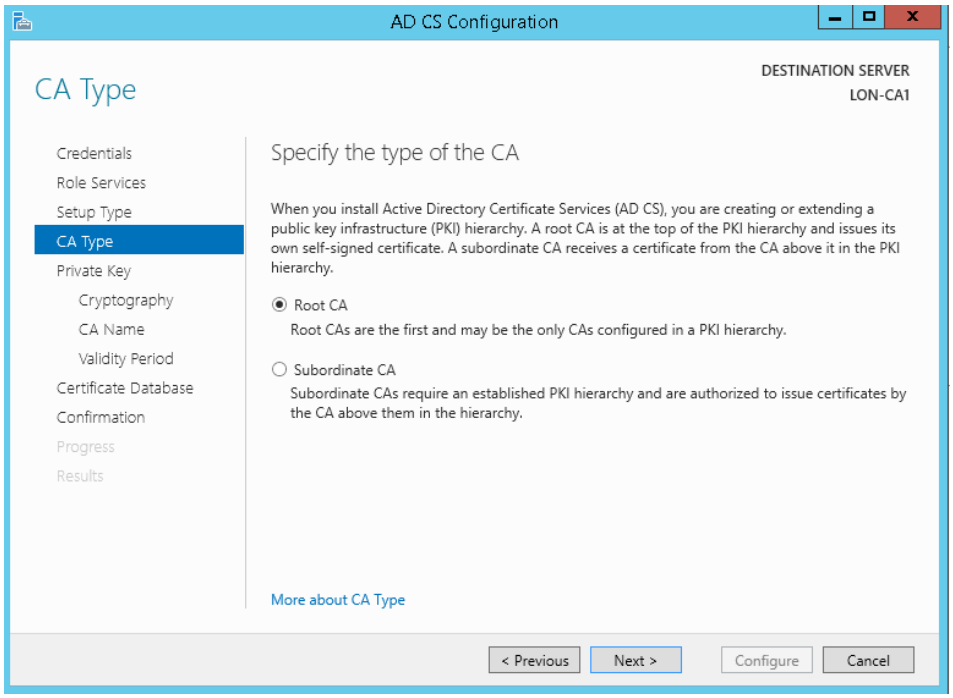
10. Cửa sổ **Role Services**, đánh dấu chọn **Certification Authority**, chọn **Next**.



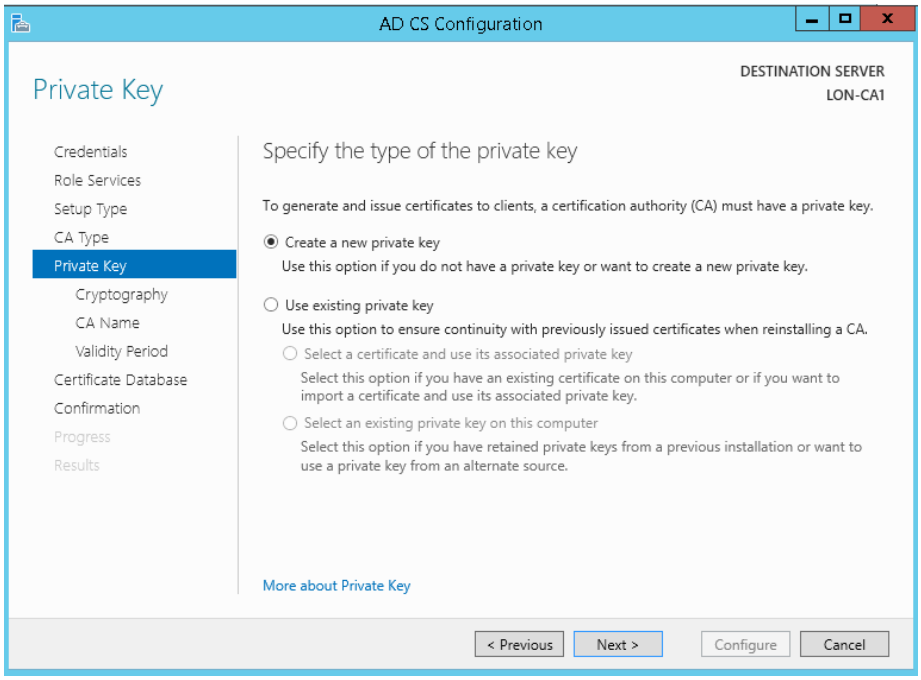

11. Cửa sổ **Setup Type**, chọn **Standalone CA**, và chọn **Next**.



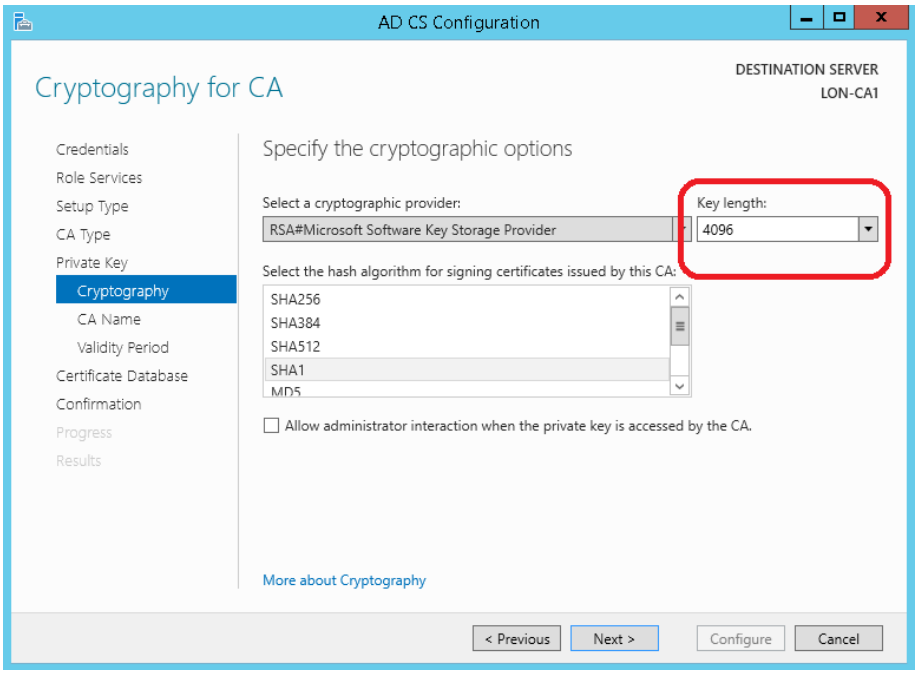
12. Cửa sổ **CA Type**, chọn **Root CA**, và chọn **Next**.



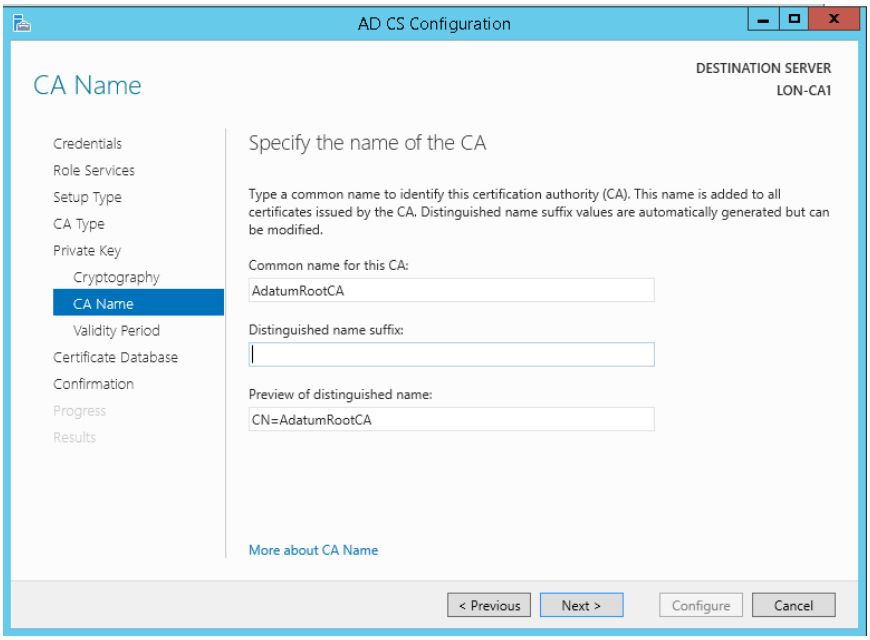

13. Cửa sổ **Private Key**, chọn **Create a new private key**, chọn **Next**.



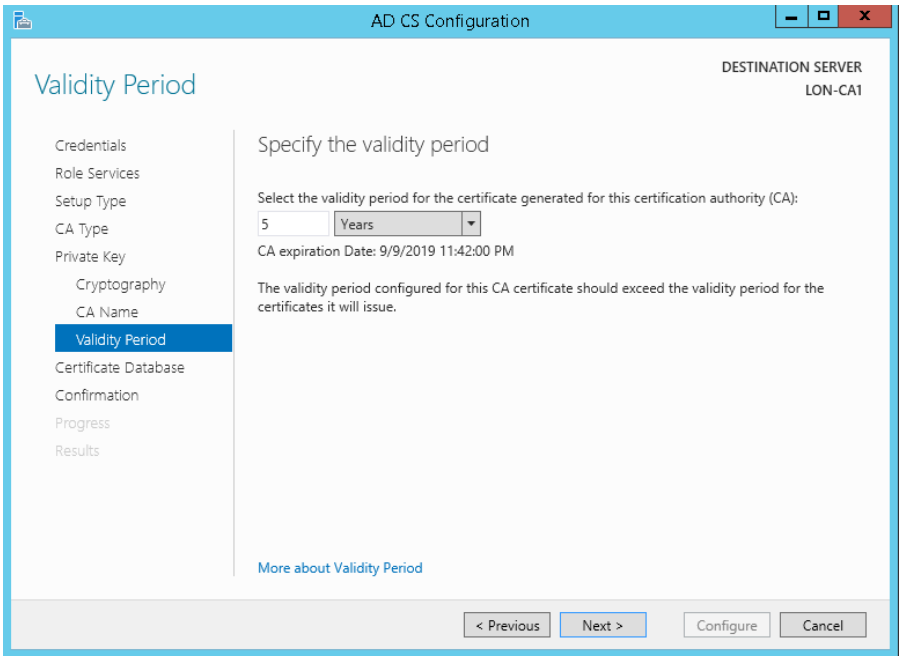
14. Cửa sổ **Cryptography for CA**, trong ô **Key length** nhập **4096**, và chọn **Next**.



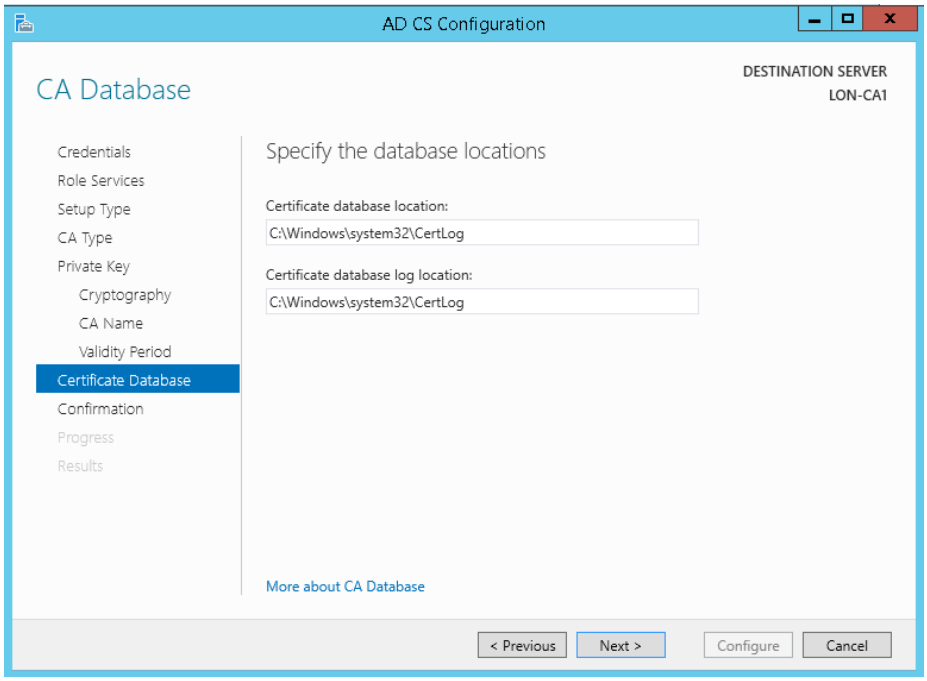

15. Cửa sổ **CA Name**, trong ô **Common name for this CA**, nhập **AdatumRootCA**, và chọn **Next**.



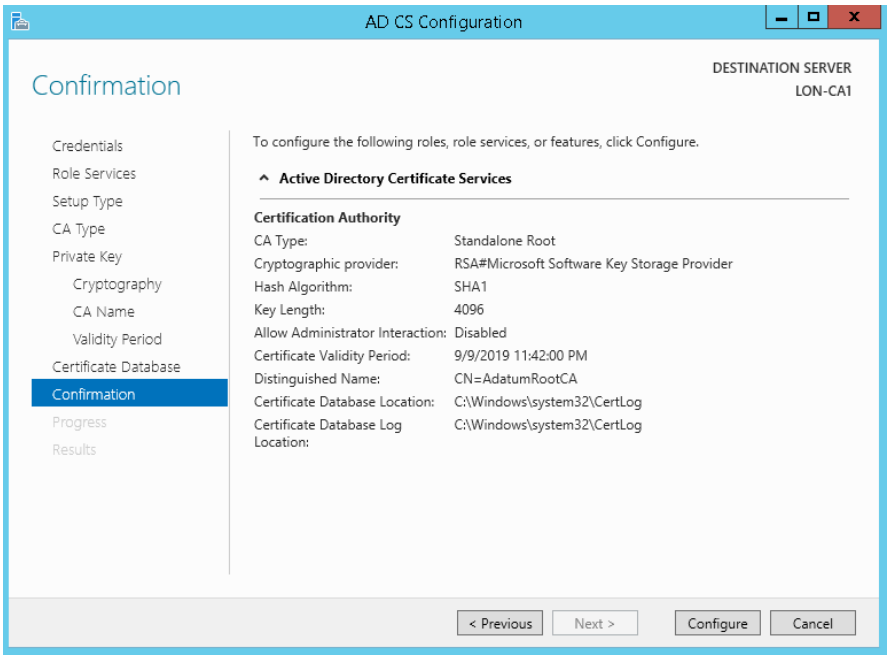
16. Cửa sổ **Validity Period**, chọn **Next**.



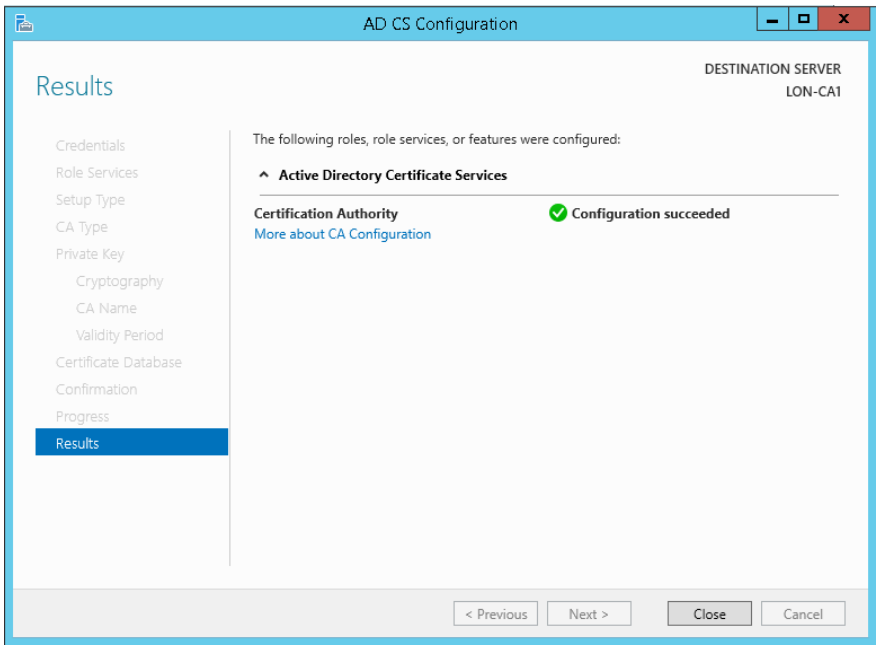

17. Cửa sổ **CA Database**, chọn **Next**.



18. Cửa sổ **Confirmation**, chọn **Configure**.




19. Cửa sổ **Results**, chọn **Close**.

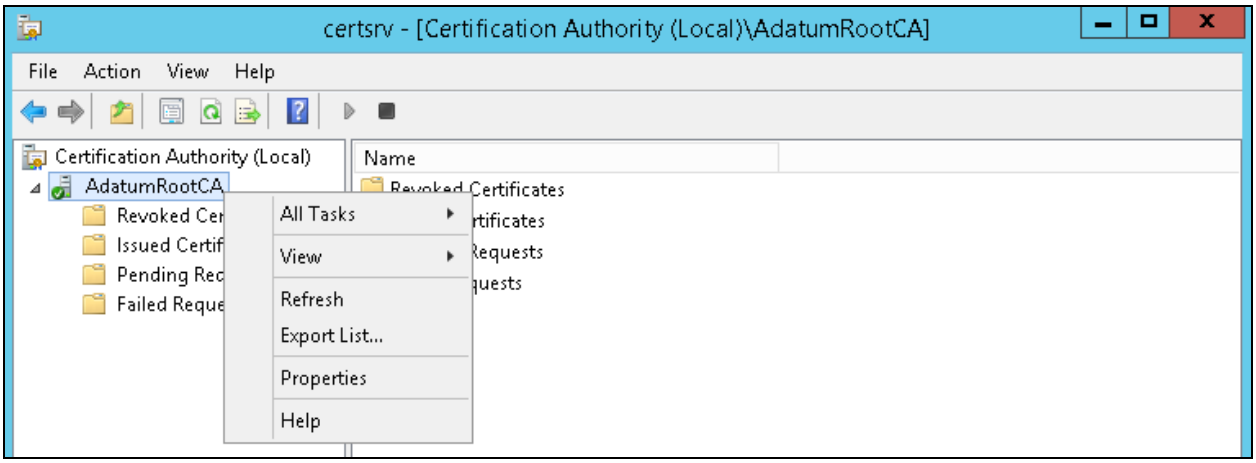



20. Cửa sổ **Installation progress**, chọn **Close**.

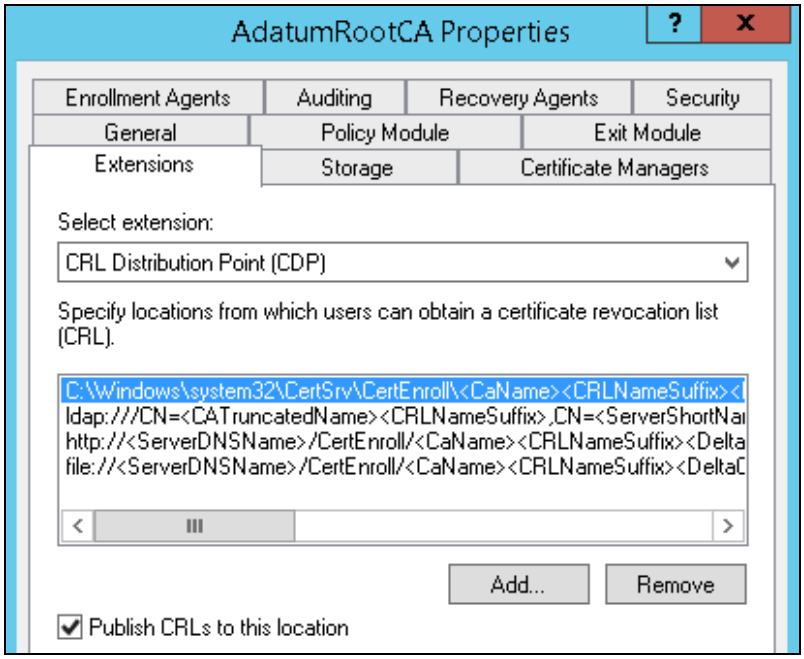
## Bước 2. Cấu hình Certificate Revocation cho Subordinate CA

1. Trên máy **LON-CA1**, trong **Server Manager**, bung menu **Tools**, mở **Certification Authority**.

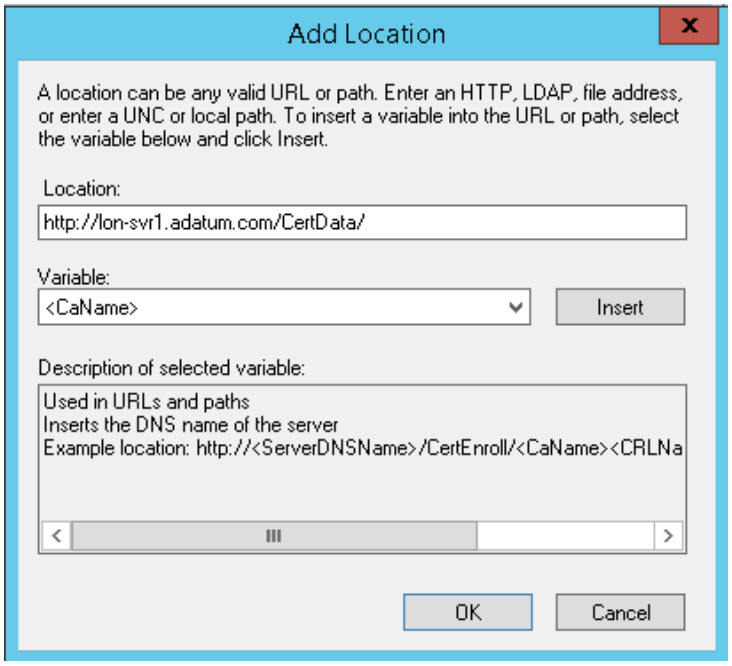
2. Trong cửa sổ **Certification Authority**, chuột phải **AdatumRootCA**, chọn **Properties**.



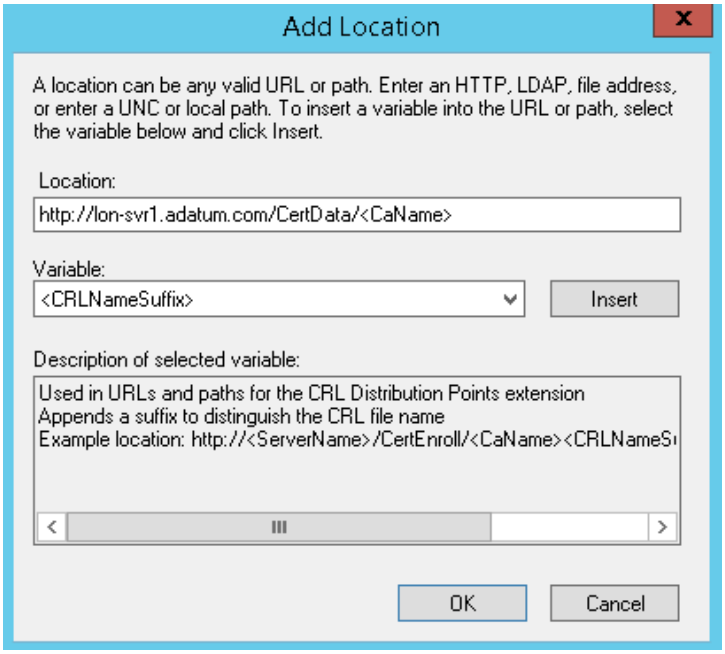

3. Trong hộp thoại **AdatumRootCA Properties**, qua tab **Extensions**, bung ô **Select extension**, chọn **CRL Distribution Point (CDP)**, và chọn **Add**.



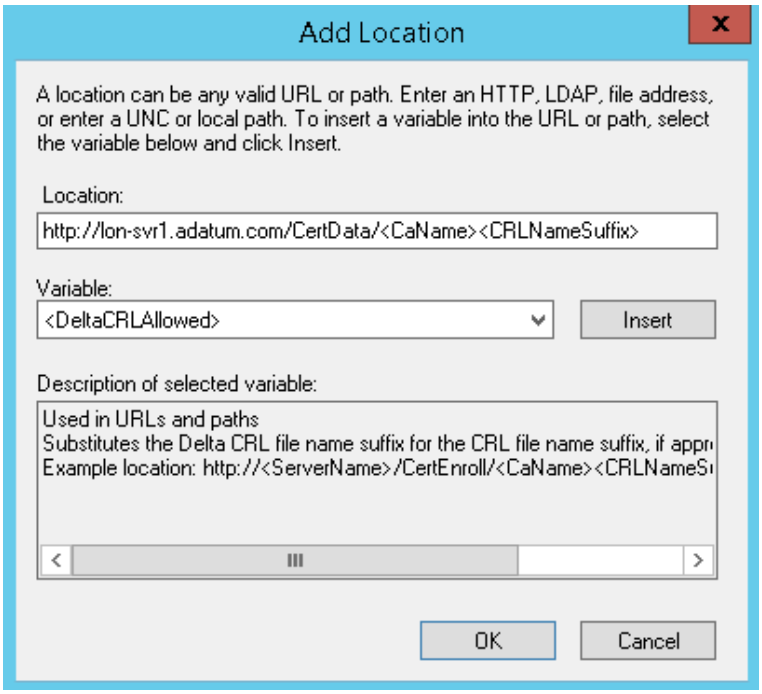
4. Trong ô **Location**, nhập **http://lon-svr1.adatum.com/CertData/**, bung ô **Variable**, chọn **<CaName>**, và chọn **Insert**.



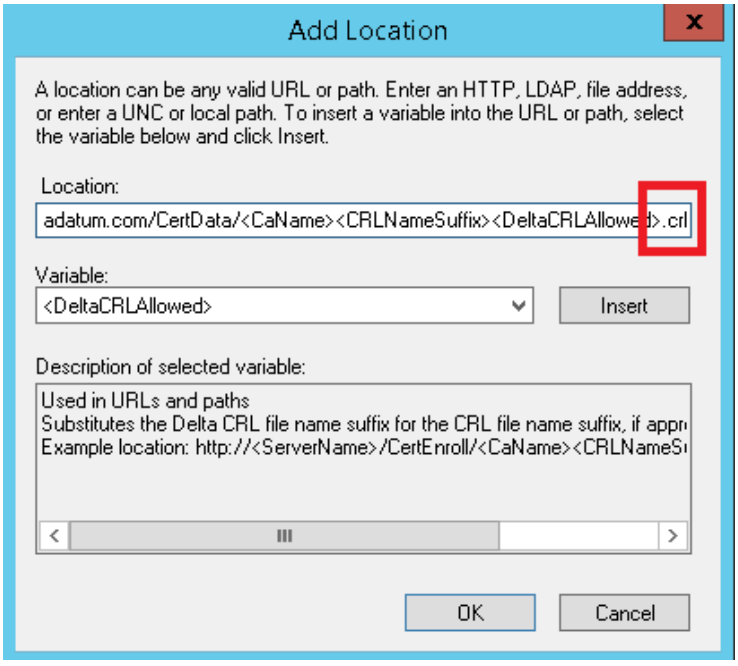

5. Bung ô **Variable**, chọn **<CRLNameSuffix>**, chọn **Insert**.



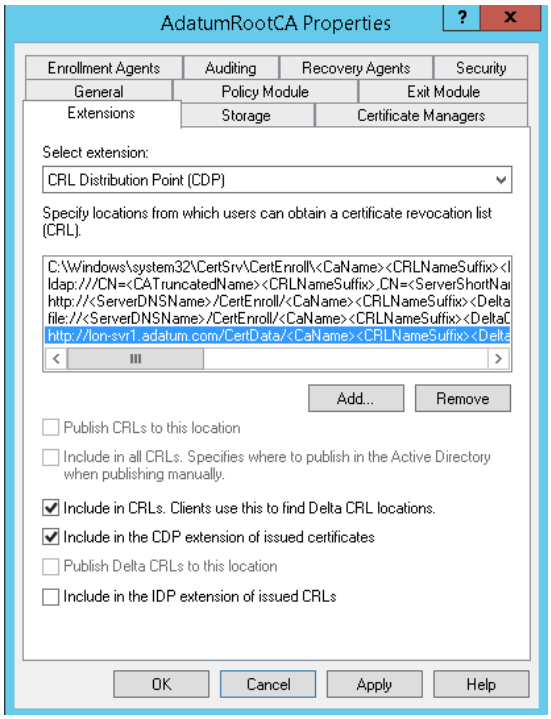
6. Bung ô **Variable**, chọn **<DeltaCRLAllowed>**, và chọn **Insert**.



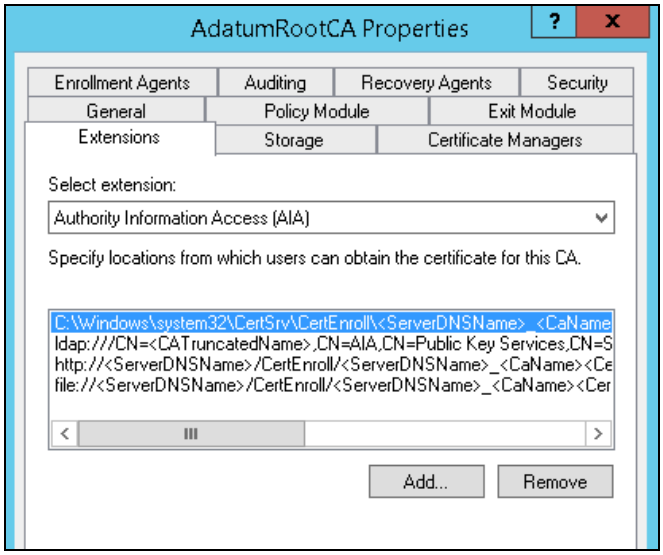

7. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập **.crl**, và chọn **OK**.



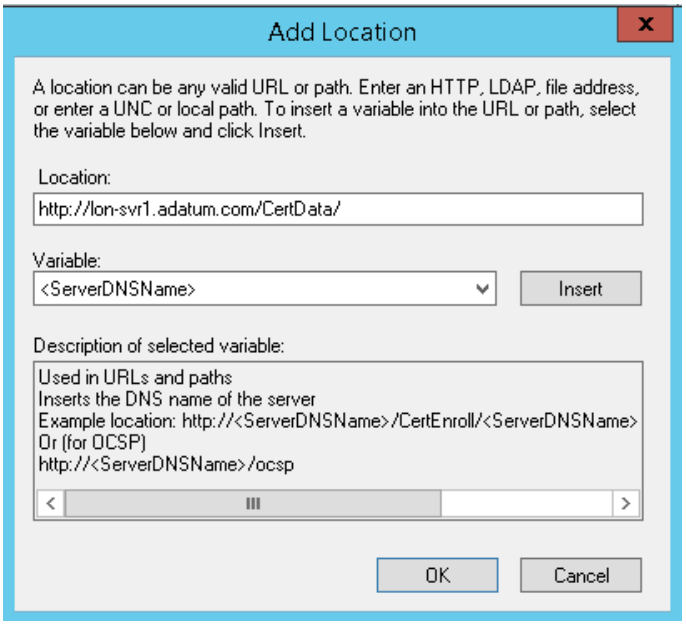
8. Đánh dấu chọn vào 2 ô **Include in the CDP extension of issued certificate**, và **Include in CRLs. Clients use this to find Delta CRL locations**. Chọn **Apply**. Hộp thoại thông báo **Certification Authority**, chọn **No**.



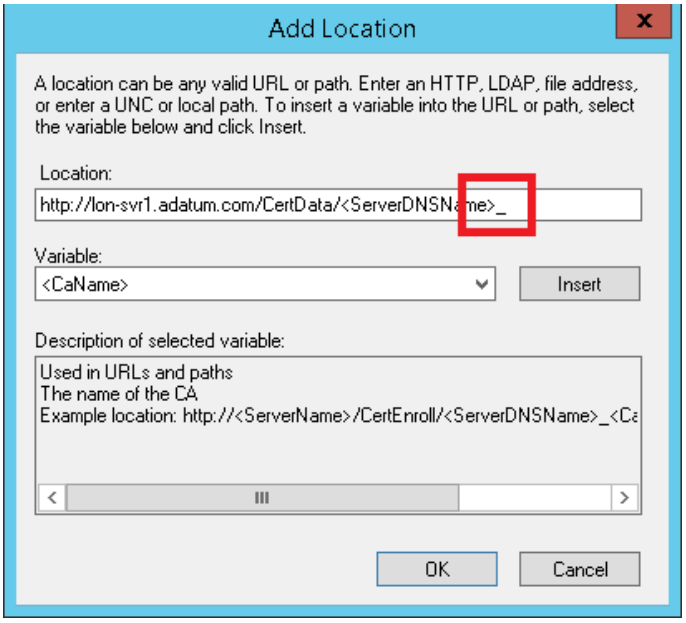

9. Bung ô **Select extension**, chọn **Authority Information Access (AIA)**, và chọn **Add**.



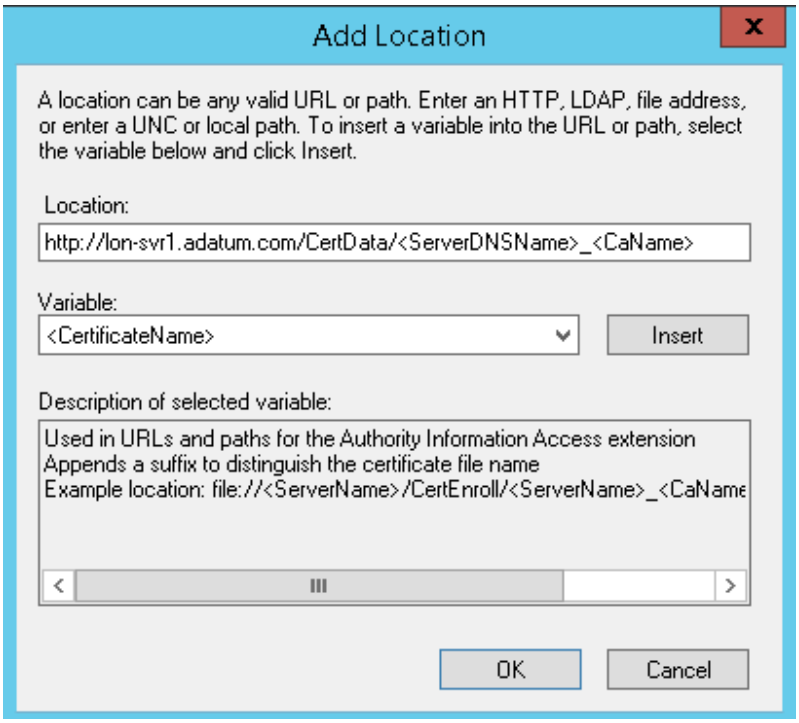
10. Trong ô **Location**, nhập **http://lon-svr1.adatum.com/CertData/**, bung ô **Variable**, **click <ServerDNSName>**, chọn **Insert**.



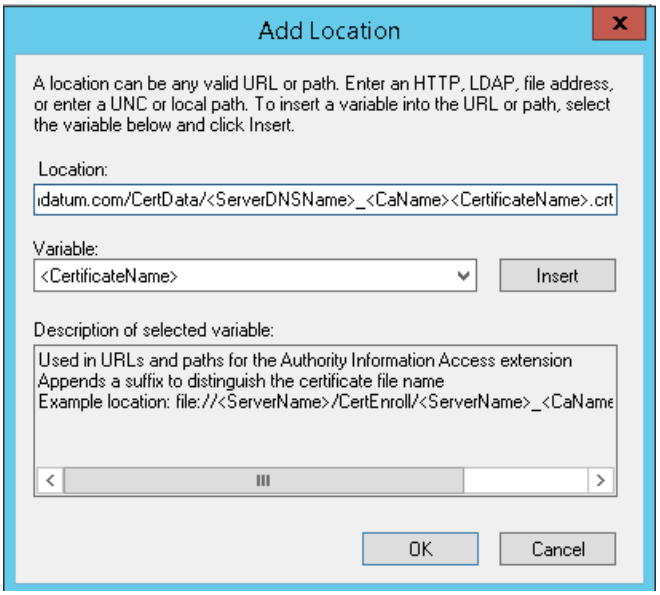

11. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập thêm dấu gạch dưới (_), bung ô **Variable**, chọn **<CaName>**, chọn **Insert**.



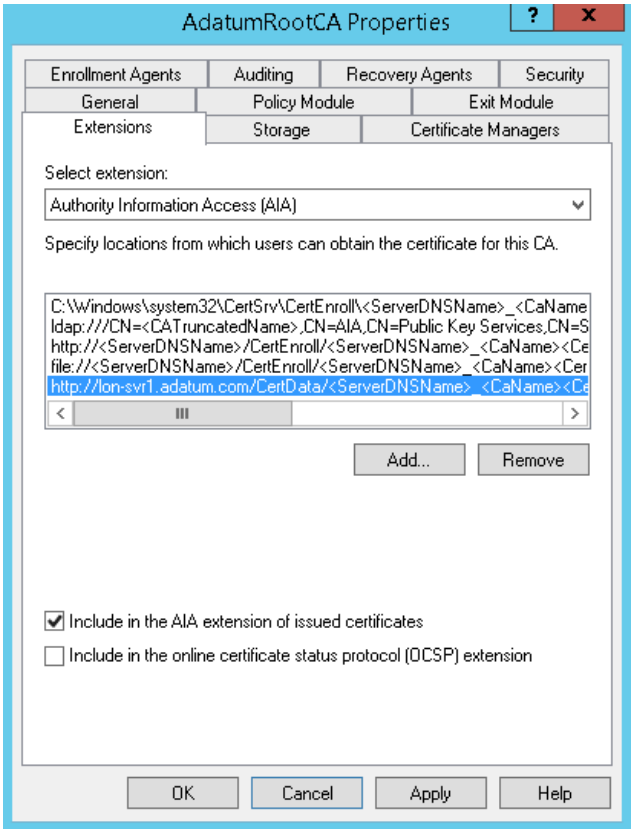
12. Bung ô **Variable**, chọn **<CertificateName>**, và chọn **Insert**.



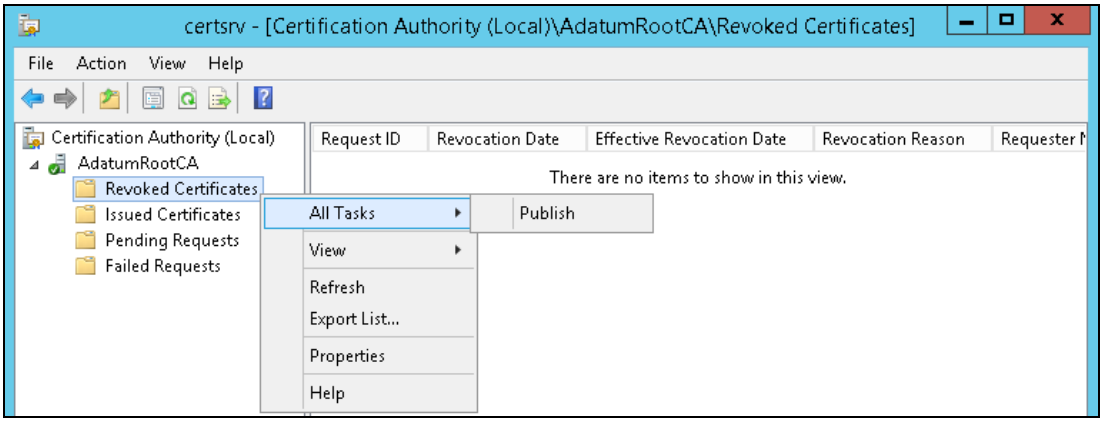

13. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập **.crt**, và chọn **OK**.



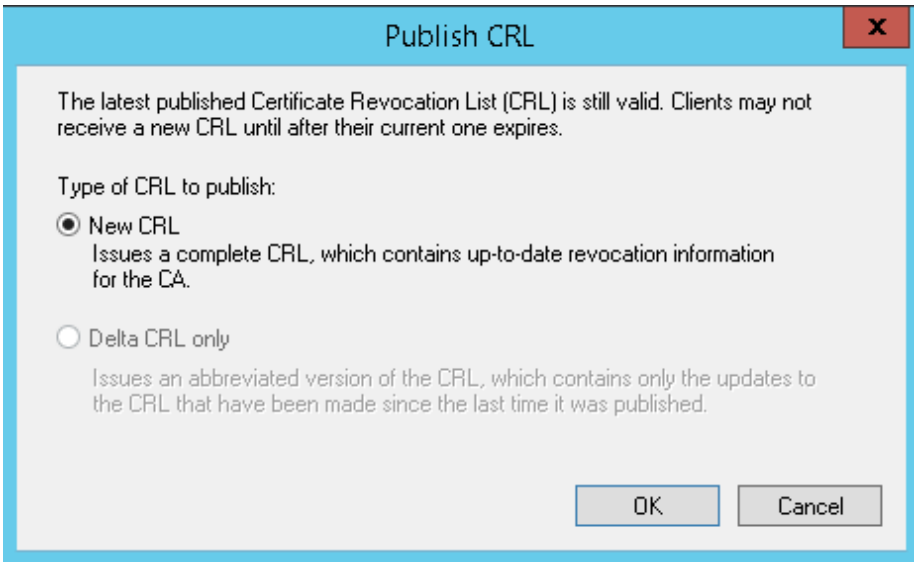
14. Đánh dấu chọn **Include in the AIA extension of issued certificates**, chọn **OK**. Hộp thoại **Certification Authority**, chọn **Yes** để restart Certification Authority service.



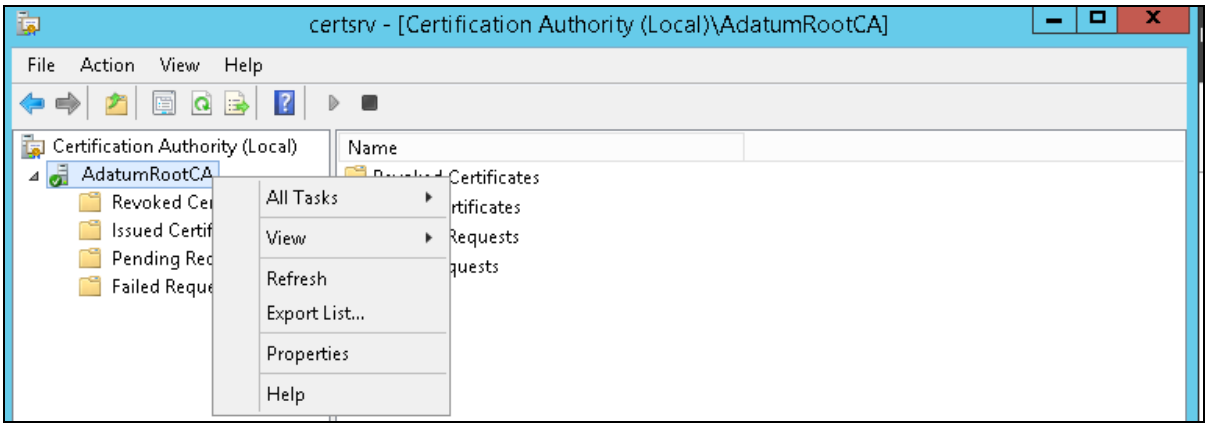

15. Trong cửa sổ **Certification Authority**, bung **AdatumRootCA**, chuột phải **Revoked Certificates**, bung **All Tasks**, và chọn **Publish**.



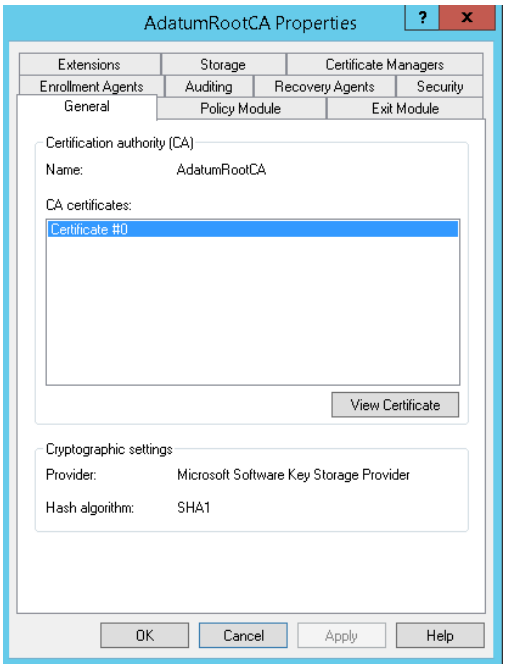
16. Hộp thoại **Publish CRL**, chọn **OK**.



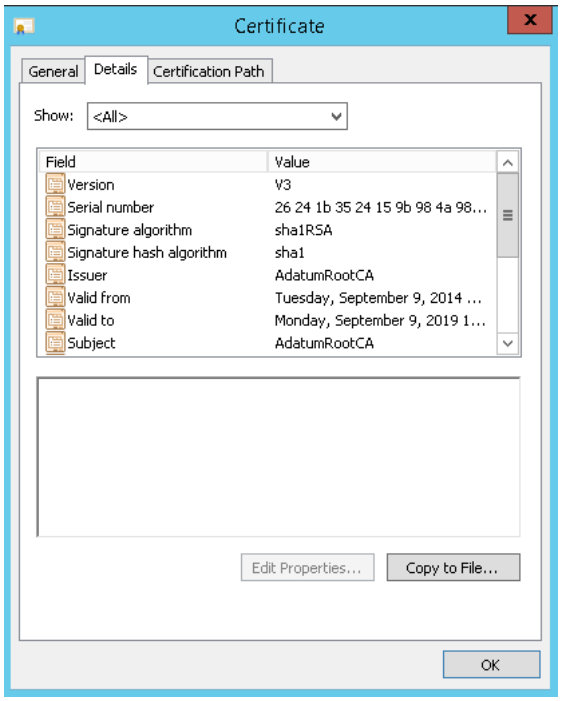

17. Chuột phải **AdatumRootCA**, chọn **Properties**.



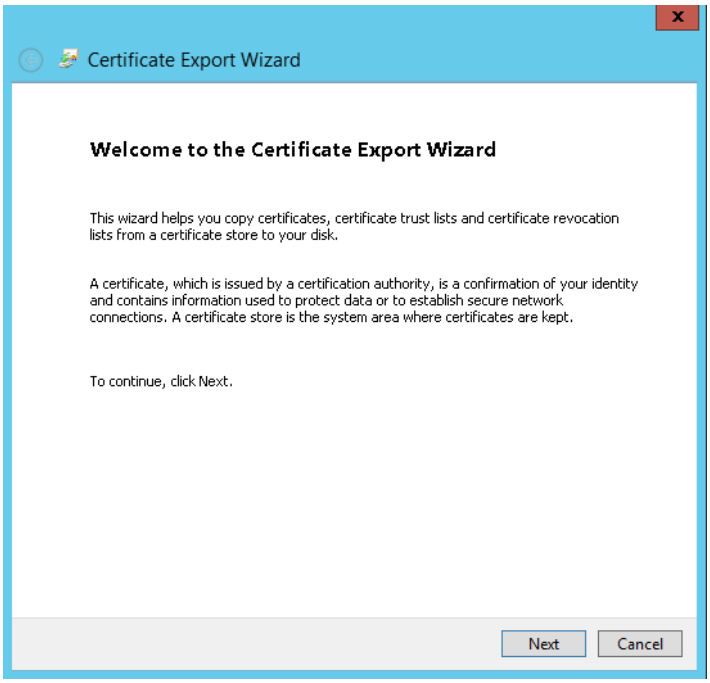
18. Trong hộp thoại **AdatumRootCA Properties**, chọn **View Certificate**.



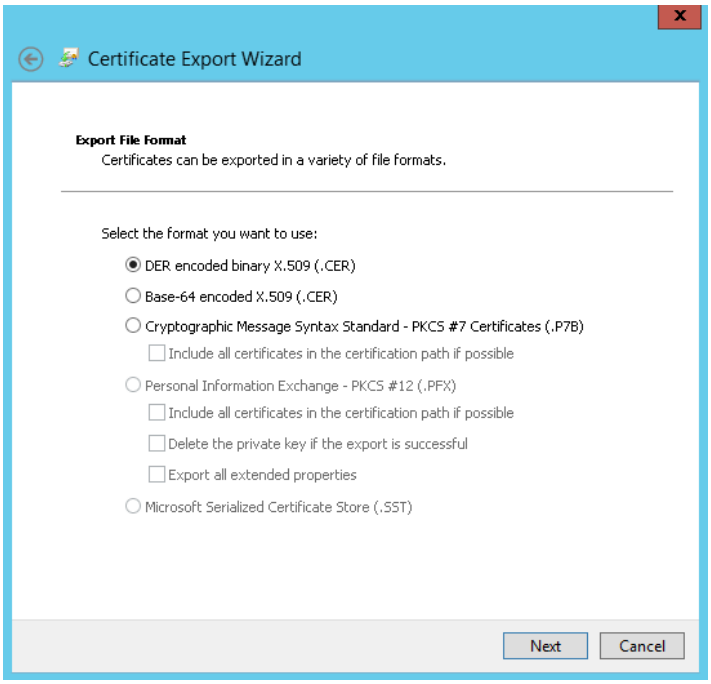

19. Hộp thoại **Certificate**, qua tab **Details**, chọn **Copy to File**.



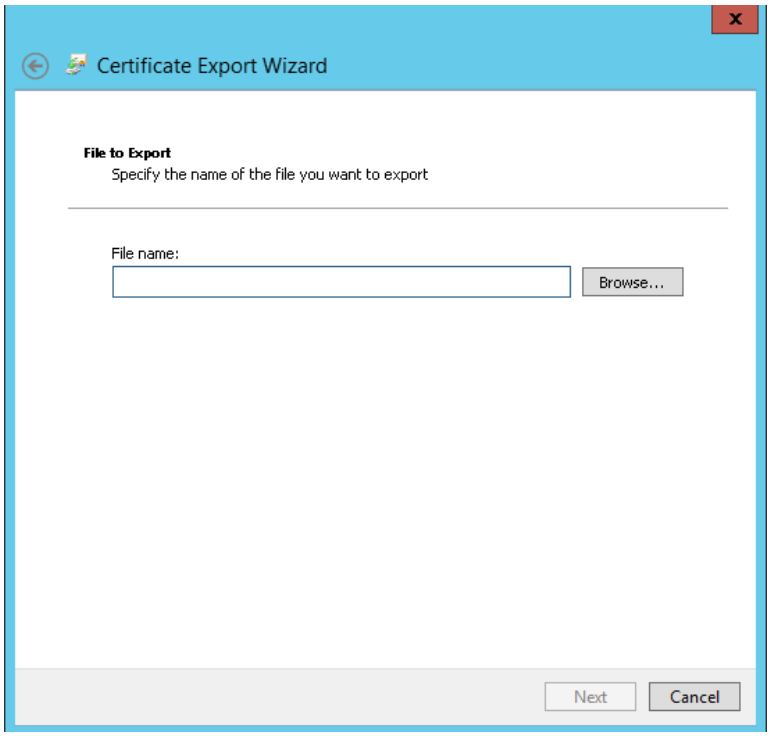
20. Cửa sổ **Certificate Export Wizard Welcome**, chọn **Next**.



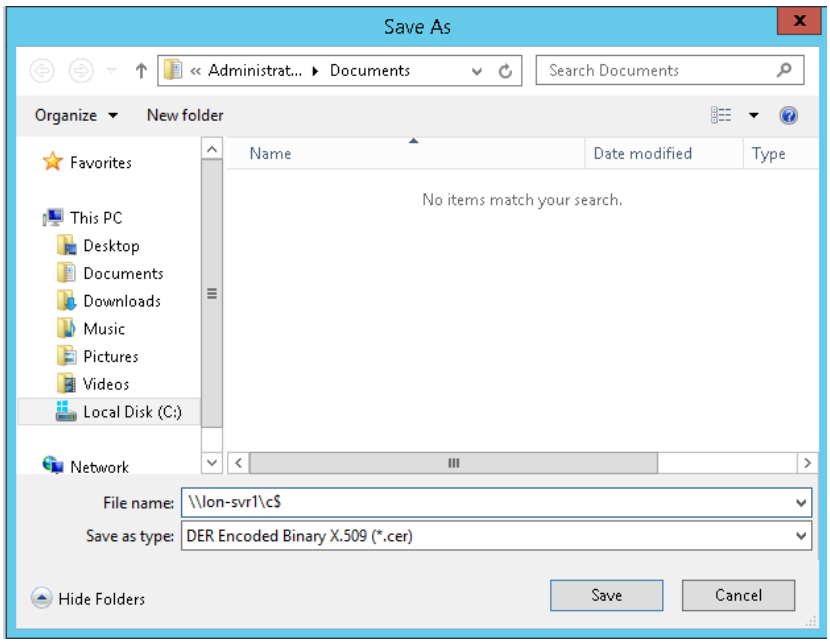

21. Cửa sổ **Export File Format**, chọn **DER encoded binary X.509 (.CER)**, chọn **Next**.



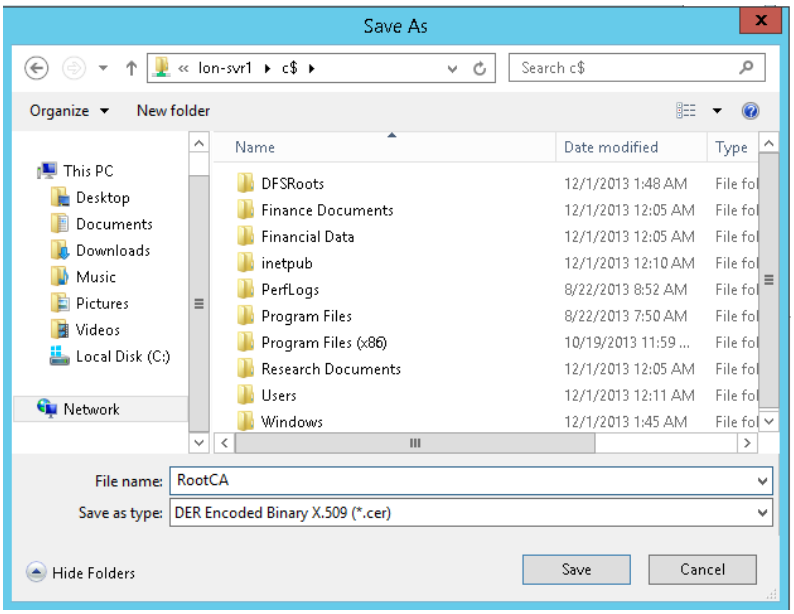
22. Cửa sổ **File to Export**, chọn **Browse**.



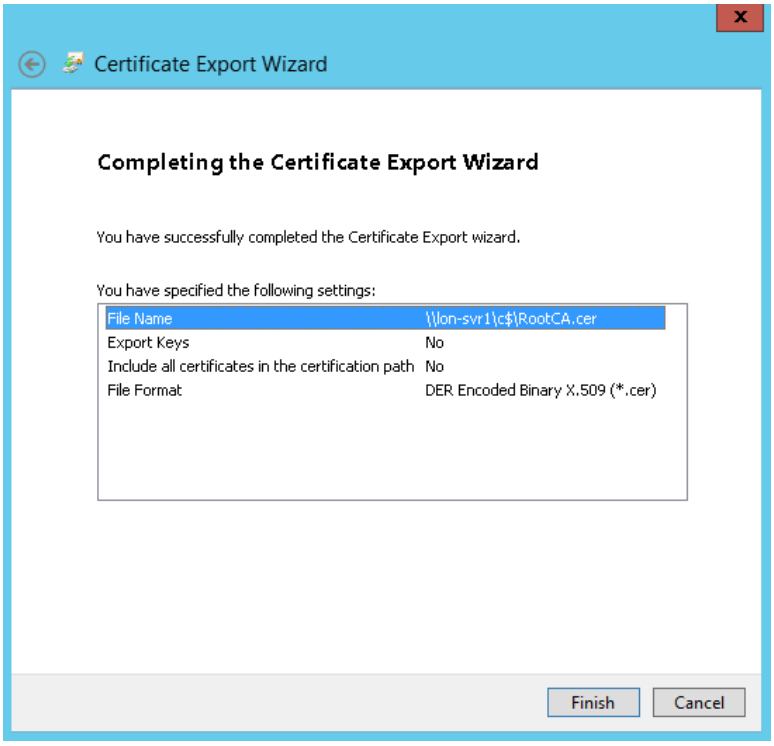

23. Trong ô **File name** text box, nhập **\\lon-svr1\C$**, và nhấn **Enter**.



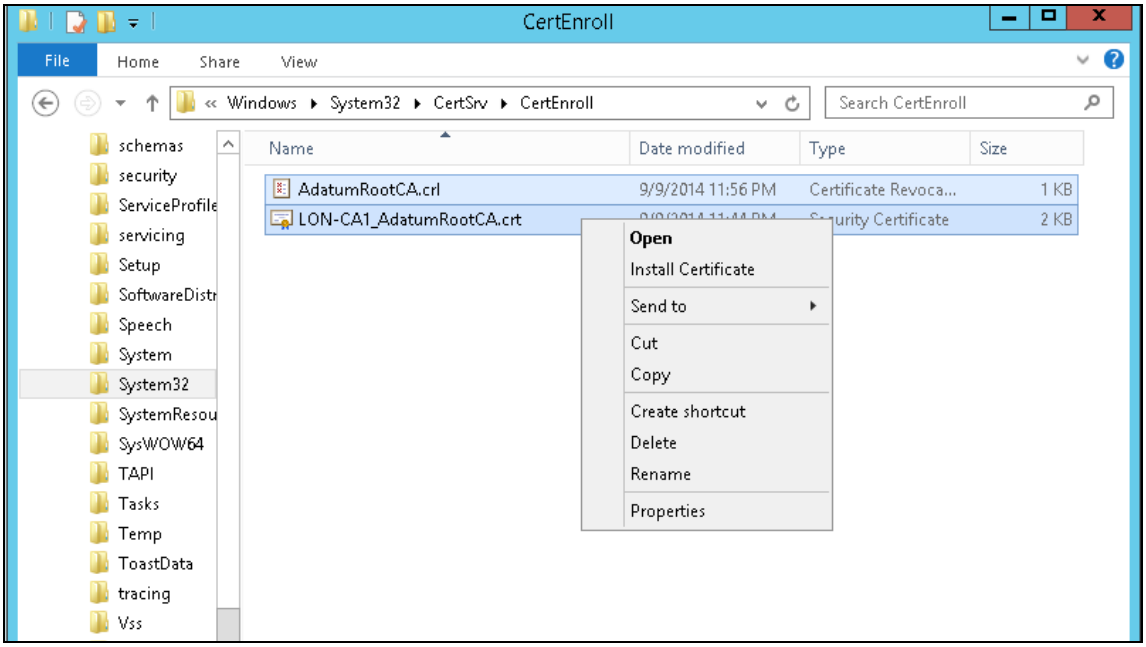
24. Trong ô **File name**, nhập **RootCA**, chọn **Save**, và chọn **Next**.



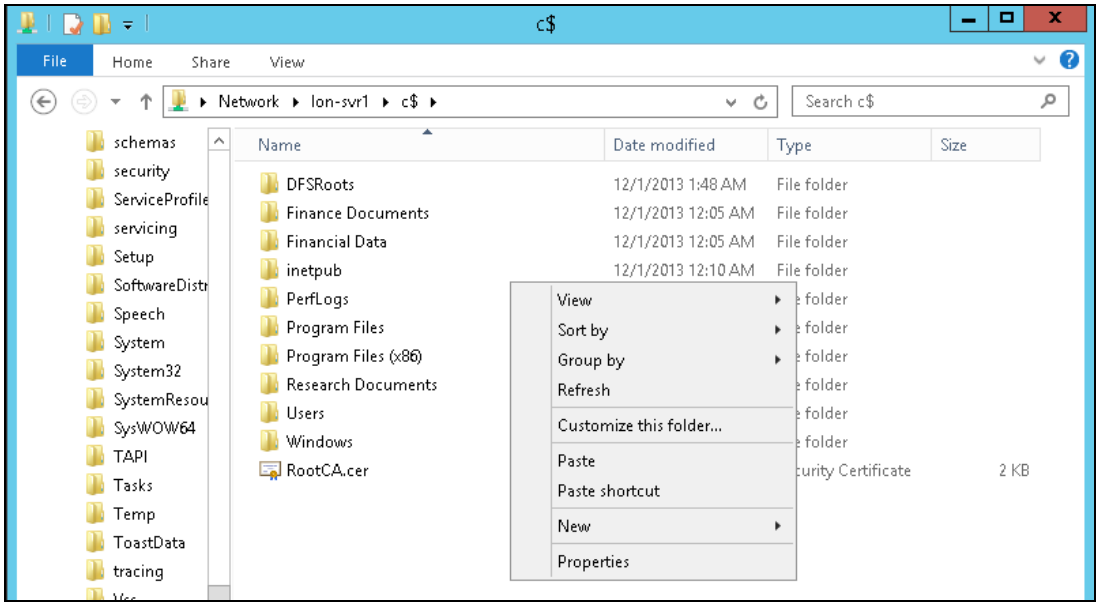

25. Chọn **Finish**, và chọn **OK** 3 lần.



26. Mở File Explorer, vào đường dẫn **C:\Windows\System32\CertSrv\CertEnroll**, copy cả 2 file đang có.




27. Cửa sổ File Explorer, truy cập **\\lon-svr1\C$** . Chuột phải lên khoảng trắng, chọn **Paste**.

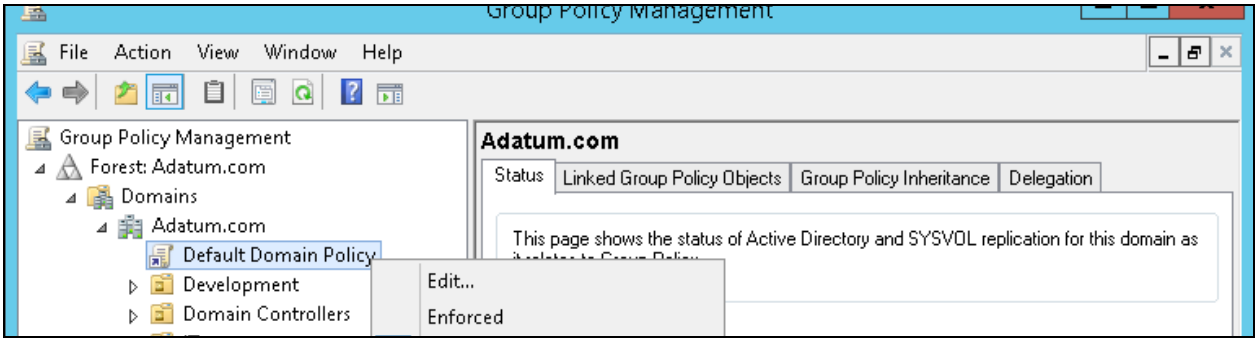



28. Tắt File Explorer.

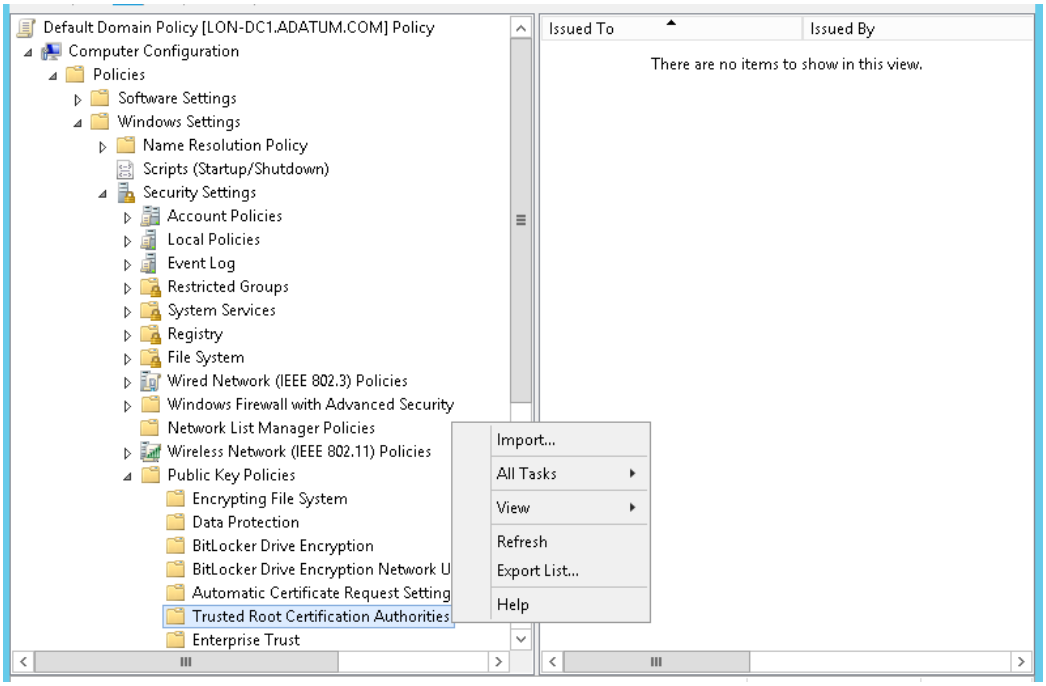
## Bước 3. Công bố Root CA certificate trong domain

1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Group Policy Management**.

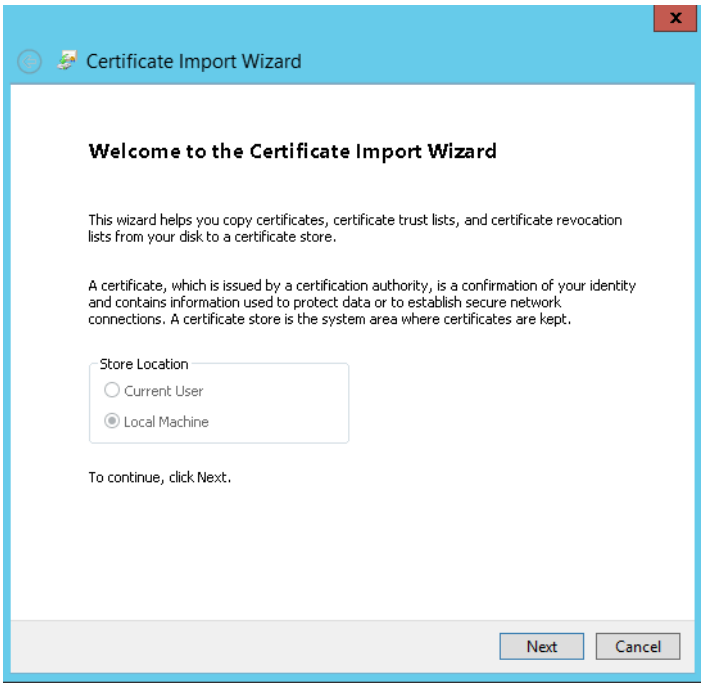
2. Trong cửa sổ **Group Policy Management**, bung **Forest:Adatum.com**, bung **Domains**, bung **Adatum.com**, chuột phải **Default Domain Policy**, và chọn **Edit**.



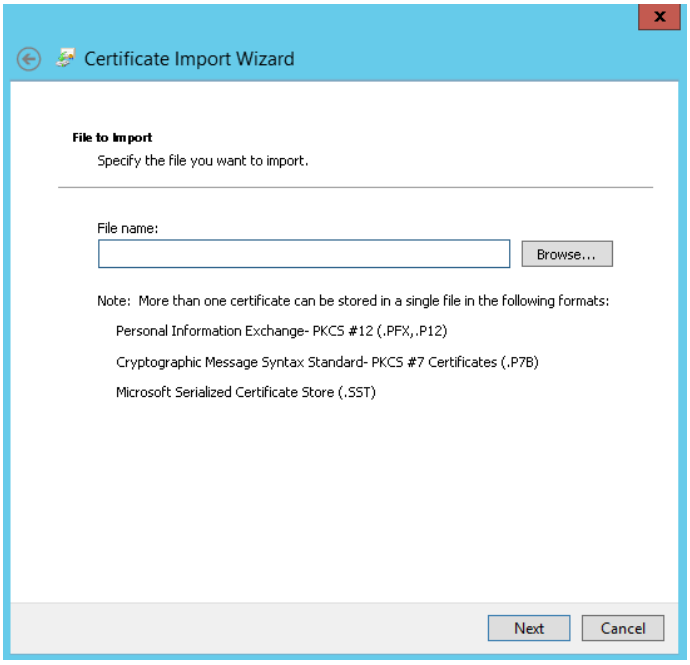

3. Bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Public Key Policies**, chuột phải **Trusted Root Certification Authorities**, và chọn **Import**.



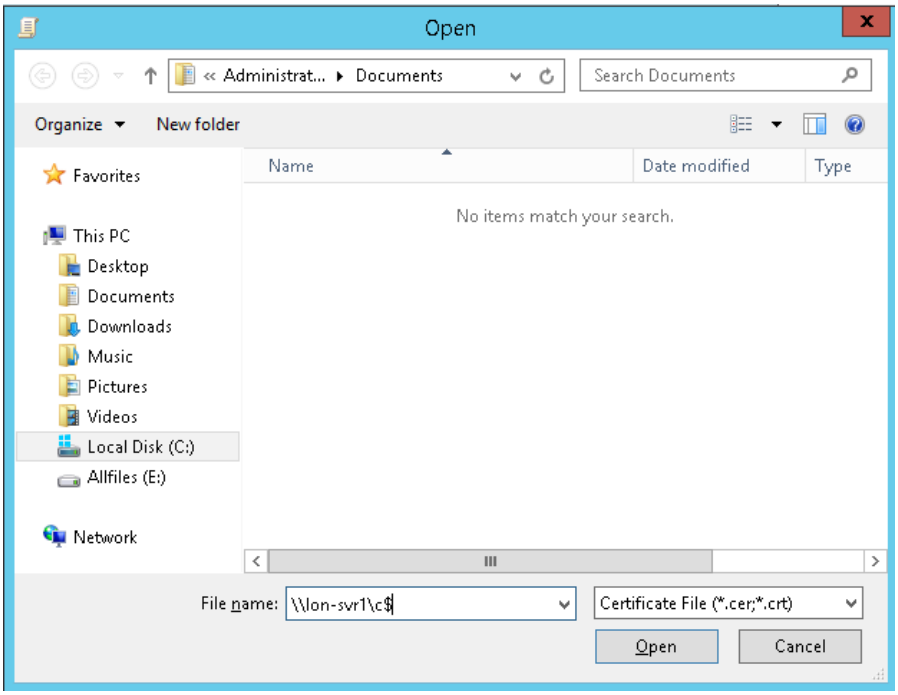
4. Cửa sổ **Welcome to Certificate Import Wizard**, chọn **Next**.



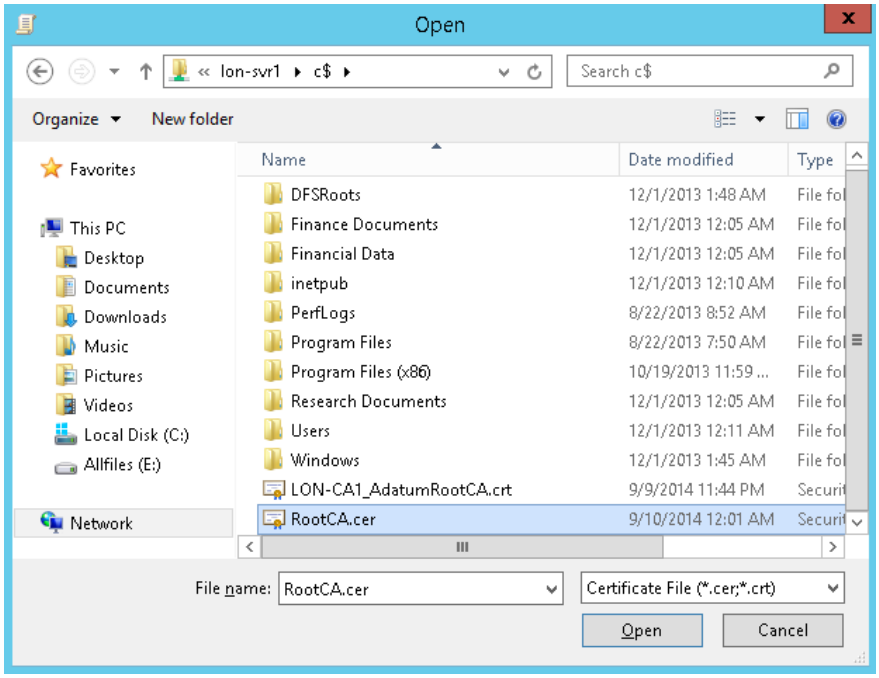

5. Cửa sổ **File to Import**, chọn **Browse**.



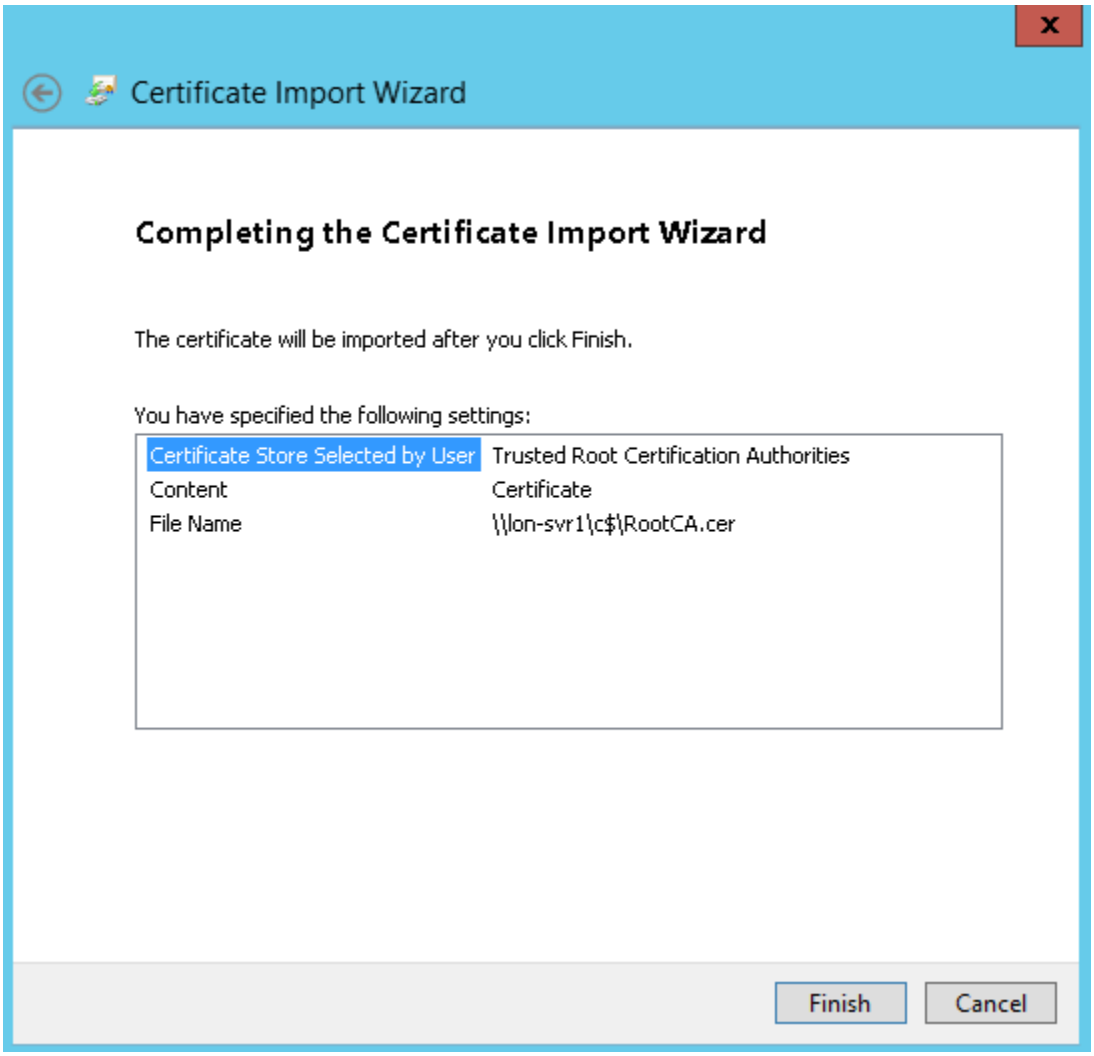
6. Trong ô **File name**, nhập **\\lon-svr1\C$**, và nhấn **Enter**.




7. Chọn file **RootCA.cer**, và chọn **Open**.



8. Chọn **Next** 2 lần, và chọn **Finish**.




9. Hộp thoại **Certificate Import Wizard**, chọn **OK**.

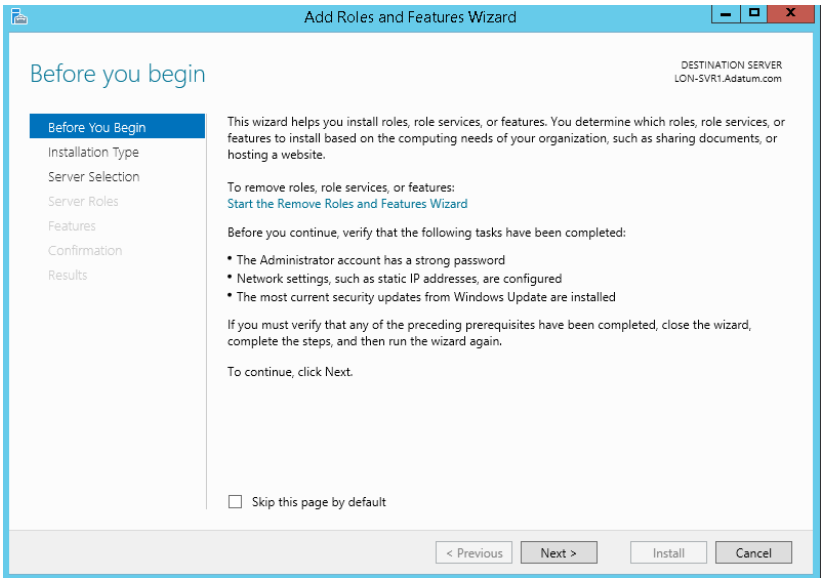
10. Tắt cửa sổ **Group Policy Management Editor** và **Group Policy Management**.

## Bước 4. Cài đặt và cấu hình Subordinate Enterprise CA

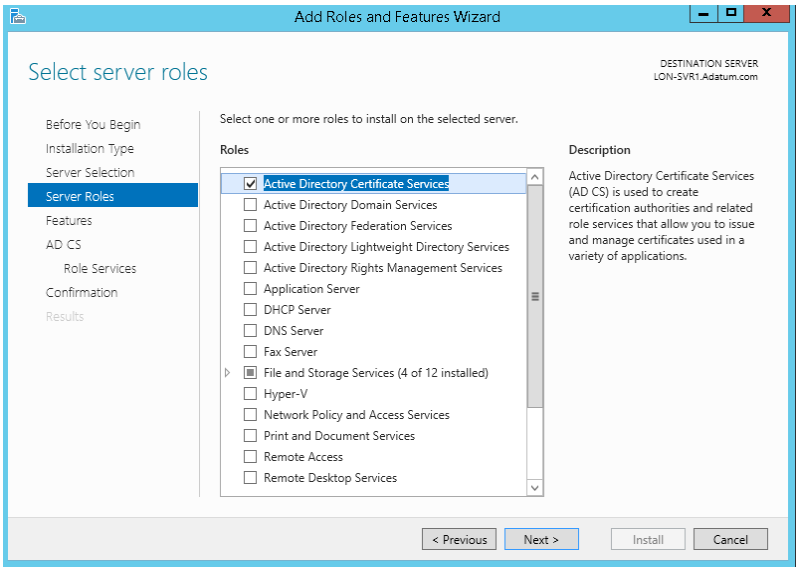
1. Sign in **LON-SVR1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

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

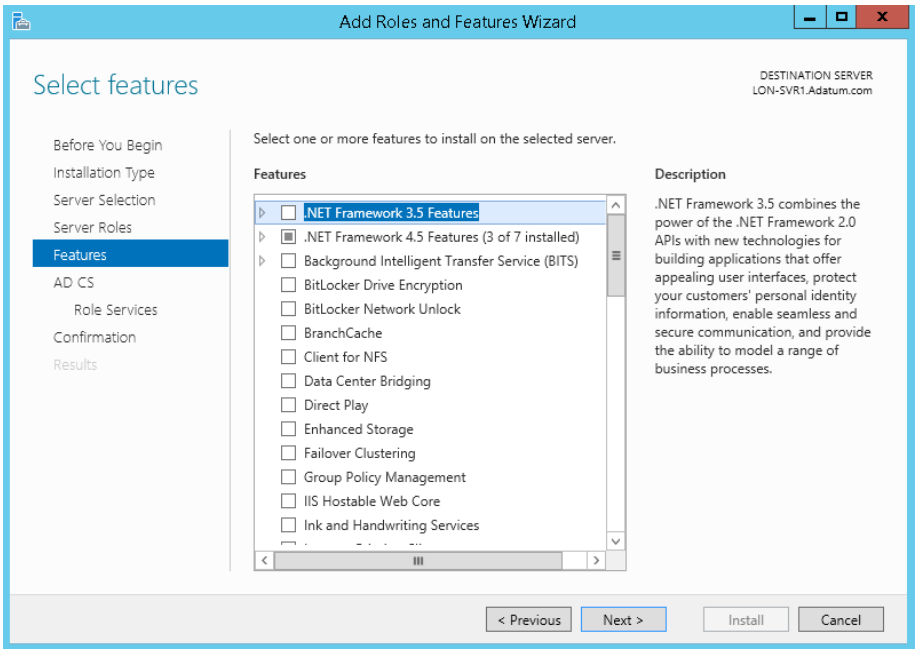
3. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.



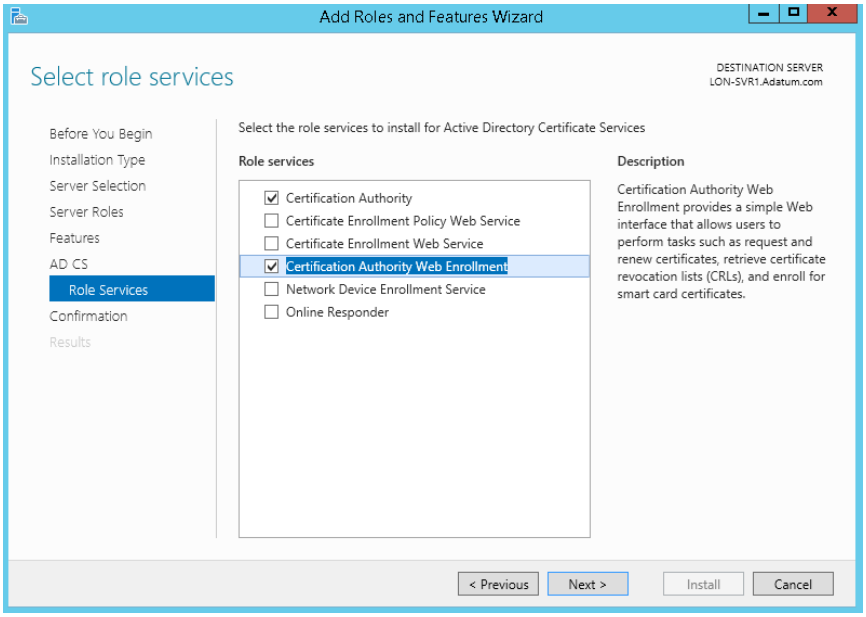

4. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Certificate Services**. Hộp thoại **Add Roles and Features Wizard**, chọn **Add Features**, và chọn **Next**.



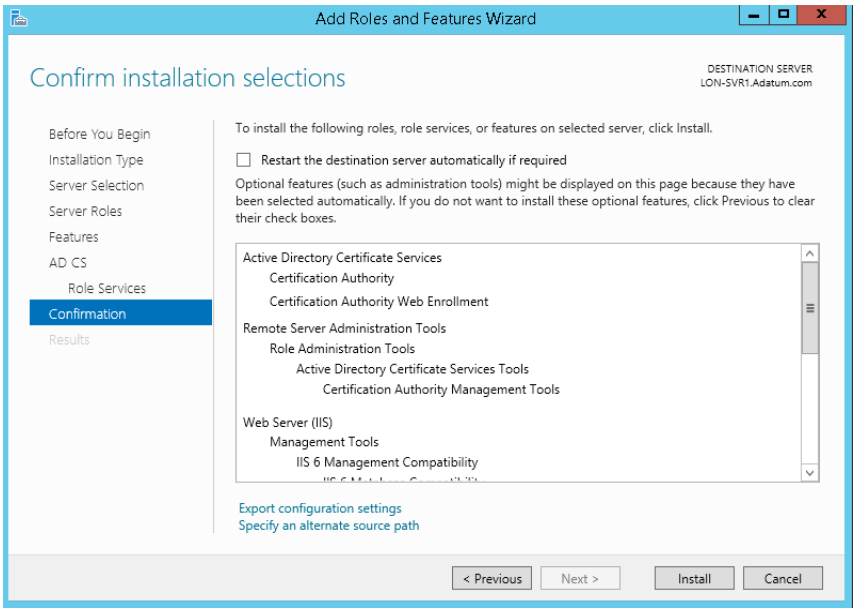
5. Cửa sổ **Select features**, chọn **Next** 2 lần.



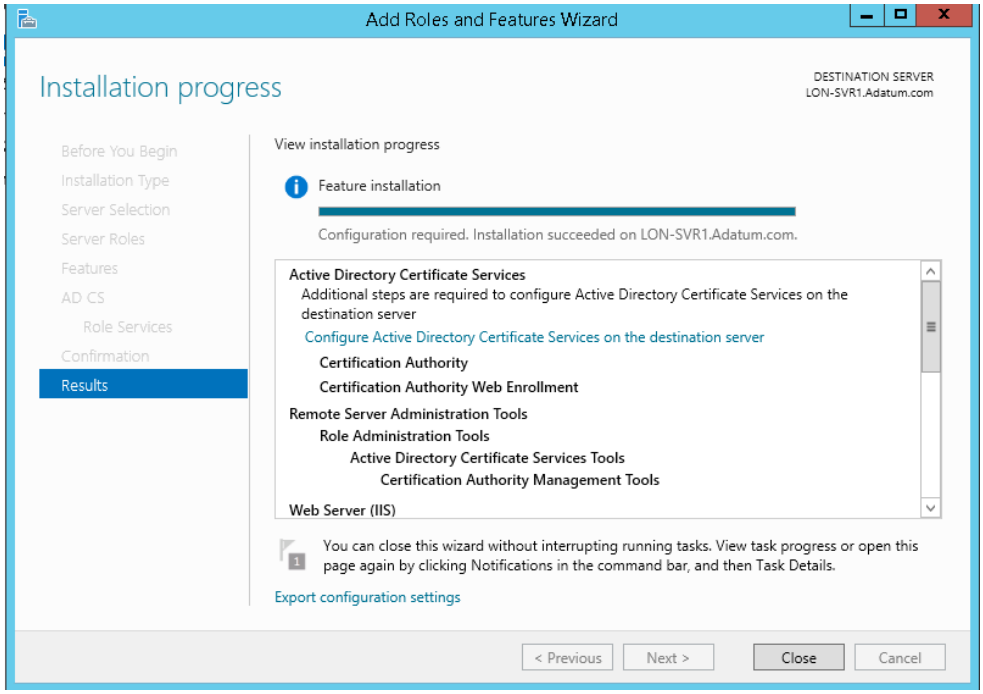

6. Cửa sổ **Select role services**, đánh dấu chọn 2 ô **Certification Authority**, và **Certification Authority Web Enrollment**. Hộp thoại **Add Roles and Features Wizard**, chọn **Add Features**, và chọn **Next**.



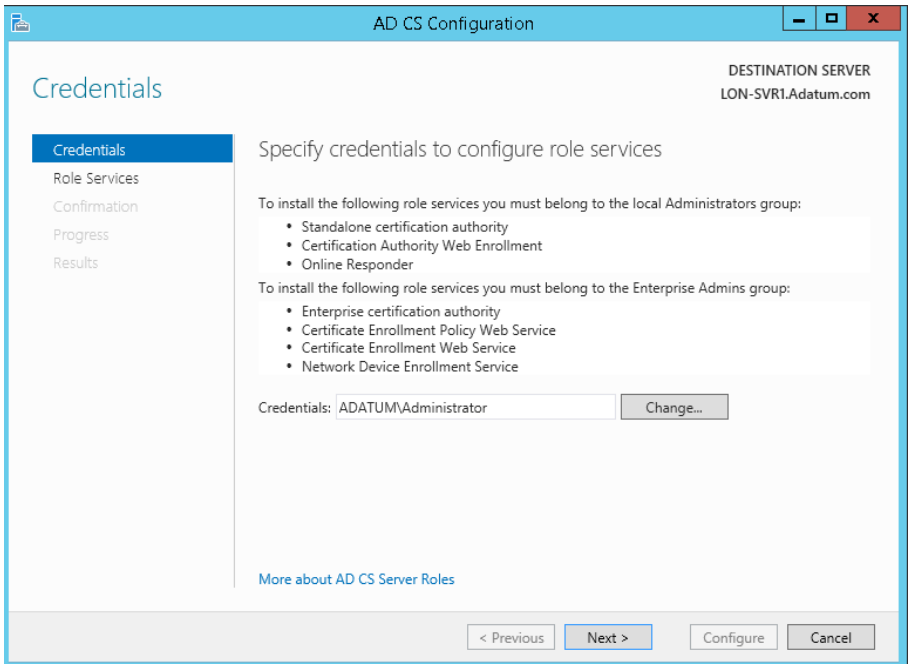
7. Cửa sổ **Confirm installation selections**, chọn **Install**.



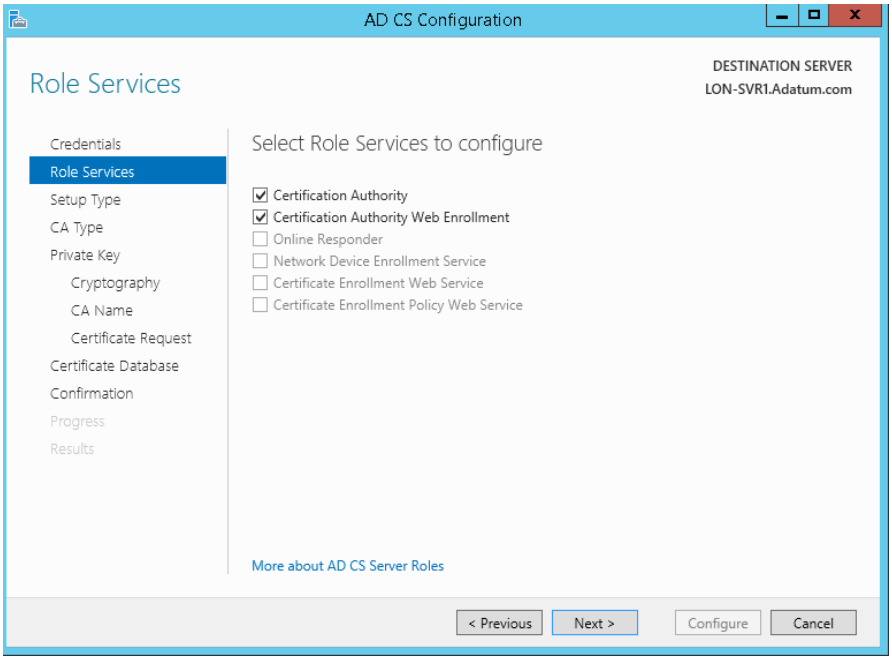

8. Cửa sổ **Installation progress**, sau khi cài đặt thành công, chọn **Configure Active Directory Certificate Services on the destination server**.



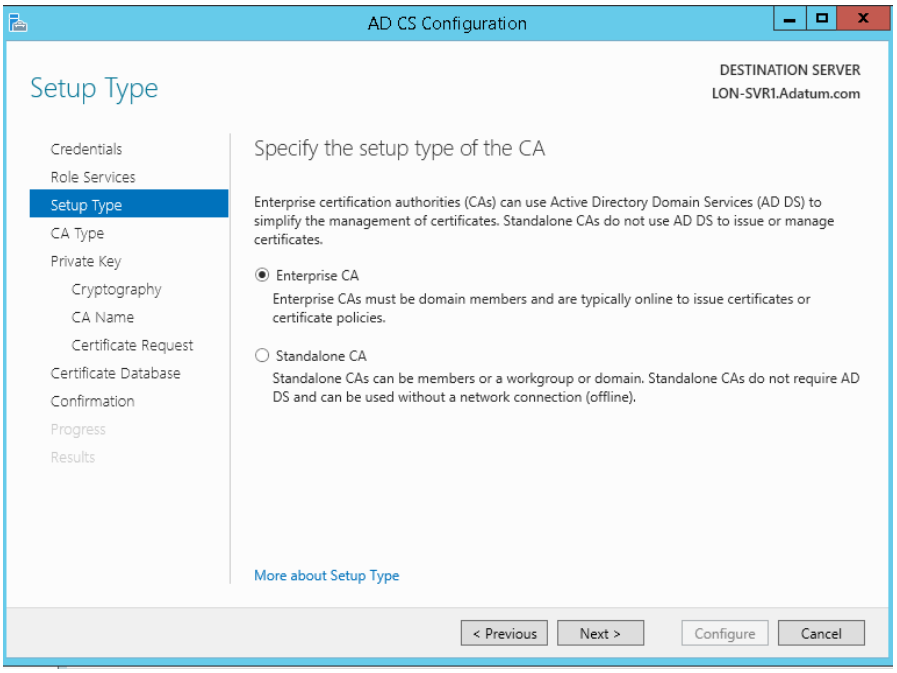
9. Cửa sổ **Credentials**, chọn **Next**.



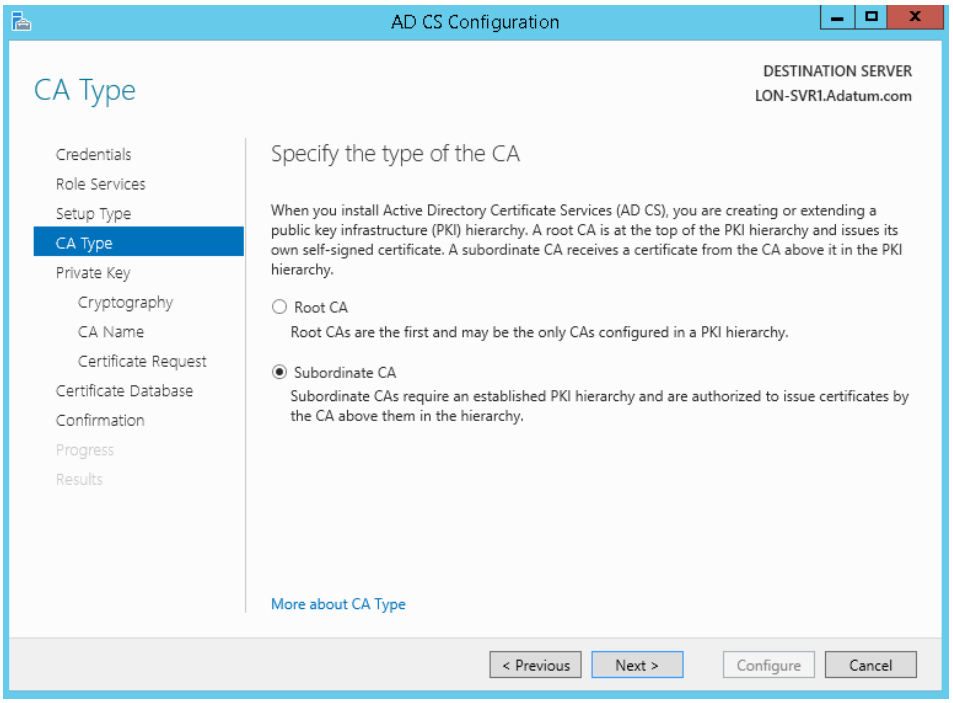

10. Cửa sổ **Role Services**, đánh dấu chọn 2 ô **Certification Authority** và **Certification Authority Web Enrollment**, và chọn **Next**.



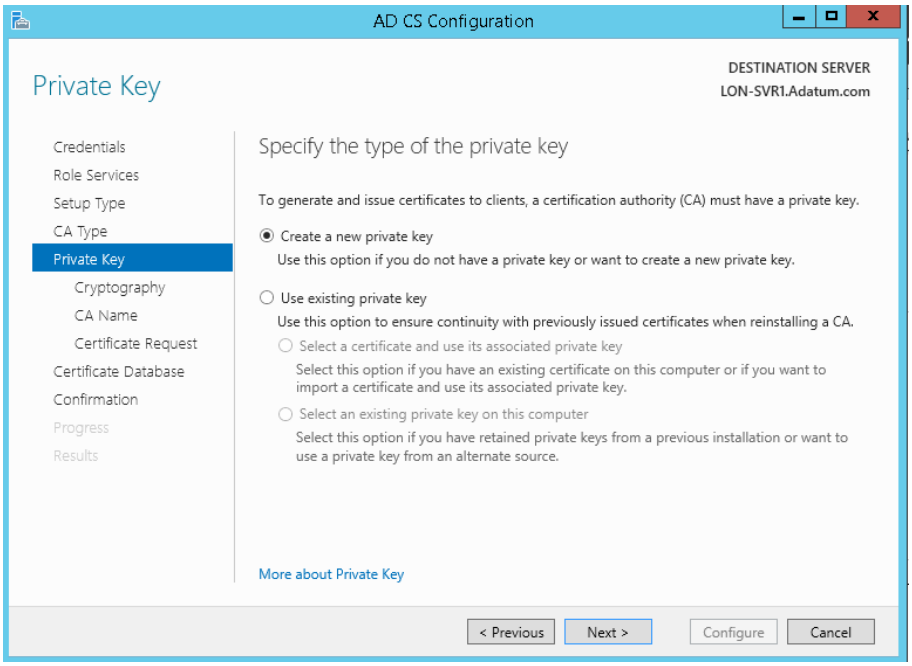
11. Cửa sổ **Setup Type**, chọn **Enterprise CA**, chọn **Next**.



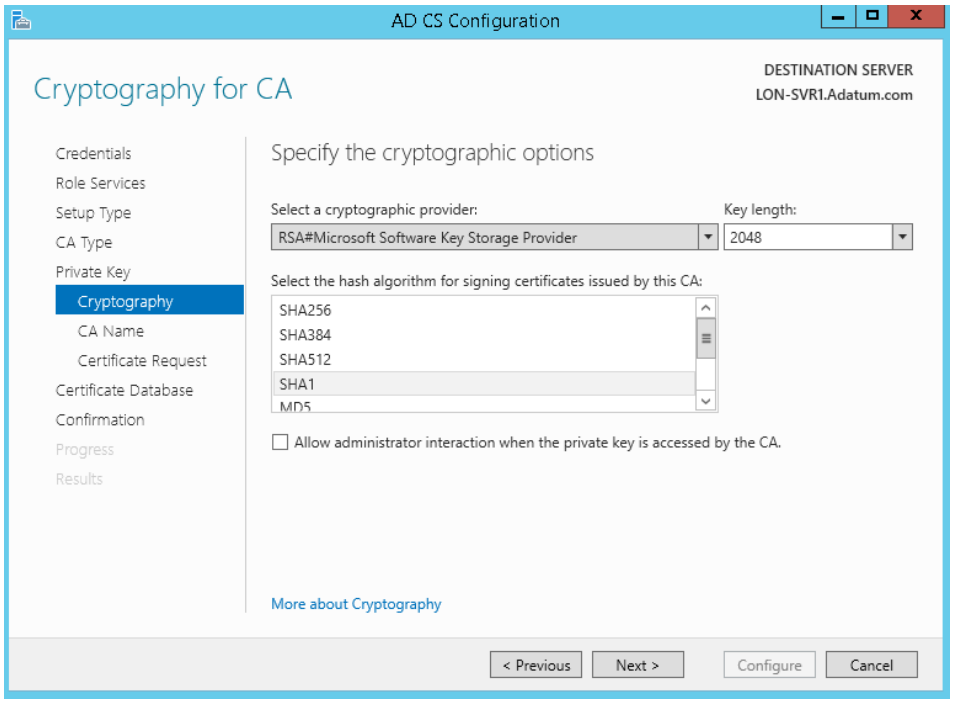

12. Cửa sổ **CA Type**, chọn **Subordinate CA**, chọn **Next**.



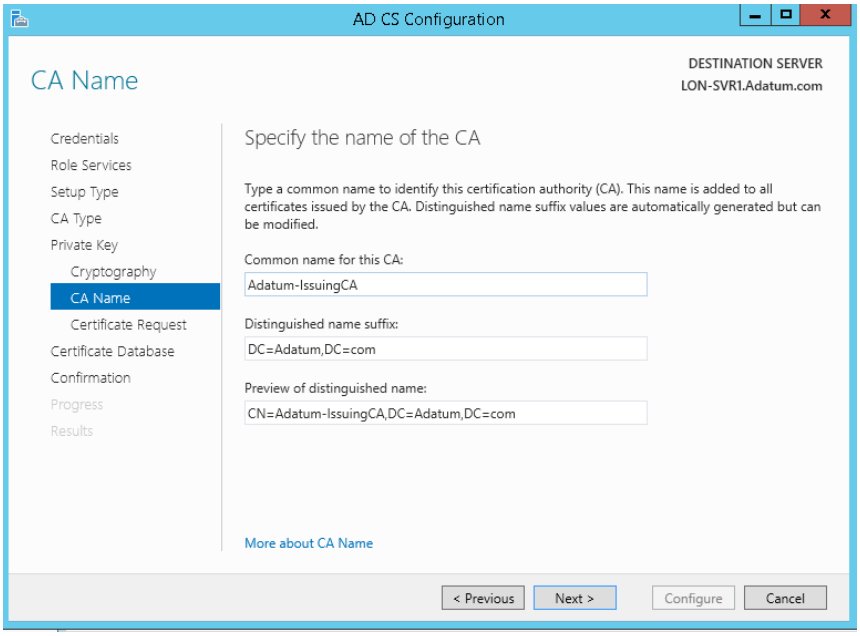
13. Cửa sổ **Private Key**, chọn **Create a new private key**, chọn **Next**.



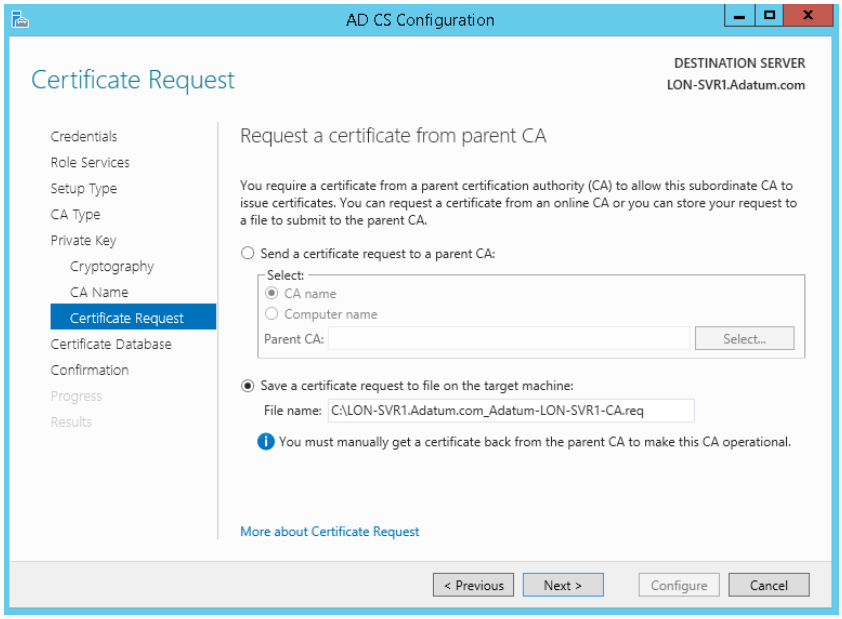

14. Cửa sổ **Cryptography for CA**, chọn **Next**.



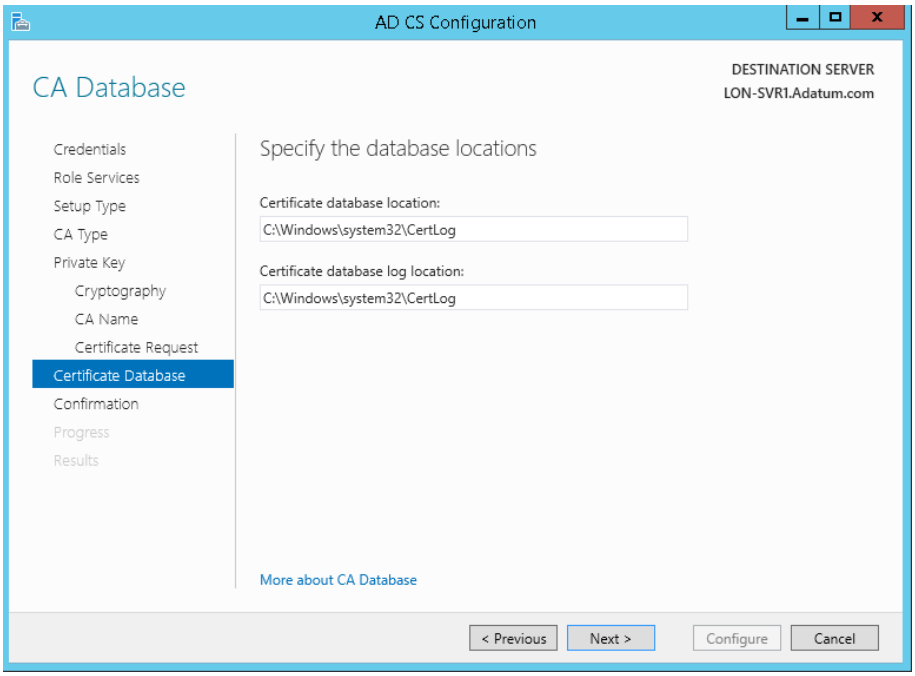
15. Cửa sổ **CA Name**, trong ô **Common name for this CA**, nhập **Adatum-IssuingCA**, chọn **Next**.



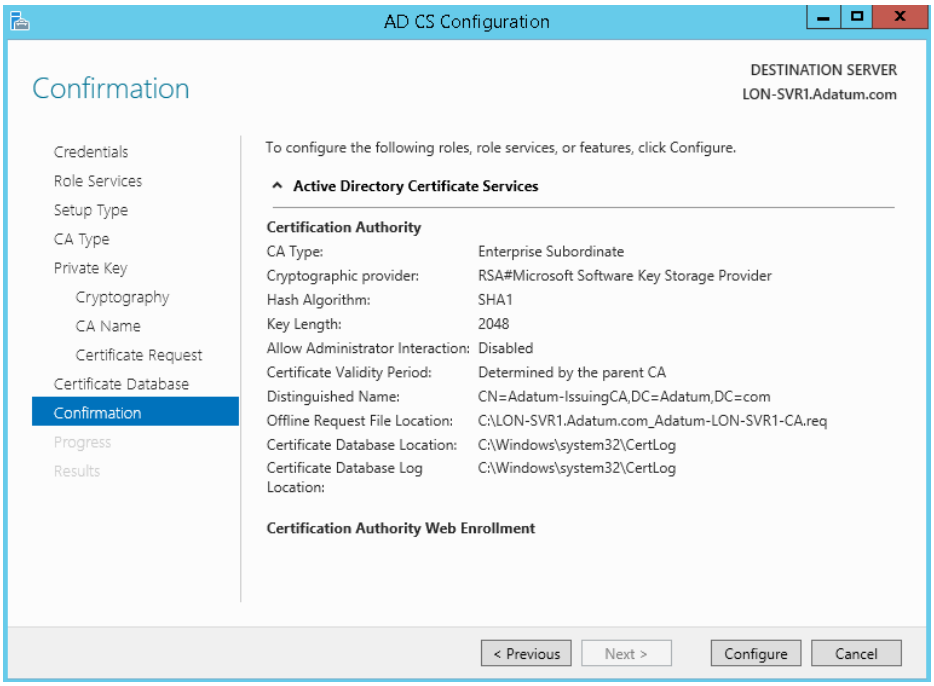

16. Cửa sổ **Certificate Request**, chọn **Save a certificate request to file on the target machine**, chọn **Next**.



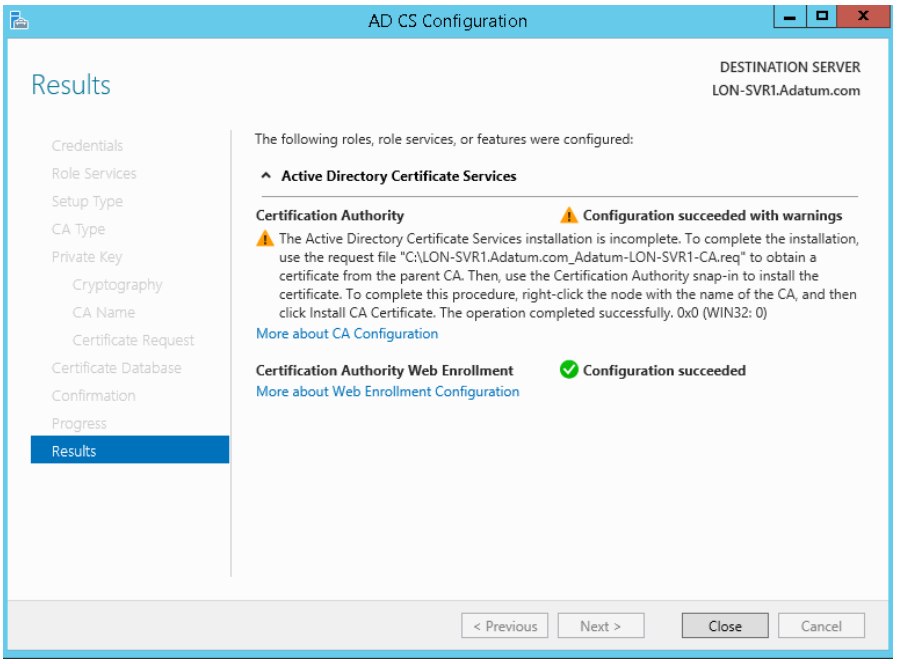
17. Cửa sổ **CA Database**, chọn **Next**.




18. Cửa sổ **Confirmation**, chọn **Configure**.

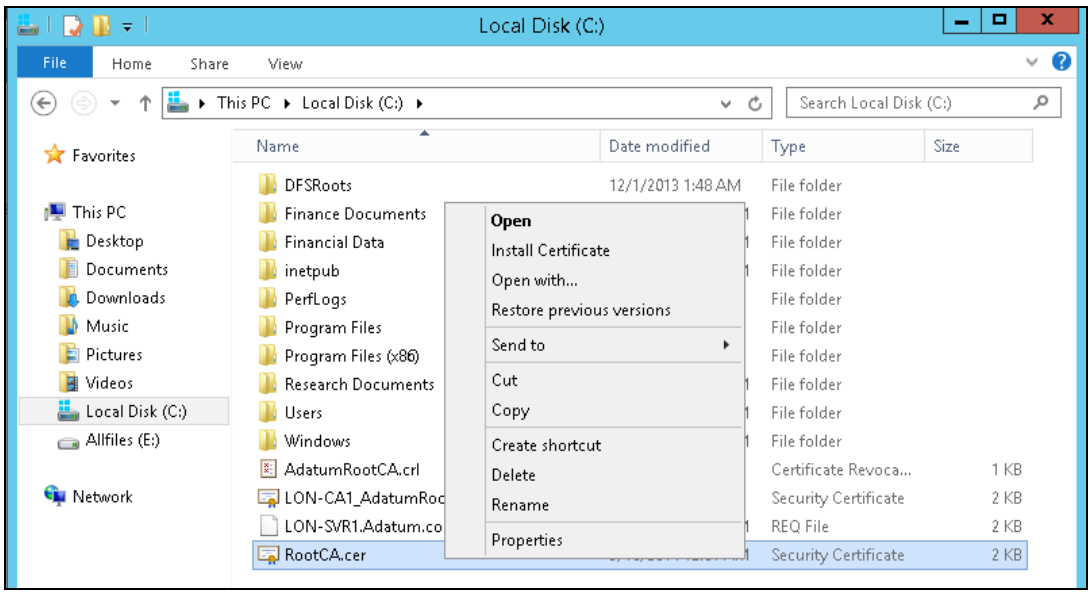


19. Cửa sổ **Results**, chọn **Close** 2 lần.

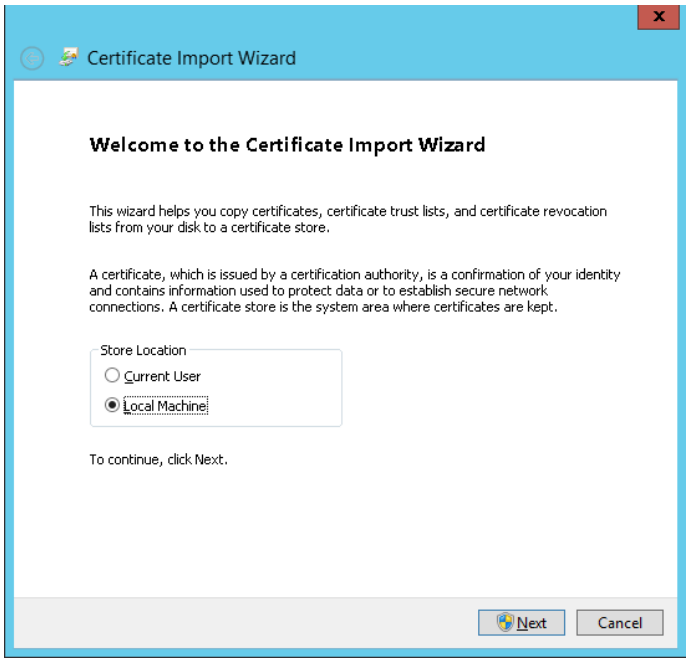



## Bước 5. Cấu hình Subordinate trust

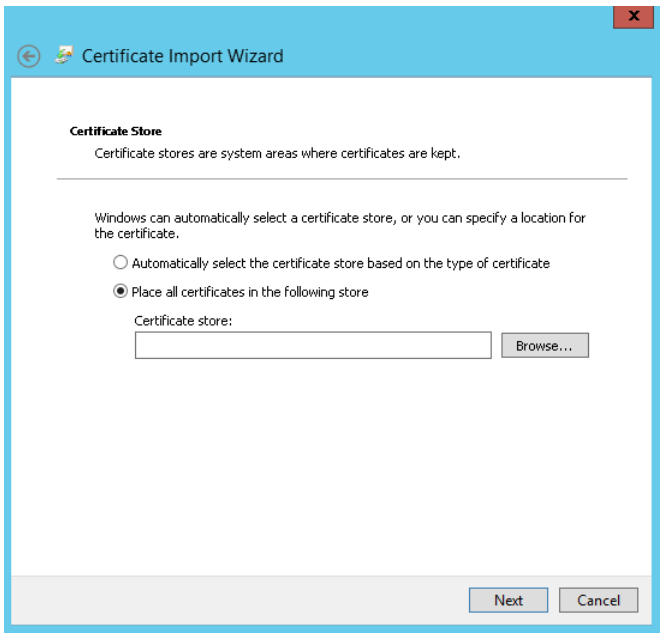
1. Trên máy **LON-SVR1**, mở **File Explorer**, vào **Local Disk (C:)**. Chuột phải lên file **RootCA.cer**, chọn **Install Certificate**.



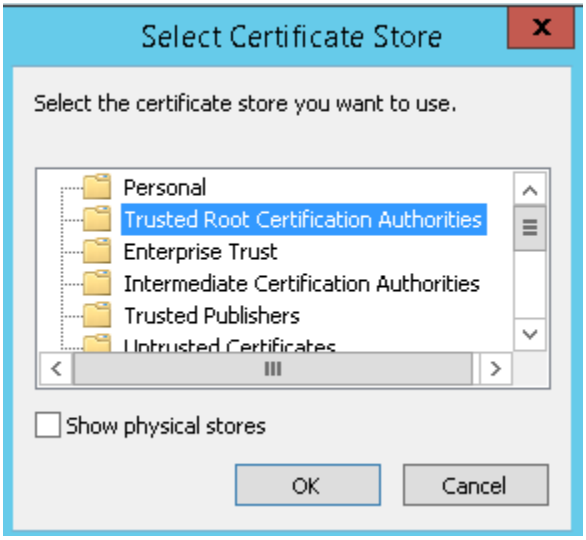
2. Trong cửa sổ **Certificate Import Wizard**, chọn **Local Machine**, và chọn **Next**.



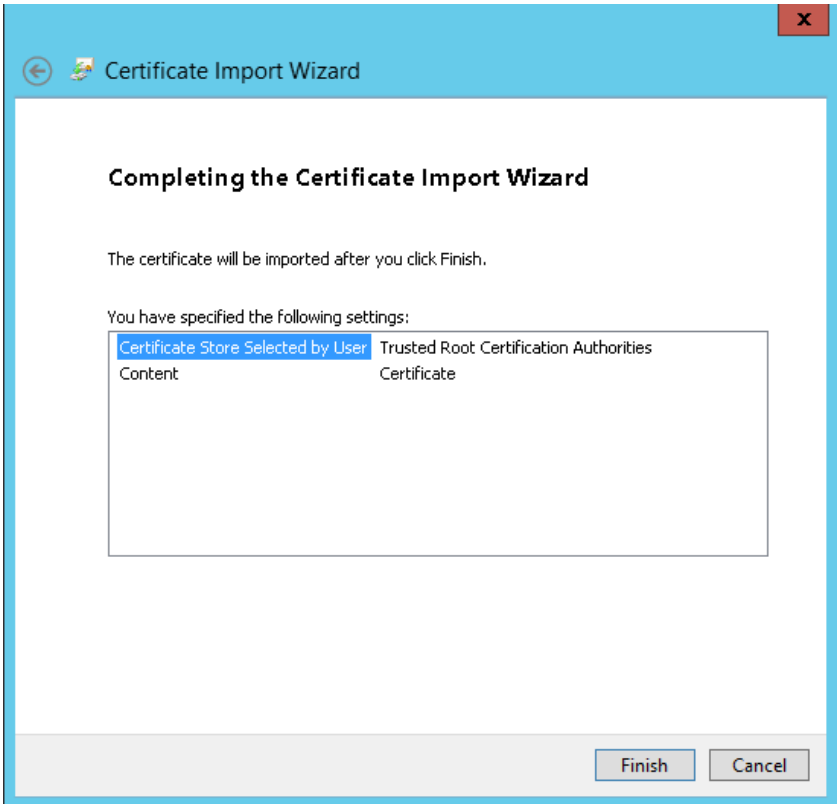

3. Cửa sổ **Certificate Store**, chọn **Place all certificates in the following store**, và chọn **Browse**.



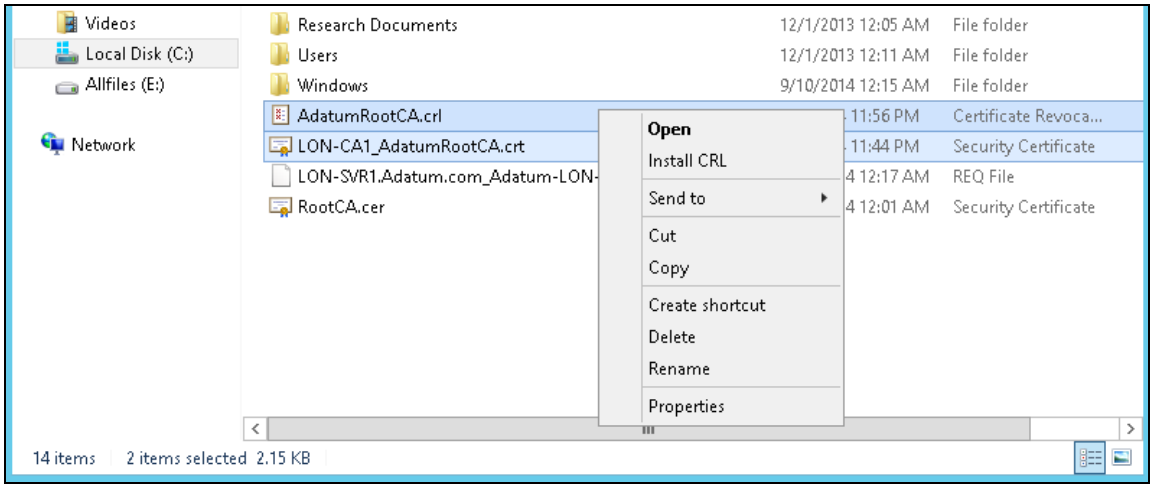
4. Chọn **Trusted Root Certification Authorities**, và chọn **OK**, và chọn **Next**



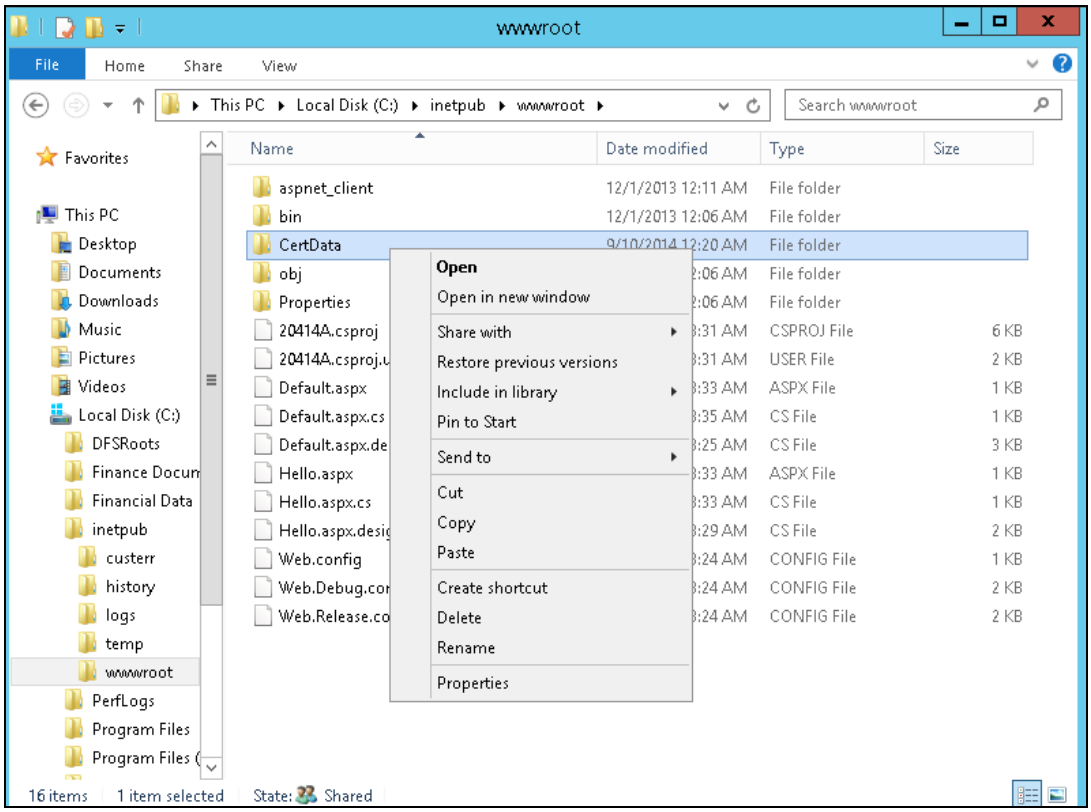

5. Chọn **Next**, và chọn **Finish**. Hộp thoại **Certificate Import Wizard**, chọn **OK**.



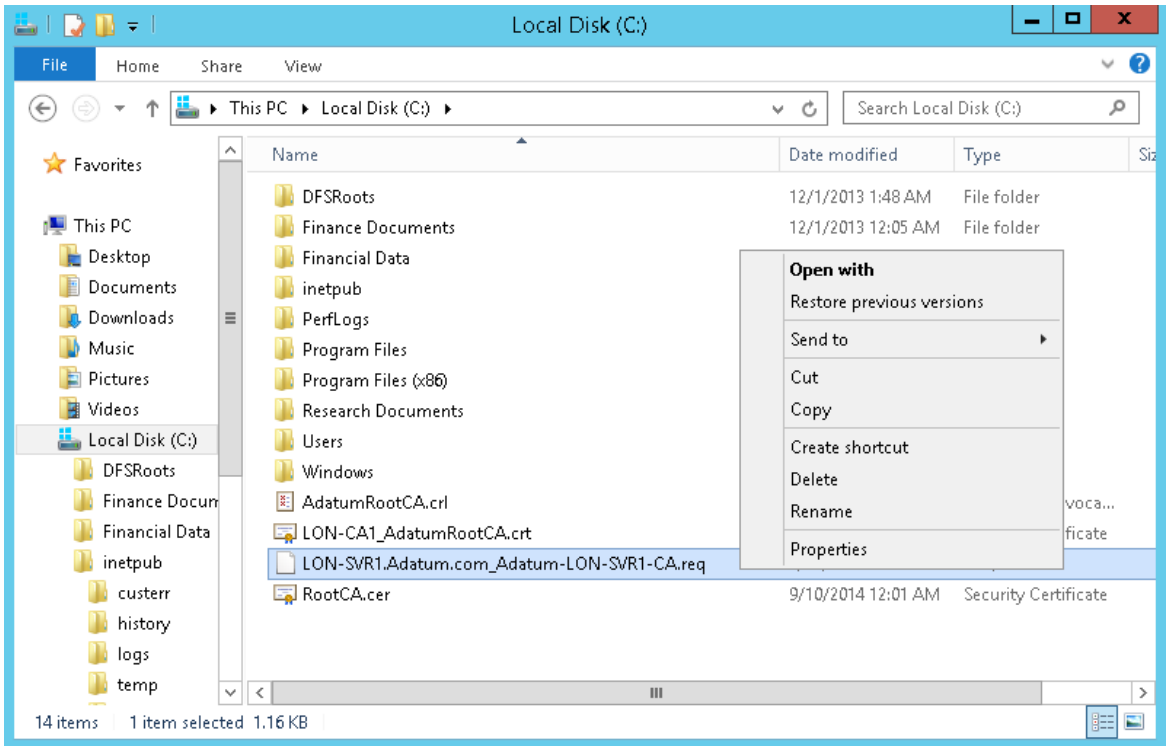
6. Trong **File Explorer**, copy 2 file **AdatumRootCA.crl** và **LON-CA1_AdatumRootCA.crt**.



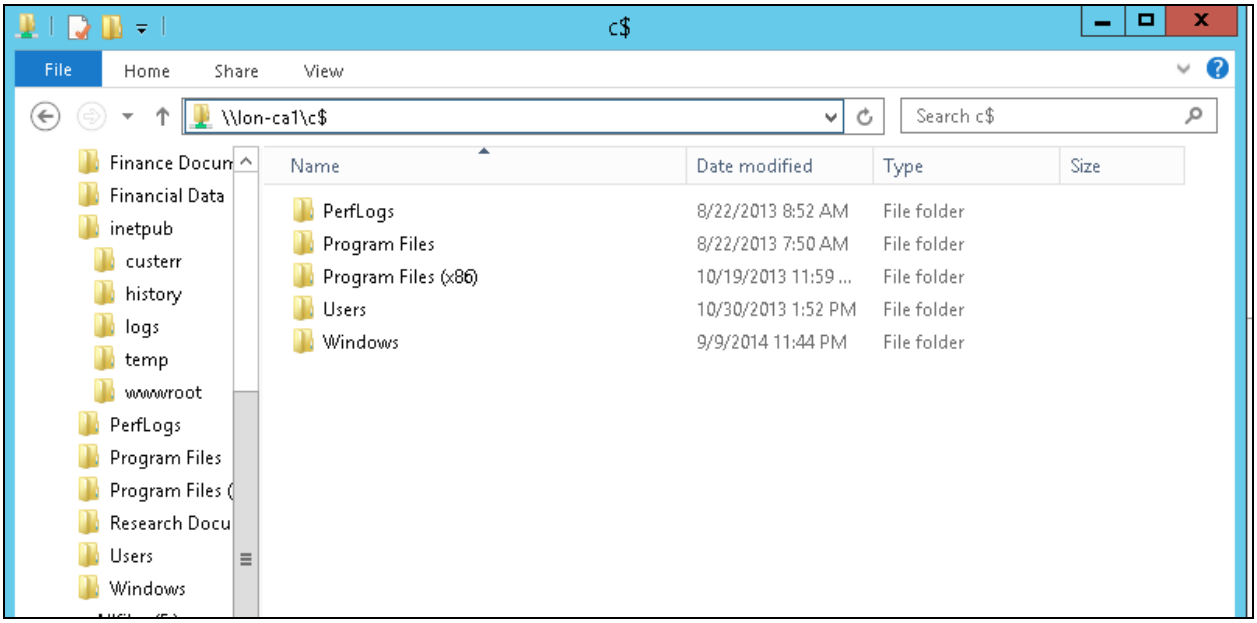

7. Vào đường dẫn C:**inetpub\wwwroot**. Tạo folder mới, đặt tên **CertData**. Chép 2 file vừa copy ở bước trên vào folder **CertData**.



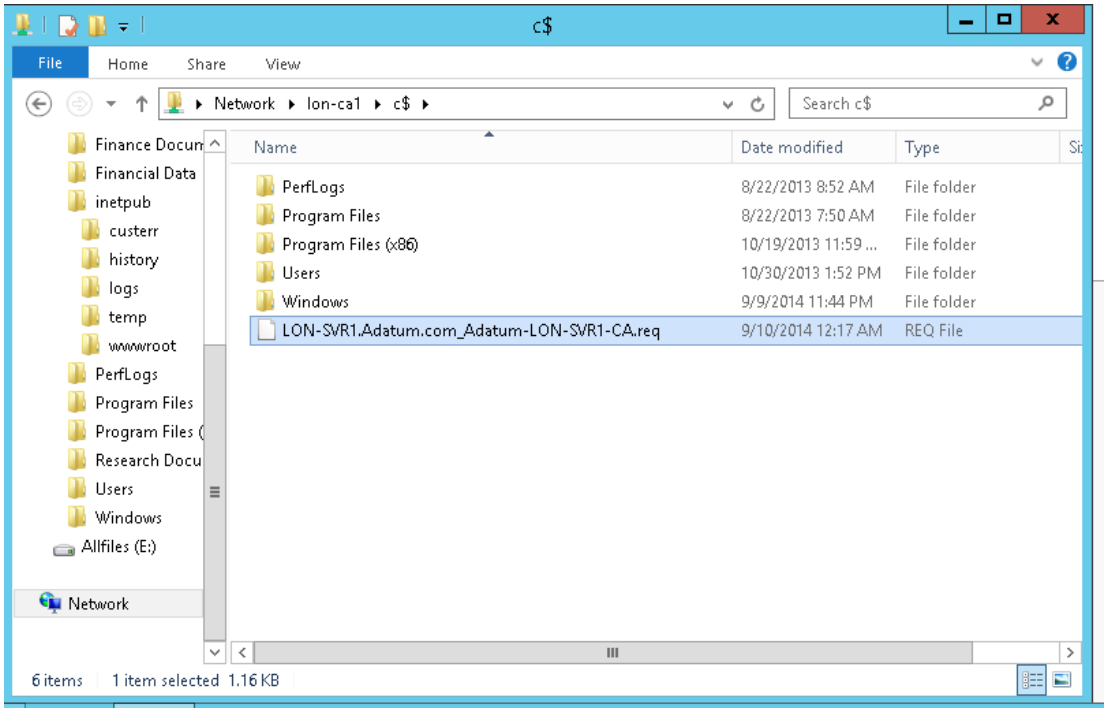
8. Quay lại **Local Disk (C:)**. Copy file **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req**




9. Trong thanh address của File Explorer, truy cập **\\LON-CA1\C$**

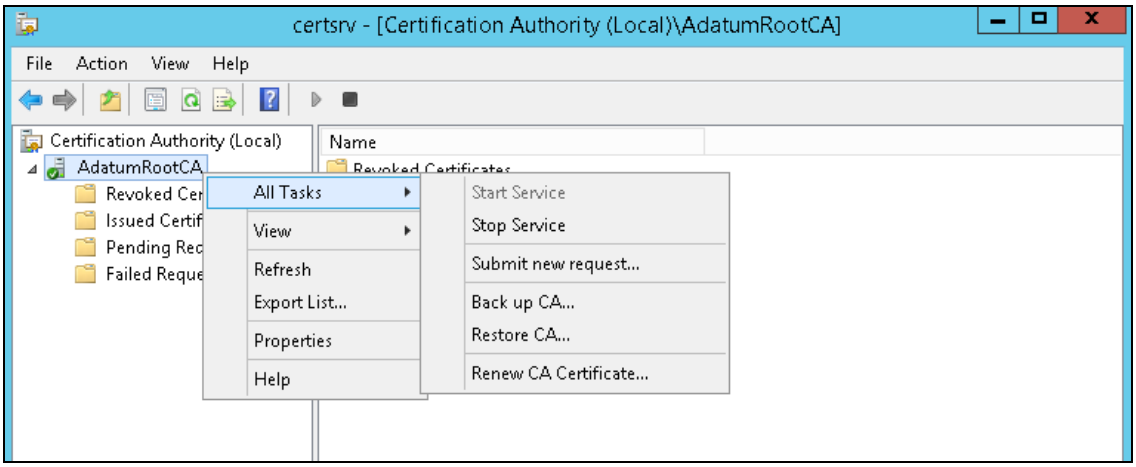


10. Trong File Explorer, chuột phải khoảng trắng, chọn **Paste**. Đảm bảo file yêu cầu được chép qua máy **LON-CA1.**

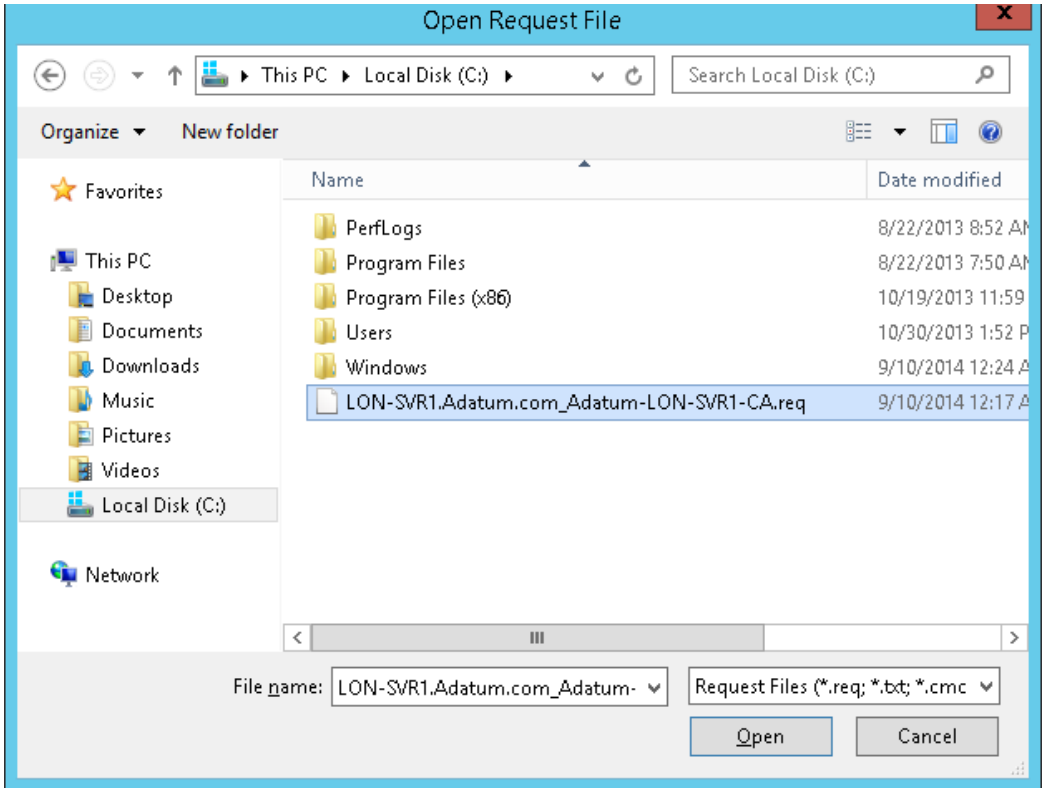



11. Qua máy **LON-CA1**.

12. Trong cửa sổ **Certification Authority**, chuột phải **AdatumRootCA**, bung **All Tasks**, chọn **Submit new request**.

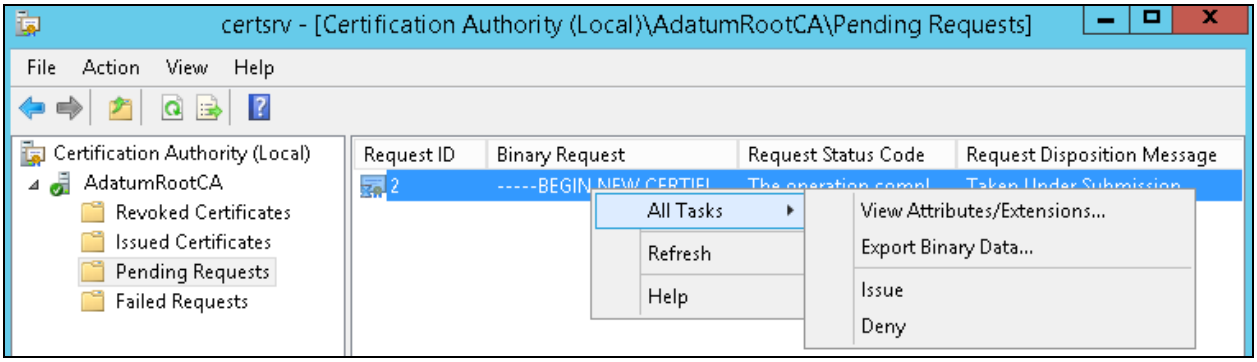


13. Trong hộp thoại **Open Request File**, trỏ đường dẫn vào **Local Disk (C:)**, chọn file **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req**, và chọn **Open**.

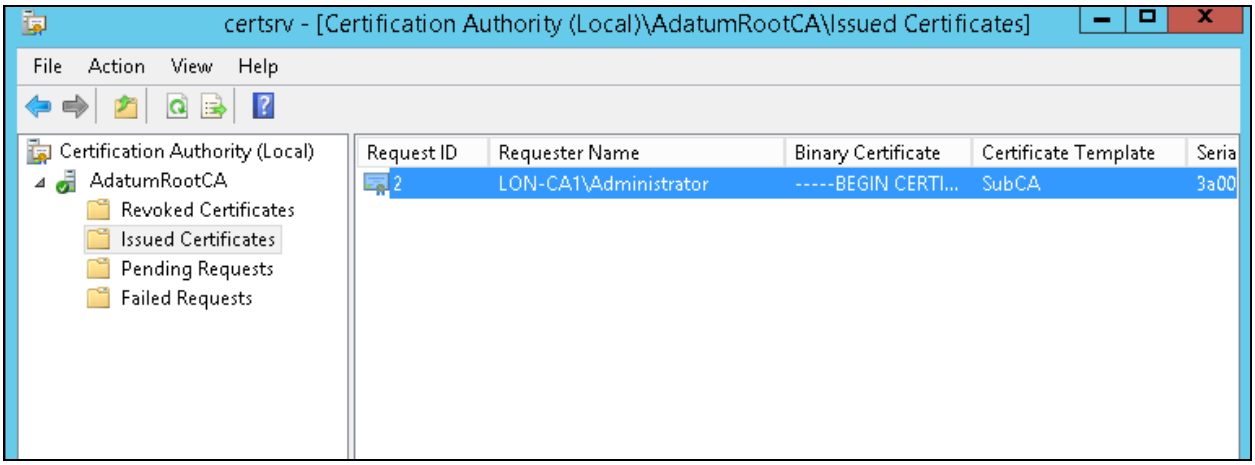



14. Trong cửa sổ **Certification Authority**, bung **AdatumRootCA**, chọn **Pending Requests**. nhấn phím **F5**.

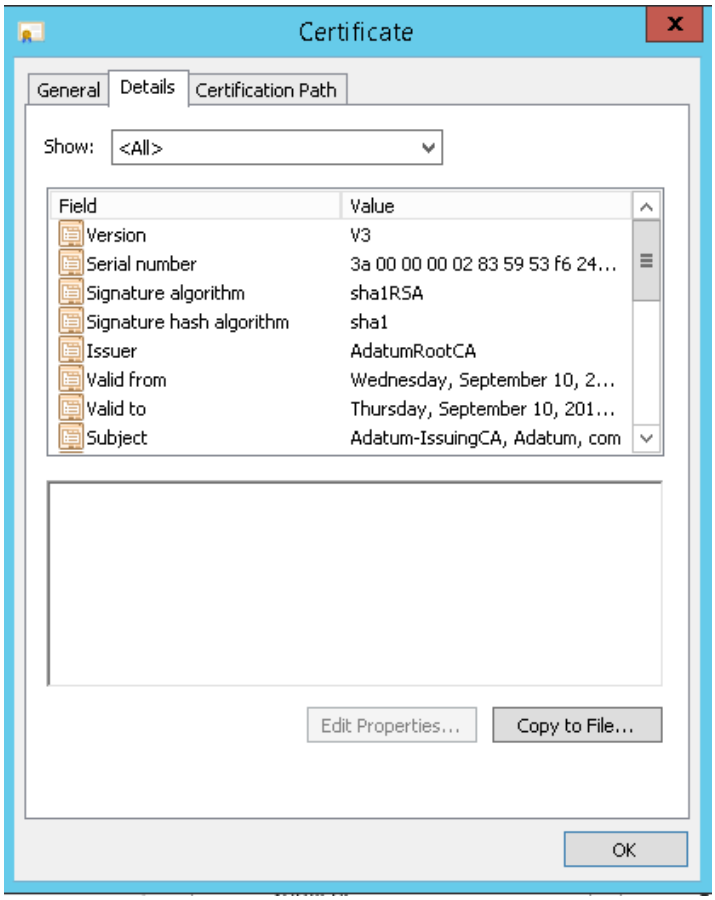
15. Trong mục **Pending Requests**, chuột phải lên file yêu cầu (có ID 2), bung **All Tasks**, và chọn **Issue**.



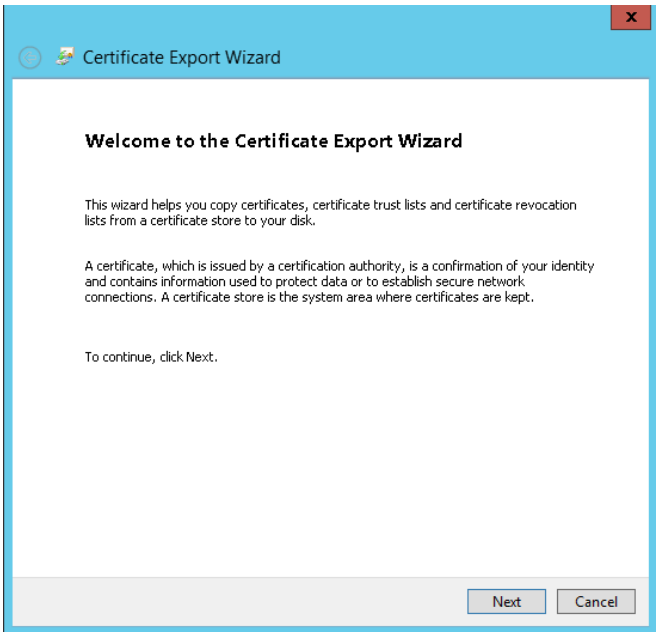
16. Qua mục **Issued Certificates**, nhấp dôi chuột lên certificate đang có (có ID 2).



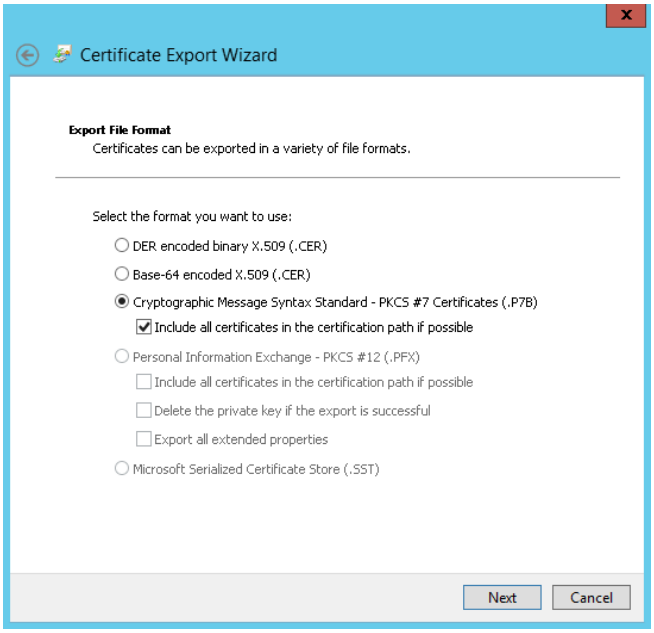

17. Qua tab **Details**, chọn **Copy to File**.



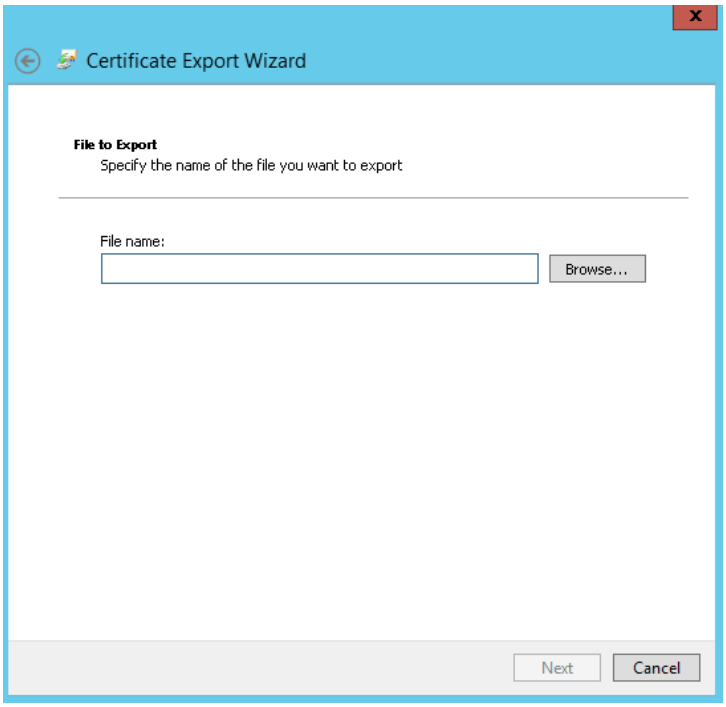
18. Cửa sổ **Welcome**, chọn **Next**.



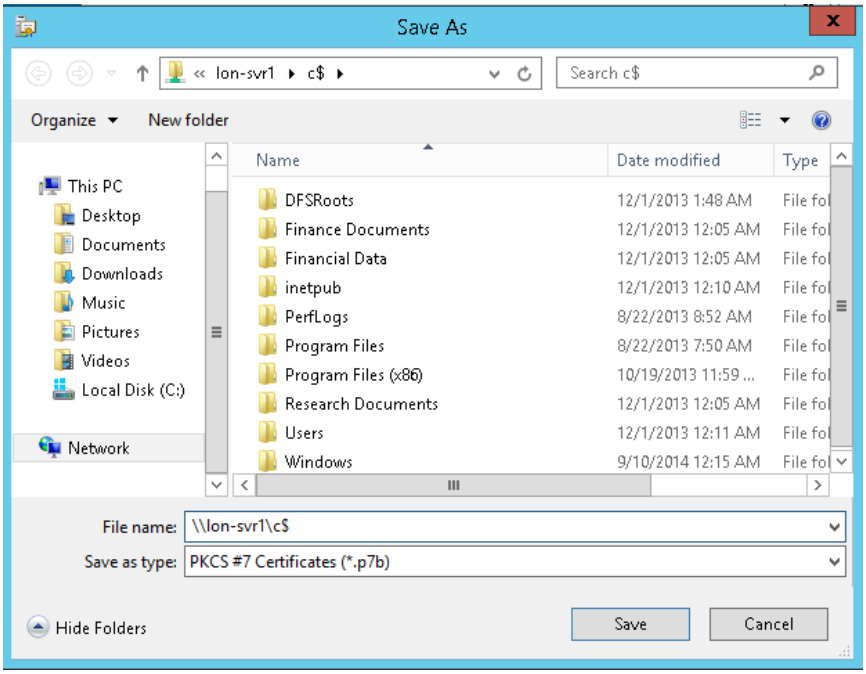

19. Cửa sổ **Export File Format**, chọn **Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)**, đánh dấu chọn **Include all certificates in the certification path if possible**, và chọn **Next**.



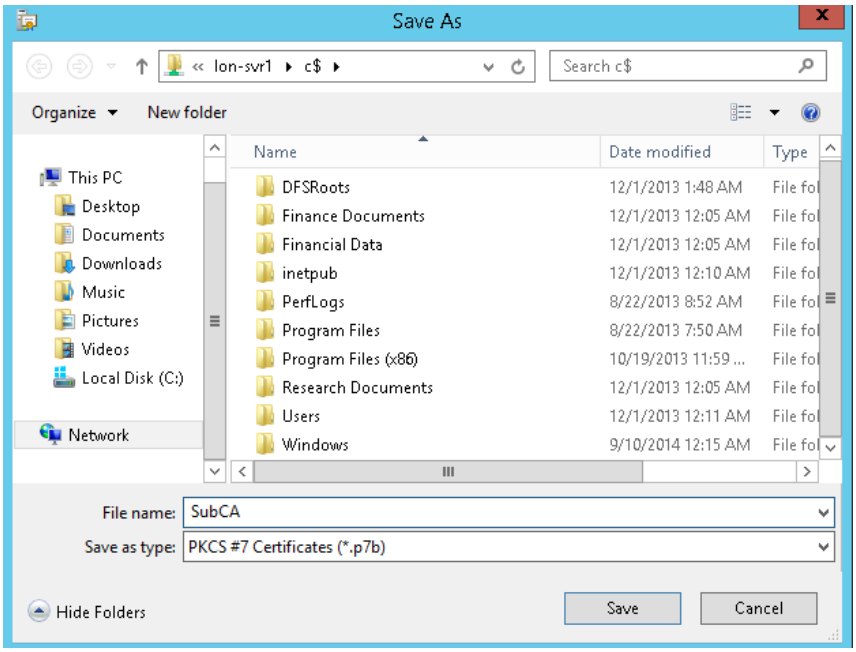
20. Cửa sổ **File to Export**, chọn **Browse**.



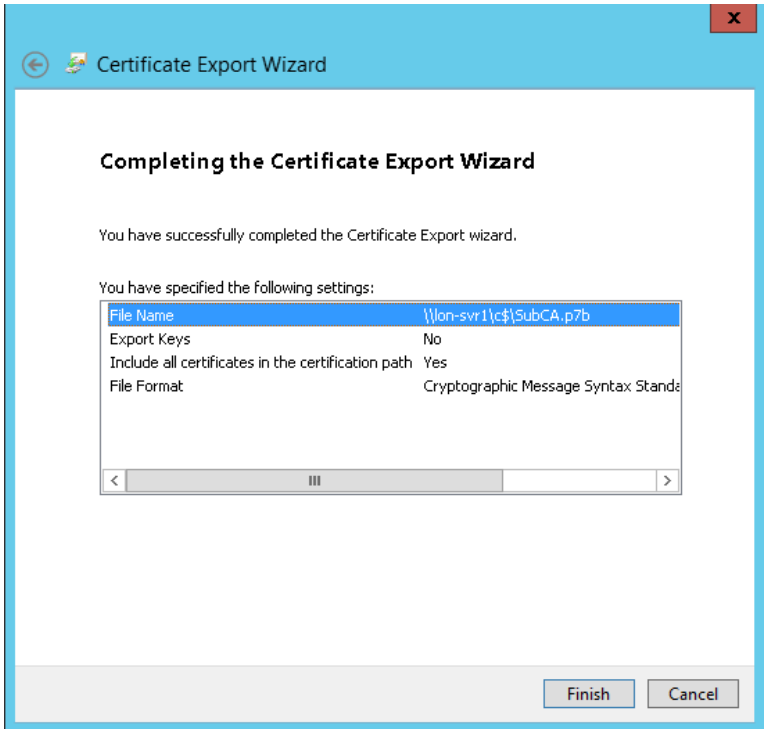

21. Trong ô **File name**, nhập **\\lon-svr1\C$**, nhấn Enter.



22. Trong ô **File name**, nhập **SubCA**, chọn **Save**, và chọn **Next**.



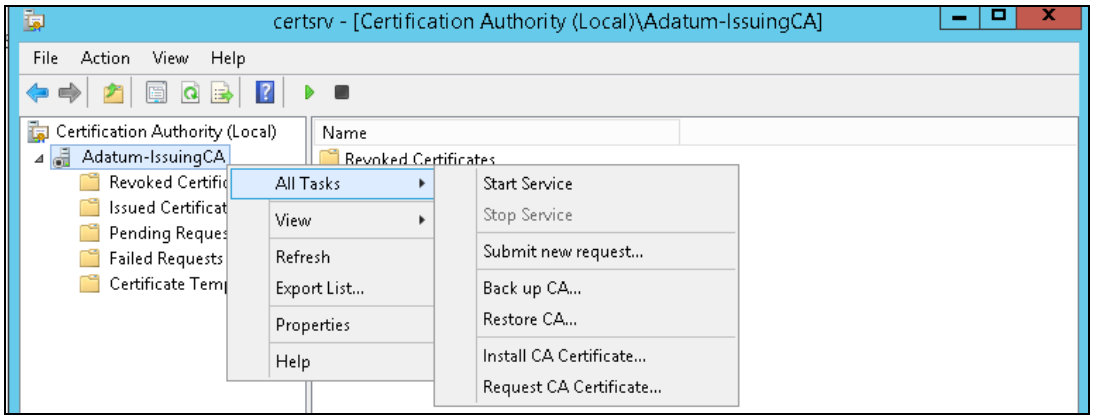

23. Chọn **Finish**, và chọn **OK** 2 lần.



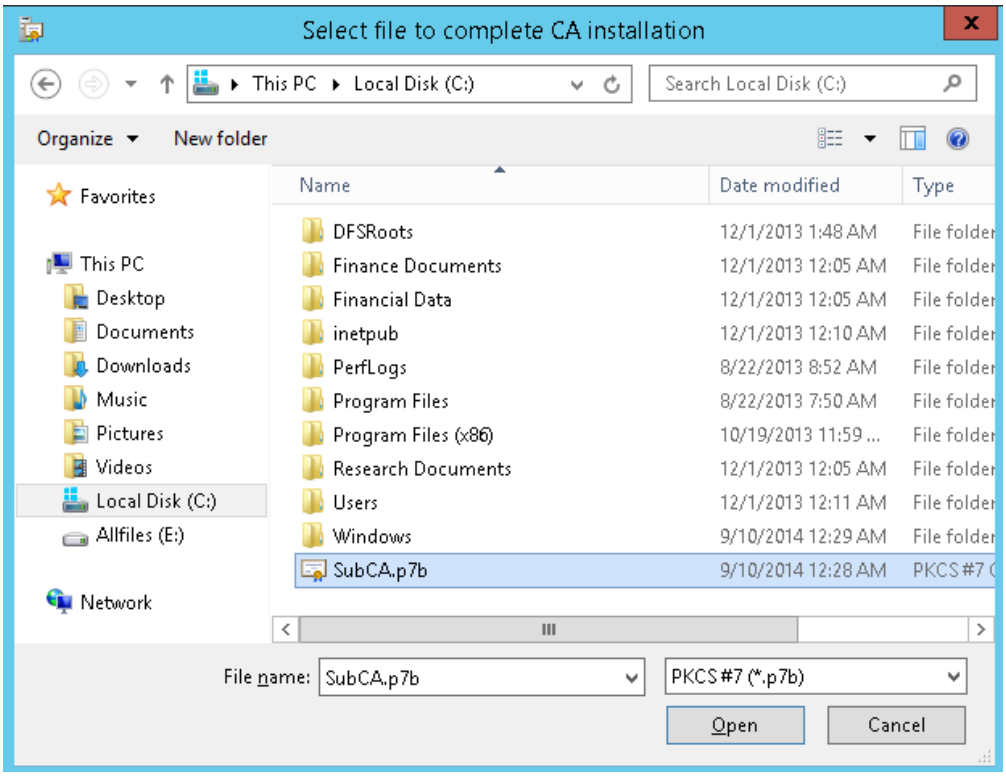
24. Qua máy **LON-SVR1**.

25. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Certification Authority**.

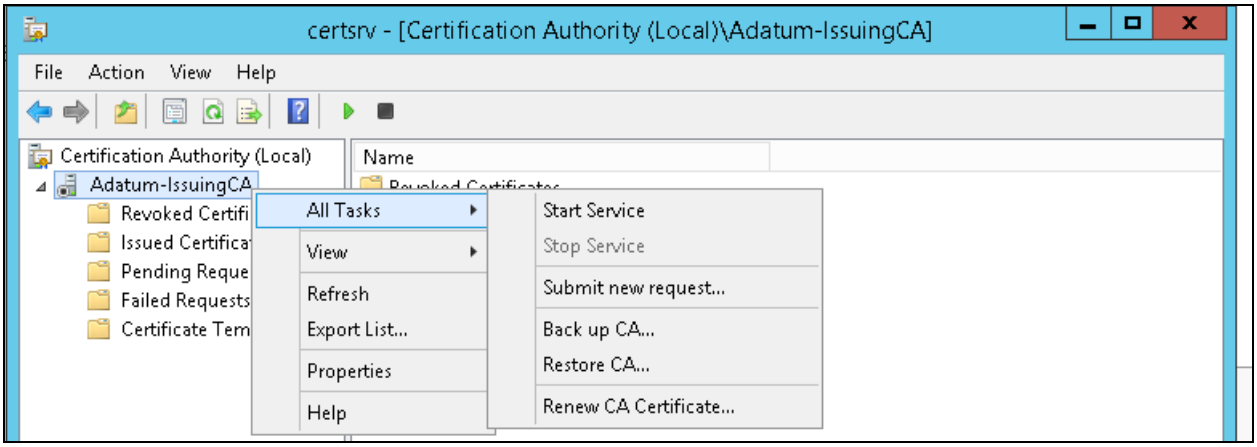
26. Trong cửa sổ **Certification Authority**, chuột phải **Adatum-IssuingCA**, bung **All Tasks**, chọn **Install CA Certificate**.




27. Trỏ đường dẫn vào **Local Disk (C:)**, chọn file **SubCA.p7b**, chọn **Open**.



28. Đợi khoảng 15 đến 20 giây, chuột phải **Adatum-IssuingCA**, bung **All Tasks**, chọn **Start**.




29. Đảm bảo khởi động CA thành công.

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công Stand-alone Root CA và Enterprise Subordinate CA.**

## Bài tập 2: Tạo và phát hành Certificate mẫu (Certificate Templates).

Sau khi triển khai các CA thành công, bước tiếp theo trong việc triển khai AD CS là cấu hình các chứng chỉ mẫu (Certificate Template)để đáp ứng các yêu cầu bảo mật.

❖ **Bài tập này bao gồm các bước:**

1. Tạo OU và Group cho máy laptop.
2. Cấu hình Web Server Certificate Template
3. Cấu hình DirectAccess Certificate Template
4. Cấu hình Smart Card Certificate Template
5. Phát hành Certificate Templates

❖ **Thực hiện:**

**Bước 1. Tạo OU và Group cho máy laptop.**

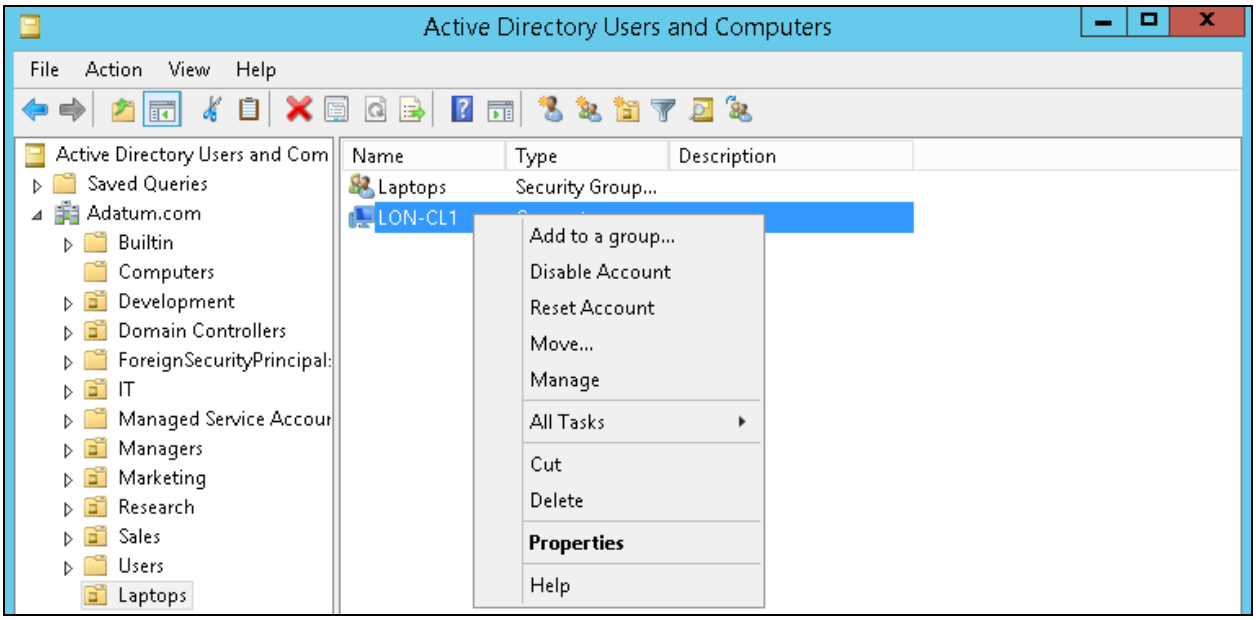
1. Trên máy **LON-DC1**, trong cửa sổ **Server Manager**, bung **Tools**, mở **Active Directory Users and Computers**.

2. Trong cửa sổ **Active Directory Users and Computers**, tạo một OU mới đặt tên **Laptops**.

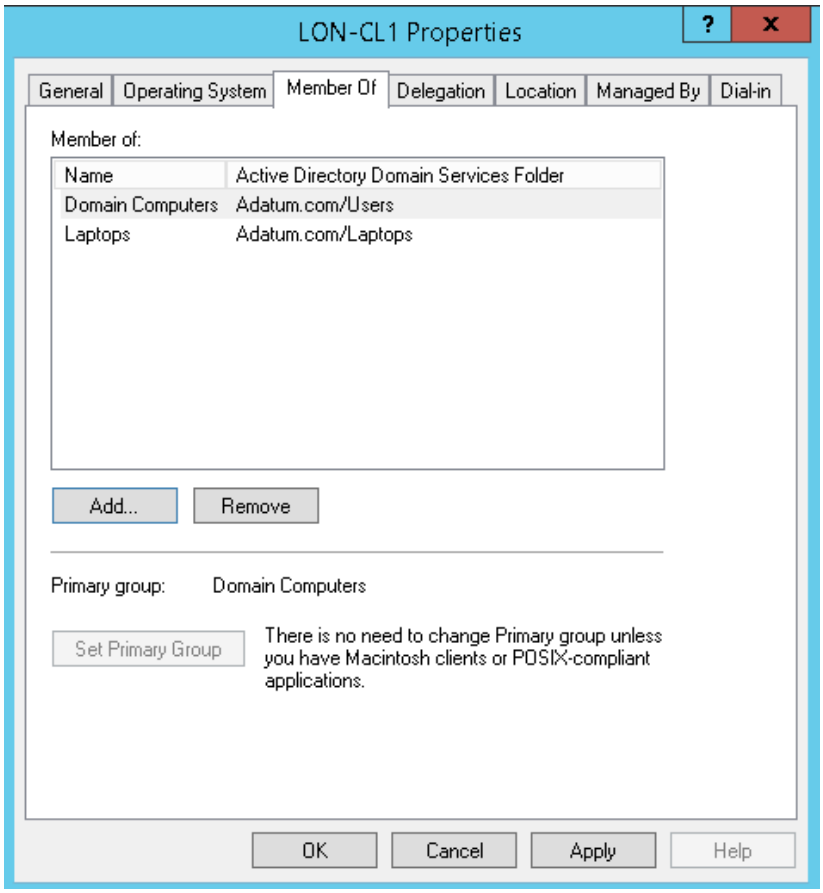
3. Trong OU **Laptops,** tạo một group mới đặt tên **Laptops**

4. Vào mục **Computers**, chuột phải **LON-CL1**, chọn **Move**, chọn OU **Laptops**, và chọn **OK**.

5. Vào OU **Laptops**, chuột phải **LON-CL1**, chọn **Properties**.

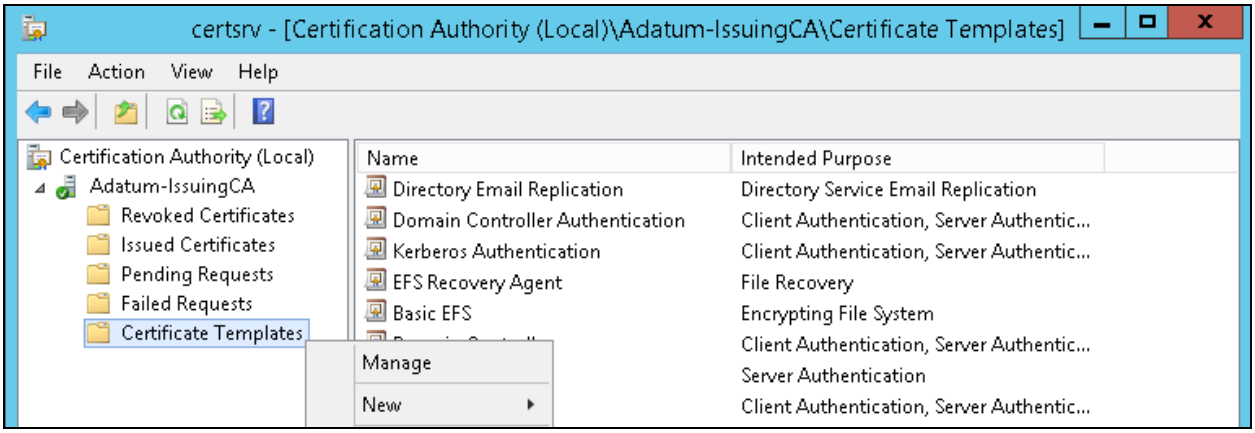


6. Qua tab **Member Of**, chọn **Add** vào group **Laptops**, và chọn **OK**

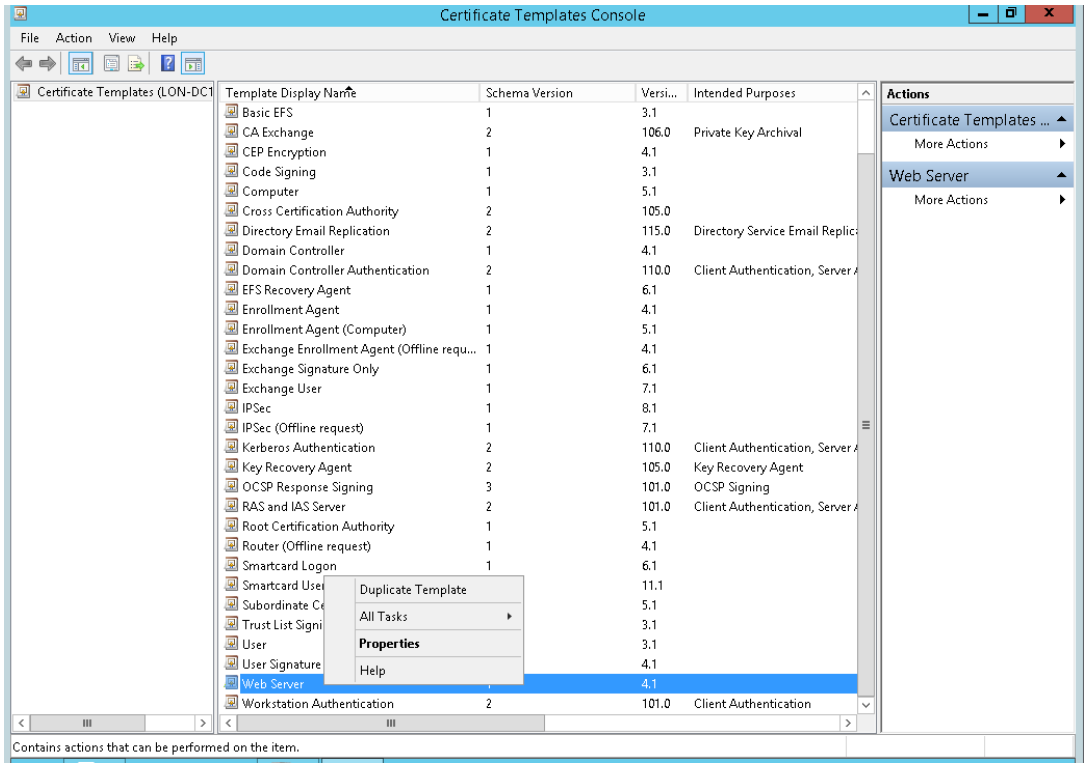


## Bước 2. Cấu hình Web Server Certificate Template

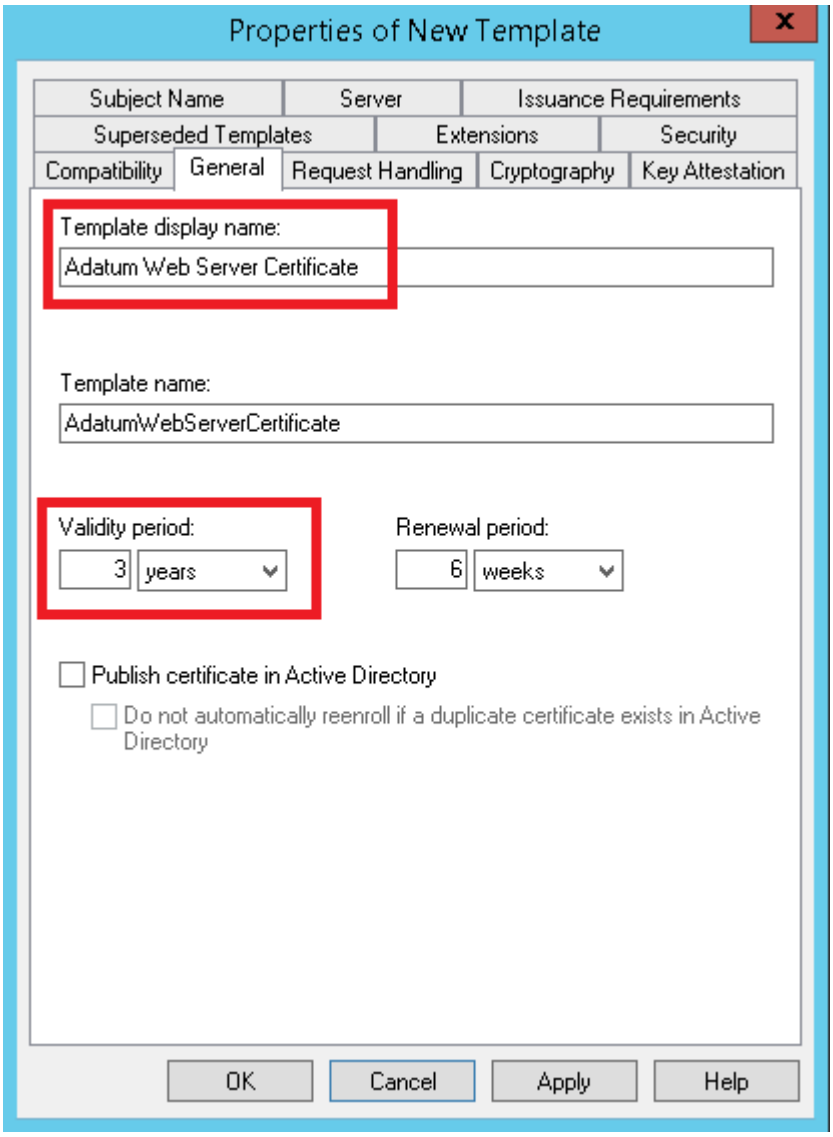
1. Trên máy **LON-SVR1**, trong cửa sổ **Certification Authority**, bung **Adatum-IssuingCA**, chuột phải **Certificate Templates**, chọn **Manage**.



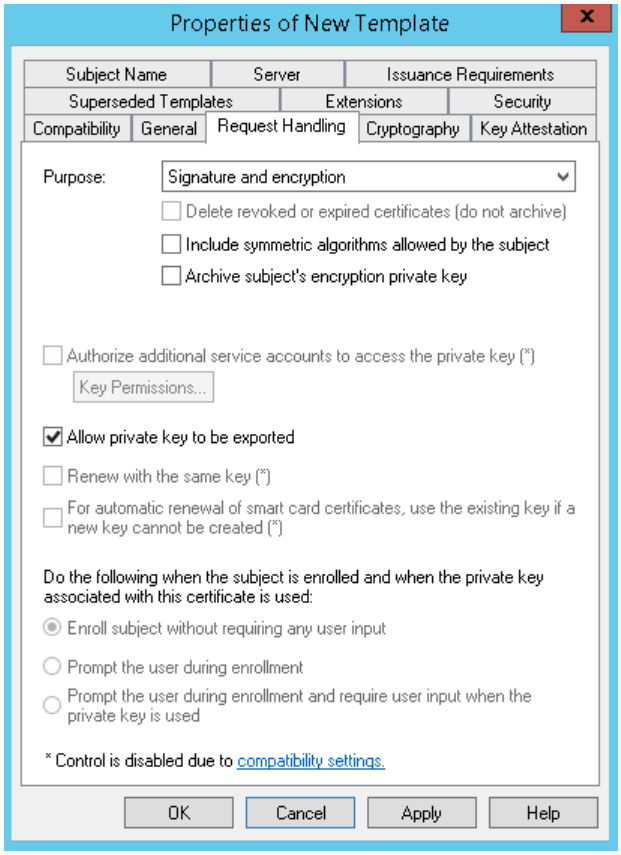

2. Trong cửa sổ **Certificate Templates** console, chuột phải **Web Server**, chọn **Duplicate Template**.



3. Trong hộp thoại **Properties of New Template,** qua tab **General**. Trong ô **Template display name**, nhập **Adatum Web Server Certificate**, và chỉnh **Validity period** thành **3 years**.

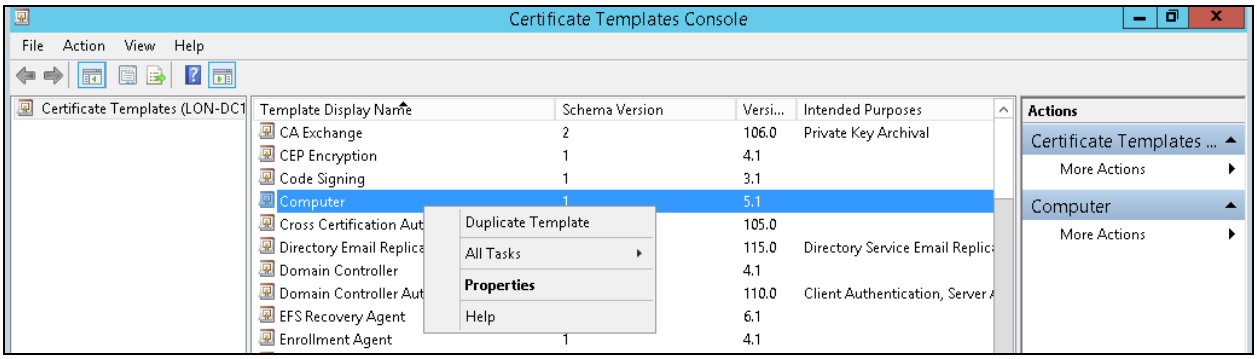


4. Qua tab **Request Handling**, đánh dấu chọn **Allow private key to be exported**, và chọn **OK**.

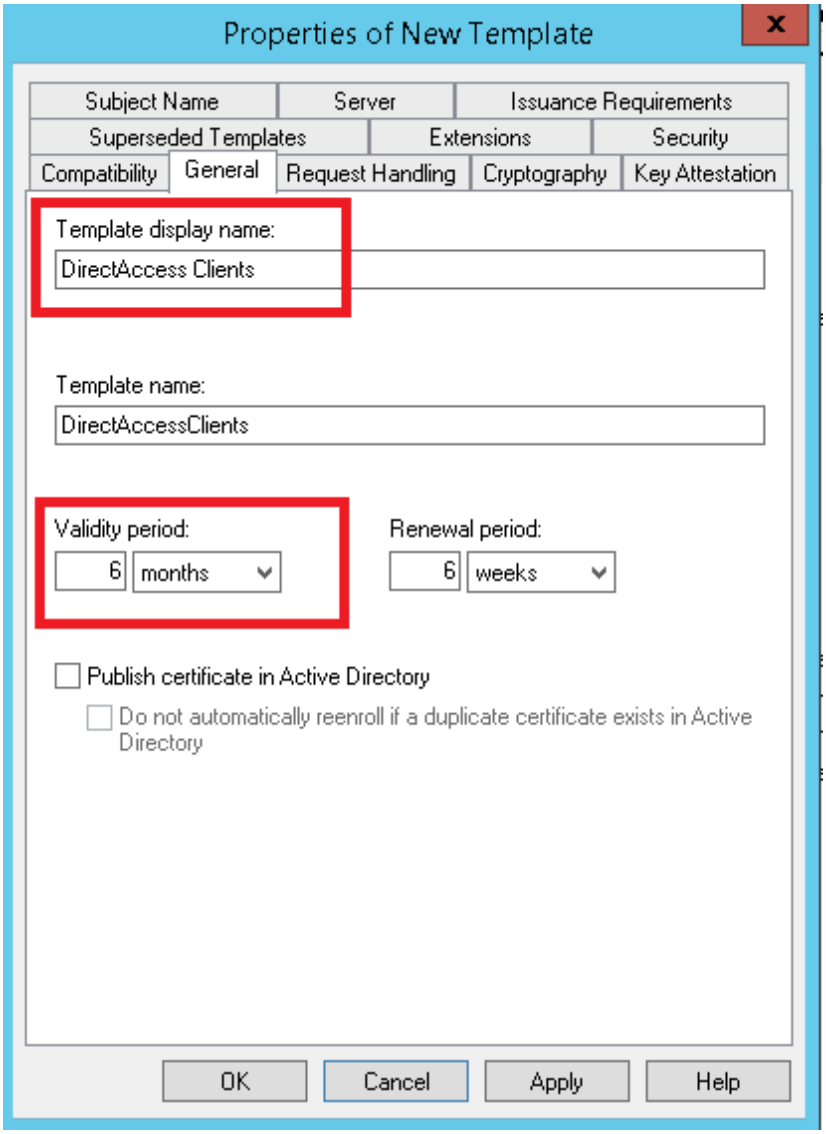



## Bước 3. Cấu hình DirectAccess Certificate Template

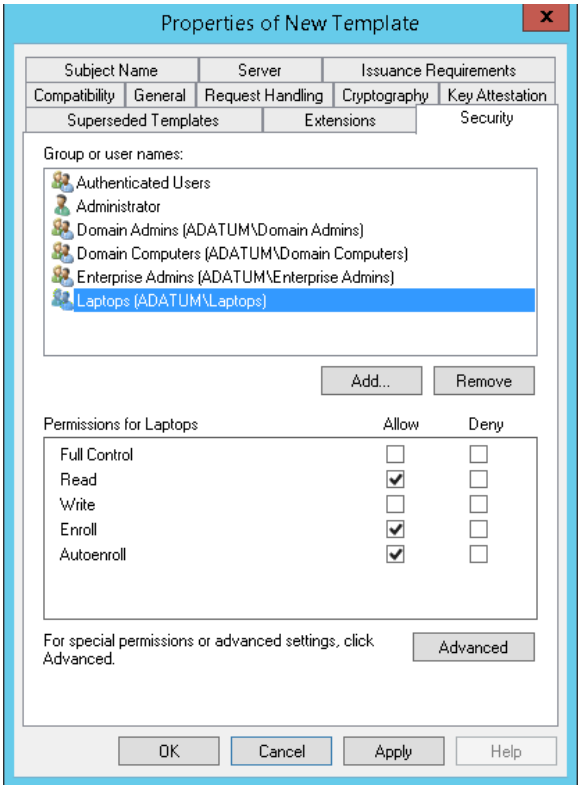
1. Trên máy **LON-SVR1**, trong cửa sổ **Certificate Templates** console, chuột phải **Computer**, chọn **Duplicate Template**.



2. Trong hộp thoại **Properties of New Template,** qua tab **General**. Trong ô **Template display name**, nhập **DirectAccess Clients**, và chỉnh **Validity period** thành **6 months**.

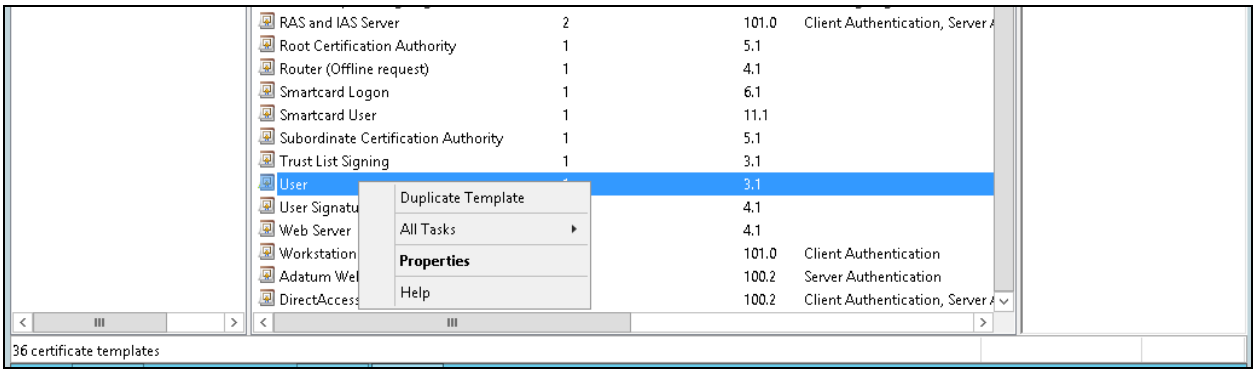


3. Qua tab **Security**, chọn **Add**, add group **Laptops** vào, và cấp cho group **Laptops** 3 quyền **Read, Enroll** và **Autoenroll** ở cột **Allow,** chọn **OK**

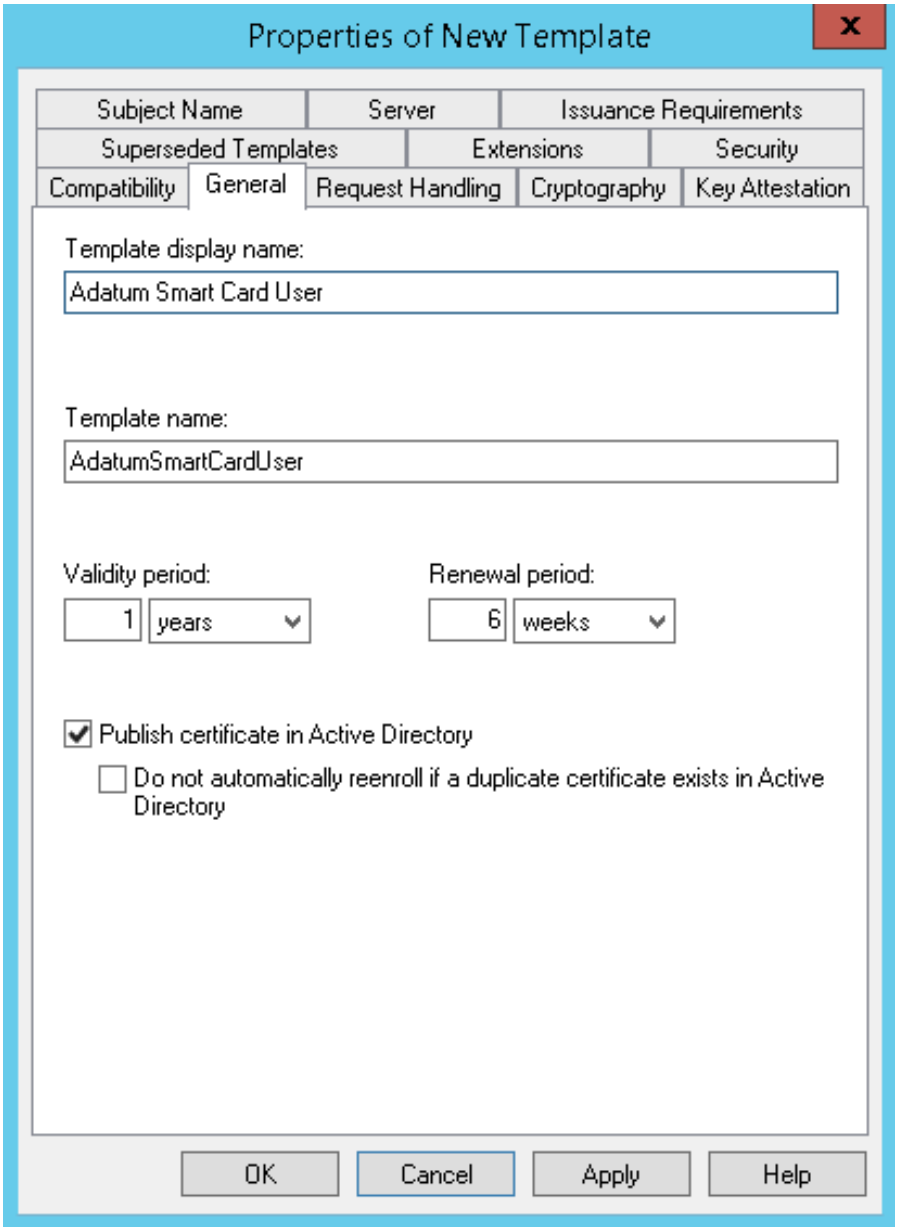



## Bước 4. Cấu hình Smart Card Certificate Template

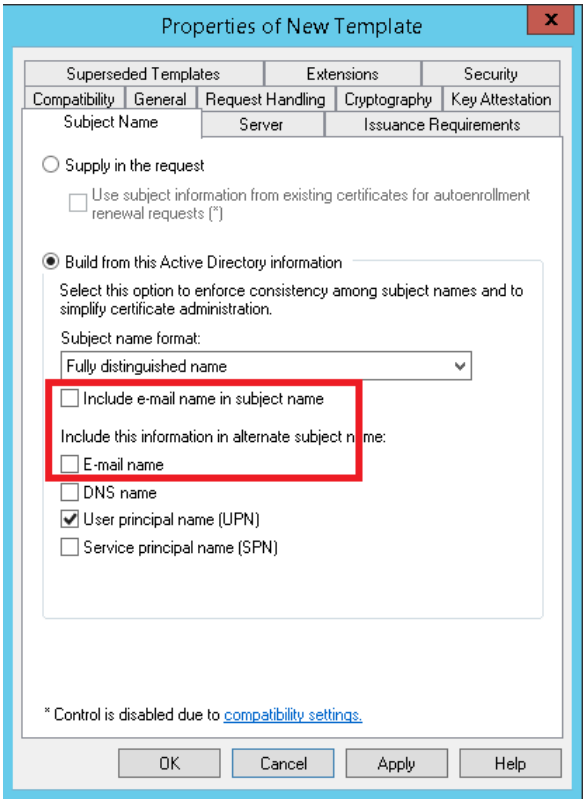
1. Trên máy **LON-SVR1**, trong cửa sổ **Certificate Templates** console, chuột phải **User**, chọn **Duplicate Template**.



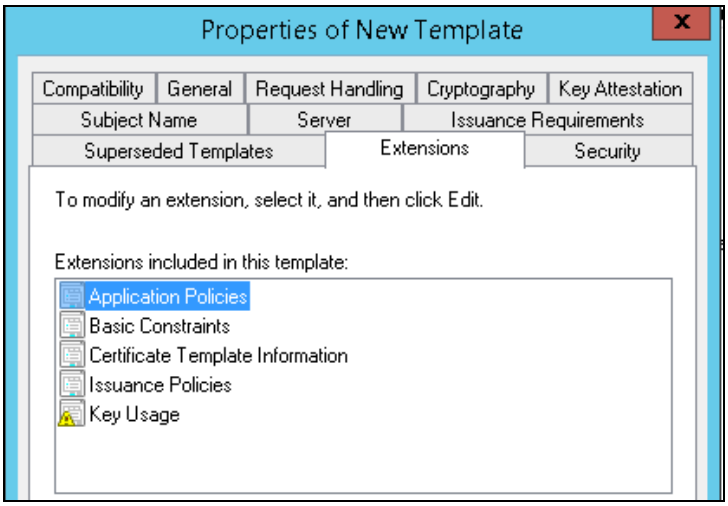
2. Trong hộp thoại **Properties of New Template**, qua tab **General**. Trong ô **Template display name**, nhập **Adatum Smart Card User**.



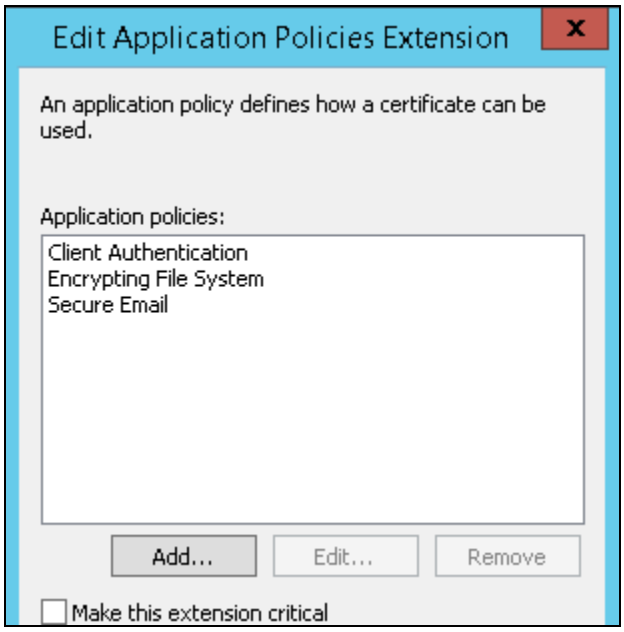
3. Qua tab **Subject Name**, bỏ dấu chọn 2 ô **Include e-mail name in subject name** và **E-mail name**.



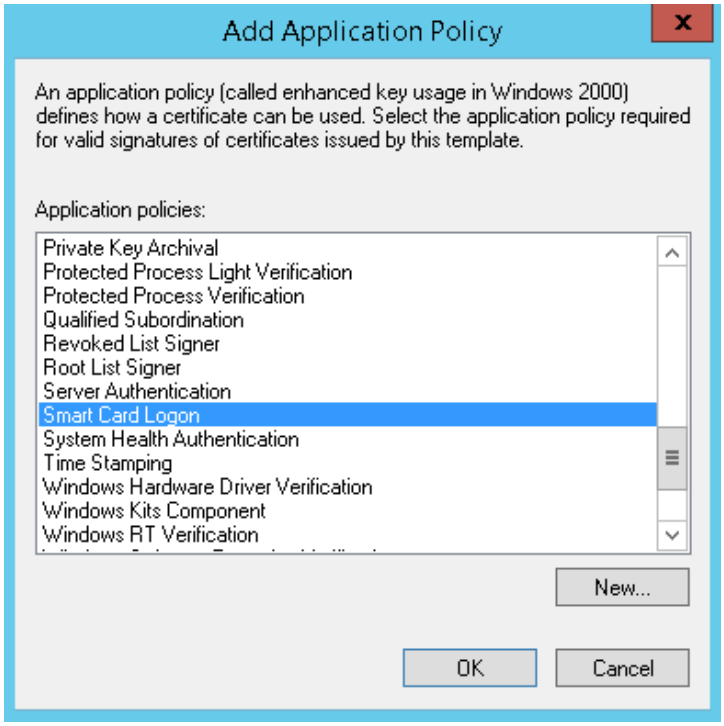

4. Qua tab **Extensions**, chọn **Application Policies**, và chọn **Edit**.



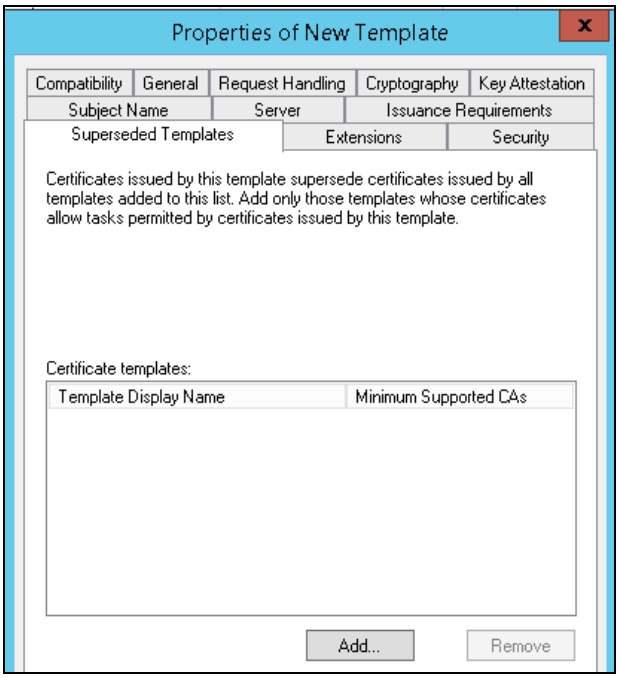
5. Hộp thoại **Edit Application Policies Extension**, chọn **Add**.



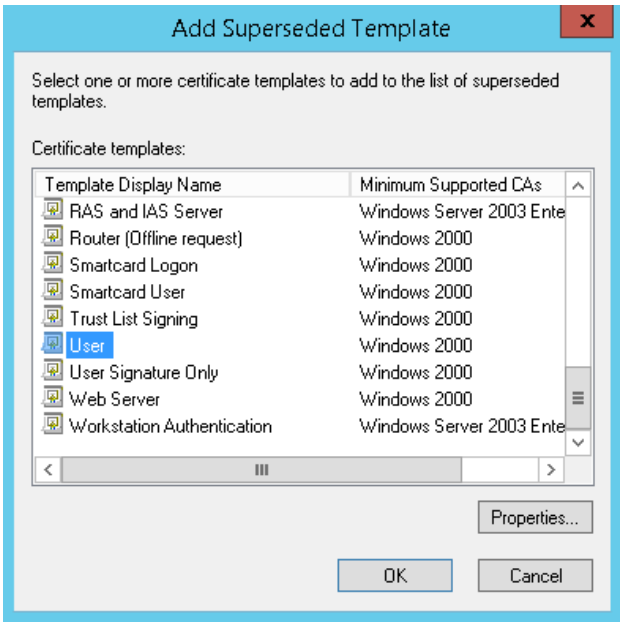

6. Hộp thoại **Add Application Policy**, chọn **Smart Card Logon**, và chọn **OK** 2 lần.



7. Qua tab **Superseded Templates**, chọn **Add**.



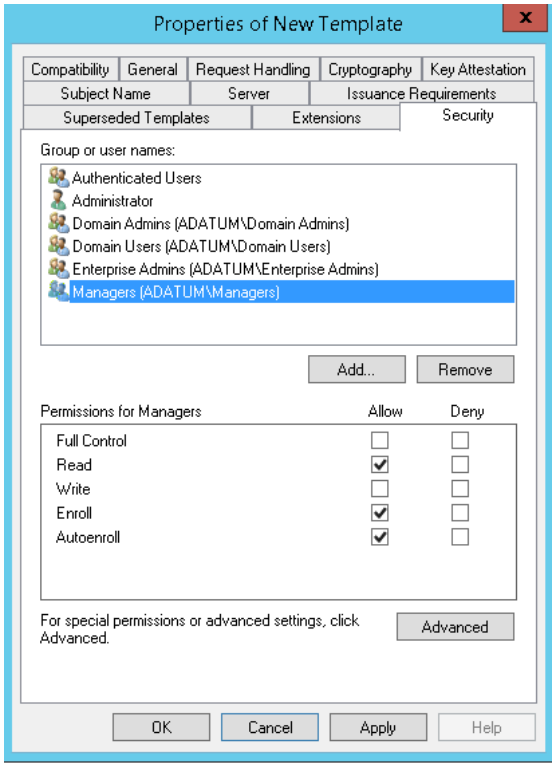

8. Chọn **User** template, và chọn **OK**.



9. Qua tab **Security**, chọn **Add**.

10. Hộp thoại **Select Users, Computers, Service Accounts, or Groups**, nhập **Managers**, chọn **Check Names**, và chọn **OK**.

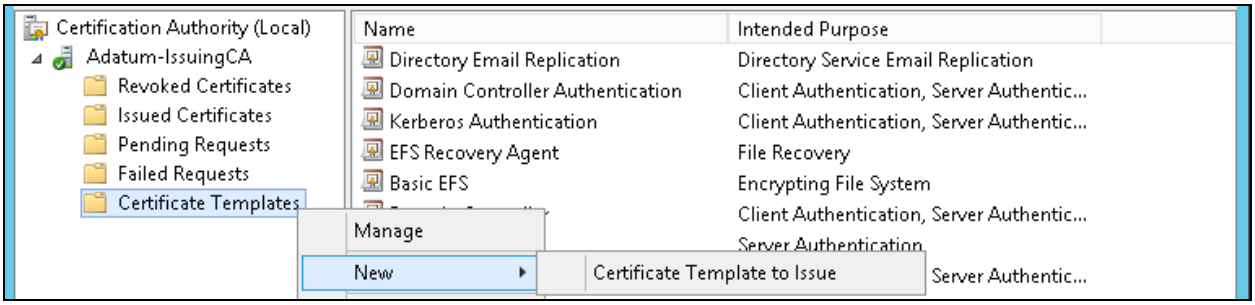
11. Trong tab **Security,** chọn group **Managers**, đánh dấu chọn 3 ô **Read**, **Enroll** and **Autoenroll** ở cột **Allow**, chọn **OK**.



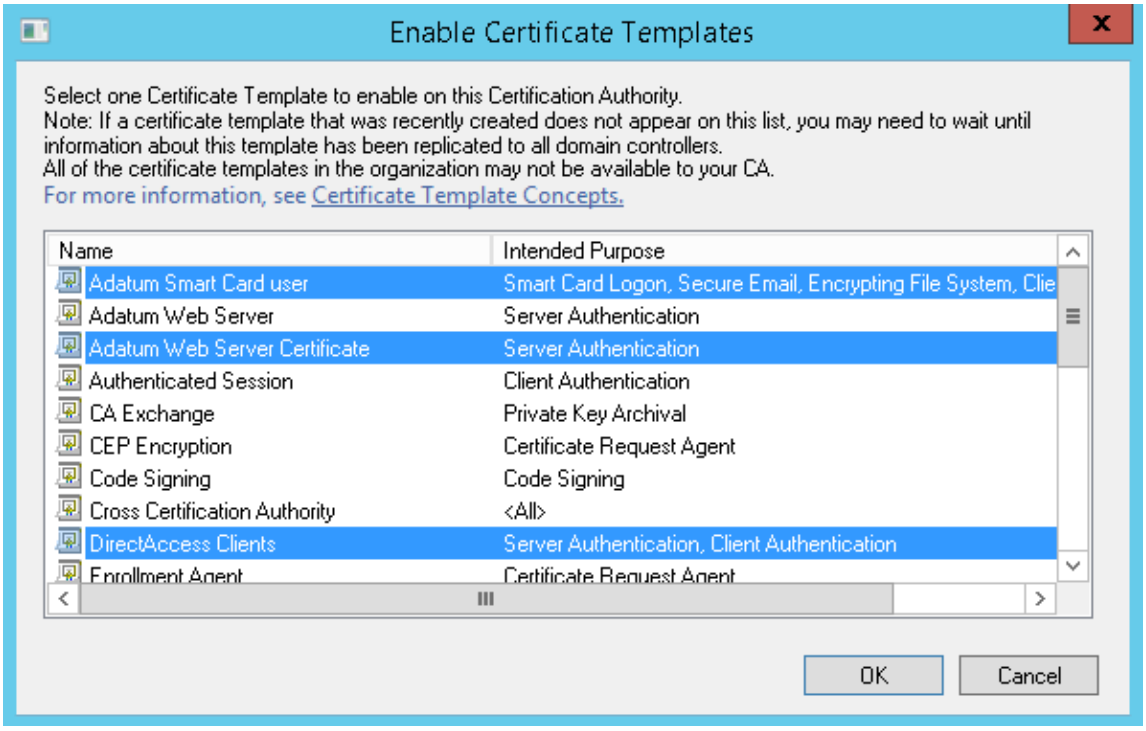

12. Tắt cửa sổ **Certificate Templates** console.

## Bước 5. Phát hành Certificate Templates

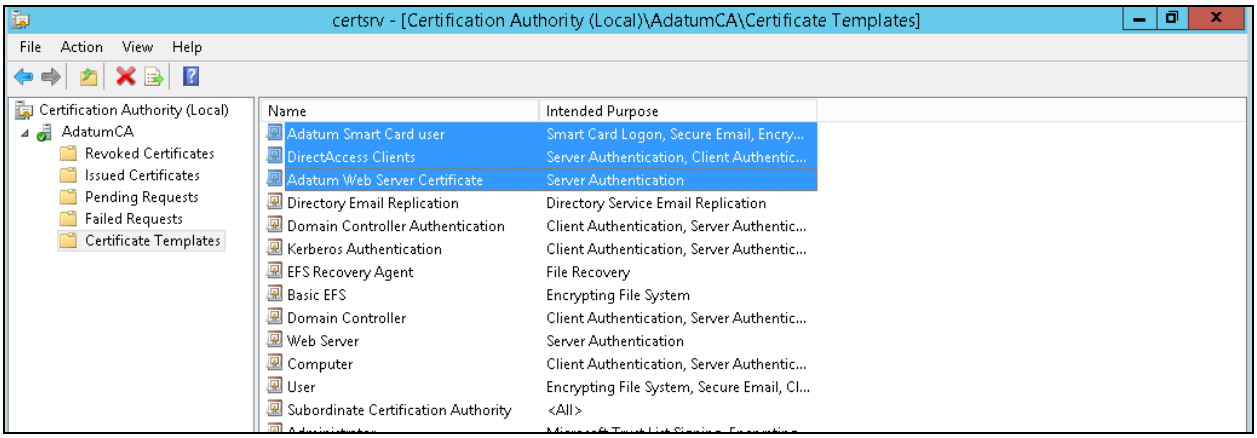
1. Trên máy **LON-SVR1**, trong cửa sổ **Certification Authority**, chuột phải **Certificate Templates**, bung **New**, chọn **Certificate Template to Issue**.




2. Cửa sổ **Enable Certificate Templates**, chọn 3 certificate **Adatum Smart Card User**, **DirectAccess Clients**, và **Adatum Web Server Certificate**, chọn **OK**.



3. Kiểm tra phát hành thành công 3 certificate **Adatum Smart Card User**, **DirectAccess Clients**, và **Adatum Web Server Certificate.**




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình và phát hành thành công các certificate mẫu để đáp ứng yêu cầu bảo mật.**

## Bài tập 3: Cấu hình chức năng tự động phân phối và thu hồi Certificate.

Sau khi triển khai các certificate mẫu, bạn phải thực hiện phương án phát hành và thu hồi certificate. Bởi vì yêu cầu an ninh của tổ chức bao gồm các tùy chọn khác nhau cho việc triển khai các certificate, nên bạn cần phải cấu hình cho phép đăng ký certificate dựa trên web và hỗ trợ chức năng tự động cấp phát certificate.

❖ **Bài tập này bao gồm các bước:**

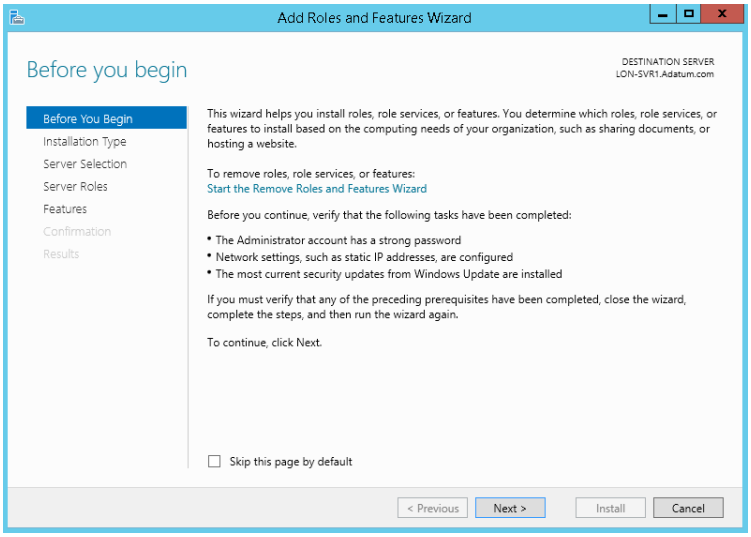
1. Cấu hình chức năng kiểm tra thu hồi certificate (Certificate Revocation Checking).
2. Cấu hình Certificate Revocation checking cho DirectAccess clients.
3. Cấu hình chức năng tự động phân phối certificate cho user và computer.
4. Xác nhận đăng ký Smart Card certificate và DirectAccess certificate.

❖ **Thực hiện:**

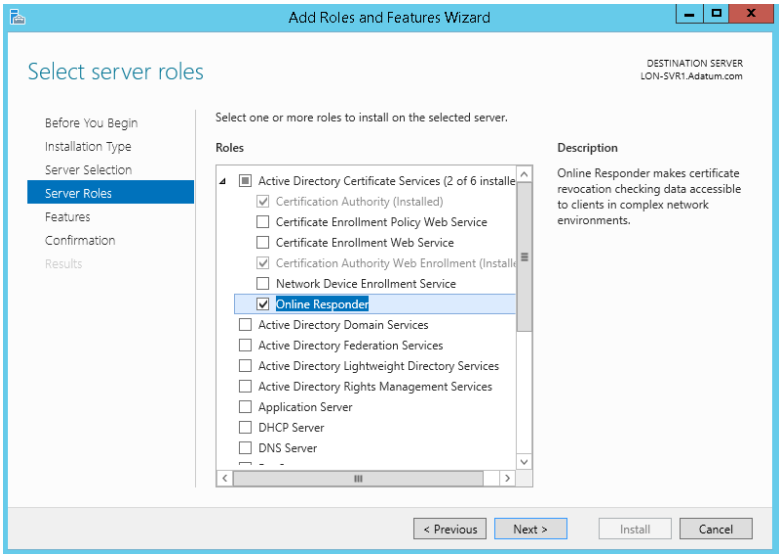
**Bước 1. Cấu hình chức năng kiểm tra thu hồi certificate (Certificate Revocation checking).**

1. Trên máy **LON-SVR1**, trong cửa sổ **Server Manager**, chọn **Add roles and features**.

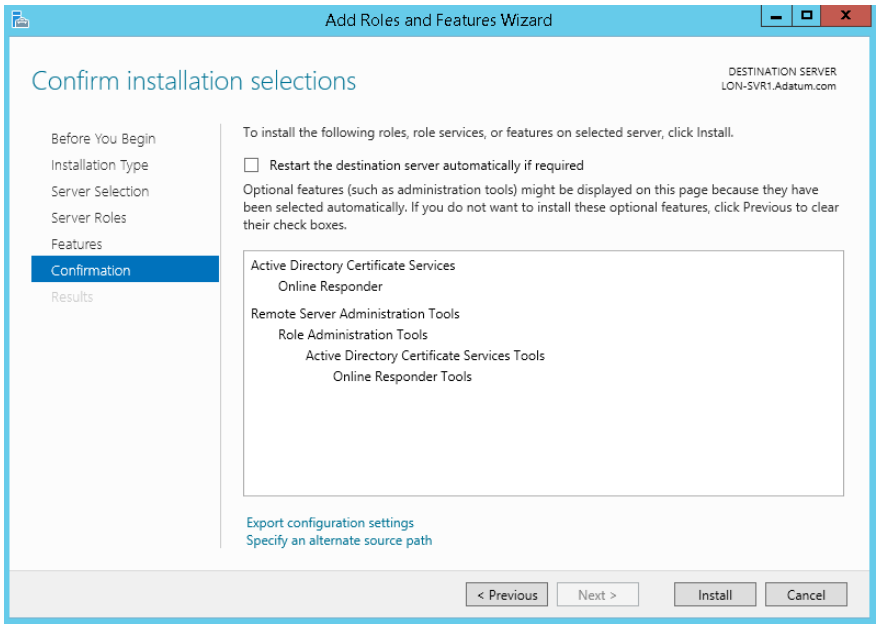
2. Cửa sổ Before you begin, chọn **Next** 3 lần.



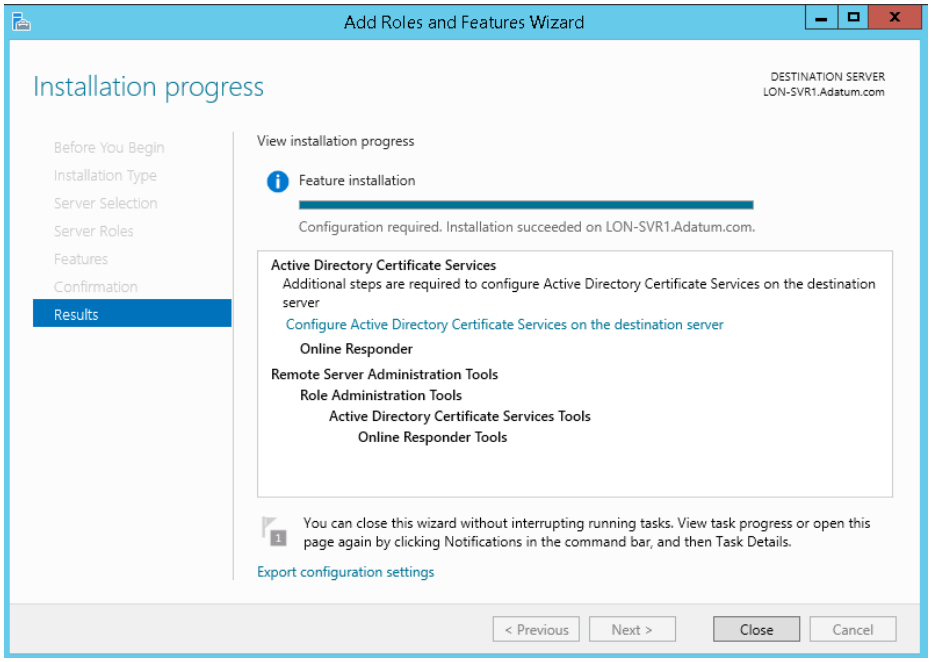

3. Cửa sổ **Select server roles**, bung **Active Directory Certificate Services (2 of 6 installed)**, đánh dấu chọn **Online Responder**, chọn **Add Features**, chọn **Next** 2 lần.



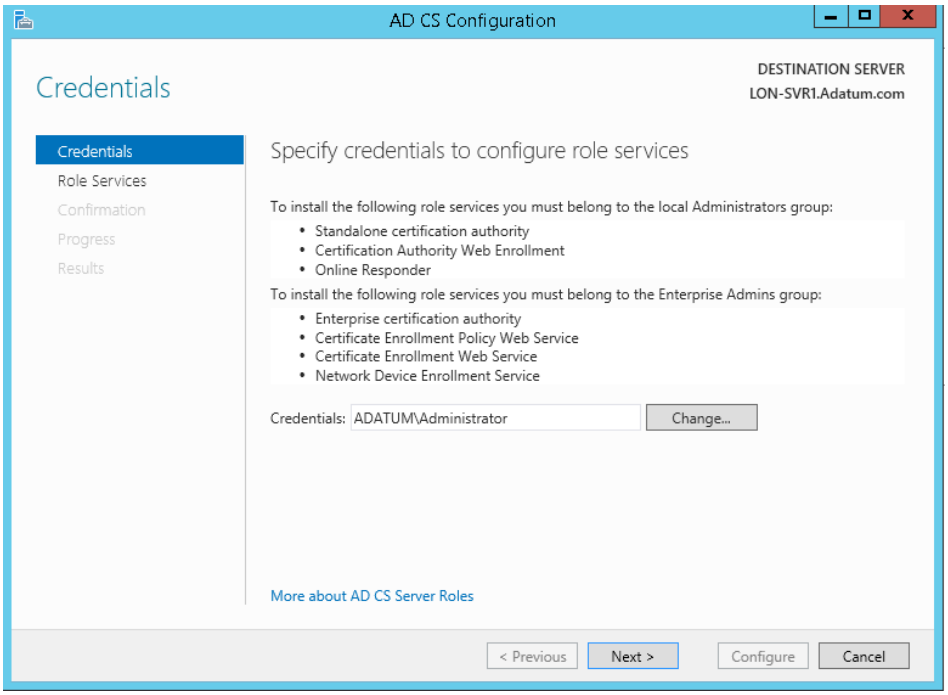
4. Cửa sổ **Confirm installation selections** và chọn **Install**.



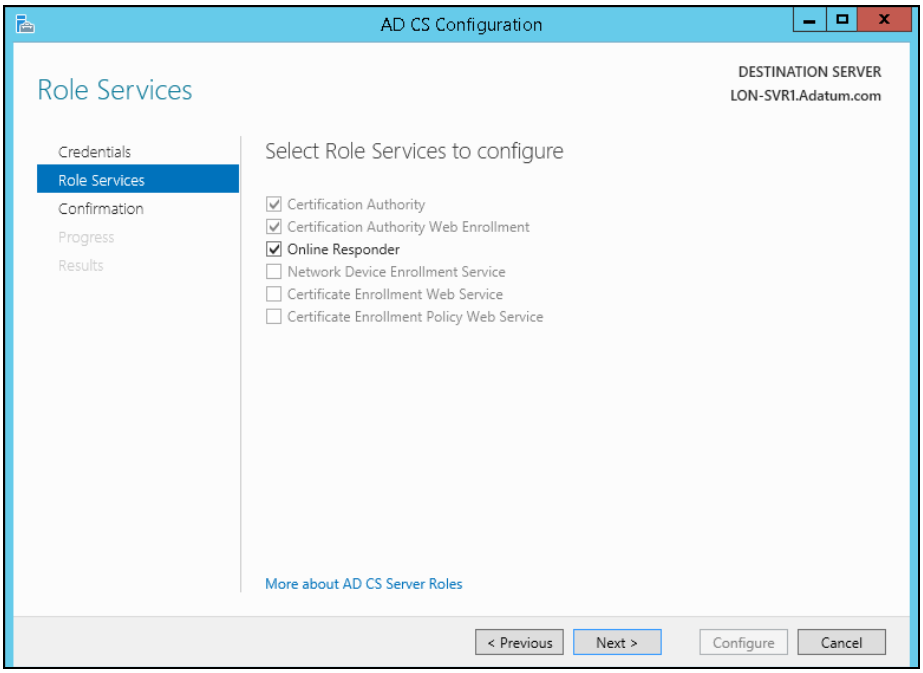

5. Sau khi cài đặt thành công, chọn **Configure Active Directory Certificate Services on the destination server**.



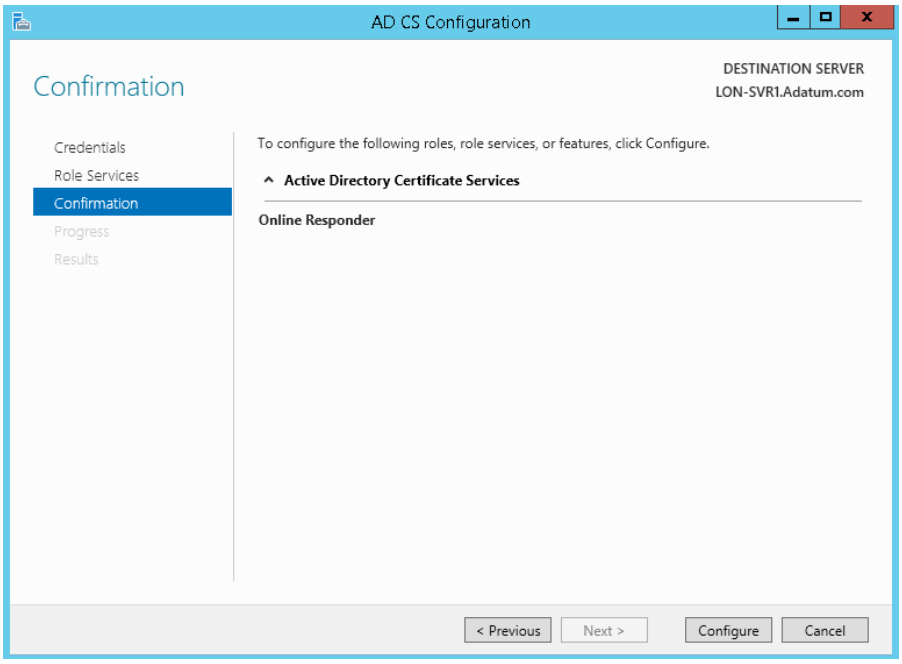
6. Cửa sổ **Credentials**, chọn **Next**.



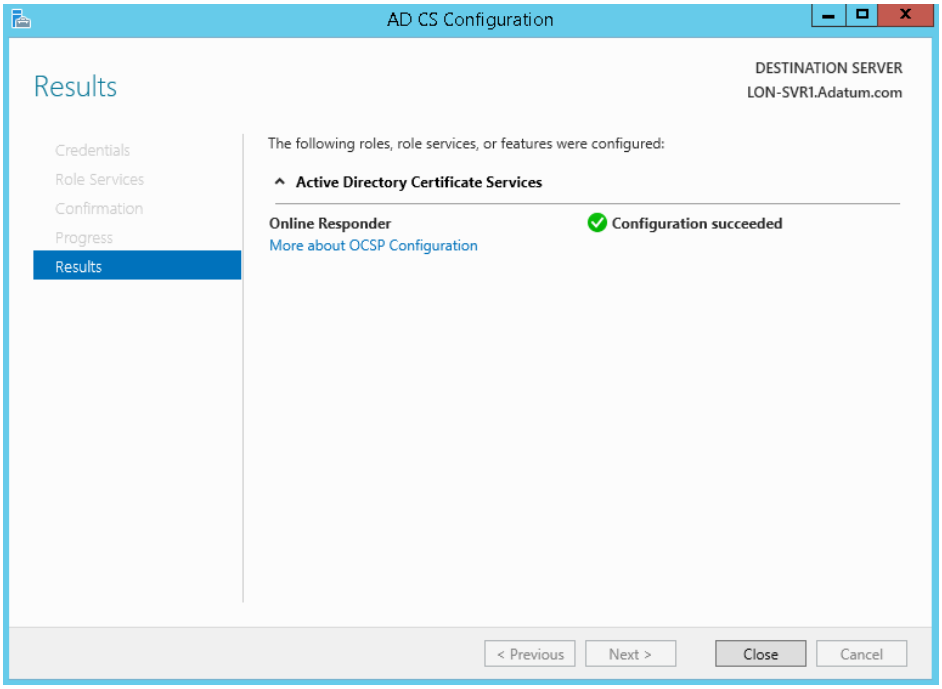

7. Cửa sổ **Role Services**, dánh dấu chọn **Online Responder**, chọn **Next**.



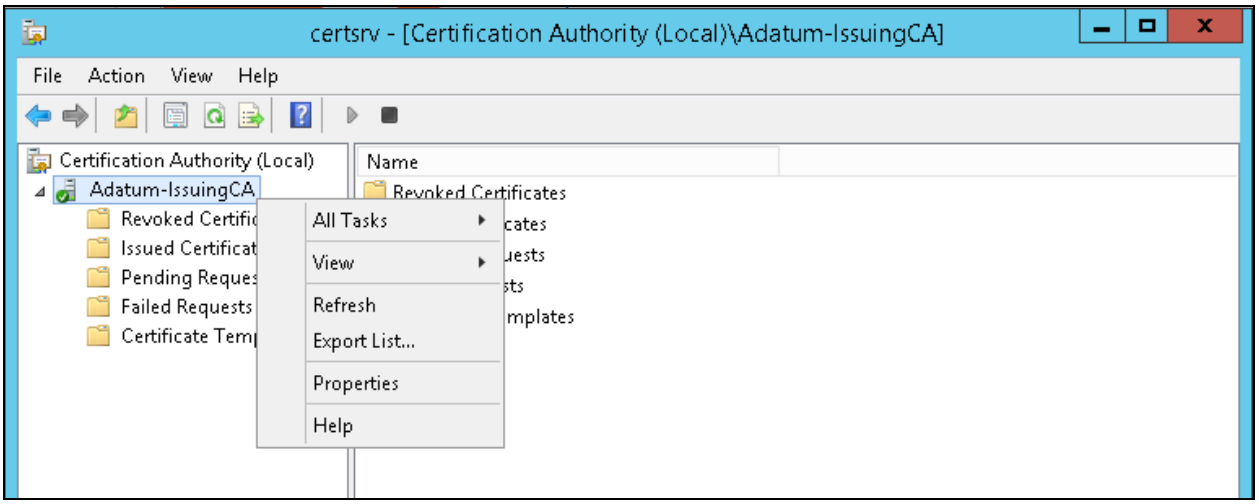
8. Cửa sổ **Confirmation**, chọn **Configure**.



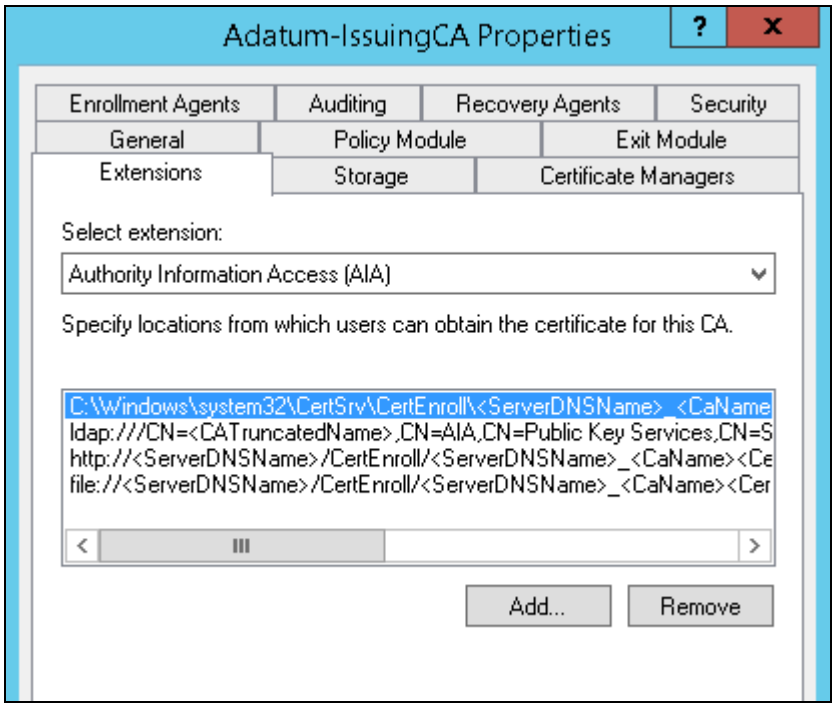

9. Cửa sổ **Results**, chọn **Close** 2 lần.



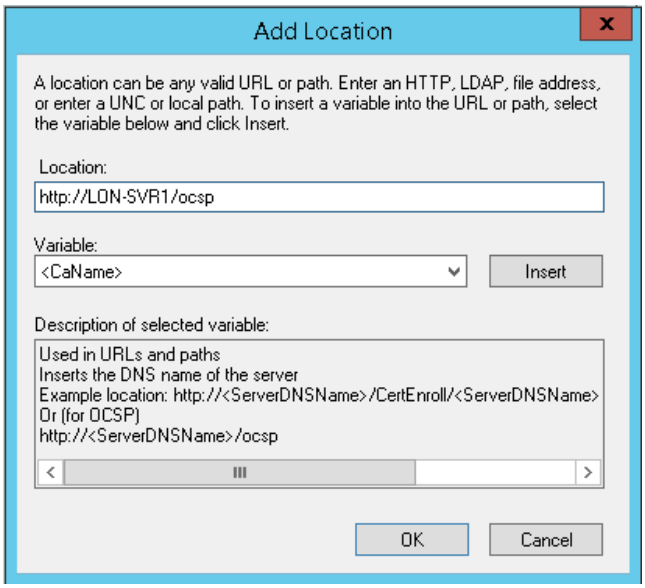
10. Trên máy **LON-SVR1**, mở công cụ **Certification Authority**, chuột phải **Adatum-IssuingCA**, chọn **Properties**.



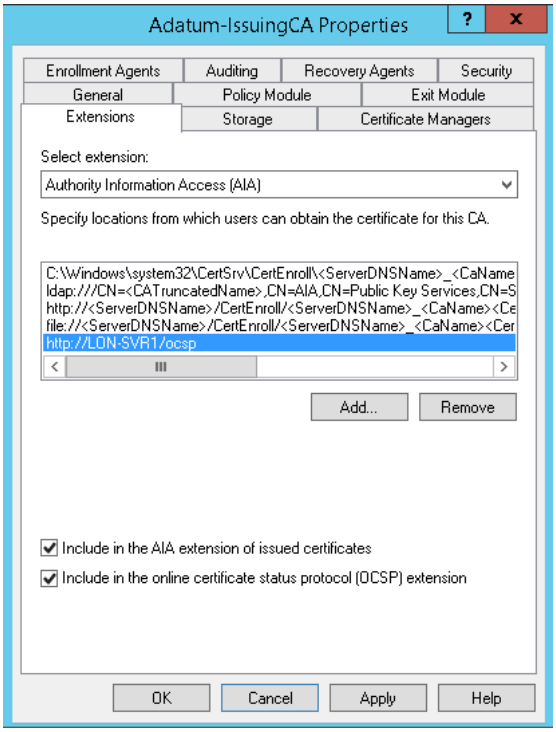

11. Trong hộp thoại **Adatum-IssuingCA Properties**, qua tab **Extensions**, bung ô **Select extension**, chọn **Authority Information Access (AIA)**, và chọn **Add**.



12. Trong ô **Add Location**, nhập **http://LON-SVR1/ocsp**, và chọn **OK**.

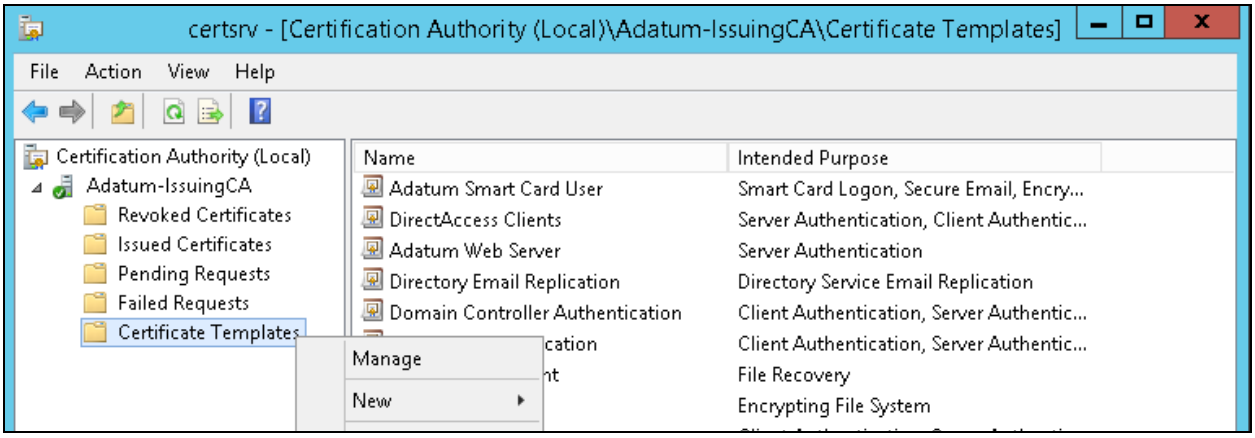



13. Đánh dấu chọn 2 ô **Include in the AIA extension of issued certificates** và **Include in the online certificate status protocol (OCSP) extension**, chọn **OK**.

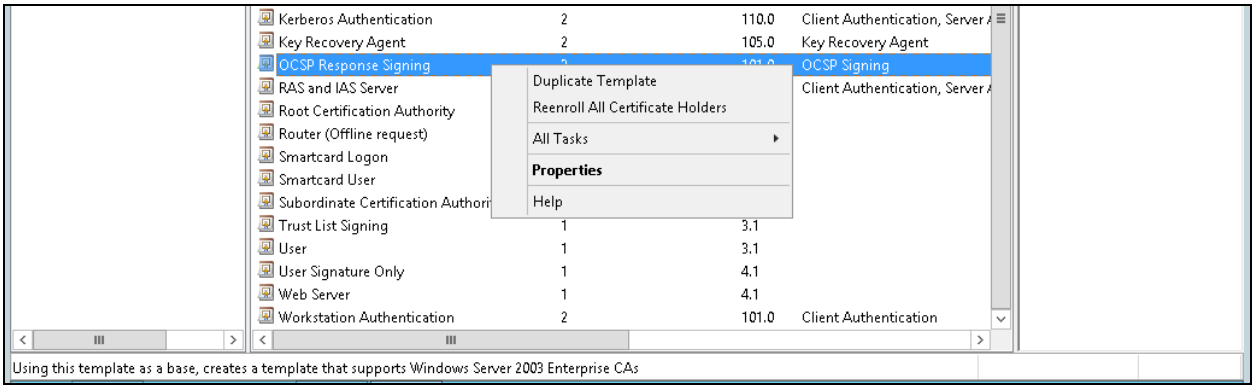


14. Hộp thoại **Certificate Authority**, chọn **Yes** để restart AD CS.

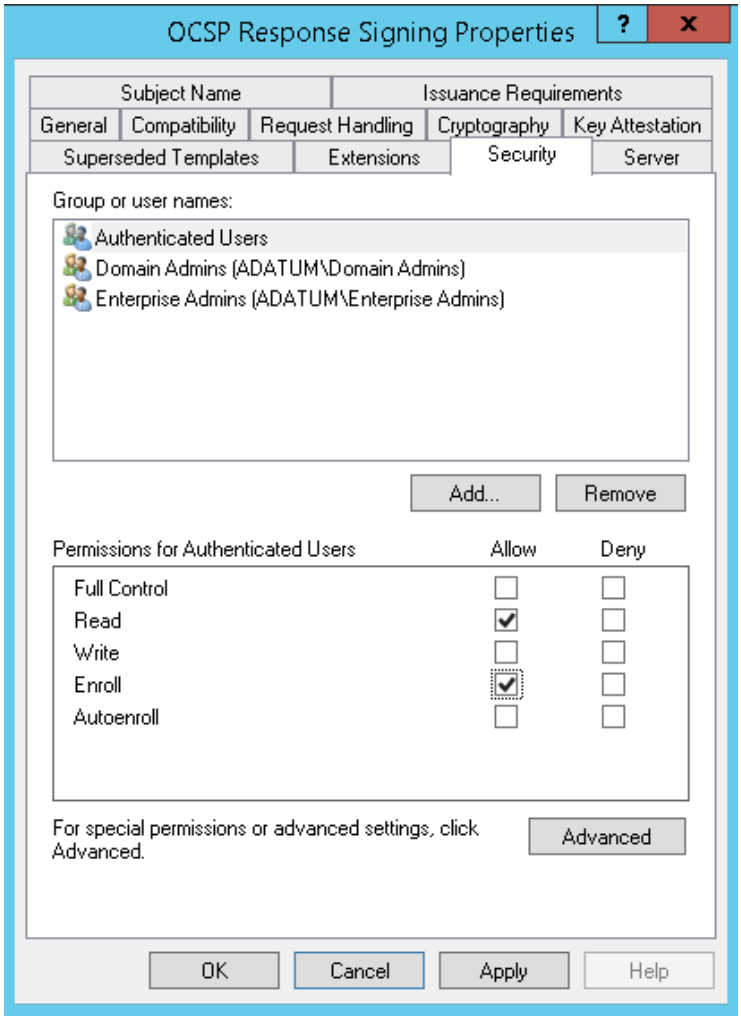
15. Trong cửa sổ **Certification Authority**, bung **Adatum-IssuingCA**, chuột phải **Certificate Templates**, chọn **Manage**.




16. Trong cửa sổ **Certificate Templates** console, chuột phải certificate **OCSP Response Signing**, chọn **Properties**

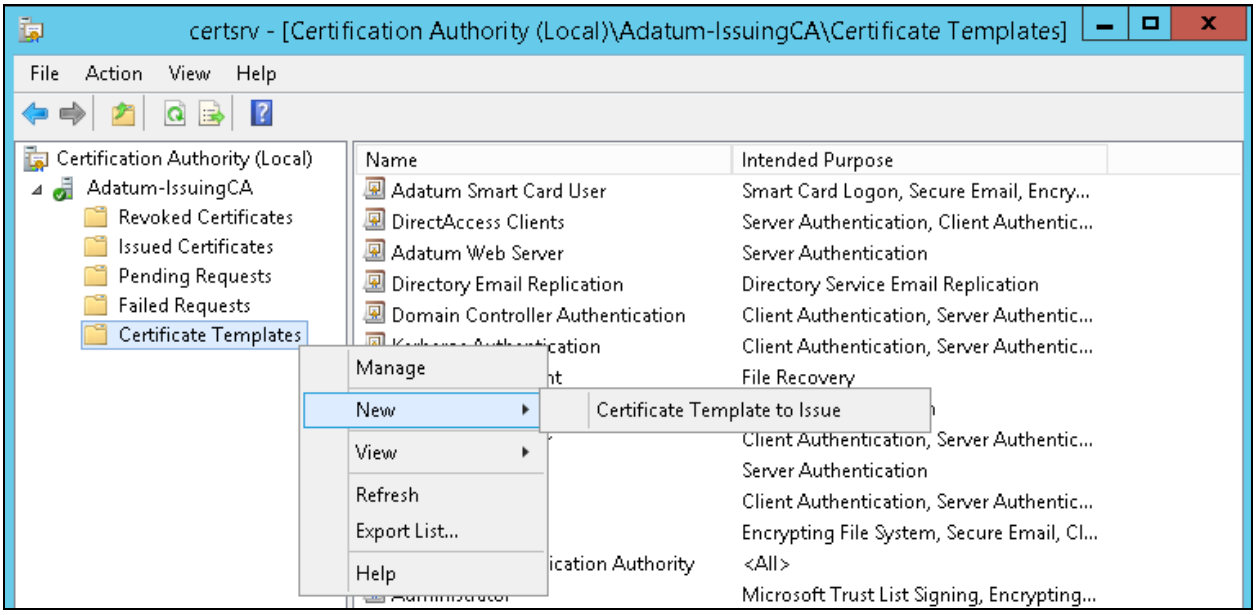


17. Trong hộp thoại **OCSP Response Signing Properties**, qua tab **Security**, chọn group **Authenticated Users**, đánh dấu chọn thêm ô **Enroll** ở cột **Allow**, chọn **OK**.

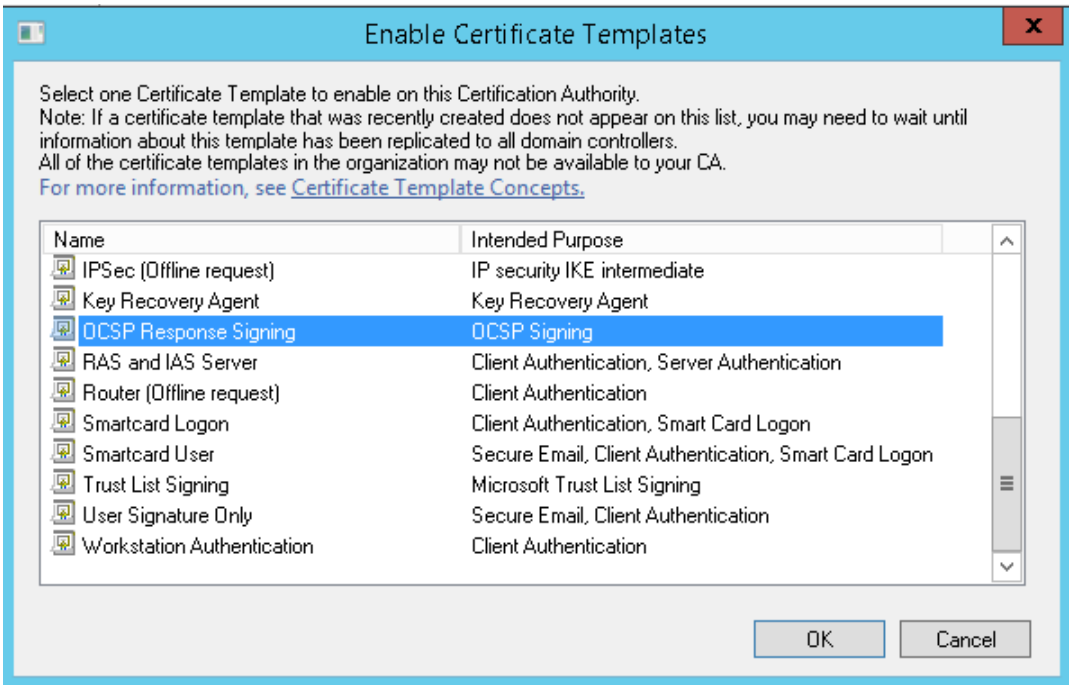



18. Tắt cửa sổ **Certificate Templates**.

19. Trong cửa sổ **Certification Authority**, chuột phải **Certificate Templates**, chọn **New**, và chọn **Certificate Template to Issue**.

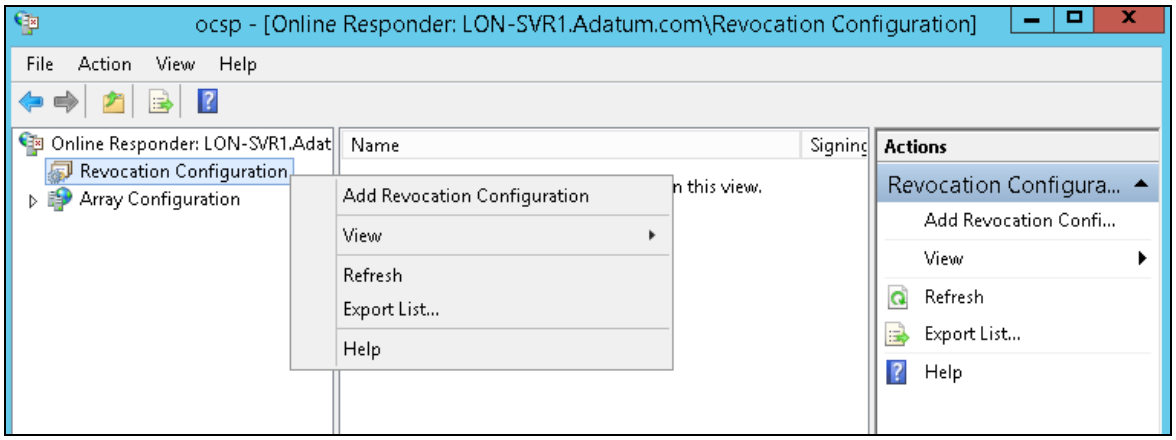



20. Hộp thoại **Enable Certificate Templates**, chọn **OCSP Response Signing**, và chọn **OK**.

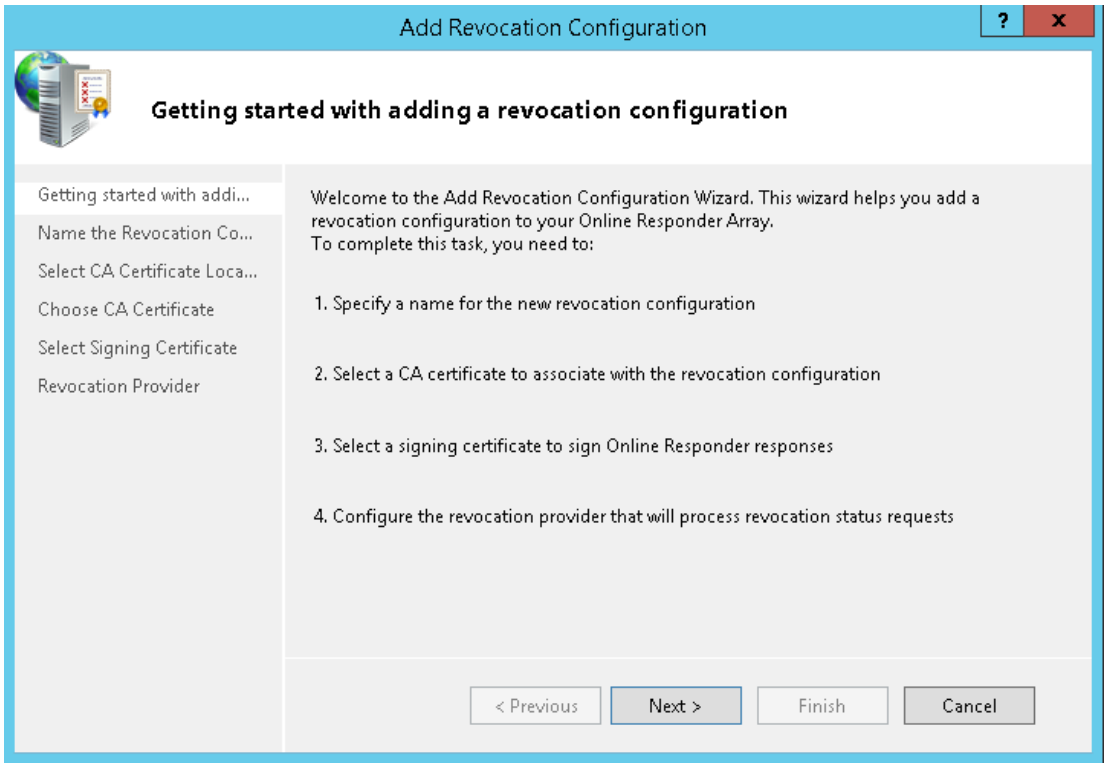


21. Trên máy **LON-SVR1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Online Responder Management**.

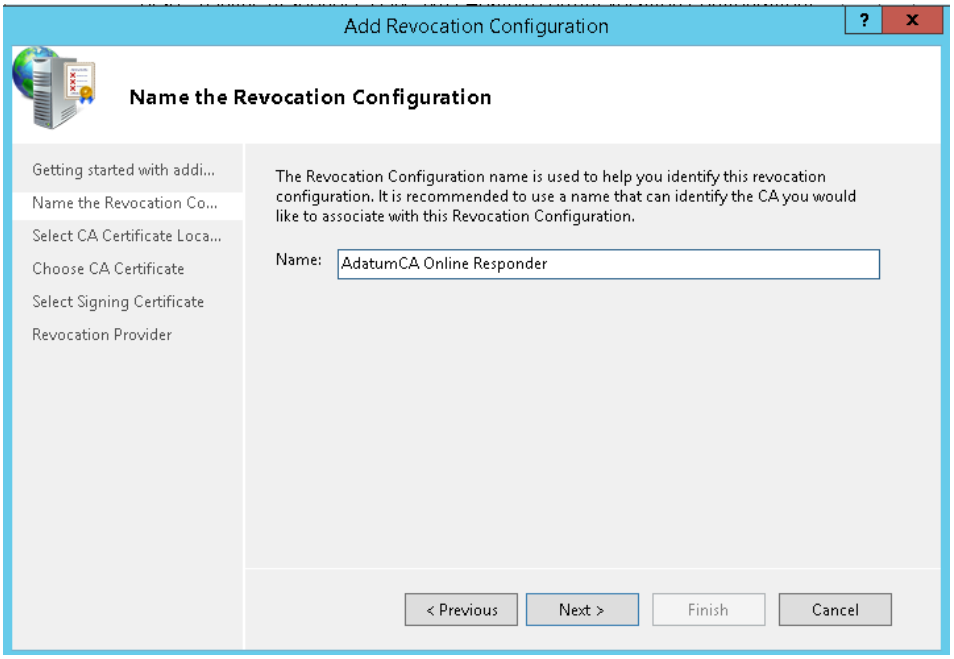
22. Trong cửa sổ **OCSP Management**, chuột phải **Revocation Configuration**, và chọn **Add Revocation Configuration**.



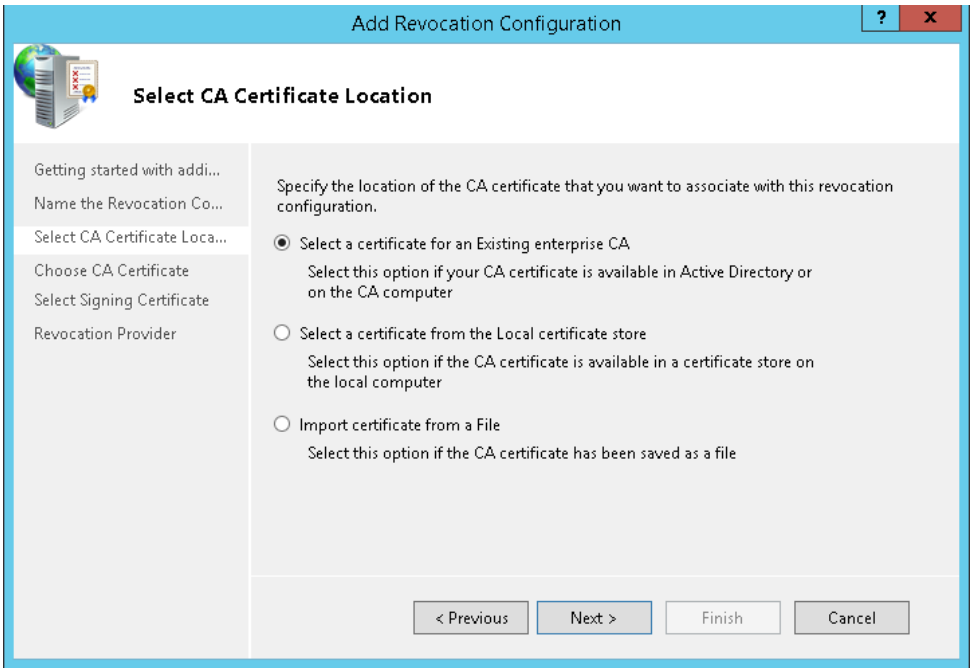

23. Cửa sổ **Add Revocation Configuration**, chọn **Next**.



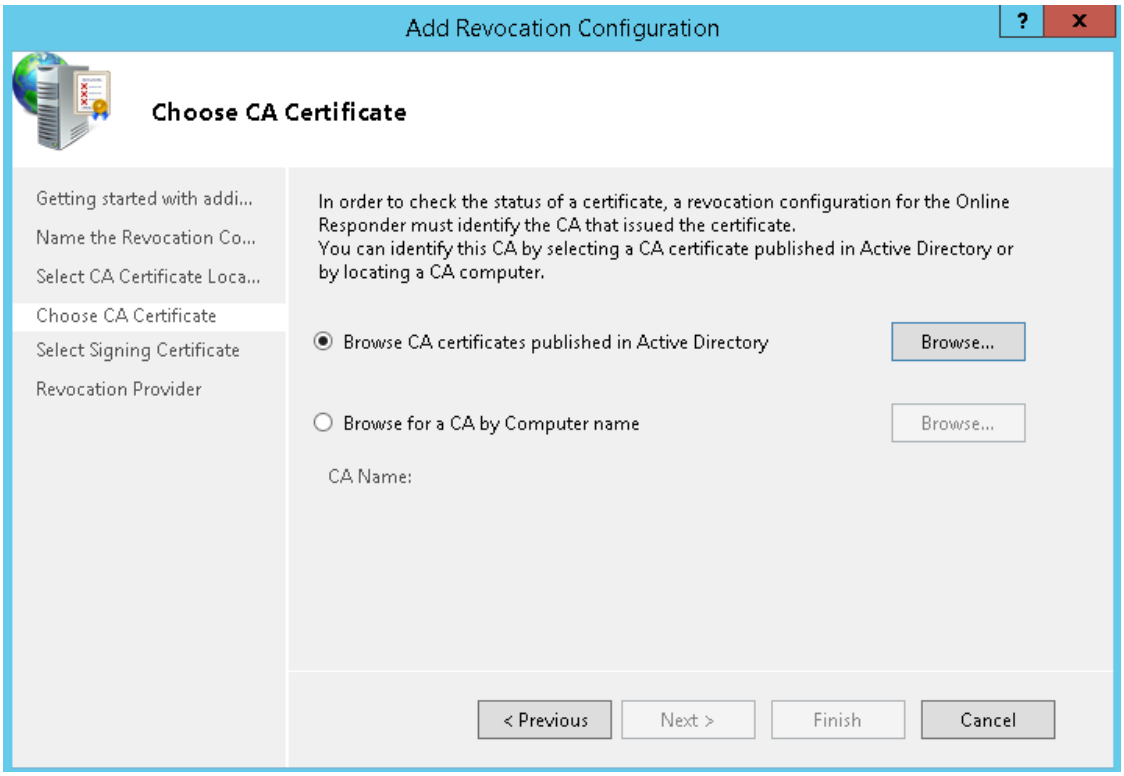
24. Cửa sổ **Name the Revocation Configuration**, trong ô **Name**, nhập **AdatumCA Online Responder**, và chọn **Next**.



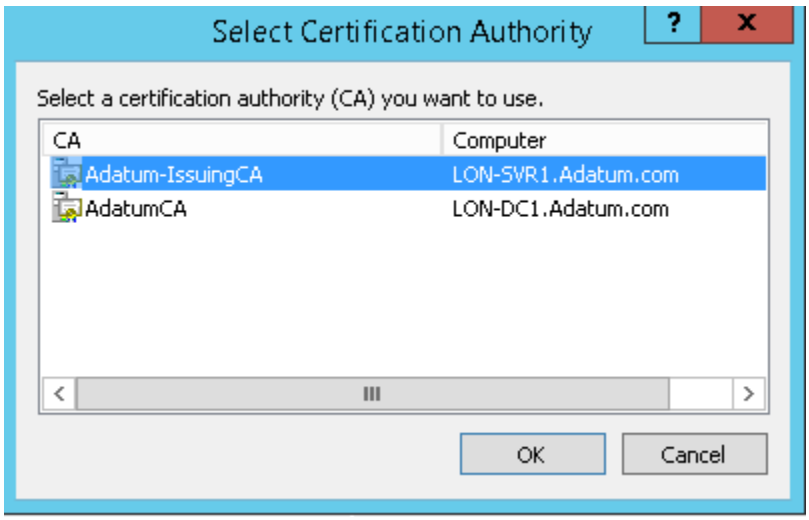

25. Cửa sổ **Select CA Certificate Location**, chọn **Next**.



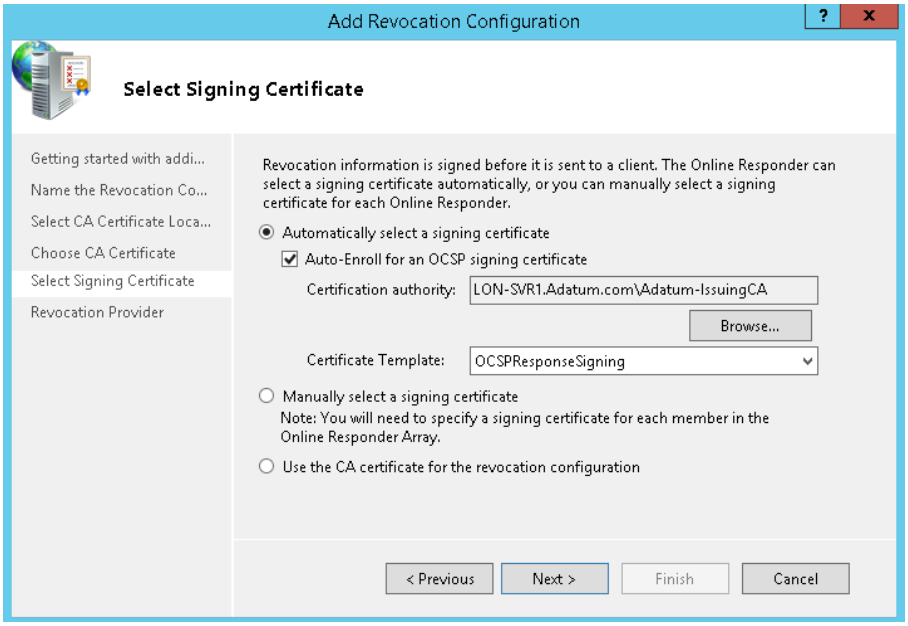
26. Cửa sổ **Choose CA Certificate**, chọn **Browse**.



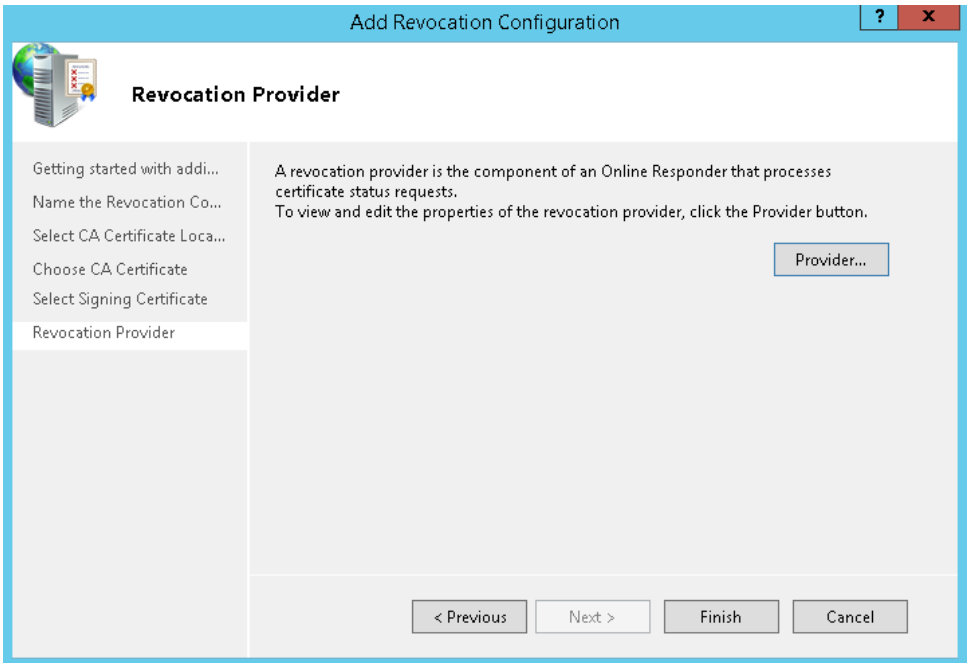

27. Chọn certificate **Adatum-IssuingCA**, chọn **OK**, và chọn **Next**.



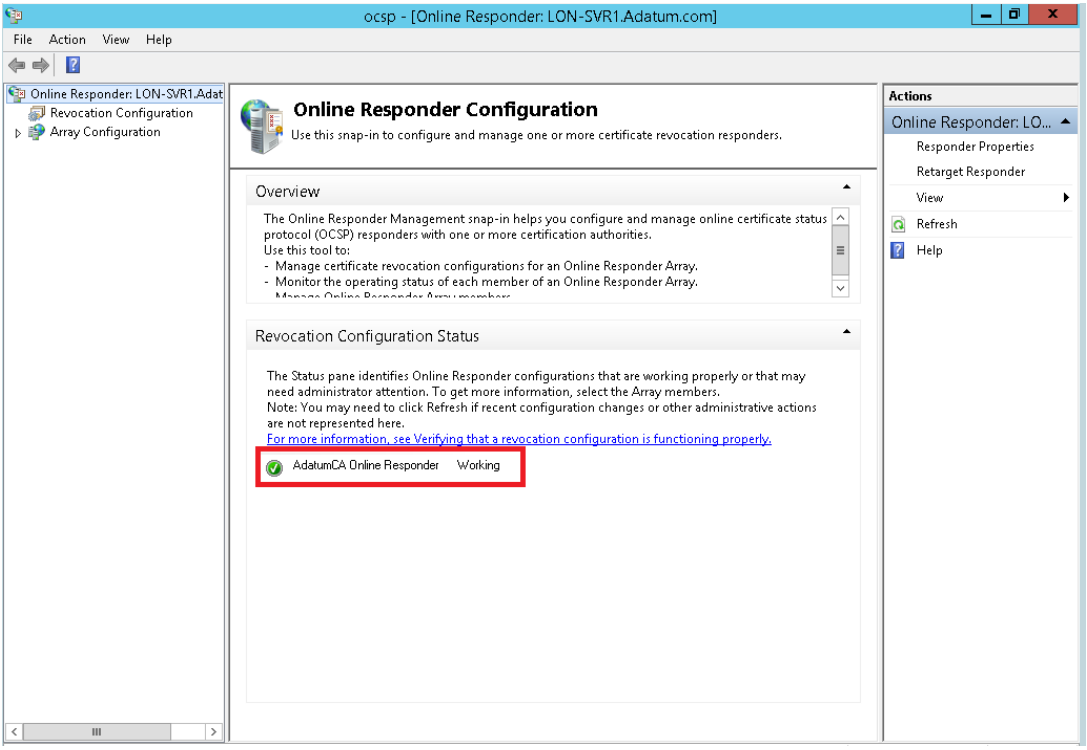
28. Cửa sổ **Select Signing Certificate**, kiểm tra có chọn **Automatically select a signing certificate** và **Auto-Enroll for an OCSP signing certificate**, chọn **Next**.




29. Cửa sổ **Revocation Provider**, chọn **Finish**.



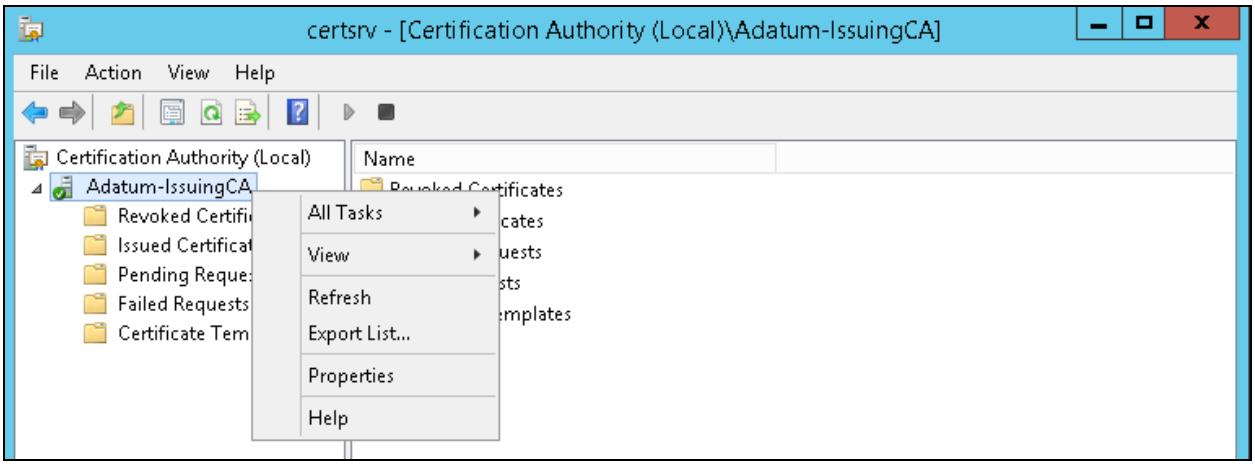
30. Kiểm tra trạng thái đang là **Working**. Tắt cửa sổ **Online Responder**.



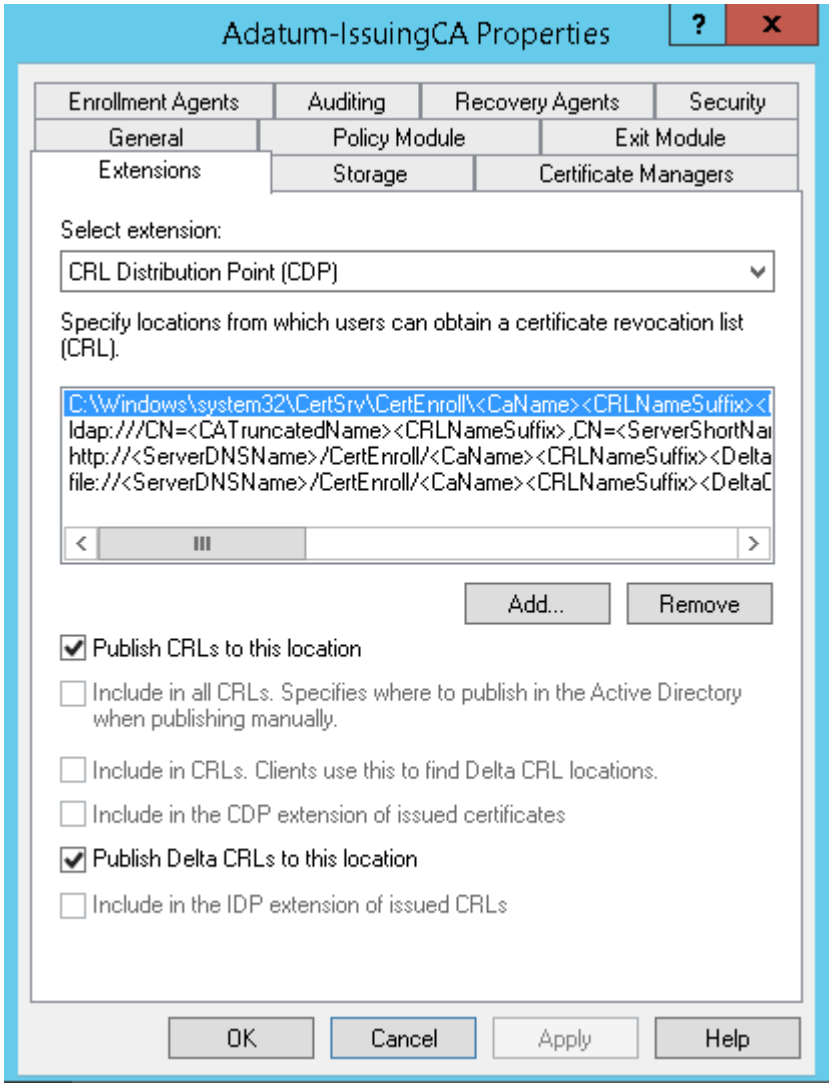

## Bước 2. Cấu hình chức năng Certificate Revocation checking cho DirectAccess clients.

1. Trên máy **LON-SVR1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Certification Authority**.

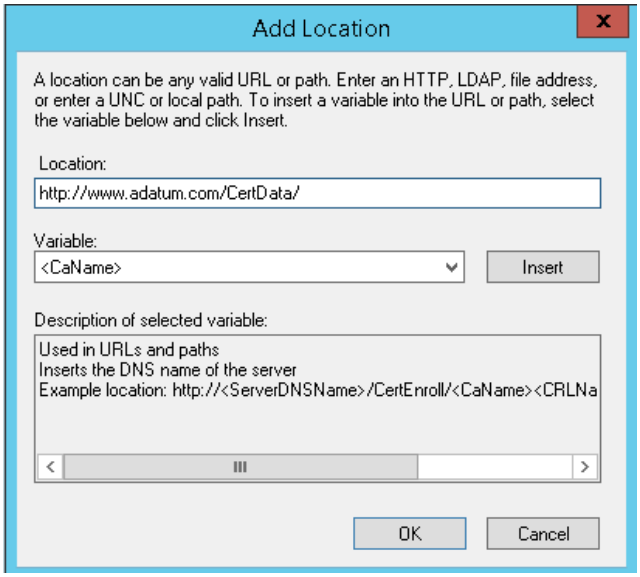
2. Trong cửa sổ **Certification Authority**, chuột phải **Adatum-IssuingCA**, chọn **Properties**.



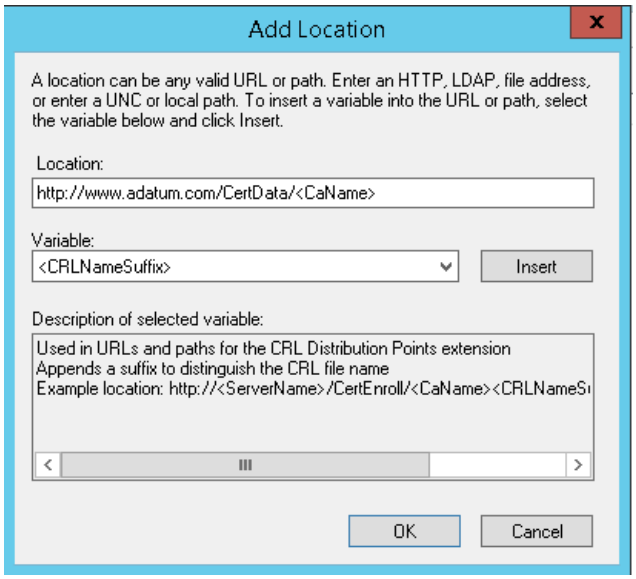
3. Trong hộp thoại **Adatum-IssuingCA Properties**, qua tab **Extensions**, bung ô **Select extension**, chọn **CRL Distribution Point (CDP)**, và chọn **Add**.



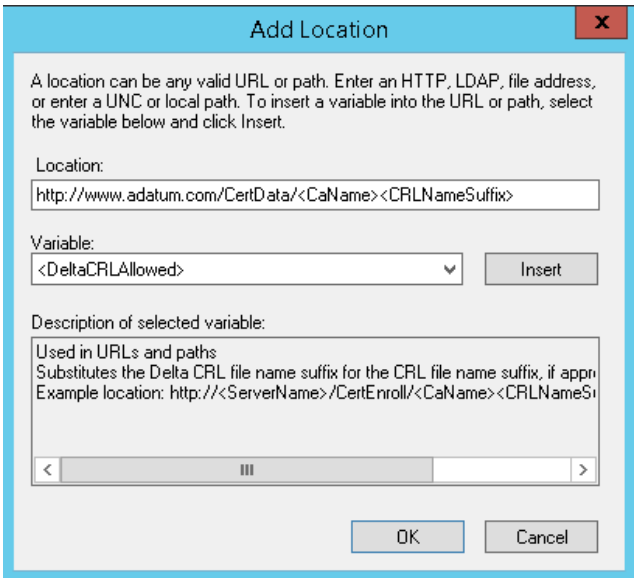
4. Trong ô **Location**, nhập **http://www.adatum.com/CertData/**, bung ô **Variable**, chọn **<CaName>**, và chọn **Insert**.



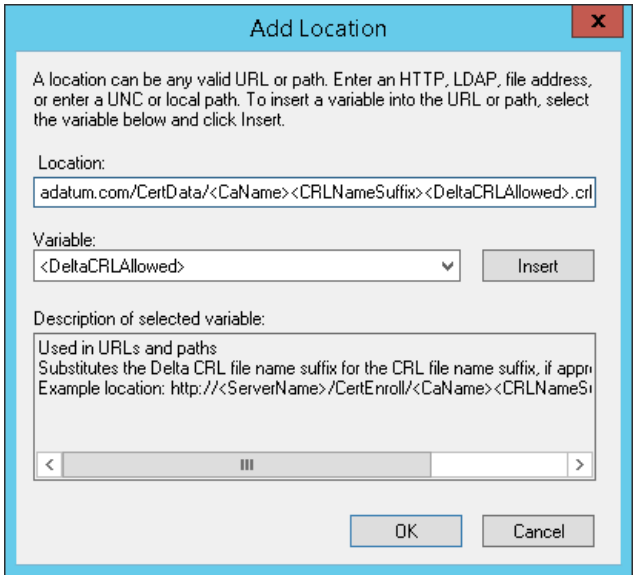

5. Bung ô **Variable**, chọn **<CRLNameSuffix>**, và chọn **Insert**.



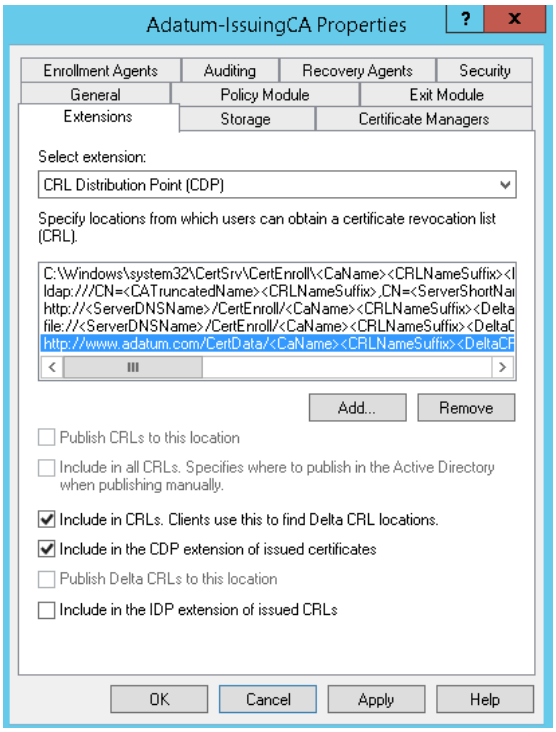
6. Bung ô **Variable**, chọn **<DeltaCRLAllowed>**, và chọn **Insert**.



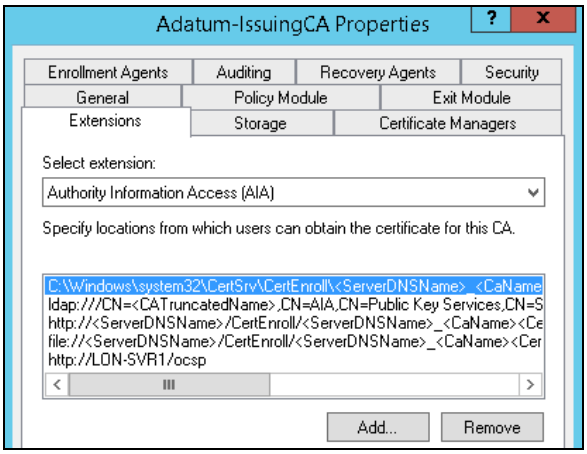

7. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập **.crl**, và chọn **OK**.



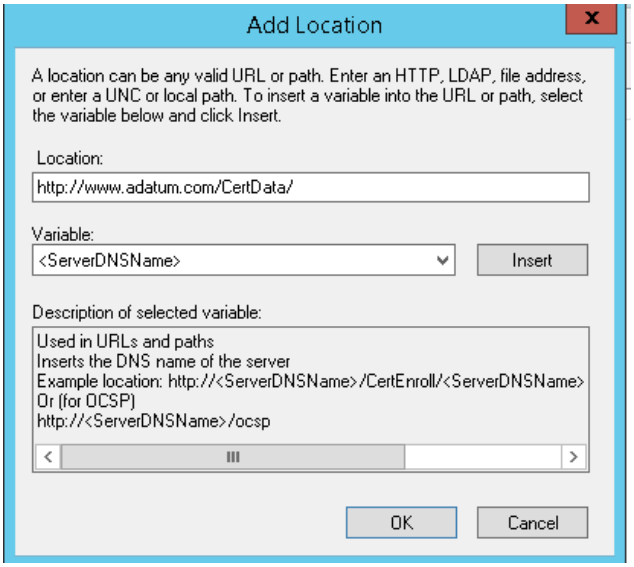
8. Đánh dấu chọn 2 ô **Include in the CDP extension of issued certificates** và **Include in CRLs**. **Clients use this to find Delta CRL locations**, chọn **Apply**. Hộp thoại **Certification Authority**, chọn **No**.



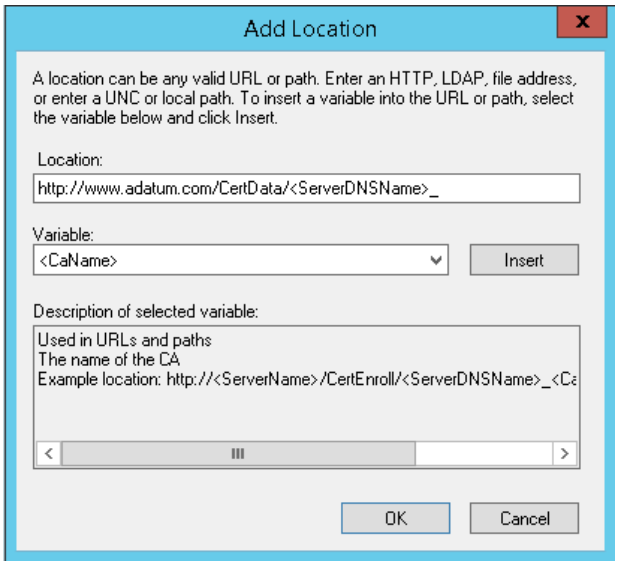

9. Trong tab **Extensions,** bung ô **Select extension**, chọn **Authority Information Access (AIA)**, và chọn **Add**.



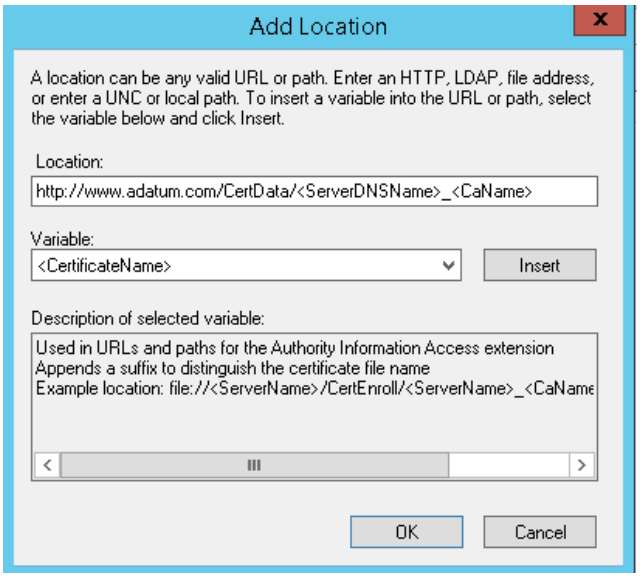
10. Trong ô **Location**, nhập **http://www.adatum.com/CertData/**, bung ô **Variable**, chọn **<ServerDNSName>**, chọn **Insert**.



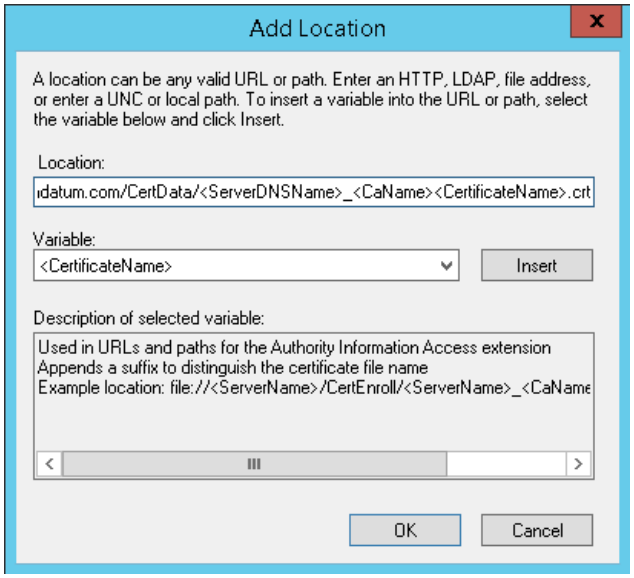

11. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập thêm dấu gạch dưới (_), bung ô **Variable**, chọn **<CaName>**, và chọn **Insert**.



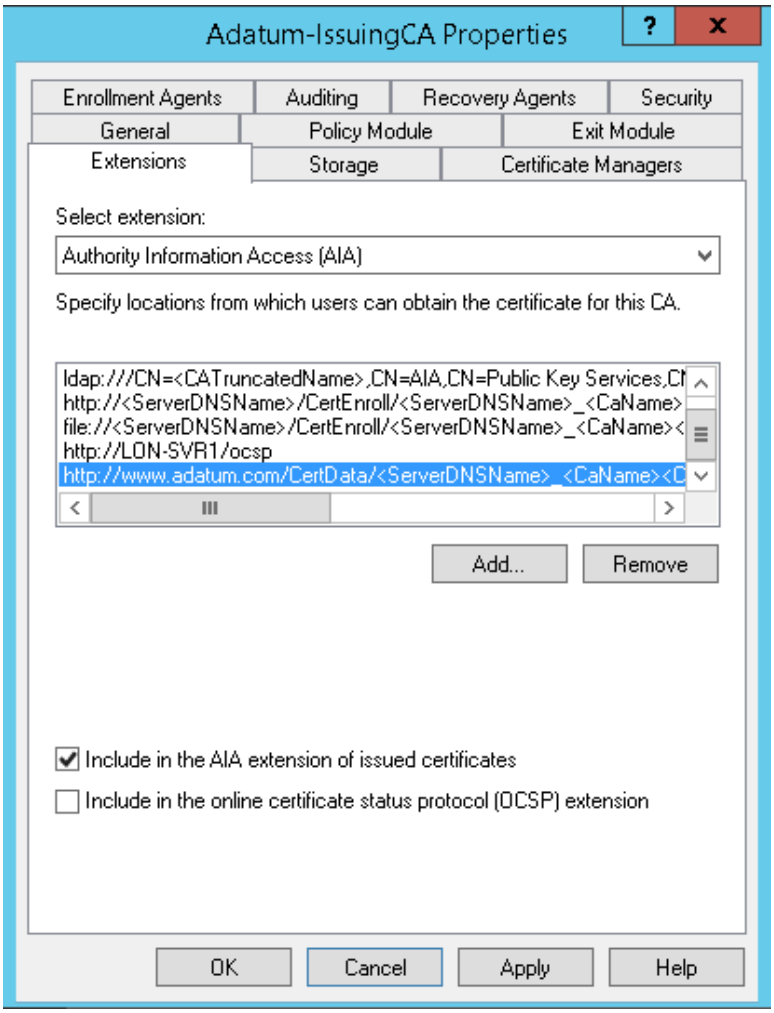
12. Bung ô **Variable**, chọn **<CertificateName>**, và chọn **Insert**.



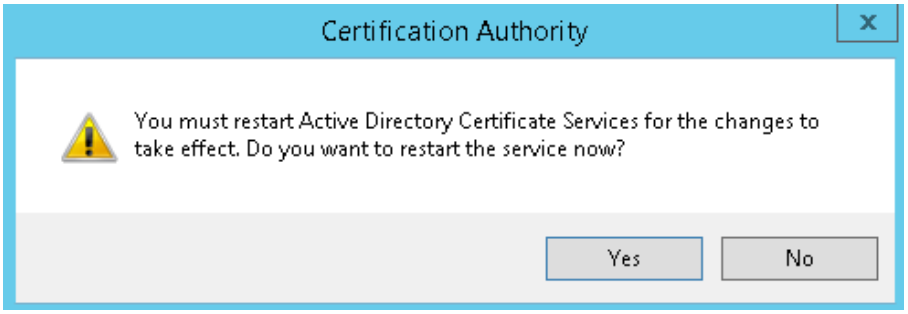

13. Trong ô **Location**, đưa con trỏ về cuối đường dẫn URL, nhập **.crt**, và chọn **OK**.



14. Đánh dấu chọn **Include in the AIA extension of issued certificates**, và chọn **OK**.



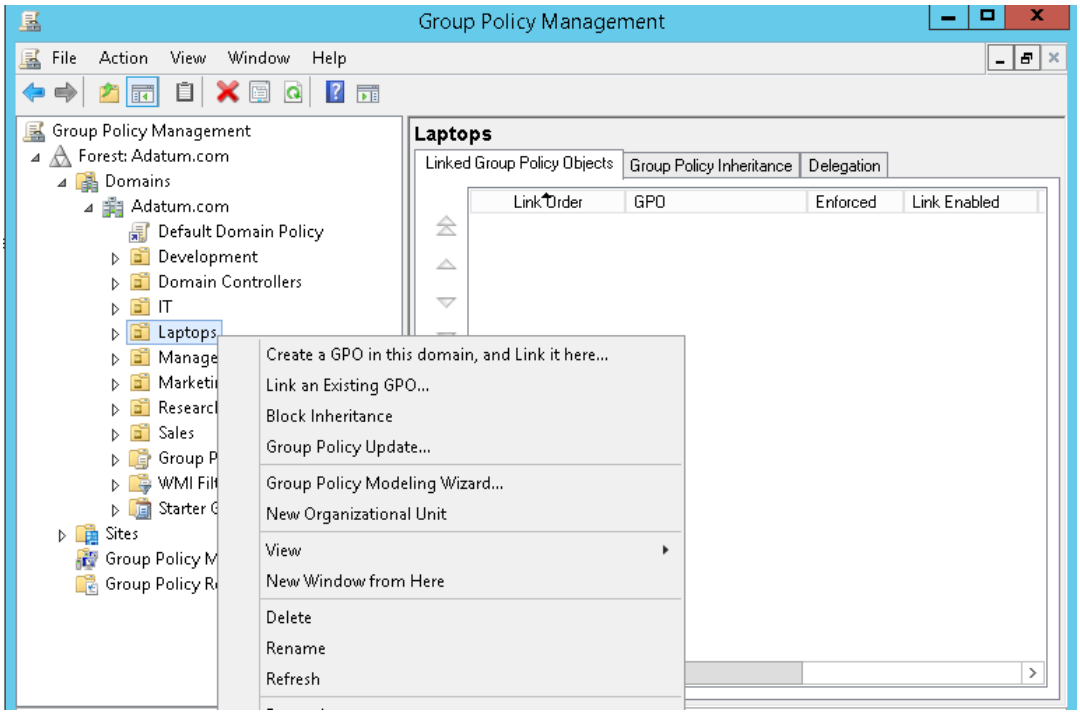

15. Hộp thoại **Certification Authority**, chọn **Yes** để restart Certification Authority service.



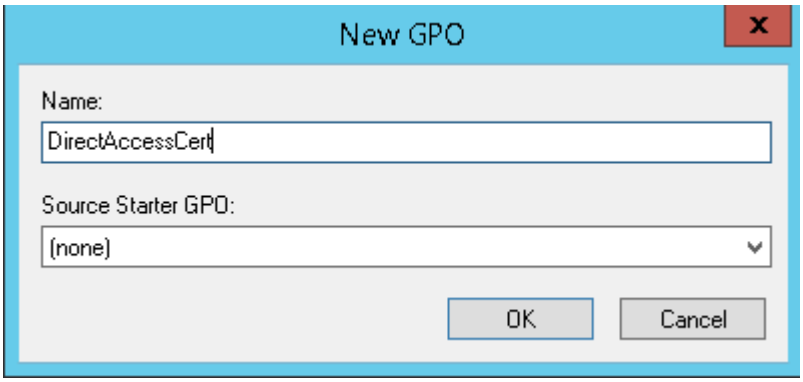
**Bước 3. Cấu hình chức năng tự động phân phối certificate cho user và computer.**

1. Trên máy **LON-DC1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Group Policy Management**.

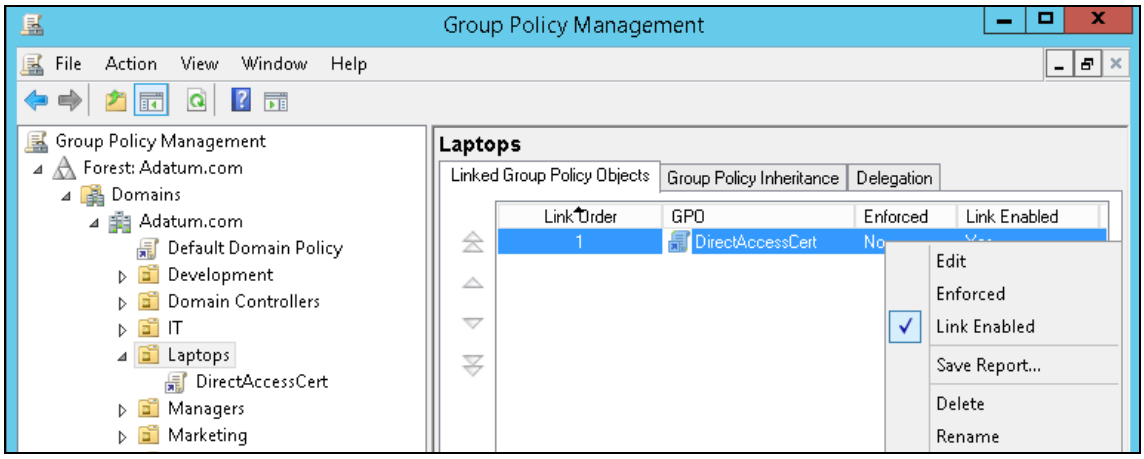
2. Trong cửa sổ **Group Policy Management**, bung **Forest:Adatum.com**, bung **Domains**, bung **Adatum.com**, chuột phải lên OU **Laptops**, chọn **Create a GPO in this domain, and Link it here**.



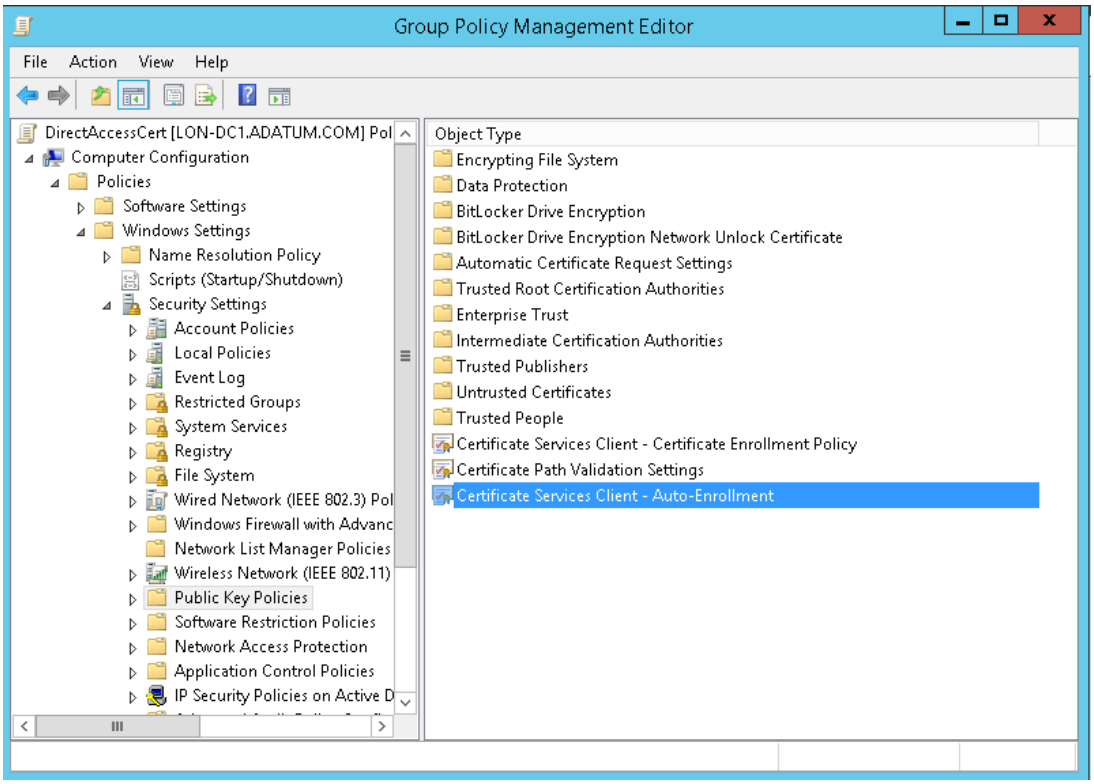

3. Hộp thoại **New GPO**, trong ô **Name**, nhập **DirectAccessCert**, và chọn **OK**.



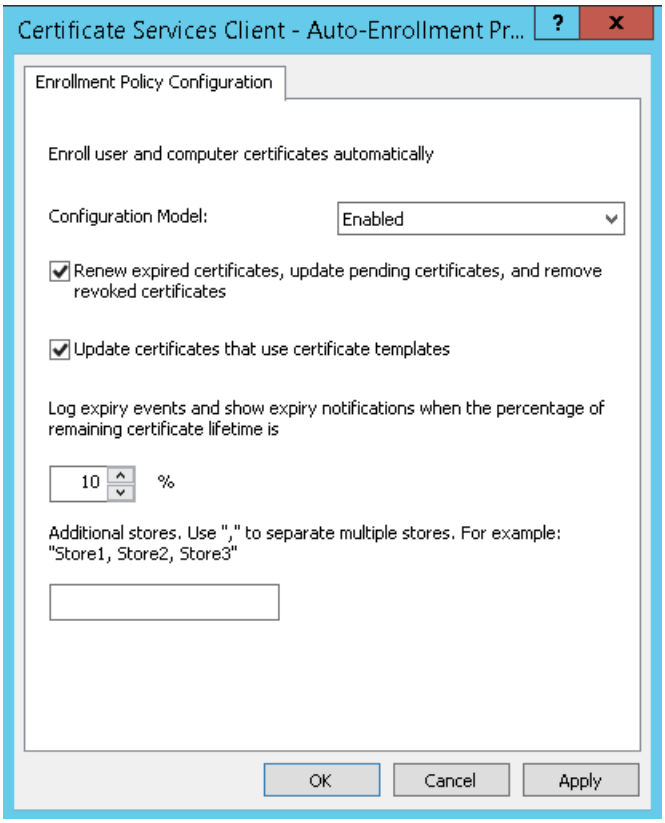
4. Trong OU **Laptops**, chuột phải lên GPO **DirectAccessCert**, chọn **Edit**.




5. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, chọn **Public Key Policies**, nhấp đôi chuột lên policy **Certificate Services Client – Auto-Enrollment**.

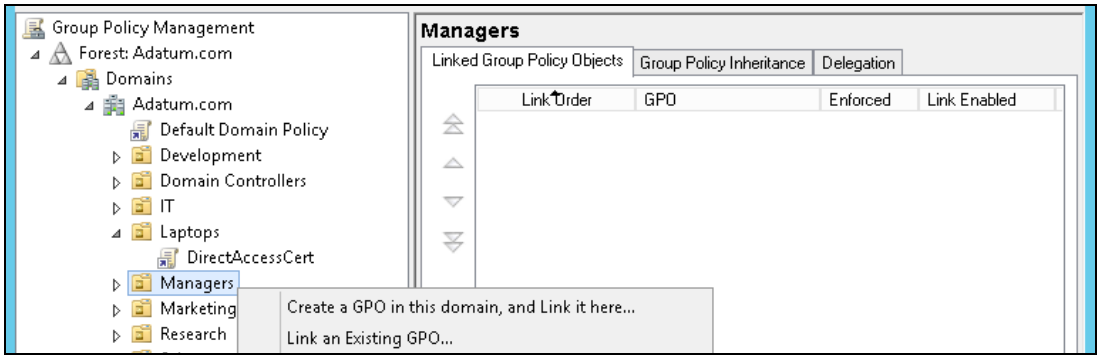


6. Hộp thoại **Certificate Services Client – Auto-Enrollment Properties**, bung ô **Configuration Model**, chọn **Enabled**. Đánh dấu chọn 2 ô **Renew expired certificates, update pending certificates, and remove revoked certificates** và **Update certificates that use certificate templates**, chọn **OK**.

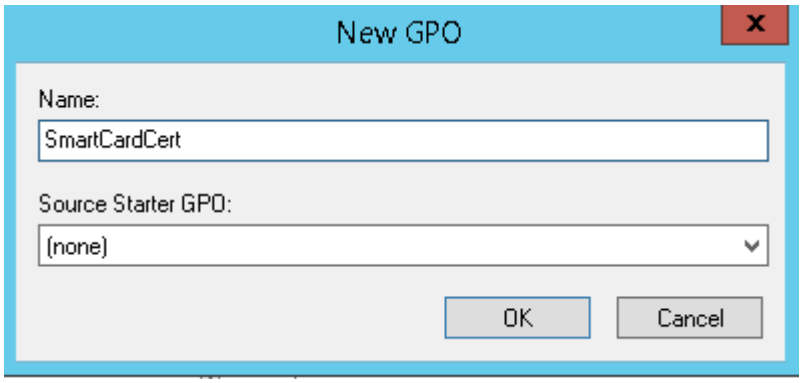



7. Tắt cửa sổ **Group Policy Management Editor**.

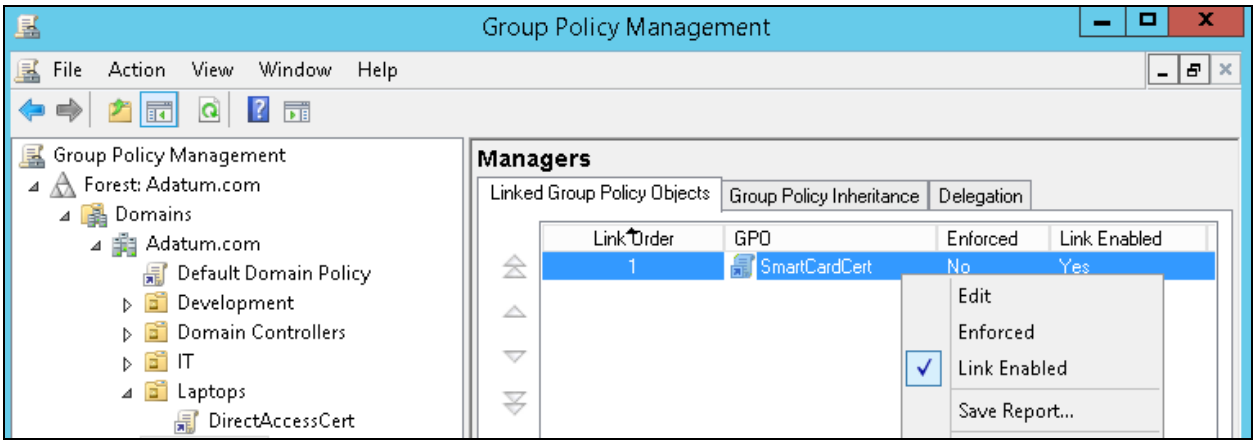
8. Trong cửa sổ **Group Policy Management**, bung **Forest:Adatum.com**, bung **Domains**, bung **Adatum.com**, chuột phải OU **Managers**, chọn **Create a GPO in this domain, and Link it here**.



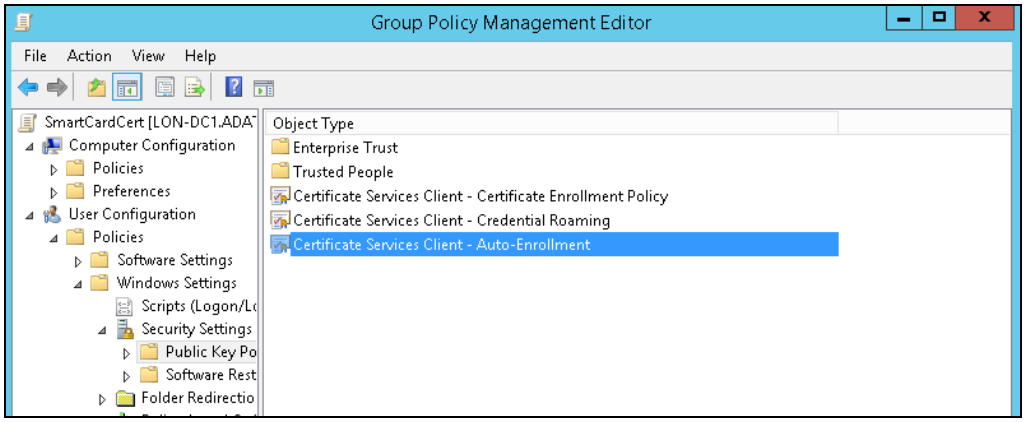

9. Hộp thoại **New GPO**, trong ô **Name**, nhập **SmartCardCert**, và chọn **OK**.



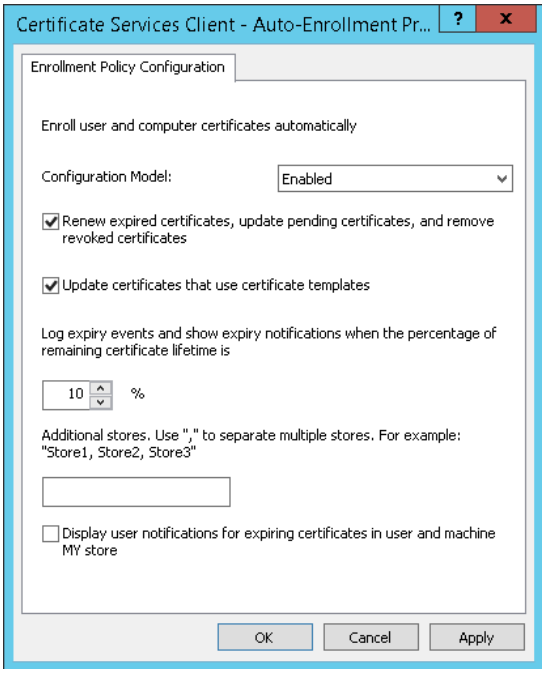

10. Trong OU **Managers**, chuột phải lên GPO **SmartCardCert**, chọn **Edit**.



11. Trong cửa sổ **Group Policy Management Editor**, bung **User Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, chọn **Public Key Policies**, nhấp đôi chuột lên policy **Certificate Services Client – Auto-Enrollment**.




12. Hộp thoại **Certificate Services Client – Auto-Enrollment Properties**, bung ô **Configuration Model**, chọn **Enabled**. Đánh dấu chọn 2 ô **Renew expired certificates, update pending certificates, and remove revoked certificates** và **Update certificates that use certificate templates**, chọn **OK**.

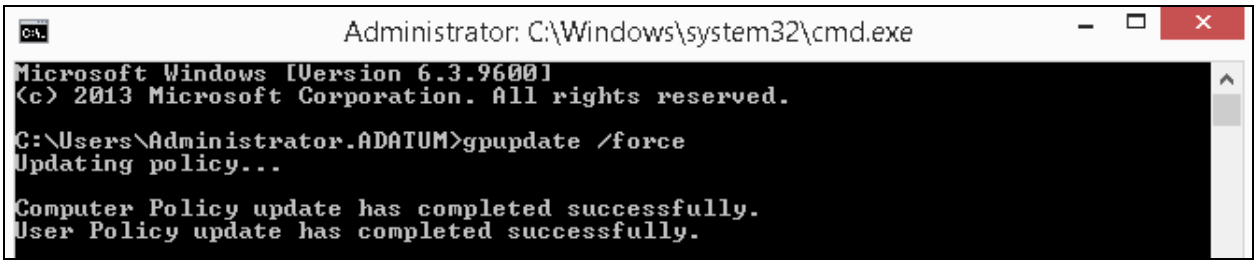


13. Tắt cửa sổ **Group Policy Management Editor** và **Group Policy Management**.

**Bước 4. Xác nhận đăng ký Smart Card certificate và DirectAccess certificate.**

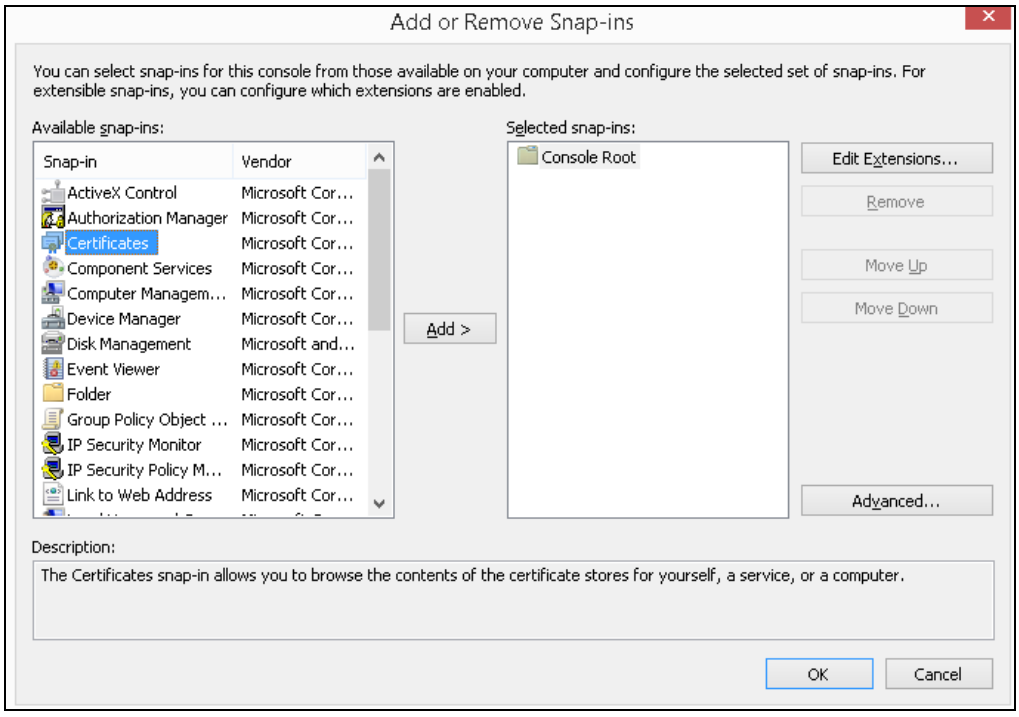
1. Sign in vào máy **LON-CL1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

2. Mở **cmd,** gõ lệnh: **gpupdate /force**

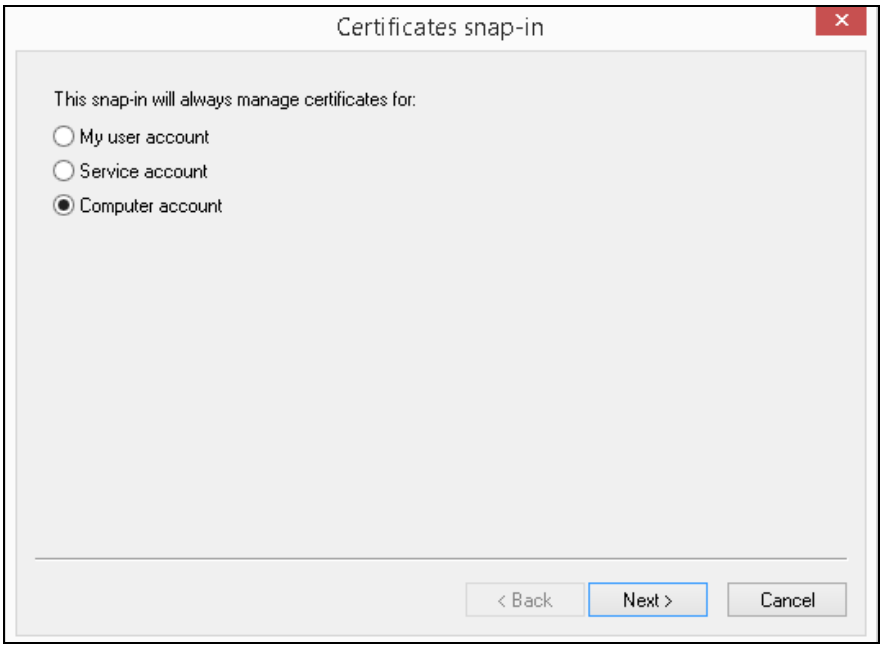



3. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.

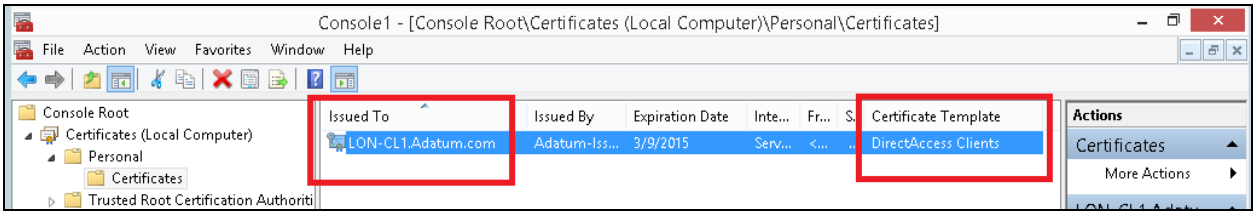
4. Trong cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add**.



5. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**, chọn **Finish**, và chọn **OK**.

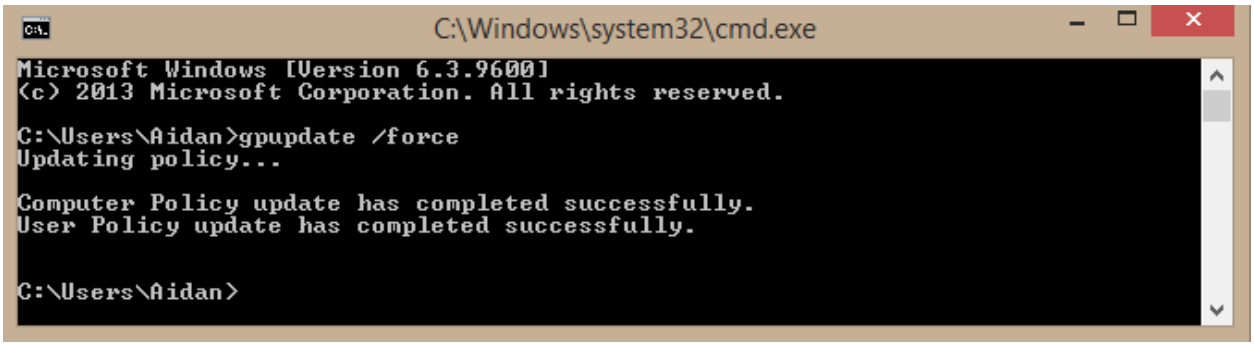



6. Trong cửa sổ **Console1**, bung **Certificates**, bung **Personal**, chọn **Certificates**. Kiểm tra có certificate **LON-CL1.Adatum.com**, sử dụng certificate mẫu là **DirectAccess Clients**.



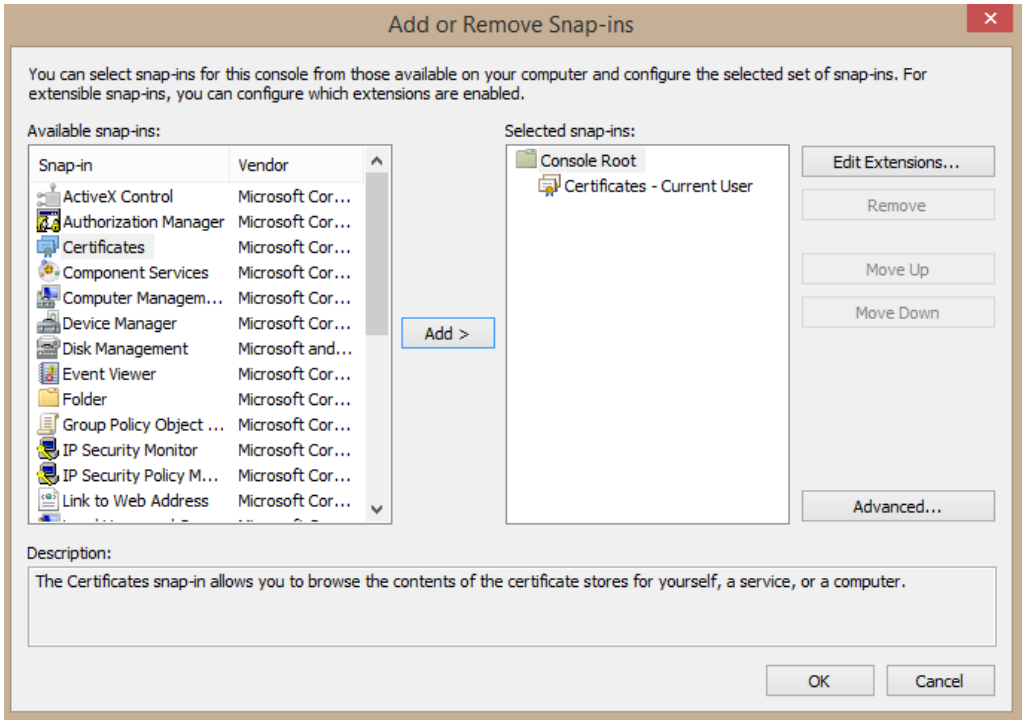

7. Sign out **LON-CL1**, và sign in bằng **Adatum\Aidan** với password **Pa$$w0rd**.

8. Mở **cmd,** gõ lệnh: **gpupdate /force**



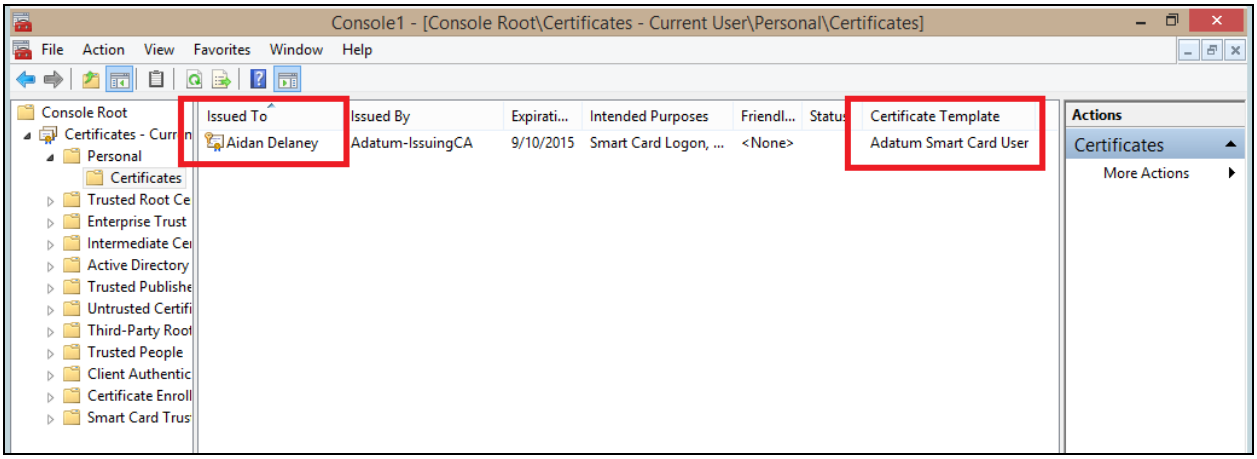

9. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**

10. Trong cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add**, và chọn **OK**.



11. Trong cửa sổ **Console1**, bung **Certificates**, bung **Personal**, chọn **Certificates**.

Kiểm tra user **Aidan Delaney** được cấp một certificate sử dụng certificate mẫu là **Adatum Smart Card User**.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công chức năng tự động phân phối và thu hồi certificate.**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên lại bước 2 và 3 cho máy ảo **20414C-LON-SVR1, 20414C-LON-CA1, và 20414C-LON-CL1.**

# Bài 10: Triển khai Active Directory Federation Services (AD FS)

**I. Mục tiêu:**

- Thiết kế mô hình AD FS.
- Cấu hình các thành phần cần thiết để triển khai AD FS.
- Triển khai AD FS cho người dùng nội bộ.
- Triển khai AD FS cho một tổ chức đối tác.
- Triển khai Web Application Proxy.

**II. Kịch bản:**

Công ty A. Datum đã thiết lập mối quan hệ kinh doanh với các công ty khác và khách hàng. Một số công ty đối tác và khách hàng phải được phép truy cập vào các ứng dụng doanh nghiệp của A. Datum. Nhóm kinh doanh tại A. Datum muốn cung cấp một mức độ truy cập tối đa chức năng đối với các công ty này. Bộ phận an ninh muốn đảm bảo rằng các đối tác và khách hàng chỉ có thể truy cập vào các nguồn tài nguyên mà họ cần truy cập. Một yêu cầu khác là giải pháp này không nên làm tăng khối lượng công việc cho nhóm quản trị hệ thống.

Để đáp ứng các yêu cầu trên, A. Datum đã quyết định triển khai AD FS. Trong việc triển khai ban đầu, công ty có kế hoạch sử dụng AD FS để hỗ trợ chứng thực Single Sign On (SSO) cho người dùng nội bộ truy cập vào một ứng dụng trên Web Server. A. Datum đã hợp tác với công ty Trey Research, và yêu cầu người sử dụng của Trey Research cũng phải có khả năng truy cập vào ứng dụng này.

**III. Yêu cầu tổng quan:**

Nhóm bảo mật tại A. Datum đưa ra các yêu cầu sau đây cho việc triển khai AD FS:

- Chỉ có người sử dụng từ phòng nghiên cứu và phòng quản lý của A. Datum mới được phép truy cập các ứng dụng thông qua ADFS.
- Các thành viên của bộ phận nghiên cứu cần được chỉ định có vai trò HighSecurity trong ứng dụng AD FS.
- Các thành viên của bộ phận quản lý cần được chỉ định có vai trò Manager trong việc ứng dụng AD FS.
- Nhóm giám đốc điều hành tại Trey Research cần phải có quyền truy cập vào các ứng dụng ADFS. Còn nhân viên nên được chỉ định có vai trò ExternalSecure trong ứng dụng AD FS.
- Những người dùng làm việc tại nhà phải có khả năng truy cập các ứng dụng ADFS bằng cách sử dụng thông tin AD DS của họ.

**IV. Mô hình thực hành gồm các máy:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-HOST1**<br>**20414C-LON-DC1**<br>**20414C-LON-SVR2**<br>**20414C-LON-SVR3**<br>**20414C-LON-CL1**<br>**20414C-TREY-DC1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy thật, khởi động vào **20414C-LON-HOST1**.
2. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
3. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
4. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
5. Thực hiên lại từ bước 2 đến 4 cho máy ảo **20414C-LON-SVR2, 20414C-LON-SVR3, 20414C-LON-CL1** và **20414C-TREY-DC1.**
6. Logon vào máy **20414C-TREY-DC1** với thông tin sau:
   - User name: **TreyResearch\Administrator**
   - Password: **Pa$$w0rd**

**VI. Thực hành:**

*Thời gian thực hành: 90 phút*

**Bài tập 1: Cấu hình các thành phần cần thiết để triển khai AD FS.**

A. Datum đã triển khai một ứng dụng Windows Identity Foundation (WIF) chạy trên nền web và cần cho phép người dùng truy cập ứng dụng này thông qua AD FS. Bạn phải chuẩn bị các thành phần cần thiết cho việc triển khai AD FS tại A. Datum bằng cách cấu hình phân giải tên DNS, Certificate, và Trust CA.

❖ **Bài tập bao gồm các bước:**

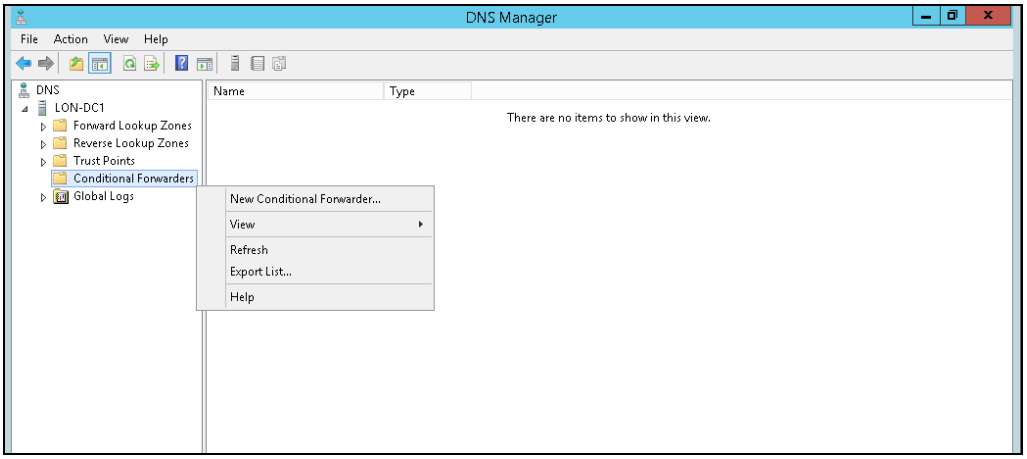
1. Cấu hình DNS Conditional Forwarder.
2. Cấu hình Trusted Root CA.
3. Xin Certificate cho Web Server.
4. Gán Certificate cho ứng dụng trên Web Server, và kiểm tra truy cập.
5. Tạo và xin Certificate cho Server của Trey Research.

❖ **Thực hiện:**

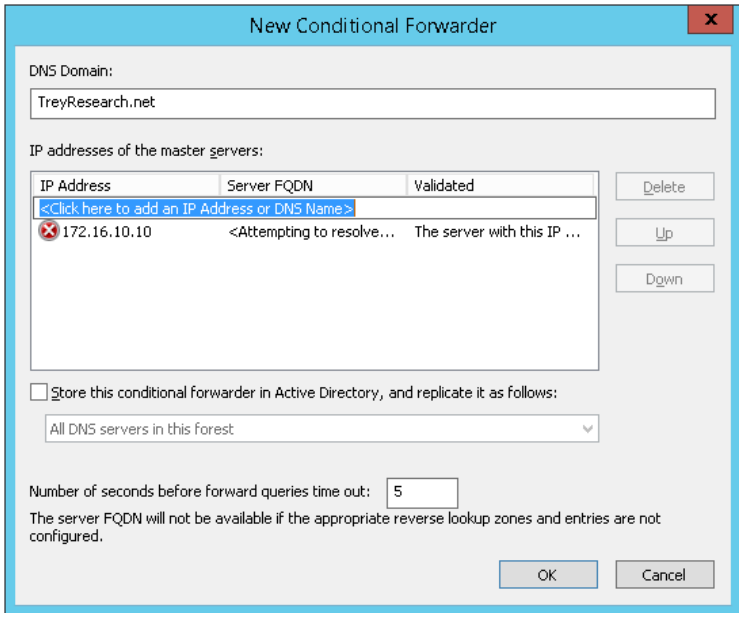
**Bước 1. Cấu hình DNS Conditional Forwarder.**

1. Trên máy **LON-DC1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **DNS**.

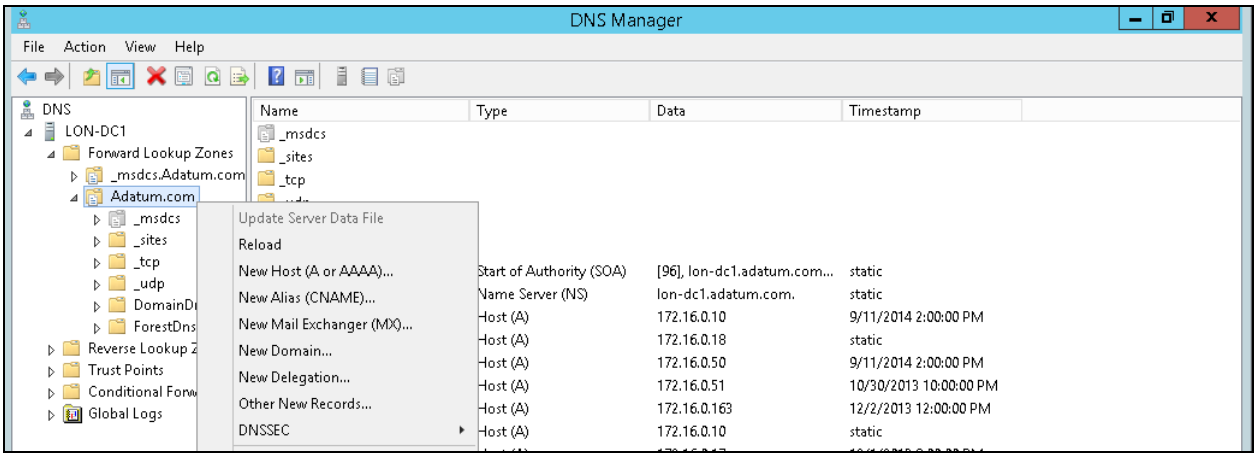
2. Trong cửa sổ **DNS Manager**, bung **LON-DC1**, chuột phải **Conditional Forwarders**, chọn **New Conditional Forwarder**.



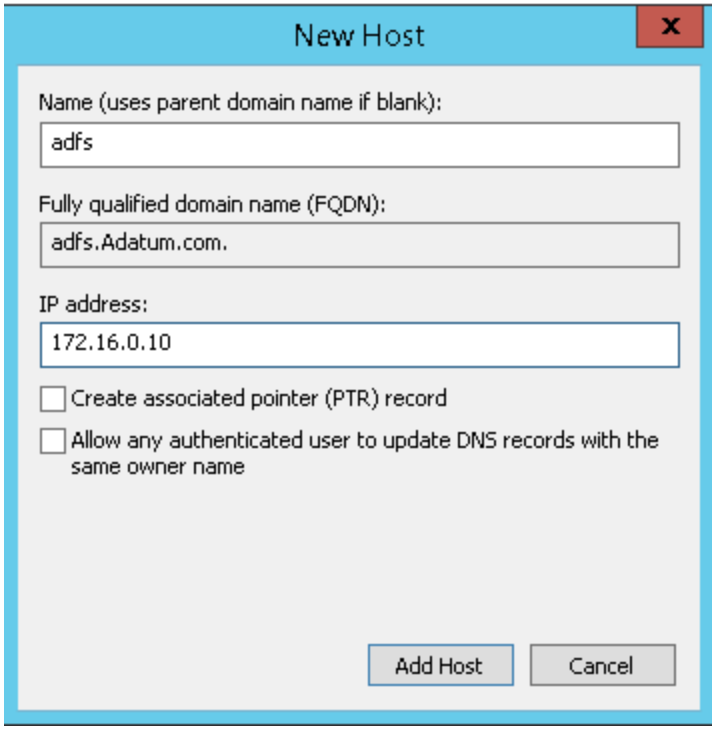

3. Trong ô **DNS Domain**, nhập **TreyResearch.net**. Trong cột **IP address**, nhập **172.16.10.10**, nhấn **Enter**, và chọn **OK**.



4. Bung **Forward Lookup Zones**, chuột phải **Adatum.com**, chọn **New Host (A or AAAA).**



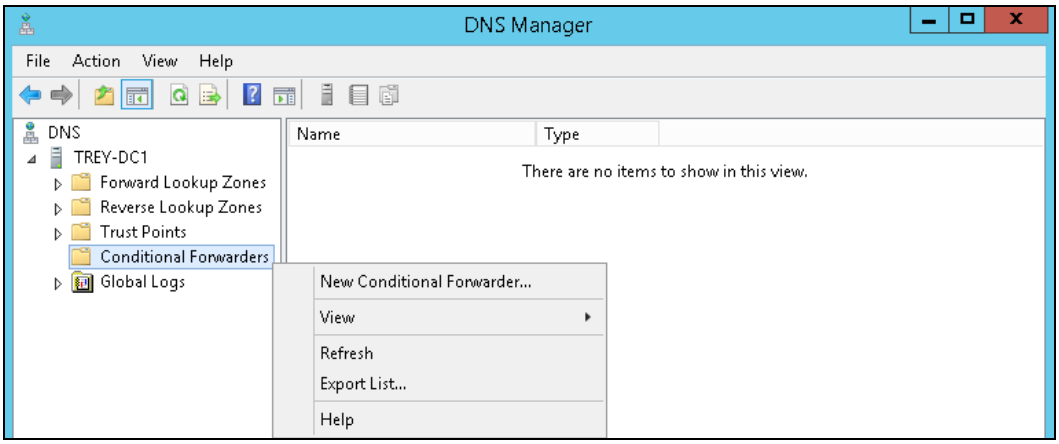

5. Hộp thoại **New Host**, nhập **adfs** vào ô **Name** và nhập **172.16.0.10** vào ô **IP address,** chọn **Add Host**, chọn **OK**, và chọn **Done**.



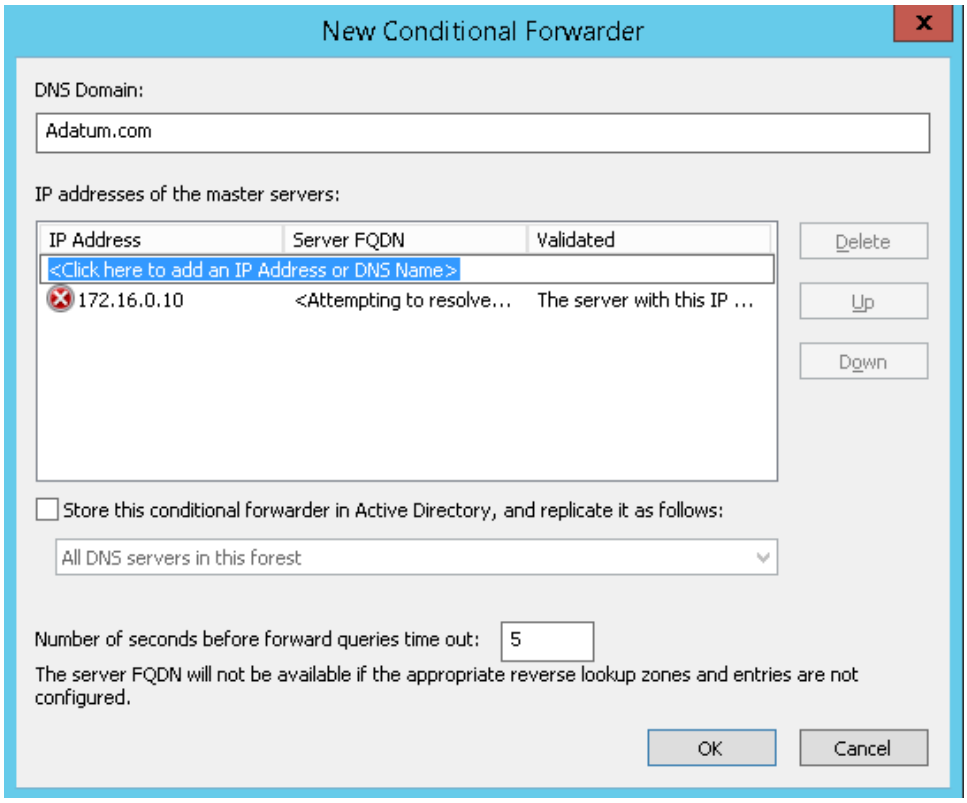

6. Tắt cửa sổ **DNS Manager**.

7. Trên máy **TREY-DC1**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **DNS**.

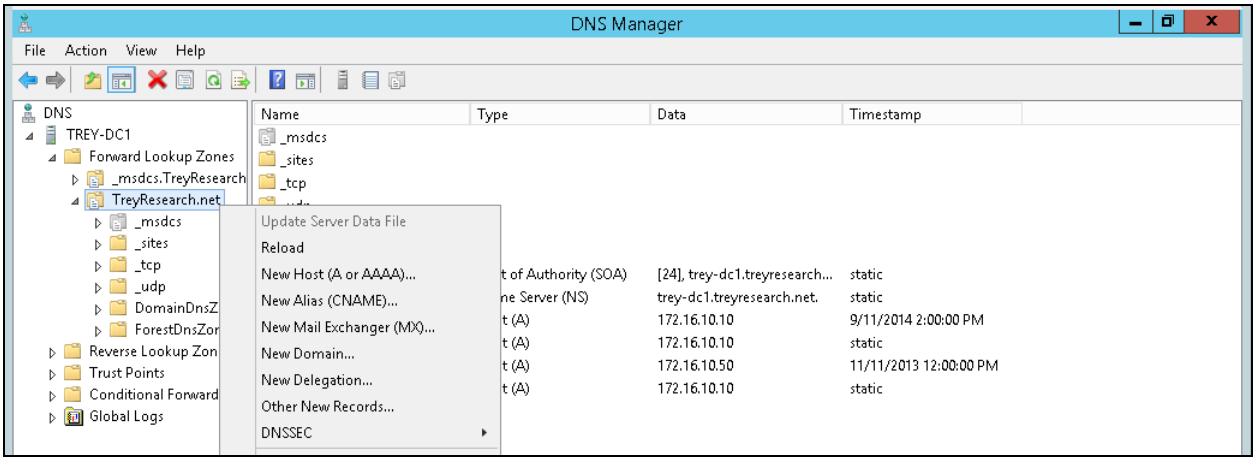
8. Bung **TREY-DC1**, chuột phải **Conditional Forwarders**, chọn **New Conditional Forwarder**.



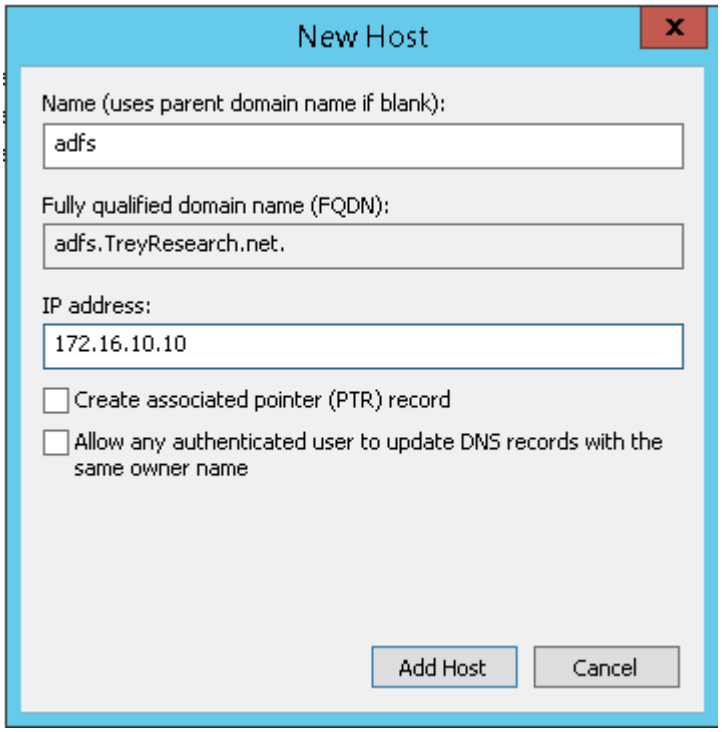

9. Trong ô **DNS Domain**, nhập **Adatum.com**, trong cột **IP address**, nhập **172.16.0.10**, nhấn **Enter**, và chọn **OK**.



10. Bung **Forward Lookup Zones**, chuột phải **TreyResearch.net**, chọn **New Host (A or AAAA)**.



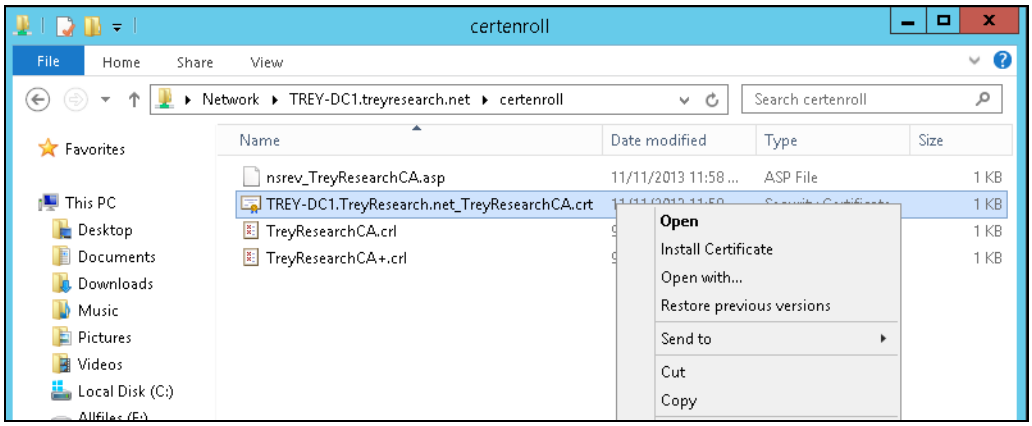

11. Hộp thoại **New Host**, nhập **adfs** vào ô **Name** và nhập **172.16.10.10** vào ô **IP address**, chọn **Add Host**, chọn **OK**, và chọn **Done**. Tắt cửa sổ **DNS Manager**.



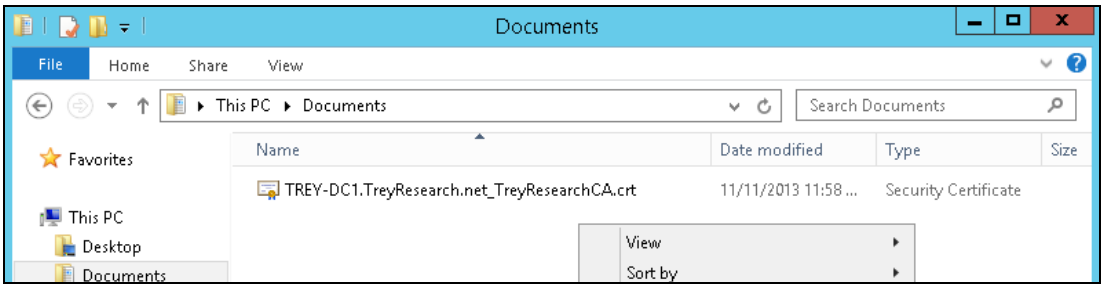
## Bước 2. Cấu hình Trusted Root CA.

1. Trên máy **LON-DC1**.

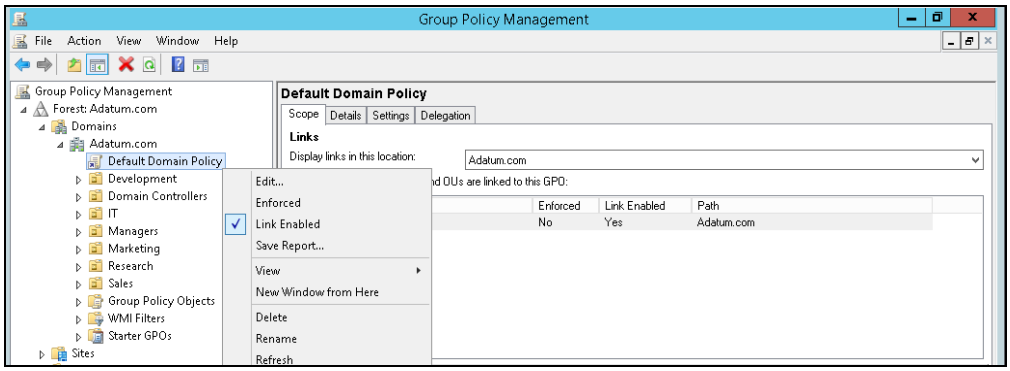
2. Mở File Explorer, truy cập **\\TREY-DC1.treyresearch.net\certenroll**, copy file **TREY-DC1.TreyResearch.net_TreyResearchCA.crt**



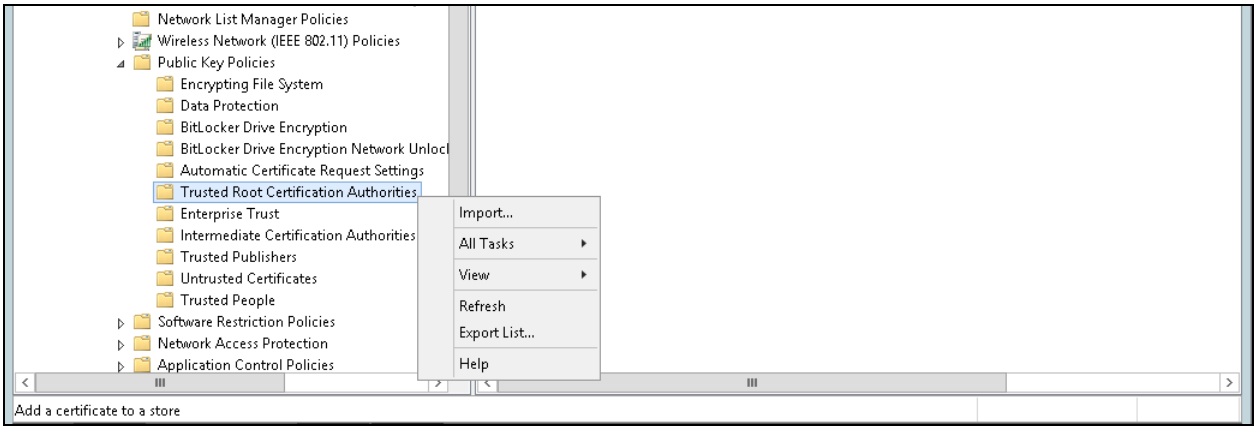

3. Chép file ở bước trên vào **Documents**




4. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Group Policy Management Editor**, chuột phải **Default Domain Policy**, chọn **Edit**.

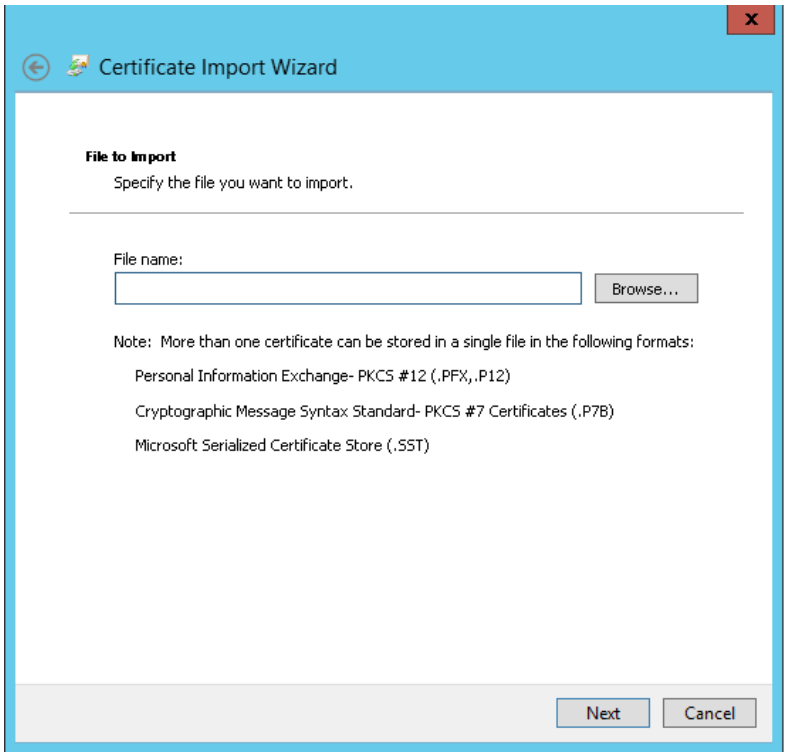


5. Bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **Public Key Policies**, chuột phải **Trusted Root Certification Authorities**, chọn **Import**.

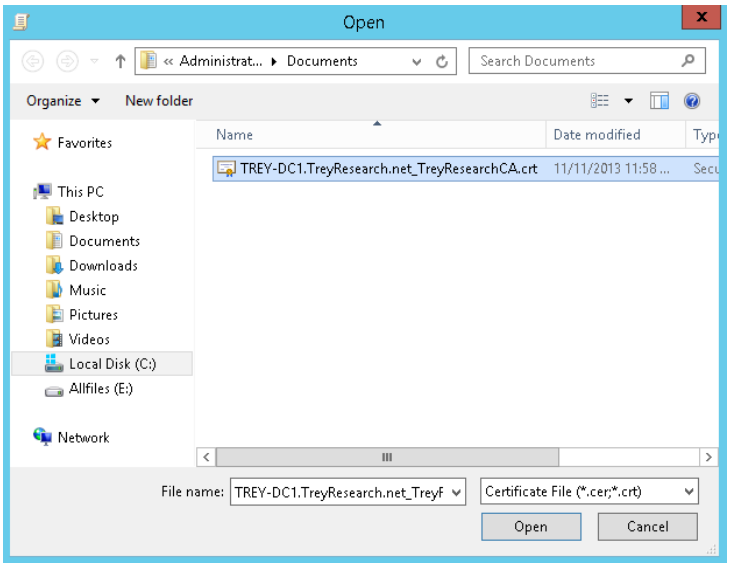



6. Cửa sổ **Welcome to the Certificate Import Wizard**, chọn **Next**.

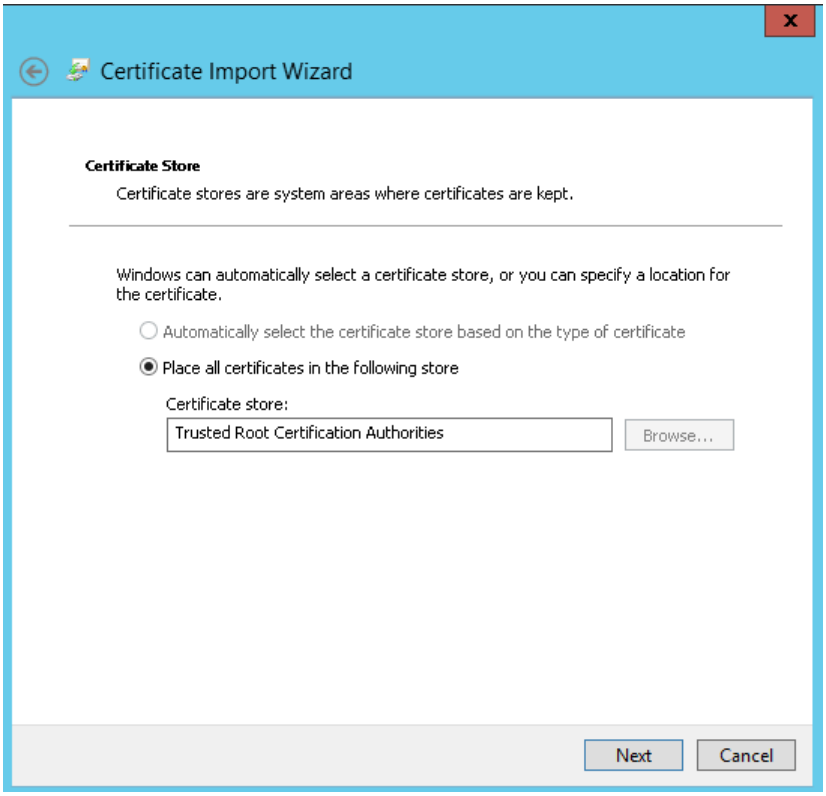
7. Cửa sổ **File to Import**, chọn **Browse**.



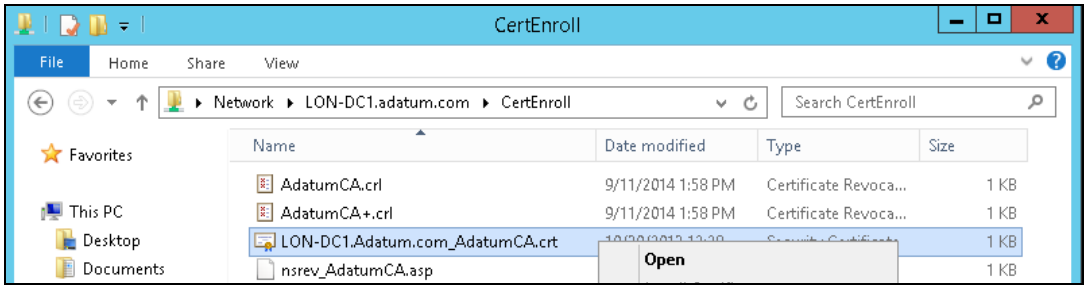
8. Chọn file **TREY-DC1.TreyResearch.net_TreyResearchCA.crt**, chọn **Open**, và chọn **Next**.



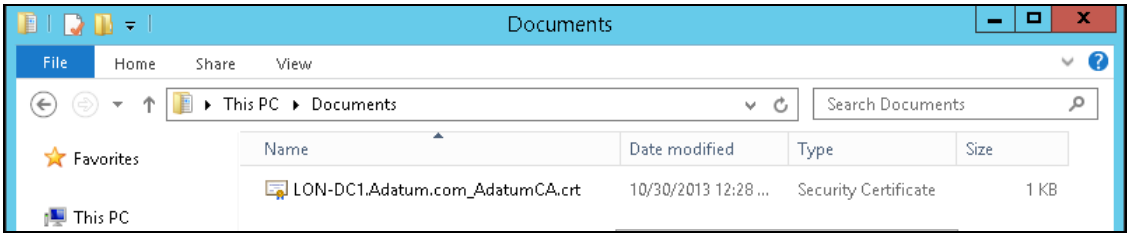

9. Cửa sổ **Certificate Store**, chọn**Next,** chọn **Finish**, chọn **OK**.



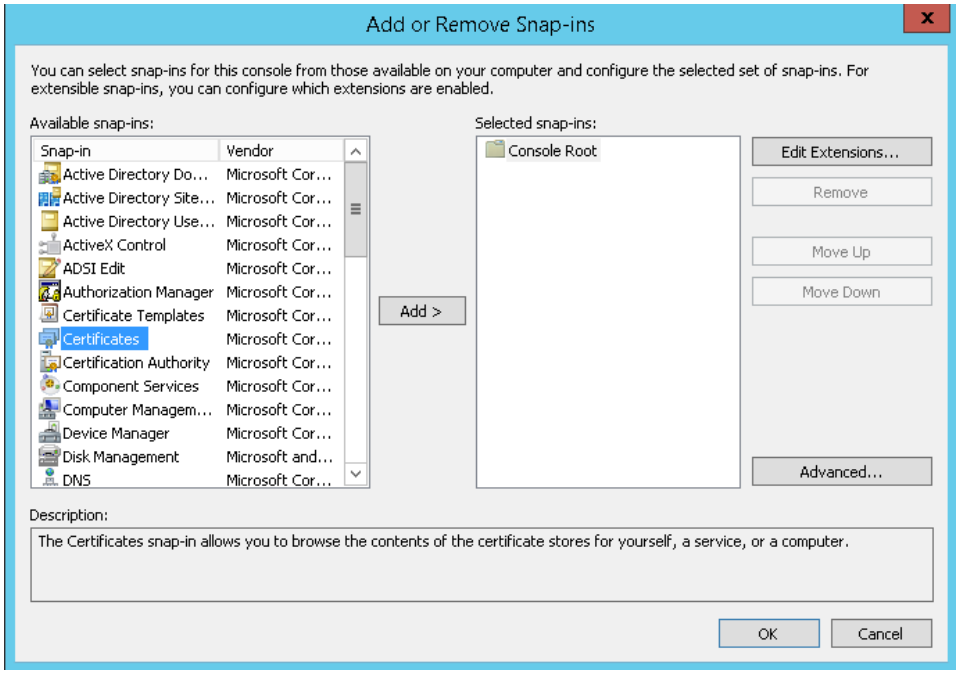
10. Trên máy **TREY-DC1,** mở File Explorer, truy cập **\\LON-DC1.adatum.com\certenroll**, copy file **LON-DC1.Adatum.com_AdatumCA.crt**



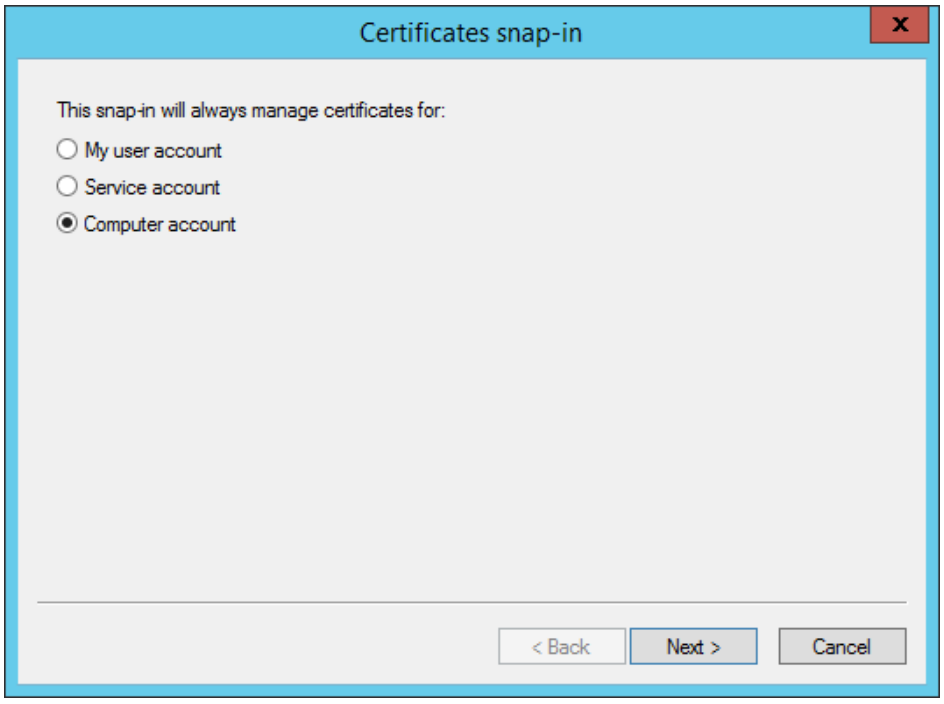

11. Chép file ở bước trên vào **Documents**.



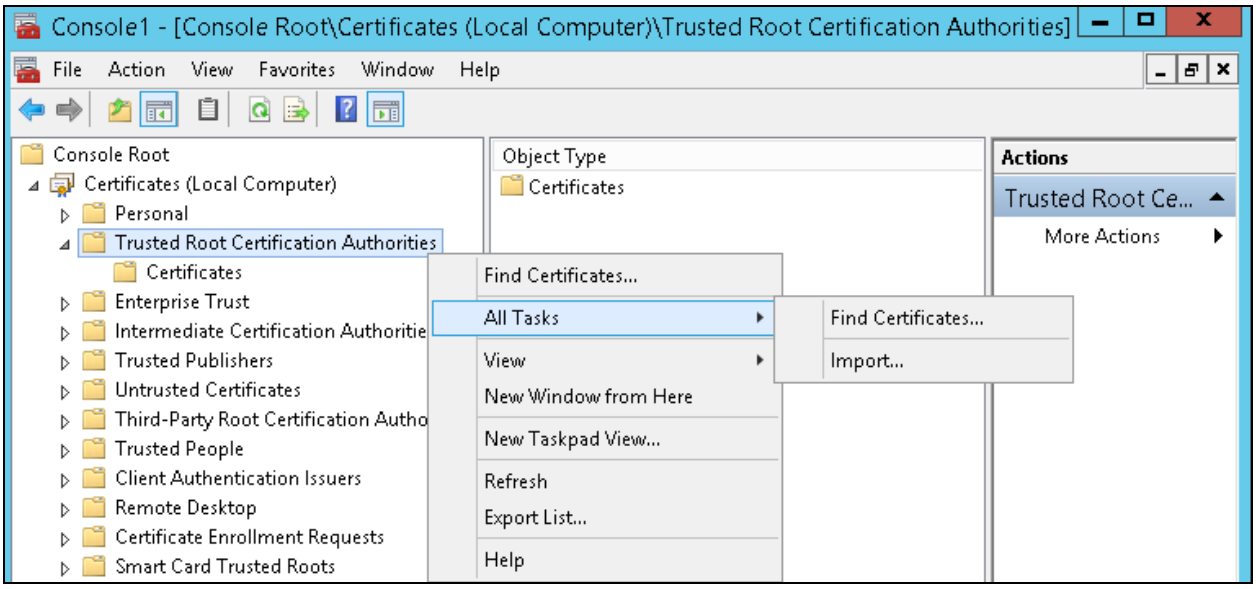

12. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**, chọn mục **Certificates**, chọn **Add**.



13. Chọn **Computer Account**, chọn **Next**, chọn **Finish**, và chọn **OK**.

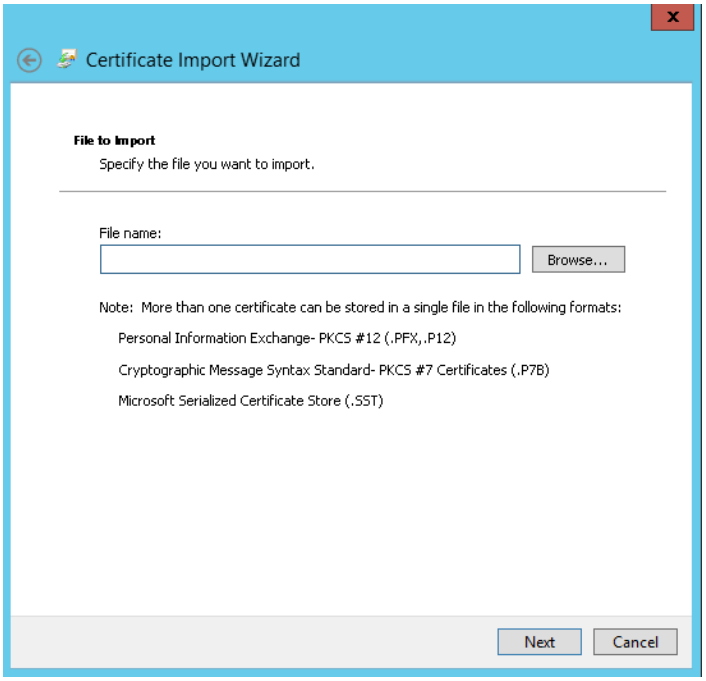



14. Bung **Certificates**, chuột phải **Trusted Root Certification Authorities**, bung **All Tasks**, chọn **Import**.

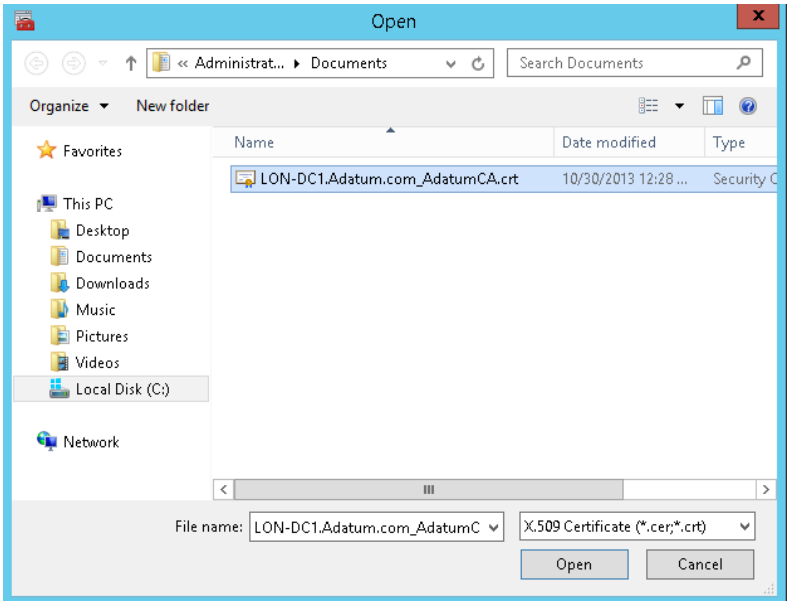


15. Cửa sổ **Welcome to the Certificate Import Wizard**, chọn **Next**.

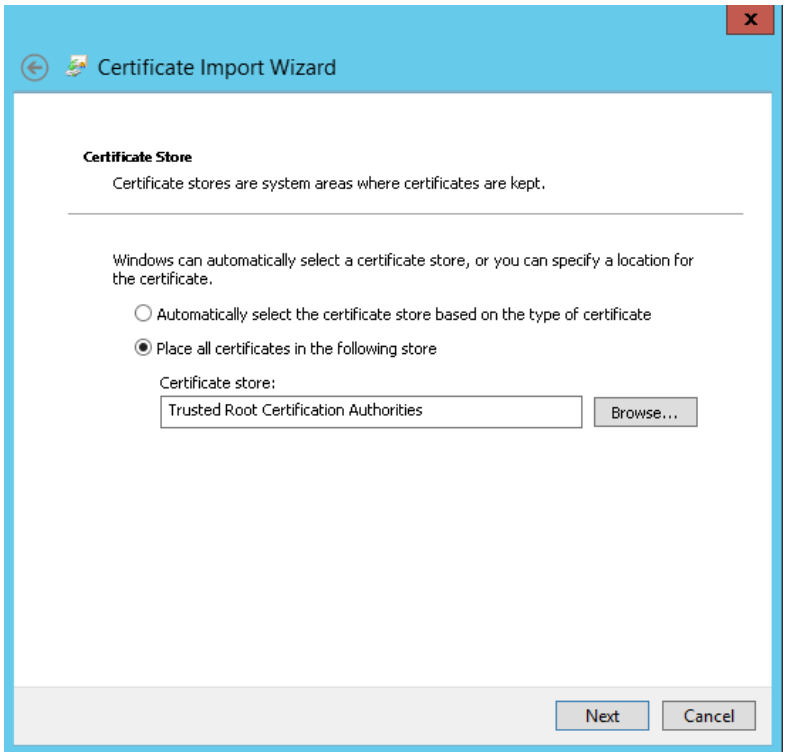
16. Cửa sổ **File to Import**, chọn **Browse**.




17. Chọn file **LON-DC1.Adatum.com_AdatumCA.crt**, chọn **Open**, chọn **Next**.



18. Cửa sổ **Certificate Store**, chọn **Next,** chọn **Finish**, và chọn **OK**.

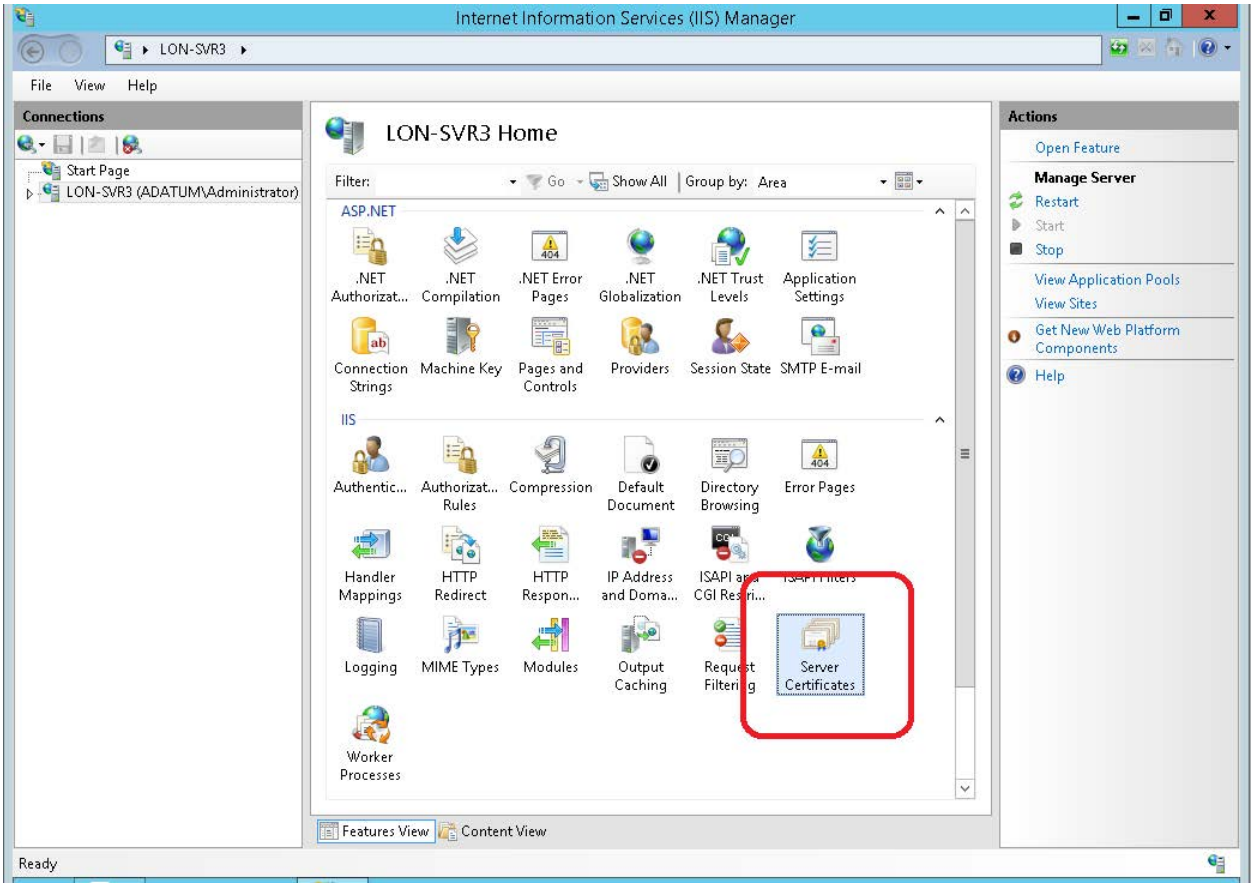



19. Tắt cửa sổ **Console1**, chọn **No**.

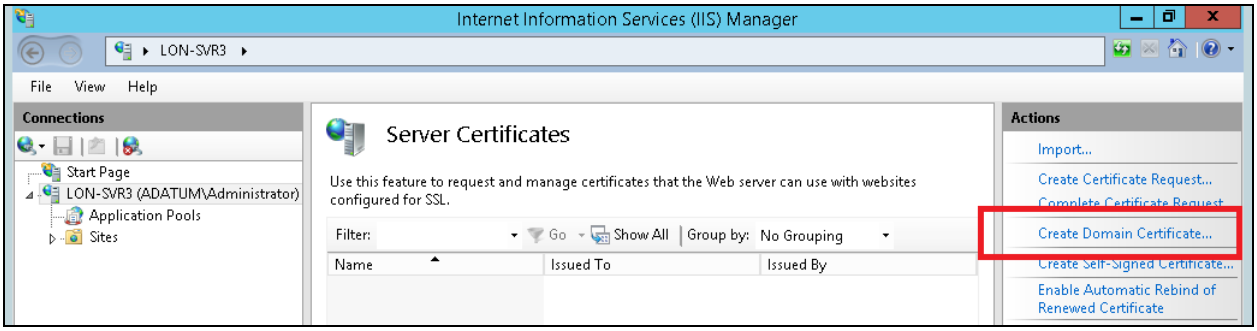
## Bước 3. Xin Certificate cho Web Server.

1. Trên máy **LON-SVR3**, trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**.

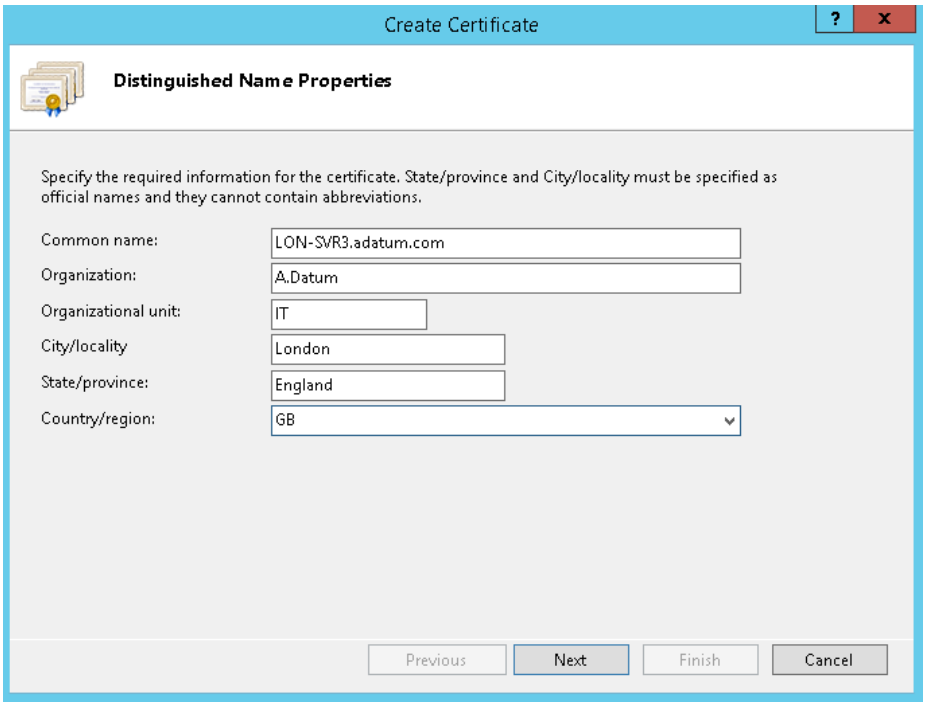
2. Chọn **LON-SVR3 (Adatum\Administrator)**. Trong cửa sổ giữa, nhấp đôi chuột **Server Certificates**.



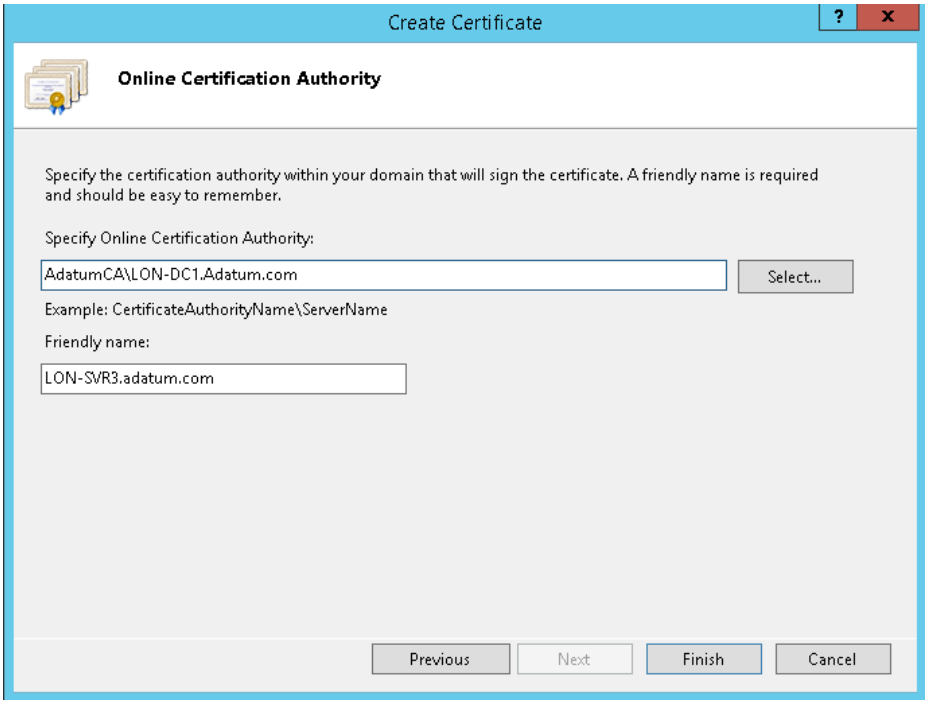
3. Trong cửa sổ **Actions**, chọn **Create Domain Certificate**.




4. Cửa sổ **Distinguished Name Properties**, nhập thông tin như hình bên dưới, và chọn **Next**.

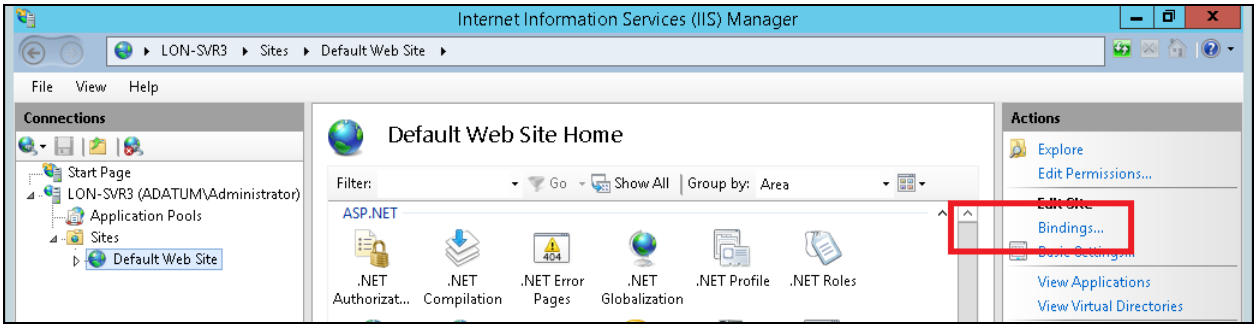


5. Cửa sổ **Online Certification Authority**, chọn **Select**, chọn certificate **AdatumCA**. Trong ô **Friendly Name**, nhập **LON-SVR3.adatum.com**, chọn **Finish**.

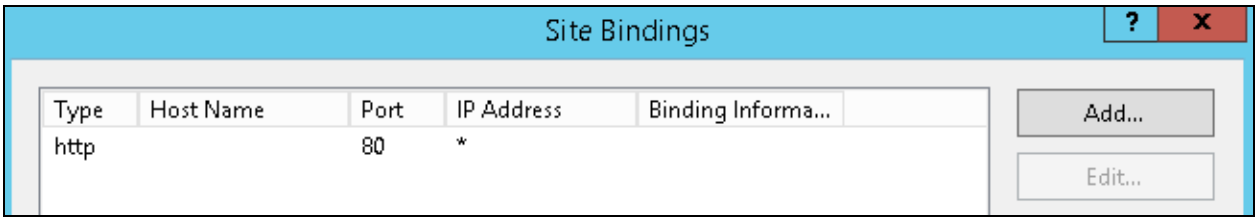



## Bước 4. Gán Certificate cho ứng dụng trên Web Server, và kiểm tra truy cập.

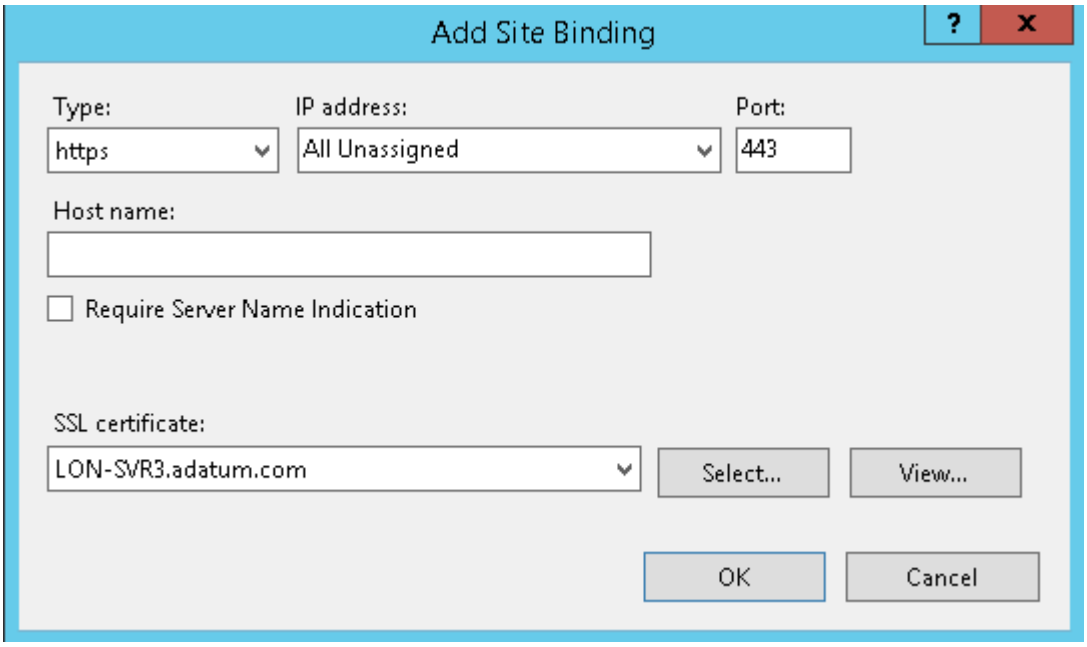
1. Trên máy **LON-SVR3**, trong **Internet Information Services (IIS) Manager**, bung **Sites**, bung **Default Web Site**, trong cửa sổ **Actions**, chọn **Bindings**.



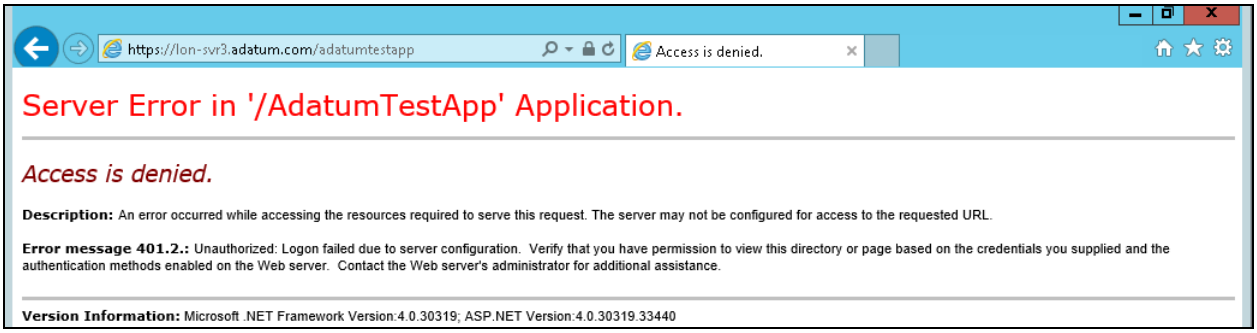
2. Hộp thoại **Site Bindings**, chọn **Add**.




3. Hộp thoại **Add Site Binding**, bung **Type**, chọn **https**, bung **SSL Certificate** , chọn **LON-SVR3.adatum.com**, chọn **OK**, chọn **Close**, và tắt **IIS**.



4. Qua máy **LON-DC1,** mở Internet Explorer®, truy cập **https://lon-svr3.adatum.com/adatumtestapp/**. Kiểm tra truy cập thất bại vì chưa cấu hình chứng thực AD FS. Tắt **Internet Explorer.**

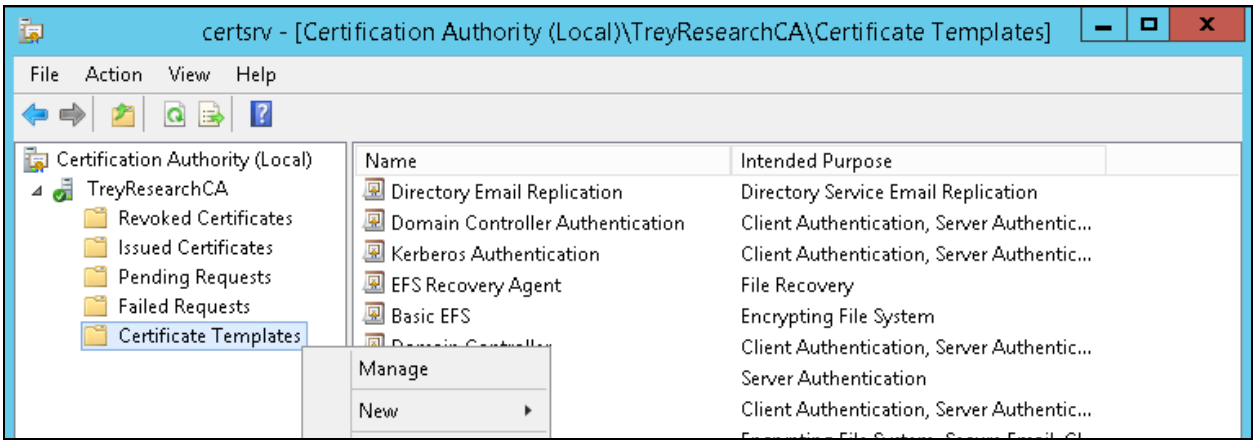



## Bước 5. Tạo và xin Certificate cho Server của Trey Research.

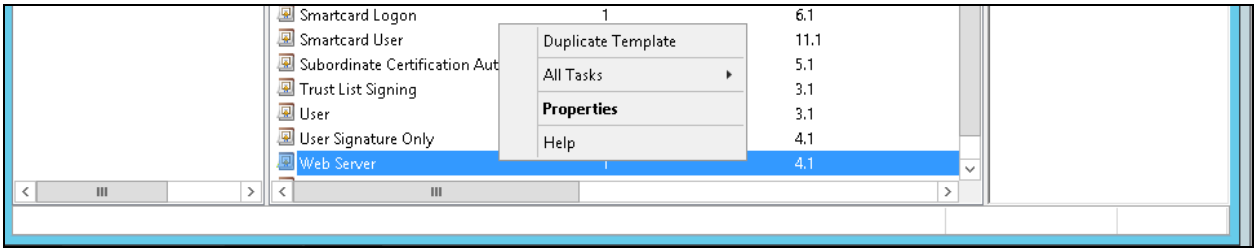
### ❖ Tạo Certificate mẫu

1. Qua máy **Trey-DC1, t**rong cửa sổ **Server Manager**, bung menu **Tools**, mở **Certification Authority**.

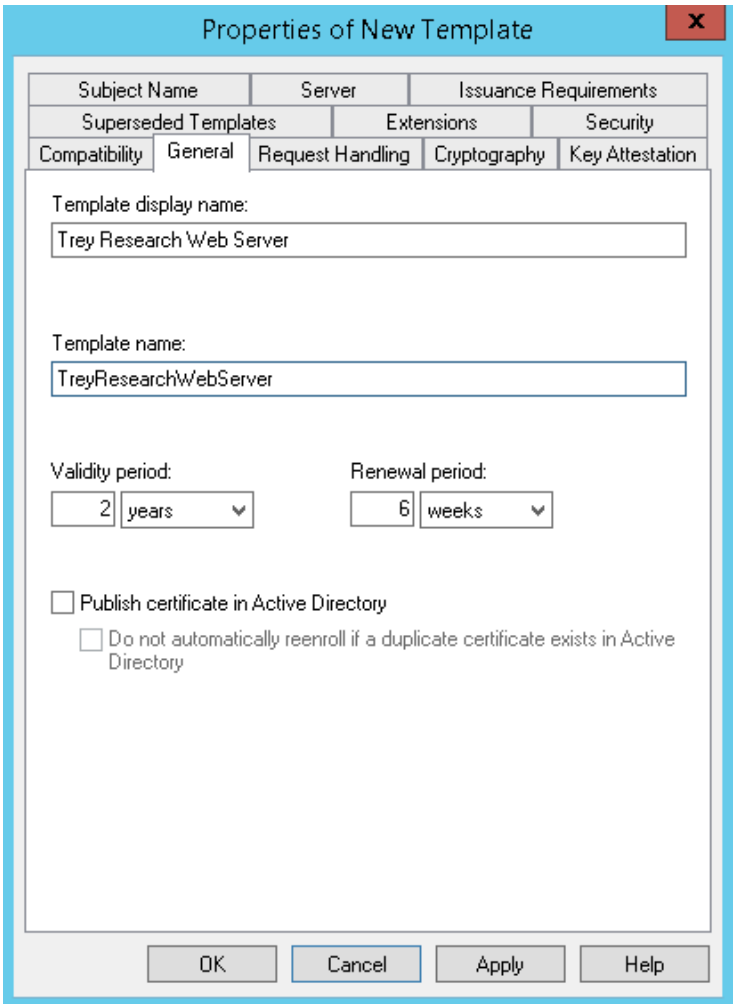
2. Bung **TreyResearchCA**, chuột phải **Certificate Templates**, chọn **Manage**.



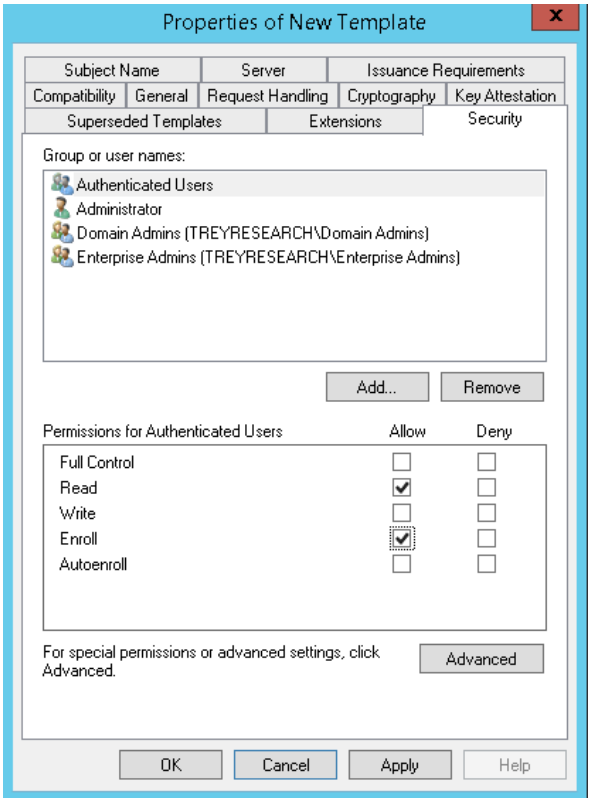
3. Trong cửa sổ **Certificate Templates Console**, chuột phải **Web Server**, chọn **Duplicate Template**.




5. Hộp thoại **Properties of New Template**, qua **General**, trong ô **Template display name**, nhập **Trey Research Web Server**.

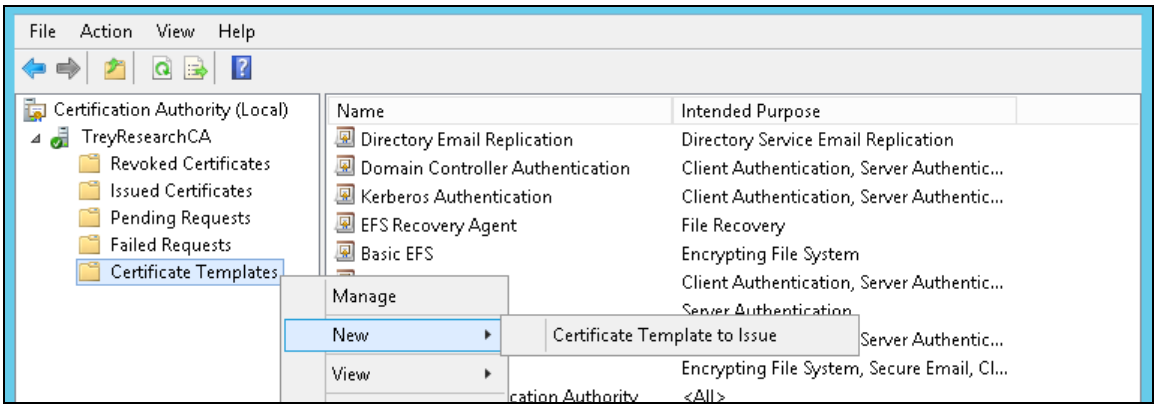


6. Qua tab **Security**, chọn **Authenticated Users**, đánh dấu chọn thêm ô **Enroll** ở cột **Allow**, chọn **OK**.

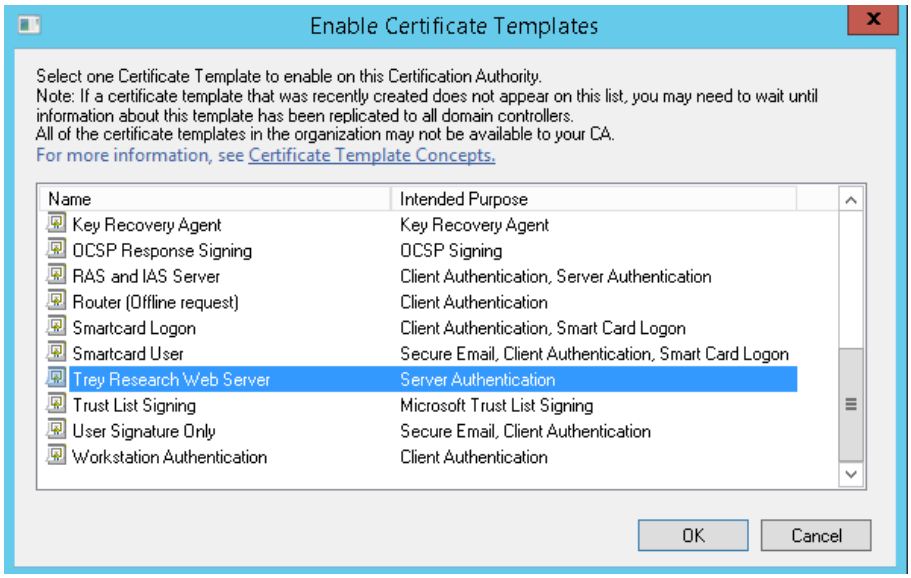



7. Tắt cửa sổ **Certificate Templates Console**.

8. Trong cửa sổ **Certification Authority**, chuột phải **Certificate Templates**, bung **New**, chọn **Certificate Template to Issue**.

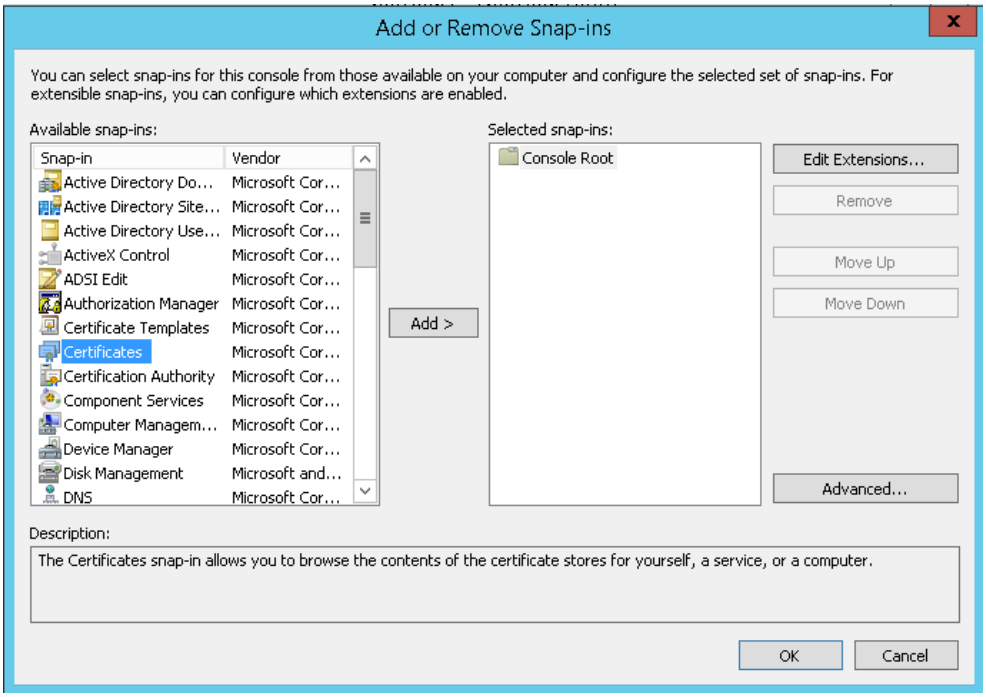


9. Cửa sổ **Enable Certificate Templates**, chọn **Trey Research Web Server**, và chọn **OK**.

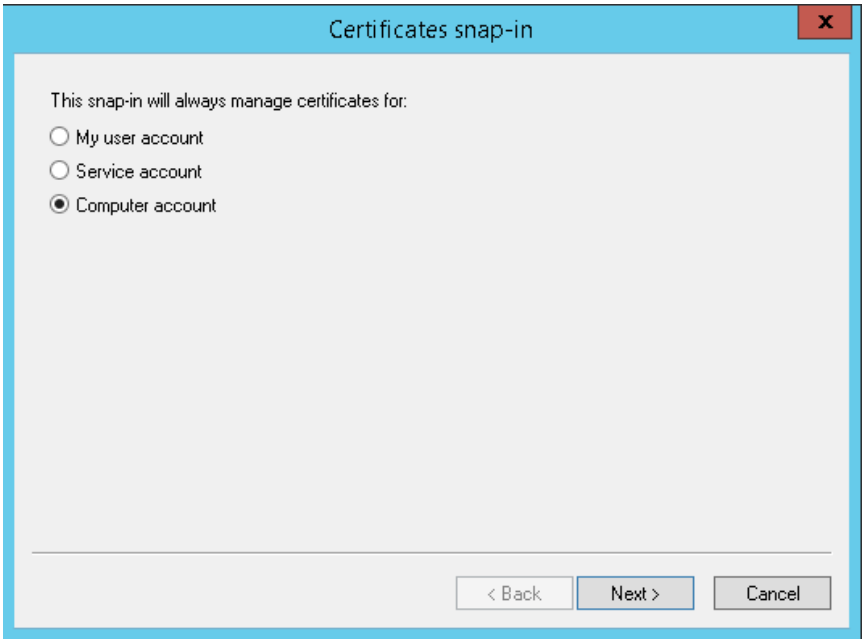



### ❖ Xin Certificate

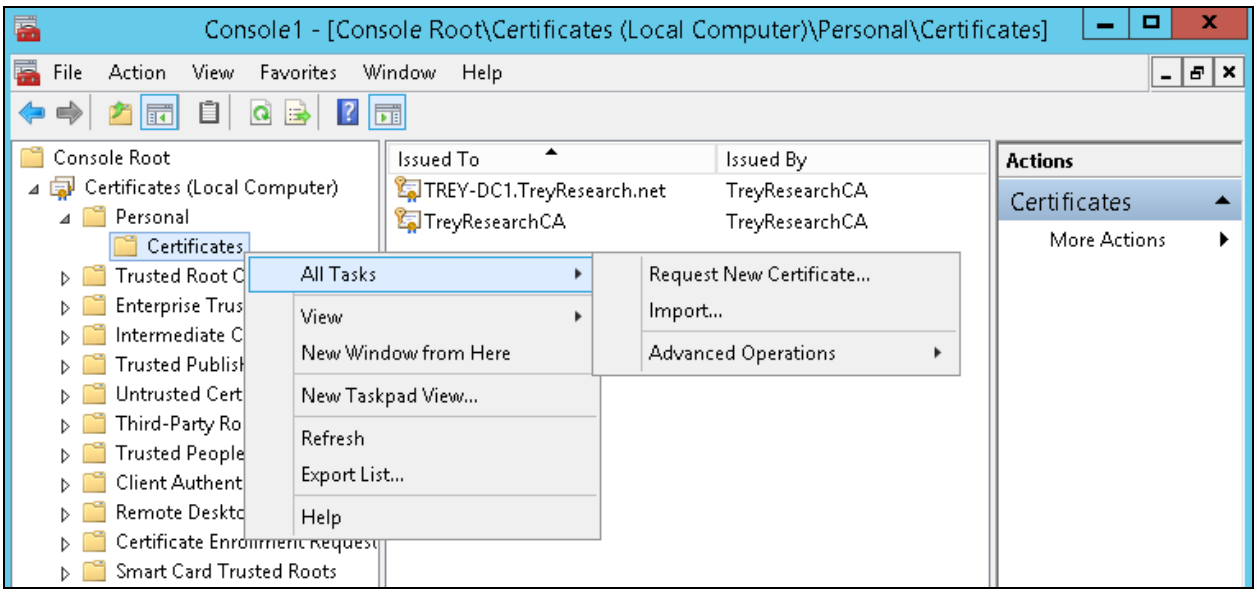
1. Trên máy **Trey-DC1,** mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**, chọn **Certificates**, và chọn **Add**.



2. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**,chọn **Finish**, chọn **OK,** và chọn **Close**.



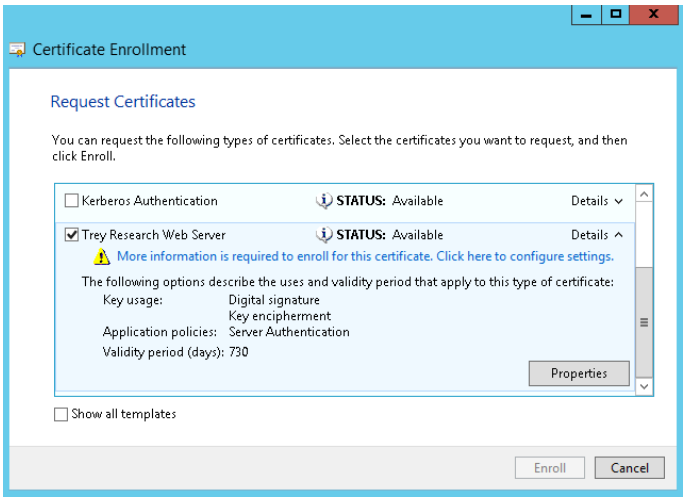

3. Trong cửa sổ **Console1**, bung **Certificates**, bung **Personal**, chuột phải **Certificates**, bung **All Tasks**, chọn **Request New Certificate**.



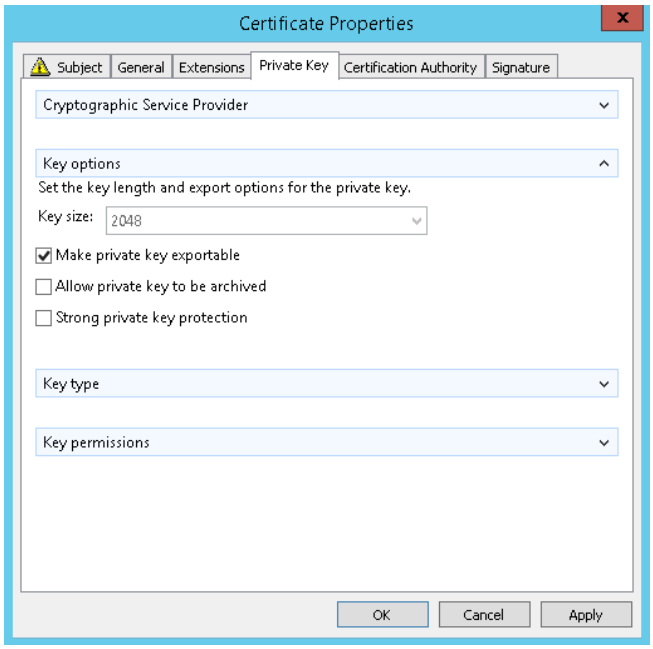
4. Cửa sổ **Before You Begin**, chọn **Next**.

5. Cửa sổ **Select Certificate Enrollment Policy**, chọn **Next**.

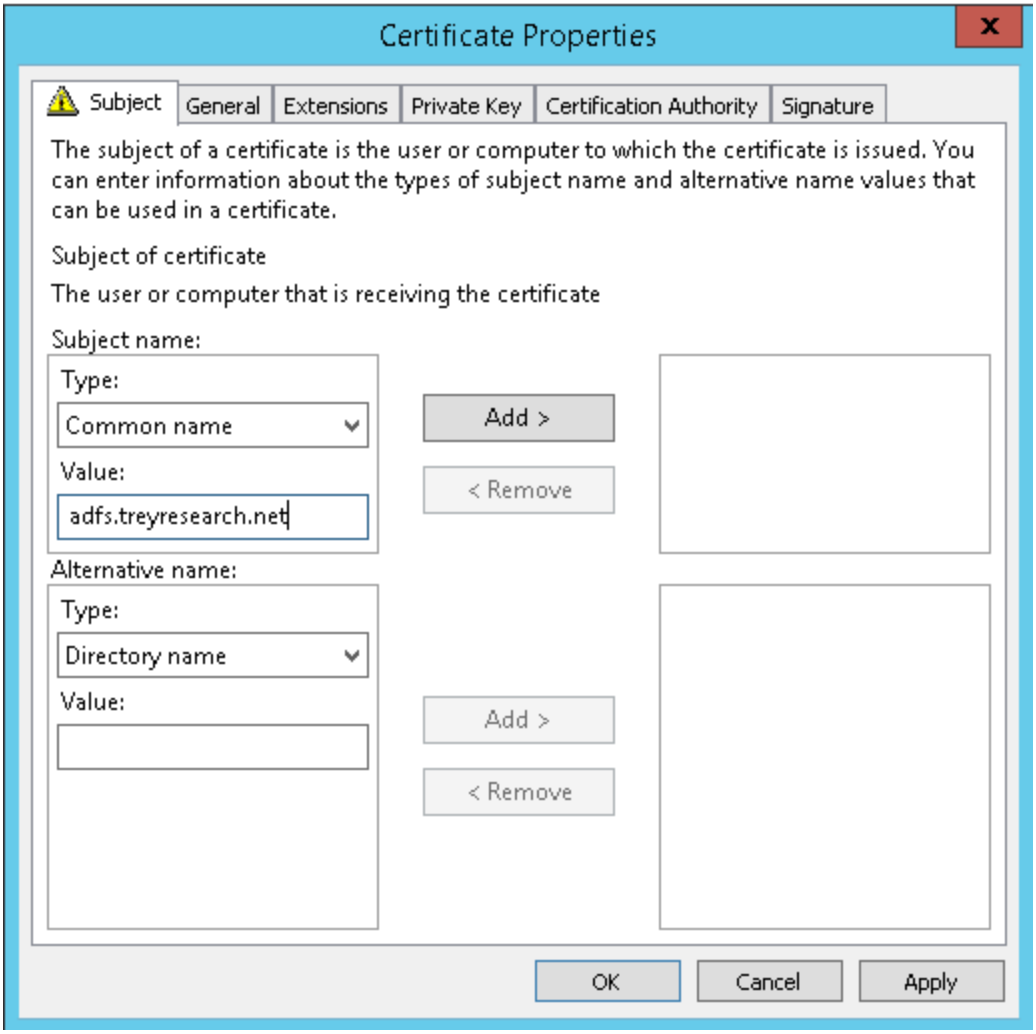
6. Cửa sổ **Request Certificates**, chọn **Trey Research Web Server**, bung **Details**, chọn **Properties**.




7. Cửa sổ **Certificate Properties**, qua tab **Private Key**, bung **Key options,** đánh dấu chọn **Make private key exportable**.



8. Qua tab **Subject**, trong phần **Subject name**, bung ô **Type**, chọn **Common name**, trong ô **Value**, nhập **adfs.treyresearch.net**, chọn **Add**, chọn **OK**, chọn **Enroll,** và chọn **Finish.**




**Kết quả: Trong bài tập này, bạn đã cấu hình DNS Conditional Forwarder để A. Datum và Trey Research phân giải tên lẫn nhau. Ngoài ra, bạn đã trao đổi CA Certificate giữa hai tổ chức, và cấu hình Certificate cho Web Server.**

## Bài tập 2: Triển khai AD FS cho người dùng nội bộ.

Trong bài tập này, bạn sẽ triển khai AD FS để hỗ trợ người dùng nội bộ truy cập. Để thực hiện AD FS, bạn phải cài đặt AD FS Server role và cấu hình Claim Provider Trust. Bạn sẽ cấu hình cho ứng dụng WIF tin tưởng AD FS, và sau đó cấu hình Relying Party Trust. Cuối cùng, bạn sẽ cấu hình các Claims Rules, và sau đó kiểm tra rằng chỉ người dùng nội bộ được chấp thuận mới có thể truy cập ứng dụng.

❖ **Bài tập bao gồm các bước:**

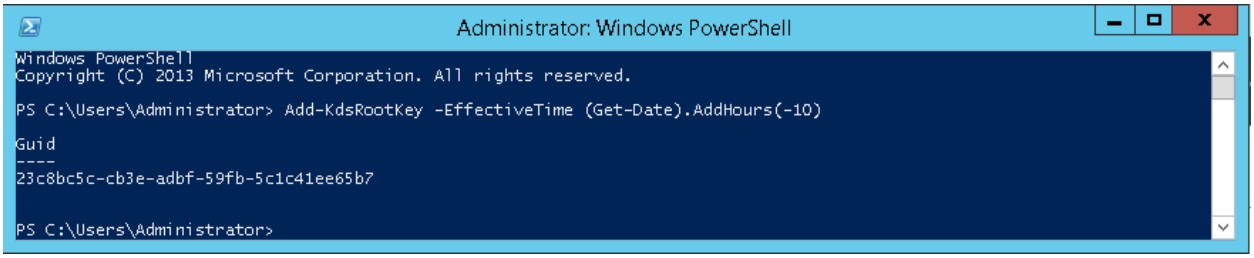
1. Cài đặt và cấu hình AD FS server role.
2. Cấu hình Claim Provider Trust.
3. Cấu hình cho ứng dụng WIF tin tưởng AD FS.
4. Cấu hình Relying Party Trust và Claims Rules.
5. Kiểm tra người dùng nội bộ truy cập ứng dụng.

❖ **Thực hiện:**

### Bước 1. Cài đặt và cấu hình AD FS server role.

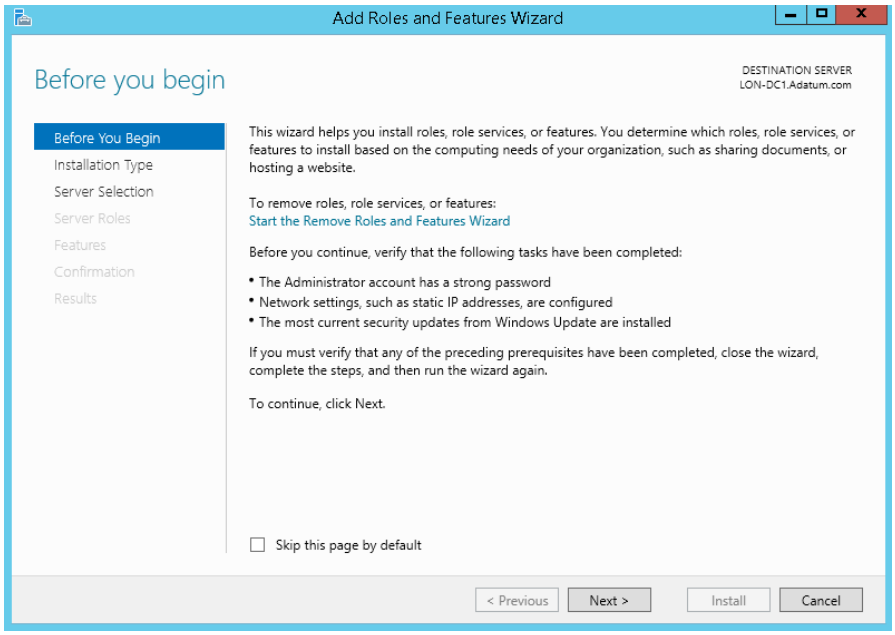
1. Trên máy **LON-DC1**, mở **Windows PowerShell**, gõ lệnh:

**Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)**

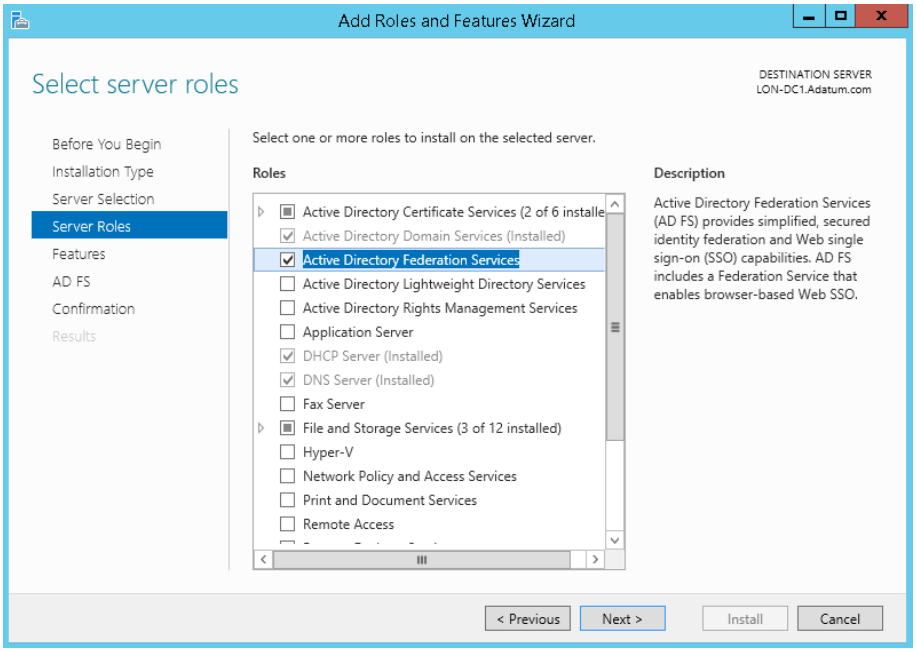



2. Tắt **Windows PowerShell**.
3. Trong cửa sổ **Server Manager**, chọn **Add Roles and Features**.

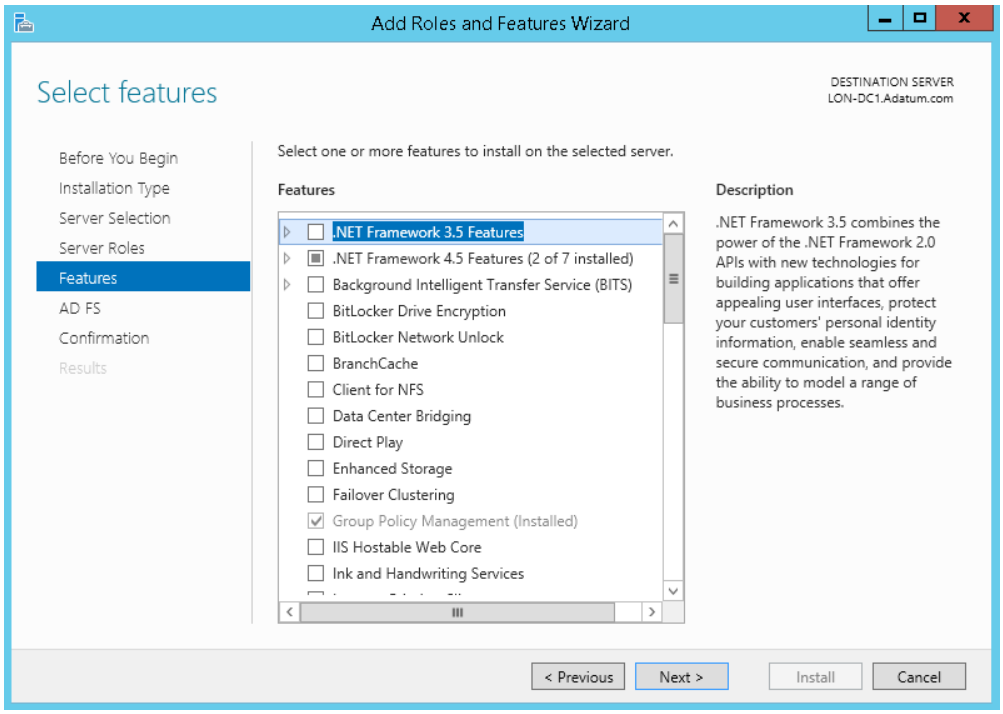
4. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



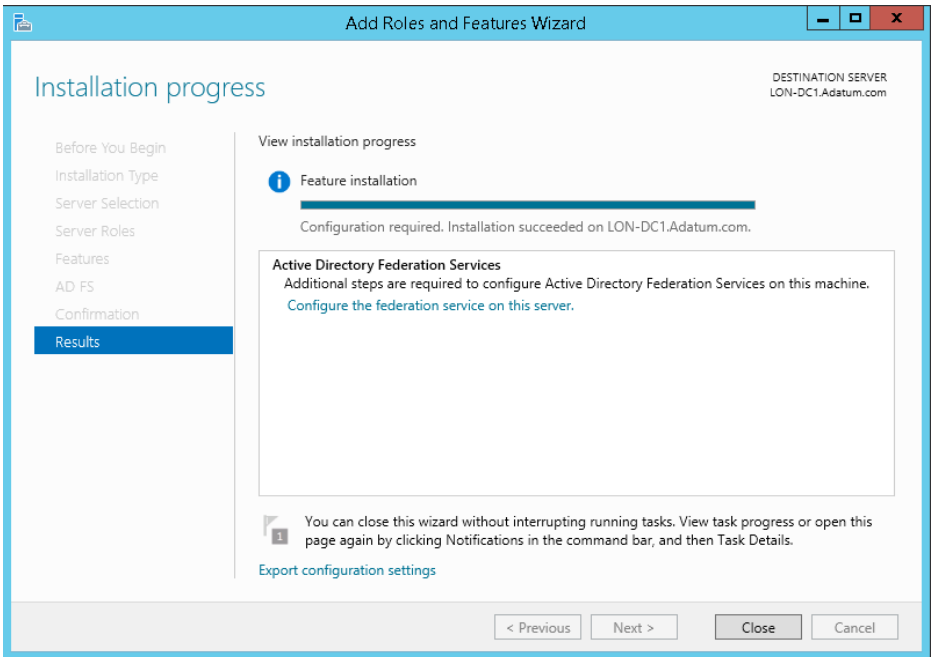

5. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Federation Services**, chọnk **Next**.



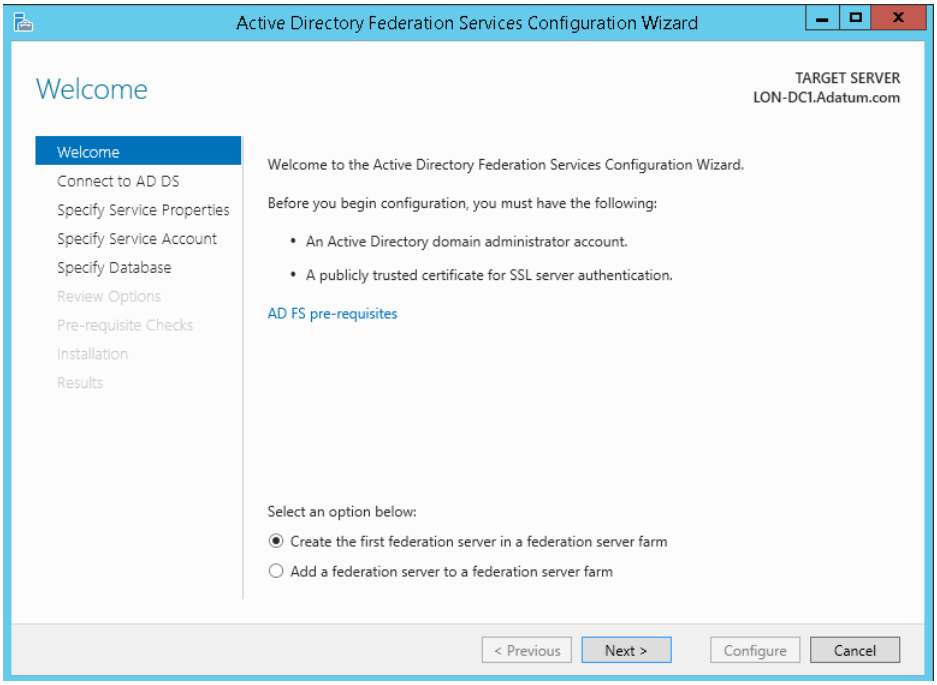
6. Cửa sổ **Select features**, chọn **Next** 2 lần, và chọn **Install.**



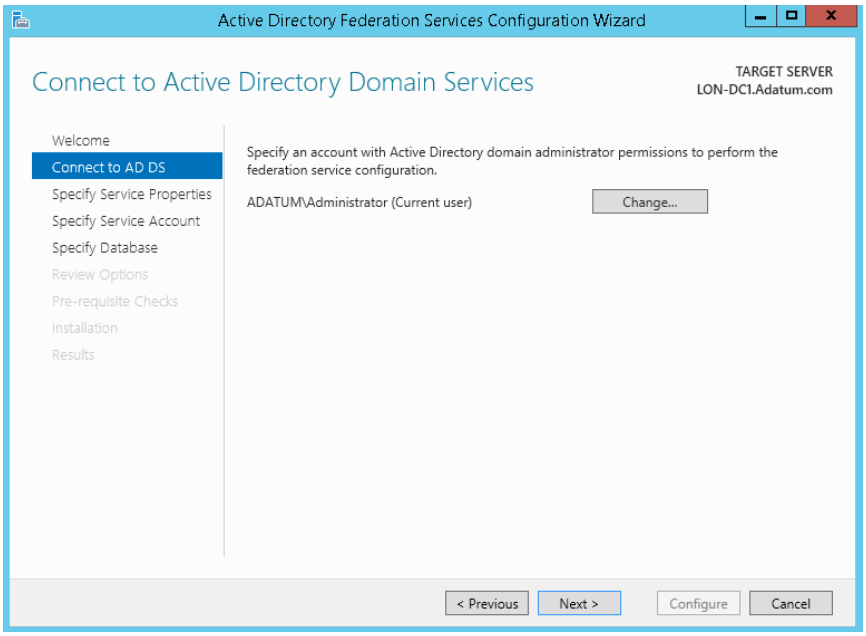

7. Sau khi cài đặt thành công, chọn **Configure the federation service on this server**.



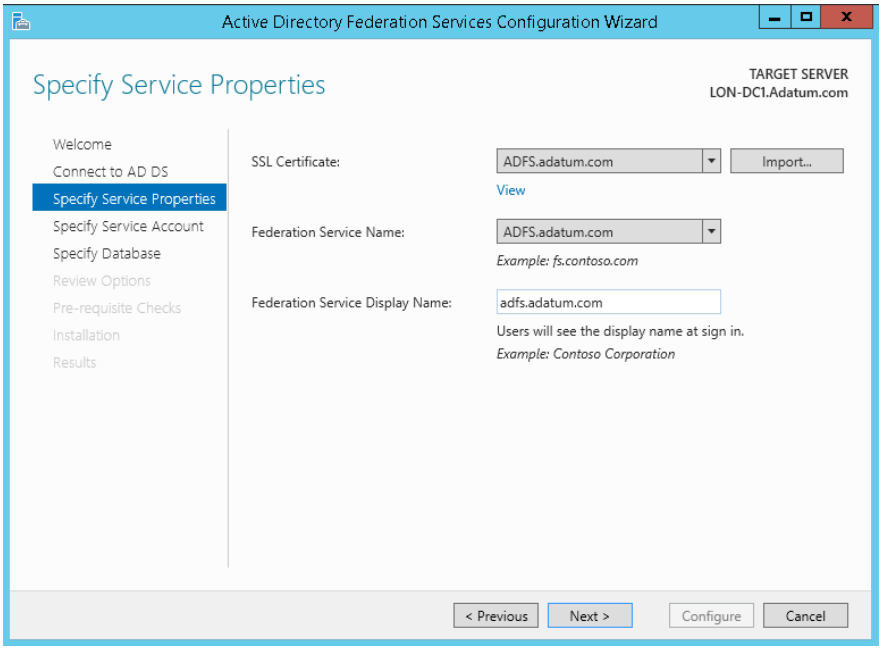
8. Cửa sổ **Welcome**, chọn **Create the first federation server in a federation server farm**, và chọn **Next**.



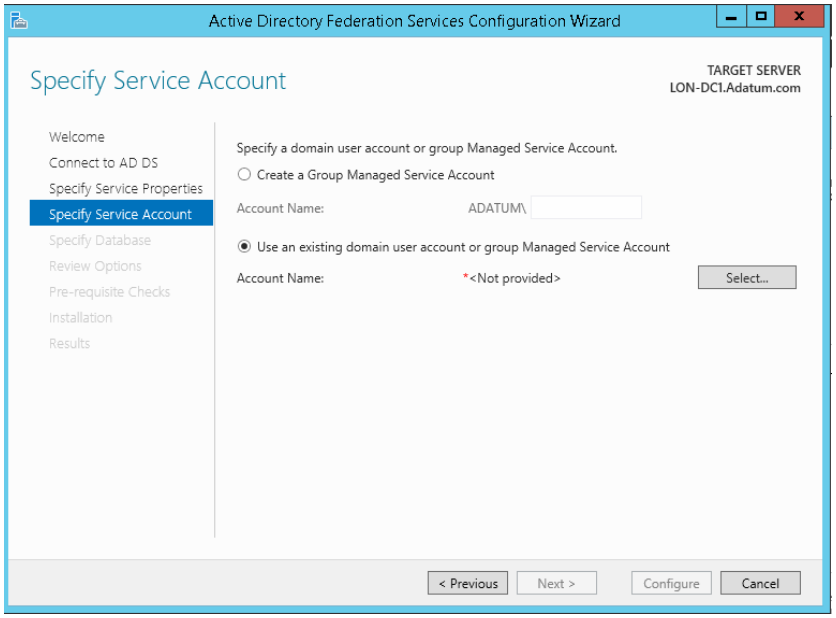

9. Cửa sổ **Connect to Active Directory Domain Services**, chọn **Next**.



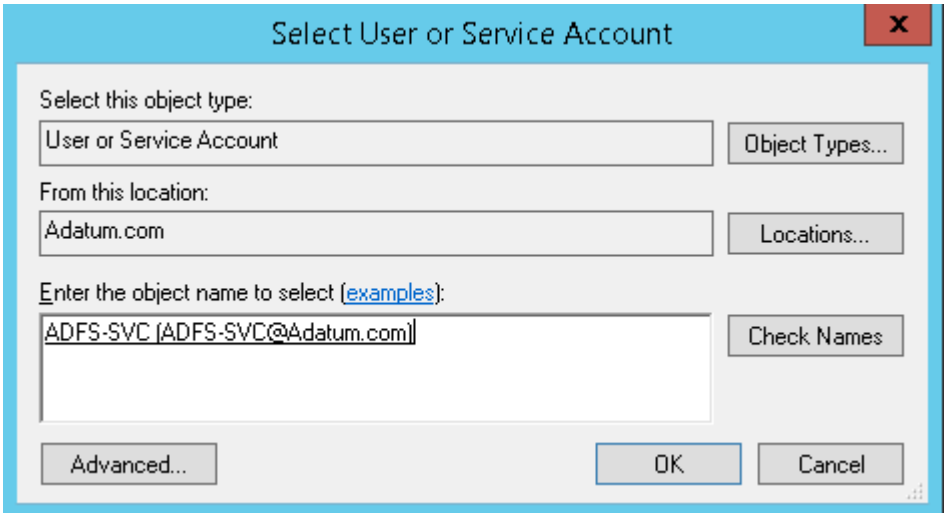
10. Cửa sổ **Specify Service Properties**, bung **SSL certificate,** chọn **adfs.adatum.com**, nhập **adfs.adatum.com** vào ô **Federation Service Display Name**, và chọn **Next**.



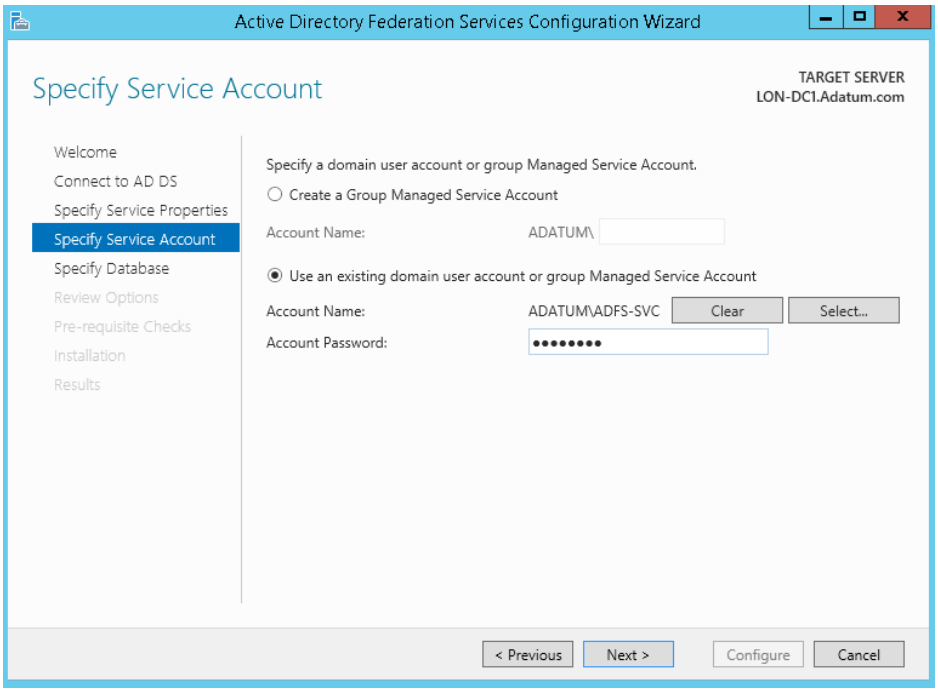

11. Cửa sổ **Specify Service Account**, chọn **Use an existing domain user account or group Managed Service Account**, chọn **Select**



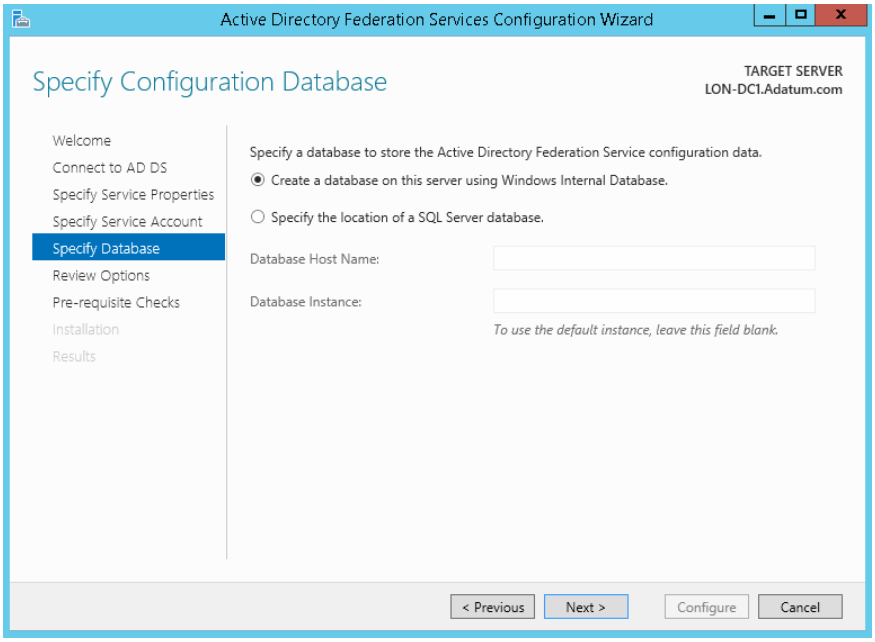
12. Hộp thoại **Select User or Service Account**, nhập **ADFS-SVC,** chọn **Check Names**, và chọn **OK**.



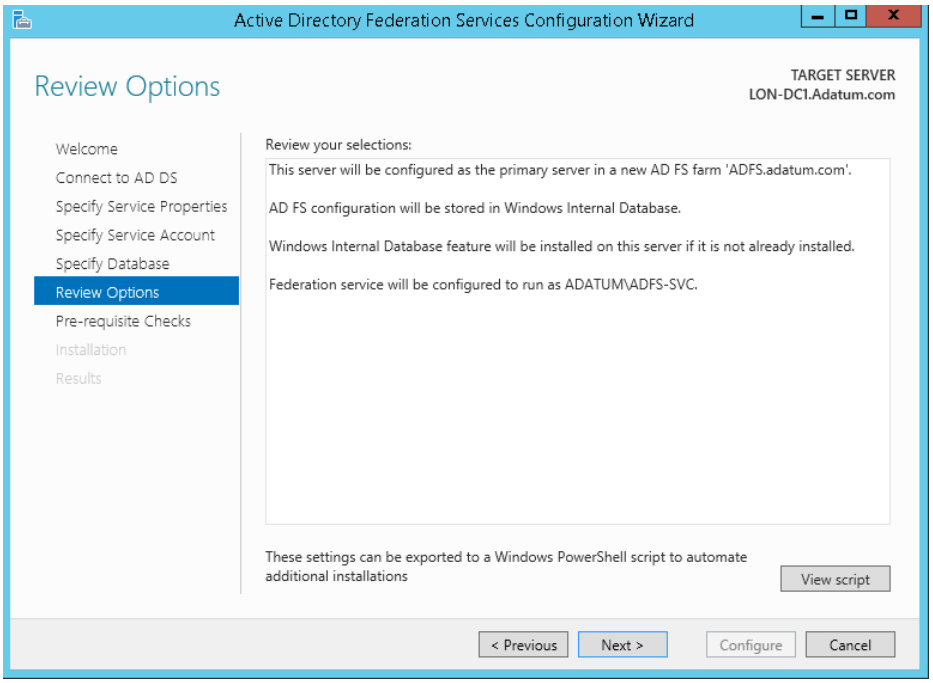

13. Cửa sổ **Specify Service Account**, nhập **Pa$$w0rd** vào ô **Account Password**, và chọn **Next**.



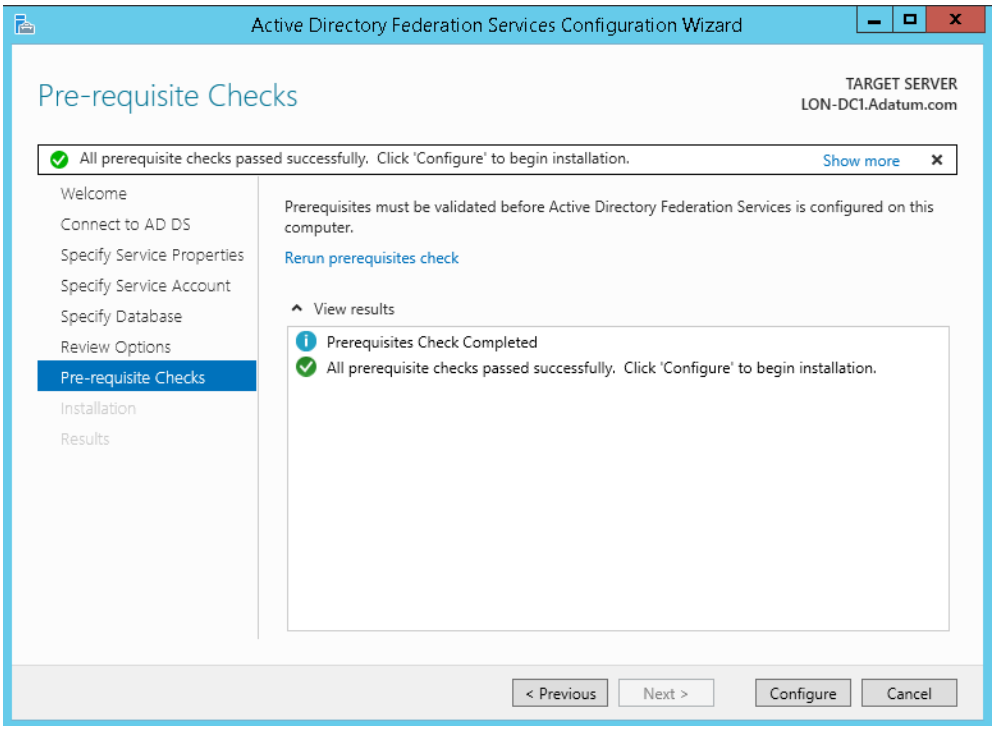
14. Cửa sổ **Specify Configuration Database**, chọn **Create a database on this server using Windows Internal Database**, và chọn **Next**.




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



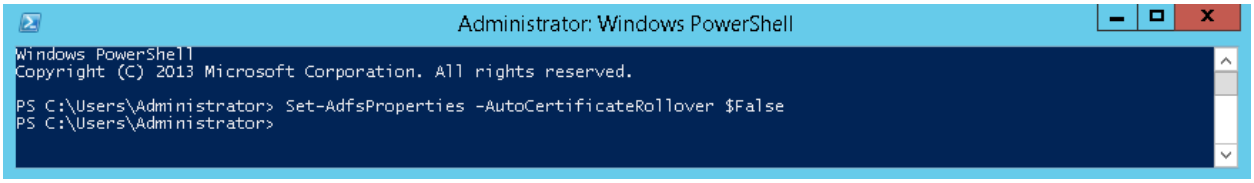
16. Cửa sổ **Pre-requisite Checks**, chọn **Configure**.




17. Sau khi cấu hình thành công, chọn **Close**.

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

**Set-ADFSProperties –AutoCertificateRollover $False**

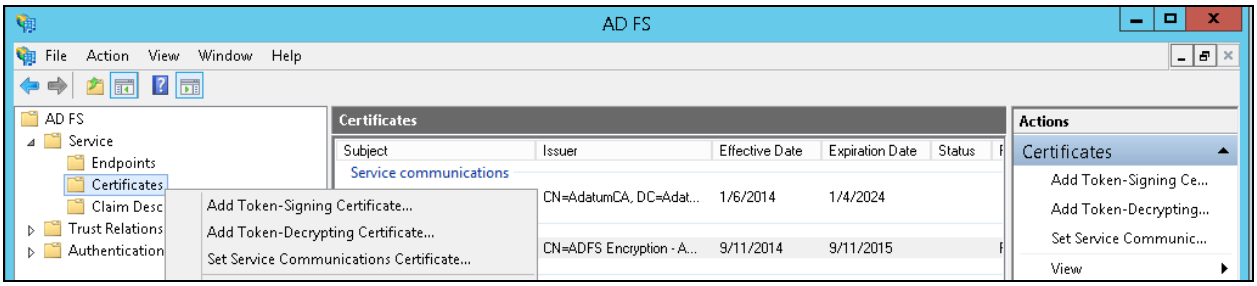



**Lưu ý: Bạn phải thực hiện bước này để có thể sửa đổi các certificate của AD FS.**

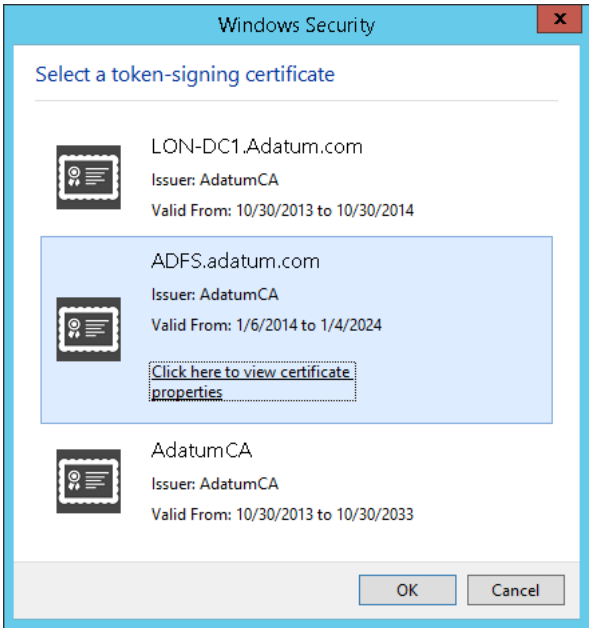
19. Tắt **Windows PowerShell**.

20. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **AD FS Management**.

21. Trong cửa sổ **AD FS**, bung **Service**, chuột phải **Certificates**, chọn **Add Token-Signing Certificate**.

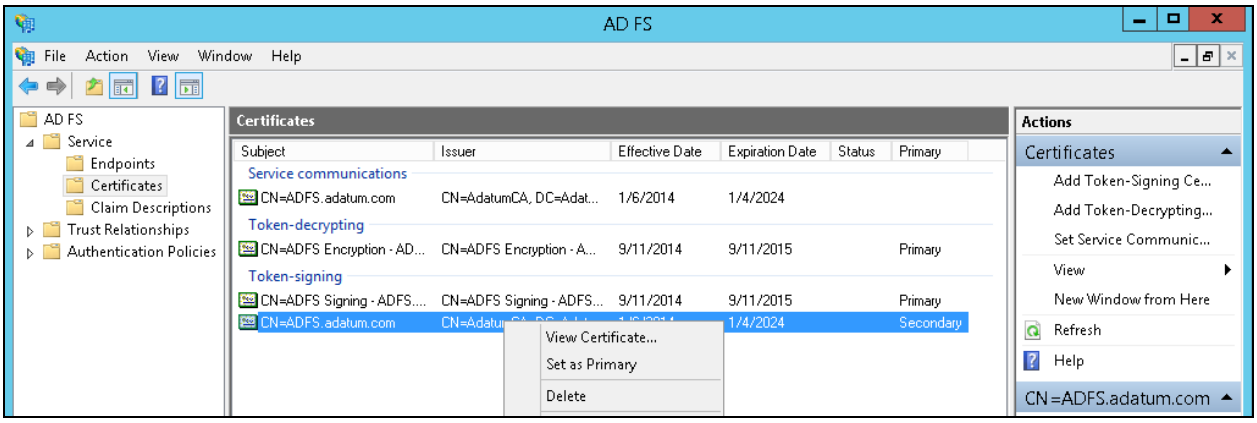



22. Cửa sổ **Select a token-signing certificate**, chọn certificate có tên **adfs.adatum.com**, chọn **OK**

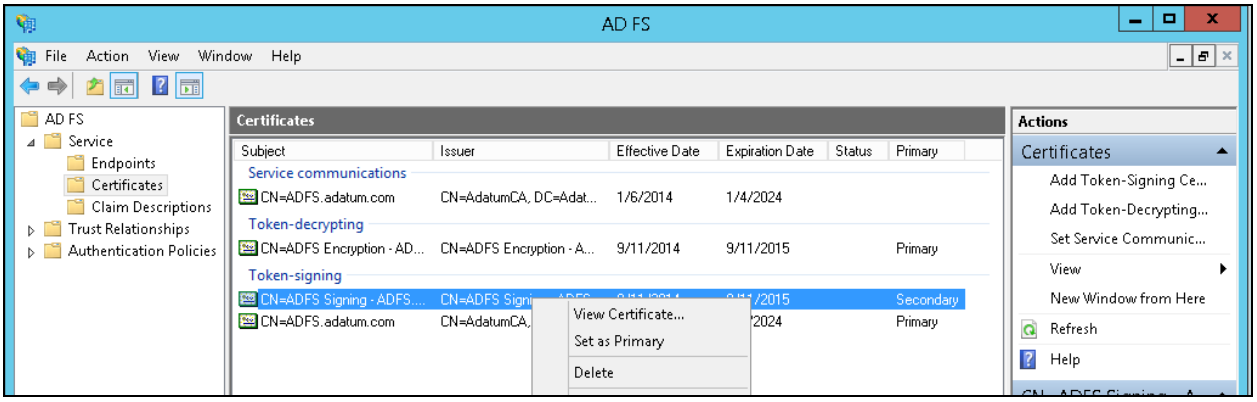



23. Hộp thoại thông báo **AD FS Management**, chọn **OK**.

24. Trong phần **Token-signing**, chuột phải lên certificate mới thêm vào (**CN=adfs.adatum.com**), chọn **Set as Primary**. Hộp thoại thông báo, chọn **Yes**.

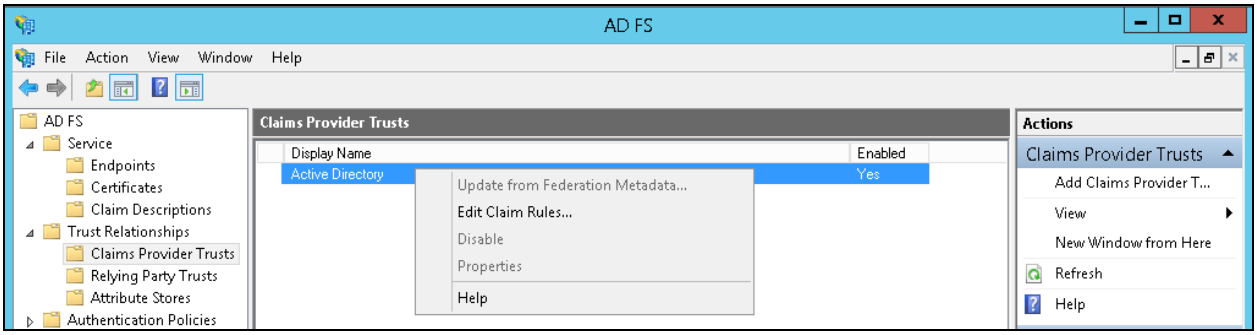



25. Chuột phải certificate đang ở chế độ **Secondary**, chọn **Delete**. Hộp thoại thông báo, chọn **Yes**.

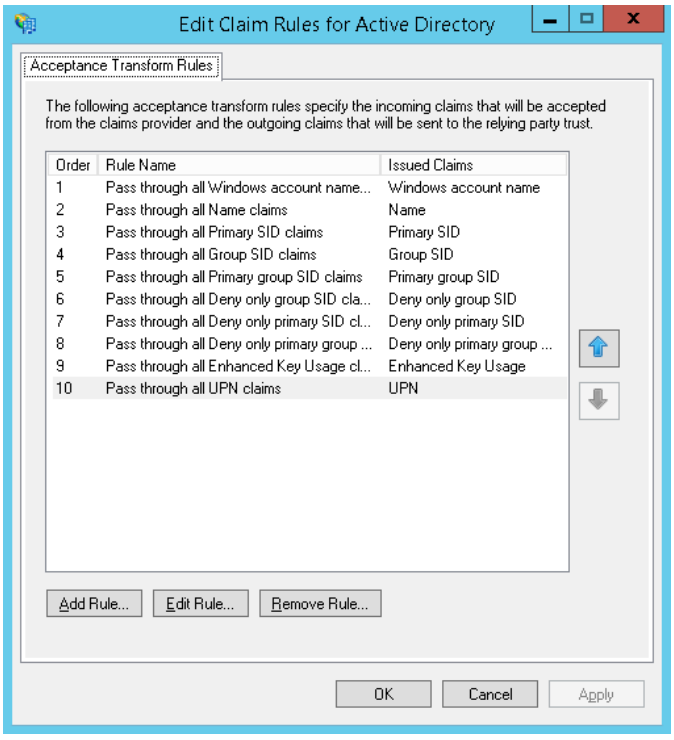


## Bước 2. Cấu hình Claim Provider Trust.

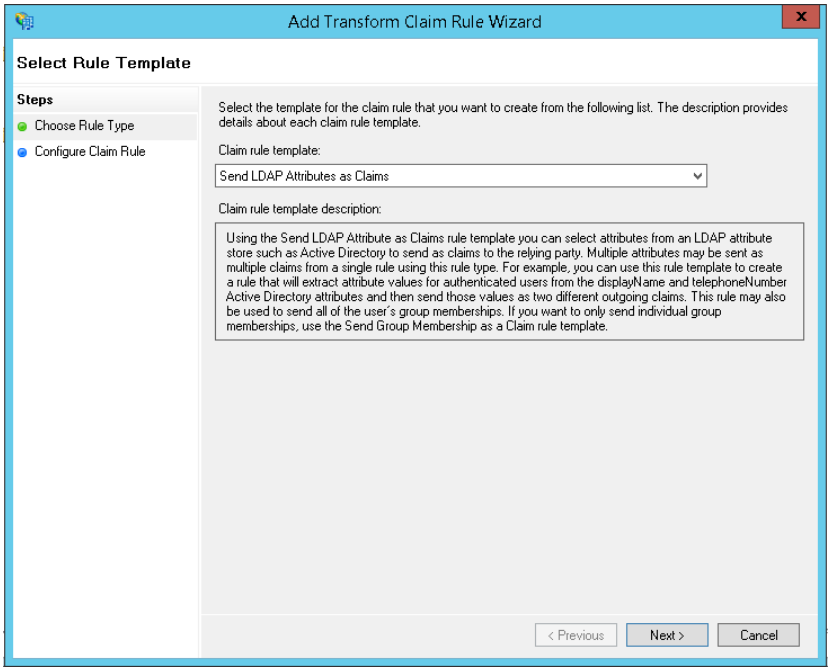
1. Trên máy **LON-DC1**, trong cửa sổ **AD FS**, bung **Trust Relationships**, chọn **Claims Provider Trusts**, chuột phải **Active Directory**, chọn **Edit Claim Rules**.




2. Cửa sổ **Edit Claims Rules for Active Directory**, trong tab **Acceptance Transform Rules**, chọn **Add Rule**.

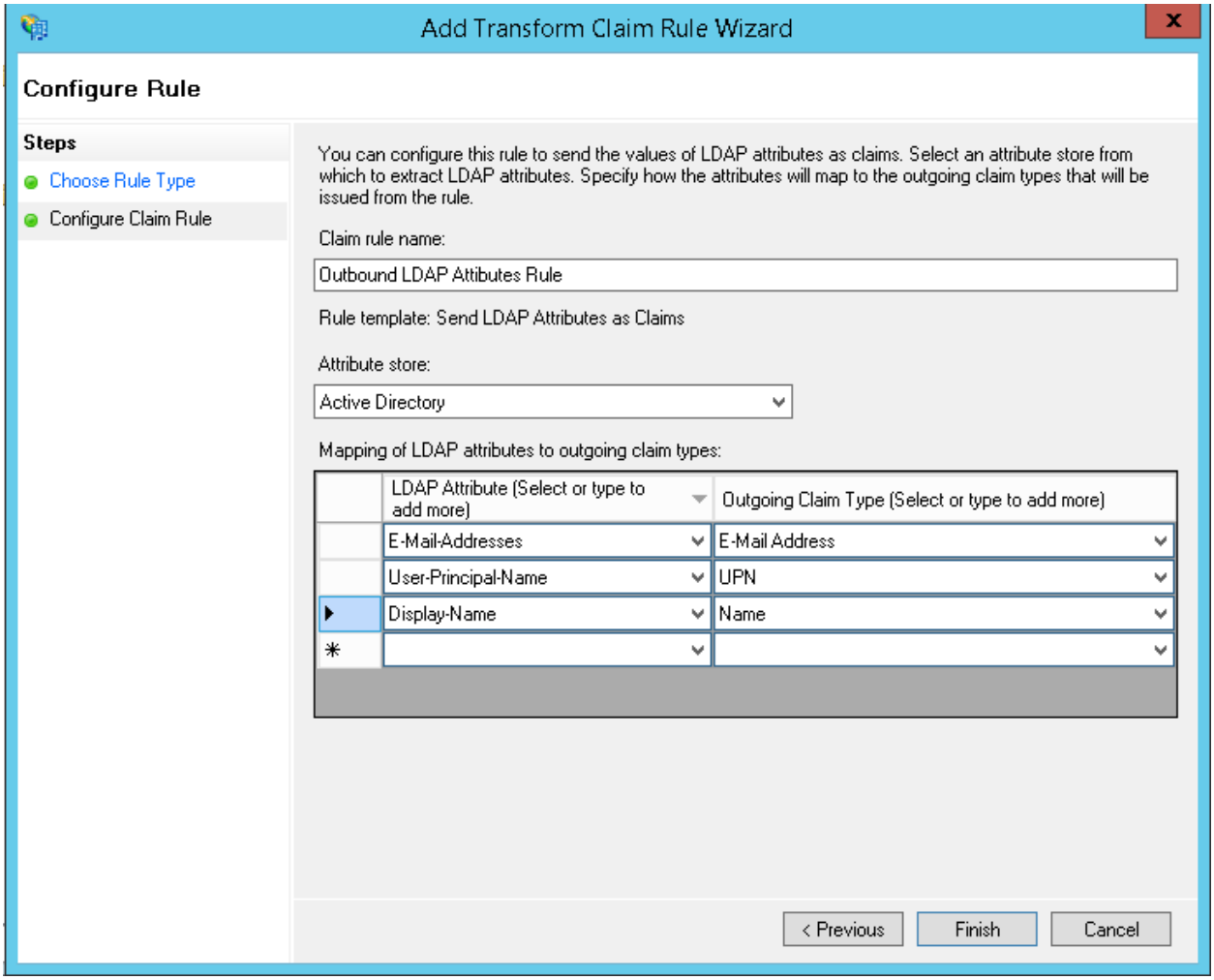


3. Cửa sổ **Select Rule Template**, bung ô **Claim rule template**, chọn **Send LDAP Attributes as Claims**, và chọn **Next**.



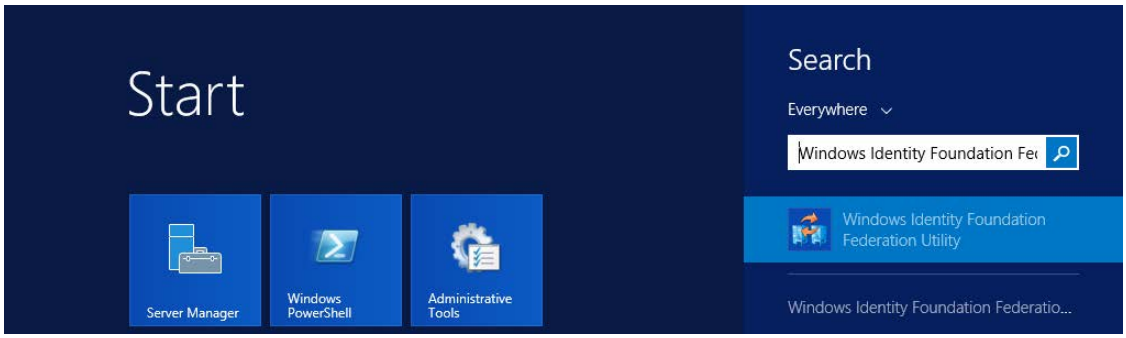
4. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Outbound LDAP Attributes Rule**. Bung ô **Attribute Store**, chọn **Active Directory**. Trong phần **Mapping of LDAP attributes to outgoing claim types**, bung **LDAP Attribute** và **Outgoing Claim Type** chọn thông tin như bên dưới, sau đó chọn **Finish**, và chọn **OK**.

- **E-mail-Addresses: E-mail Address**
- **User-Principal-Name: UPN**
- **Display-Name: Name**

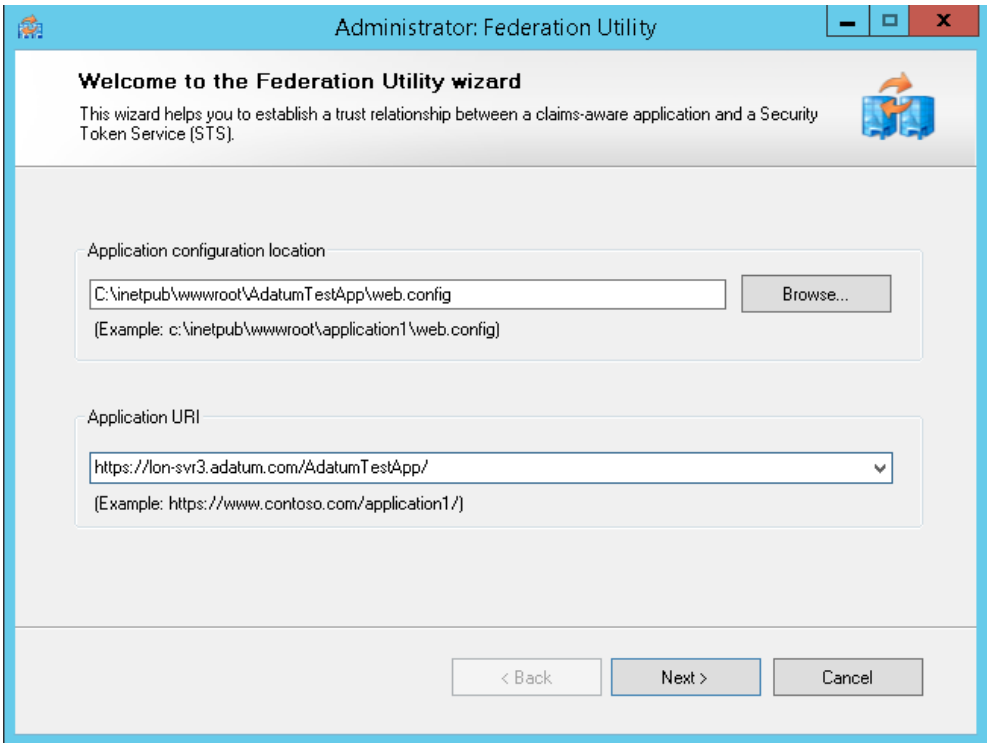


## Bước 3. Cấu hình cho ứng dụng WIF tin tưởng AD FS.

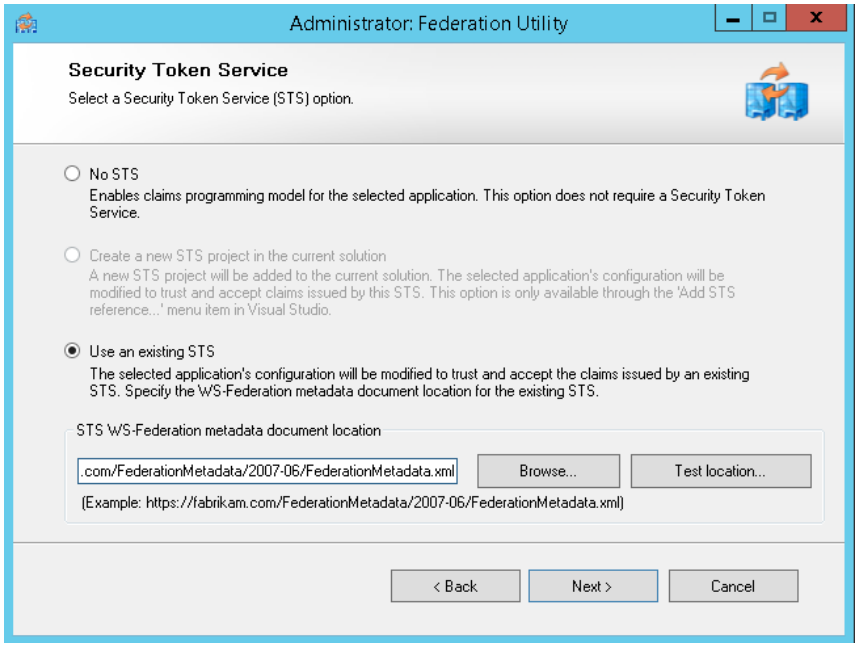
1. Qua máy **LON-SVR3**, bung **Start**, gõ **Windows Identity Foundation Federation Utility**, mở **Windows Identity Foundation Federation Utility**.



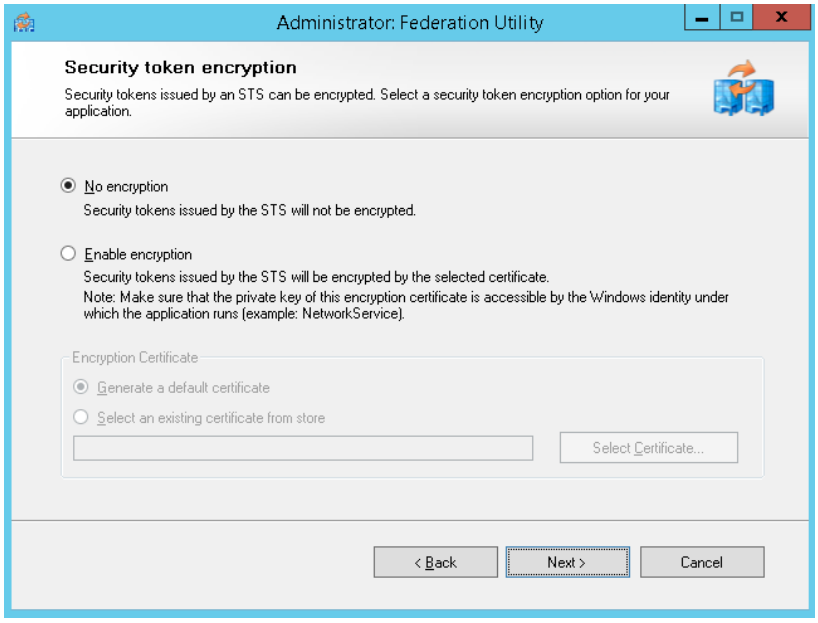

2. Cửa sổ **Welcome to the Federation Utility Wizard**, trong ô **Application configuration location**, nhập **C:\inetpub\wwwroot\AdatumTestApp\web.config .** Trong ô **Application URI**, nhập **https://lon-svr3.adatum.com/AdatumTestApp/** (*Lưu ý: có dấu / ở cuối dòng*), chọn **Next**.



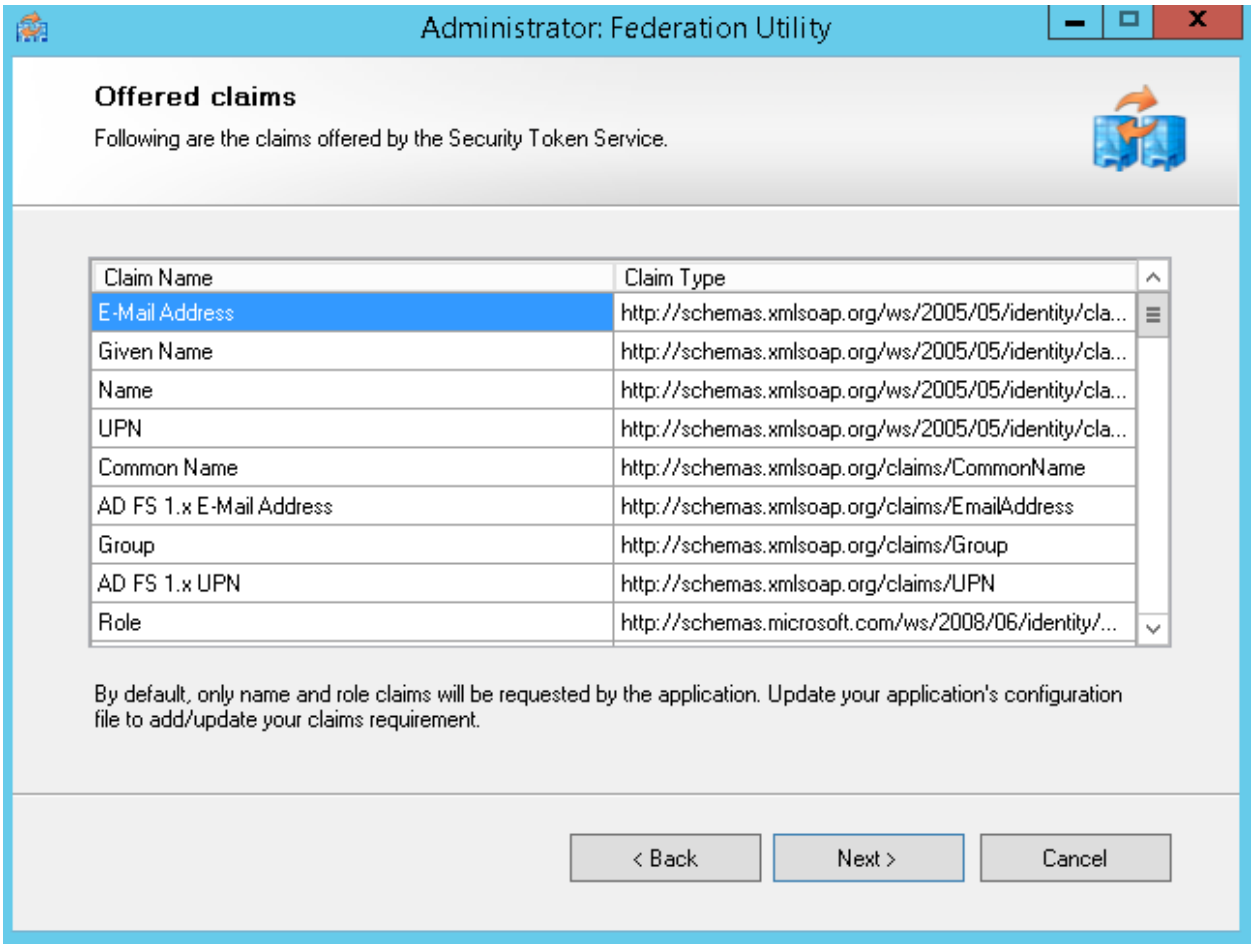
3. Cửa sổ **Security Token Service**, chọn **Use an Existing STS**, nhập **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml** vào ô **STS WS-Federation metadata document location**, và chọn **Next**.




4. Cửa sổ **Security Token Encryption**, chọn **No encryption**, và chọn **Next**.



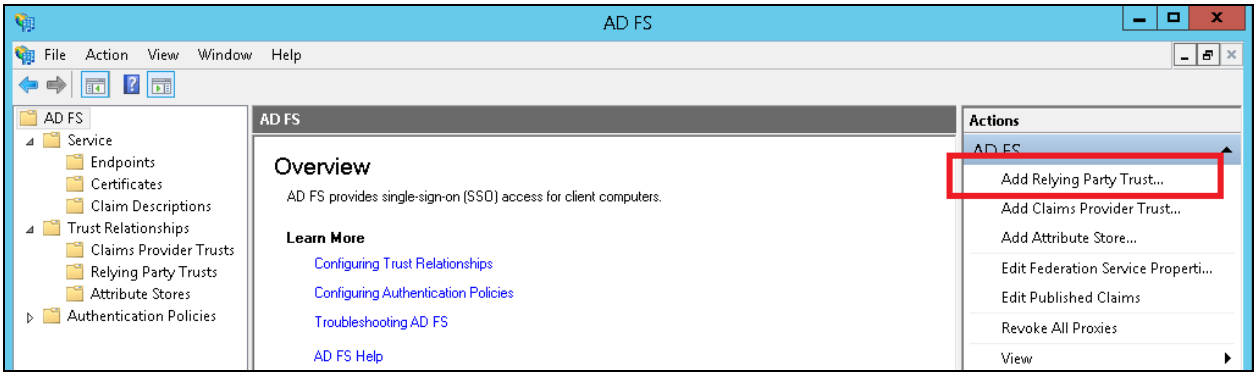
5. Cửa sổ **Offered claims**, chọn **Next.**




6. Cửa sổ **Summary**, chọn **Finish**. Hộp thoại thông báo, chọn **OK**

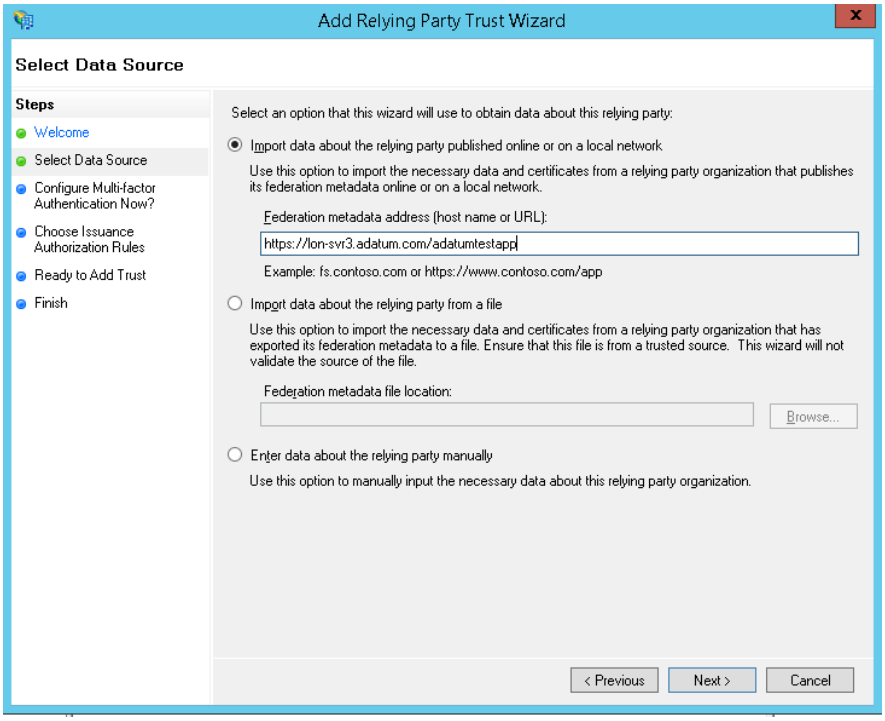
## Bước 4. Cấu hình Relying Party Trust và Claims Rules.

1. Qua máy **LON-DC1**, trong cửa sổ **AD FS Management**, chọn **AD FS**. Trong cửa sổ bên phải, chọn **Add Relying Party Trust**.

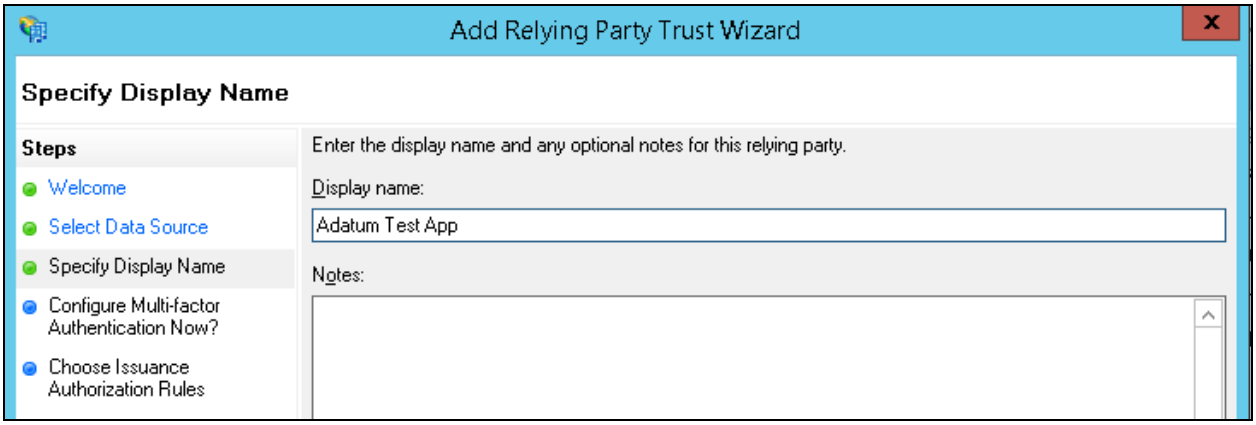



2. Cửa sổ **Welcome**, chọn **Start**.

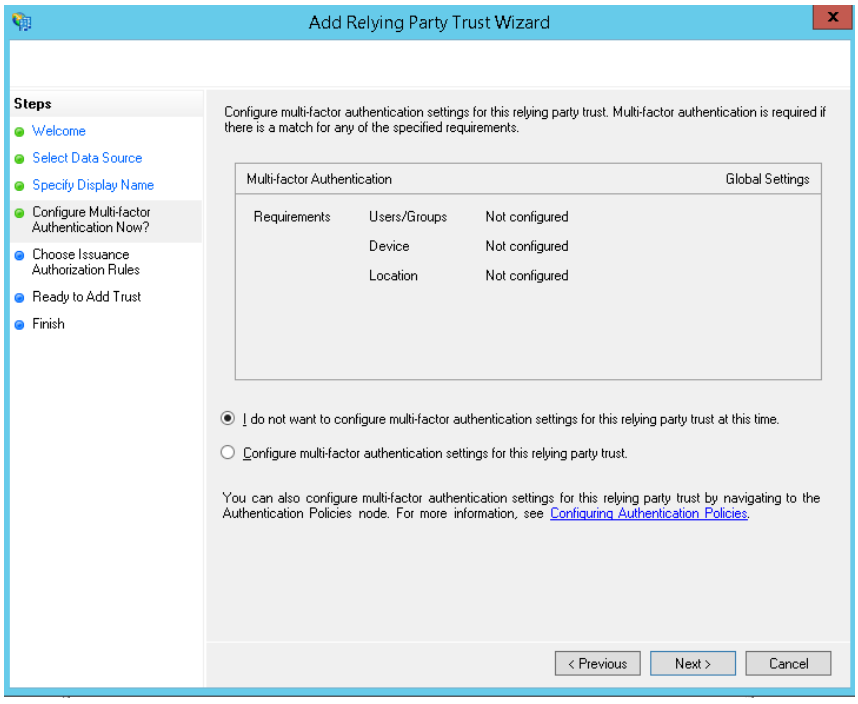
3. Cửa sổ **Select Data Source**, chọn **Import data about the relying party published online or on a local network**, và nhập **https://lon-svr3.adatum.com/adatumtestapp** vào ô **Federation metadata address**, chọn **Next**



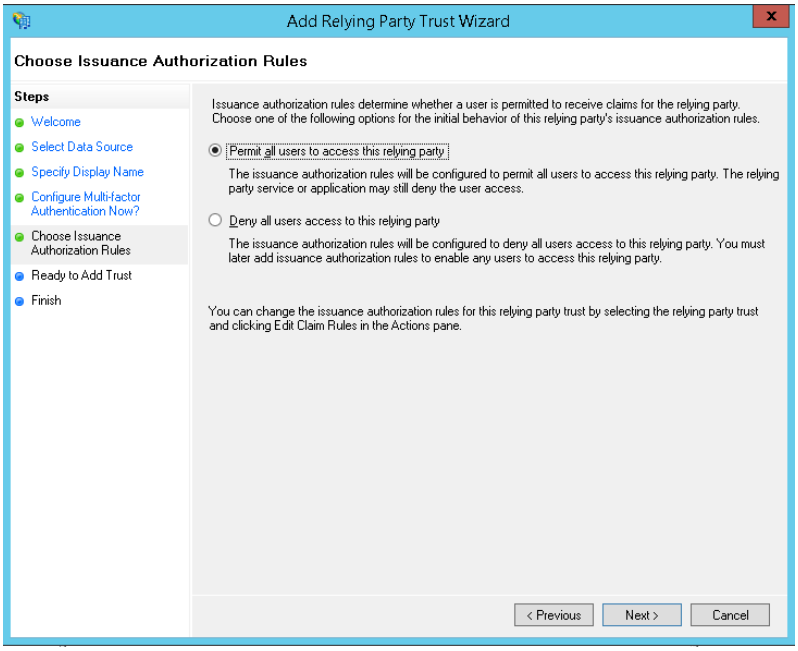
4. Cửa sổ **Specify Display Name**, trong ô **Display Name**, nhập **Adatum Test App**, và chọn **Next**.



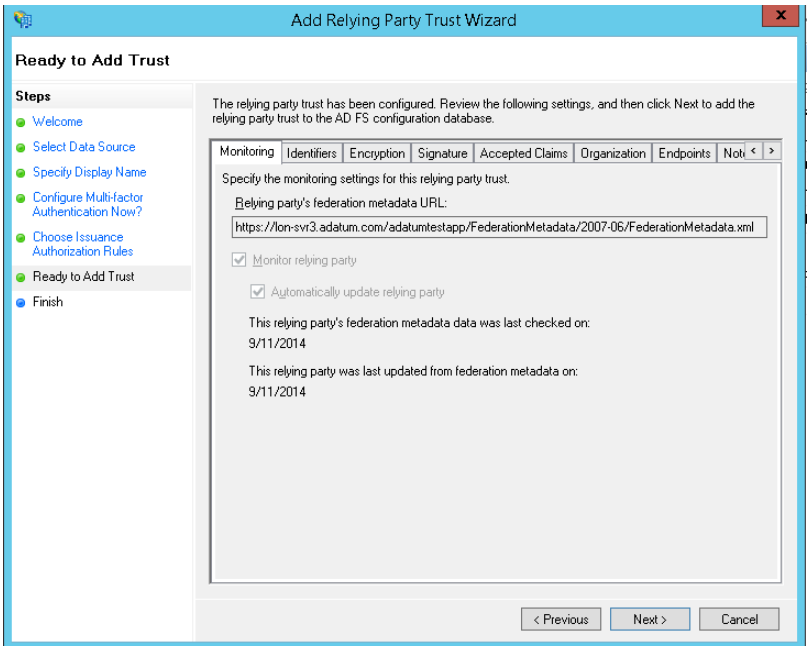

5. Cửa sổ **Configure Multi-Factor Authentication Now?**, chọn **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, chọn **Next**.



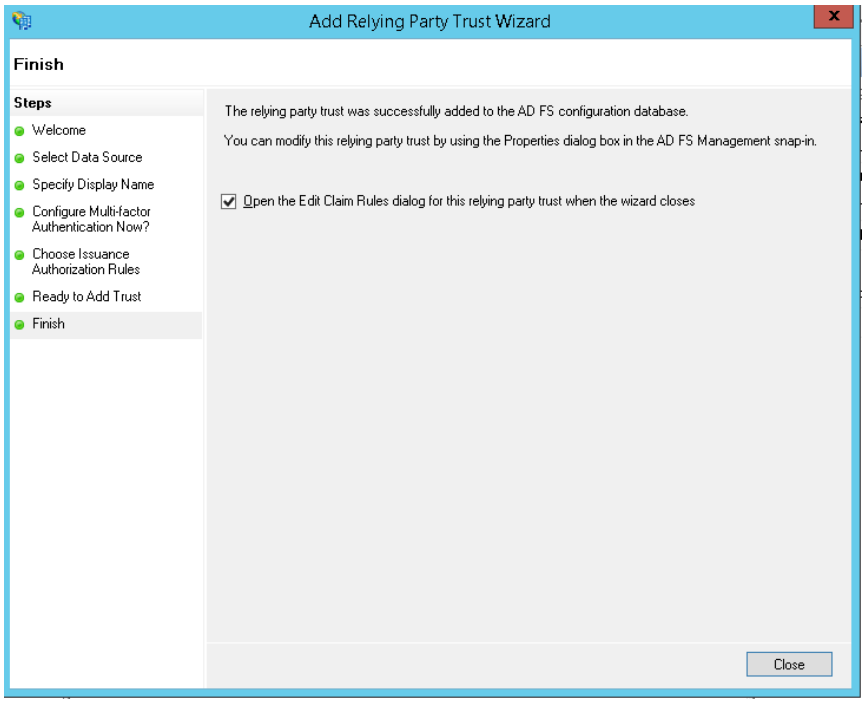
6. Cửa sổ **Choose Issuance Authorization Rules**, chọn **Permit all users to access this relying party**, và chọn **Next**.



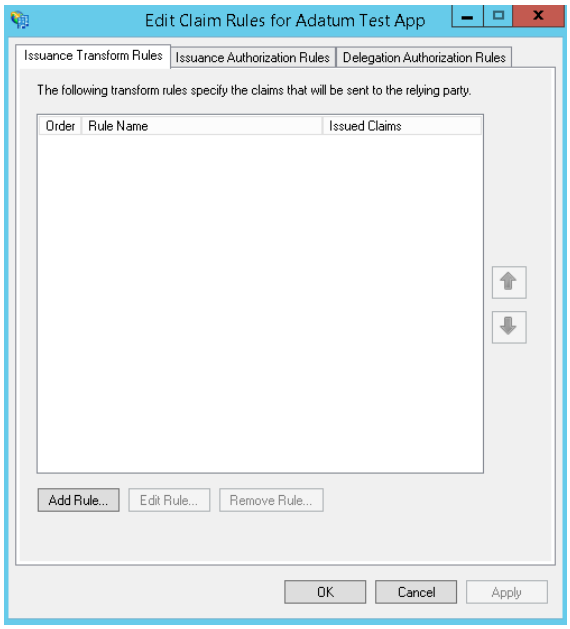

7. Cửa sổ **Ready to Add Trust**, chọn **Next**.



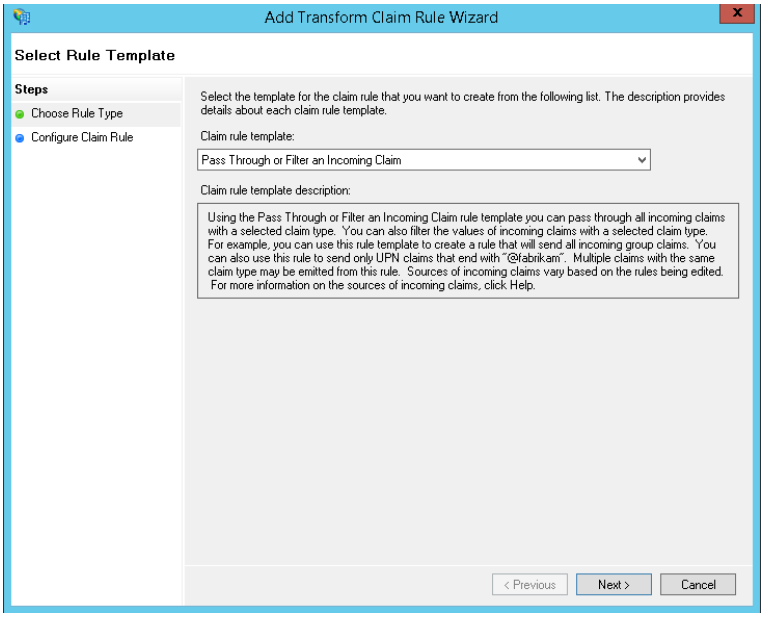
8. Cửa sổ **Finish**, chọn **Close**.



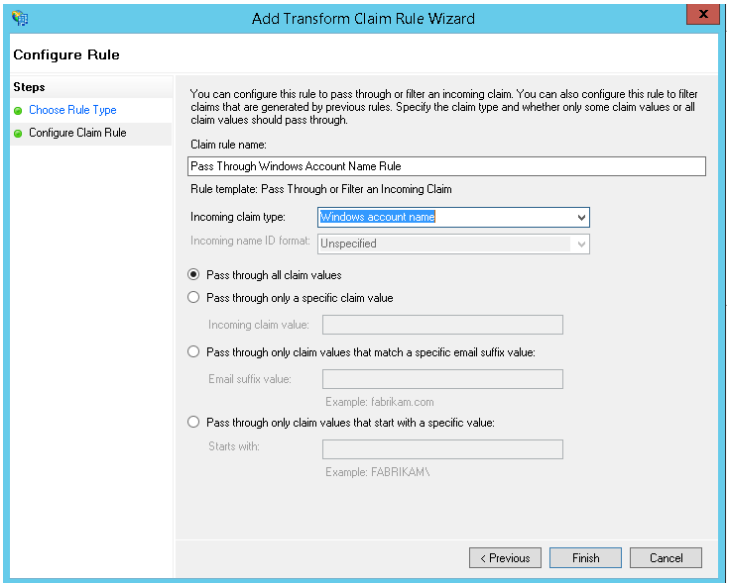

9. Cửa sổ **Edit Claim Rules for Adatum Test App properties**, trong tab **Issuance Transform Rules**, chọn **Add Rule**.



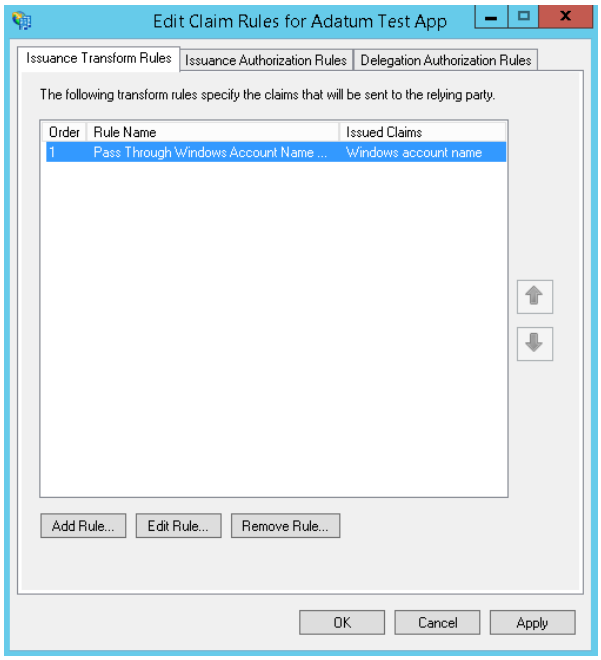
10. Cửa sổ **Select Rule Template**, bung ô **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim,** chọn **Next**.



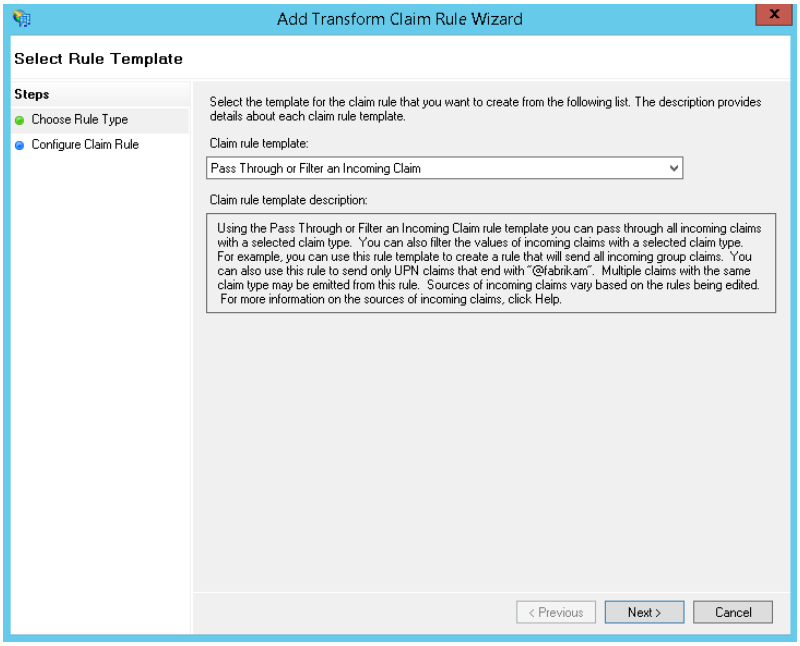

11. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Pass Through Windows Account Name Rule**. Bung ô **Incoming claim type**, chọn **Windows account name**, và chọn **Finish**.



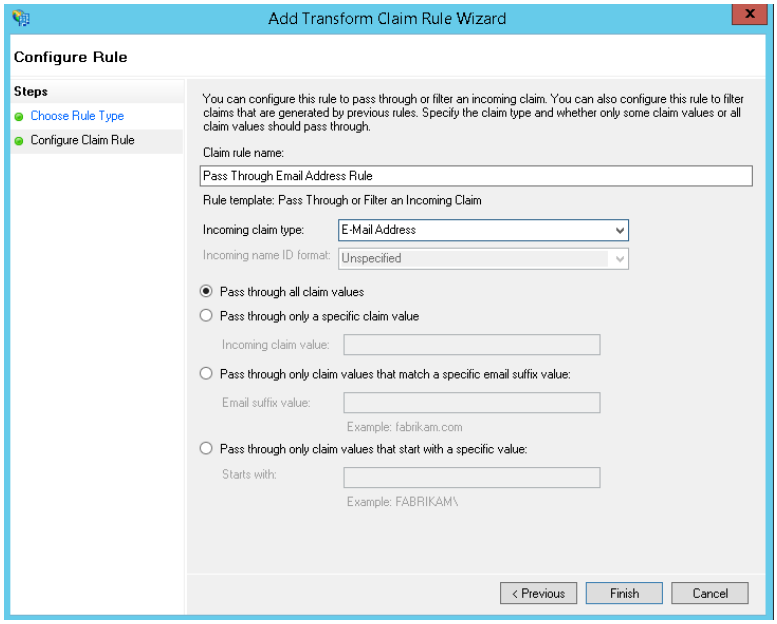
12. Cửa sổ **Edit Claim Rules for Adatum Test App properties,** chọn **Add Rule**.



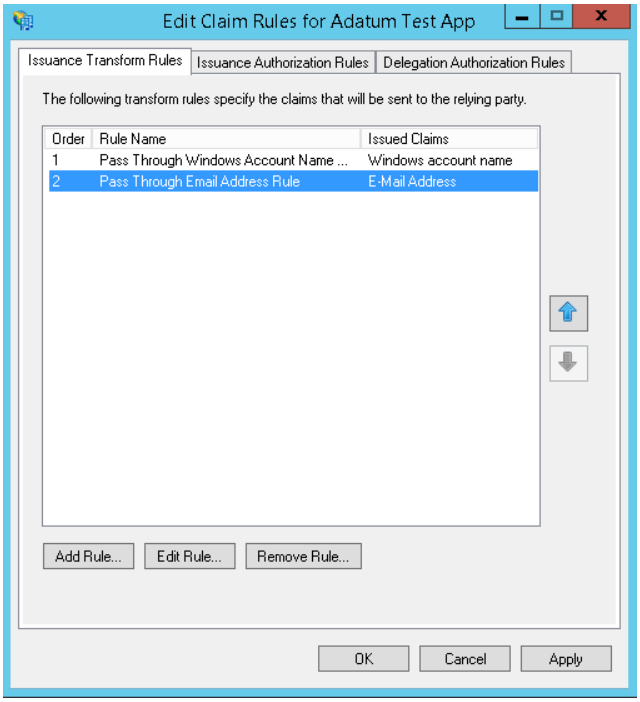

13. Cửa sổ **Select Rule Template**, bung **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.



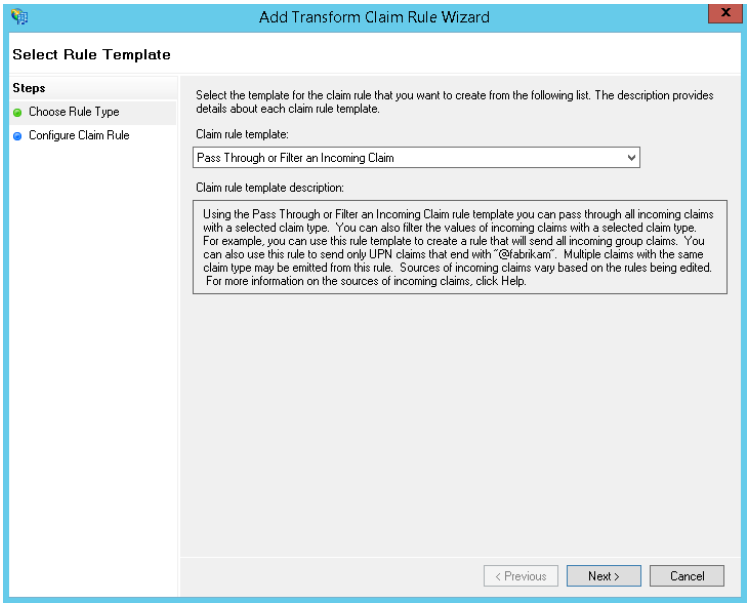
14. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Pass Through Email Address Rule**, bung ô **Incoming Claim Type**, chọn **E-mail Address**, và chọn **Finish**.



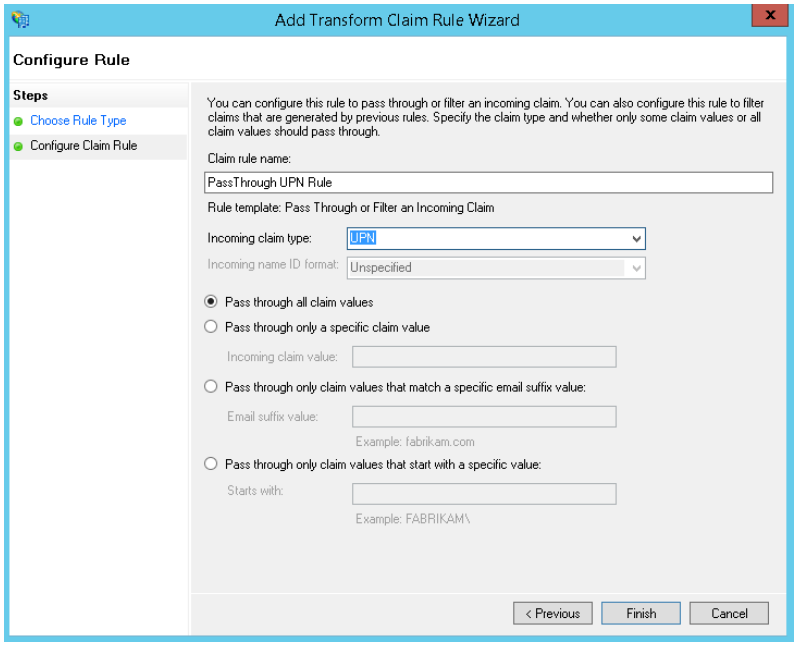

15. Cửa sổ **Edit Claim Rules for Adatum Test App properties,** chọn **Add Rule**.



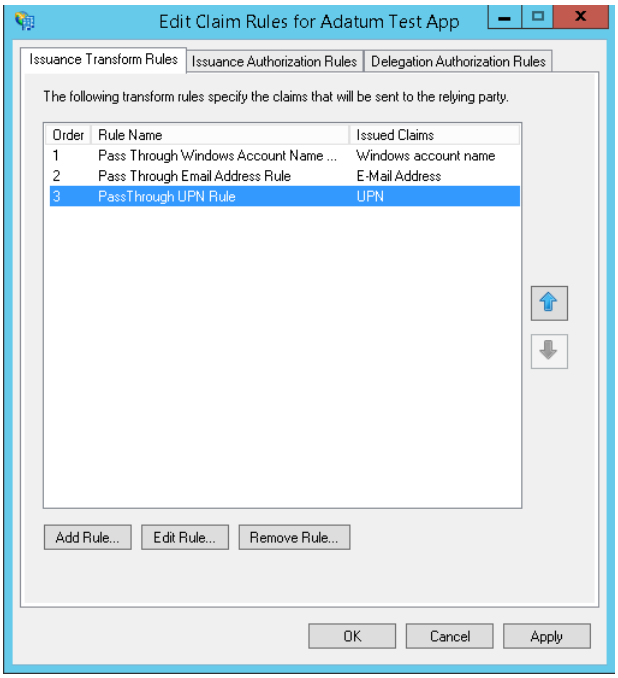
16. Cửa sổ **Select Rule Template**, bung **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim**, chọn **Next**.



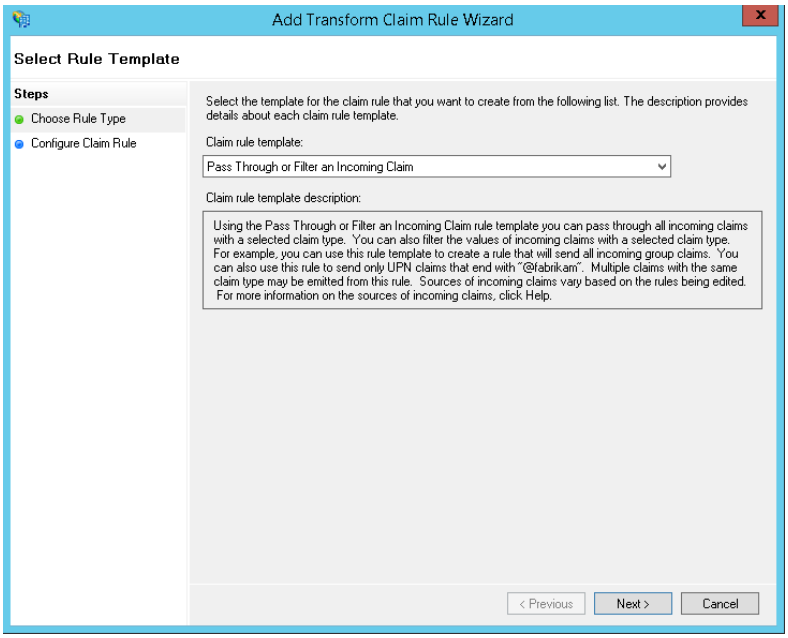

17. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Pass Through UPN Rule**, bung ô **Incoming Claim Type**, chọn **UPN**, và chọn **Finish**.



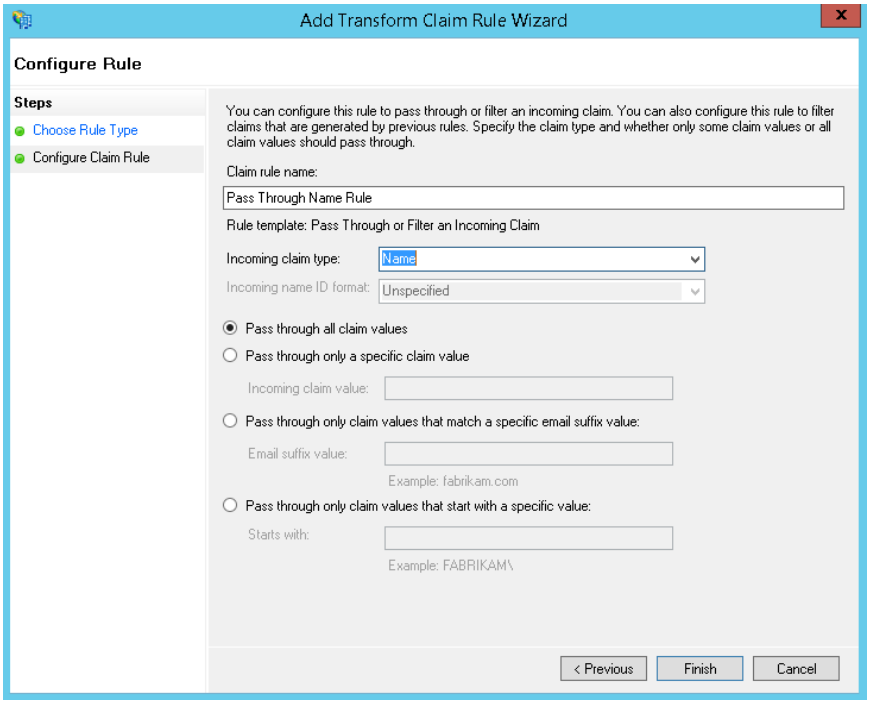
18. Cửa sổ **Edit Claim Rules for Adatum Test App properties,** chọn **Add Rule**.




19. Cửa sổ **Select Rule Template**, bung ô **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.

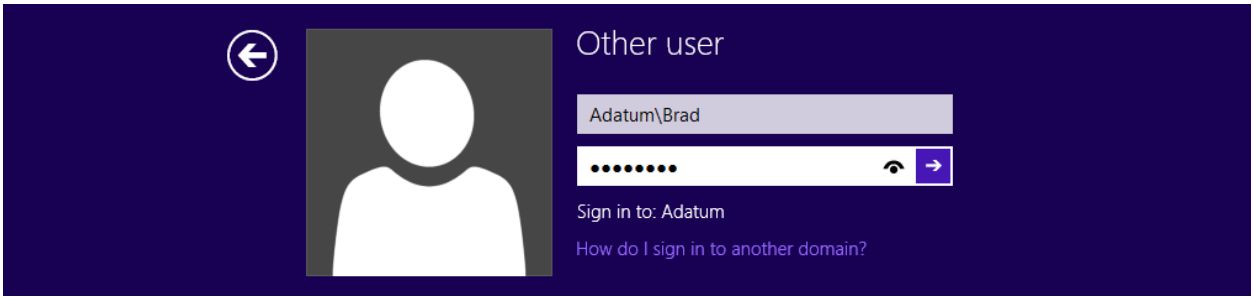


20. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Pass Through Name Rule**, bung ô **Incoming Claim Type**, chọn **Name**, chọn **Finish**, và chọn **OK.**




## Bước 5. Kiểm tra người dùng nội bộ truy cập ứng dụng.

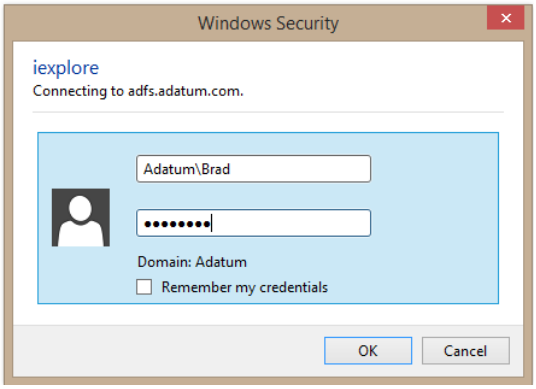
1. Sign in máy **LON-CL1** bằng **Adatum\Brad** với password **Pa$$w0rd**.



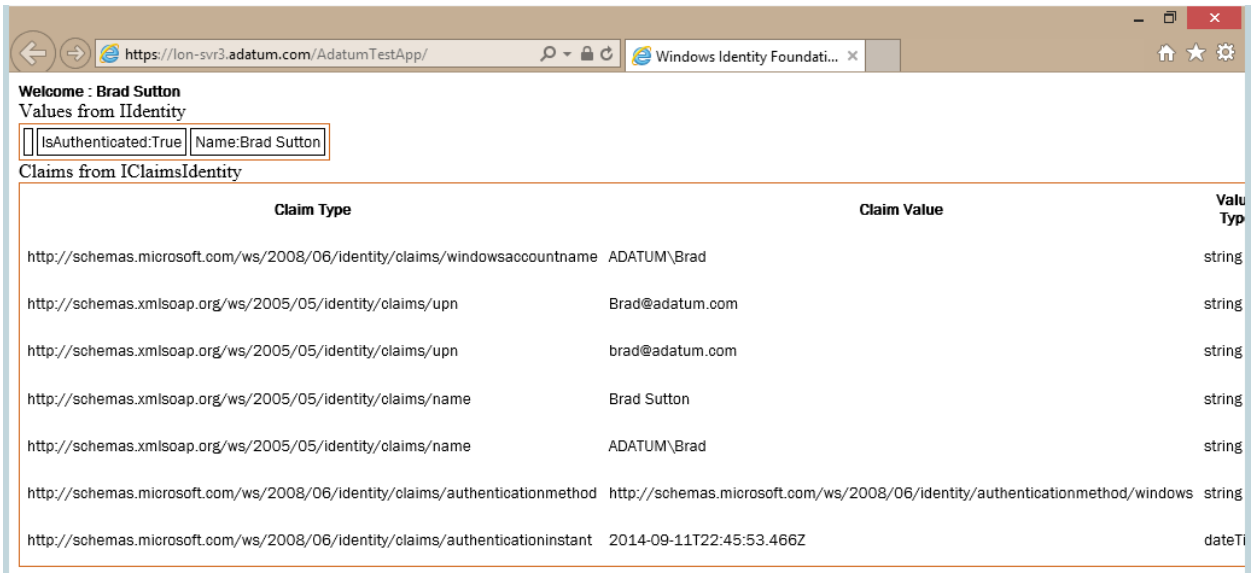

2. Mở **Internet Explorer**, truy cập **https://lon-svr3.adatum.com/AdatumTestApp/**

***Lưu ý: Phải đảm bảo có dấu gạch chéo (/) ở cuối dòng.***

3. Hộp thoại chứng thực, nhập **Adatum\Brad** với password **Pa$$w0rd**, chọn **OK**.




4. Kiểm tra truy cập thành công.




5. Tắt **Internet Explorer**.

**Kết quả: Trong bài tập này, bạn đã cài đặt và cấu hình thành công AD FS hỗ trợ người dùng trong nội bộ truy cập ứng dụng WIF của A. Datum.**

## Bài tập 3: Triển khai AD FS cho một tổ chức đối tác.

Trong bài tập này, bạn phải cấu hình ADFS cho phép người dùng của Trey Research truy cập ứng dụng web. Bạn phải cấu hình tích hợp AD FS tại Trey Research với AD FS tại A. Datum, và sau đó xác minh rằng người sử dụng của Trey nghiên cứu có thể truy cập ứng dụng. Ngoài ra, bạn phải cấp quyền truy cập dựa trên các nhóm người dùng.

❖ **Bài tập bao gồm các bước:**

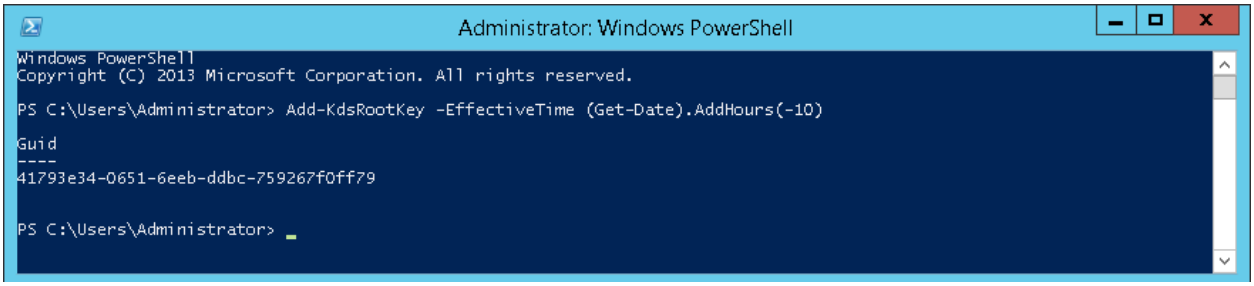
1. Cài đặt và cấu hình AD FS Server role trên Trey-DC1.
2. Thêm Claims Provider Trust cho AD FS Server của TreyResearch.net.
3. Cấu hình Relying Party Trust trên TREY-DC1 cho ứng dụng web của A. Datum.
4. Kiểm tra người dùng của Trey Research truy cập ứng dụng của A. Datum.
5. Cấu hình Claim rules để cấp quyền truy cập cho một nhóm cụ thể.
6. Kiểm tra truy cập.

❖ **Thực hiện:**

### Bước 1. Cài đặt và cấu hình AD FS Server role trên Trey-DC1.

1. Qua máy **Trey-DC1**, mở **Windows PowerShell,** gõ lệnh:

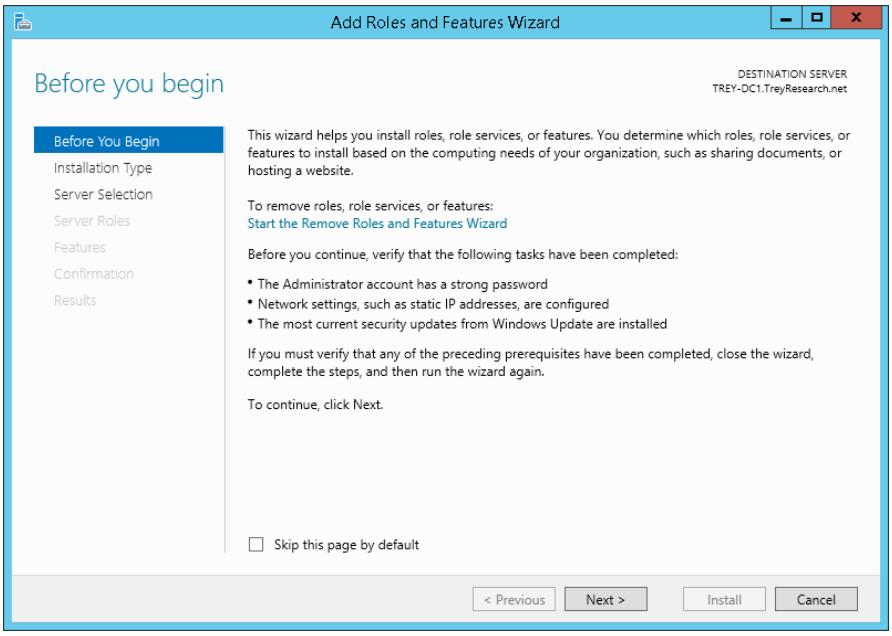
**Add-KdsRootKey –EffectiveTime (Get-Date).AddHours(-10)**



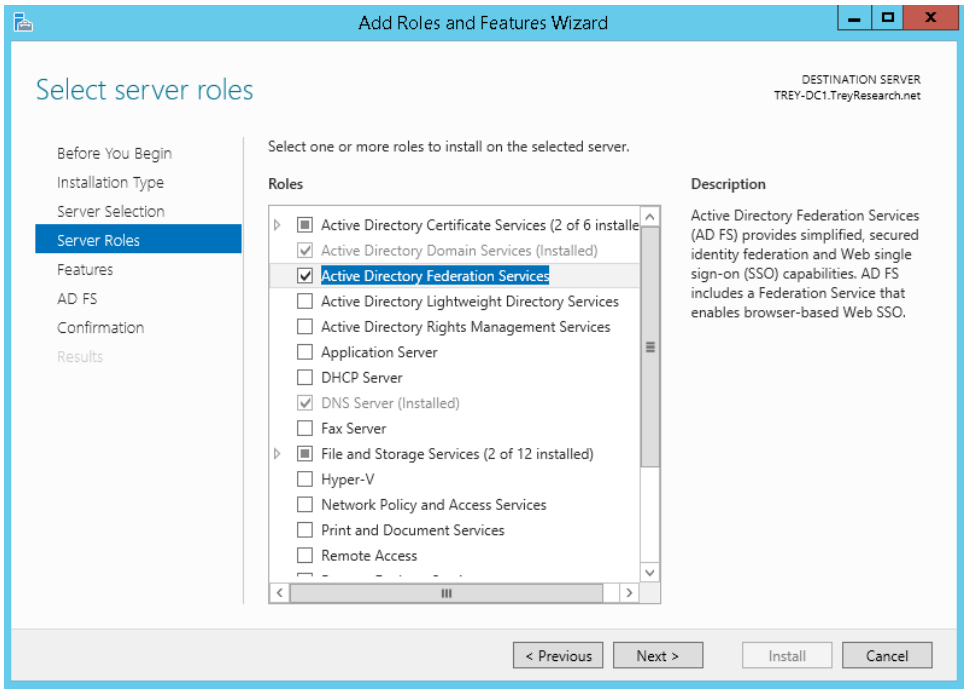

2. Tắt **Windows PowerShell**.

3. Trong cửa sổ **Server Manager**, chọn **Add Roles and Features**.

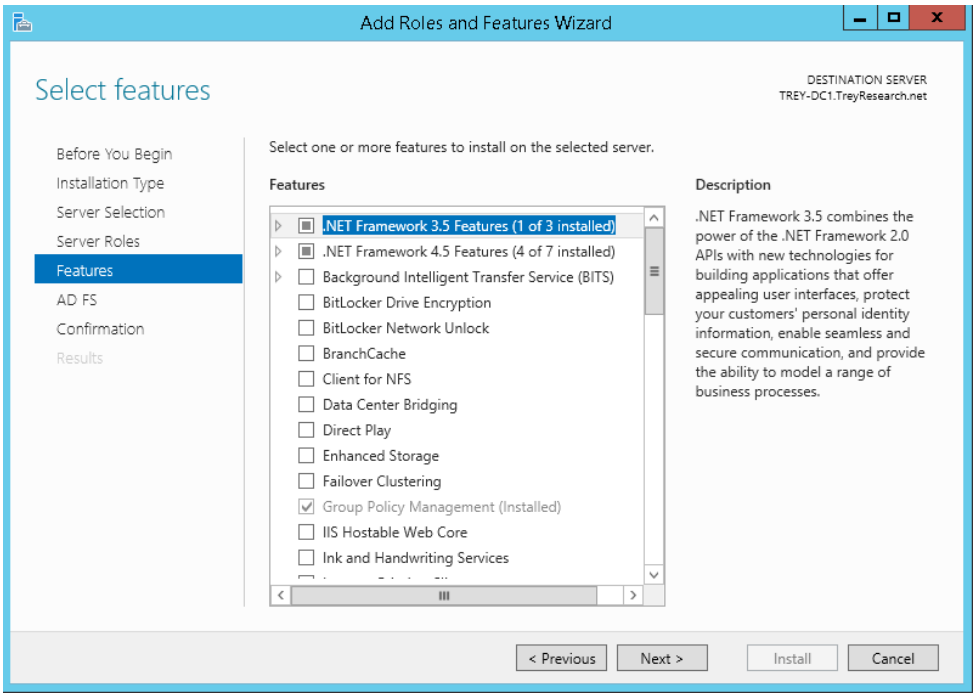
4. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



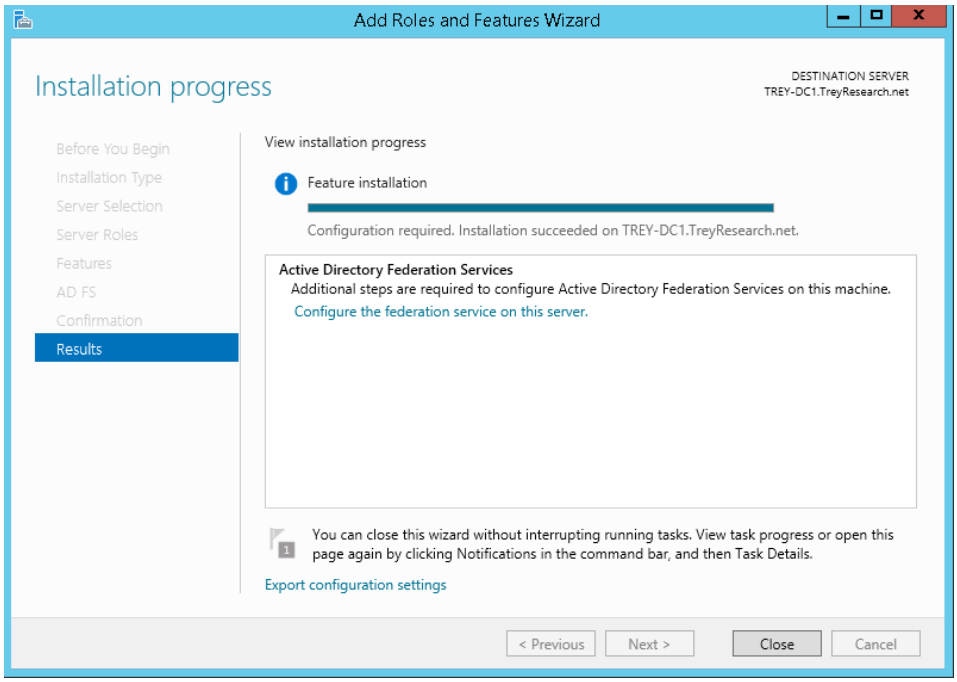

5. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Federation Services**, và chọn **Next**.



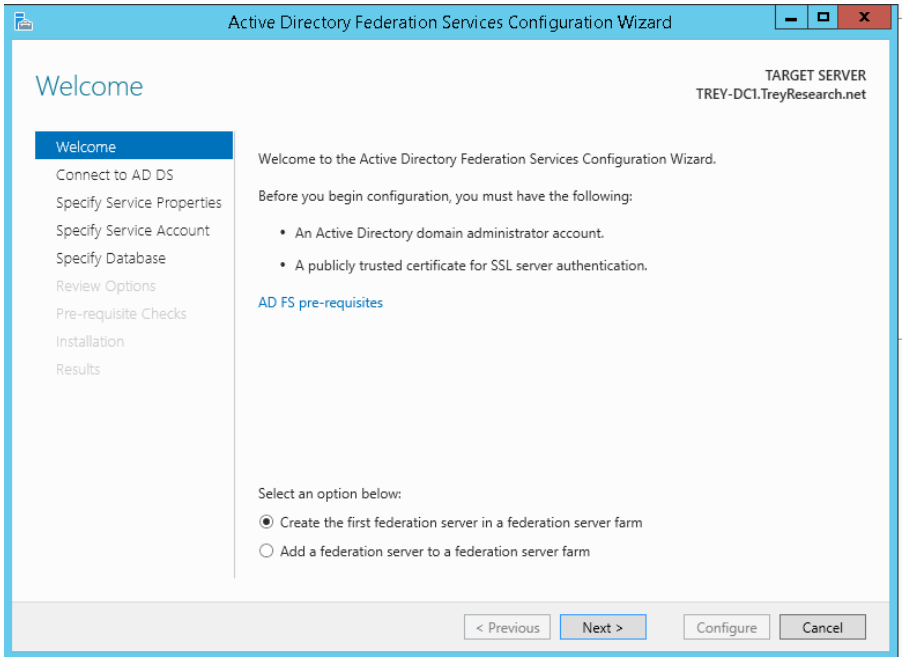
6. Cửa sổ **Select features**, chọn **Next** 2 lần, và chọn **Install.**



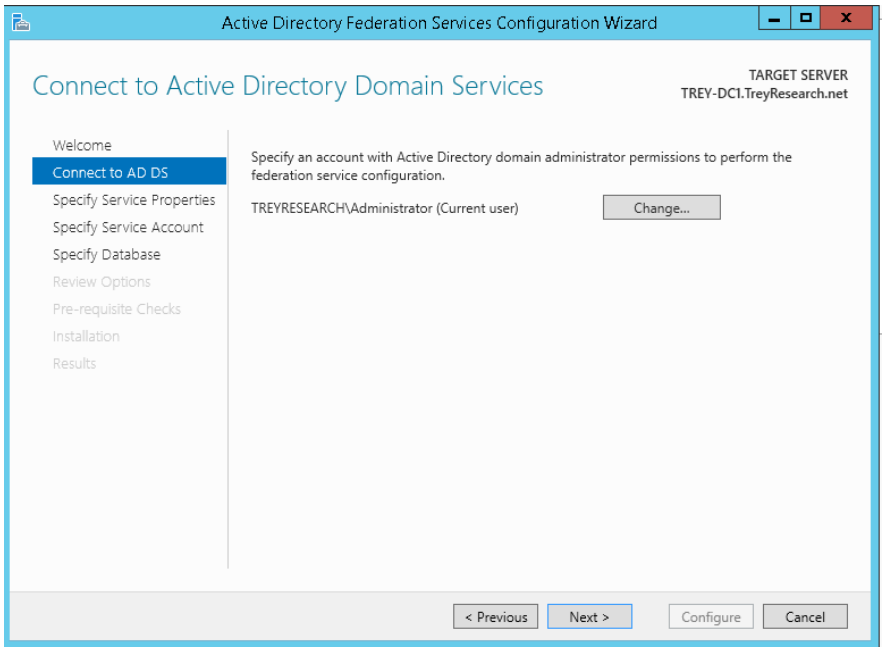

7. Sau khi cài đặt thành công, chọn **Configure the federation service on this server**.



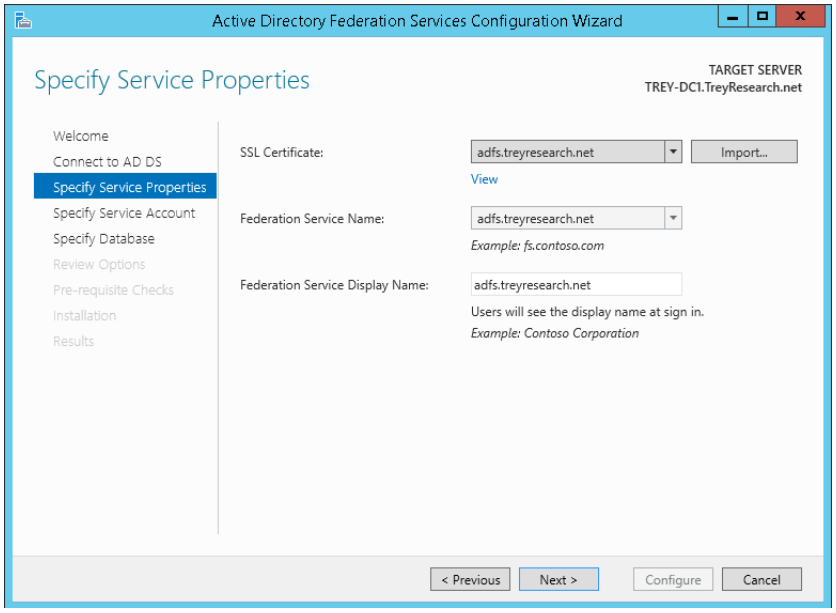
8. Cửa sổ **Welcome**, chọn **Create the first federation server in a federation server farm**, và chọn **Next**.



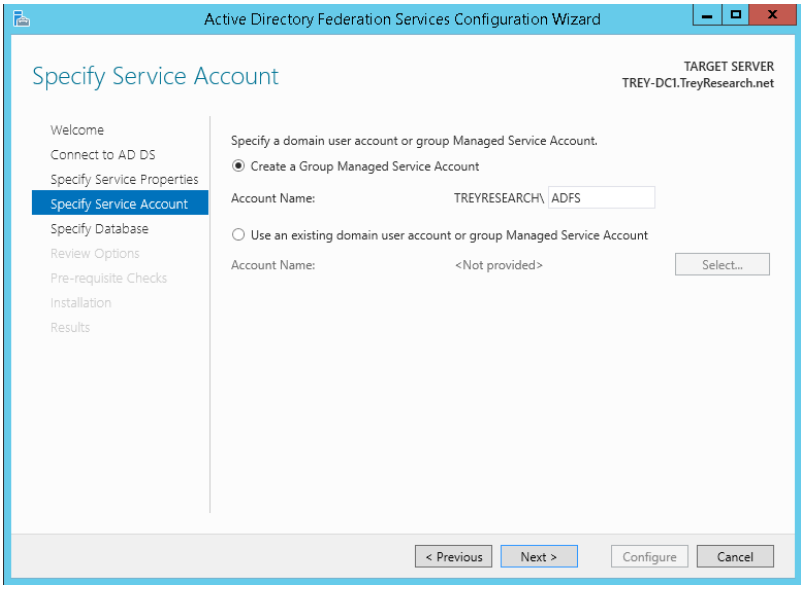

9. Cửa sổ **Connect to Active Directory Domain Services**, chọn **Next**.



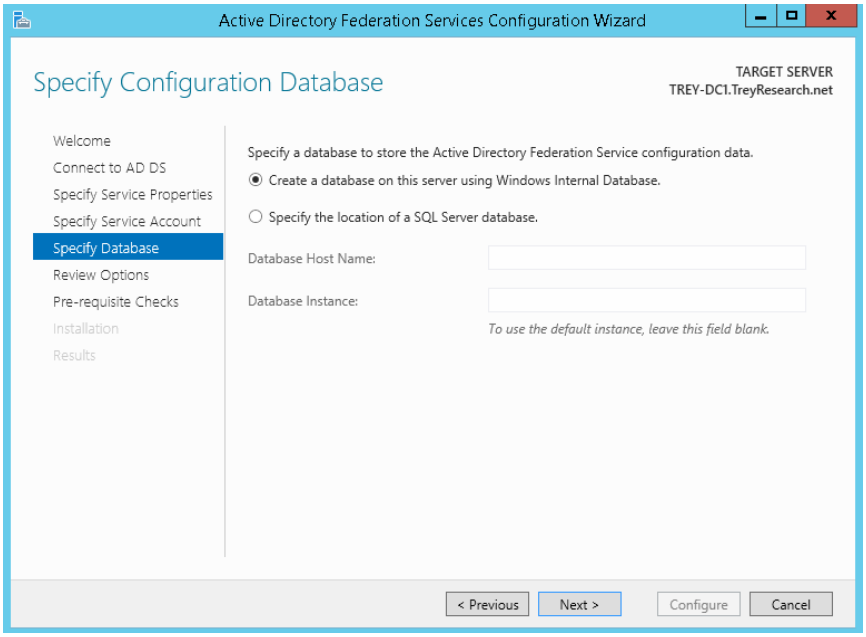
10. Cửa sổ **Specify Service Properties**, bung ô **SSL certificate,** chọn certificate tên **adfs.treyresearch.net**. Nhập **adfs.treyresearch.net** vào ô **Federation Service Display Name**, và chọn **Next**.



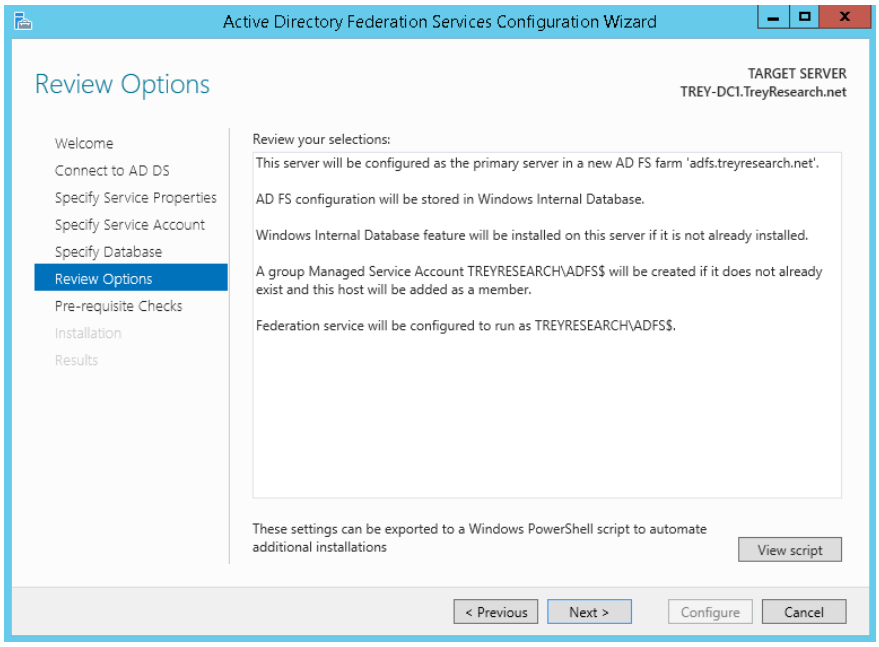

11. Cửa sổ **Specify Service Account**, chọn **Create a Group Managed Service Account**, trong ô **Account Name**, nhập **ADFS**, và chọn **Next**.



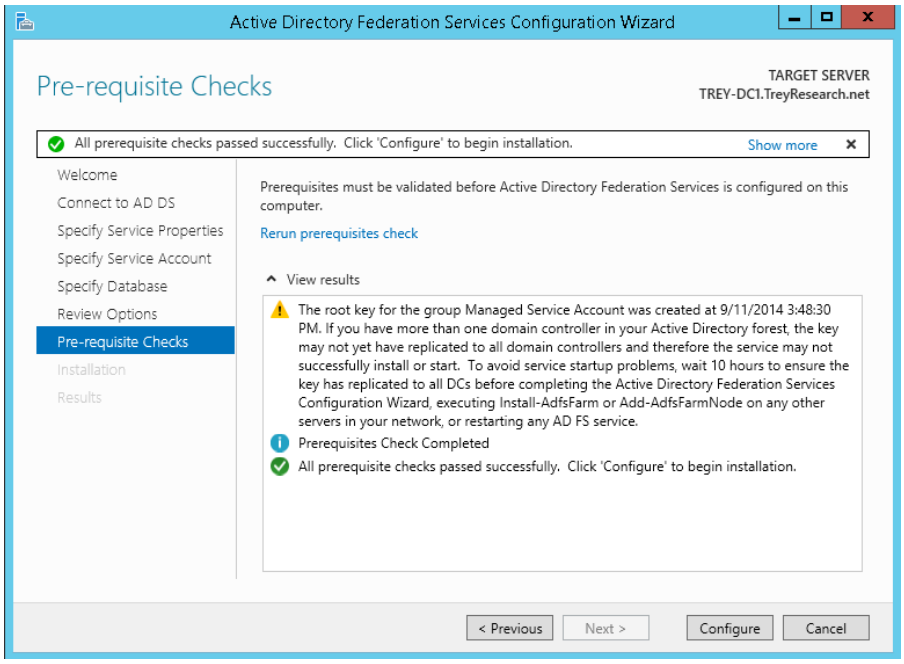
12. Cửa sổ **Specify Configuration Database**, chọn **Create a database on this server using Windows Internal Database**, và chọn **Next**.



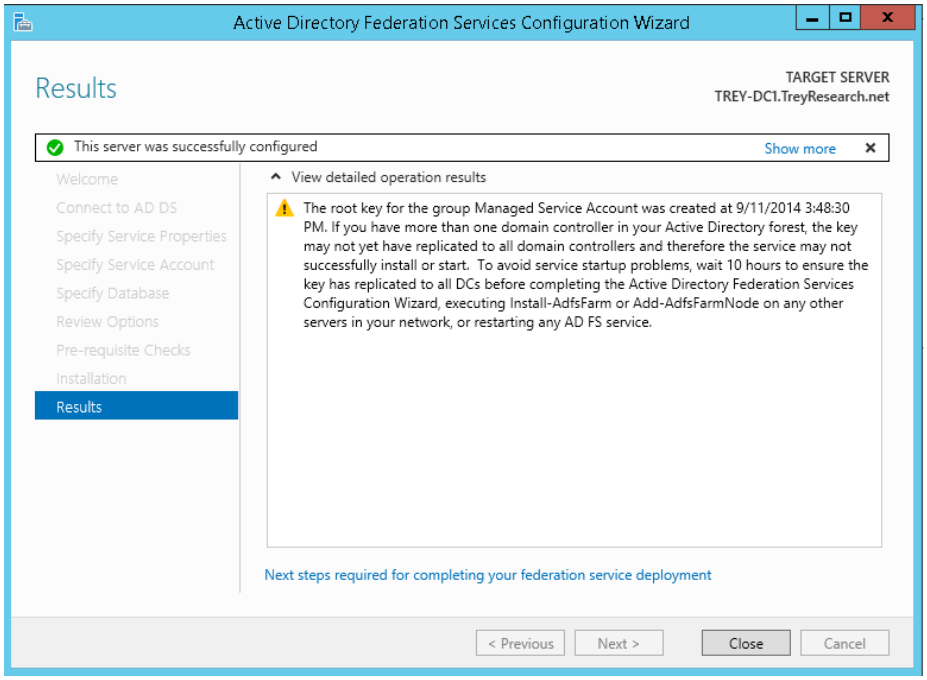

13. Cửa sổ **Review Options**, chọn **Next**.



14. Cửa sổ **Pre-requisite Checks**, chọn **Configure**.




15. Cửa sổ **Results** (lưu ý có lỗi dịch vụ đăng ký tên chính), chọn **Close**.



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

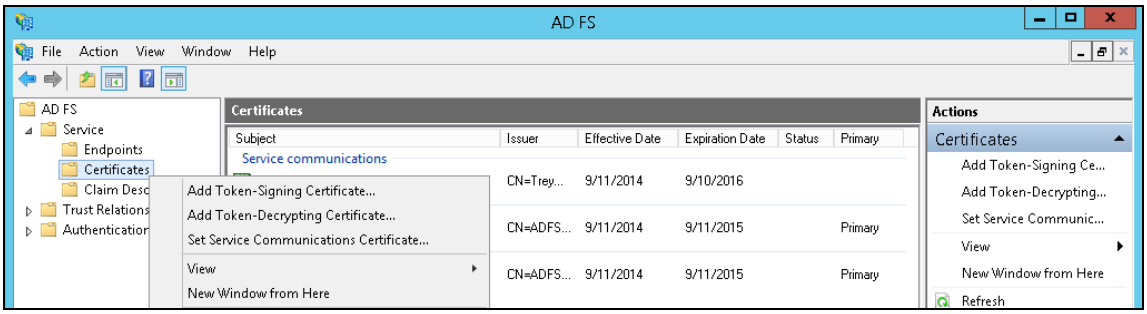
**Set-ADFSProperties –AutoCertificateRollover $False**



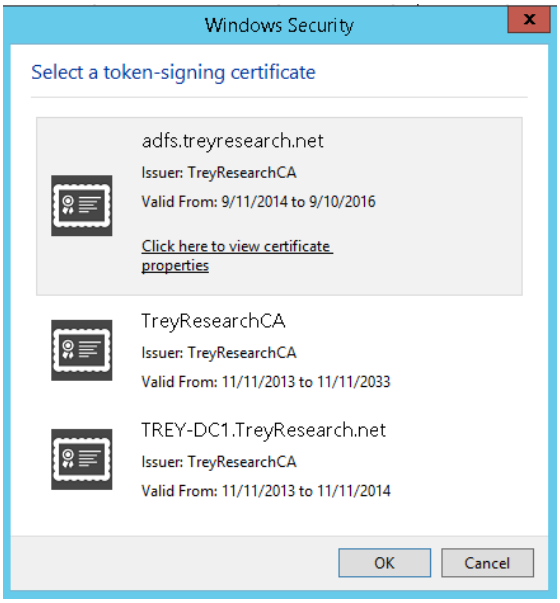

17. Tắt **Windows PowerShell**.

18. Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **AD FS Management**.

19. Trong cửa sổ **AD FS**, bung **Service**, chuột phải **Certificates**, chọn **Add Token-Signing Certificate**.

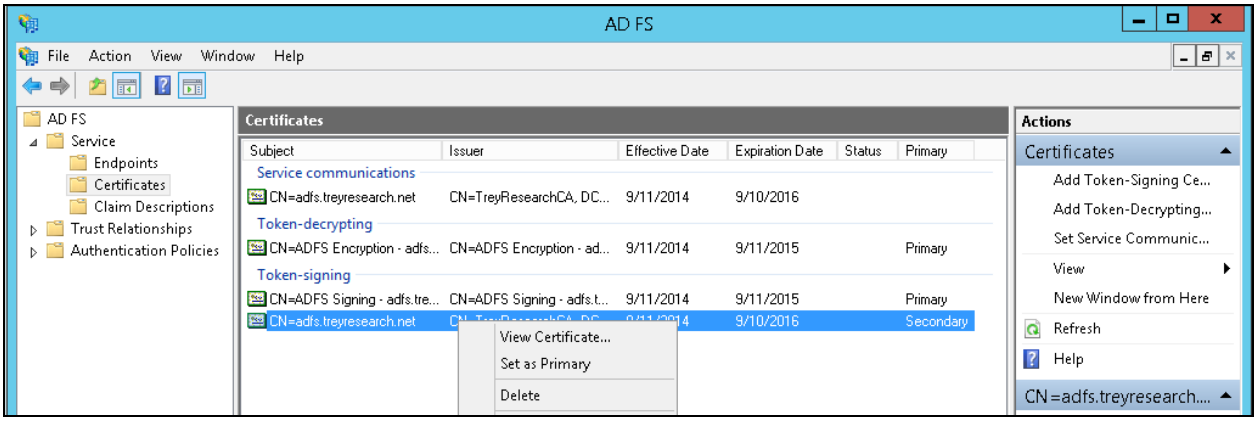



20. Cửa sổ **Windows Security,** chọn certificate tên **adfs.treyresearch.net**, chọn **OK.**

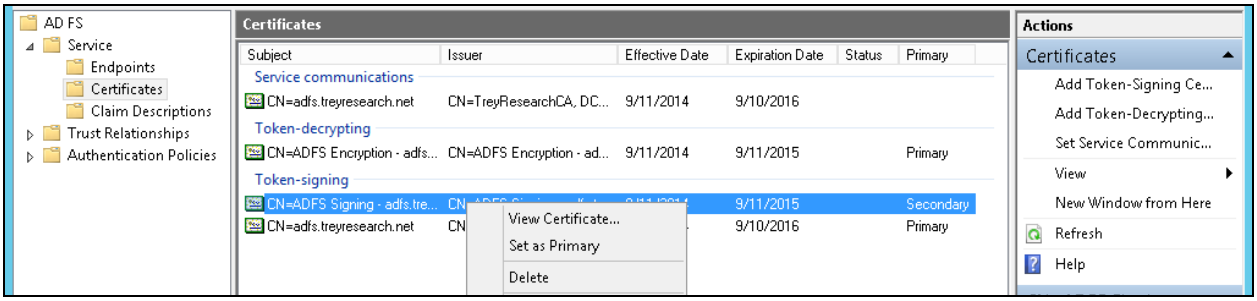


21. Hộp thoại thông báo **AD FS Management**, chọn **OK**.

22. Trong phần **Token-signing**, chuột phải lên certificate mới dược thêm vào (**CN=adfs.treyresearch.net**), chọn **Set as Primary**. Hộp thoại thông báo, chọn **Yes**.



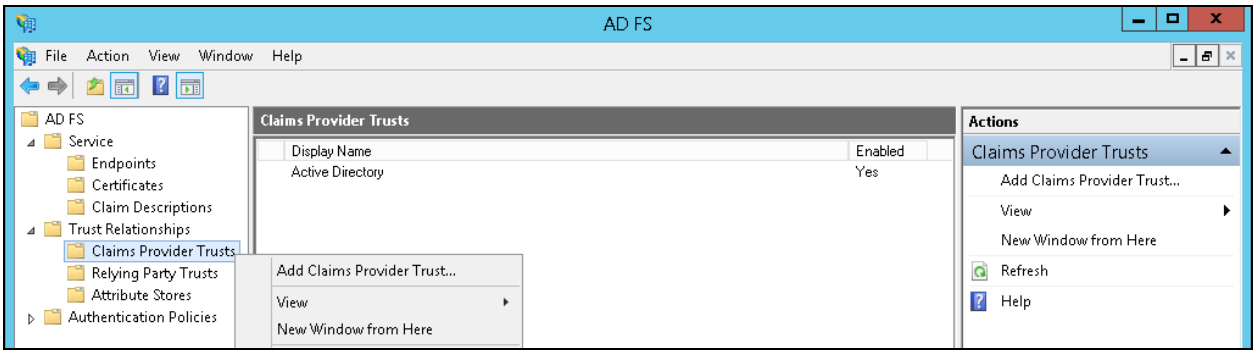

23. Chuột phải lên certificate đang ở chế độ **Secondary**, chọn **Delete**. Hộp thoại thông báo, chọn **Yes.**



## Bước 2. Thêm Claims Provider Trust cho AD FS Server của TreyResearch.net.

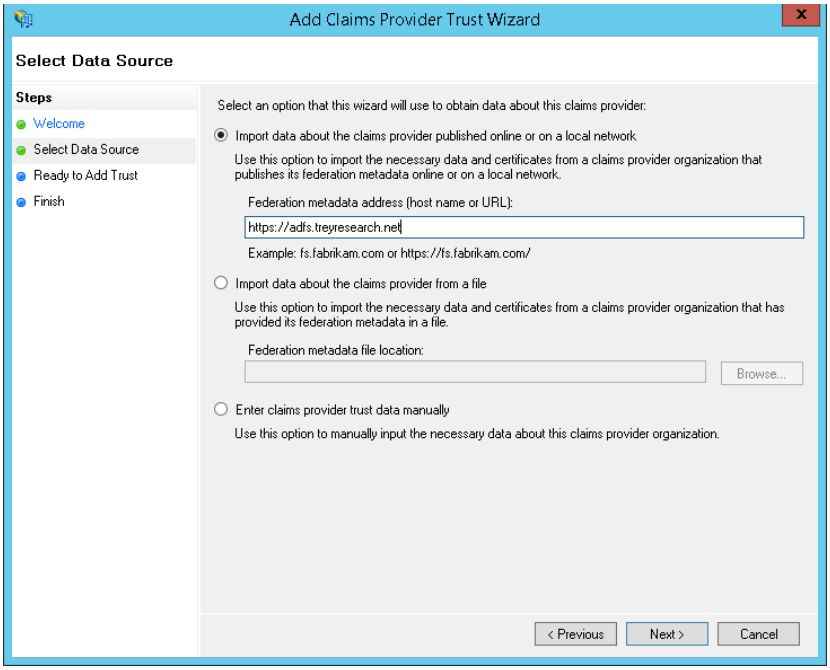
1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **AD FS Management**.

2. Trong cửa sổ **AD FS**, bung **Trust Relationships**, chuột phải **Claims Provider Trusts**, chọn **Add Claims Provider Trust**.

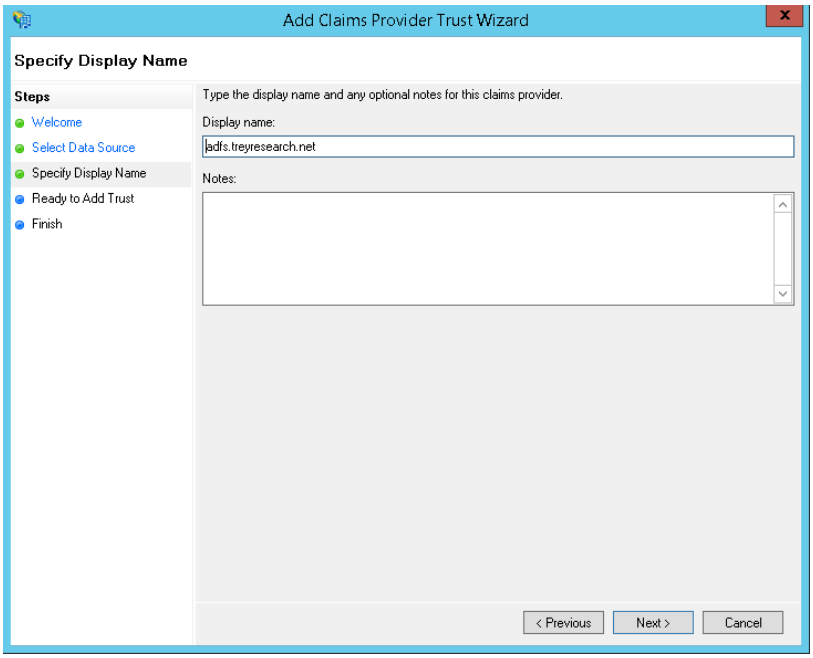



3. Cửa sổ **Welcome**, chọn **Start**.

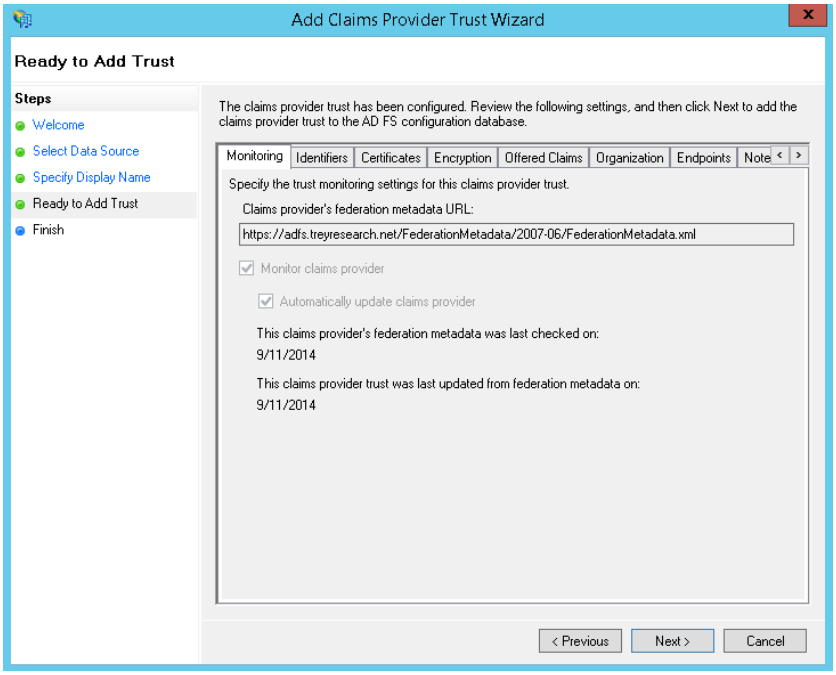
4. Cửa sổ **Select Data Source**, chọn **Import data about the claims provider published online or on a local network**, nhập **https://adfs.treyresearch.net** vào ô **host name**, và chọn **Next**.



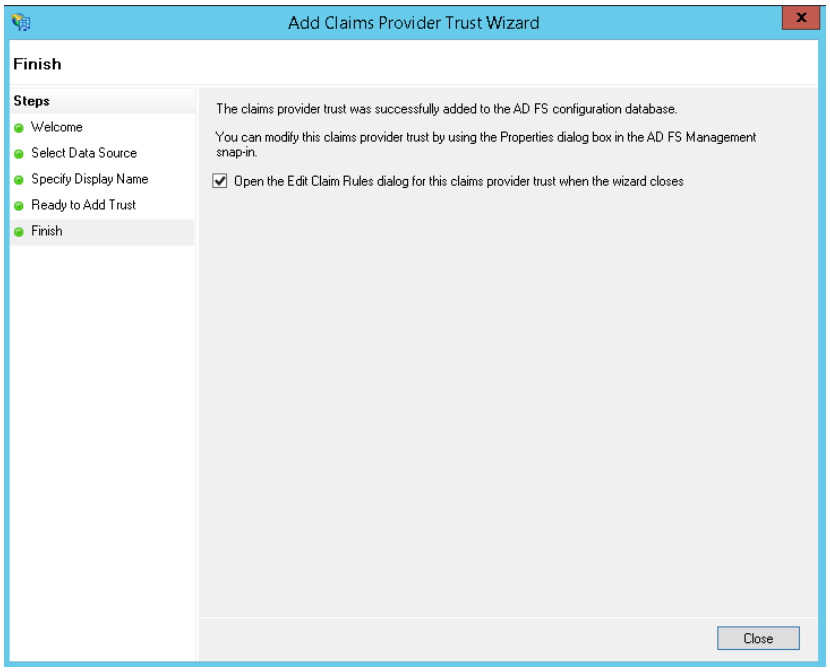
5. Cửa sổ **Specify Display Name**, chọn **Next**.



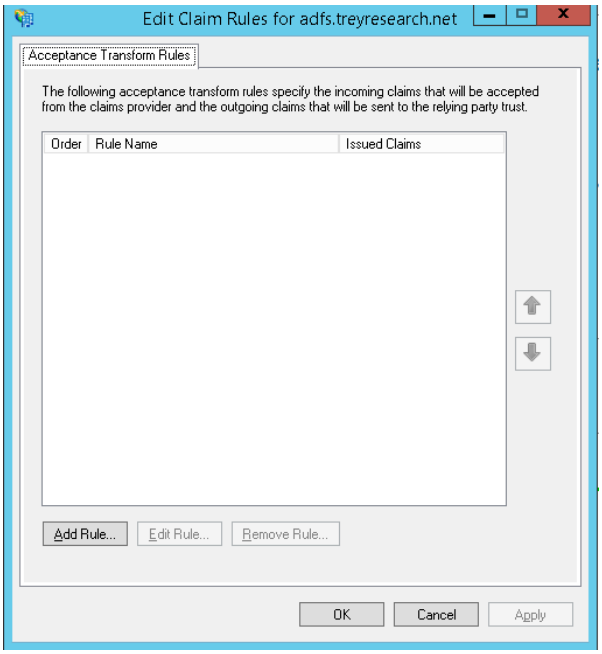

6. Cửa sổ **Ready to Add Trust**, chọn **Next**.



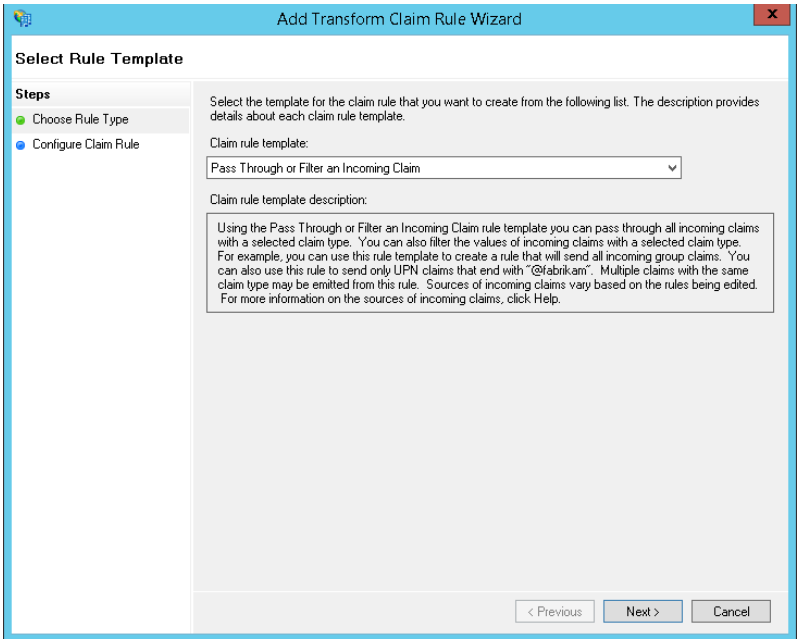
7. Cửa sổ **Finish**, chọn **Close**.



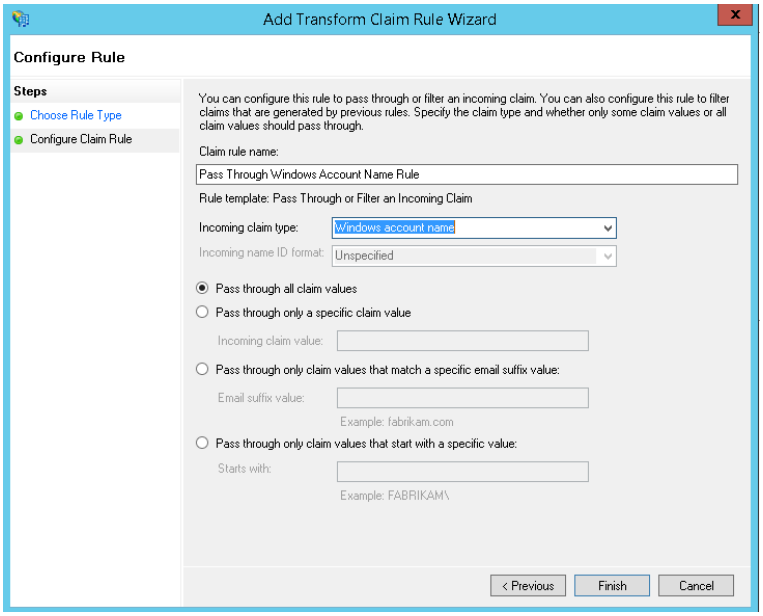

8. Hộp thoại **Edit Claim Rules for adfs.treyresearch.net properties**, trong tab **Acceptance Transform Rules**, chọn **Add Rule**.



9. Bung ô **Claim Rule Template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.

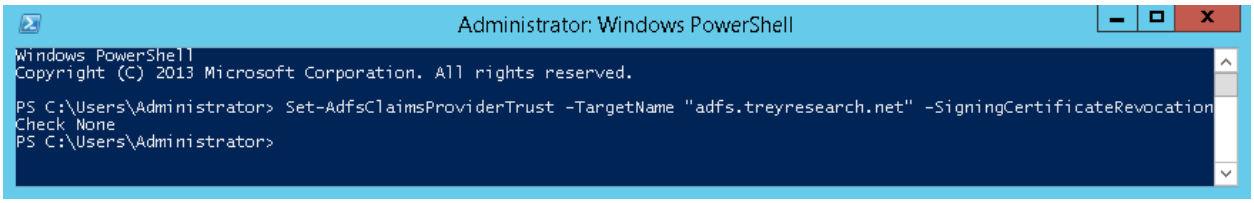



10. Trong ô **Claim rule name**, nhập **Pass Through Windows Account Name Rule**, bung ô **Incoming claim type**, chọn **Windows account name**, chọn **Finish**, chọn **Yes,** và chọn **OK**.



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

**Set-ADFSClaimsProviderTrust –TargetName "adfs.treyresearch.net" –SignningCertificateRevocationCheck None**

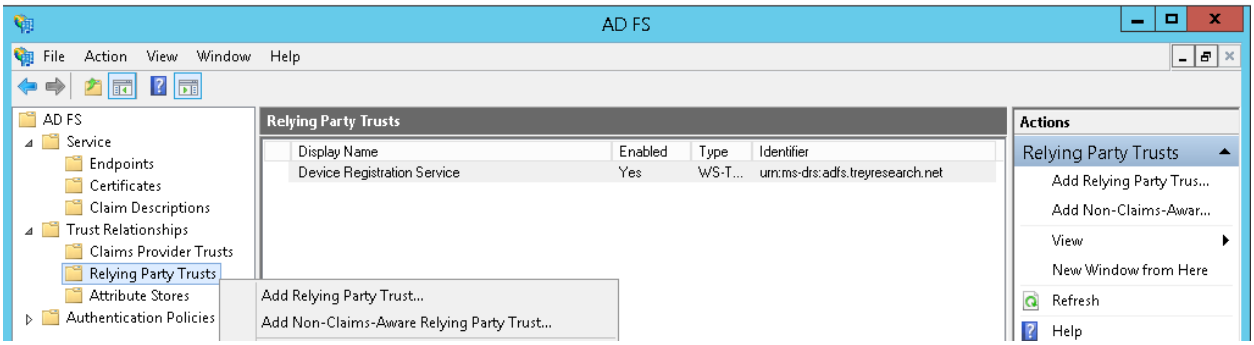



12. Tắt **Windows PowerShell**.

## Bước 3. Cấu hình Relying Party Trust trên TREY-DC1 cho ứng dụng web của A. Datum.

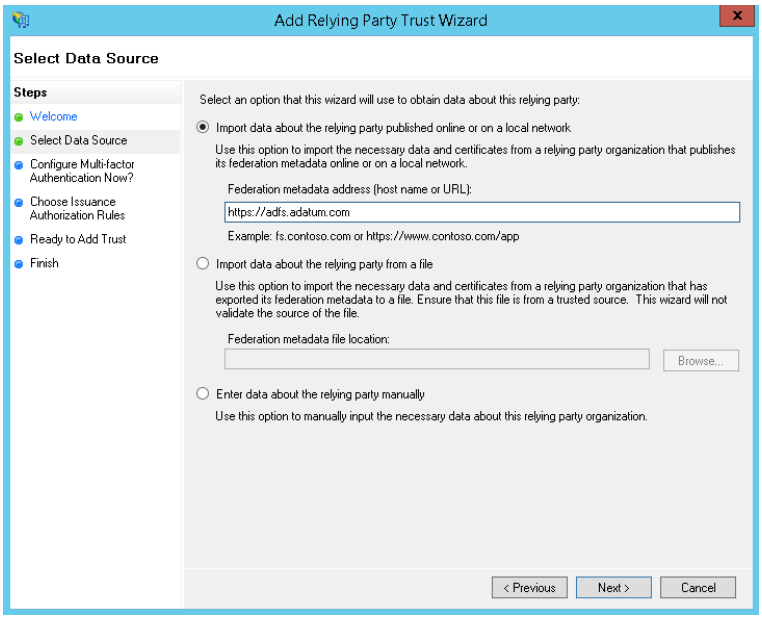
1. Qua máy **TREY-DC1**, trong **Server Manager**, bung menu **Tools**, mở **AD FS Management**.

2. Trong cửa sổ **AD FS**, bung **Trust Relationships**, chuột phải **Relying Party Trusts**, chọn **Add Relying Party Trust**.

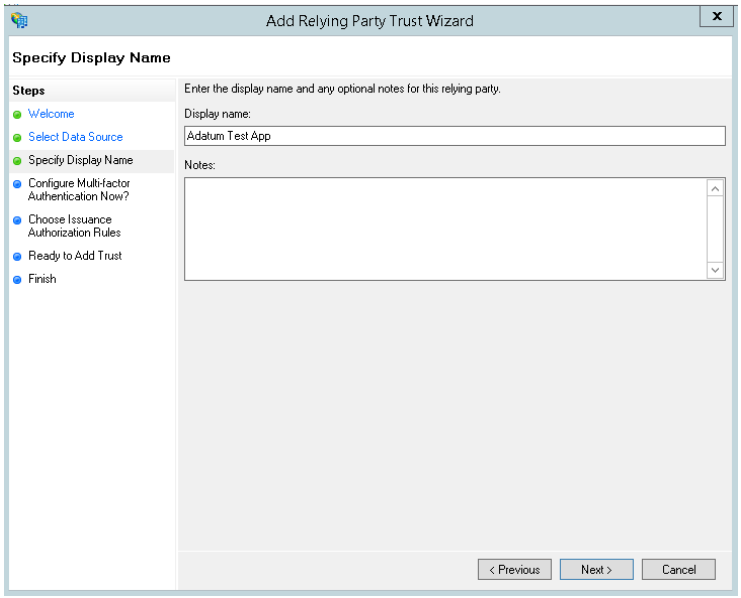



3. Cửa sổ **Welcome**, chọn **Start**.

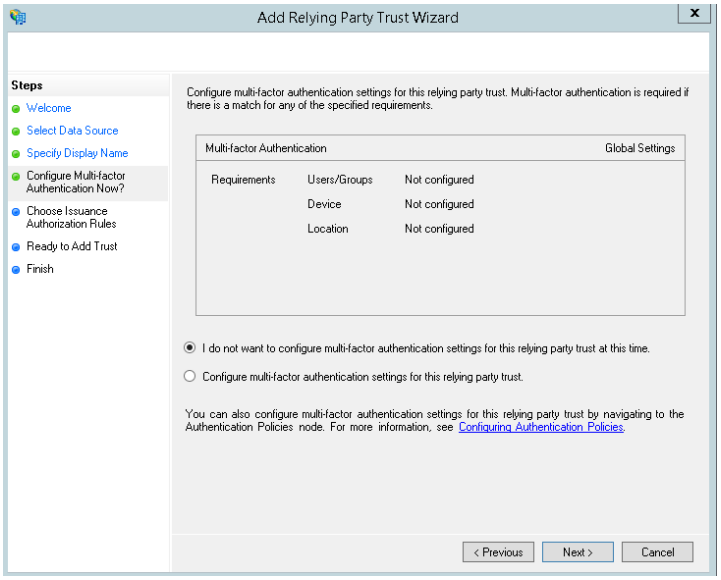
4. Cửa sổ **Select Data Source**, chọn **Import data about the relying party published online or on a local network**, nhập **https://adfs.adatum.com** vào ô **host name**, chọn **Next**.



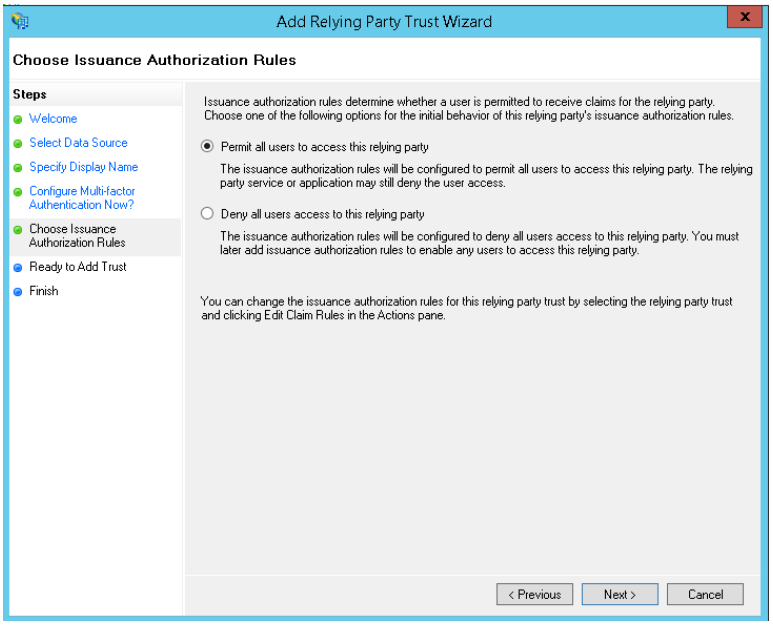

5. Cửa sổ **Specify Display Name**, trong ô **Display name**, nhập **Adatum TestApp**, chọn **Next**.



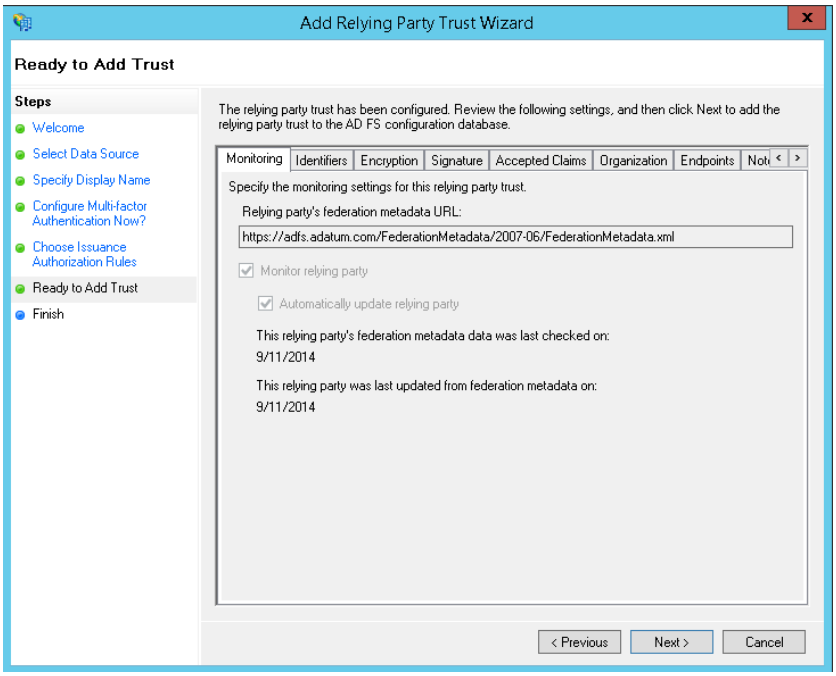
6. Cửa sổ **Configure Multi-factor Authentication Now?**, chọn **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, và chọn **Next**.



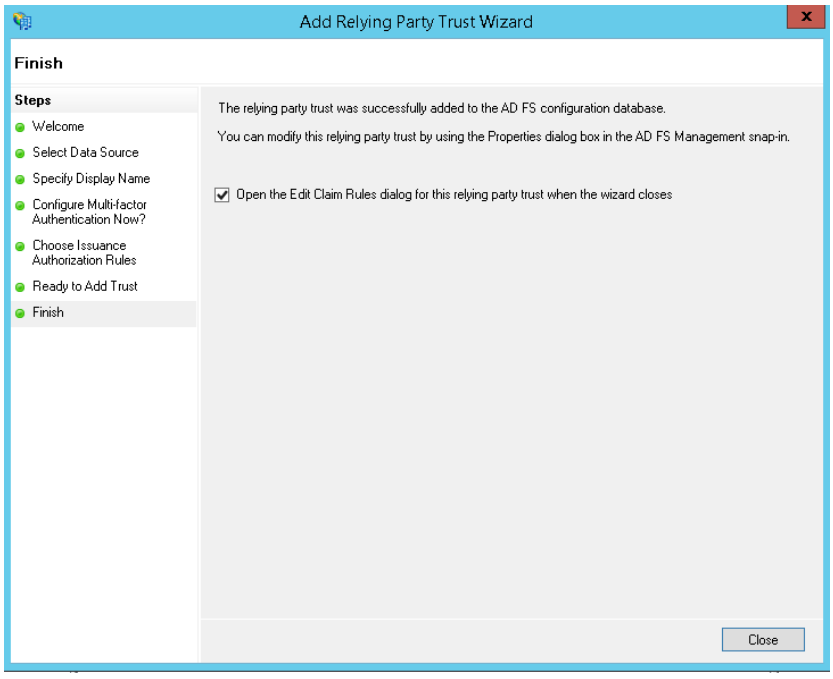

7. Cửa sổ **Choose Issuance Authorization Rules**, chọn **Permit all users to access this relying party**, chọn **Next**.



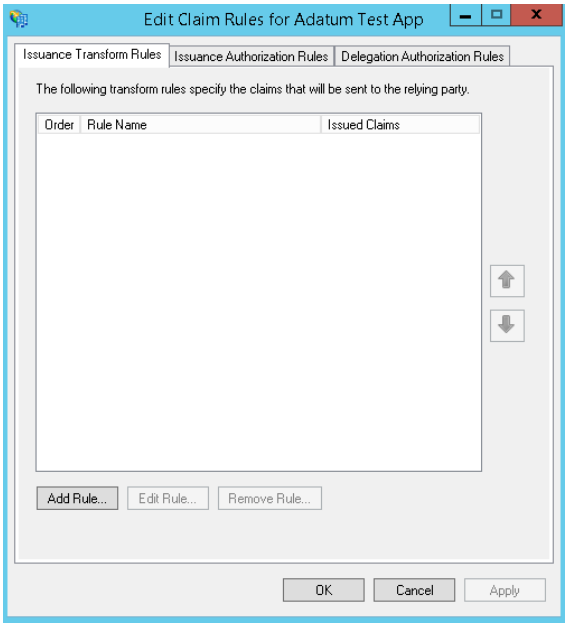
8. Cửa sổ **Ready to Add Trust**, chọn **Next**.



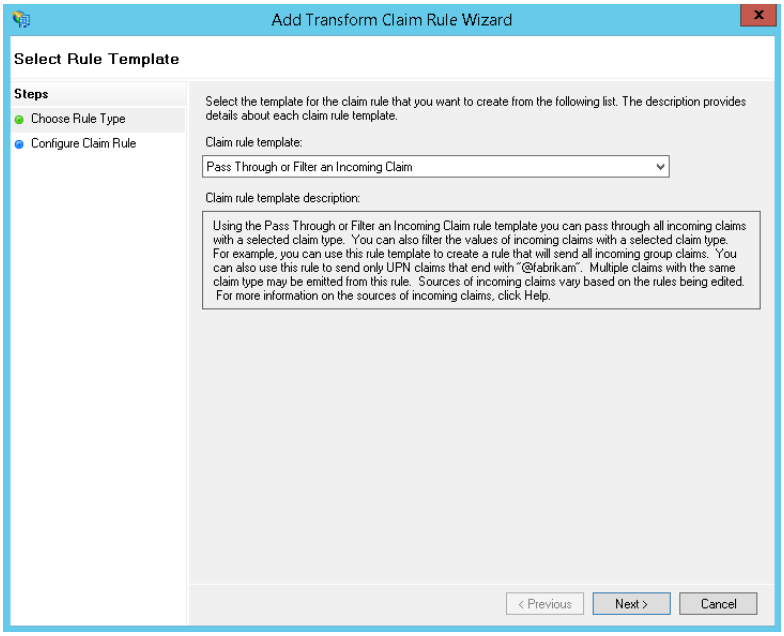

9. Cửa sổ **Finish**, chọn **Close**.



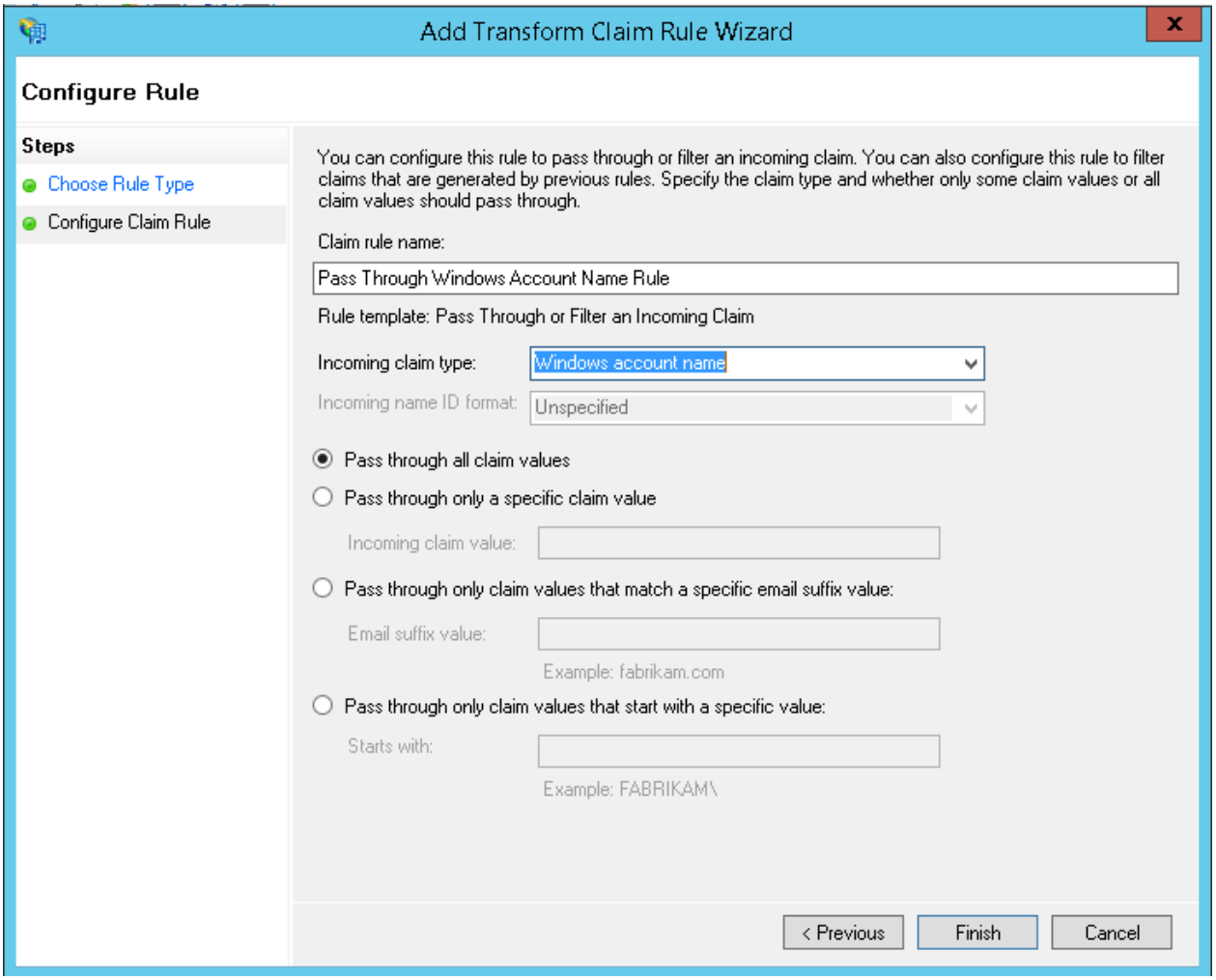
10. Cửa sổ **Edit Claim Rules for Adatum TestApp**, trong tab **Issuance Transform Rules**, chọn **Add Rule**.




11. Bung ô **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.



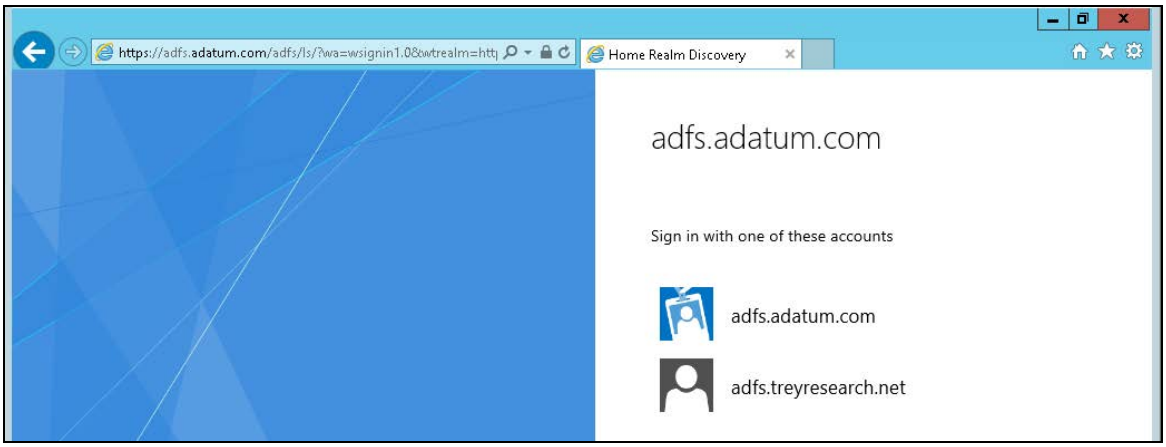
12. Trong ô **Claim rule name**, nhập **Pass Through Windows Account Name Rule**, bung ô **Incoming claim type**, chọn **Windows account name**, chọn **Finish**. chọn **OK**, và tắt cửa sổ **AD FS**.



**Bước 4. Kiểm tra người dùng của Trey Research truy cập ứng dụng của A. Datum.**

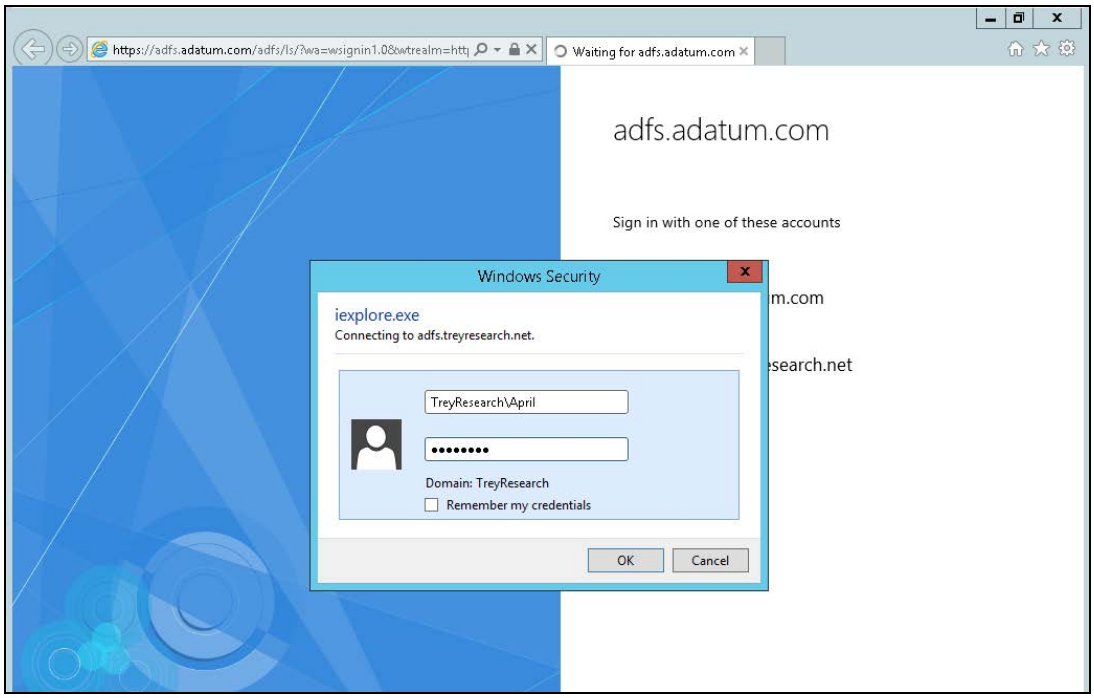
1. Trên máy **TREY-DC1**

2 Mở **Internet Explorer**, truy cập **https://lon-svr3.adatum.com/adatumtestapp/**, chọn **adfs.treyresearch.net**.




3. Hộp thoại chứng thực, nhập **TreyResearch\April** với password **Pa$$w0rd**, chọn **OK**.

Kiểm tra truy cập ứng dụng thành công



4. Tắt **Internet Explorer**.

5. Mở **Internet Explorer**, truy cập **https://lon-svr3.adatum.com/adatumtestapp/**

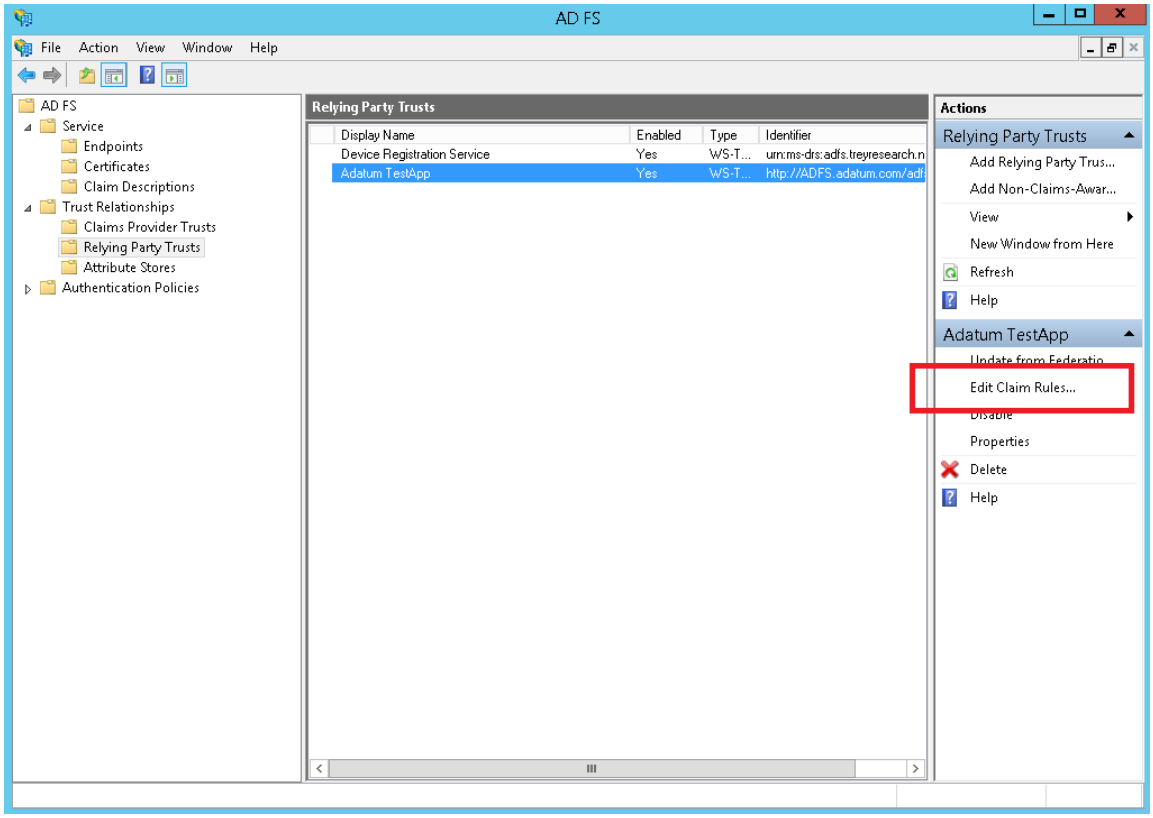
6. Hộp thoại chứng thực, nhập **TreyResearch\April** với password **Pa$$w0rd**, chọn **OK**.

Kiểm tra truy cập ứng dụng thành công.

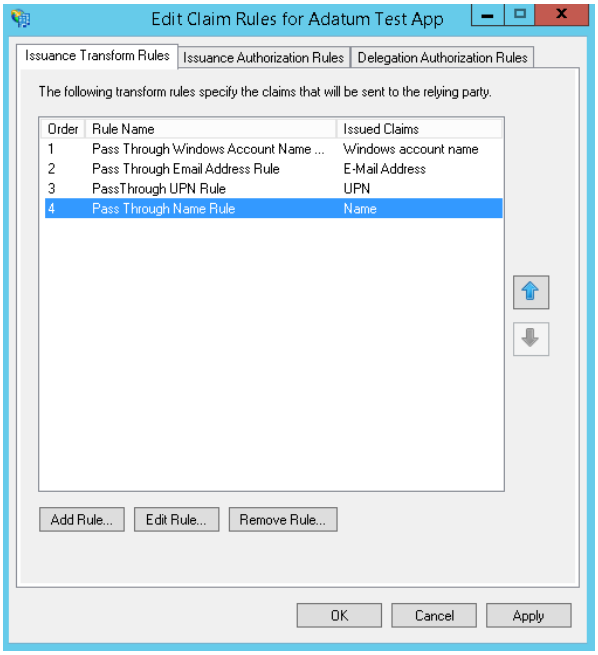
**Chú ý: Từ lần truy cập thứ 2, trong giao diện chứng thực sẽ không thấy 2 lựa chọn adfs.adatum.com và adfs.treyresearch.net . Để thấy được giao diện lựa chọn adfs.adatum.com và adfs.treyresearch.net bạn phải xóa Cookie trong Internet Explorer.**

## Bước 5. Cấu hình Claim rules để cấp quyền truy cập cho một nhóm cụ thể.

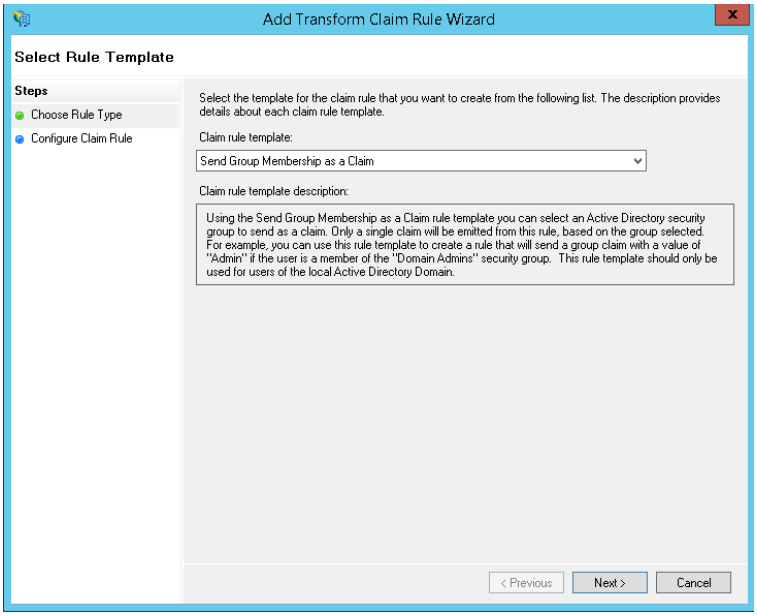
1. Trên máy **TREY-DC1**, mở công cụ **AD FS**, bung **Trust Relationships**, chọn **Relying Party Trusts**, chọn **Adatum TestApp**, trong cửa sổ **Actions**, chọn **Edit Claim Rules**.



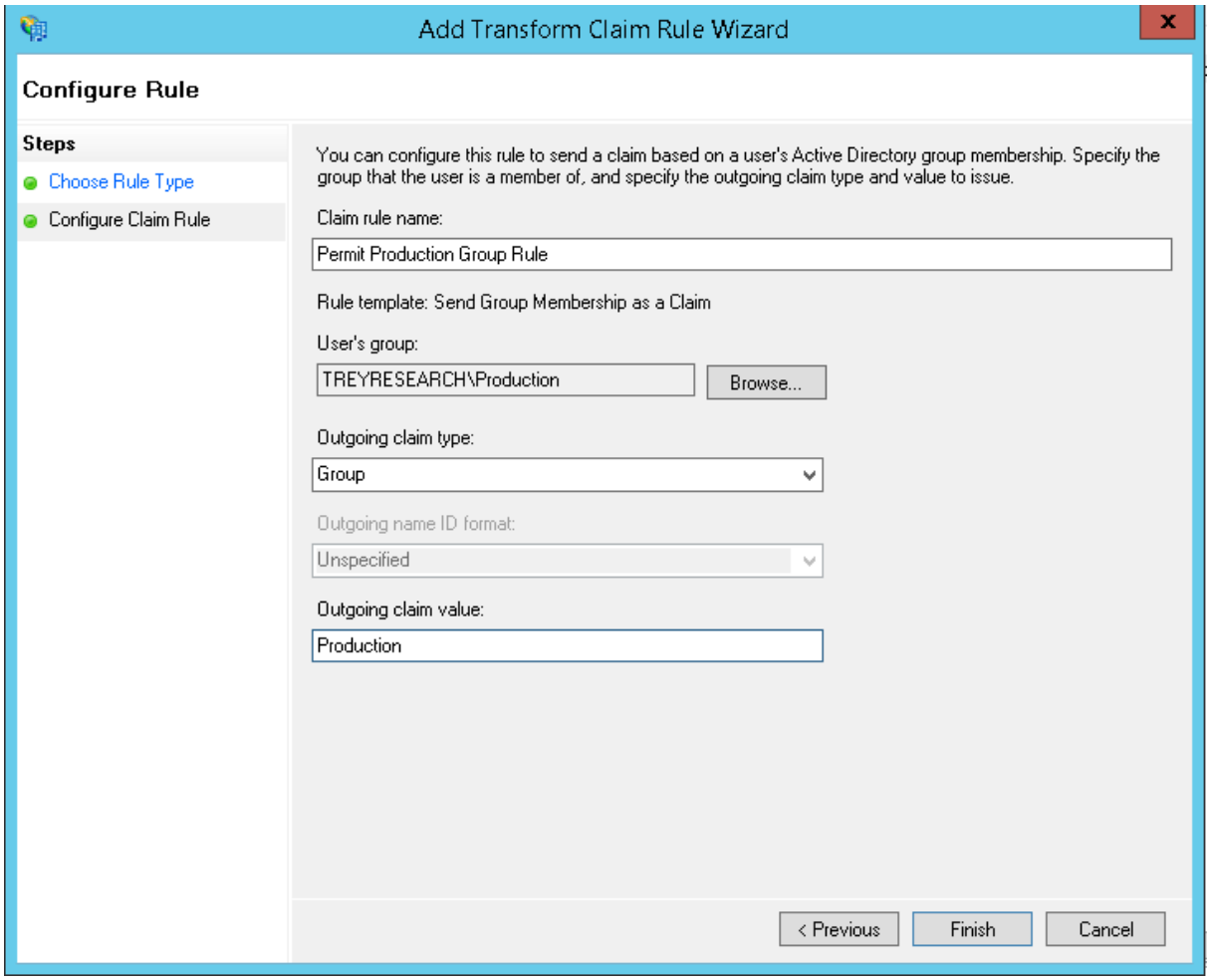
2. Cửa sổ **Edit Claim Rules for Adatum TestApp**, trong tab **Issuance Transform Rules**, chọn **Add Rule**.



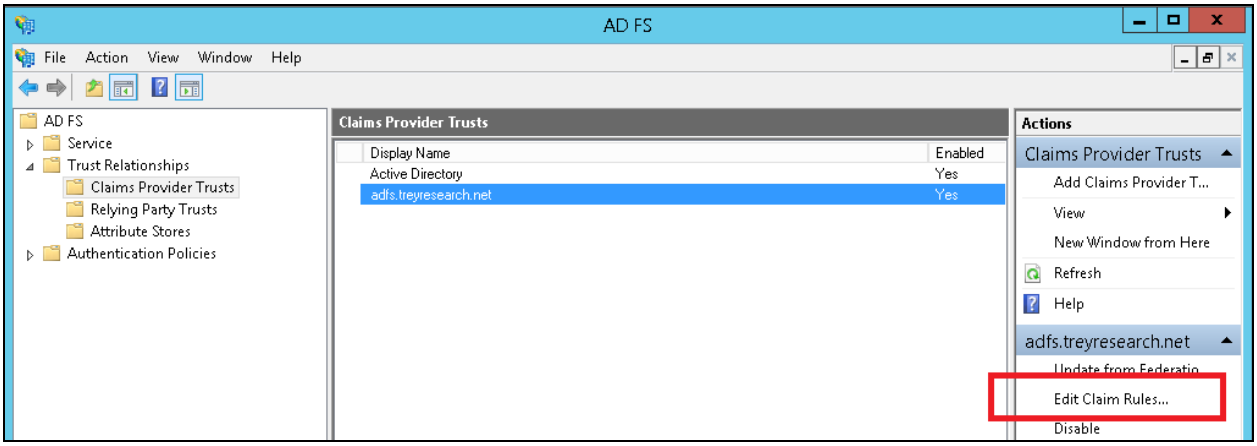

3. Cửa sổ **Select Rule Template**, bung **Claim rule template**, chọn **Send Group Membership as a Claim**, và chọn **Next**.



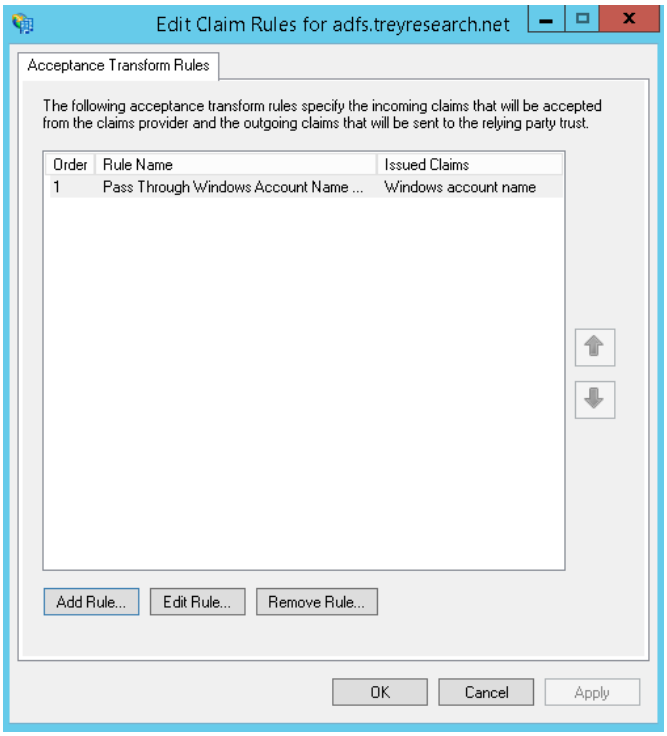
4. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Permit Production Group Rule**. Trong ô **Users group**, chọn **Browse**, nhập **Production**, và chọn **OK**. Bung ô **Outgoing claim type**, chọn **Group**. Trong ô **Outgoing claim value**, nhập **Production**, chọn **Finish**, và chọn **OK**.



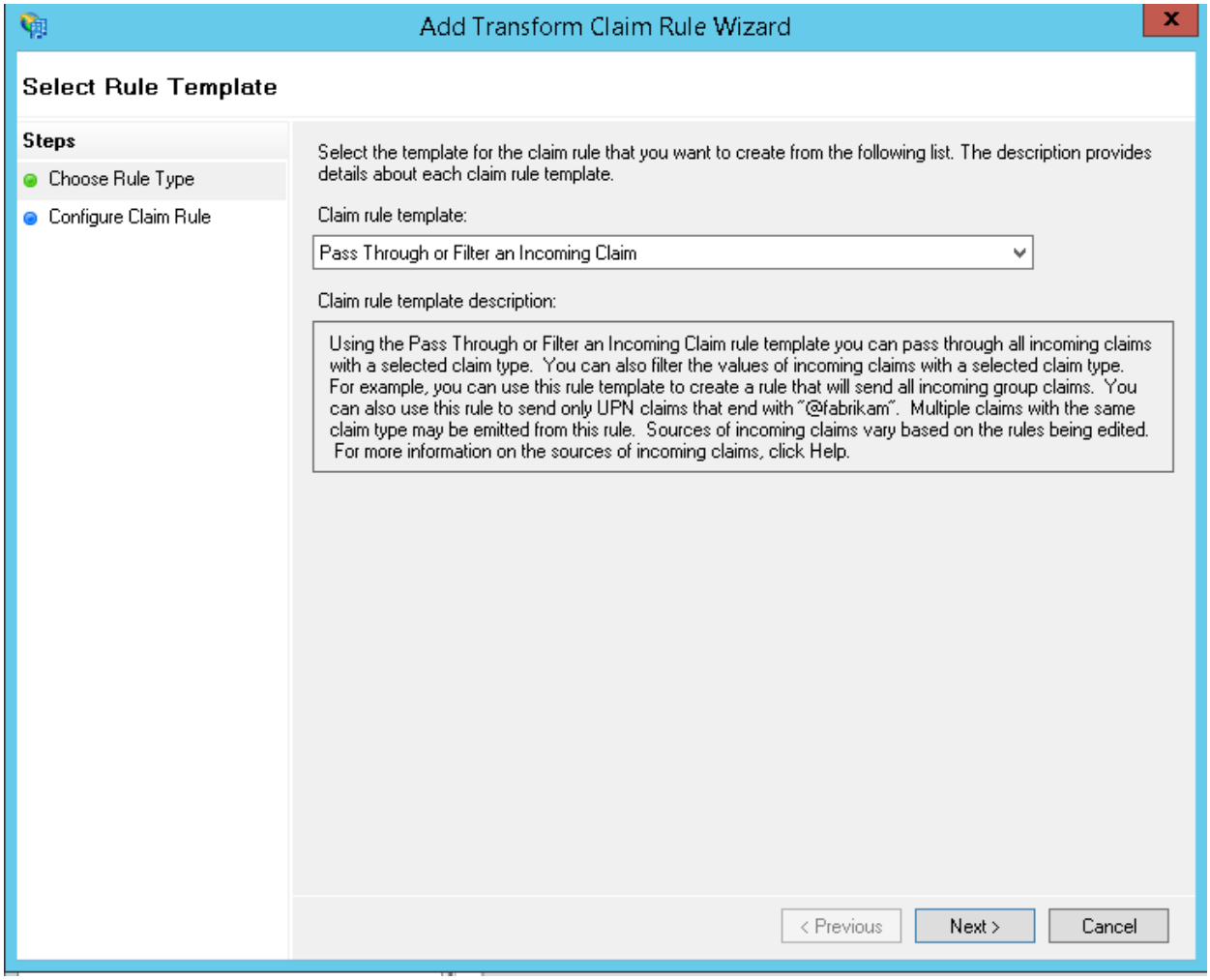
5. Qua máy **LON-DC1**, mở công cụ **AD FS Management**, bung **Trust Relationships**, chọn **Claims Provider Trusts**, chọn **adfs.treyresearch.net**, trong cửa sổ **Actions**, chọn **Edit Claim Rules**.



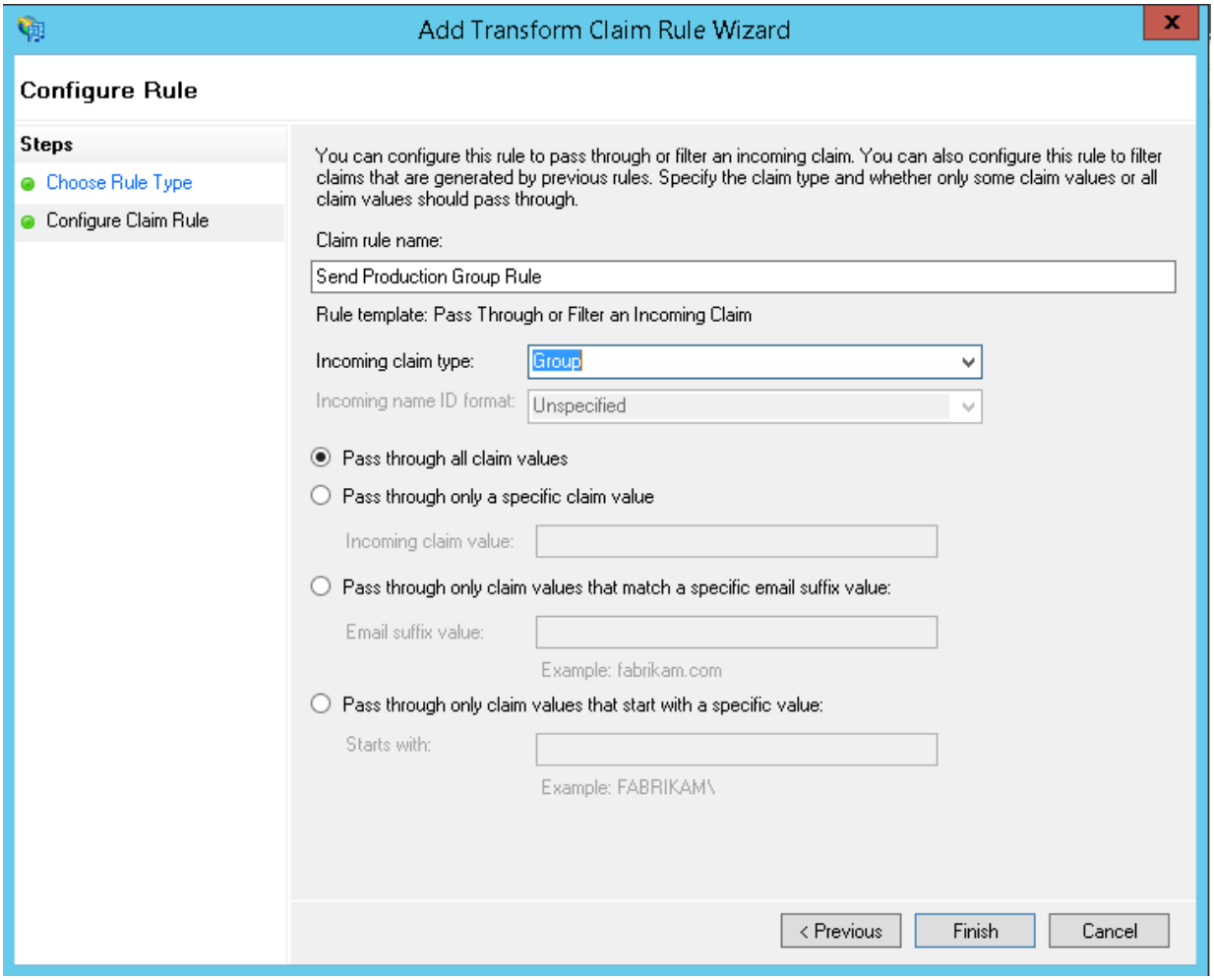

6. Trong tab **Acceptance Transform Rules**, chọn **Add Rule**.



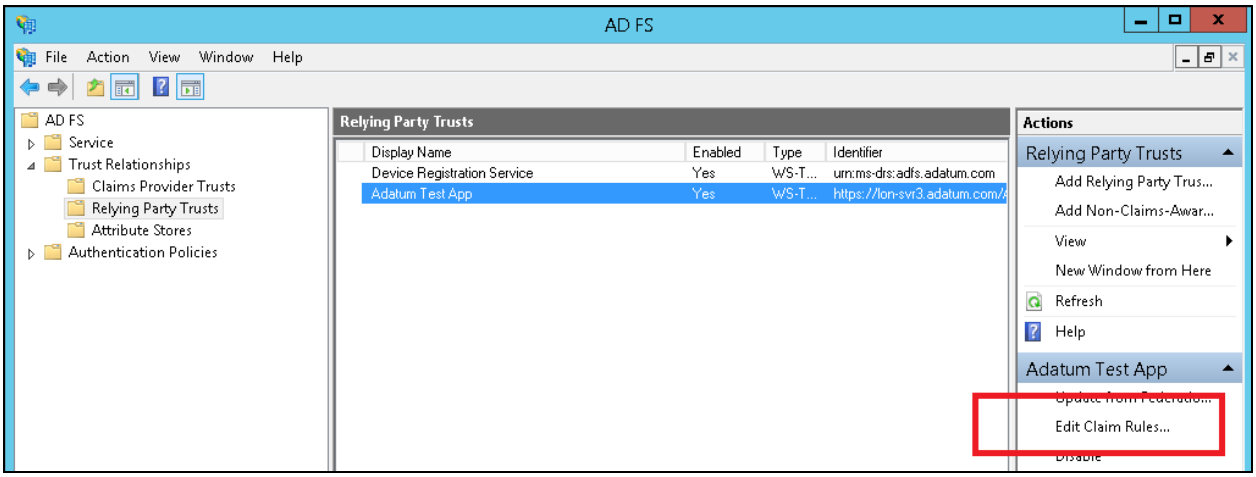
7. Cửa sổ **Select Rule Template**, bung **Claim rule template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.



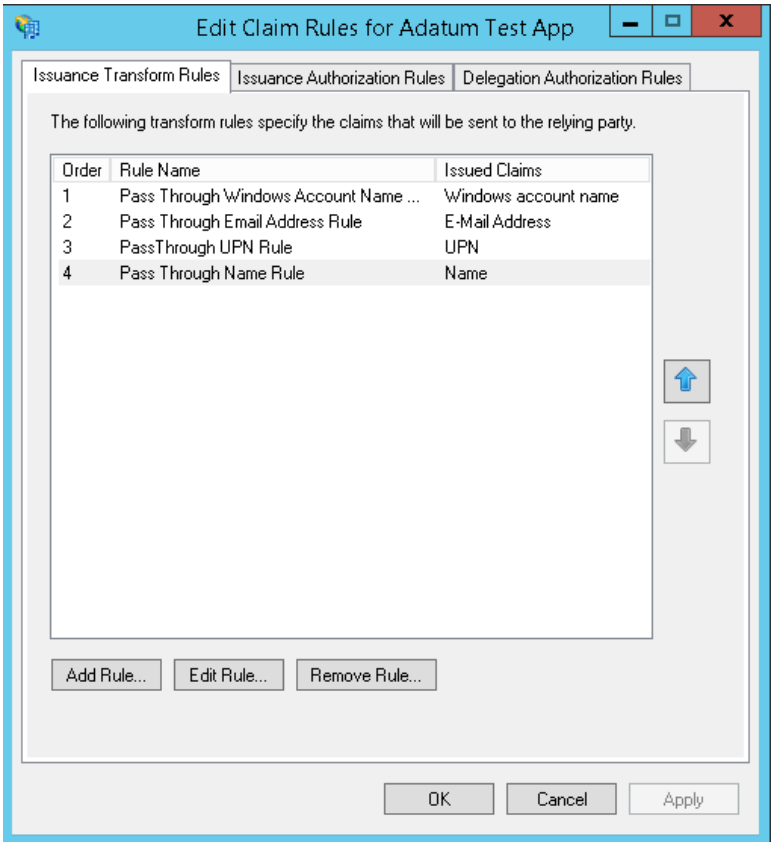
8. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Send Production Group Rule**, bung ô **Incoming claim type**, chọn **Group**, chọn **Finish**, chọn **Yes**, và chọn **OK**.



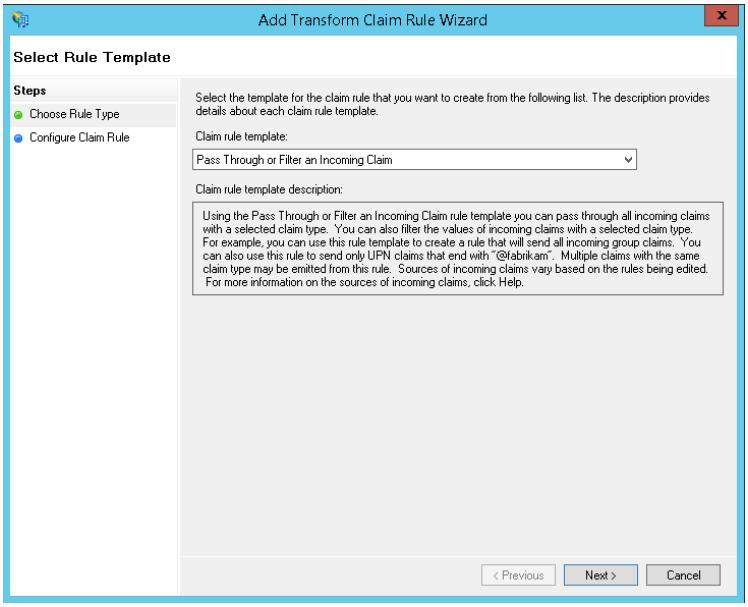
9. Trong cửa sổ **AD FS**, bung **Trust Relationships**, chọn **Relying Party Trusts**, chọn **Adatum Test App**, trong cửa sổ **Actions**, chọn **Edit Claim Rules**.



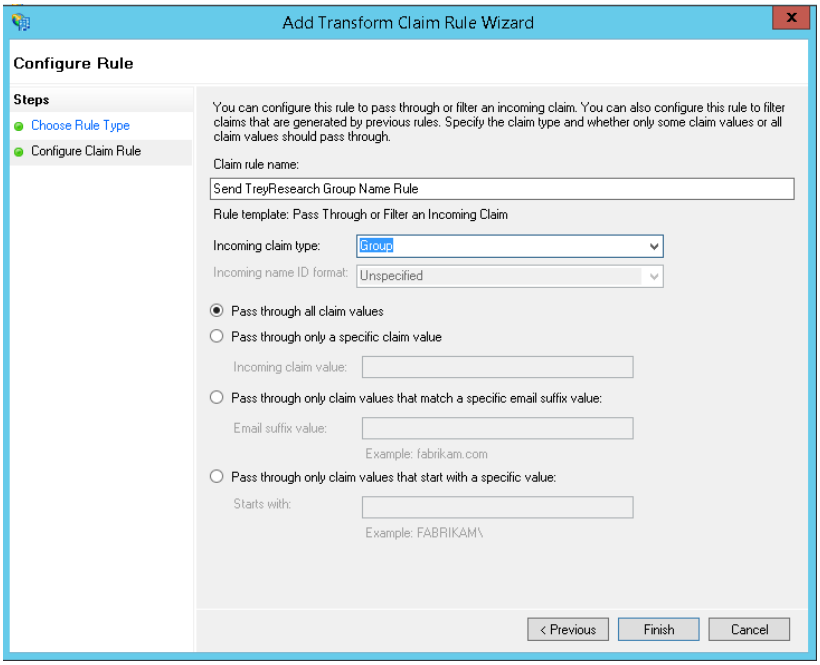

10. Trong tab **Issuance Transform Rules**, chọn **Add Rule**.



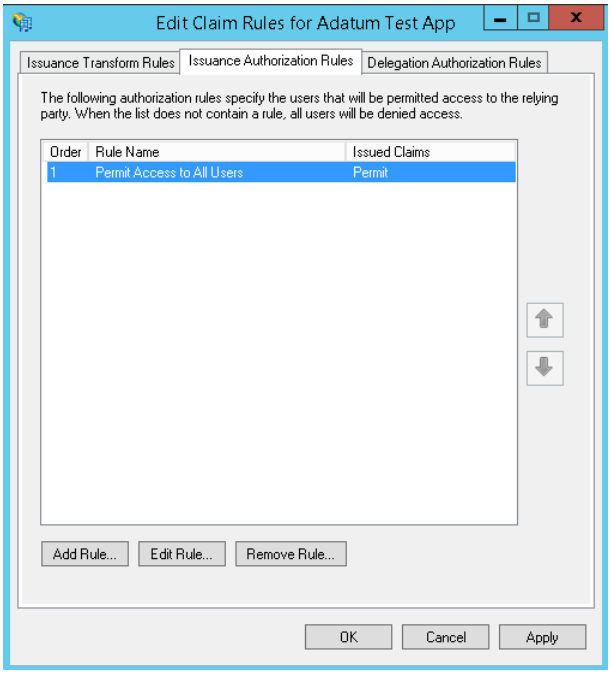
11. Bung **Claim Rule Template**, chọn **Pass Through or Filter an Incoming Claim**, và chọn **Next**.



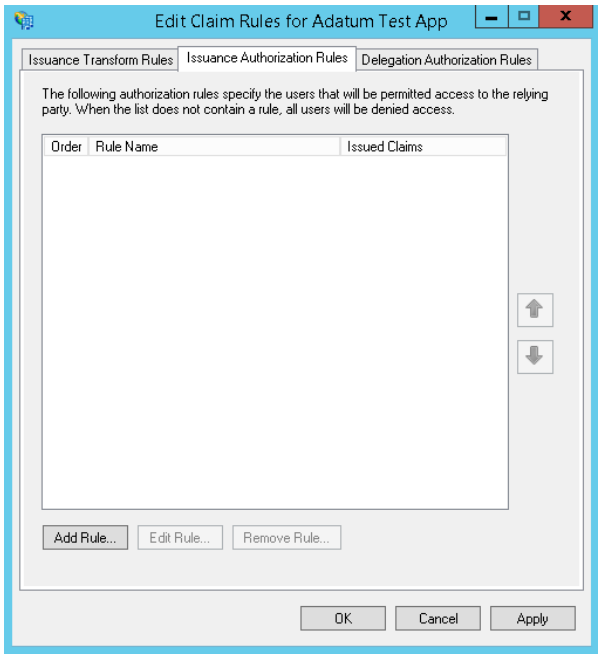

12. Trong ô **Claim rule name**, nhập **Send TreyResearch Group Name Rule**, bung ô **Incoming claim type**, chọn **Group**, và chọn **Finish**.



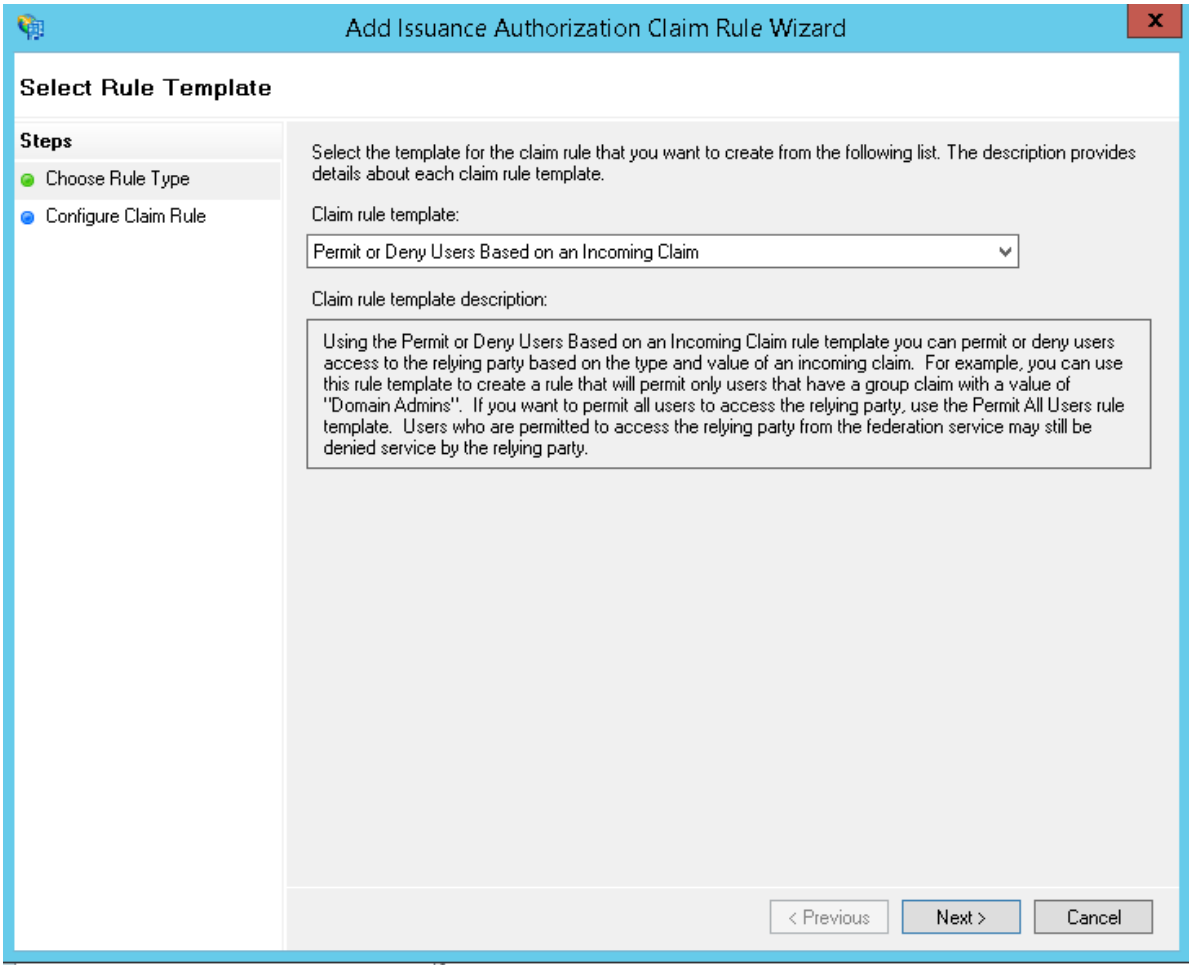
13. Cửa sổ **Edit Claim Rules for Adatum Test App**, qua tab **Issuance Authorization Rules**, chọn rule tên **Permit Access to All Users**, chọn **Remove Rule**. và chọn **Yes**.



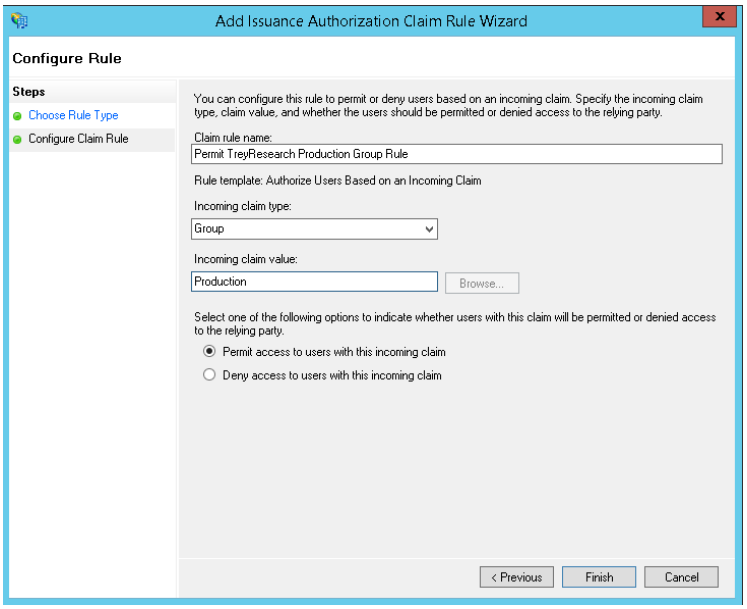

14. Trong tab **Issuance Authorization Rules**, chọn **Add Rule**.



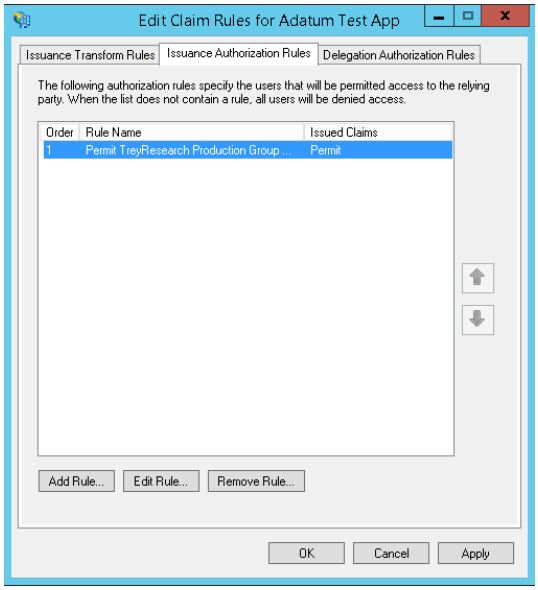
15. Cửa sổ **Select Rule Template**, bung ô **Claim rule template**, chọn **Permit or Deny Users Based on an Incoming Claim**, chọn **Next**.



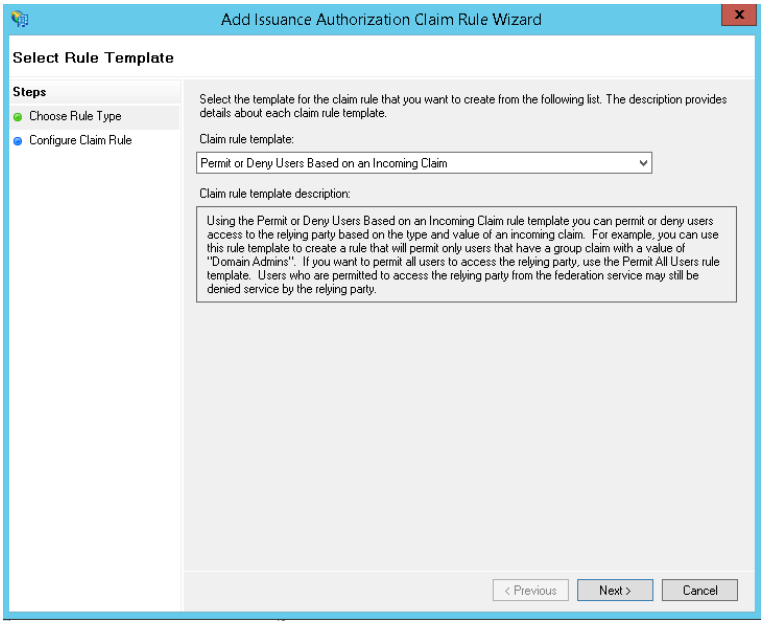
16. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Permit TreyResearch Production Group Rule**, bung ô **Incoming claim type**, chọn **Group**. Trong ô **Incoming claim value**, nhập **Production**, chọn **Permit access to users with this incoming claim**, và chọn **Finish**.



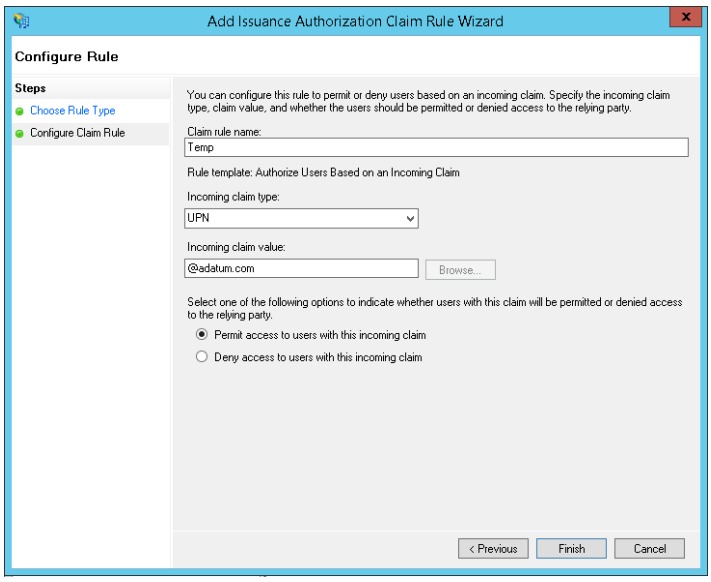

17. Trong tab **Issuance Authorization Rules**, chọn **Add Rule**.



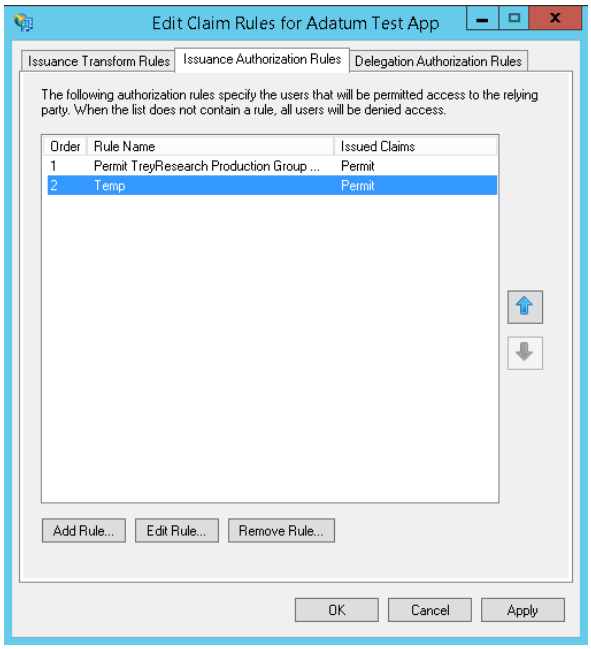
18. Cửa sổ **Select Rule Template**, bung ô **Claim rule template**, chọn **Permit or Deny Users Based on an Incoming Claim**, và chọn **Next**.



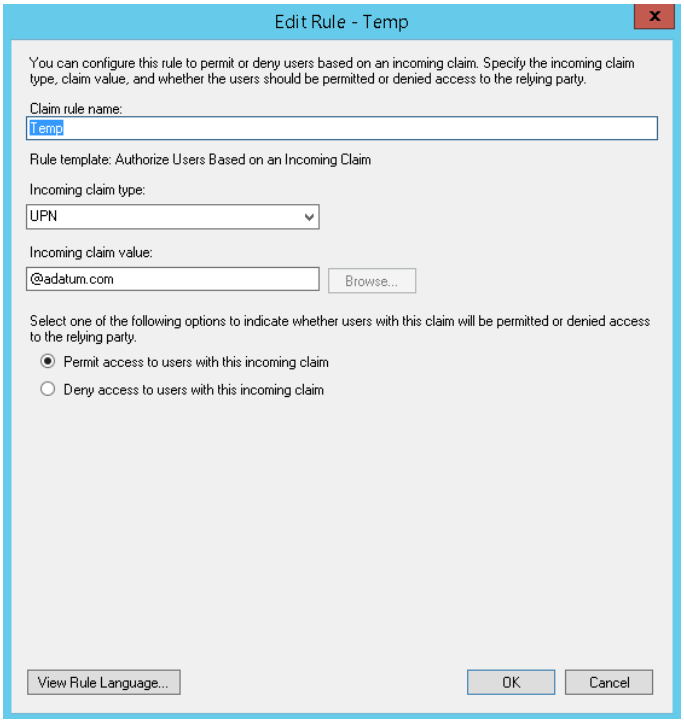

19. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **Temp**, bung ô **Incoming Claim Type**, chọn **UPN**, trong ô **Incoming Claim Value**, nhập **@adatum.com**, chọn **Permit access to users with this incoming claim**, và chọn **Finish**.



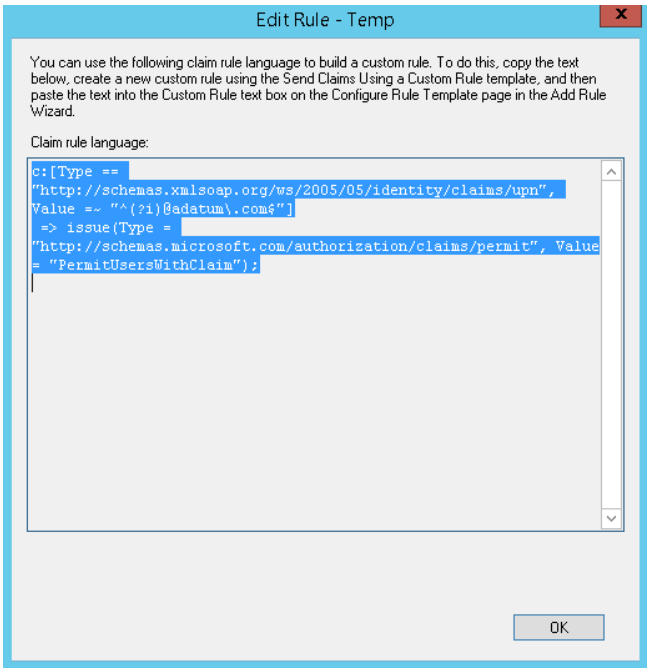
20. Chọn rule tên **Temp**, chọn **Edit Rule**.



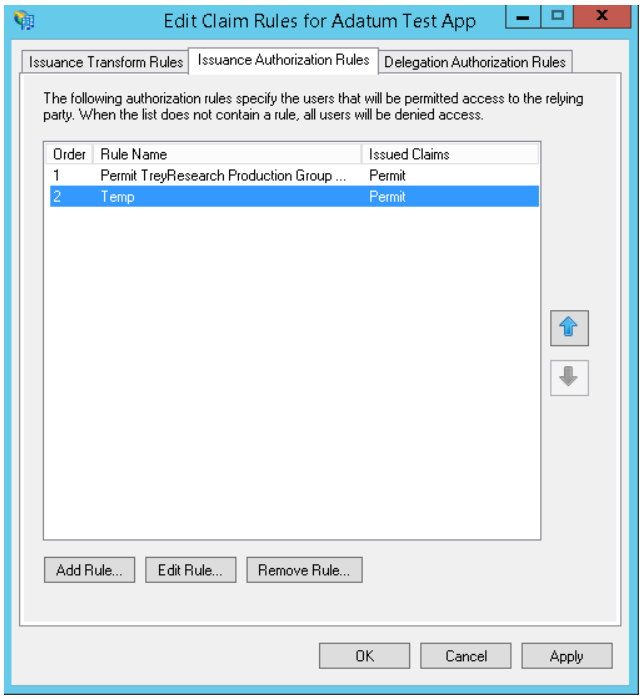

21. Hộp thoại **Edit Rule –Temp**, chọn **View Rule Language**.



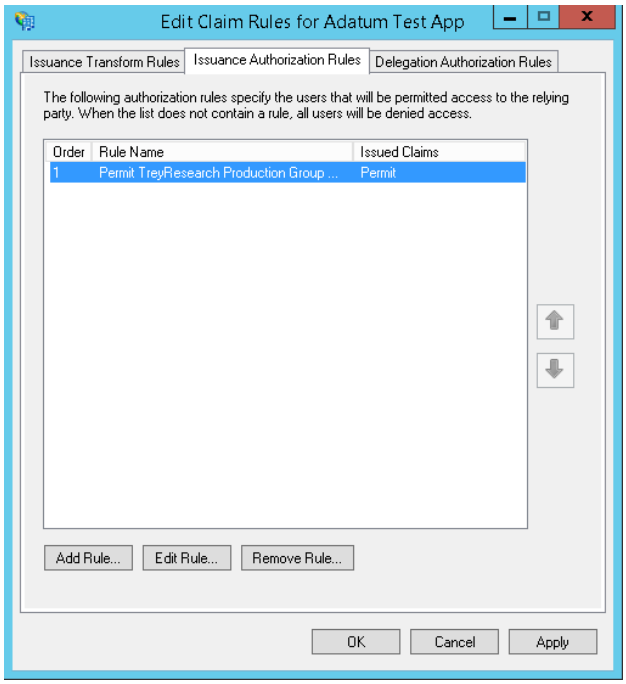
22. Nhấn **Ctrl+C** để copy nội dung, chọn **OK**, chọn **Cancel**.



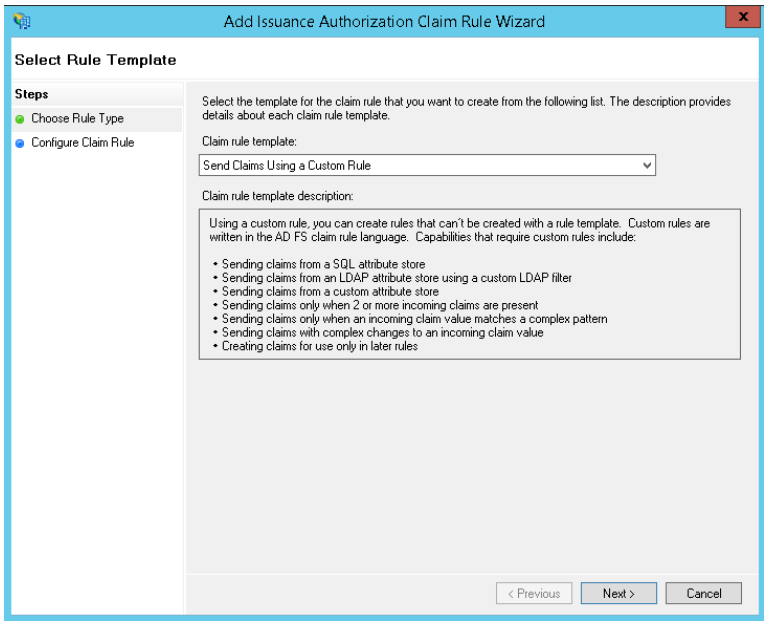

23. Chọn rule tên **Temp**, chọn **Remove Rule**, và chọn **Yes**.



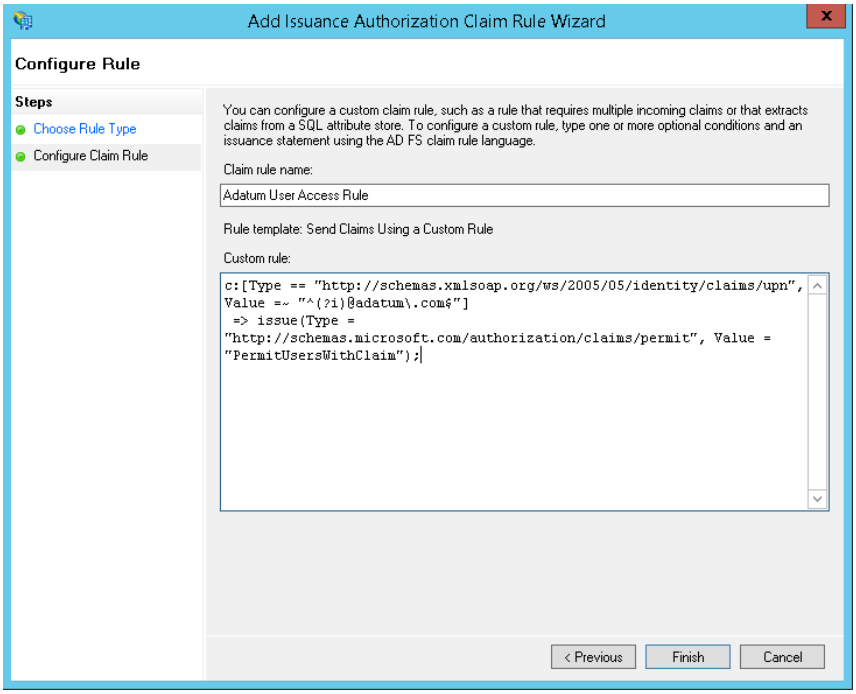
24. Trong tab **Issuance Authorization Rules**, chọn **Add Rule**.




25. Cửa sổ **Select Rule Template**, bung **Claim rule template**, chọn **Send Claims Using a Custom Rule**, chọn **Next**.



26. Cửa sổ **Configure Rule**, trong ô **Claim rule name**, nhập **ADatum User Access Rule**, trong ô **Custom rule**, nhấn **Crtl+V** để dán nội dụng vào, chọn **Finish**, và chọn **OK**.

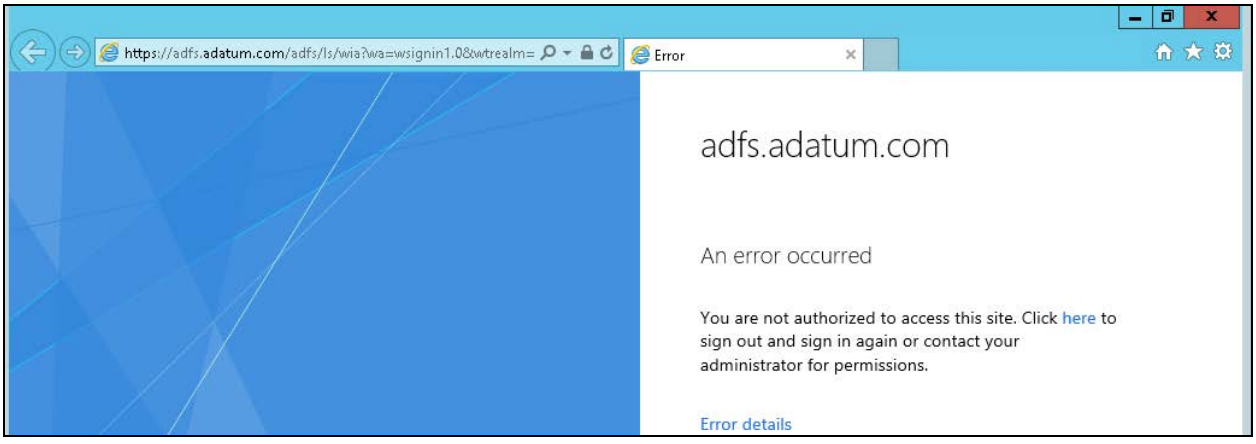



## Bước 6. Kiểm tra truy cập.

1. Trên máy **TREY-DC1**,

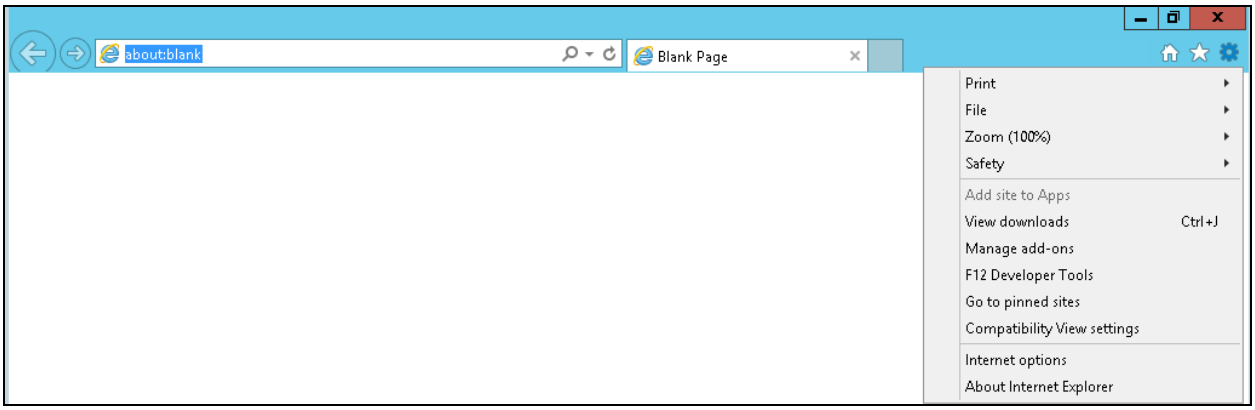
2. Mở **Internet Explorer**, truy cập **https://lon-svr3.adatum.com/adatumtestapp/**.

3. Hộp thoại chứng thực, nhập **TreyResearch\April** với password **Pa$$w0rd**, chọn **OK**.

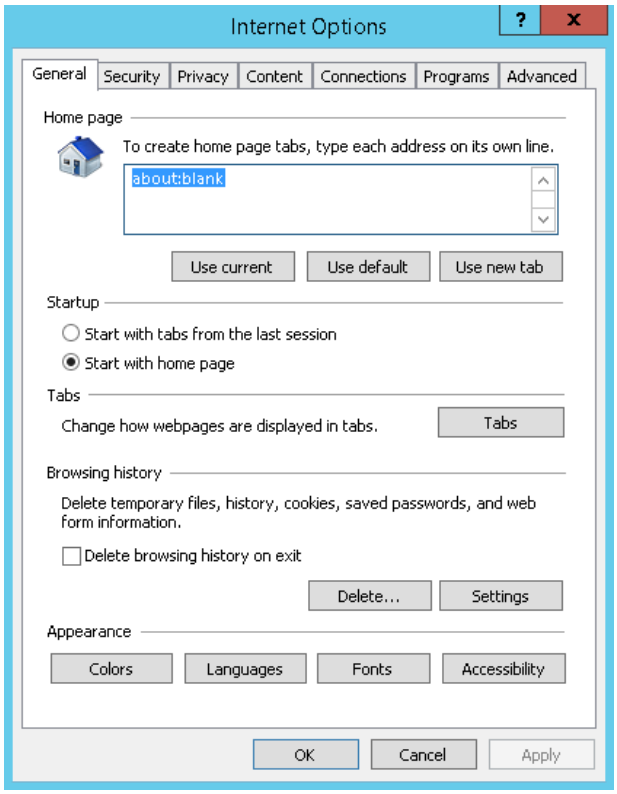


**Chú ý: April không phải là thành viên của nhóm Production nên không có quyền truy cập ứng dụng.**

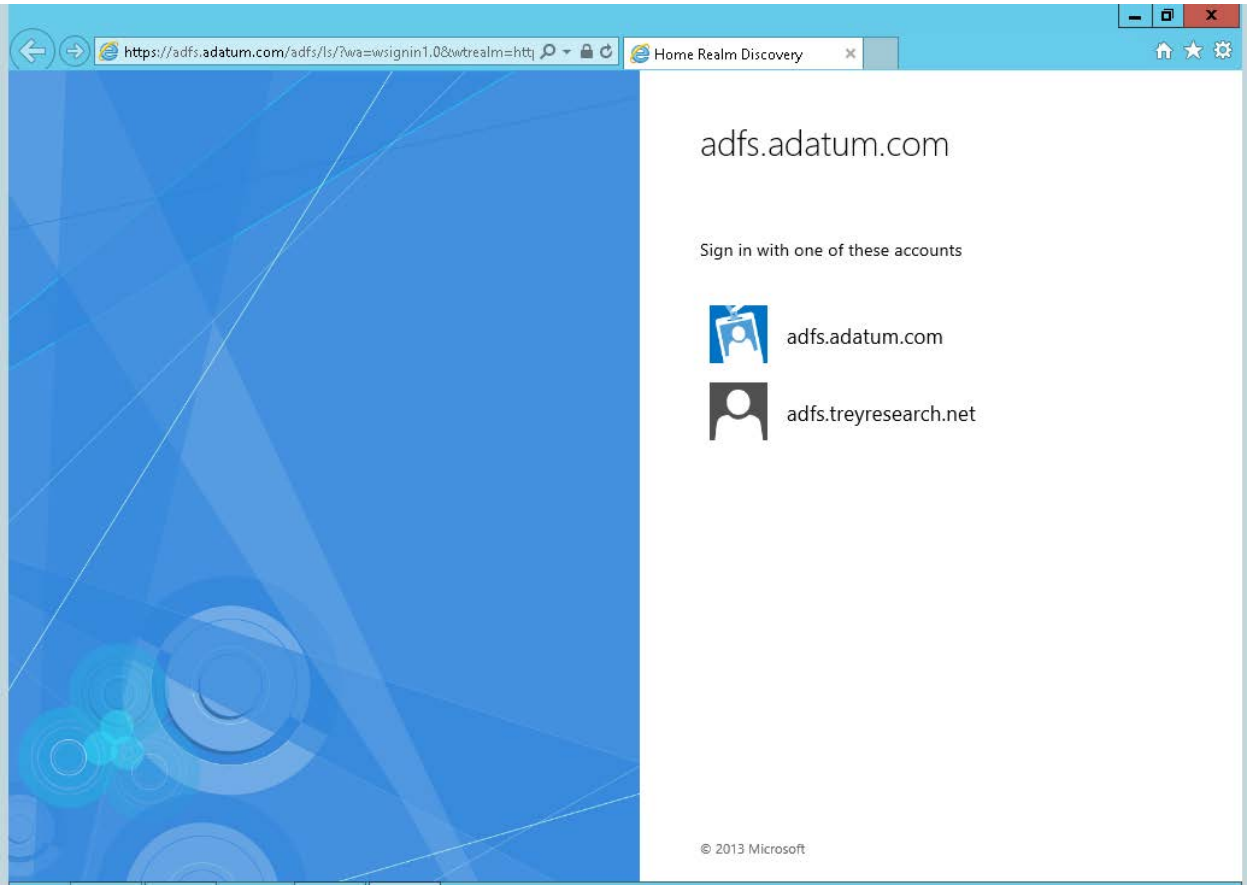
4. Tắt và mở lại **Internet Explorer**. bung biểu tượng **Settings**, chọn **Internet Options**.




5. Trong phần **Browsing History**, chọn **Delete** 2 lần, và chọn **OK**.



6. Truy cập **https://lon-svr3.adatum.com/adatumtestapp/**, chọn **adfs.treyresearch.net**.




7. Hộp thoại chứng thực, nhập **TreyResearch\Morgan** với password **Pa$$w0rd**, chọn **OK**.

**Chú ý: Morgan** là một thành viên của nhóm **Production** nên có quyền truy cập ứng dụng.

**Kết quả: Trong bài tập này, bạn đã cấu hình AD FS cho phép người dùng của Trey Research truy cập ứng dụng web của A. datum thành công**

## Bài tập 4: Triển khai Web Application Proxy.

Trong bài tập này, để hỗ trợ người dùng truy cập khi làm việc tại nhà và đáp ứng yêu cầu an ninh ngăn chặn truy cập trực tiếp đến AD FS Server của bạn từ Internet, bạn cần phải triển khai và cấu hình một Federation Proxy Server.

❖ **Bài tập bao gồm các bước:**

1. Cấu hình Certificates cho Web Application Proxy server.
2. Cài đặt Web Application Proxy role.
3. Cấu hình truy cập vào trang web nội bộ.
4. Kiểm tra quyền truy cập vào các trang web nội bộ từ máy client.

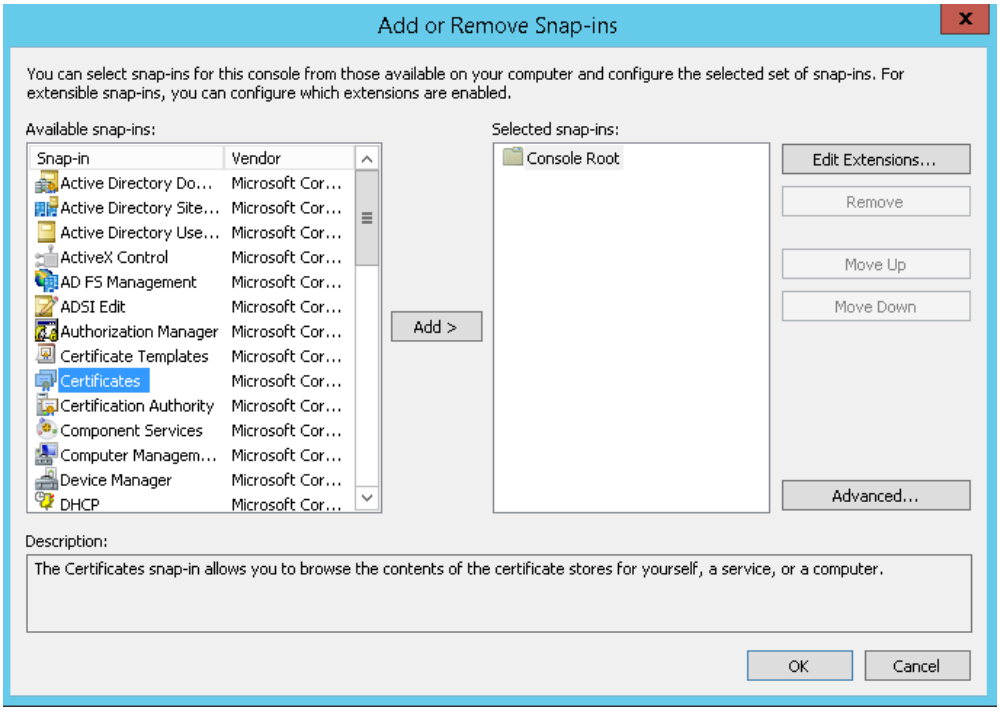
❖ **Thực hiện:**

### Bước 1: Cấu hình Certificates cho Web Application Proxy server.

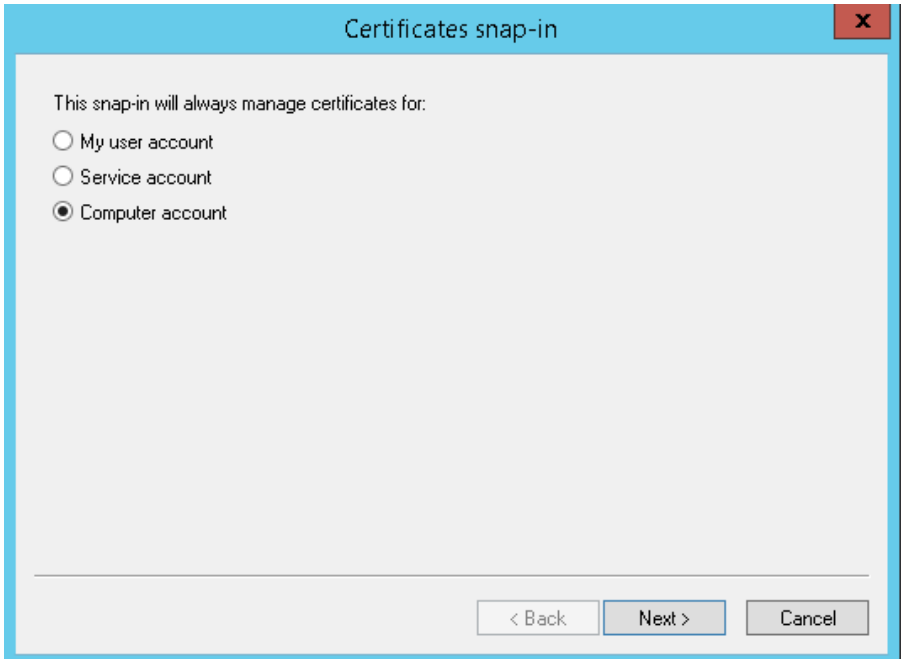
1. Trên máy **LON-DC1**.

2. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.

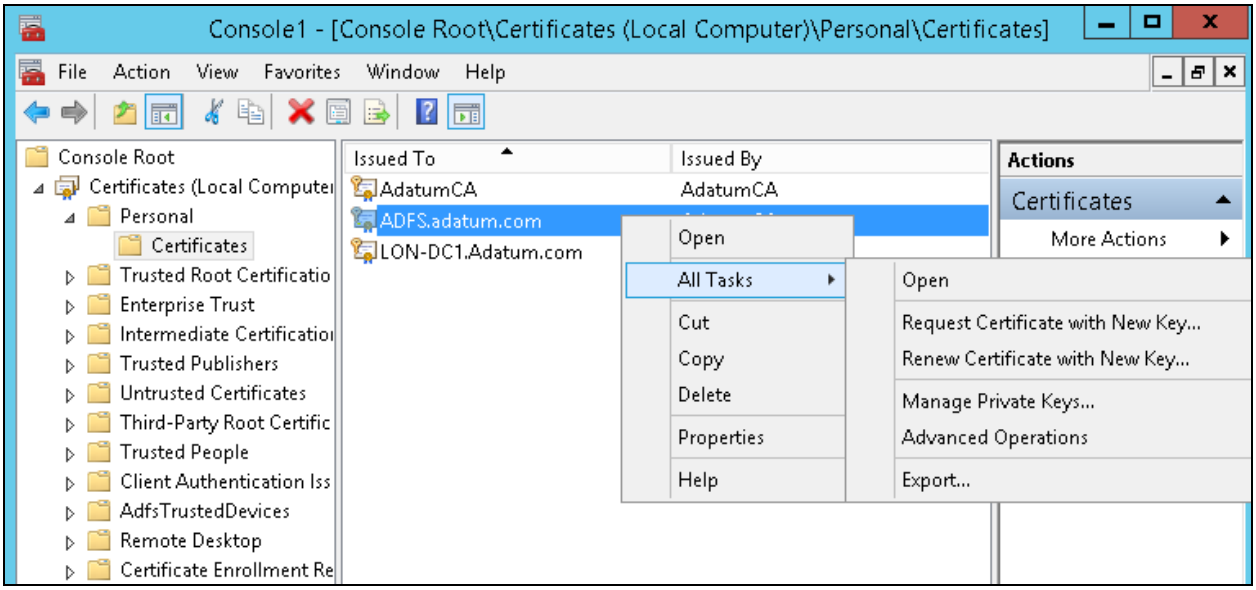
3. Trong cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add**.



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)**, bung **Personal**, chọn **Certificates**, chuột phải certificate **adfs.adatum.com**, bung **All Tasks**, chọn **Export**.

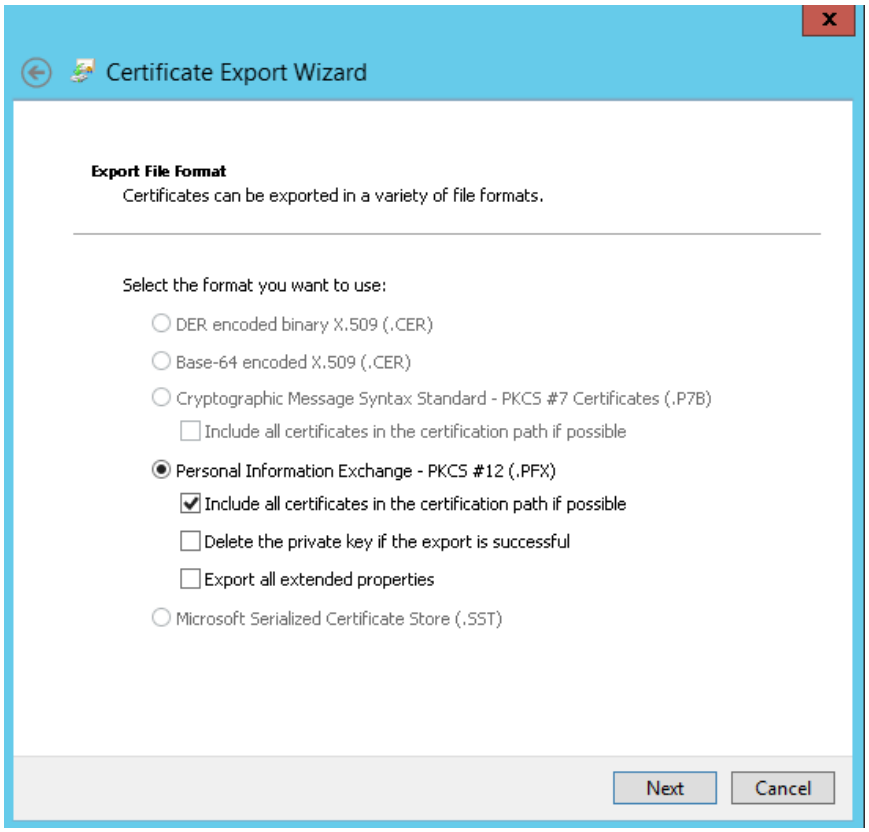


6. Cửa sổ **Welcome**, chọn **Next**.

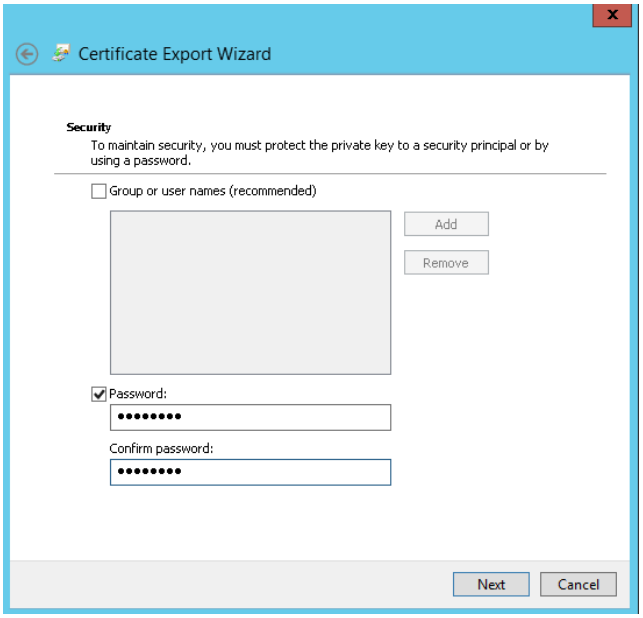
7. Cửa sổ **Export Private Key**, chọn **Yes, export the private key**, và chọn **Next**.



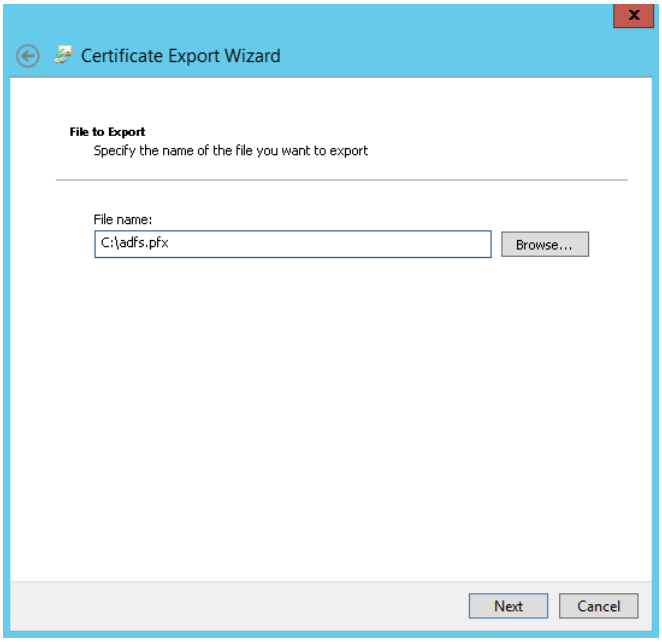

8. Cửa sổ **Export File Format**, chọn **Next**.



9. Cửa sổ **Security**, đánh dấu chọn **Password**. Nhập **Pa$$w0rd** vào ô **Password** và **Confirm password**, chọn **Next**.

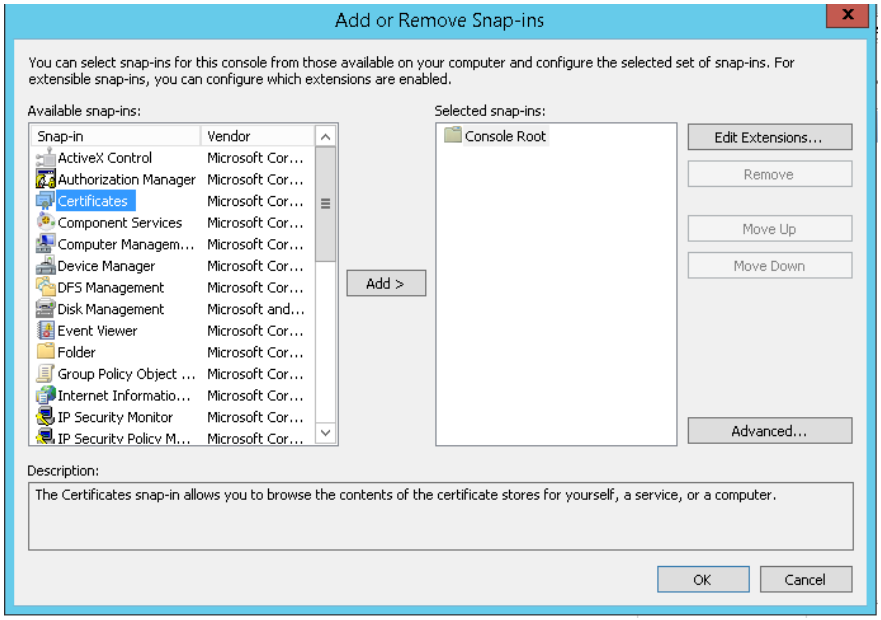



10. Cửa sổ **File to Export**, trong ô **File name**, nhập **C:\adfs.pfx**, chọn **Next**, chọn **Finish**, và chọn **OK**. Tắt cửa sổ **MMC**, không cần Save.

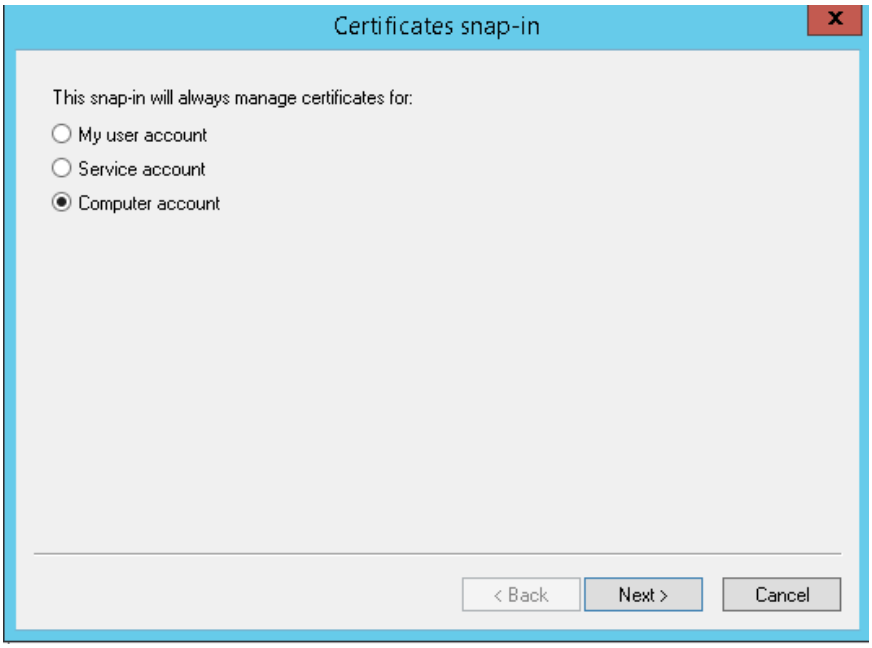


11. Qua máy **LON-SVR2**, mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.

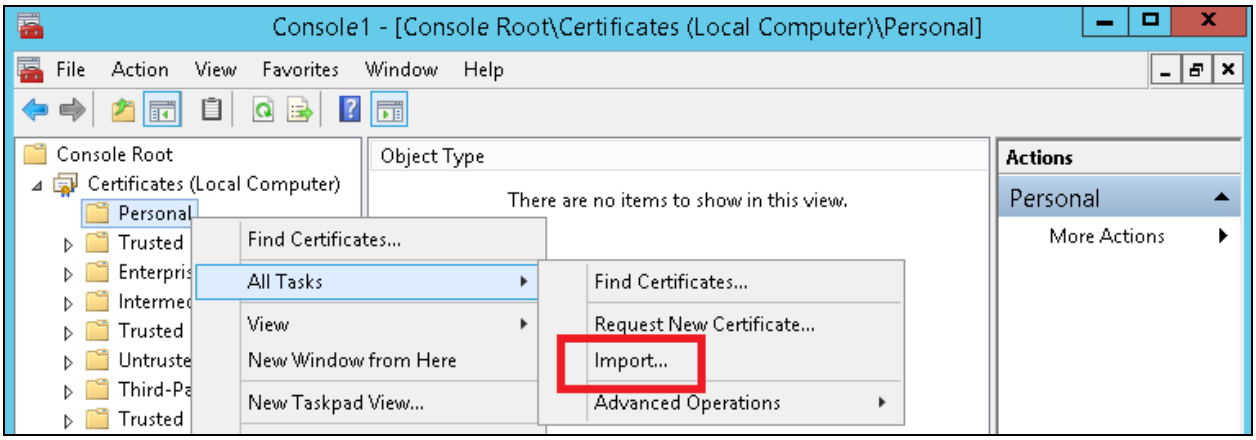
12. Cửa sổ **Add or Remove Snap-ins** chọn **Certificates,** chọn **Add**.




13. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next,** chọn **Finish**, và chọn **OK**.

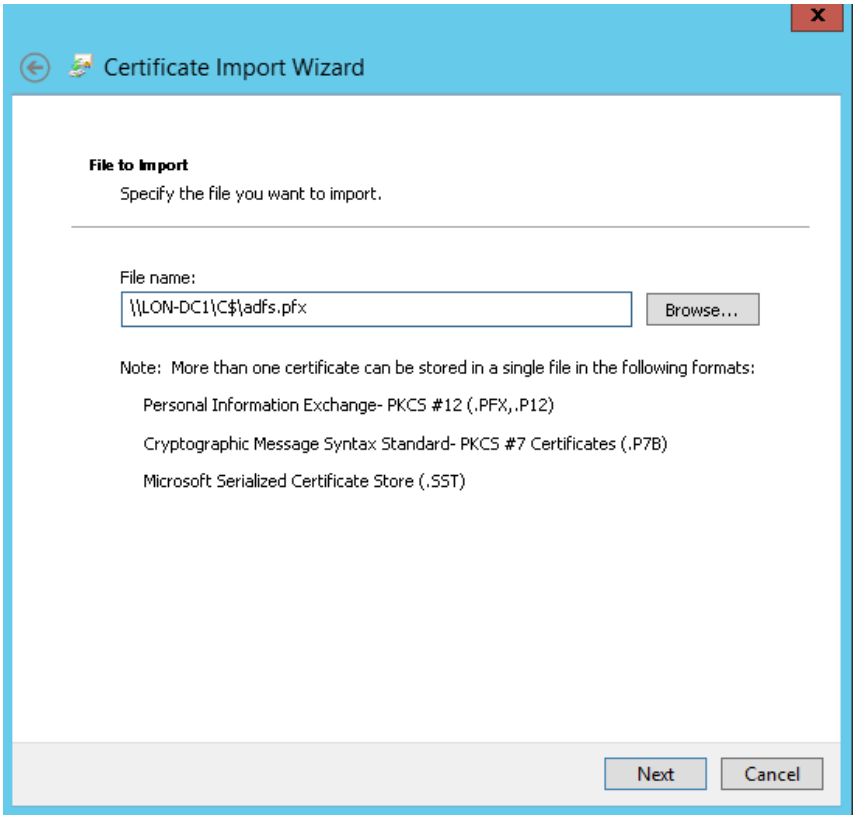


14. Trong cửa sổ **Console1**, bung **Certificates (Local Computer)**, chọn và chuột phải **Personal**, bung **All Tasks**, chọn **Import**.

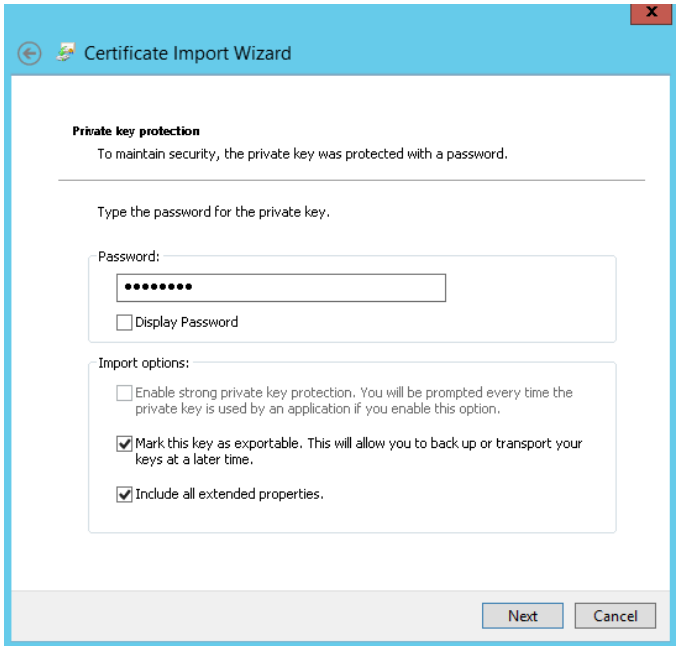



15. Cửa sổ **Welcome**, chọn **Next**.

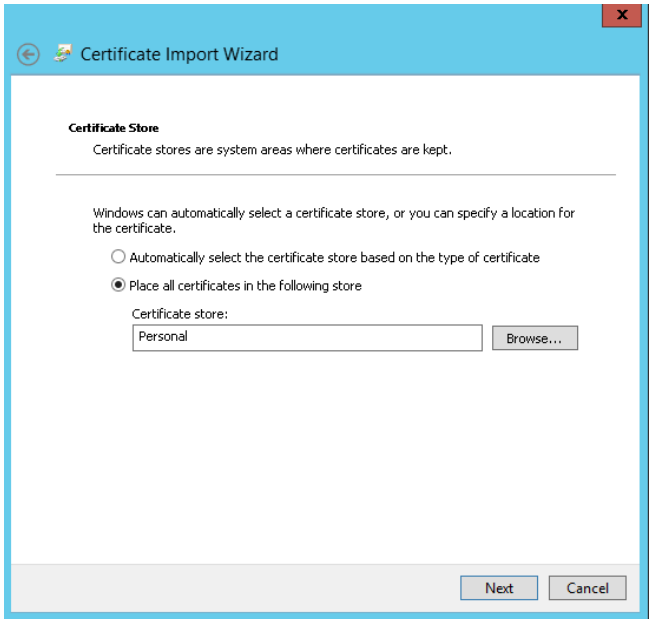
16. Cửa sổ **File to Import**, trong ô **File name**, nhập **\\LON-DC1\c$\adfs.pfx**, chọn **Next**.



17. Cửa sổ **Private key protection**, trong ô **Password**, nhập **Pa$$w0rd**. Đánh dấu chọn **Mark this key as exportable**, chọn **Next**.



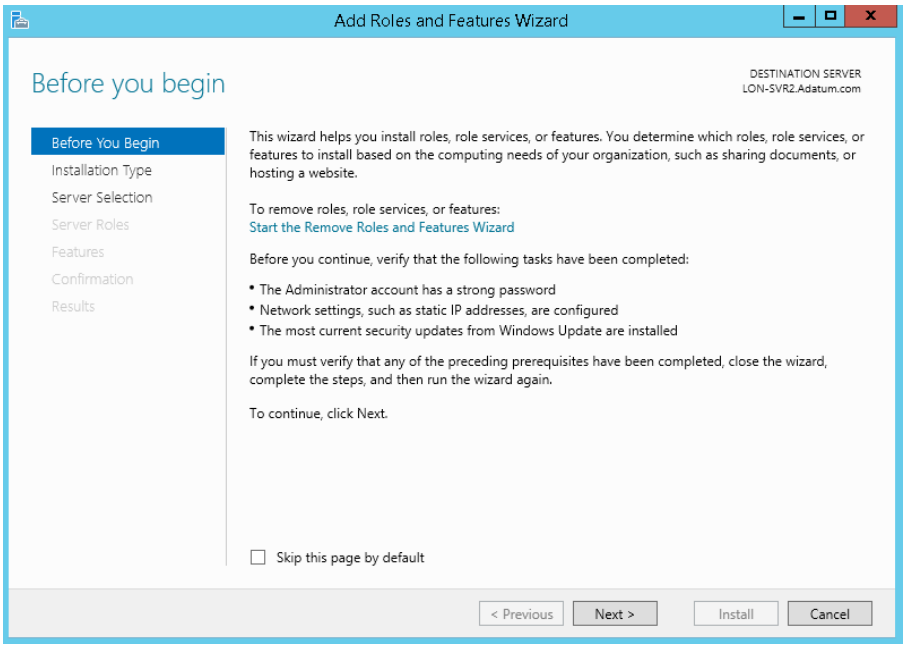

18. Cửa sổ **Certificate Store**, chọn **Next**, chọn **Finish**, và chọn **OK**. Tắt cửa sổ **MMC**, không cần save.



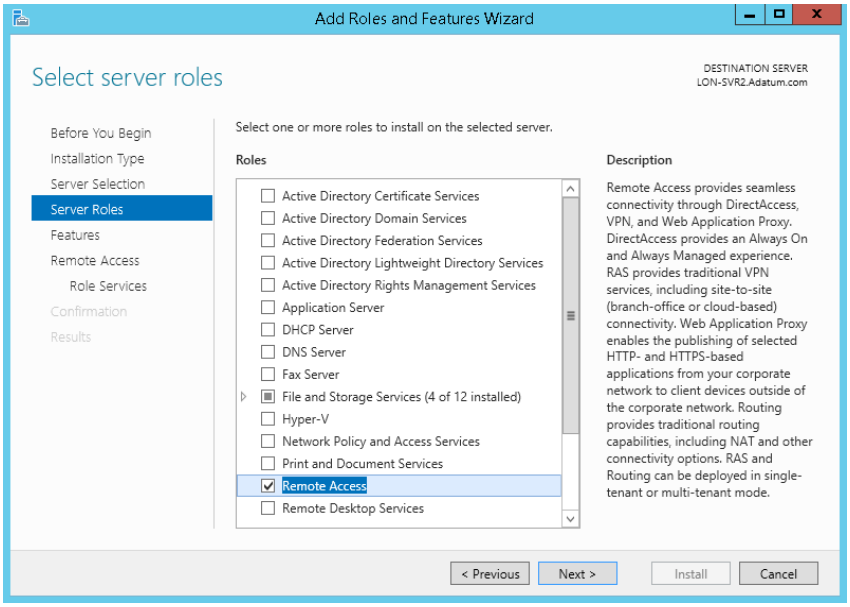
## Bước 2: Cài đặt Web Application Proxy role.

1. Trên máy **LON-SVR2**, trong **Server Manager**, chọn **Add Roles and Features**.

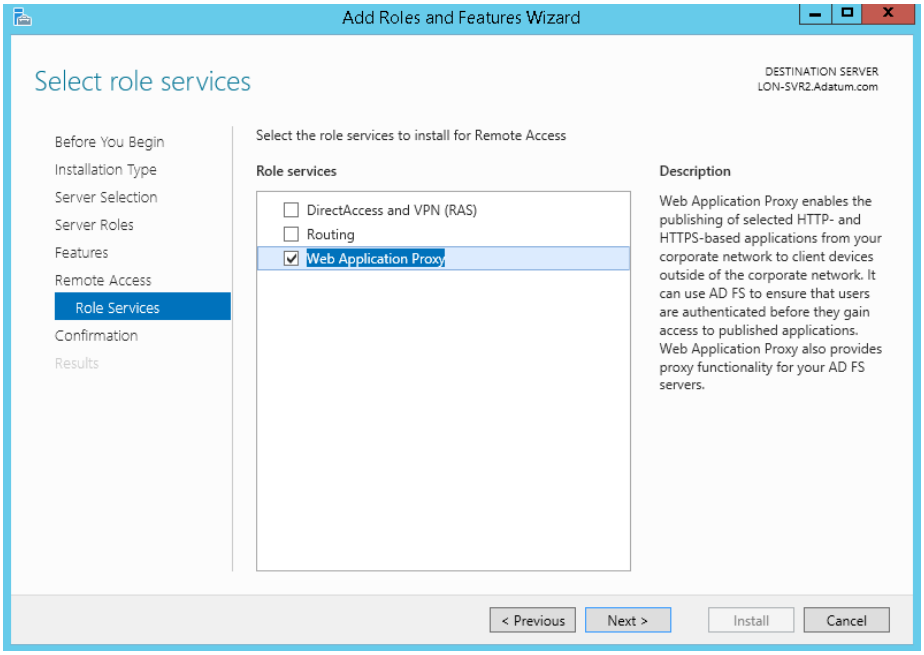
2. Cửa sổ **Before you begin**, chọn **Next** 3 lần.




3. Cửa sổ **Select server roles**, đánh dấu chọn **Remote Access**, chọn **Next** 3 lần.



4. Cửa sổ **Select role services**, đánh dấu chọn **Web Application Proxy**, chọn **Add Features**, và chọn **Next**.

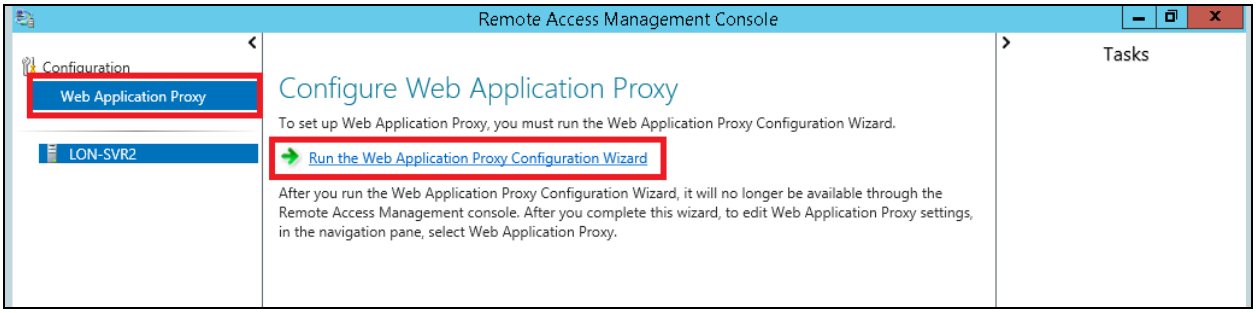



5. Cửa sổ **Confirm installation selections** page, click **Install**. Sau khi cài đặt thành công, chọn **Close**.

**Bước 3: Cấu hình truy cập vào trang web nội bộ.**

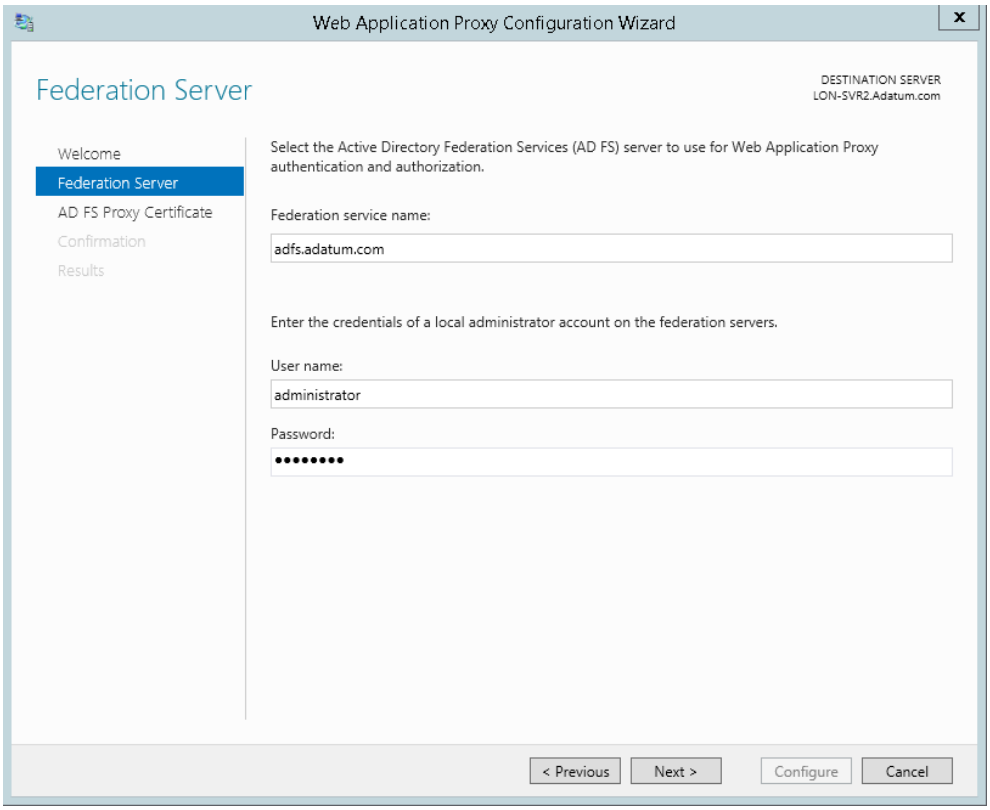
1. Trên máy **LON-SVR2**, trong **Server Manager,** bung menu **Tools**, mở **Remote Access Management**.

2. Trong cửa sổ **Remote Access Management Console**, chọn **Web Application Proxy**, chọn **Run the Web Application Proxy Configuration Wizard**.

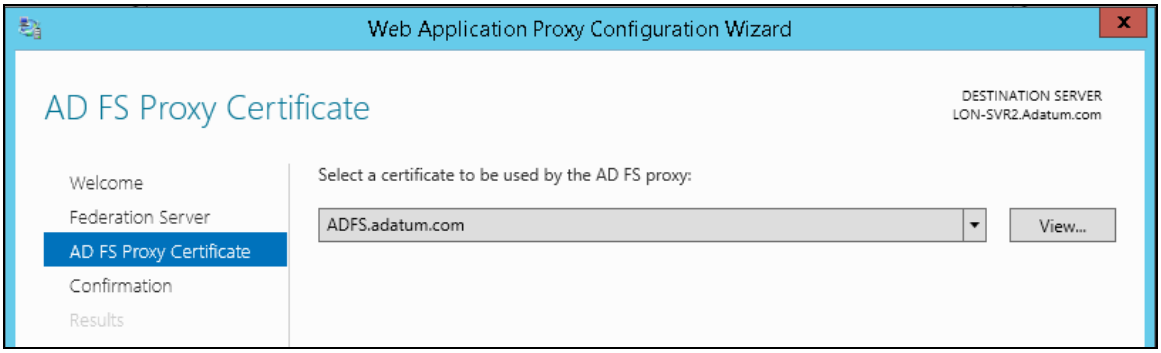


3. Cửa sổ **Welcome**, chọn **Next**.

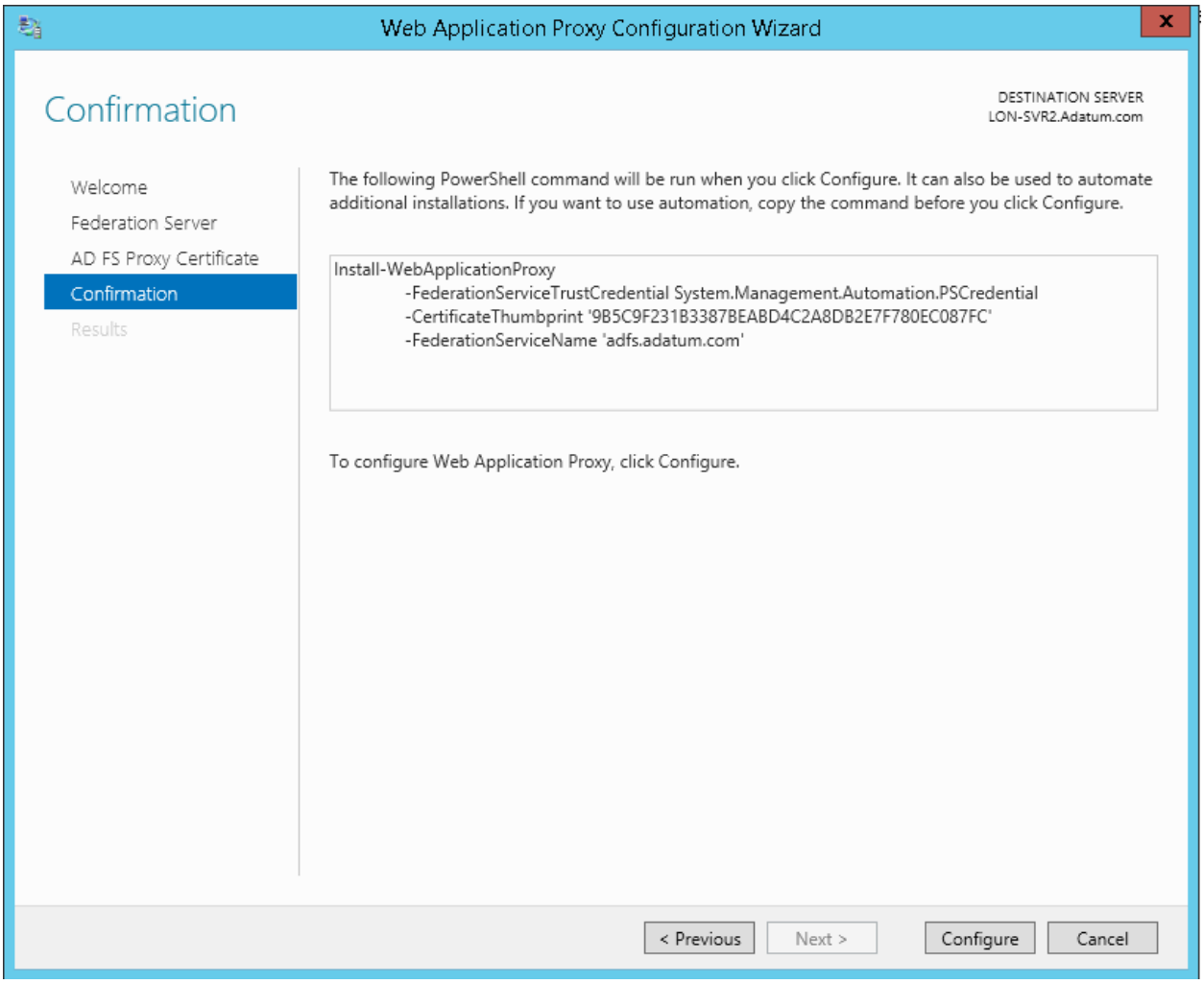
4. Cửa sổ **Federation Server**, trong ô **Federation service name,** nhập **adfs.adatum.com.** Trong ô **User name**, nhập **administrator**, trong ô **Password,** nhập **Pa$$w0rd**, chọn **Next**.



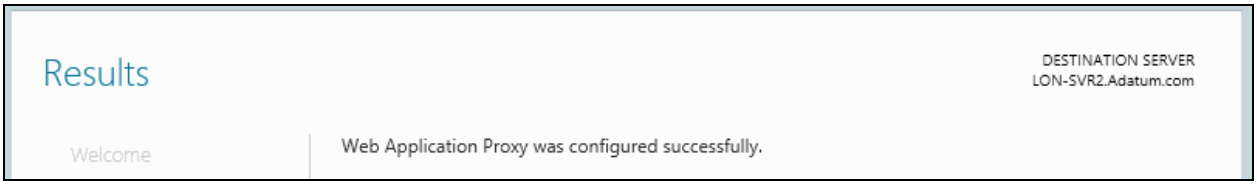

5. Cửa sổ **AD FS Proxy Certificate**, bung ô **Select a certificate to be used by the AD FS proxy**, chọn **adfs.adatum.com**, và chọn **Next**.



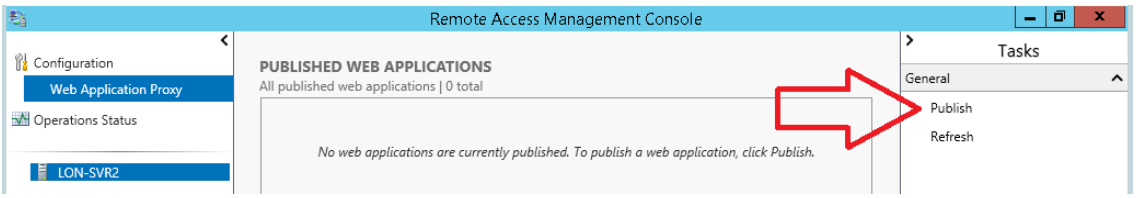
6. Cửa sổ **Confirmation**, chọn **Configure**.




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

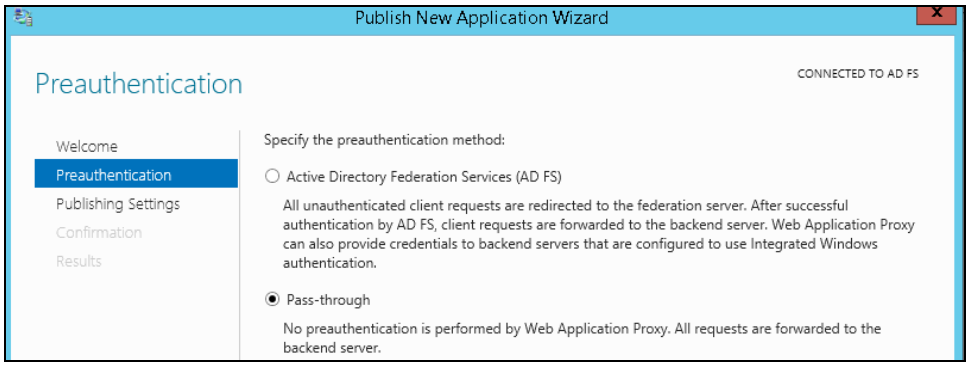


8. Trong cửa sổ **Remote Access Management Console**, chọn **Publish**.

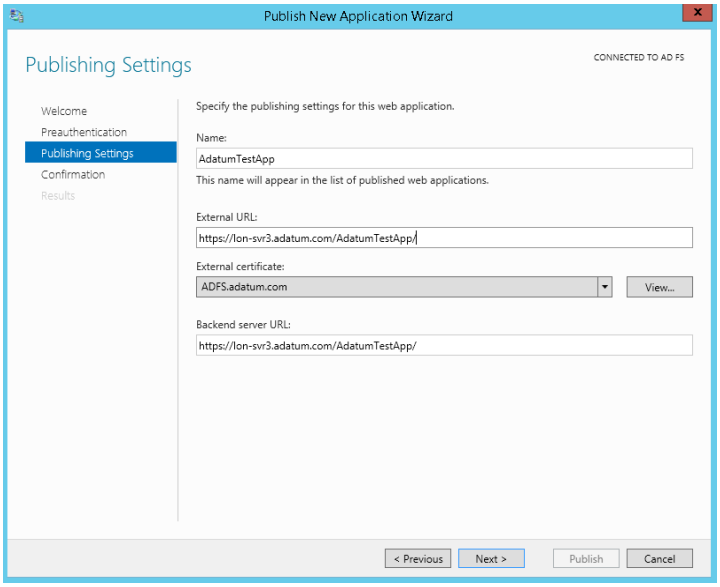



9. Cửa sổ **Welcome**, chọn **Next**.

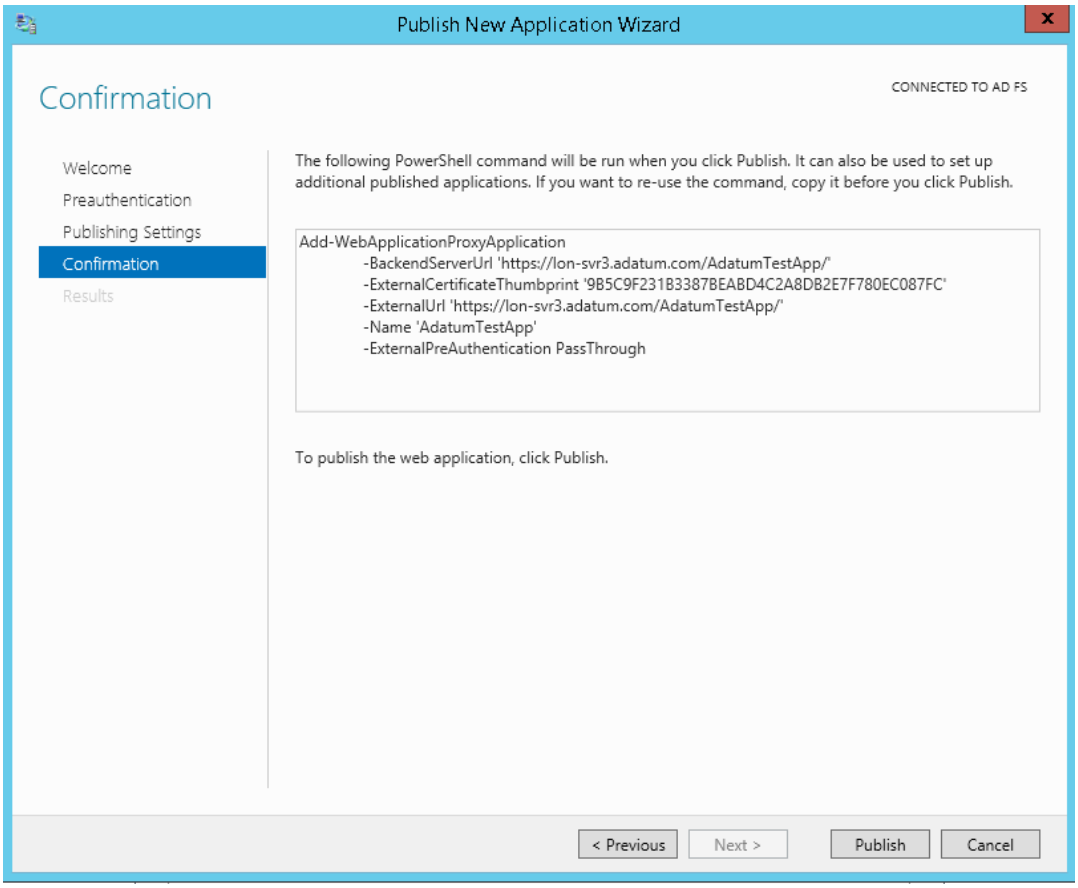
10. Cửa sổ **Preauthentication**, cửa sổ **Pass-through**, chọn **Next**.




11. Cửa sổ **Publishing Settings**, trong ô **Name,** nhập **AdatumTestApp**, trong ô **External URL,** nhập **https://lon-svr3.adatum.com/AdatumTestApp/**, bung ô **External Certificate,** chọn **adfs.adatum.com**, chọn **Next**.



12. Cửa sổ **Confirmation**, chọn **Publish**.



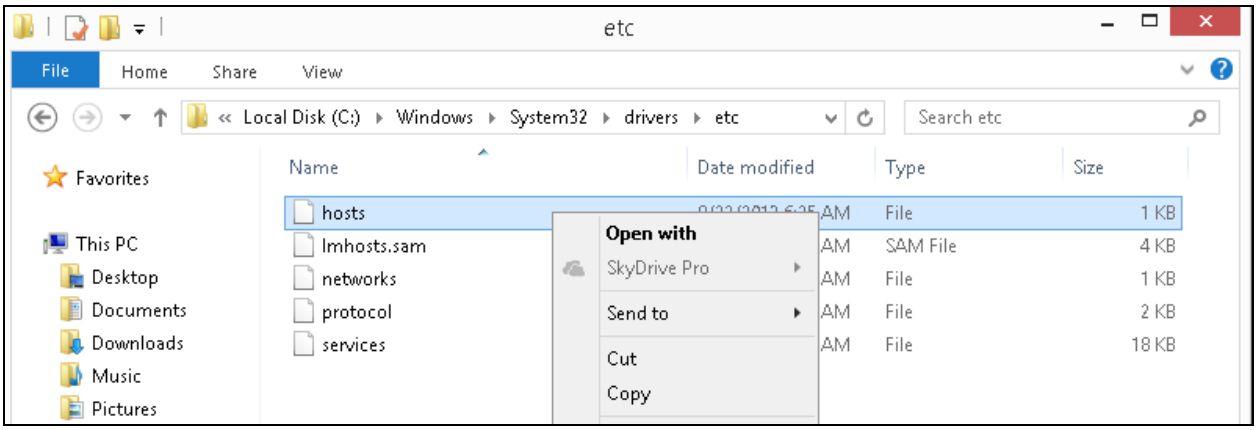

13. Cửa sổ **Results**, chọn **Close**.



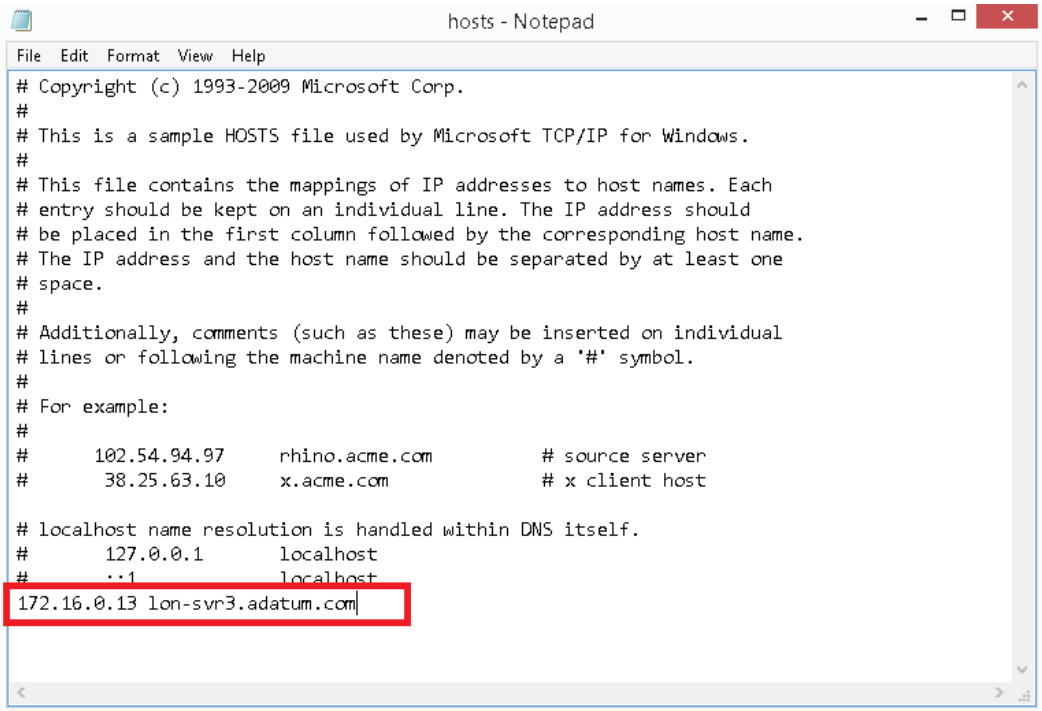
**Bước 4: Kiểm tra quyền truy cập vào các trang web nội bộ từ máy client.**

1. Sign in vào máy **LON-CL1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

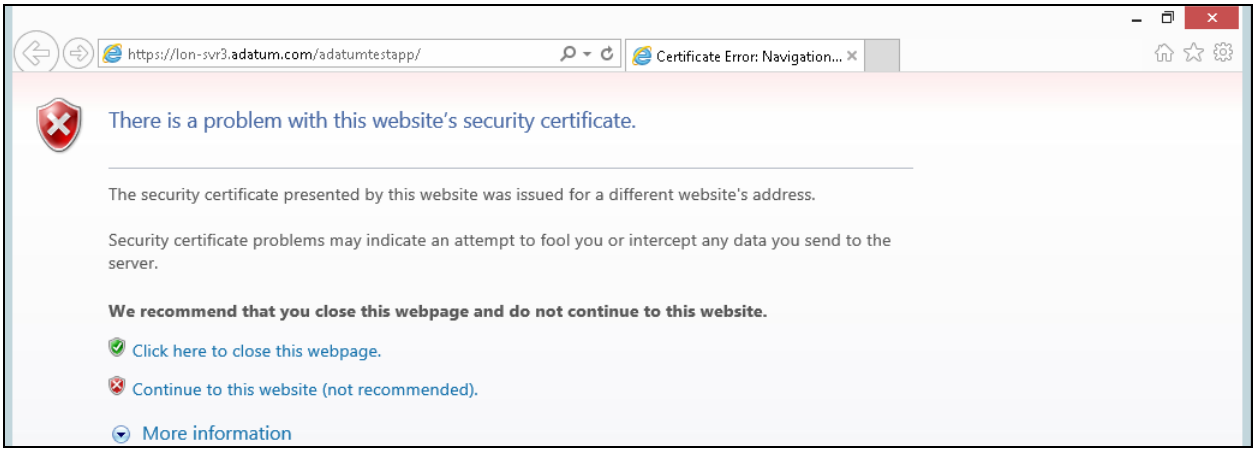
2. Mở **File Explorer**, vào đường dẫn **C:\Windows\System32\Drivers\etc**, mở file **host** bằng **Notepad**



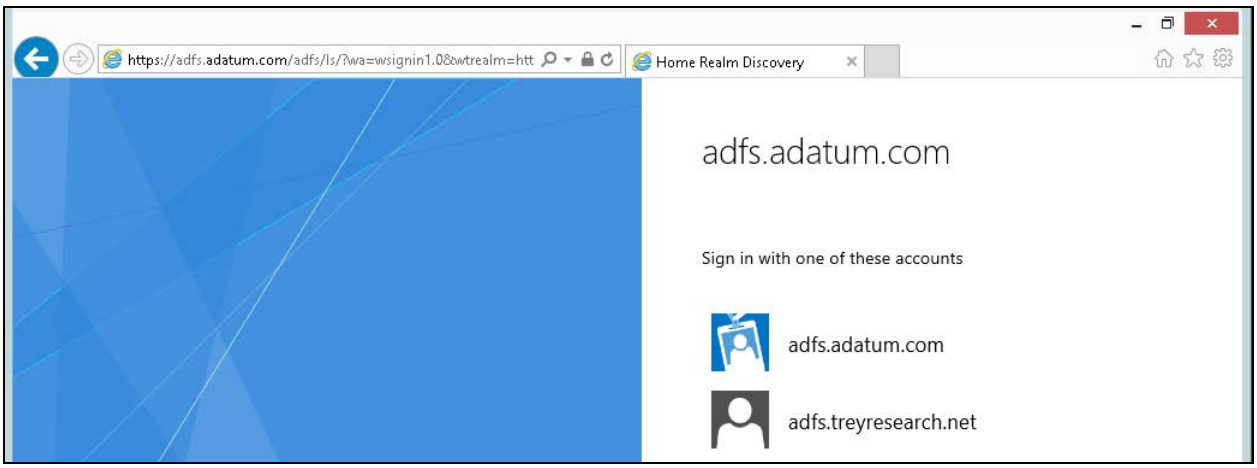

3. Trong file **host**, ở cuối trang, nhập **172.16.0.13 lon-svr3.adatum.com.** Lưu và tắt **Notepad.**



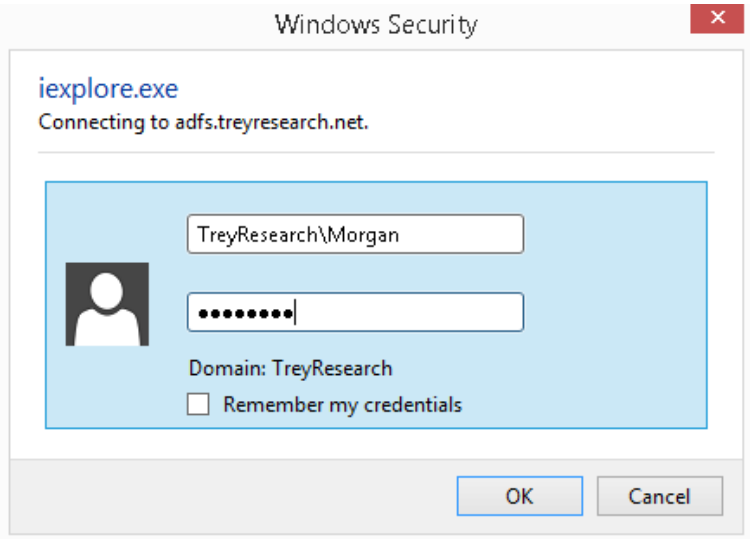
4. Mở **Internet Explorer**, truy cập **https://lon-svr3.adatum.com/adatumtestapp/**, chọn **Continue to this website (not recommended)**.




5. Trong phần **Sign in with one of these accounts**, chọn **adfs.treyresearch.net**.



6. Hộp thoại **Windows Security**, sign in bằng **TreyResearch\Morgan** với password **Pa$$w0rd**. Kiểm tra truy cập Application thành công.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình Web Application Proxy để hỗ trợ các máy client bên ngoài truy cập thành công Web Application trong nội bộ.**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiên bước 2 và 3 cho các máy ảo còn lại.

# Bài 11: Triển khai Dynamic Access Control (DAC) và Access-Denied Assistance

**I. Mục tiêu:**

- Cấu hình Dynamic Access Control (DAC)
- Cấu hình Access-Denied Assistance.

**II. Kịch bản:**

Công ty A. Datum đã thành lập một nhóm bán hàng mới ở châu Âu. Kết quả là, văn phòng chi nhánh đã trang bị nhiều chức năng để hỗ trợ nhóm bán hàng này. Bạn chịu trách nhiệm lập kế hoạch cơ sở hạ tầng mạng của văn phòng chi nhánh. Vì vậy, bạn phải thiết lập các tiêu chuẩn để truy cập các dữ liệu trong hệ thống.

Nhóm nghiên cứu của A. Datum thực hiện các công việc rất bí mật, và dữ liệu của họ được lưu trữ trên các File Servers của công ty. Bộ phận an ninh của A. Datum muốn đảm bảo rằng chỉ các nhân viên có thẩm quyền mới được phép truy cập các dữ liệu bí mật này.

Là một quản trị mạng cao cấp, bạn có trách nhiệm giải quyết các yêu cầu bảo mật bằng cách triển khai chức năng Dynamic Access Control (DAC) trên các máy File Servers. Bạn sẽ làm việc với nhóm kinh doanh và bộ phận an ninh để xác định các dữ liệu cần được bảo vệ và những người nào cần phải có quyền truy cập vào các dữ liệu bí mật. Sau đó, bạn sẽ lập kế hoạch để triển khai DAC dựa trên các yêu cầu của công ty.

**III. Yêu cầu tổng quan:**

Triển khai chiến lược bảo mật dữ liệu hỗ trợ các mục tiêu sau đây:

- Chỉ có các thành viên của bộ phận nghiên cứu mới có quyền truy cập và sửa đổi các thư mục thuộc về phòng nghiên cứu.
- Chỉ có người quản lý mới có quyền truy cập vào các tài liệu được phân loại là rất bí mật (highly confidential).

- Nhóm quản lý chỉ được phép truy cập vào tài liệu bí mật từ các máy tính được chỉ định. Các máy tính này phải là thành viên của nhóm ManagerWks.
- Nhóm hỗ trợ báo cáo có một số lượng lớn các cuộc gọi yêu cầu hỗ trợ từ những người dùng không thể truy cập tài nguyên. Vì vậy bạn phải cấu hình chức năng Access-Denied Assistance để giúp người dùng hiểu được các thông báo lỗi mà họ nhận được và cho phép họ yêu cầu truy cập tự động.

**IV. Mô hình thực hành:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-DC1**<br>**20414C-LON-SVR1**<br>**20414C-LON-CL1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy **LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên từ bước 1 đến 3 cho máy ảo **20414C-LON-SVR1** và **20414C-LON-CL1.**

**VI. Thực hành:**

*Thời gian thực hành: 70 phút*

## Bài tập 1: Chuẩn bị cho việc triển khai DAC.

Bước đầu tiên trong việc triển khai DAC là cấu hình các Claims (yêu cầu) cho người sử dụng và các thiết bị truy cập các tập tin. Trong bài tập này, bạn sẽ xem xét các Claims mặc định và tạo ra các Claims mới dựa trên thuộc tính Department và Computer Group Ngoài ra, bạn sẽ cấu hình Resource Property Lists (danh sách thuộc tính tài nguyên) và các Resource Property Definitions (định nghĩa thuộc tính tài nguyên). Sau đó, bạn sẽ sử dụng các thuộc tính tài nguyên để phân loại tập tin.

❖ **Bài thực hành bao gồm các bước:**

1. Chuẩn bị AD DS cho DAC, và xem xét các Claim mặc định.
2. Cấu hình Claims cho người dùng và thiết bị.
3. Cấu hình Resource Properties cho các files.
4. Phân loại file và folder.

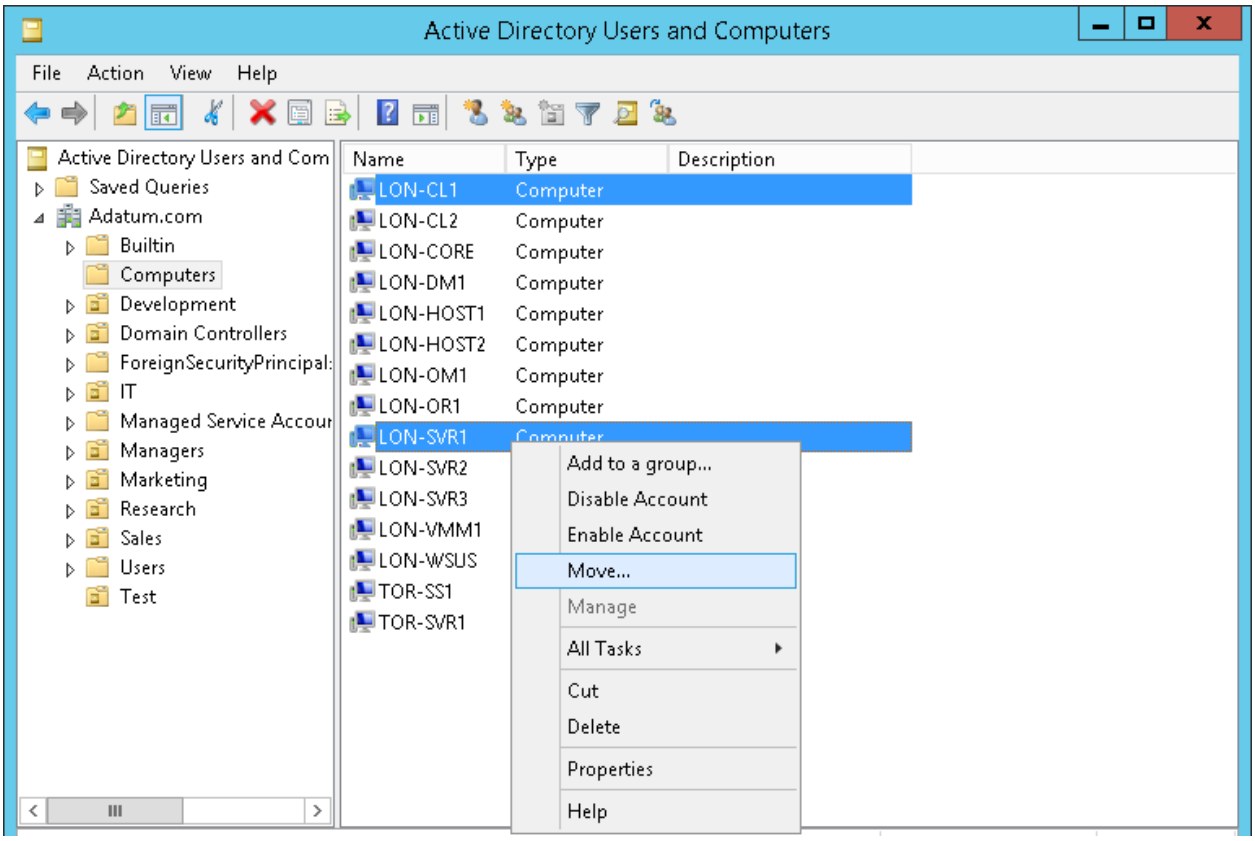
❖ **Thực hiện:**

**Bước 1: Chuẩn bị AD DS cho DAC, và xem xét các Claim mặc định.**

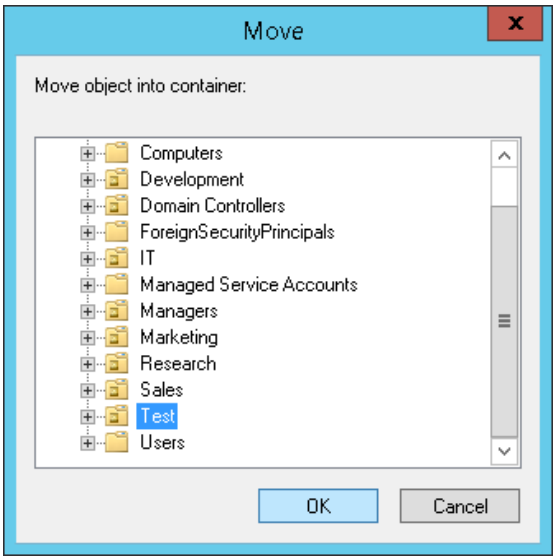
1. Trên máy **LON-DC1**, Trong cửa sổ **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**, chuột phải **Adatum.com**, chọn **New**, chọn **Organizational Unit**.

2. Hộp thoại **New Object – Organizational Unit**, trong ô **Name**, nhập **Test**, và chọn **OK**.

3. Trong cửa sổ **Active Directory Users and Computers**, bung **Adatum.com,** chọn **Computers**, giữ phím **Ctrl**, chọn **LON-SVR1** và **LON-CL1**, chuột phải **LON-SVR1** và **LON-CL1**, chọn **Move**.

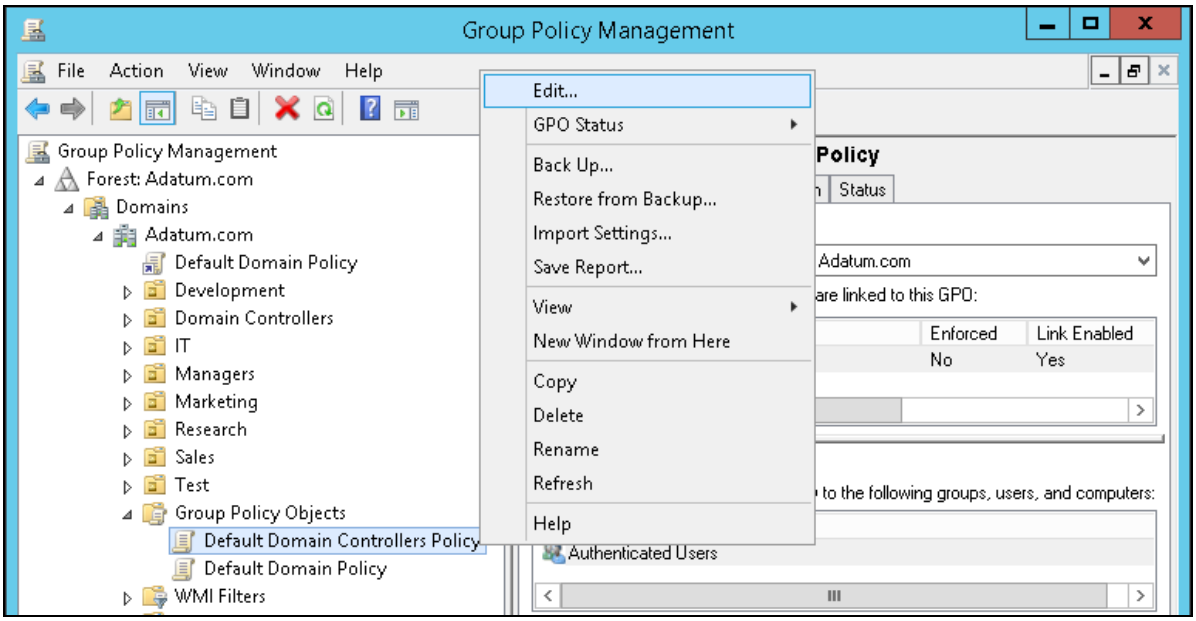


4. Hộp thoại **Move**, chọn OU **Test**, và chọn **OK**.

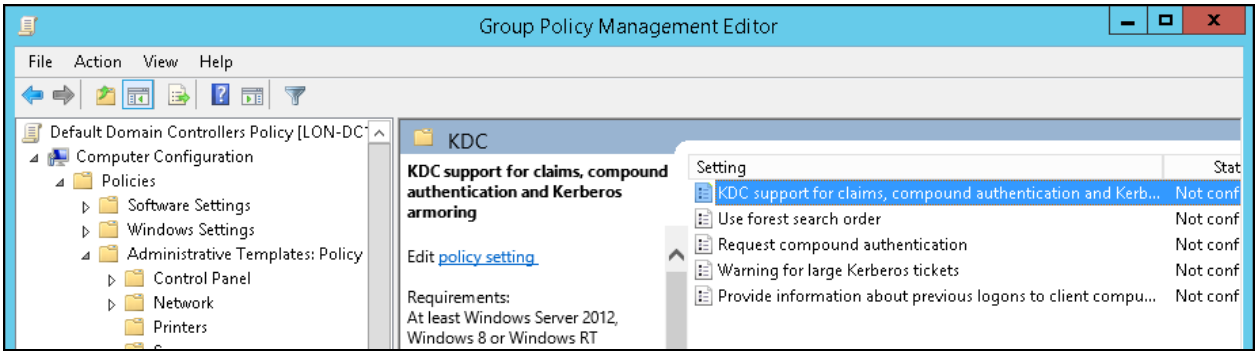



5. Tắt cửa sổ **Active Directory Users and Computers**.

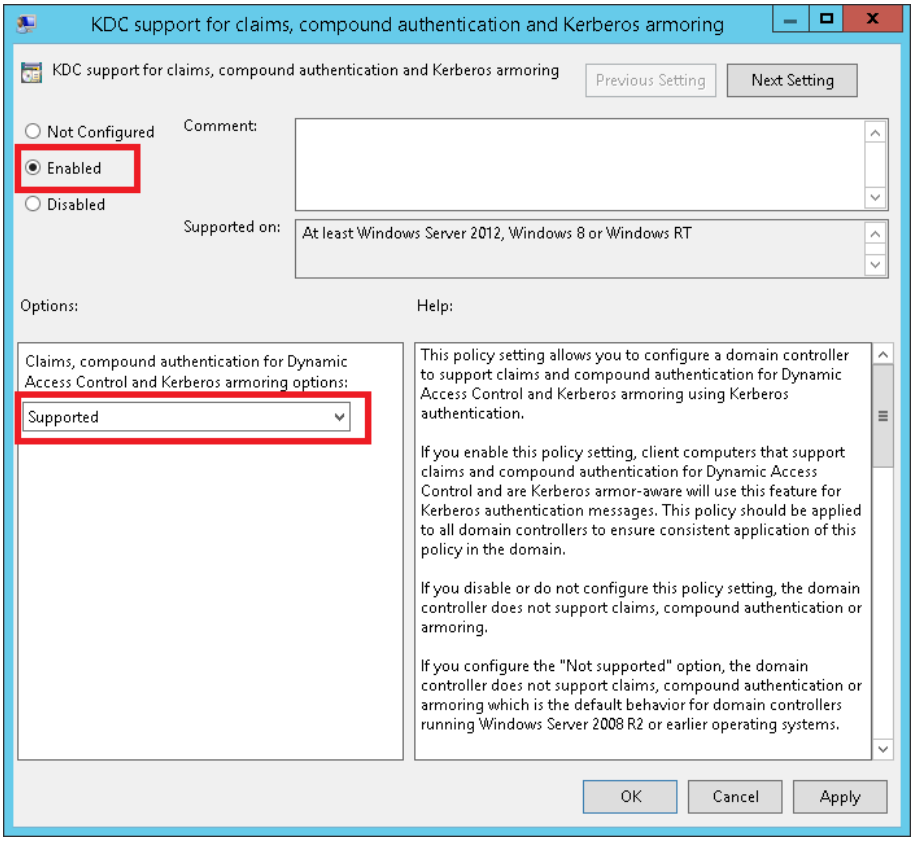
6. Trong **Server Manager**, bung menu **Tools**, mở **Group Policy Management**, bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, chọn **Group Policy Objects,** chuột phải **Default Domain Controllers Policy**, chọn **Edit**.



7. Cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Administrative Templates**, bung **System**, chọn **KDC**, nhấp đôi chuột mở policy **KDC support for claims, compound authentication and Kerberos armoring**.




8. Cửa sổ **KDC support for claims, compound authentication and Kerberos armoring**, chọn **Enabled**, bung ô **Options**, chọn **Supported**, và chọn **OK**.

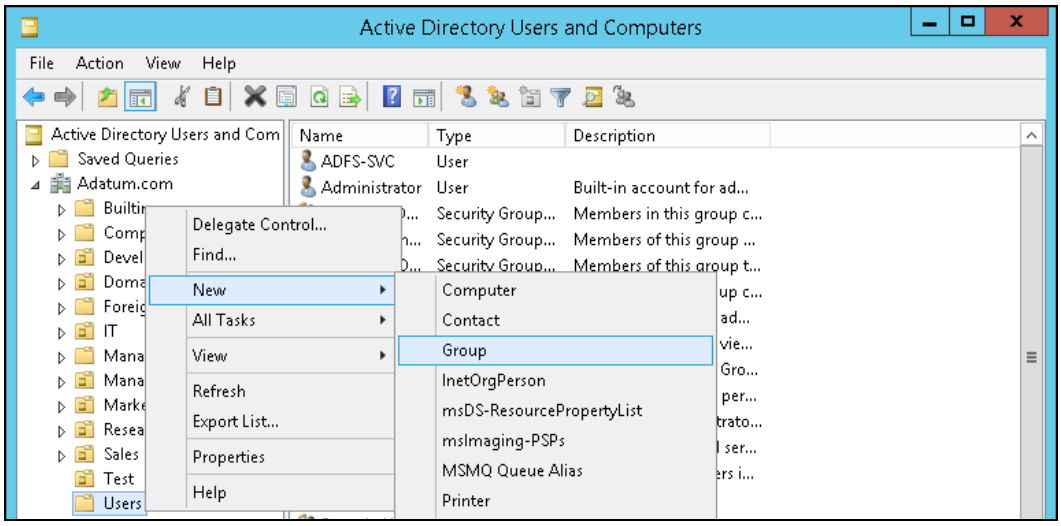


9. Tắt cửa sổ **Group Policy Management Editor** và **Group Policy Management Console**.

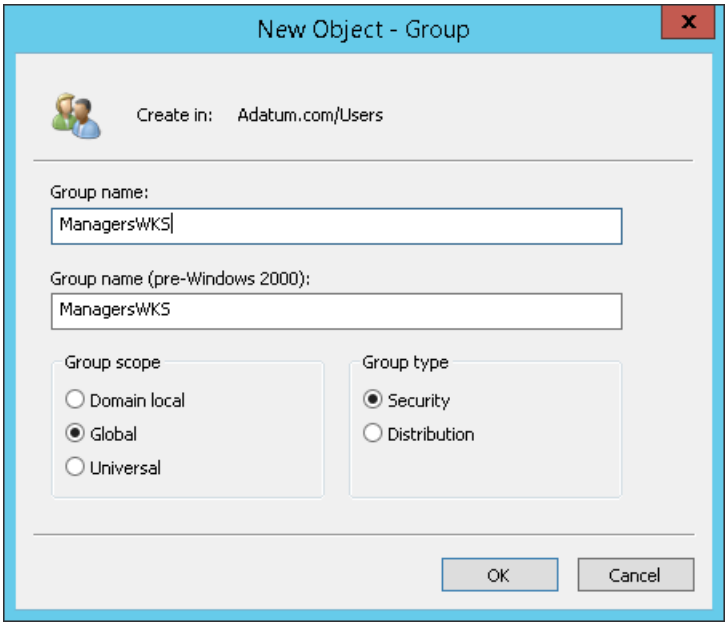
10. Mở **Windows PowerShell**, gõ lệnh: **gpupdate /force**

11. Tắt **Windows PowerShell**

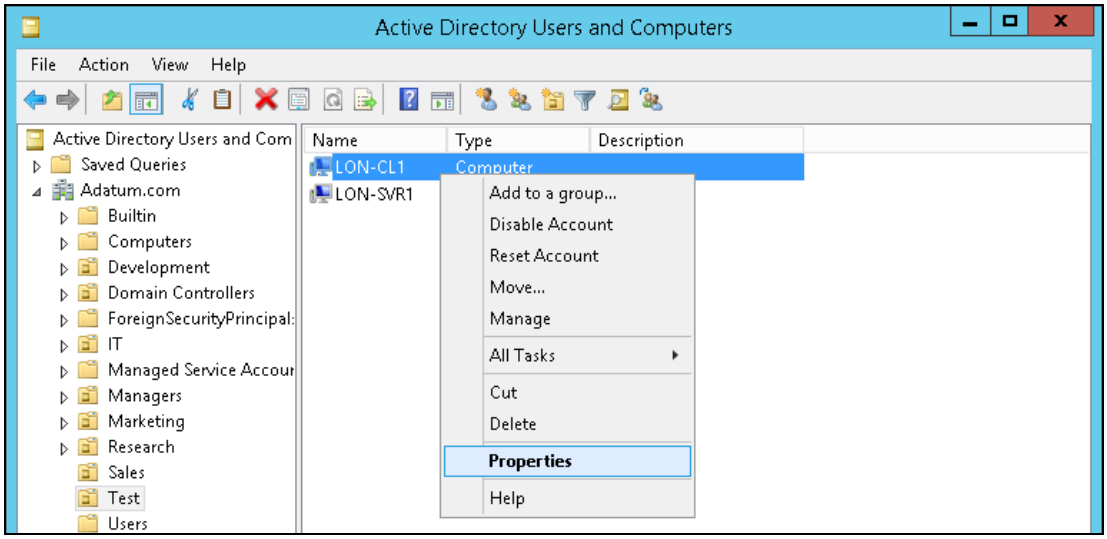
12. Trong **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**, chuột phải **Users**, chọn **New**, và chọn **Group**.



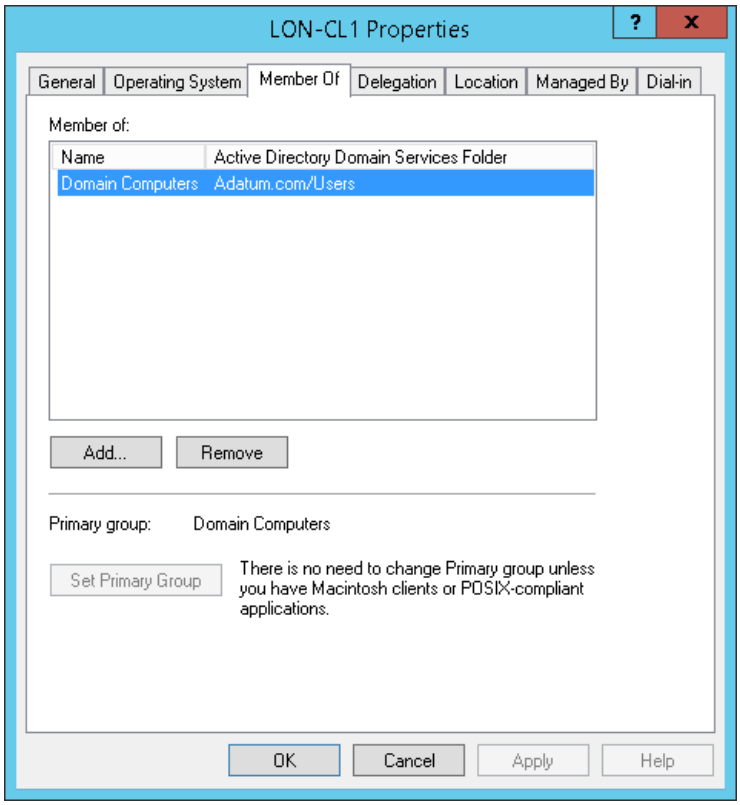

13. Trong ô **Group name**, nhập **ManagersWKS,** chọn **OK**.



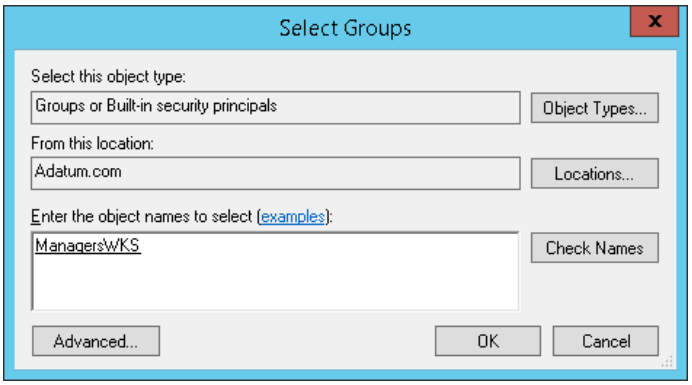
14. Chọn OU **Test,** chuột phải **LON-CL1**, chọn **Properties**.



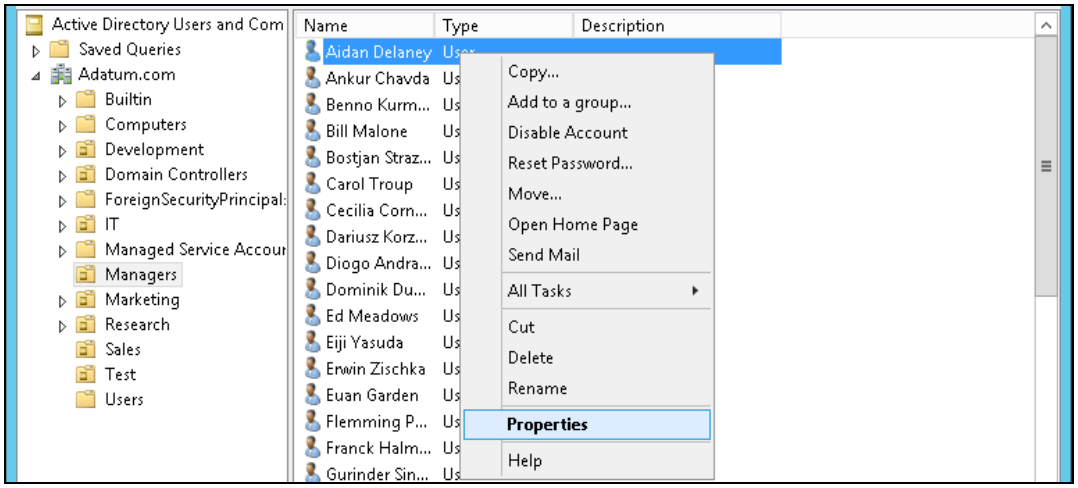

15. Hộp thoại **LON-CL1 Properties**, qua tab **Member Of**, chọn **Add**.



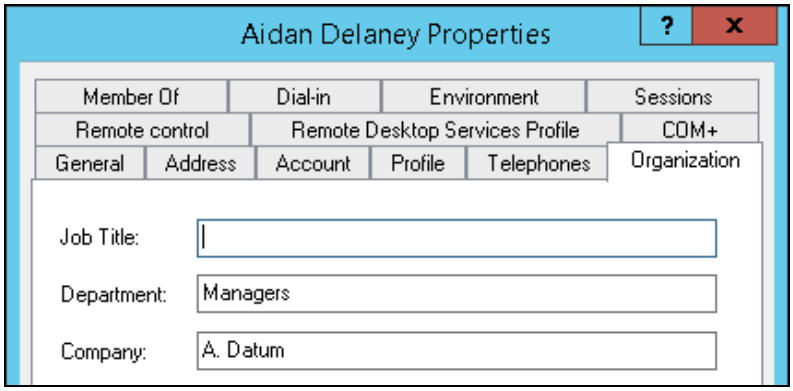
16. Hộp thoại **Select Groups**, nhập **ManagersWKS**, chọn **Check Names**, và chọn **OK** 2 lần.



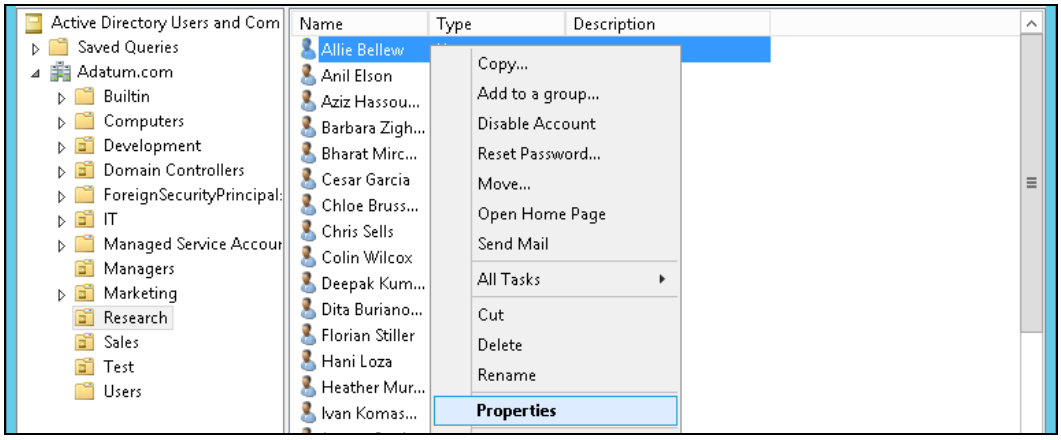

17. Chọn OU **Managers,** chuột phải **Aidan Delaney**, chọn **Properties**.



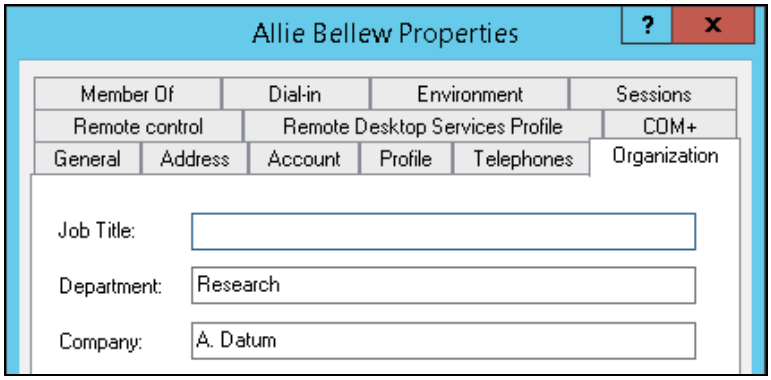

18. Hộp thoại **Aidan Delaney Properties**, qua tab **Organization**, đảm bảo trong ô **Department** nhập **Managers**, và chọn **OK**.



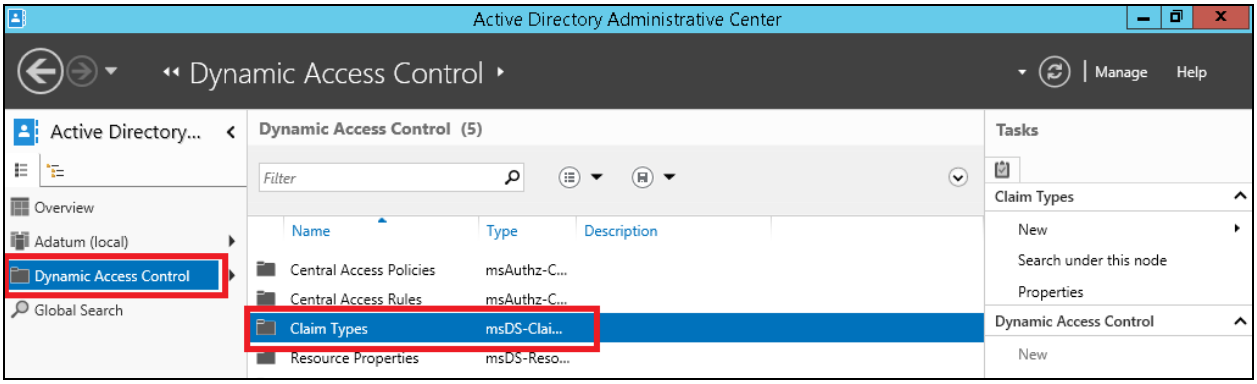
19. Vào OU **Research**, chuột phải **Allie Bellew**, chọn **Properties**.



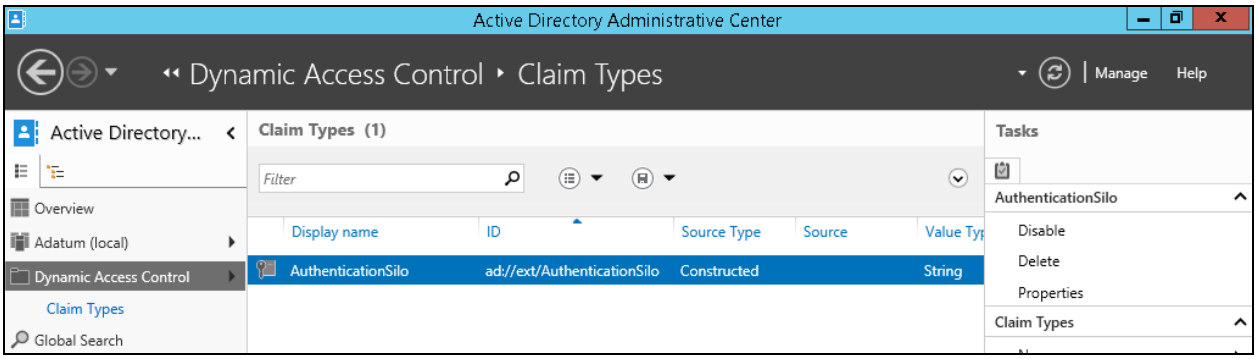

20. Hộp thoại **Allie Bellew Properties**, qua tab **Organization**, đảm bảo trong ô **Department** nhập **Research**, và chọn **OK**.



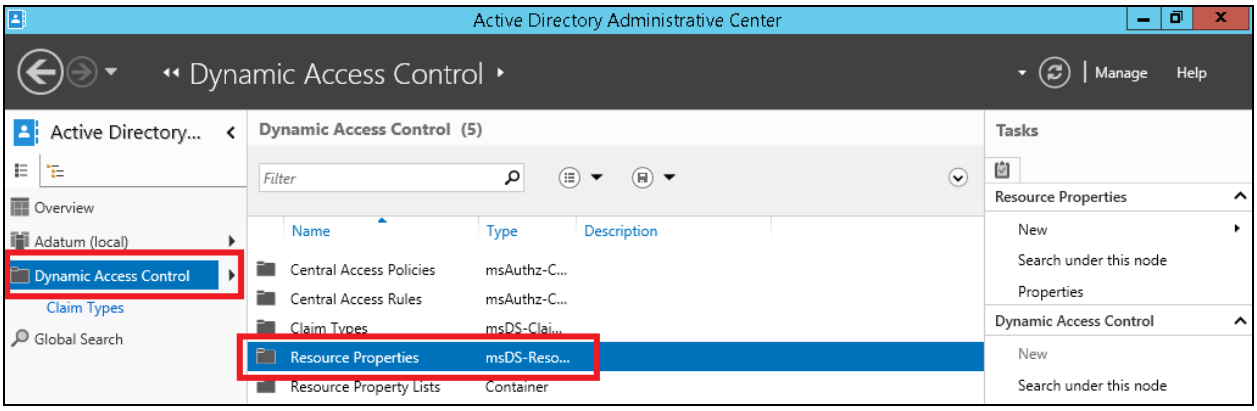

21. Trong **Server Manager**, bung menu **Tools**, mở **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Claim Types**.



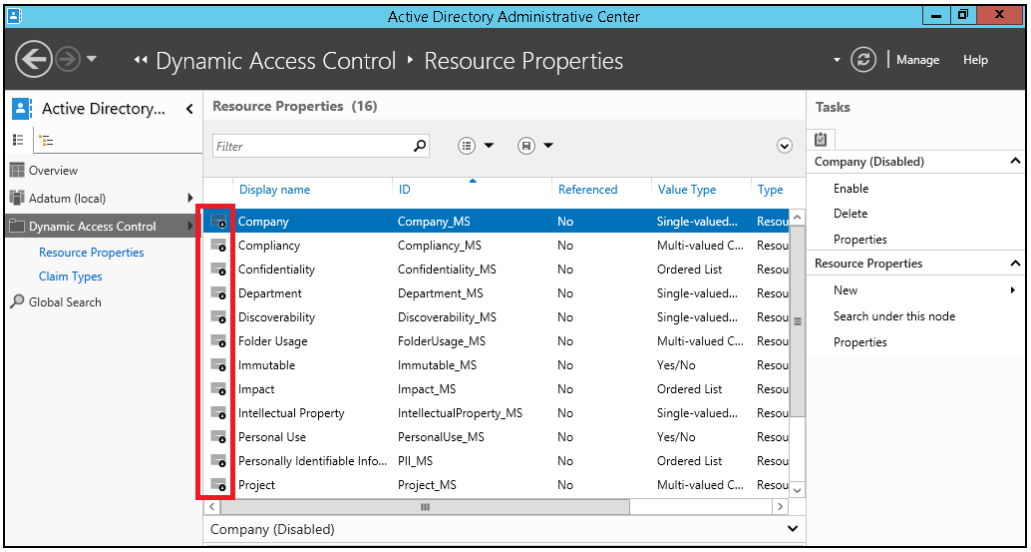
22. Kiểm tra chỉ có 1 claims mặc định tên **AuthenticationSilo**.



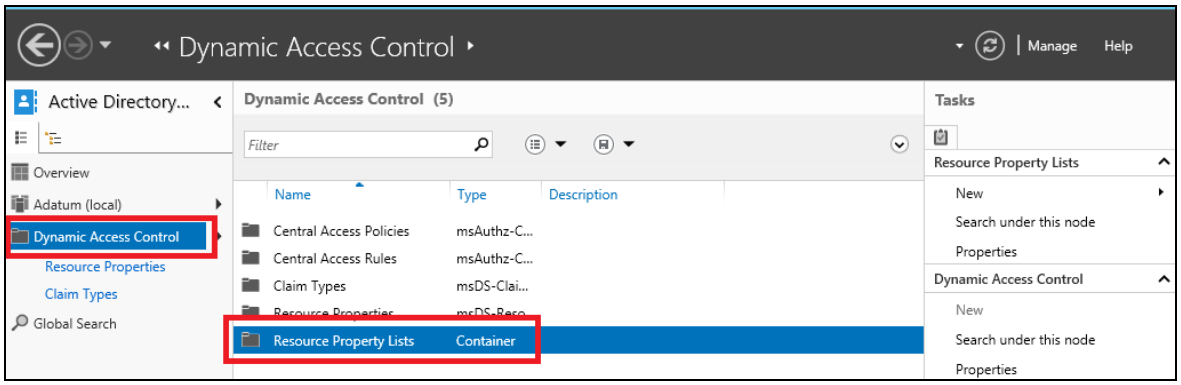

23. Chọn **Dynamic Access Control**, nhấp đôi chuột **Resource Properties**.



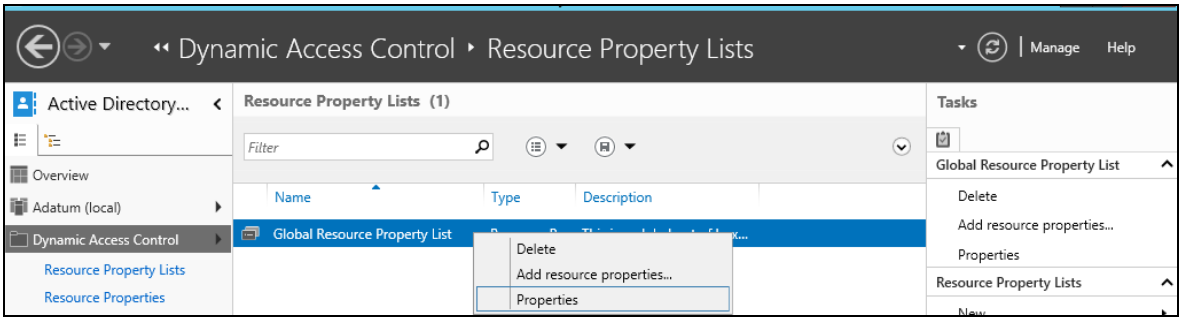

24. Kiểm tra tất cả Resource Properties đang ở trạng thái Disabled.



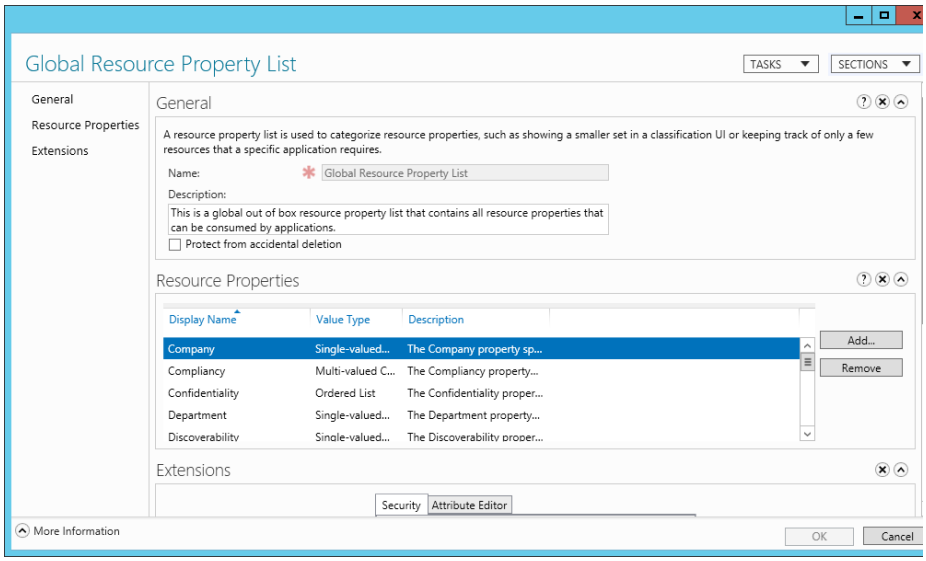
25. Chọn **Dynamic Access Control**, nhấp đôi chuột **Resource Property Lists**.




26. Chuột phải **Global Resource Property List**, chọn **Properties**.

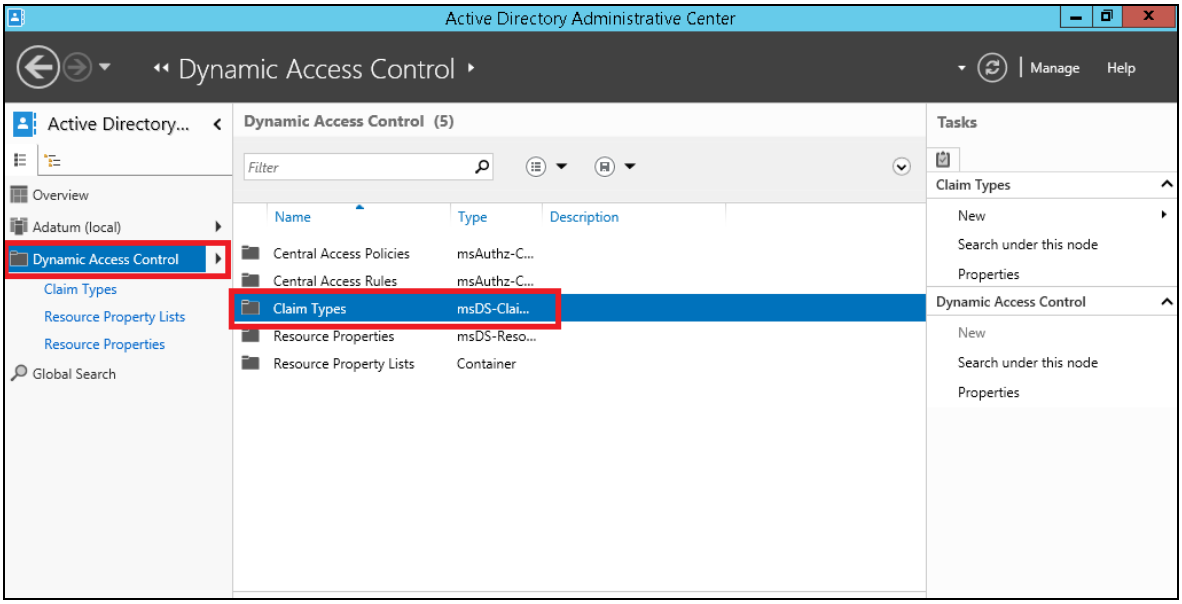



27. Cửa sổ **Global Resource Property List**, trong phần **Resource Properties**, kiểm tra các Resource Properties đang có, và chọn **Cancel**.

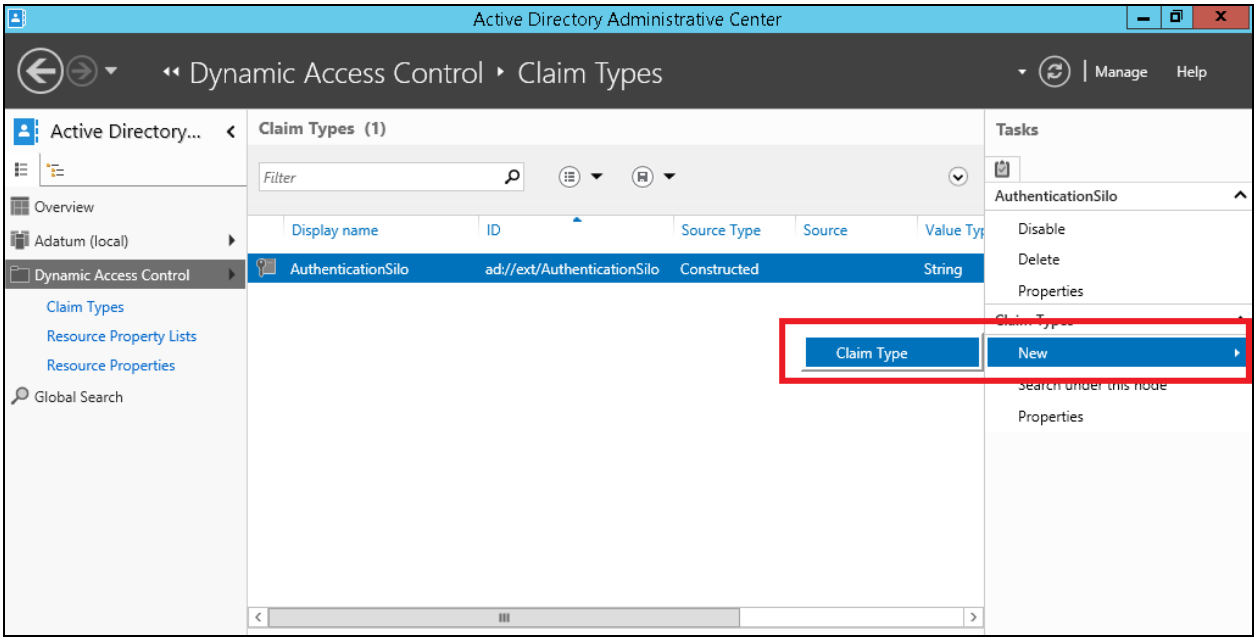


## Bước 2: Cấu hình Claims cho người dùng và thiết bị.

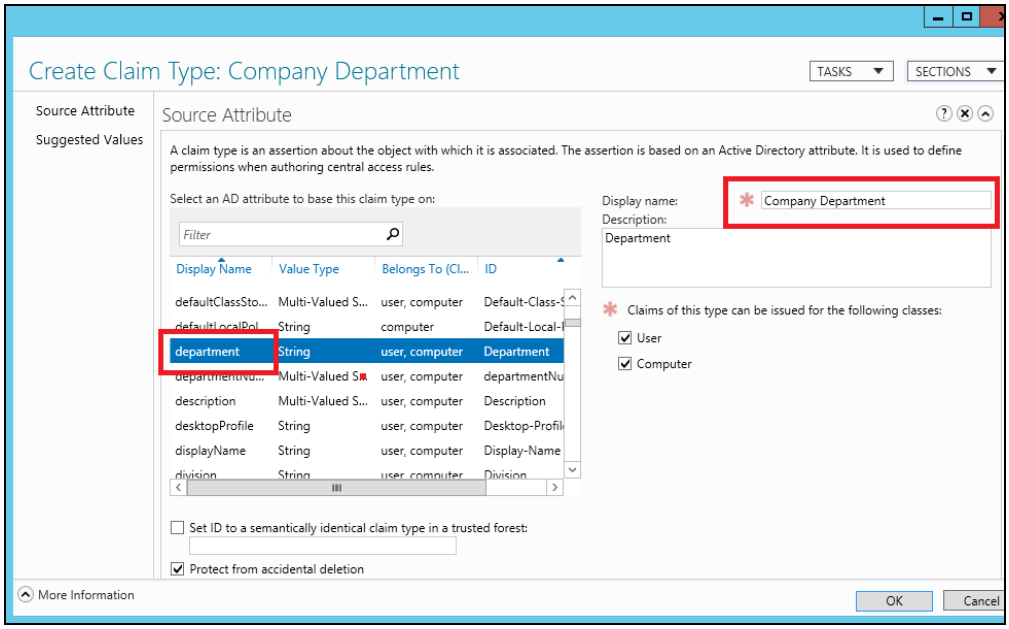
1. Trên máy **LON-DC1**, trong cửa sổ **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Claim Types**



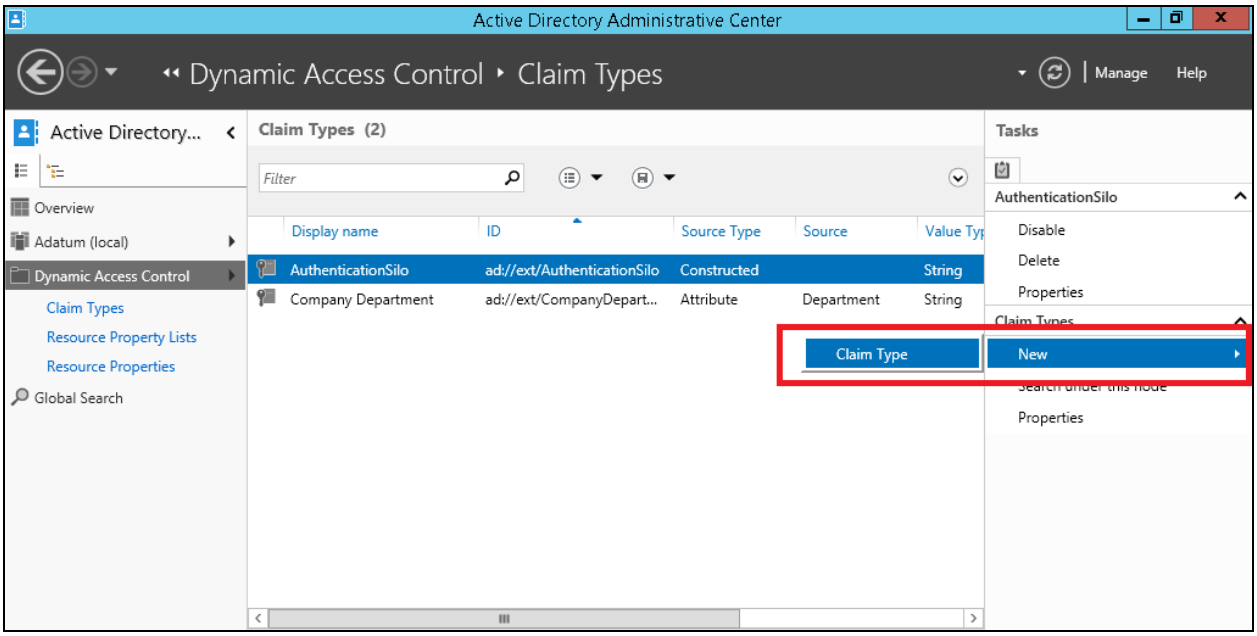

2. Chọn **New**, và chọn **Claim Type**.



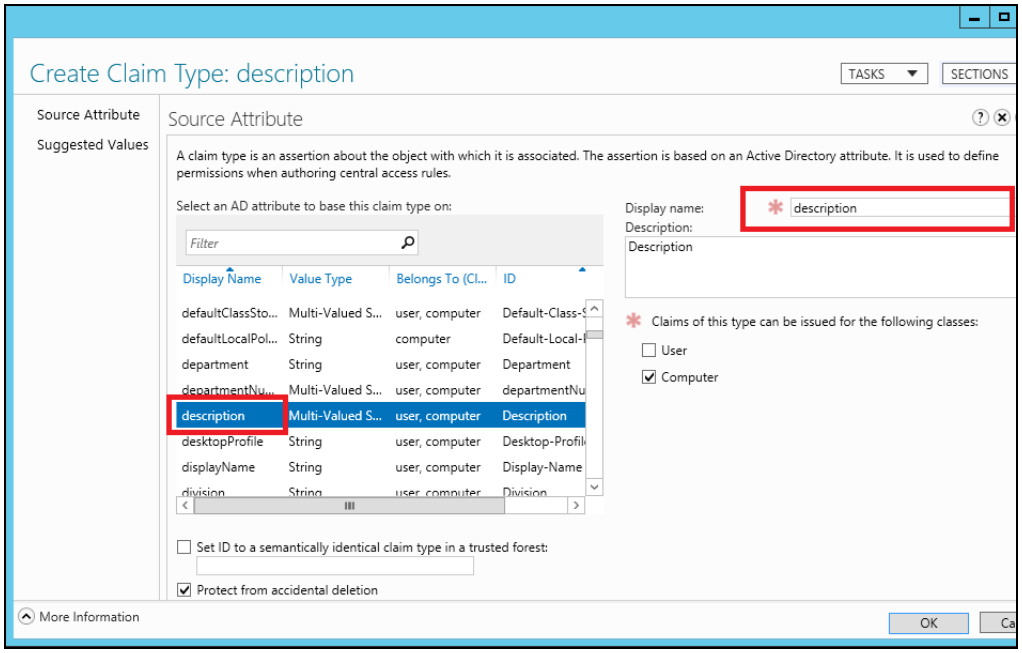
3. Cửa sổ **Create Claim Type**, trong phần **Source Attribute**, chọn **department**. Trong ô **Display name**, nhập **Company Department**. Đánh dấu chọn 2 ô **User** và **Computer**, chọn **OK**.




4. Trong cửa sổ **Active Directory Administrative Center**, chọn **New**, và chọn **Claim Type**.

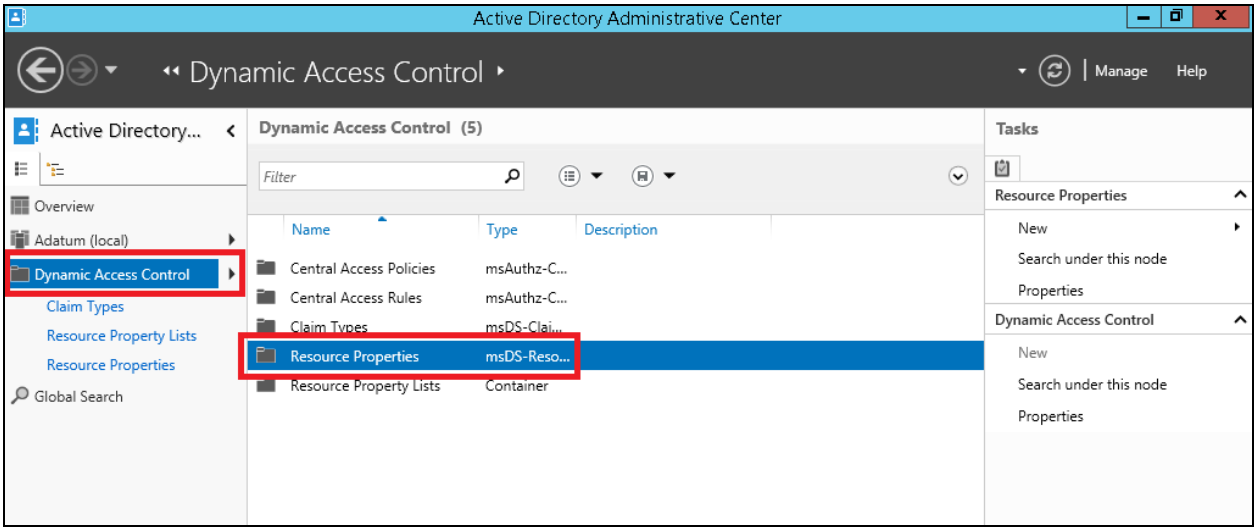


5. Cửa sổ **Create Claim Type**, trong phần **Source Attribute**, chọn **description**, bỏ dấu chọn ô **User**, đánh dấu chọn ô **Computer**, và chọn **OK**.

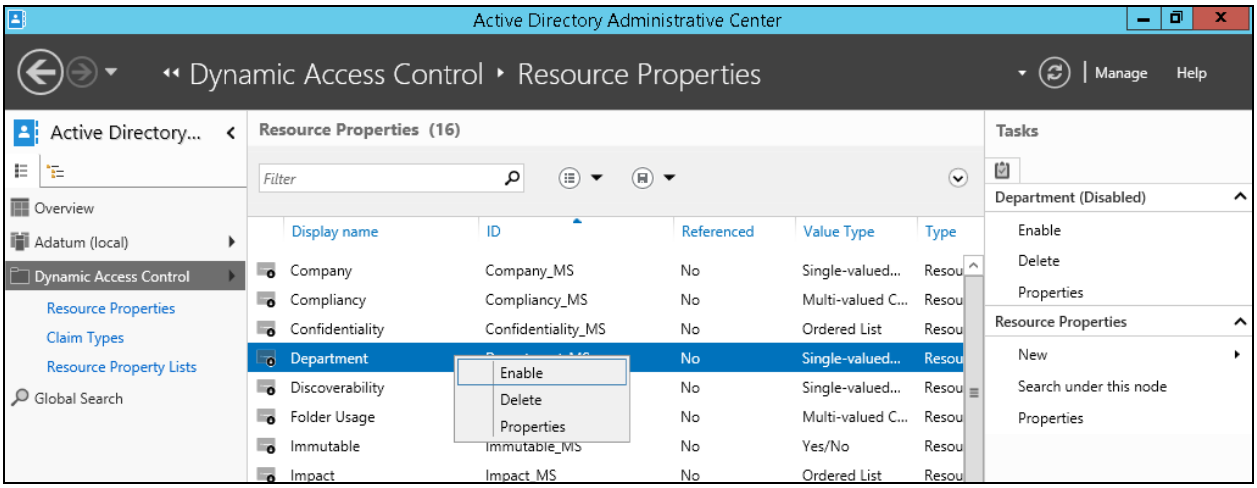



## Bước 3: Cấu hình Resource Properties cho các files.

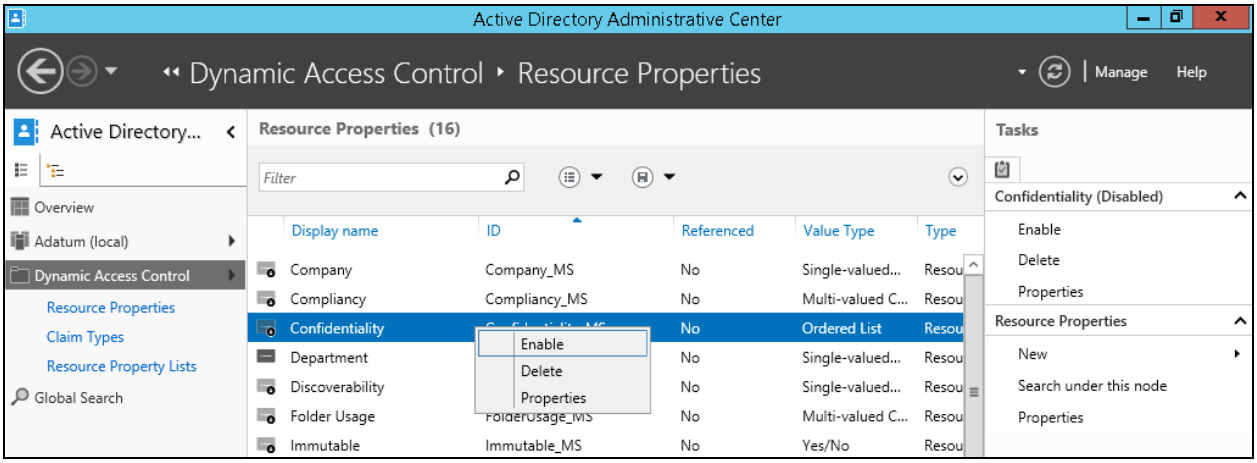
1. Trên máy **LON-DC1**, trong cửa sổ **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Resource Properties**.



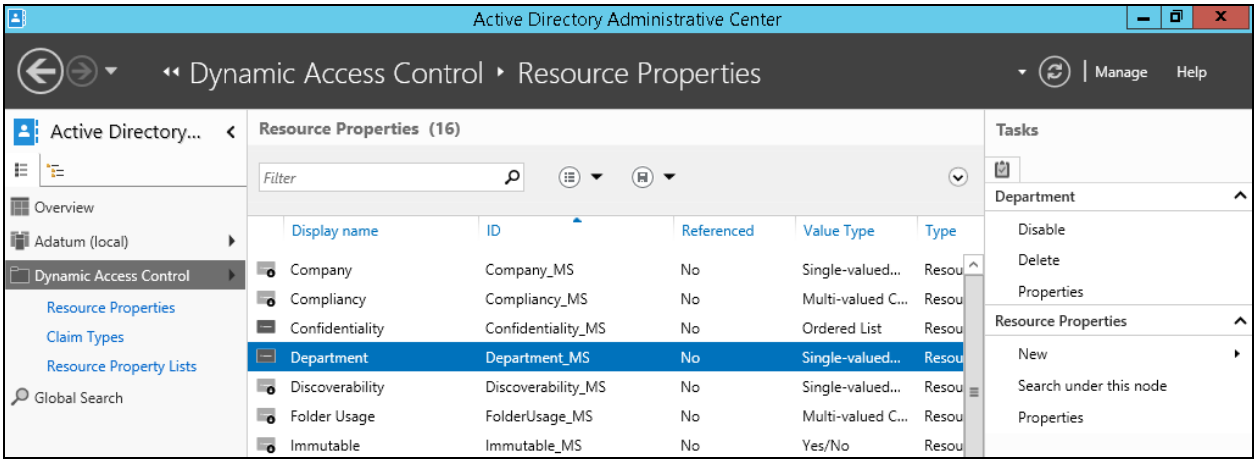
2. Trong danh sách **Resource Properties**, chuột phải **Department**, chọn **Enable**.



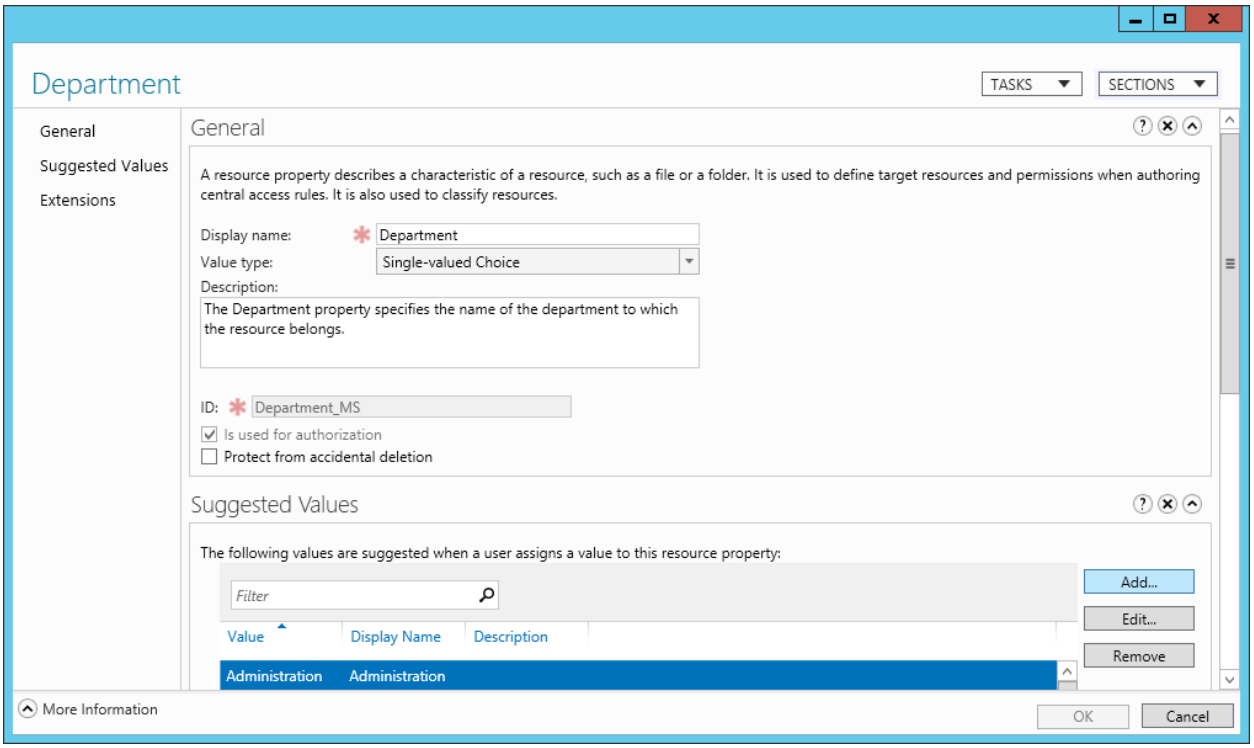

3. Chuột phải **Confidentiality**, chọn **Enable**.



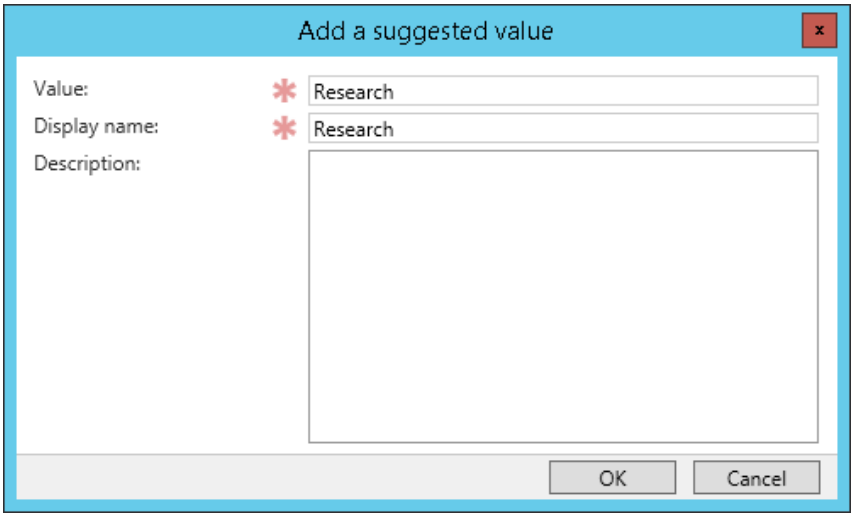
4. Nhấp đôi chuột **Department**.



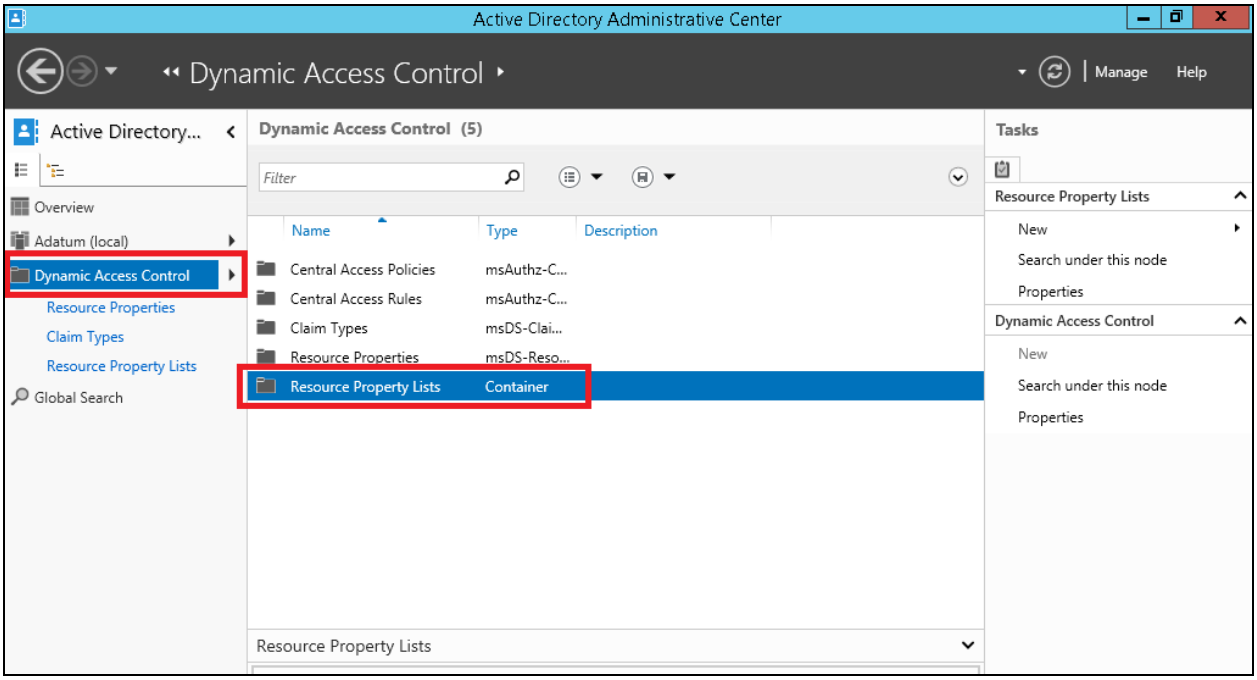

5. Cửa sổ **Department** , trong phần **Suggested Values**, chọn **Add**.



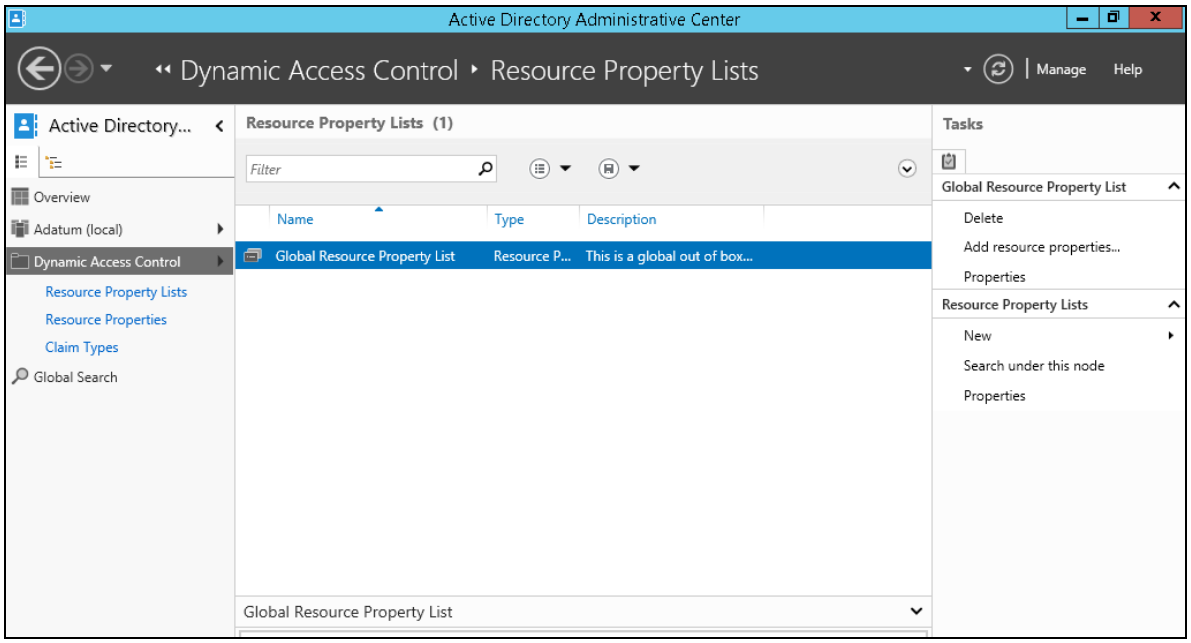
6. Hộp thoại **Add a suggested value**, nhập **Research** vào ô **Value** và ô **Display name**, chọn **OK** 2 lần.



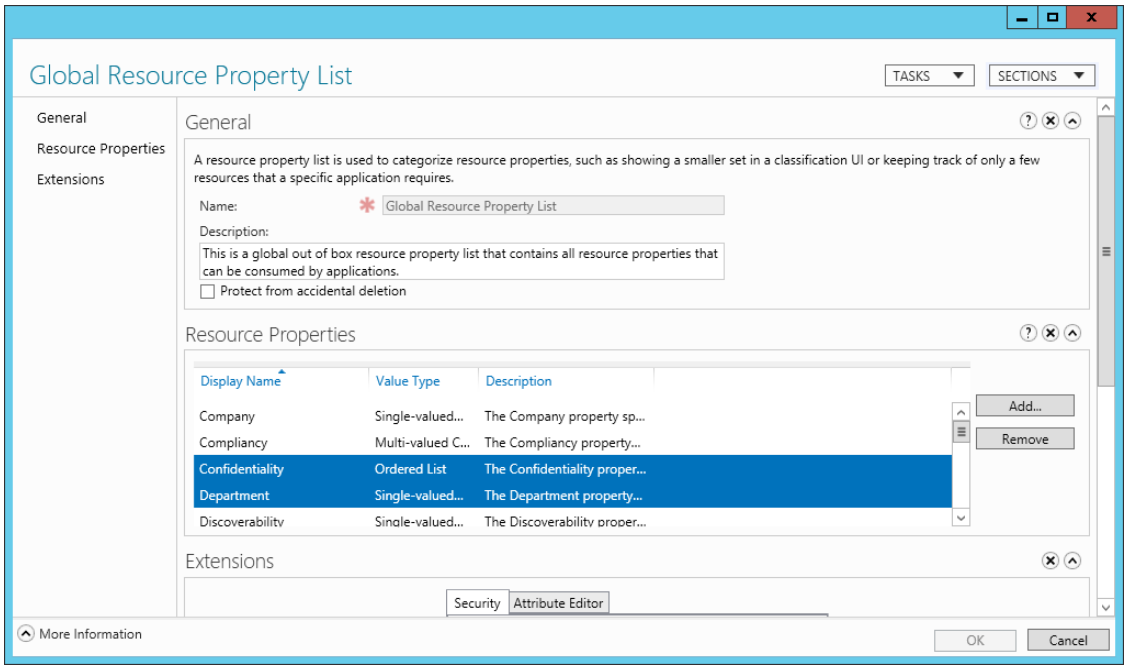

7. Trong cửa sổ **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Resource Property Lists**.



8. Nhấp đôi chuột **Global Resource Property List**.



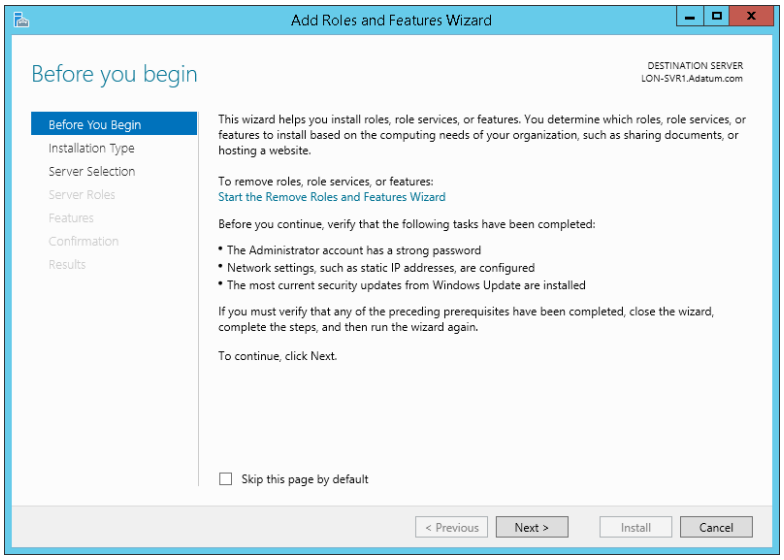

9. Trong cửa sổ **Global Resource Property List,** trong danh sách **Resource Properties** đảm bảo có **Department** và **Confidentiality**, chọn **Cancel**.



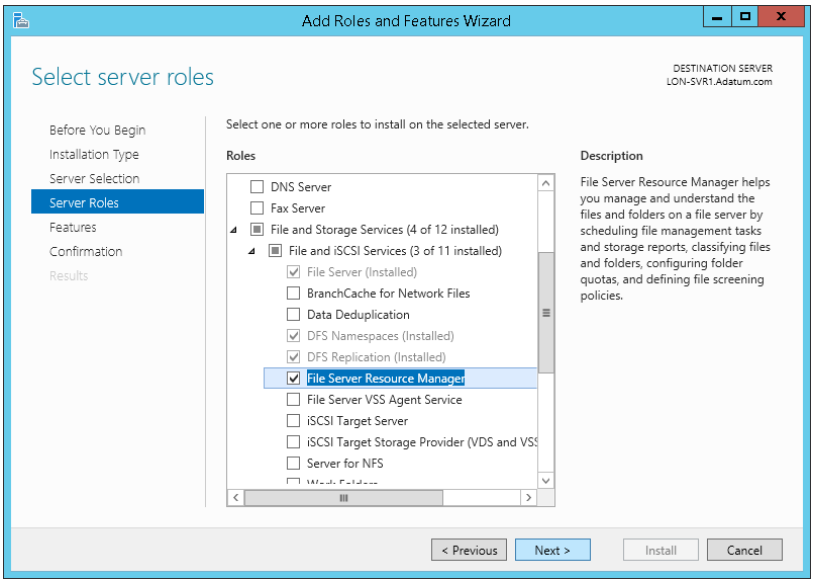
## Bước 4: Phân loại file và folder.

1. Qua máy **LON-SVR1.** Trong **Server Manager**, chọn **Add roles and features**.

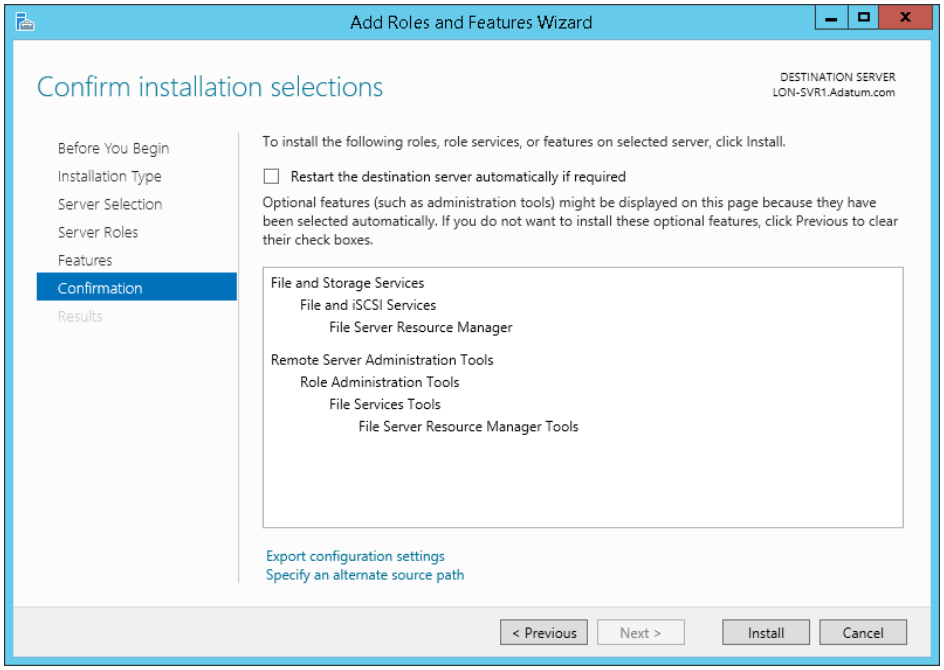
2. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



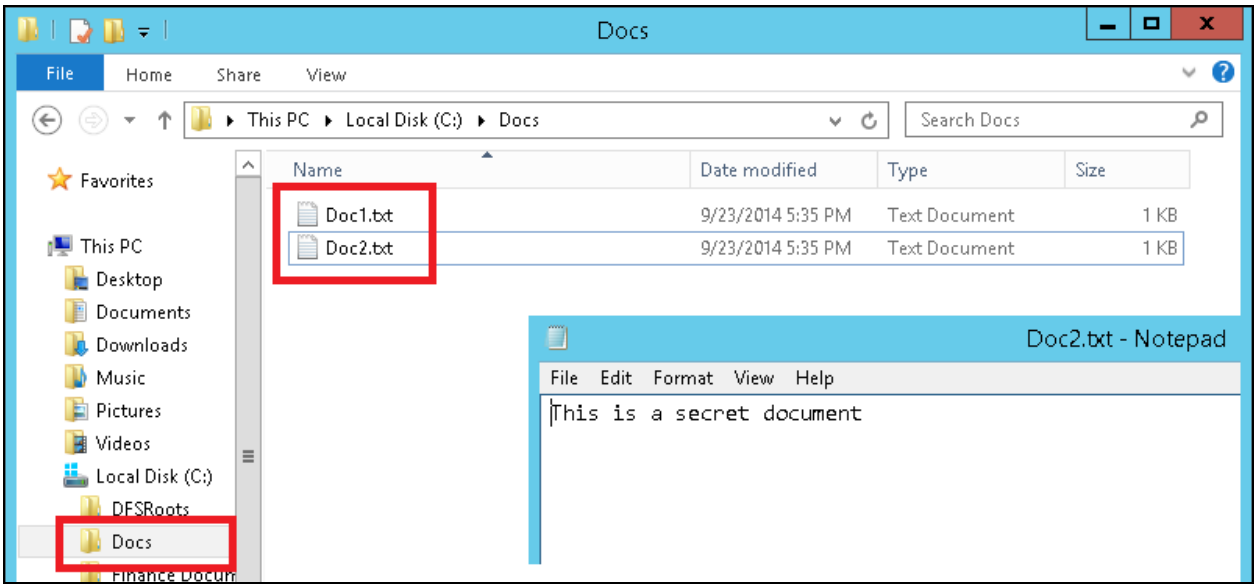

3. Cửa sổ **Select server roles**, bung **File and Storage Services (Installed)**, bung **File and iSCSI Services**, đánh dấu chọn **File Server Resource Manager**, chọn **Add Features**, và chọn **Next** 2 lần.



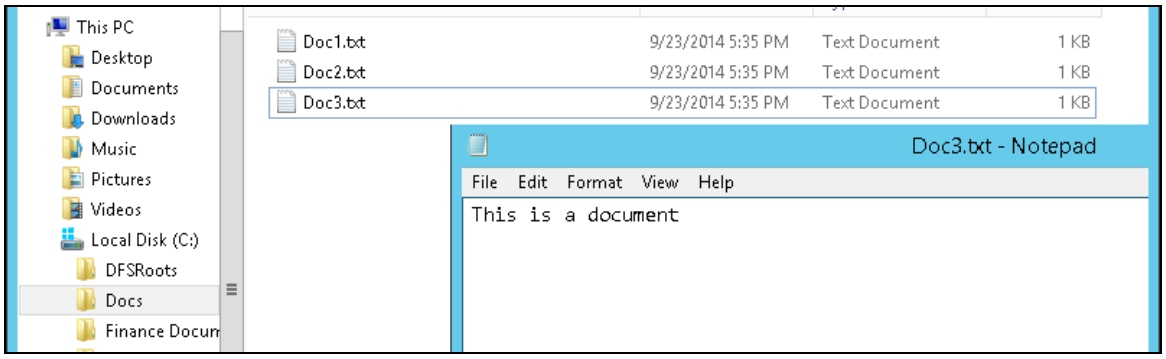
4. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.



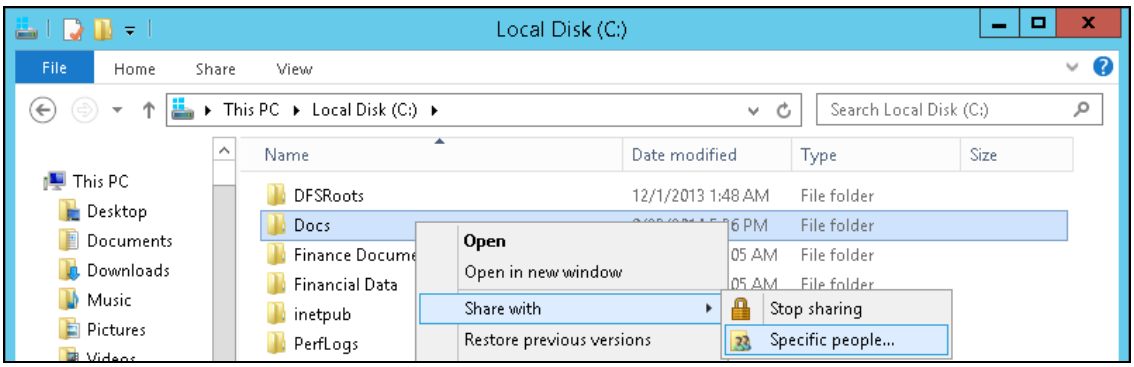

5. Mở **File Explorer,** vào ổ **C:**, tạo một thư mục mới, đặt tên **Docs**. Trong thư mục **Docs**, tạo 2 file text **Doc1.txt** và **Doc2.txt** có nội dung " **This is a secret document**. "



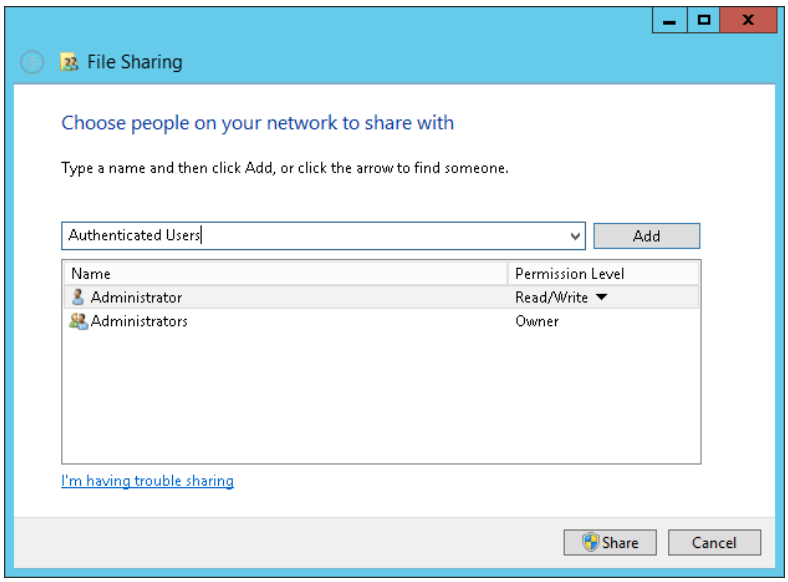
6. Trong thư mục **Docs**, tạo file text **Doc3.txt** có nội dung " **This is a document**."



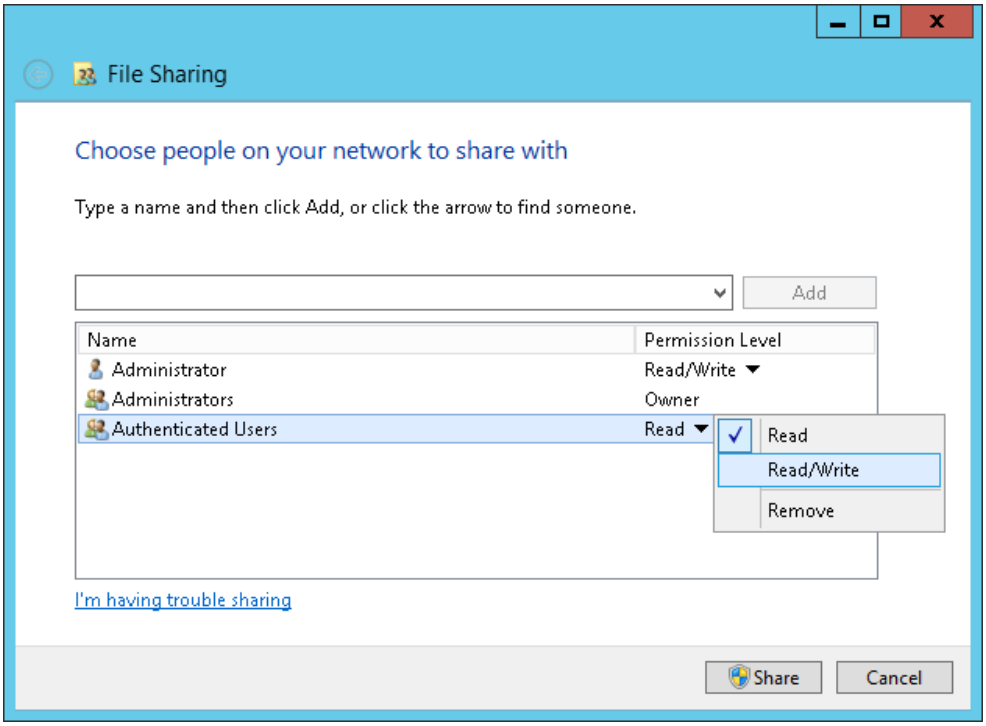

7. Trong **File Explorer**, chuột phải **Docs**, chọn **Share with**, chọn **Specific people**.



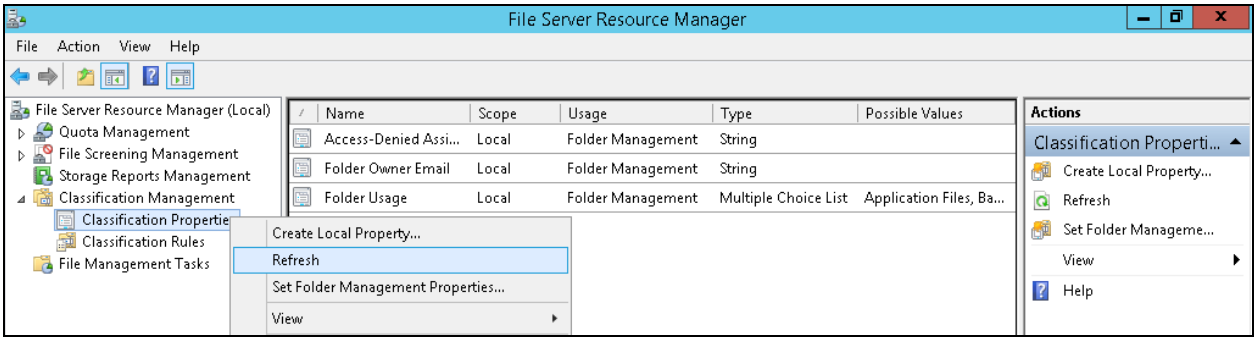

8. Hộp thoại **File Sharing**, nhập **Authenticated Users,** và chọn **Add**.



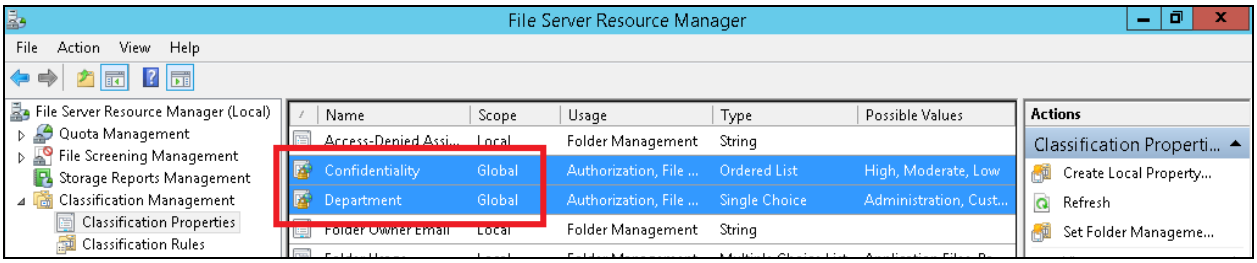
9. Chọn **Authenticated Users**, bung **Permission Level**, chọn **Read/Write**, chọn **Share**, và chọn **Done**.



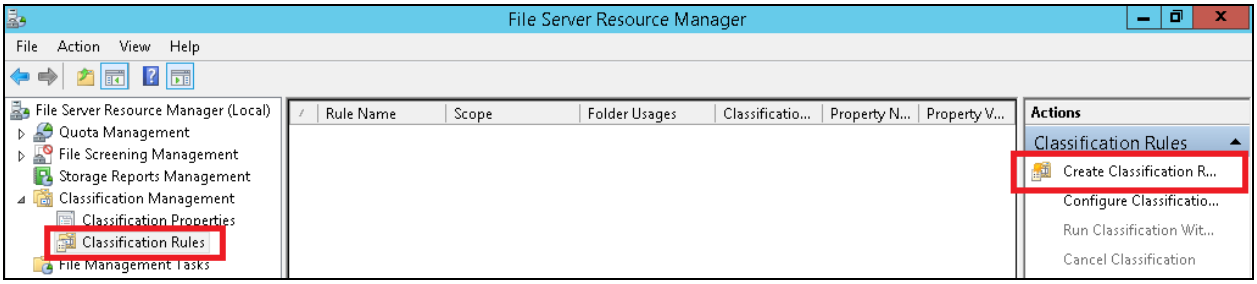

10. Trong **Server Manager**, bung menu **Tools**, mở **File Server Resource Manager**, bung **Classification Management**, chuột phải **Classification Properties**, chọn **Refresh**.



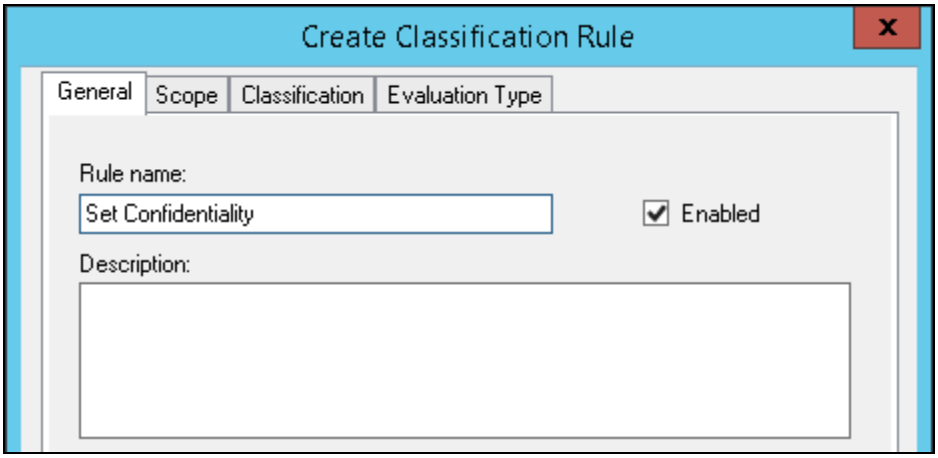
11. Kiểm tra **Confidentiality** và **Department** đã được hiển thị.



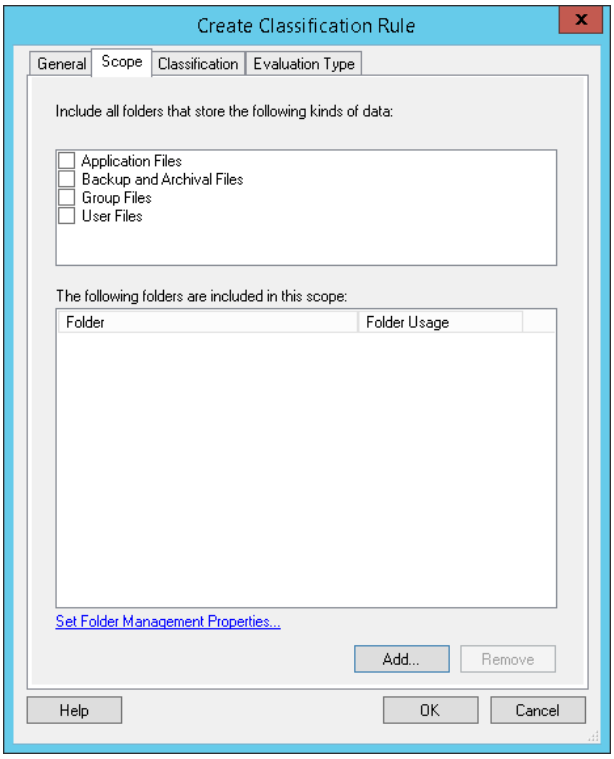

12. Chọn **Classification Rules**, trong cửa sổ **Actions**, chọn **Create Classification Rule**.



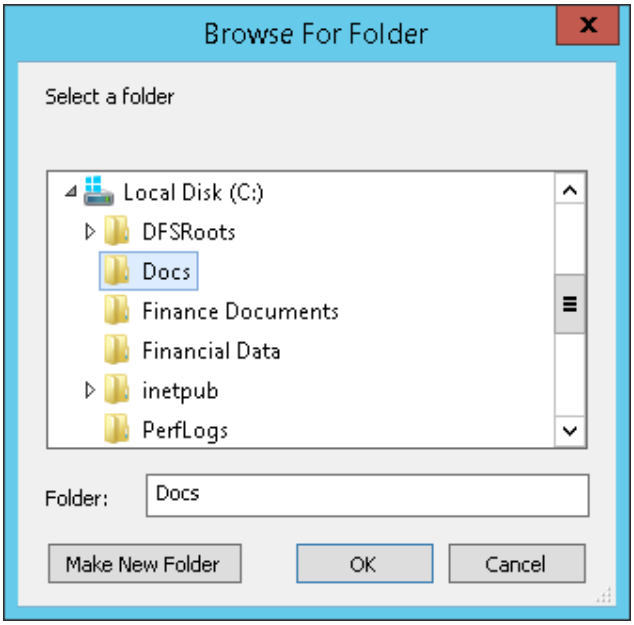

13. Hộp thoại **Create Classification Rule**, trong ô **Rule name**, nhập **Set Confidentiality**.



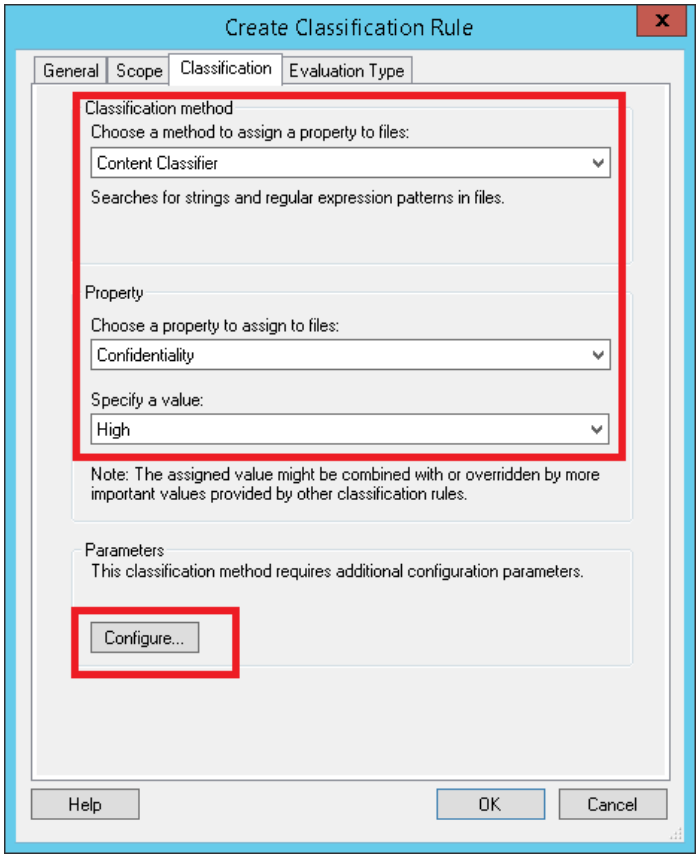
14. Qua tab **Scope**, chọn **Add**.



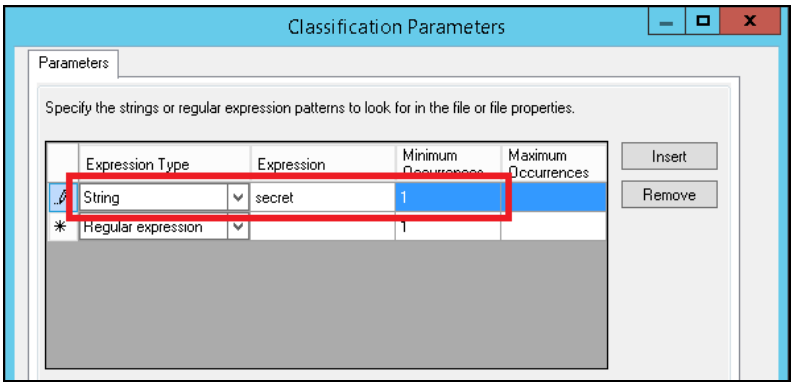

15. Hộp thoại **Browse For Folder**, bung **Local Disk (C:)**, chọn thư mục **Docs**, và chọn **OK**.



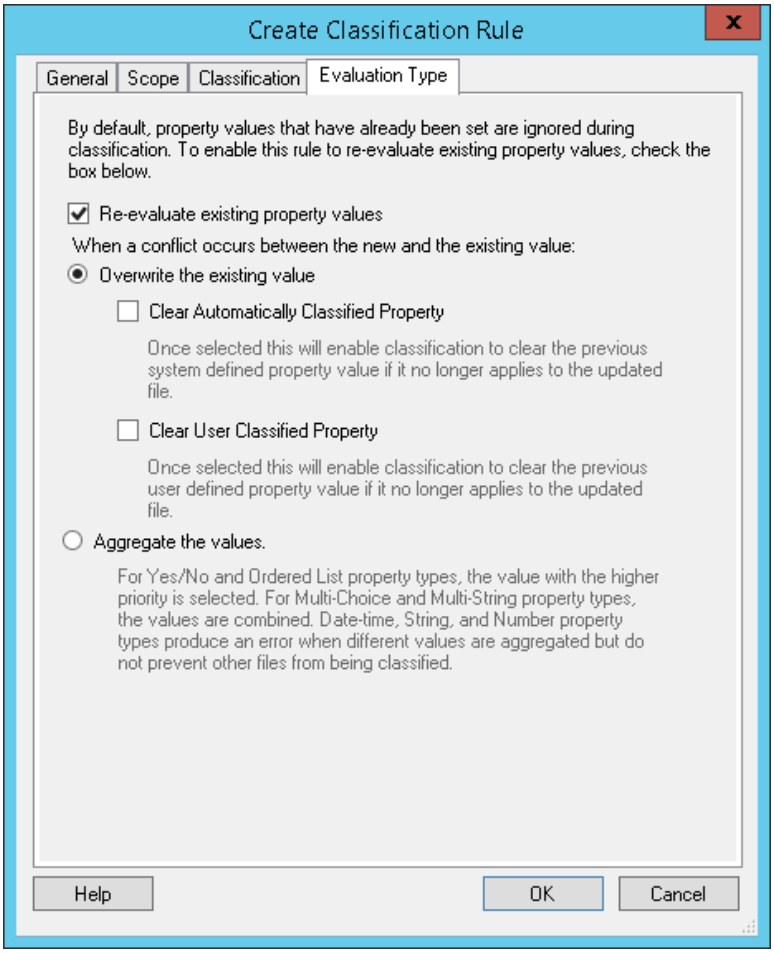
16. Qua tab **Classification**, kiểm tra các thiết lập như trong hình bên dưới, và chọn **Configure**.



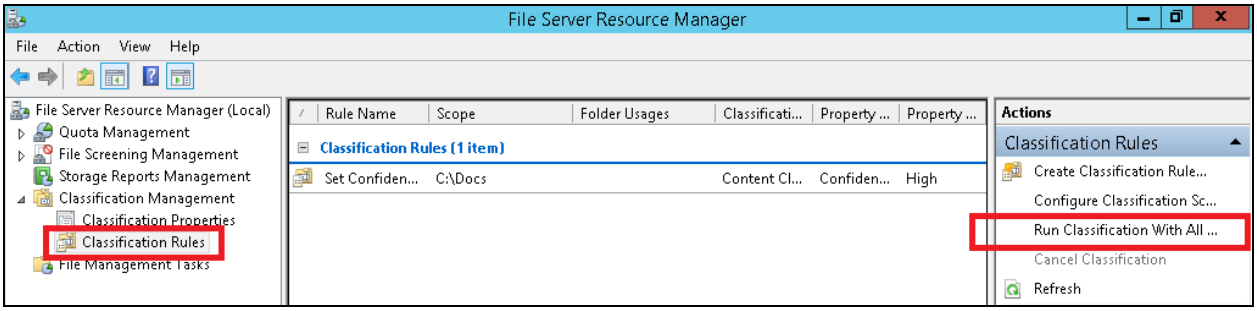

17. Hộp thoại **Classification Parameters,** bung ô **Expression Type,** chọn **String**, trong ô **Expression**, nhập **secret**, và chọn **OK**.



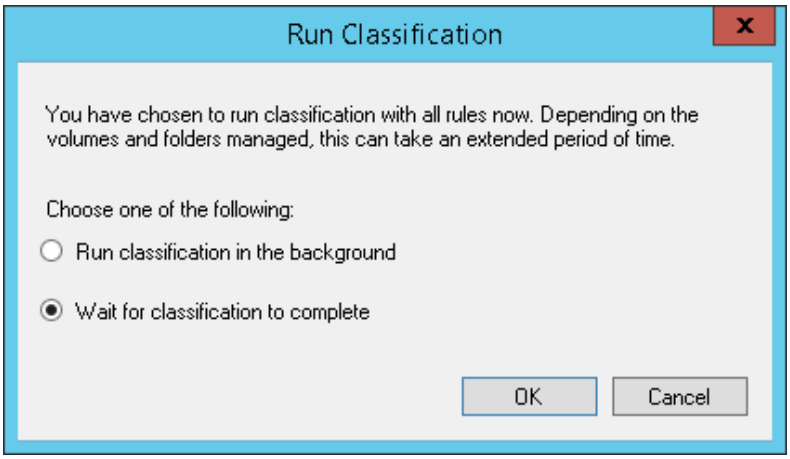
18. Qua tab **Evaluation Type**, đánh dấu chọn **Re-evaluate existing property values**, chọn **Overwrite the existing value**, và chọn **OK**.



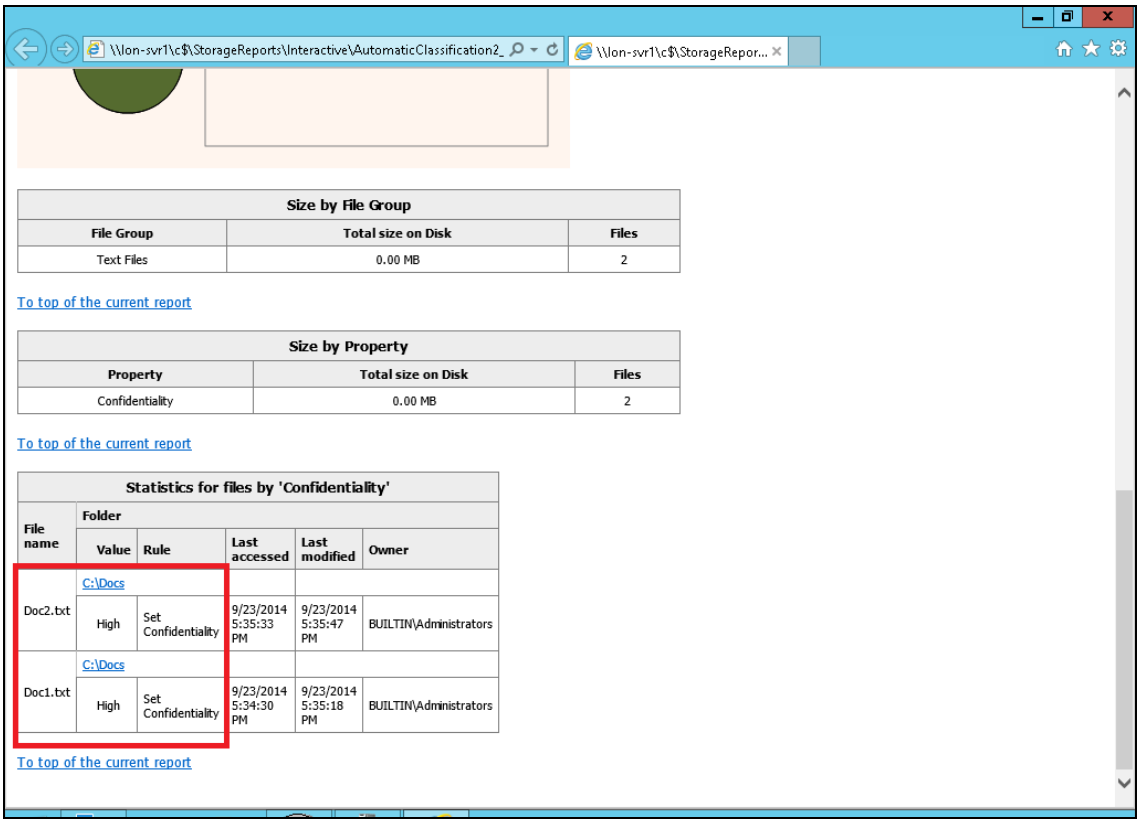

19. Trong cửa sổ **File Server Resource Manager**, chọn **Run Classification with all rules now**.



20. Hộp thoại **Run Classification,** chọn **Wait for classification to complete**, và chọn **OK**.




21. Trong cửa sổ report, kiểm tra 2 file **Doc1.txt** và **Doc2.txt** được thiết lập "**Confidentiality**" . Tắt cửa sổ report.



| Size by File Group | | |
|---|---|---|
| File Group | Total size on Disk | Files |
| Text Files | 0.00 MB | 2 |

To top of the current report

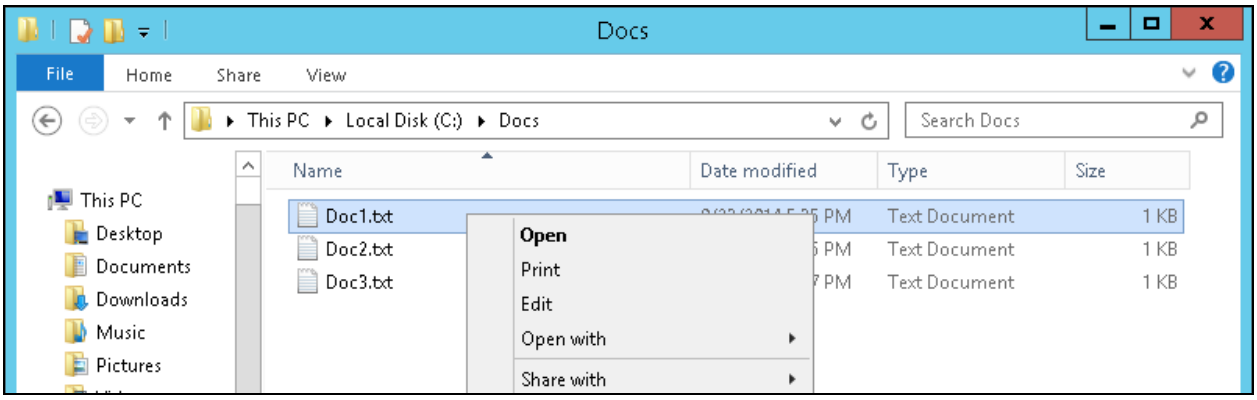
| Size by Property | | |
|---|---|---|
| Property | Total size on Disk | Files |
| Confidentiality | 0.00 MB | 2 |

To top of the current report

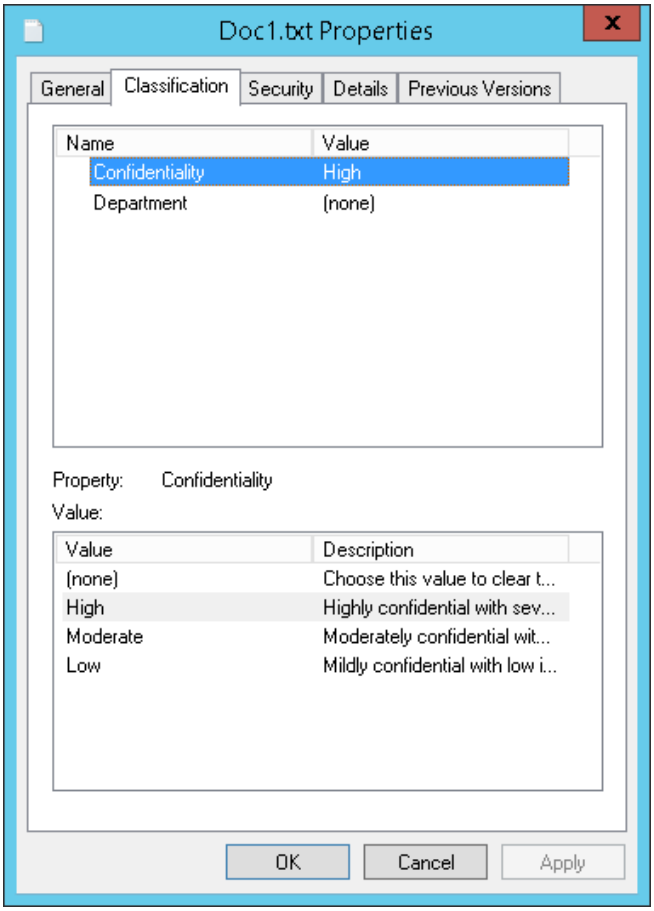
| Statistics for files by 'Confidentiality' | | | | | | |
|---|---|---|---|---|---|---|
| File name | Folder | | | | | |
| | Value | Rule | Last accessed | Last modified | Owner | |
| Doc2.txt | C:\Docs | | | | | |
| | High | Set Confidentiality | 9/23/2014 5:35:33 PM | 9/23/2014 5:35:47 PM | BUILTIN\Administrators | |
| Doc1.txt | C:\Docs | | | | | |
| | High | Set Confidentiality | 9/23/2014 5:34:30 PM | 9/23/2014 5:35:18 PM | BUILTIN\Administrators | |

To top of the current report

22. Mở **File Explorer**, vào thư mục **C:\Docs,** chuột phải **Doc1.txt**, chọn **Properties**.

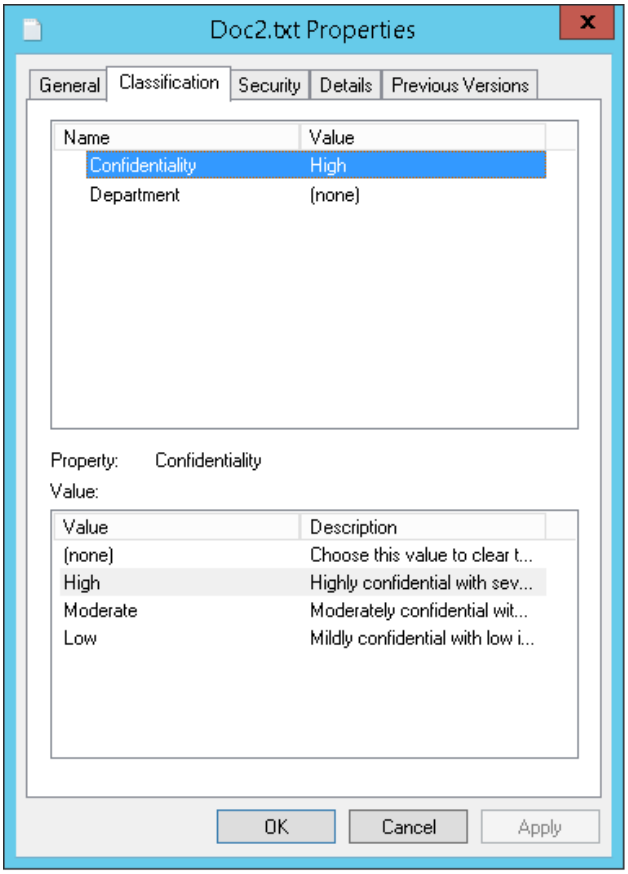


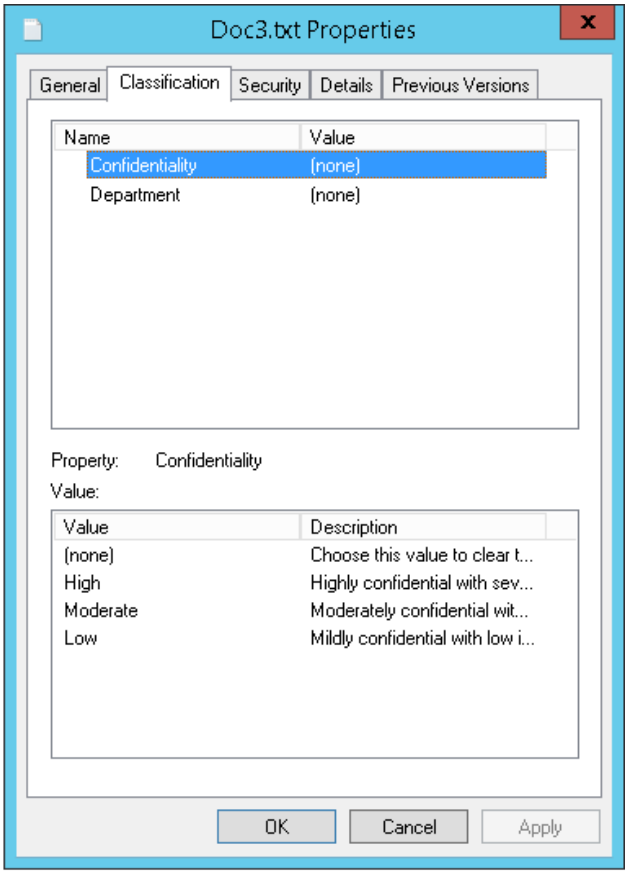

23. Hộp thoại **Doc1.txt Properties**, qua tab **Classification**, kiểm tra **Confidentiality** là **High**.



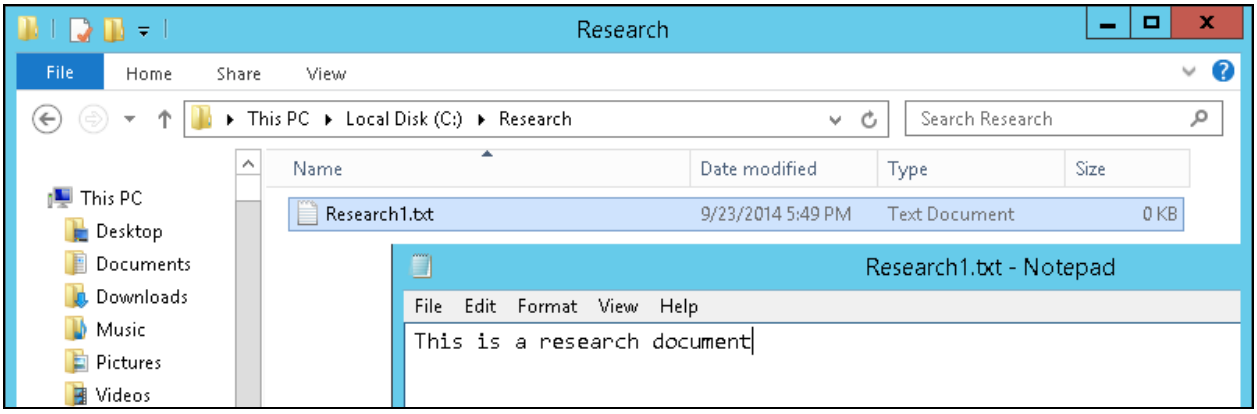
24. Lặp lại bước 22 và 23 trên file **Doc2** and **Doc3**.

**Chú ý: Trên file Doc1.txt và Doc2.txt thiết lập Confidentiality là High, file Doc3.txt không thiết lập confidentiality. Bởi vì trong nội dung của file Doc3.txt không có chữ *secret*.**

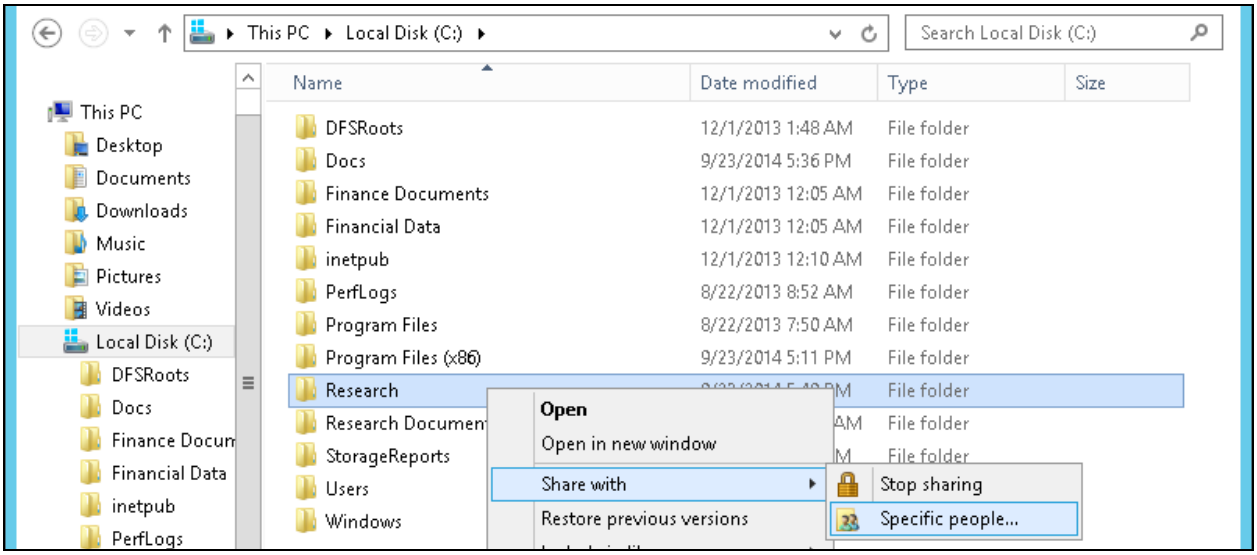


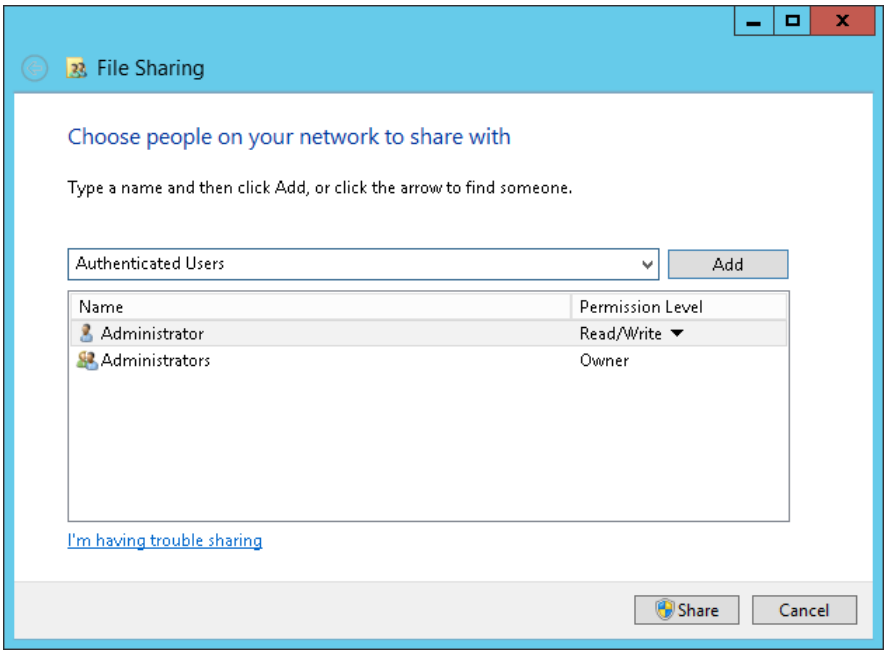
25. Trong cửa sổ **File Explorer**, vào ổ đĩa **C:**, tạo một thư mục mới, đặt tên **Research**. Trong thư mục **Research**, tạo file text tên **Research1.txt** có nội dung là "**This is a research document**"



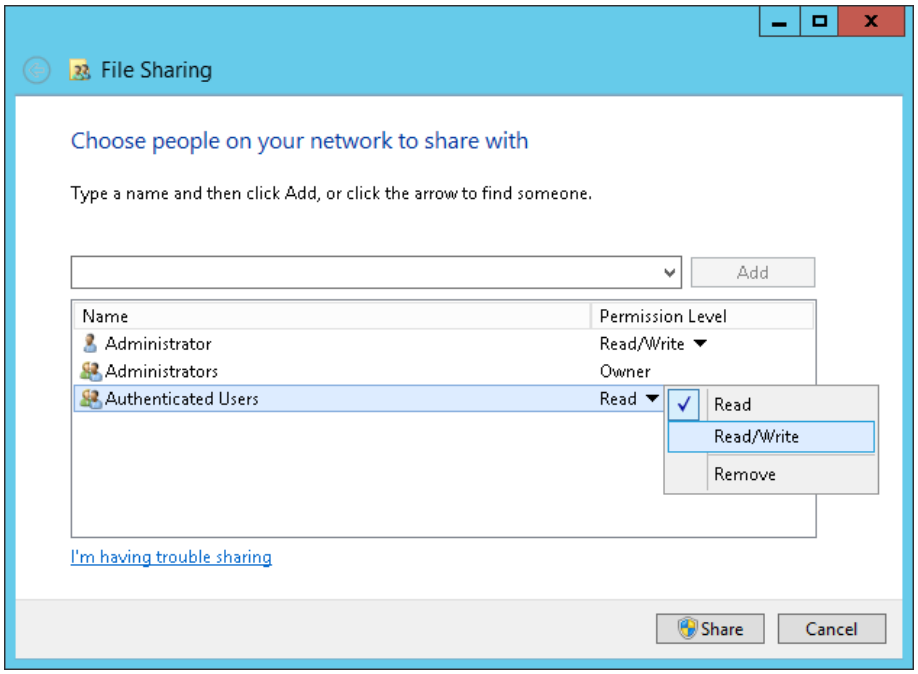

26. Chuột phải thư mục **Research**, chọn **Share with**, chọn **Specific people**.



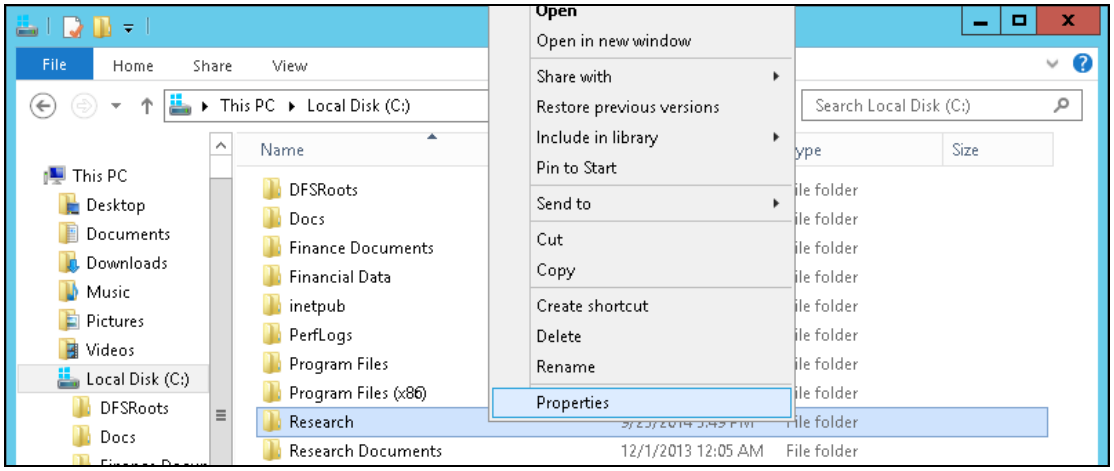
27. Hộp thoại **File Sharing**, nhập **Authenticated Users,** và chọn **Add**.



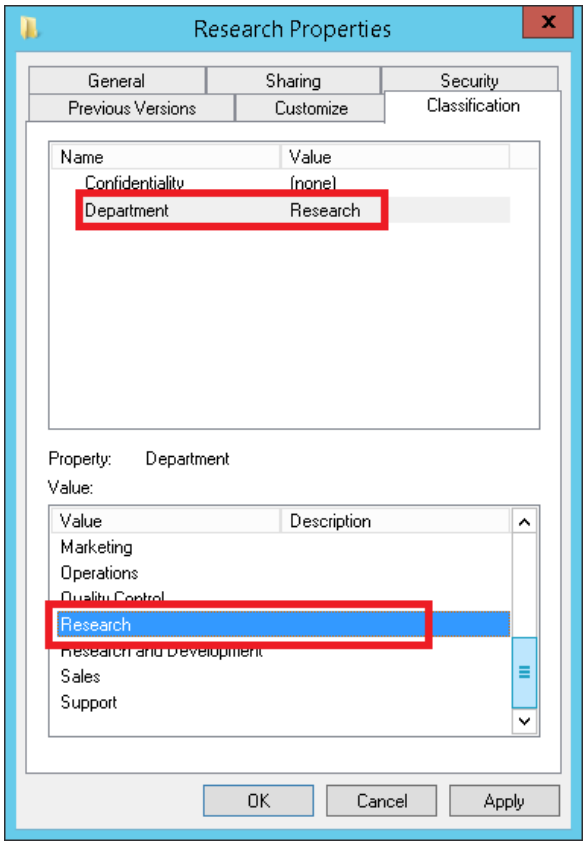

28. Chọn **Authenticated Users**, bung ô **Permission Level**, chọn **Read/Write**, chọn **Share**, và chọn **Done**.



29. Trong cửa sổ File Explorer, chuột phải thư mục **Research**, chọn **Properties**.




30. Hộp thoại **Research Properties**, qua tab **Classification**, chọn **Department**, trong phần **Value**, chọn **Research**, chọn **Apply**, và chọn **OK**.



**Kết quả: Sau khi hoàn thành bài tập này, bạn đã thực hiện các bước chuẩn bị để triển khai DAC.**

## Bài tập 2: Triển khai DAC.

Bước tiếp theo trong việc thực hiện DAC là cấu hình Central Access Rules và Central Access Policy để liên kết các Claims và Property Definitions. Bạn sẽ cấu hình các rule cho DAC để giải quyết yêu cầu của A. Datum. Sau khi bạn cấu hình các DAC Rules và DAC Policy, bạn sẽ áp dụng các policy này cho File Server.

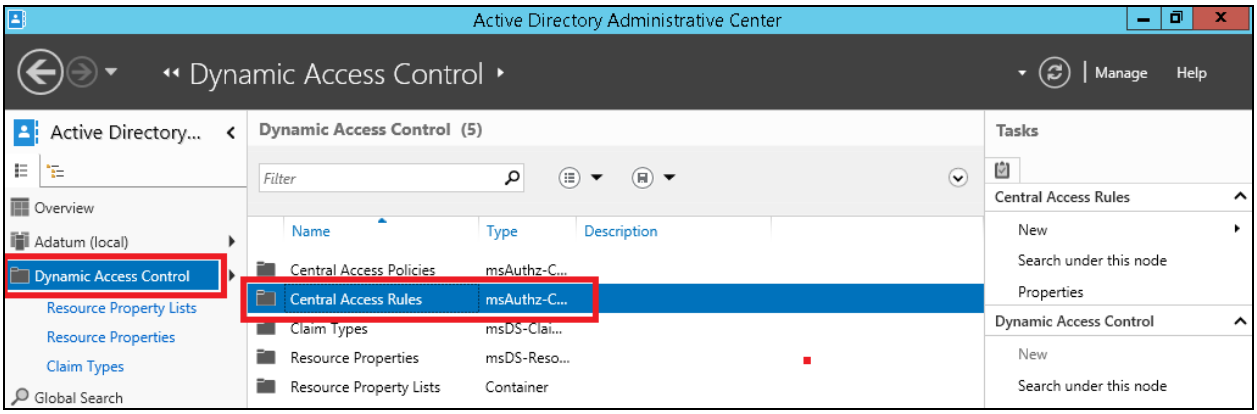
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Central Access Policy Rules.
2. Tạo và công bố Central Access Policy.
3. Áp dụng Central Access Policy.

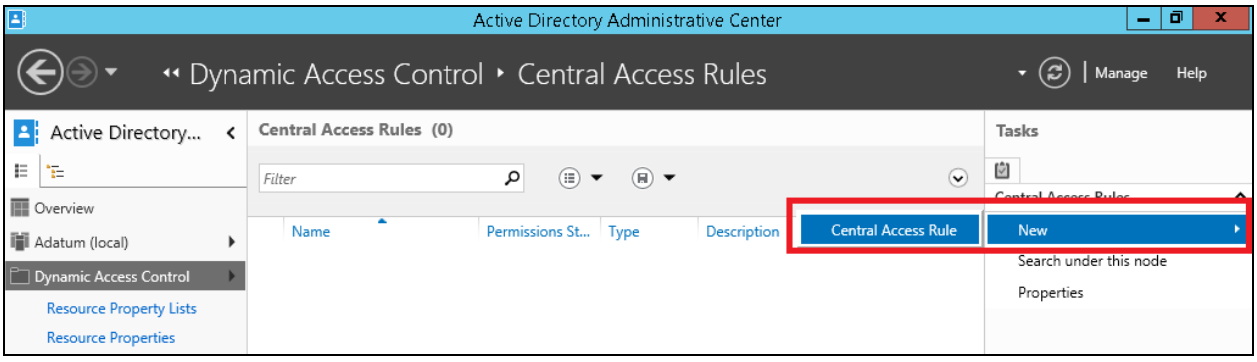
❖ **Thực hành:**

### Bước 1: Cấu hình Central Access Policy Rules.

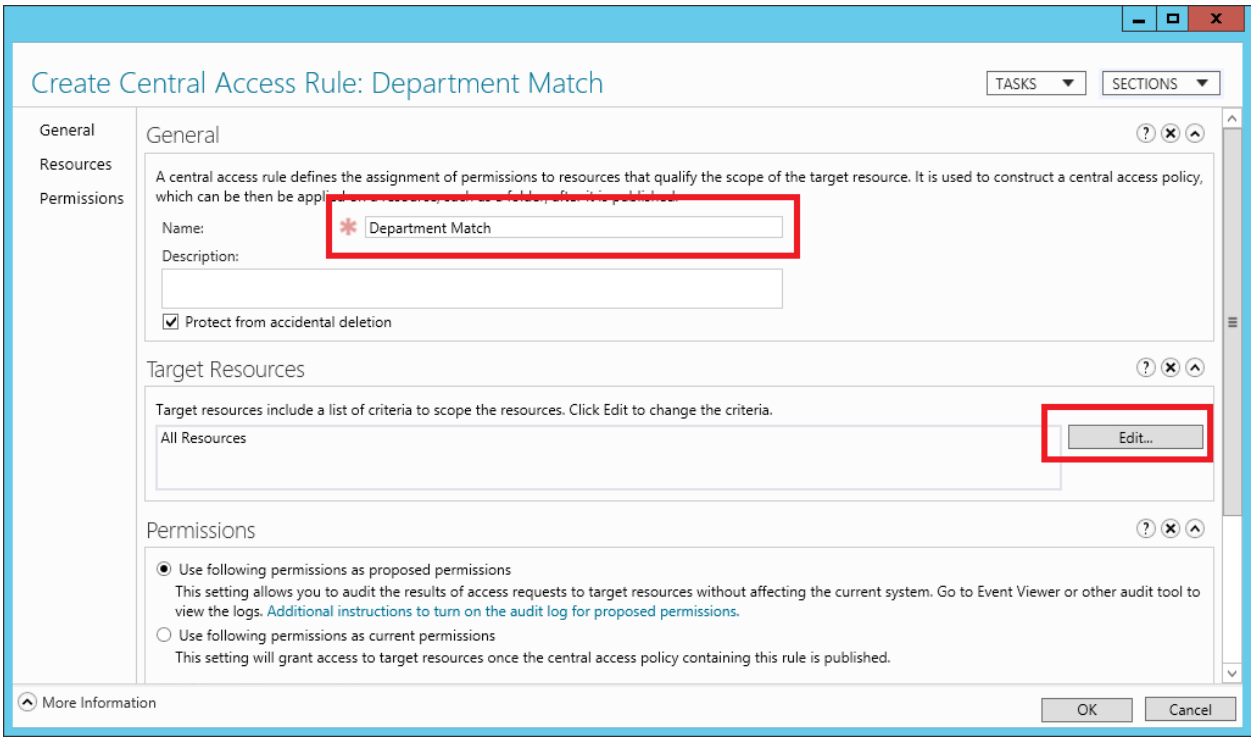
1. Qua máy **LON-DC1**. Trong **Server Manager**, bung menu **Tools**, mở **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Central Access Rules**.



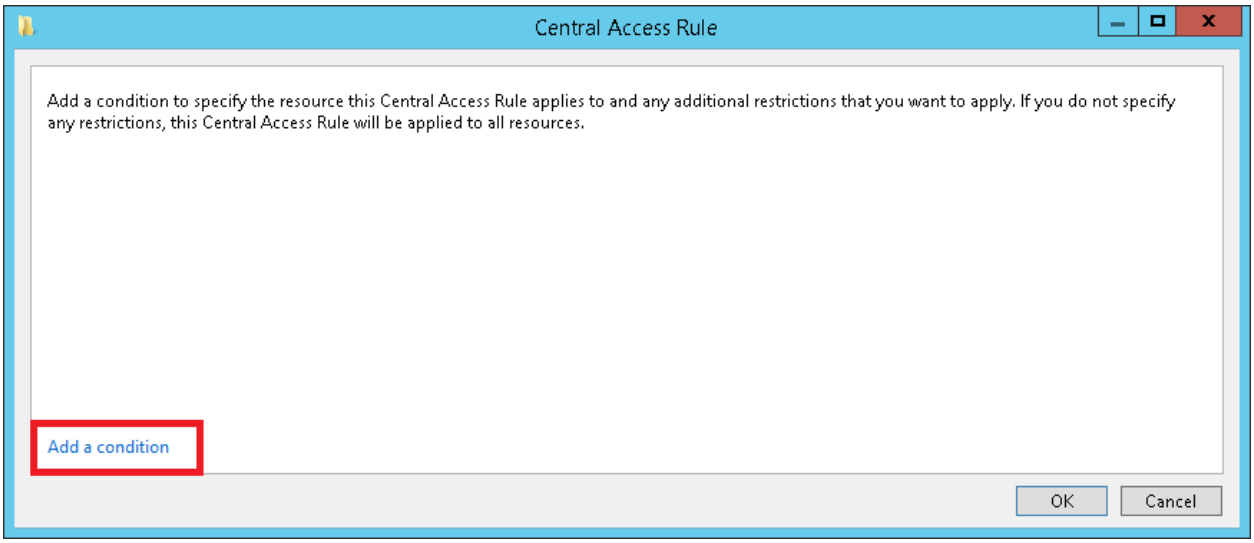
2. Trong cửa sổ **Tasks**, chọn **New**, và chọn **Central Access Rule**.



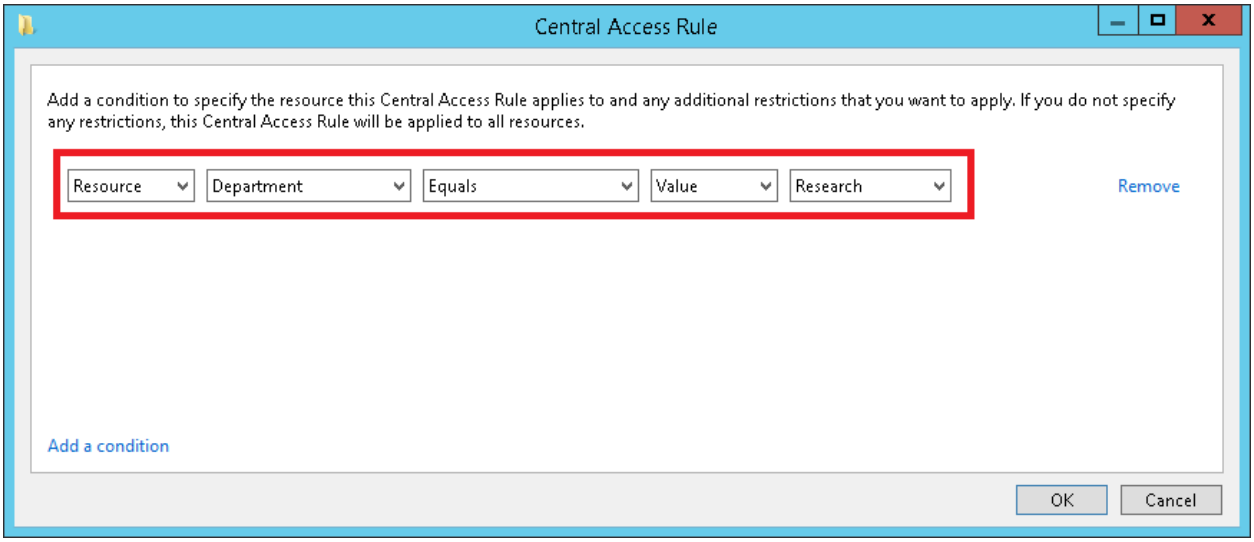

3. Cửa sổ **Create Central Access Rule**, trong ô **Name**, nhập **Department Match**, trong phần **Target Resources**, chọn **Edit**.



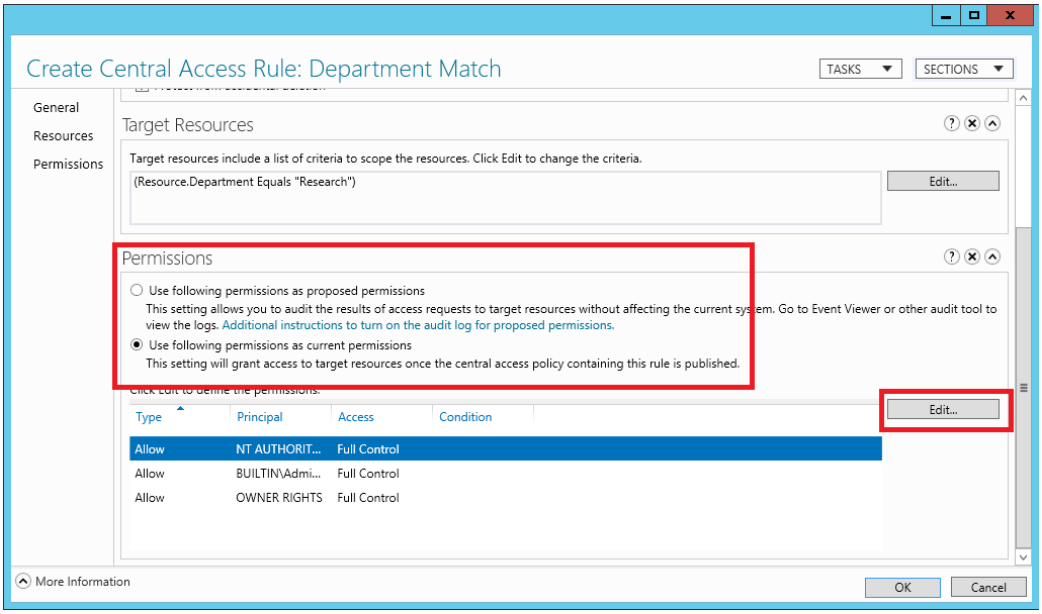
4. Cửa sổ **Central Access Rule**, chọn **Add a condition**.



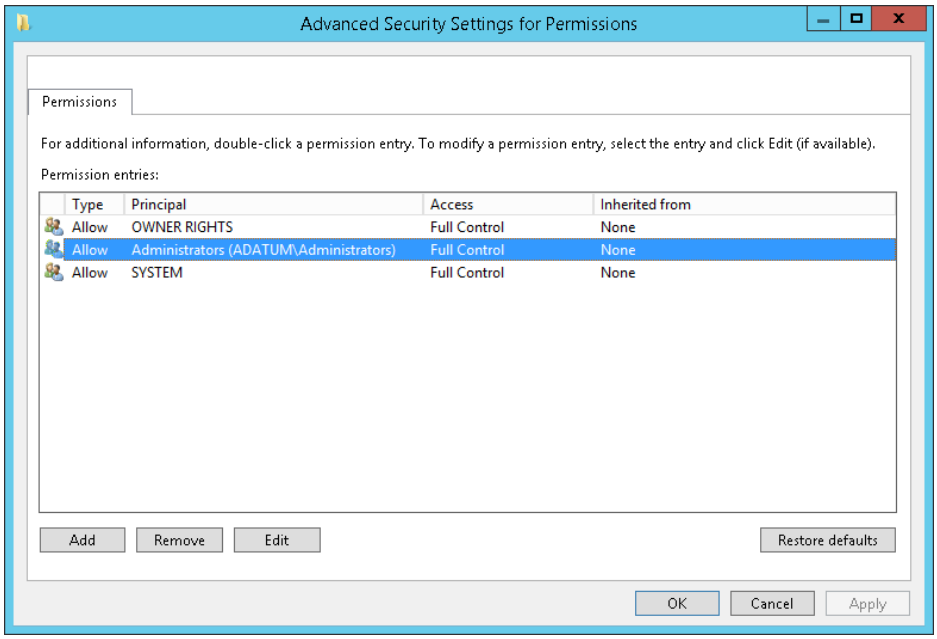

5. Thiết lập condition như trong hình bên dưới: **Resource-Department-Equals-Value-Research**. Chọn **OK**.



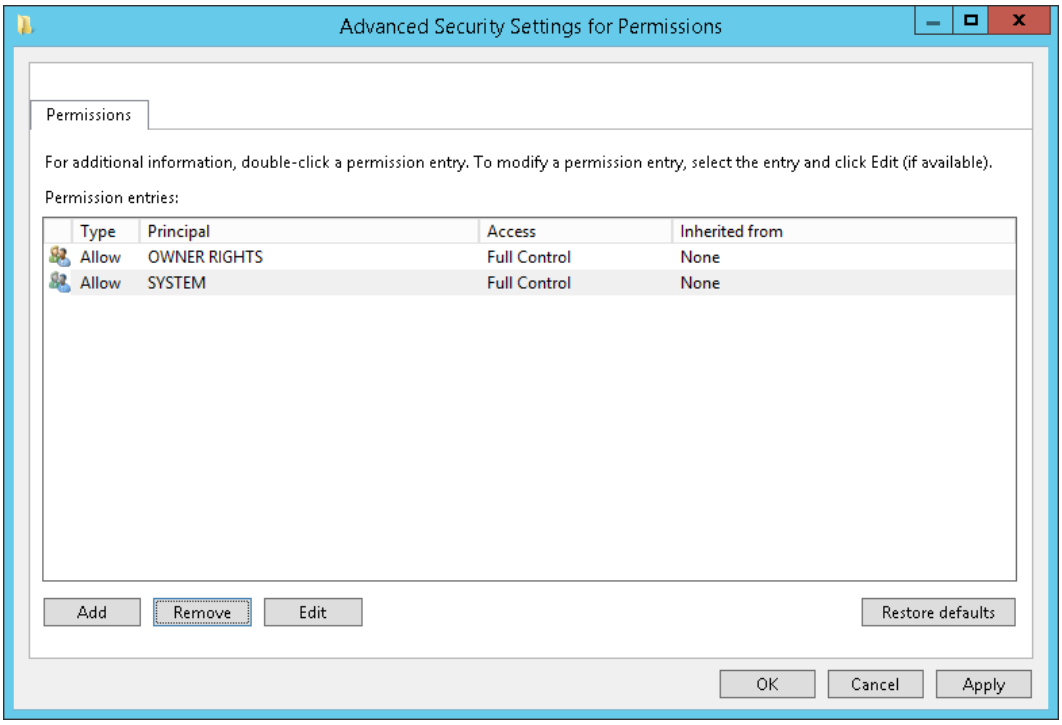
6. Kéo thanh trượt xuống phần **Permissions**, chọn **Use following permissions as current permissions**, chọn **Edit**.



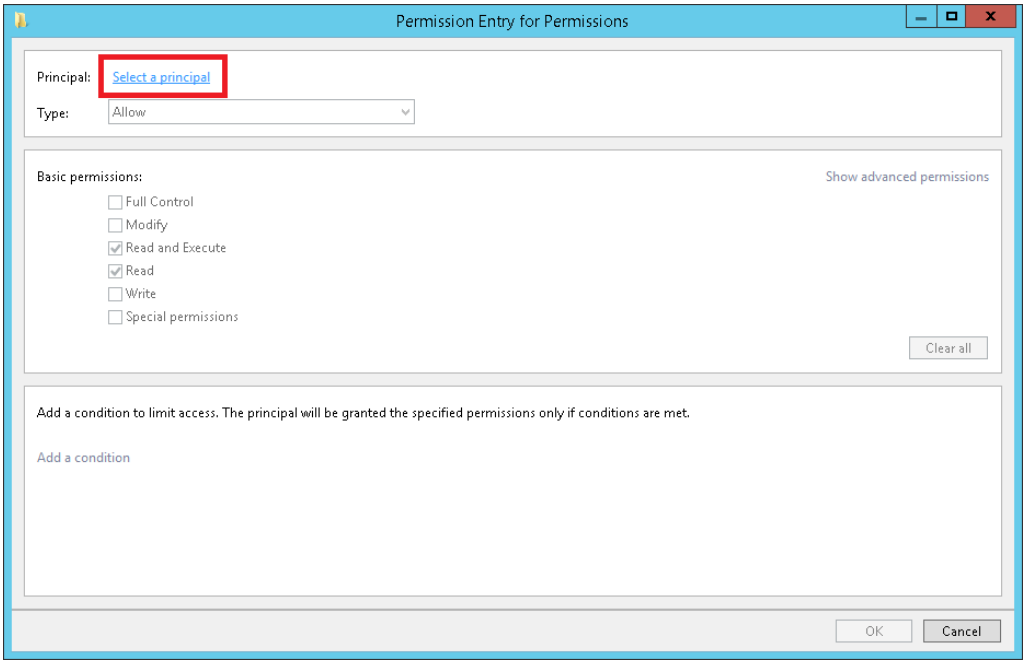

7. Cửa sổ **Advanced Security Settings for Permisssion**, chọn **Administrators (ADATUM\Administrators)**, và chọn **Remove**.



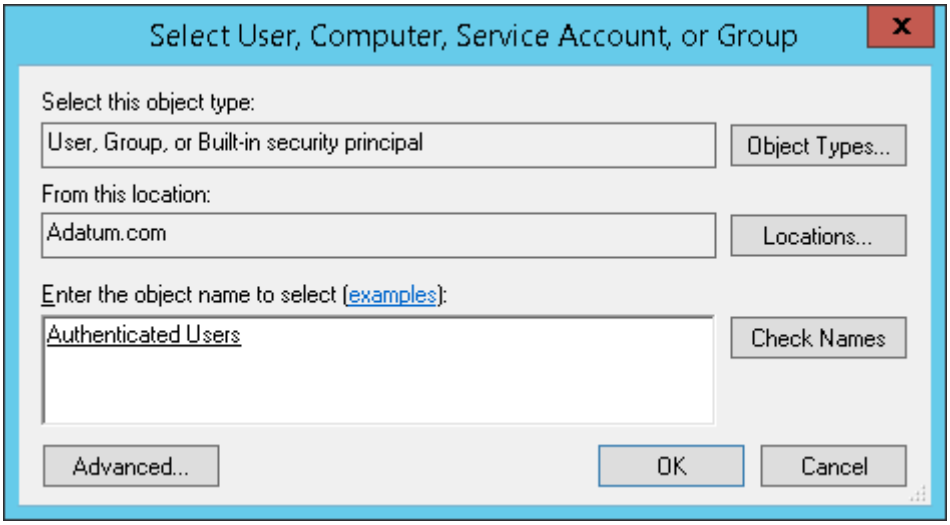
8. Cửa sổ **Advanced Security Settings for Permissions**, chọn **Add**.



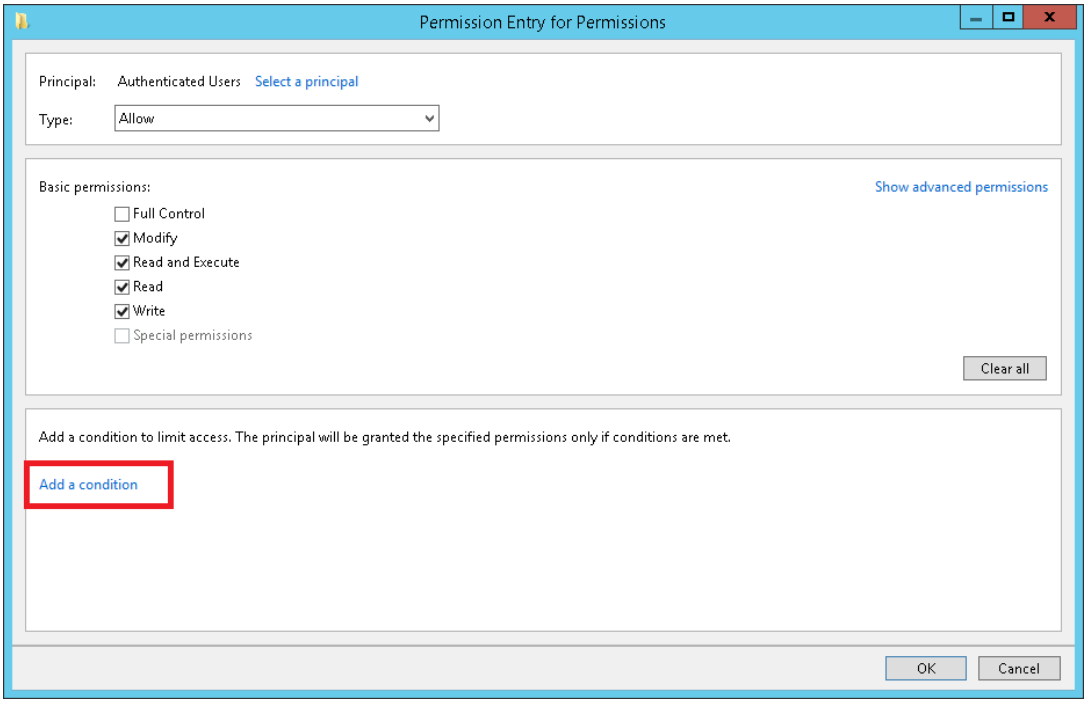

9. Cửa sổ **Permission Entry for Permissions**, chọn **Select a principal**.



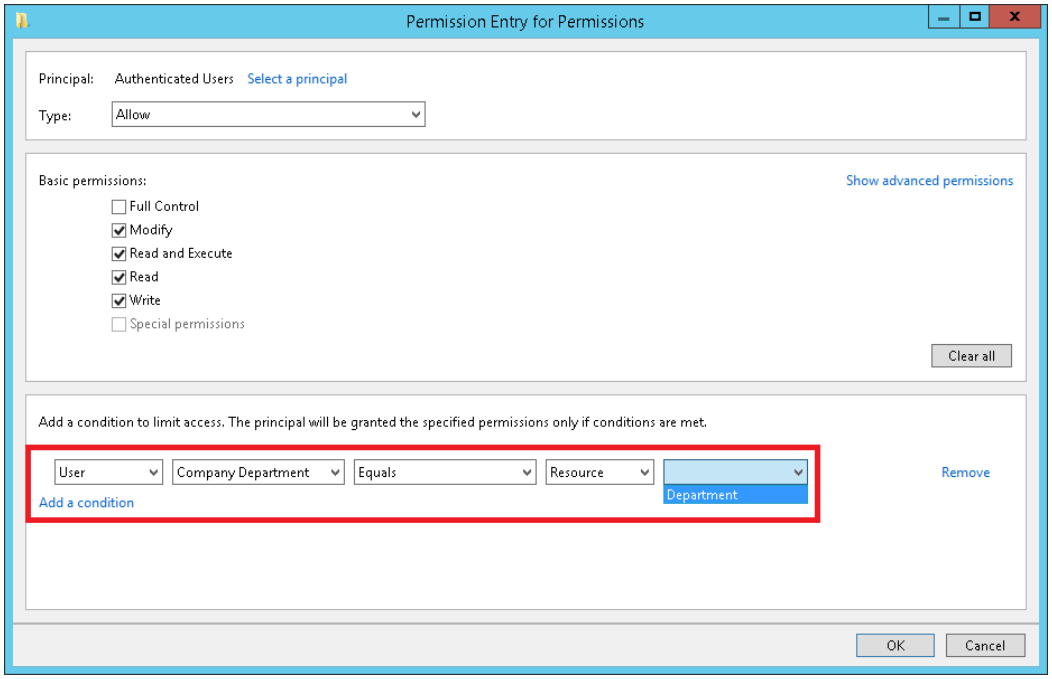
10. Hộp thoại **Select User, Computer, Service Account or Group**, nhập **Authenticated Users**, chọn **Check Names**, và chọn **OK**.



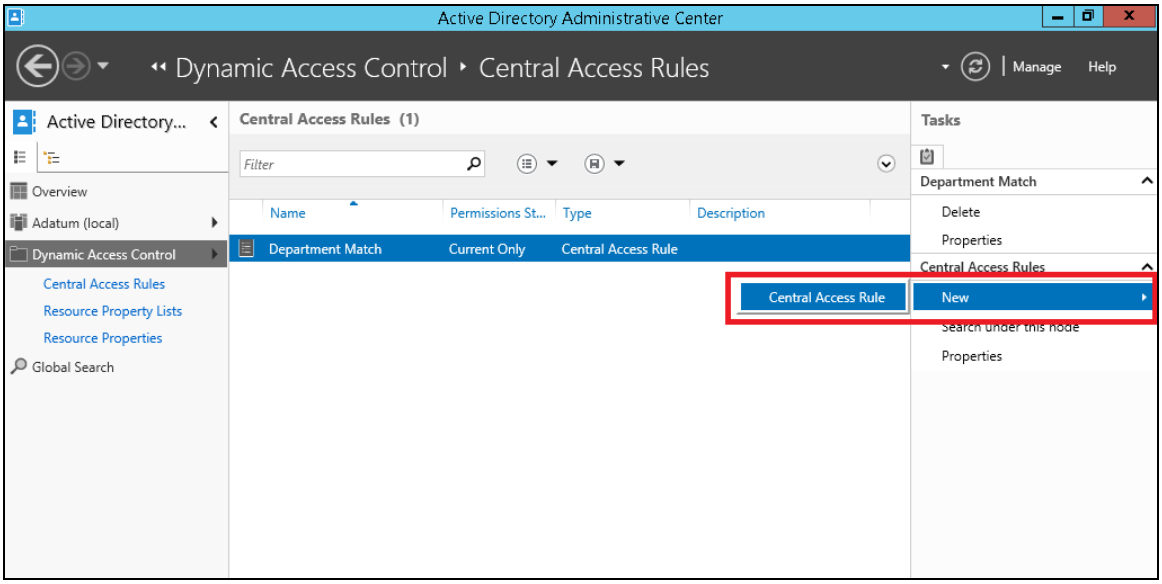

11. Trong phần **Basic permissions**, đánh dấu chọn **Modify**, **Read and Execute**, **Read**, và **Write**, chọn **Add a condition**.



12. Thiết lập conditions như hình bên dưới : **User-Company Department- Equals-Resource-Department**. Chọn **OK** 3 lần.

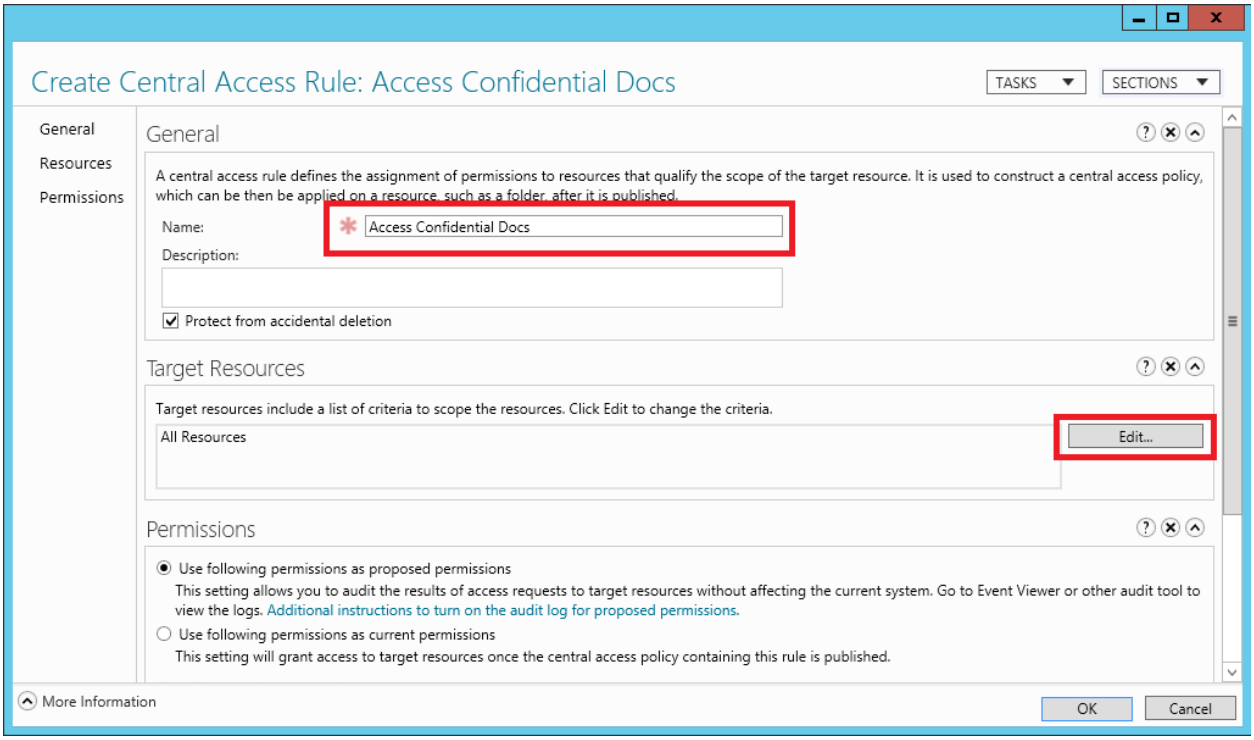



13. Cửa sổ **Active Directory Administrative Center,** chọn **New**, và chọn **Central Access Rule**.

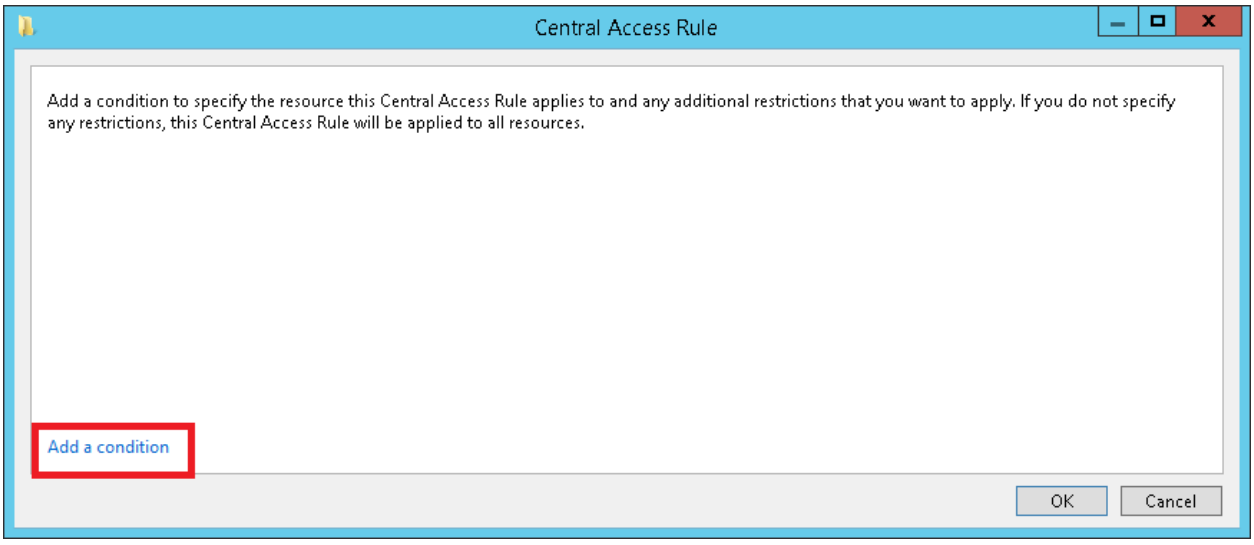


14. Cửa sổ **Create Central Access Rule,** trong ô **Name**, nhập **Access Confidential Docs**.

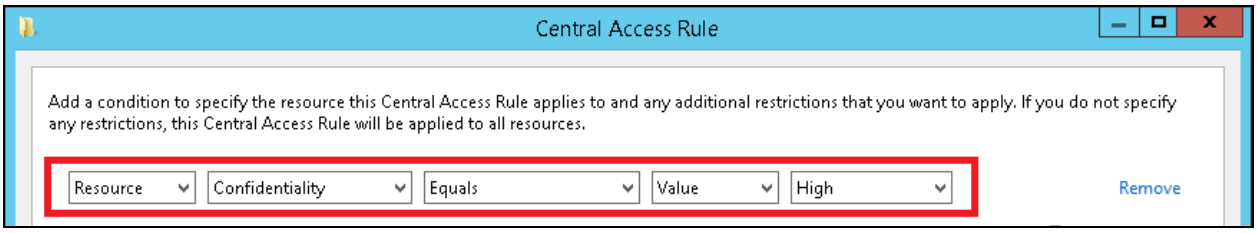
Trong phần **Target Resources**, chọn **Edit**.



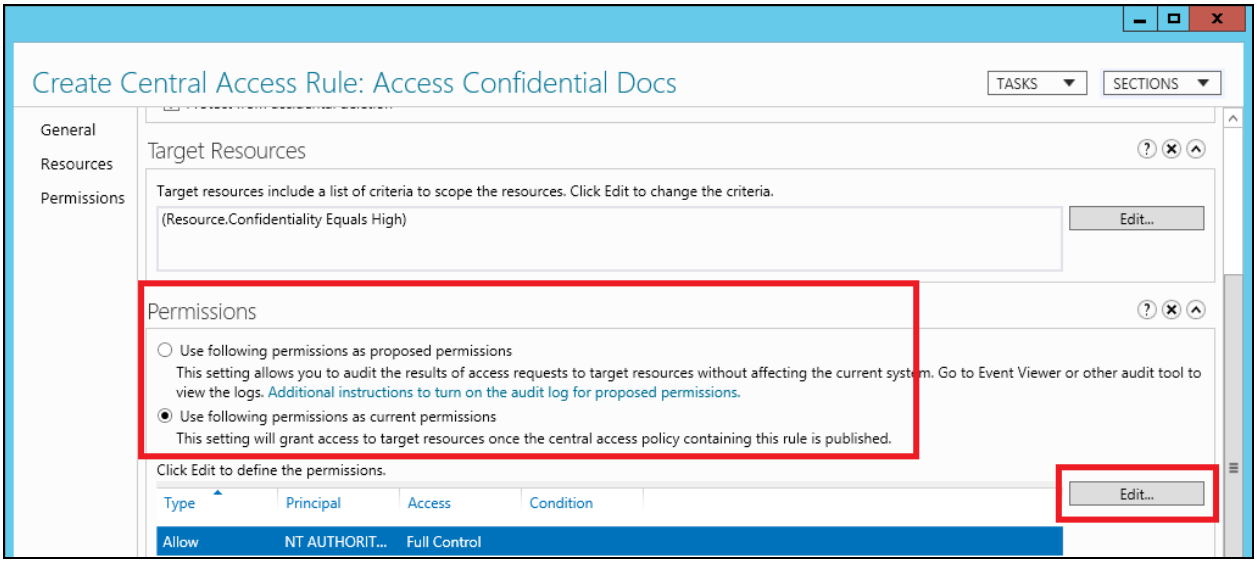

15. Cửa sổ **Central Access Rule**, chọn **Add a condition**.



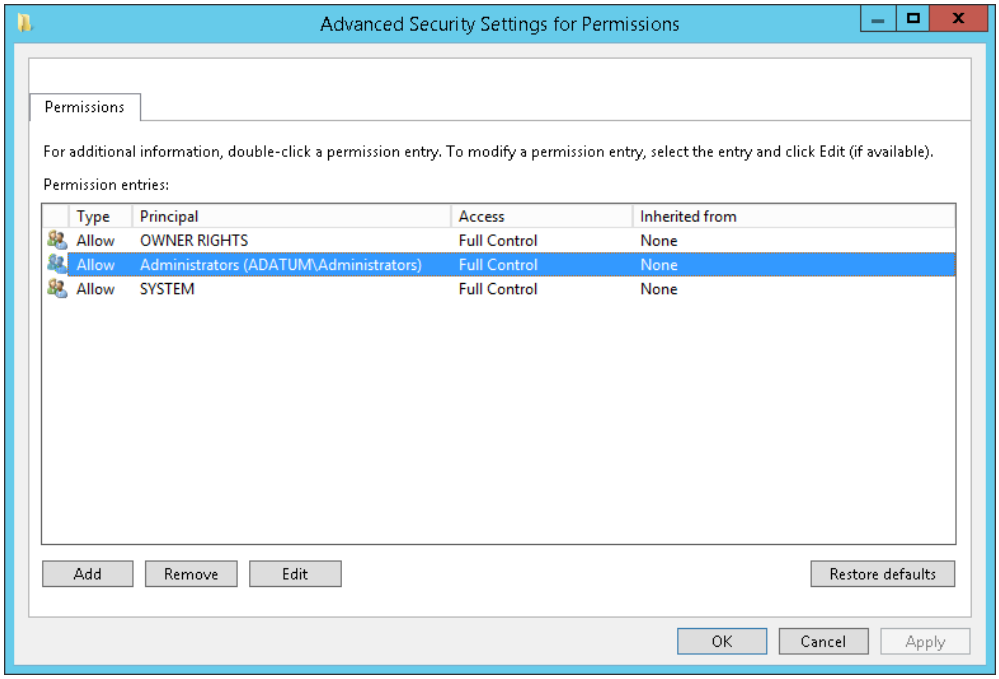
16. Bung ô cuối cùng, chọn **High**. Kiểm tra conditions thiết lập như sau: **Resource-Confidentiality- Equals-Value-High.** Chọn **OK**.



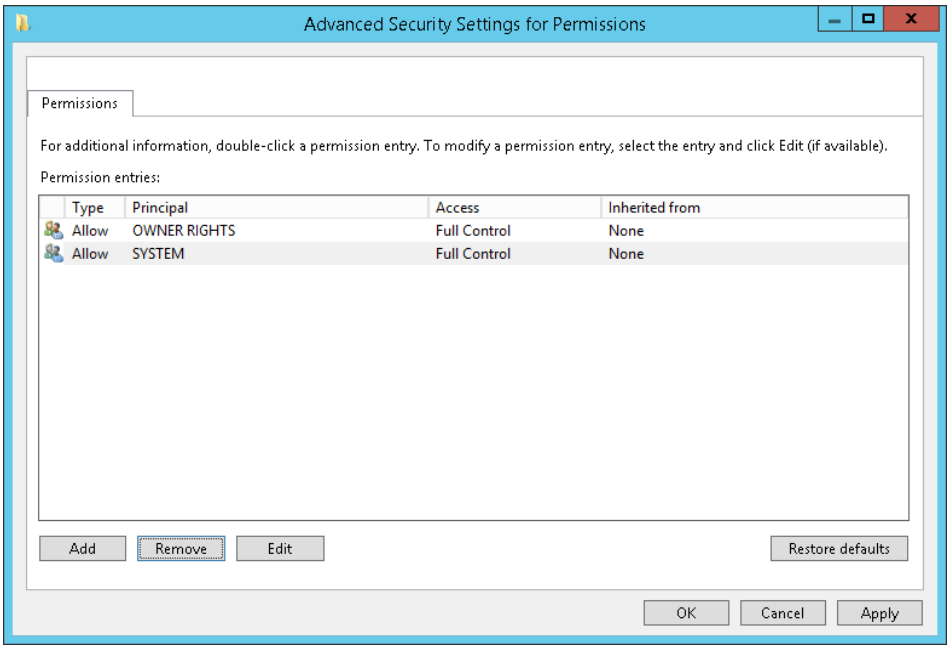

17. Kéo thanh trượt xuống phần **Permissions**, chọn **Use following permissions as current permissions**, và chọn **Edit**.



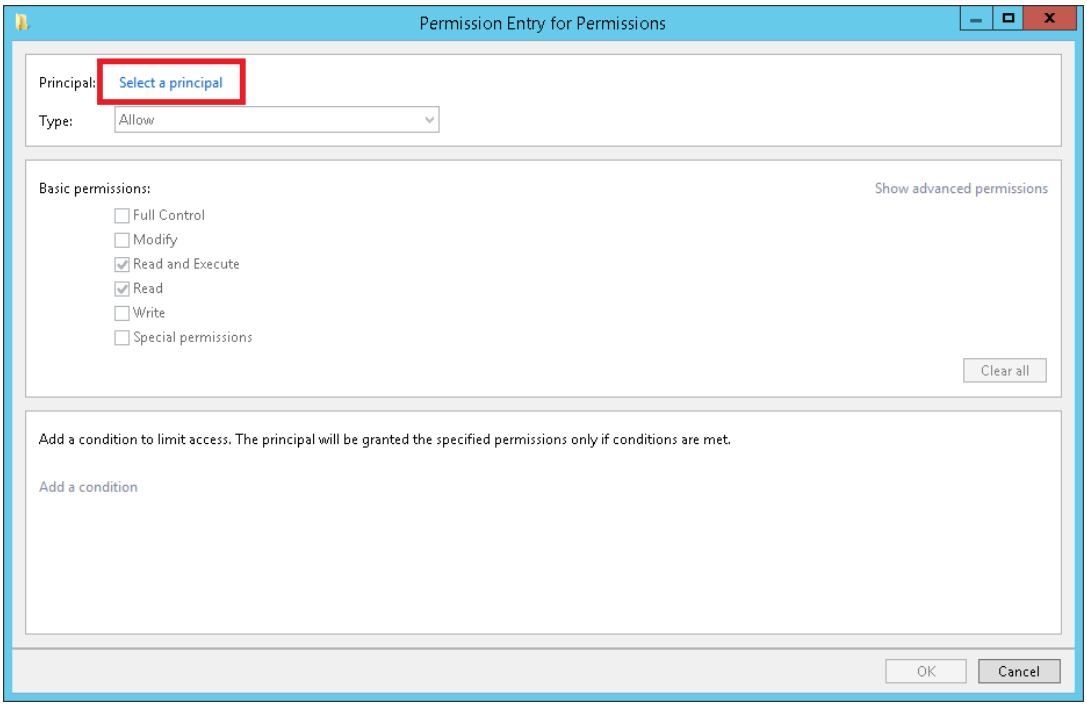
18. Cửa sổ **Advanced Security Settings for Permisssion,** chọn **Administrators (ADATUM\Administrators)**, và chọn **Remove**.



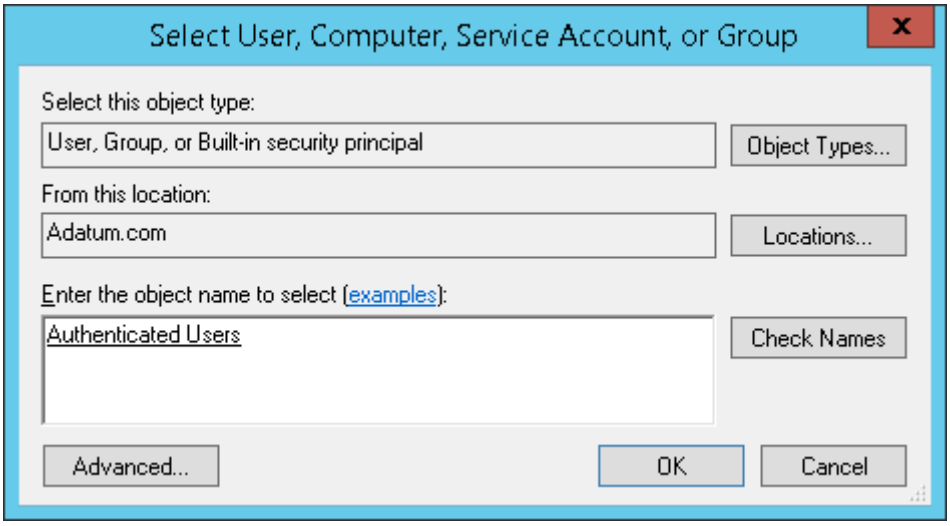

19. Cửa sổ **Advanced Security Settings for Permissions**, chọn **Add**.



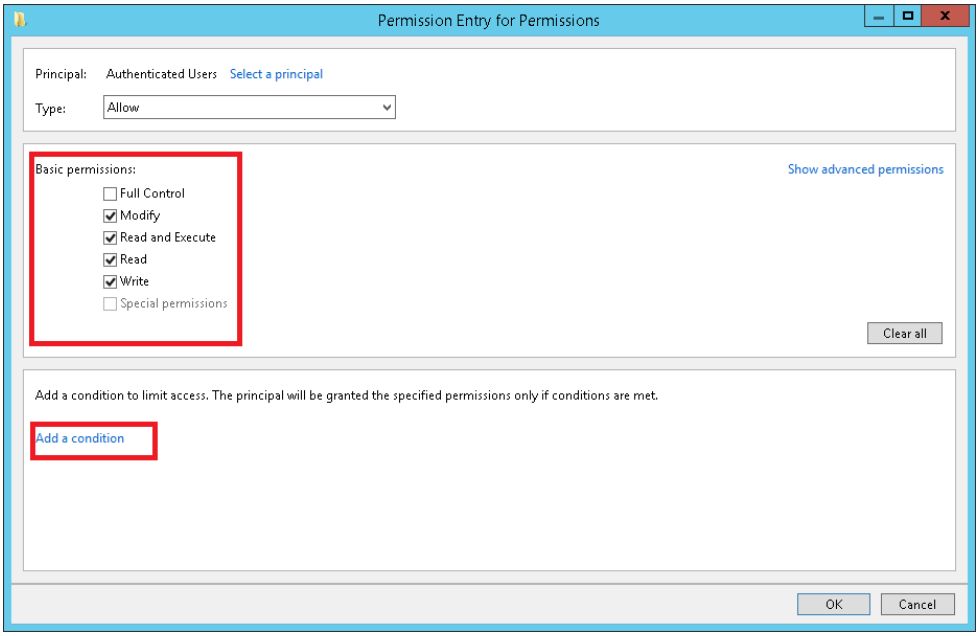
20. Cửa sổ **Permission Entry for Permissions**, chọn **Select a principal**.



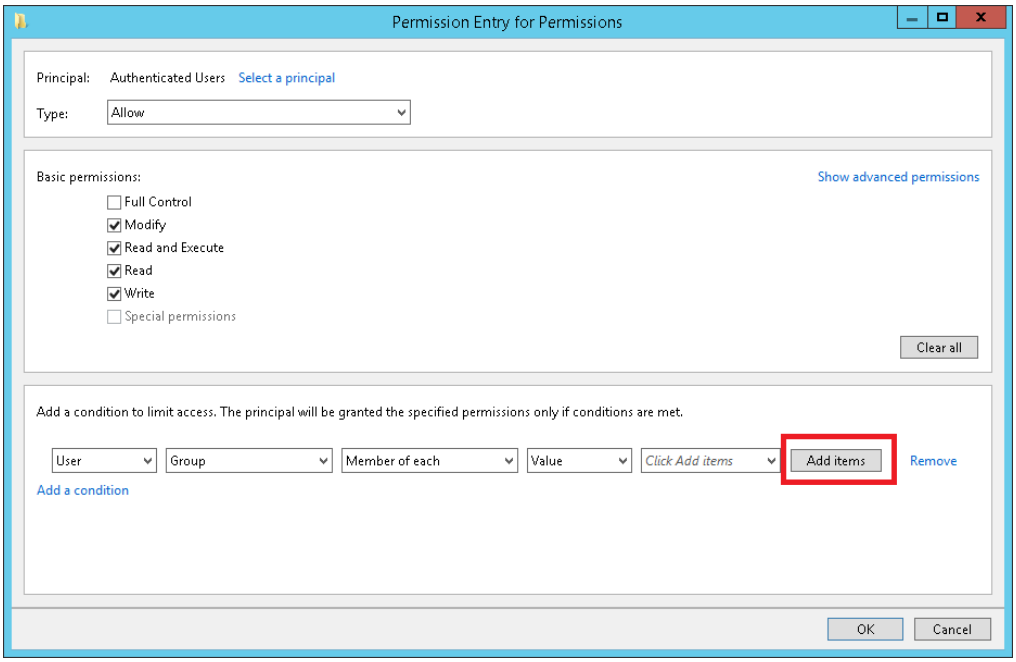

21. Hộp thoại **Select User, Computer, Service Account or Group**, nhập **Authenticated Users**, chọn **Check Names**, và chọn **OK**.



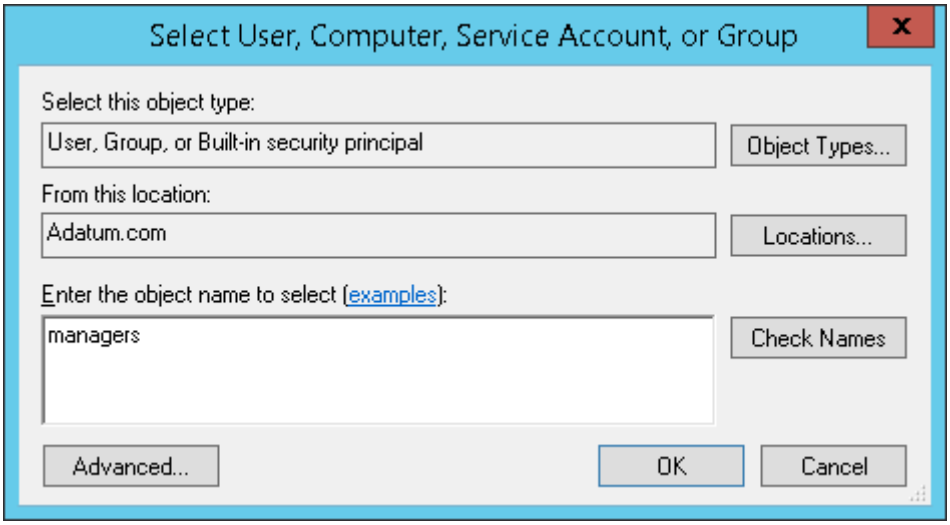
22. Trong phần **Basic permissions**, đánh dấu chọn **Modify**, **Read and Execute**, **Read**, và **Write**, chọn **Add a condition**.



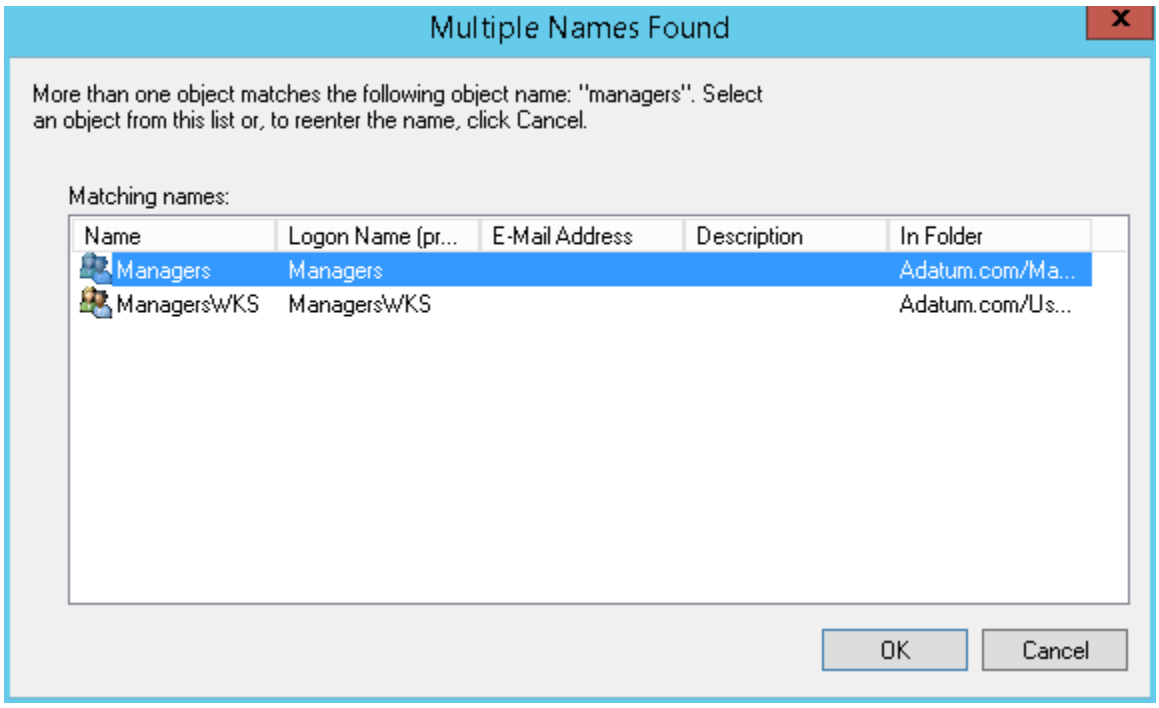

23. Chọn **Add items**.



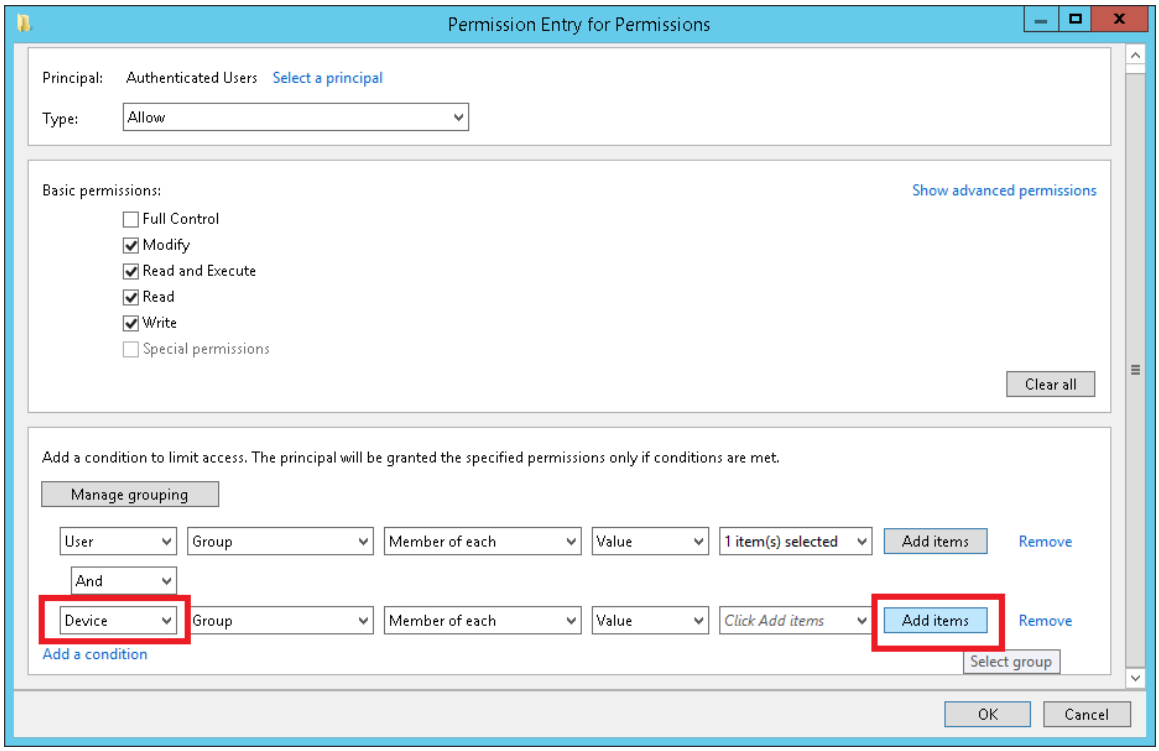
24. Hộp thoại **Select User, Computer, Service Account or Group**, nhập **Managers,** chọn **OK**.



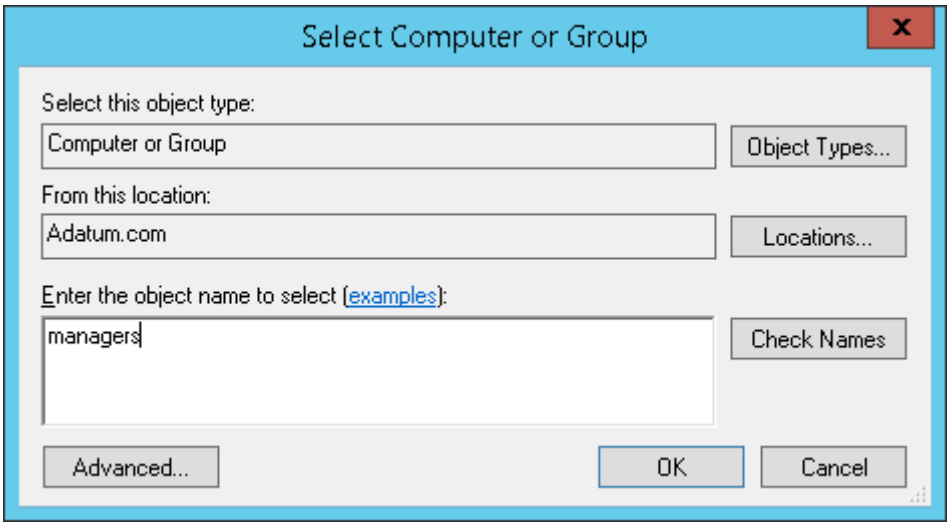

25. Hộp thoại **Multiple Names Found**, chọn group **Managers**, và chọn **OK**.



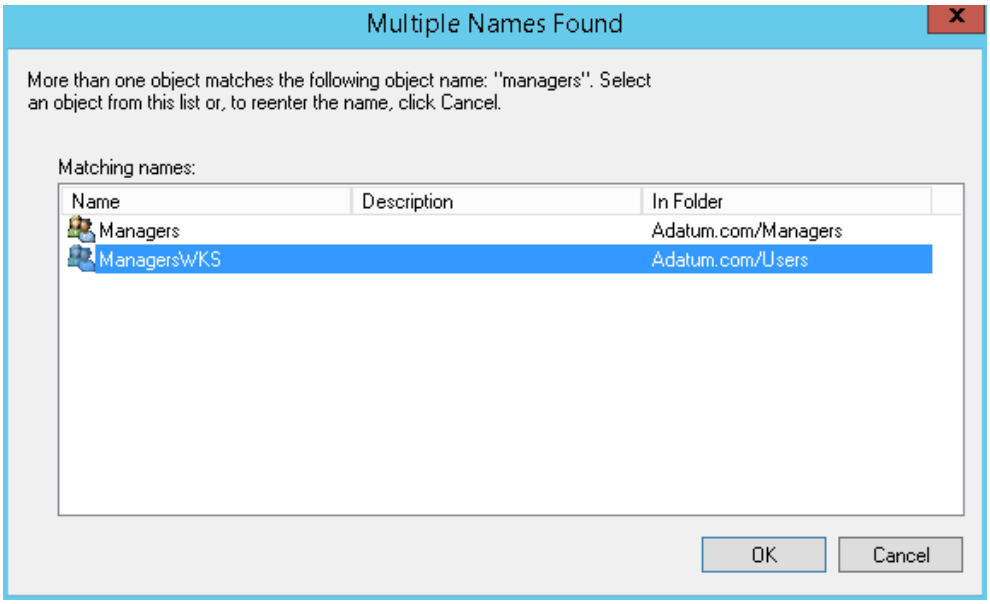
26. Chọn **Add a condition**, và chọn **Add items** ở dòng dưới.



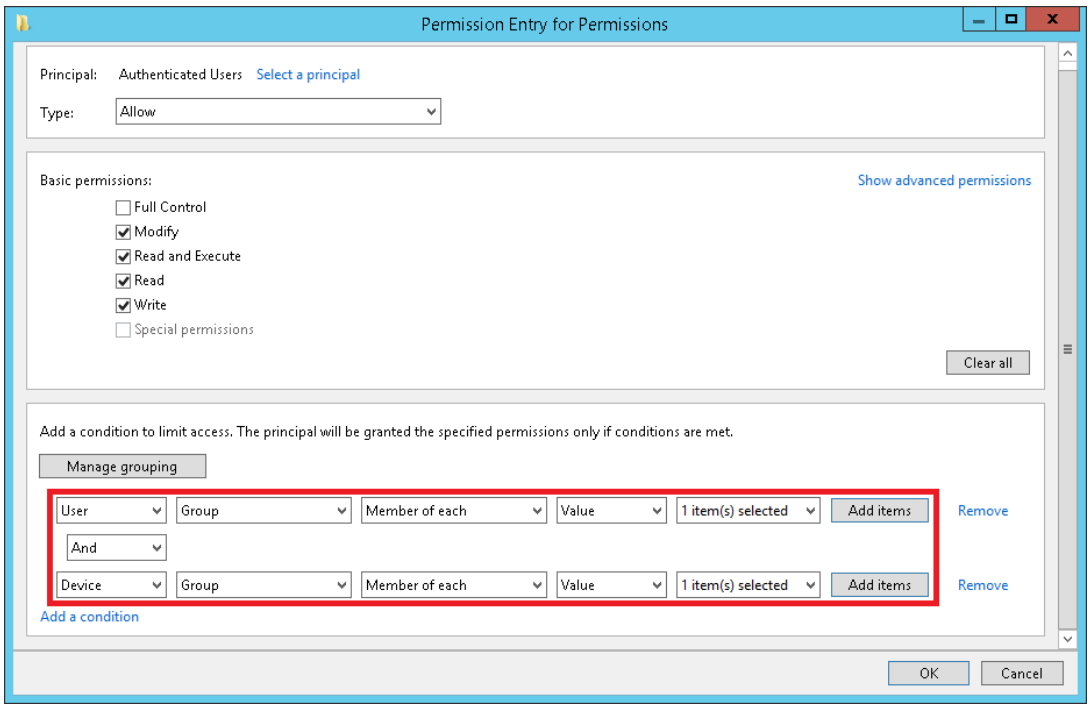

27. Hộp thoại **Select User, Computer, Service Account or Group**, nhập **Managers**, và chọn **OK**.



28. Hộp thoại **Multiple Names Found**, chọn group **ManagersWKS**, chọn **OK**.

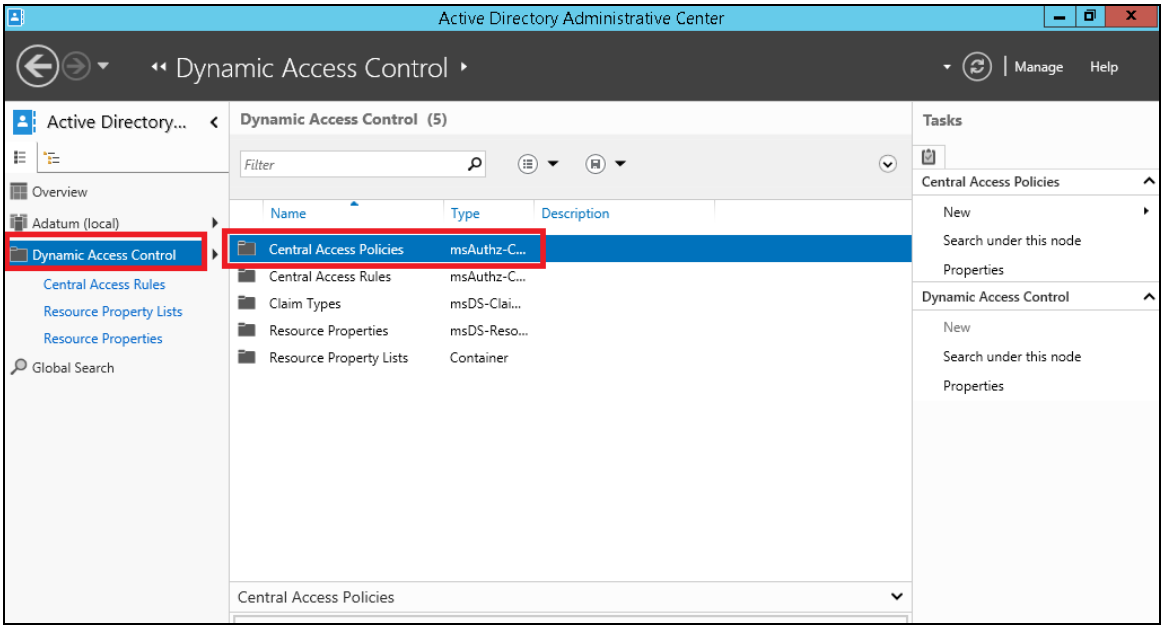



29. Thiết lập condition của dòng thứ 2 như sau: **Device-Group-Member of each-Value-**. Chọn **OK** 3 lần

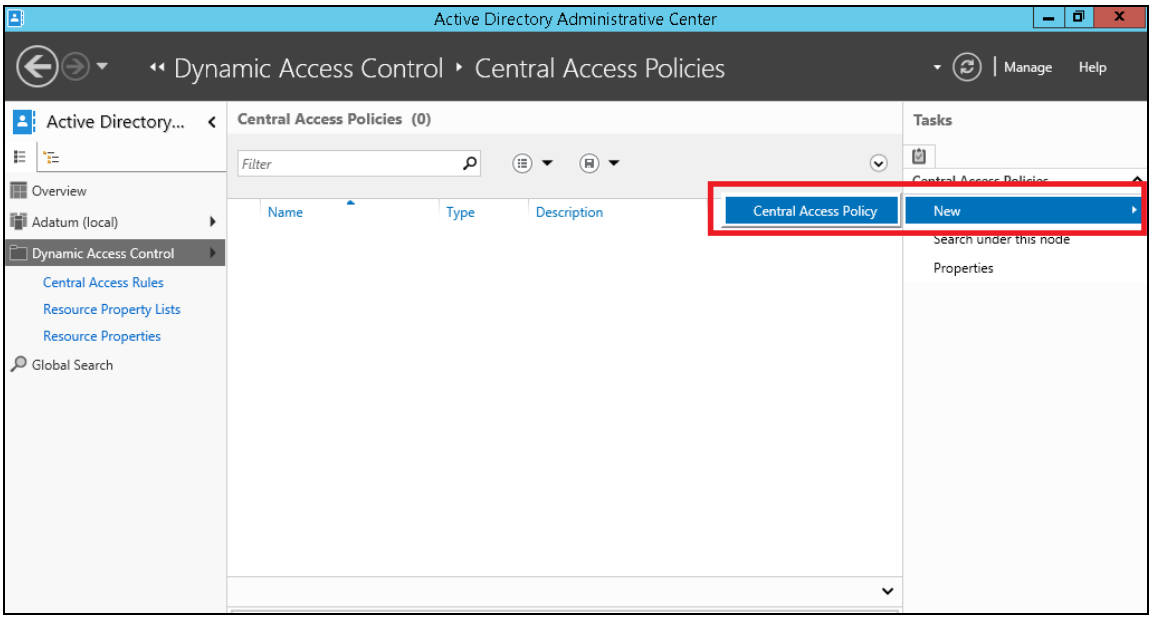


## Bước 2: Tạo và công bố Central Access Policy.

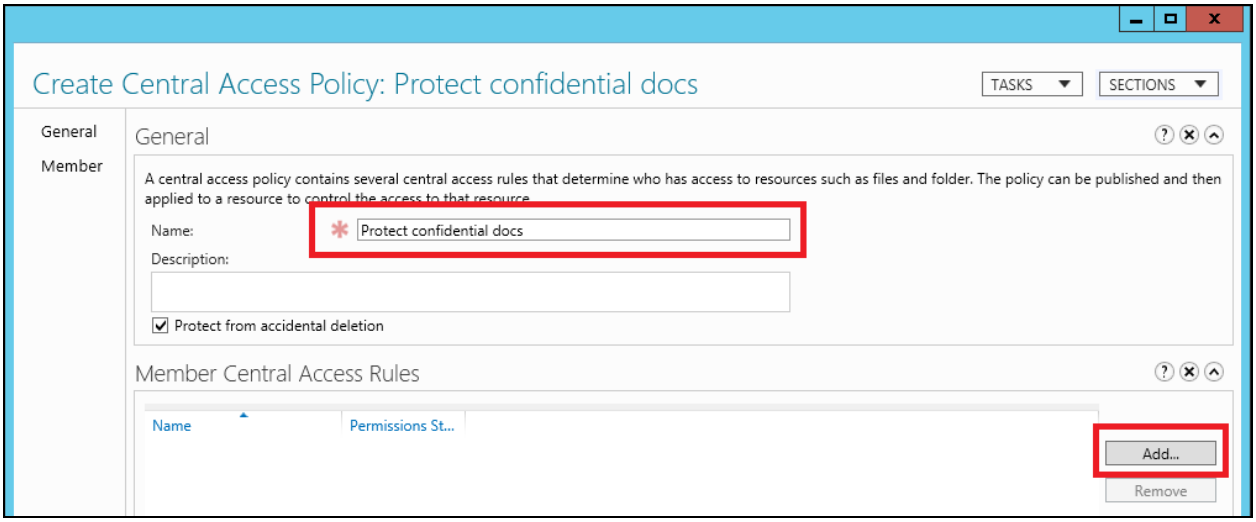
1. Trên máy **LON-DC1**, trong cửa sổ **Active Directory Administrative Center**, chọn **Dynamic Access Control**, nhấp đôi chuột **Central Access Policies**.



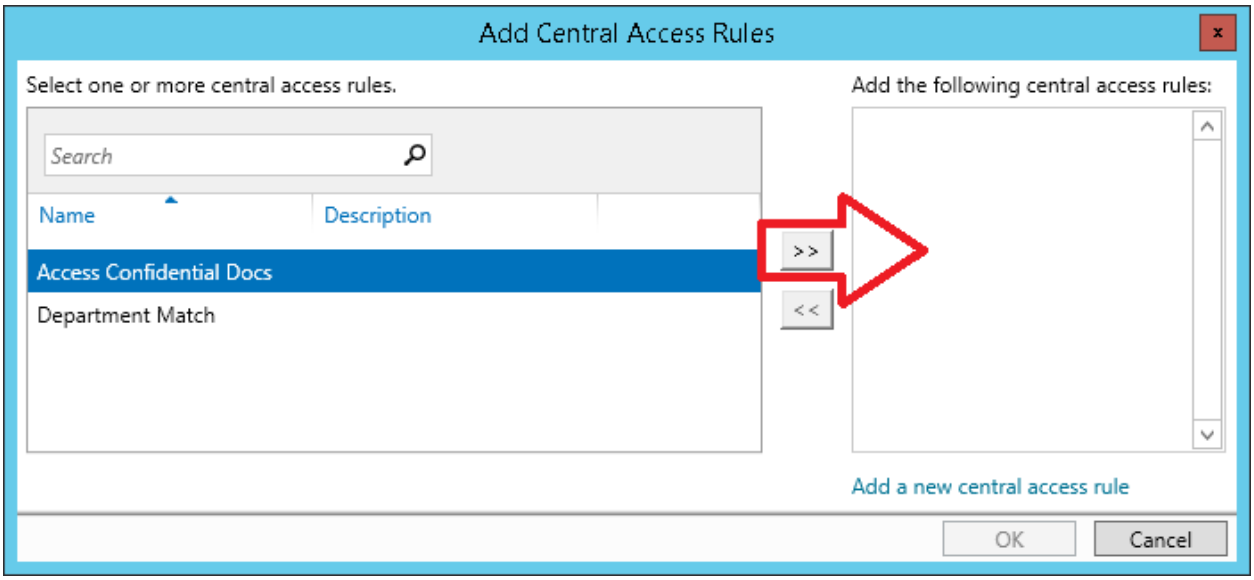

2. Trong cửa sổ **Tasks**, chọn **New**, và chọn **Central Access Policy**.



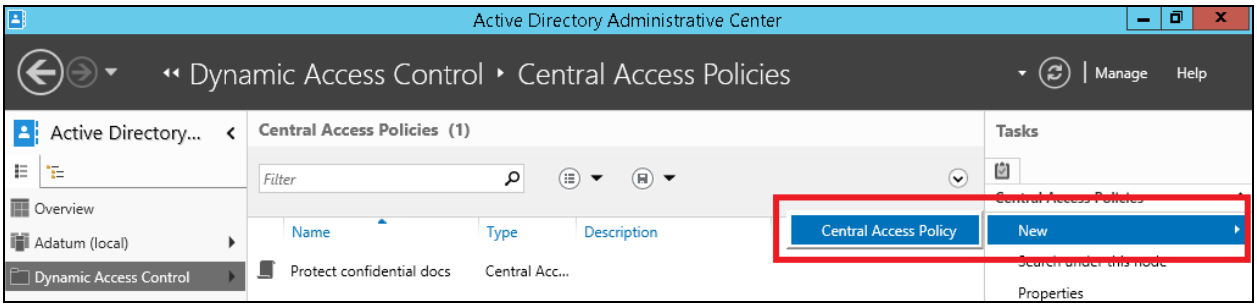
3. Cửa sổ **Create Central Access Policy,** trong ô **Name**, nhập **Protect confidential docs**, và chọn **Add**.



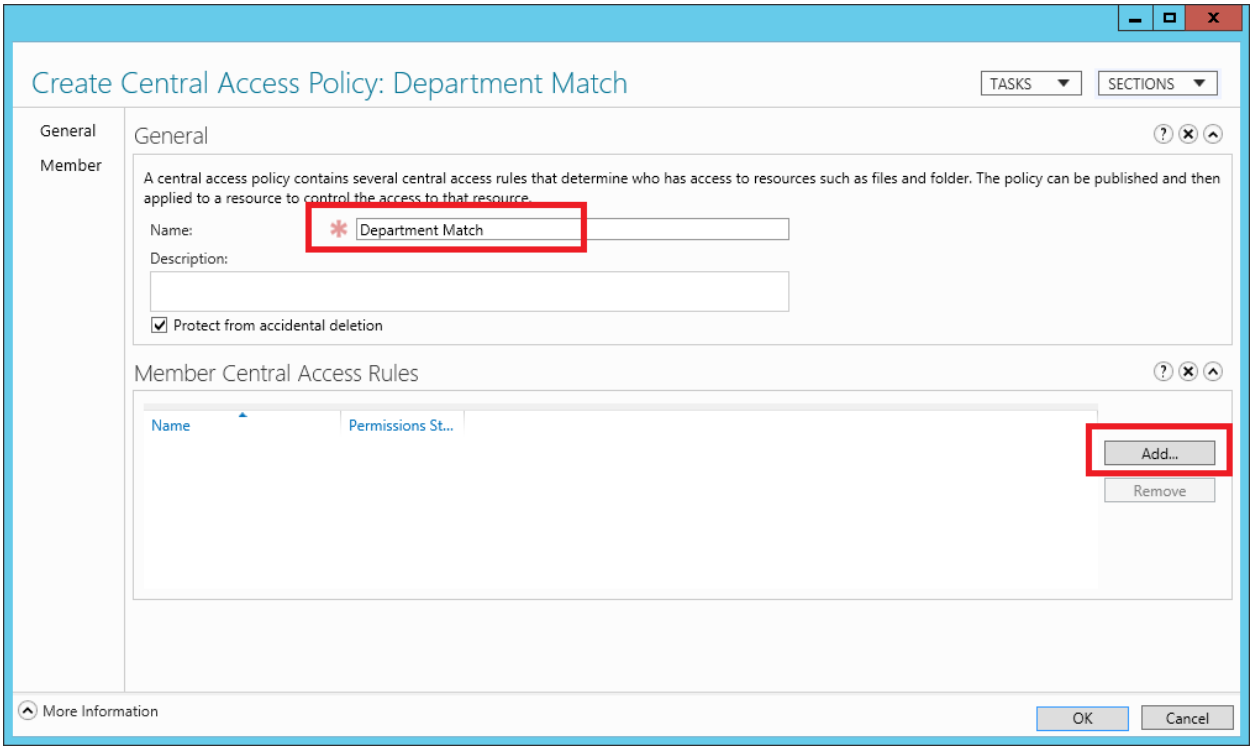

4. Chọn **Access Confidential Docs**, và chọn biểu tượng **Move** (>>). Chọn **OK** 2 lần.



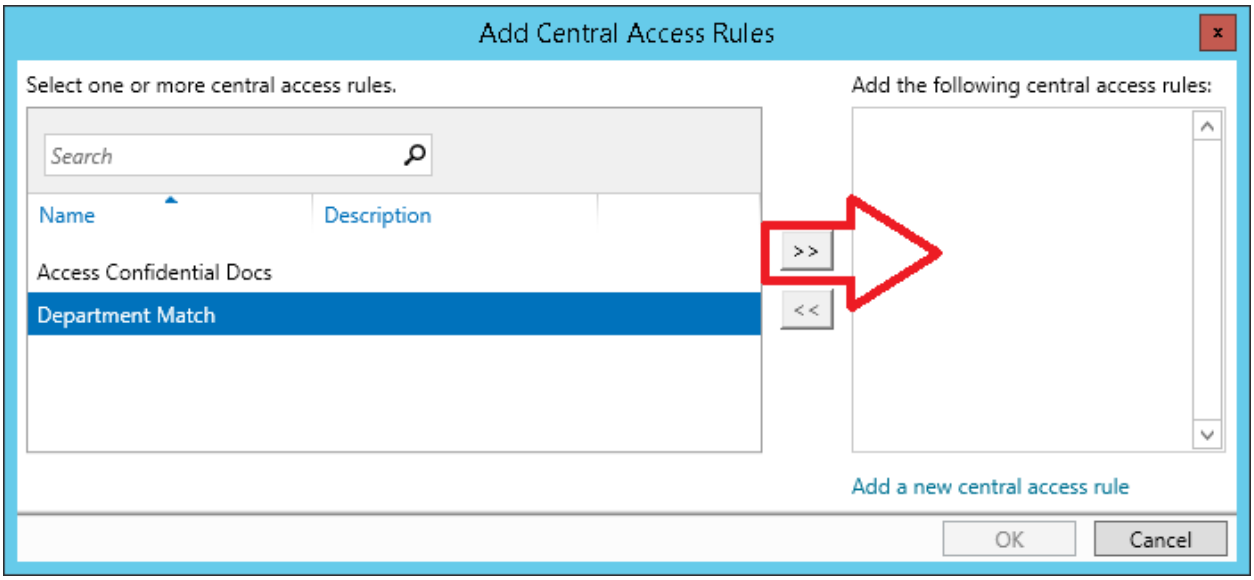
5. Trong cửa sổ **Tasks**, chọn **New**, và chọn **Central Access Policy**.



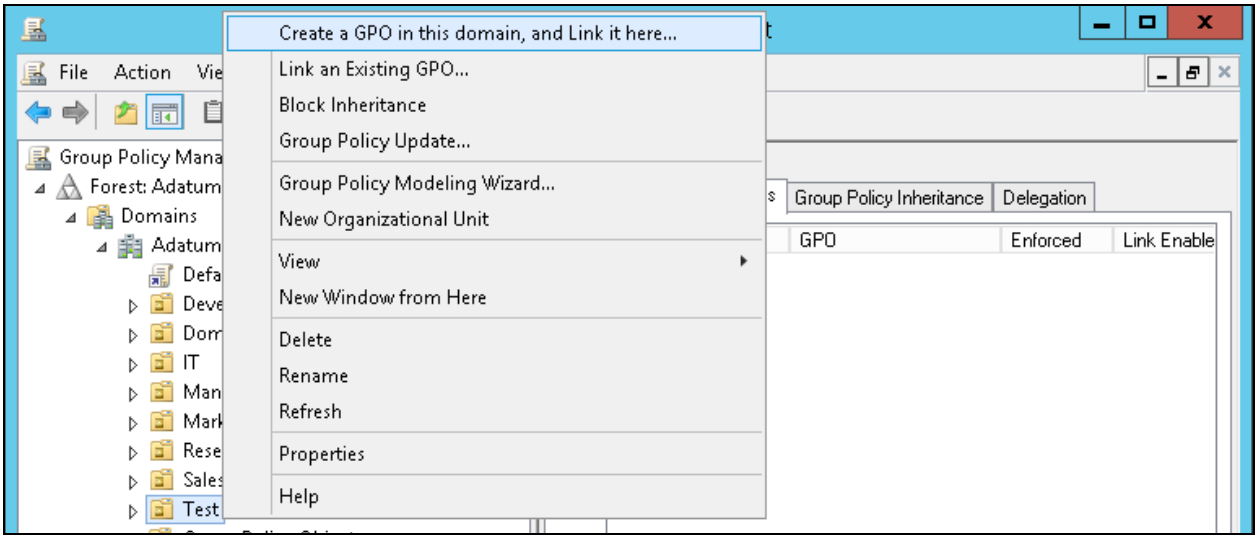

6. Cửa sổ **Create Central Access Policy,** trong ô **Name**, nhập **Department Match**, và chọn **Add**.



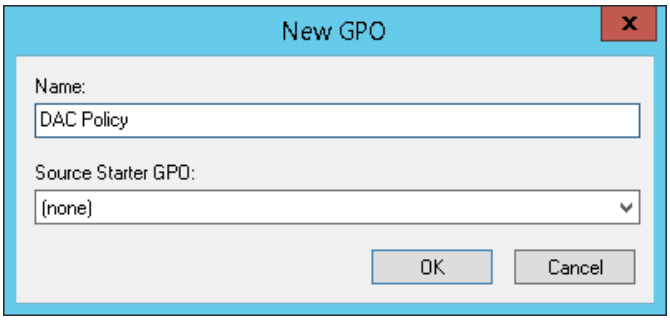
7. Chọn **Department Match**, chọn biểu tượng **More** (>>), chọn **OK** 2 lần.



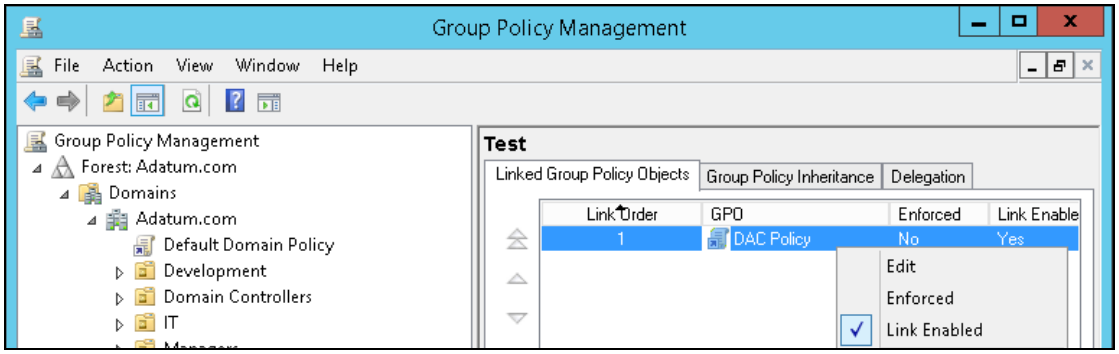

8. Qua cửa sổ **Server Manager**, bung **Tools**, mở **Group Policy Management**. Bung **Domains**, bung **Adatum.com**, chuột phải OU **Test**, chọn **Create a GPO in this domain, and link it here**.



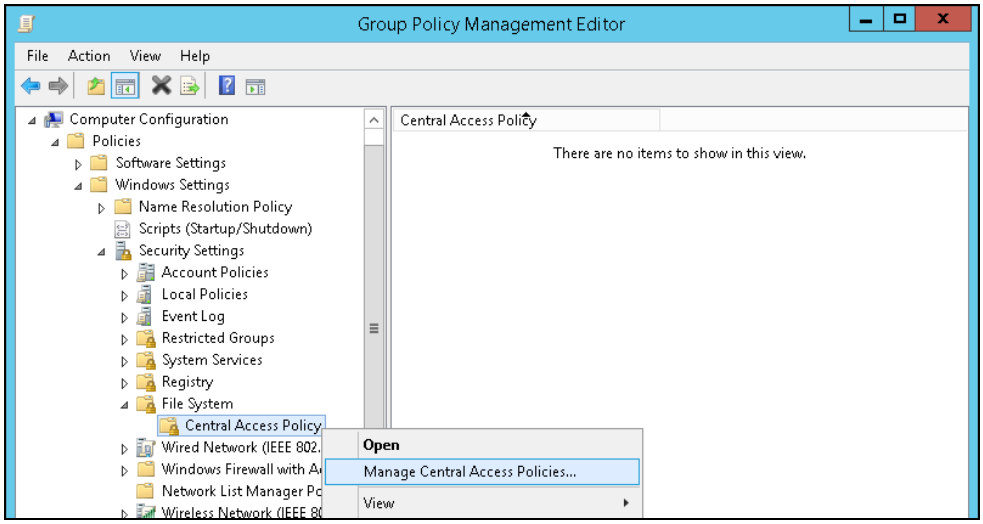
9. Hộp thoại **New GPO**, trong ô **Name**, nhập **DAC Policy**, chọn **OK**.



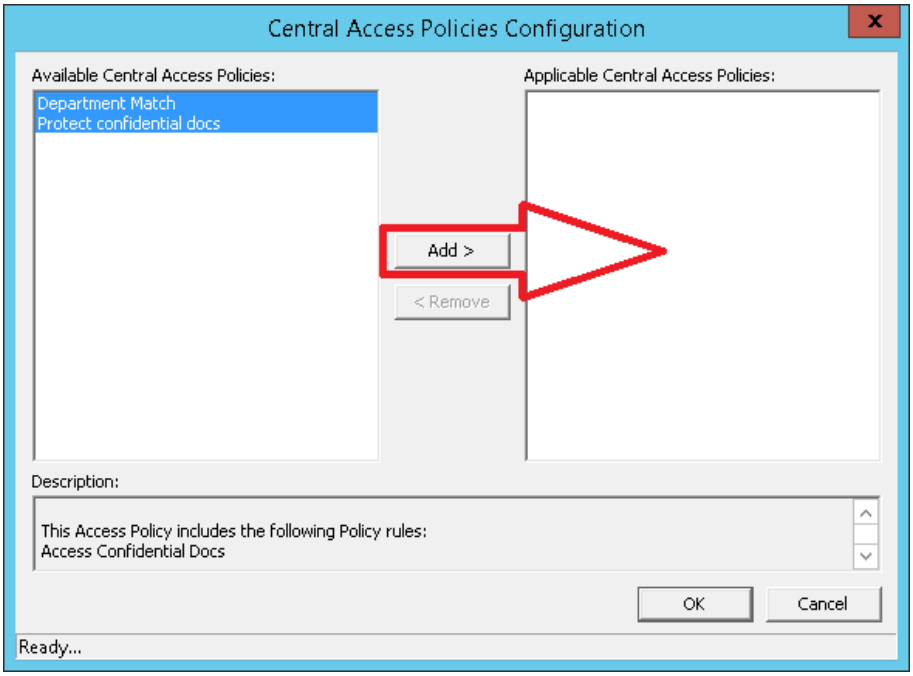

10. Chuột phải **DAC Policy**, chọn **Edit**.




11. Trong cửa sổ **Group Policy Management Editor**, bung **Computer Configuration**, bung **Policies**, bung **Windows Settings**, bung **Security Settings**, bung **File System**, chuột phải **Central Access Policy**, chọn **Manage Central Access Policies**.



12. Hộp thoại **Central Access Policies Configuration,** chọn cả 2 mục **Department Match** và **Protect confidential docs**, chọn **Add**, và chọn **OK**.

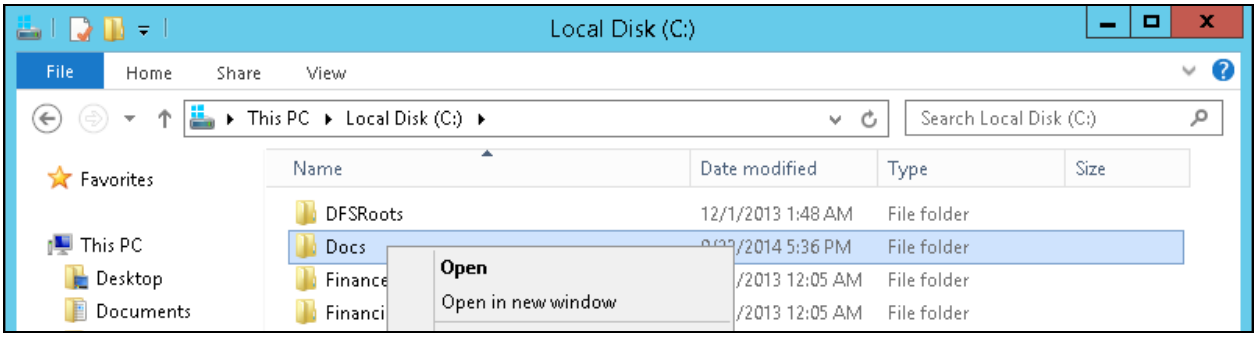



## Bước 3: Áp dụng Central Access Policy.

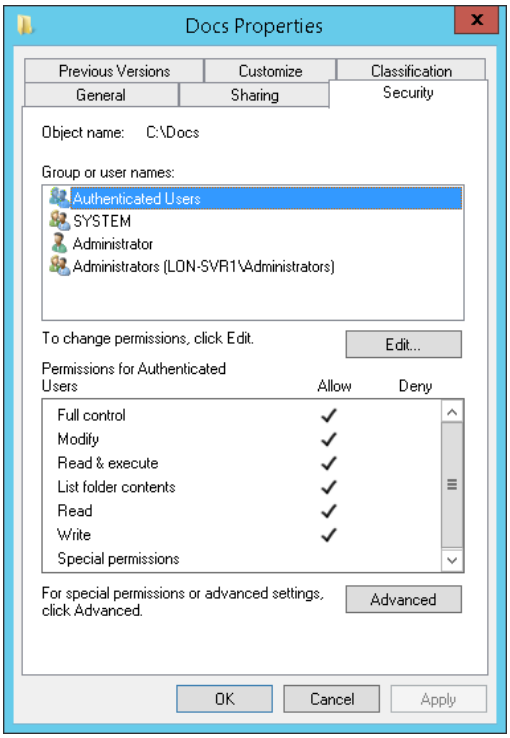
1. Qua máy **LON-SVR1**.

2. Mở **Windows PowerShell**, gõ lệnh: **gpupdate /force**

3. Mở **File Explorer**, vào ổ **C:**, chuột phải thư mục **Docs**, chọn **Properties**.

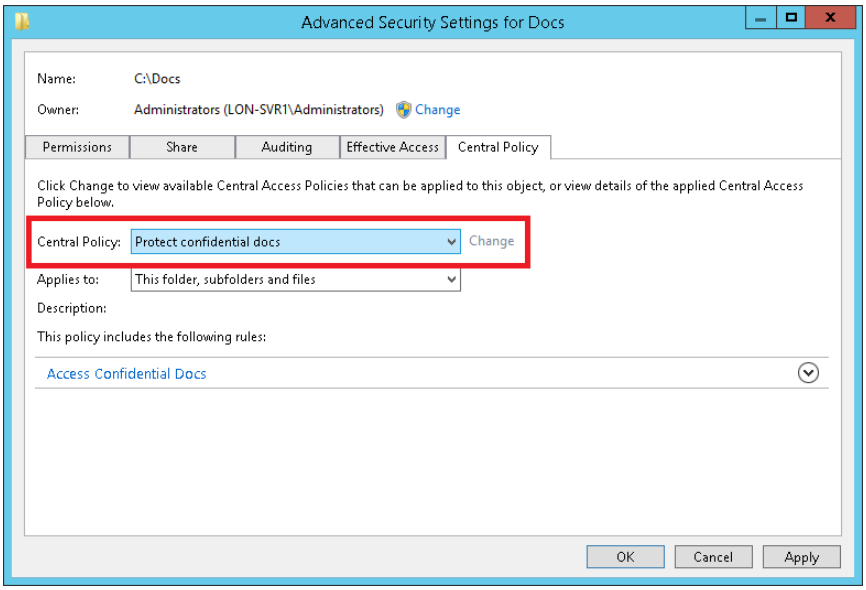


4. Hộp thoại **Docs Properties**, qua tab **Security**, chọn **Advanced**.

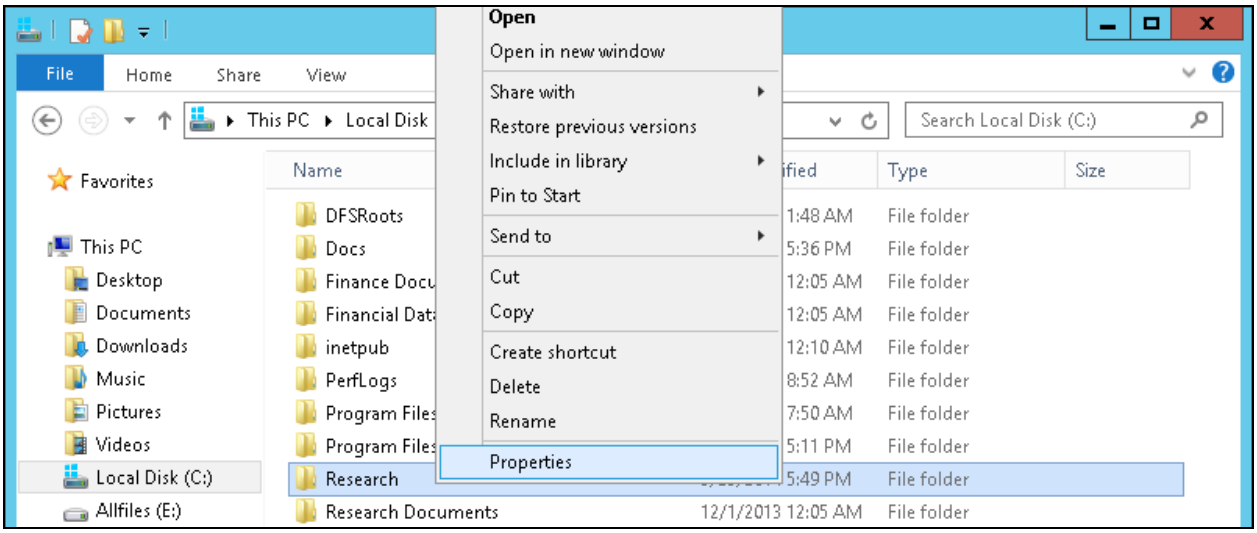



5. Cửa sổ **Advanced Security Settings for Docs**, qua tab **Central Policy**, chọn **Change**.

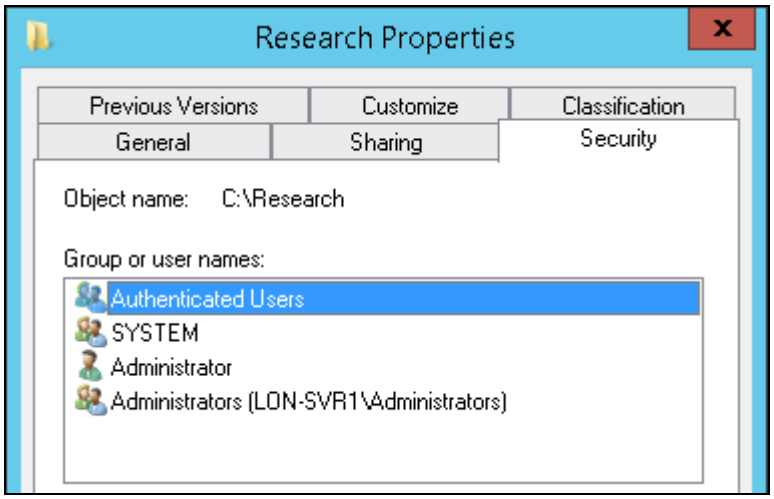
Bung ô **Central Policy**, chọn **Protect confidential docs**, chọn **OK** 2 lần.



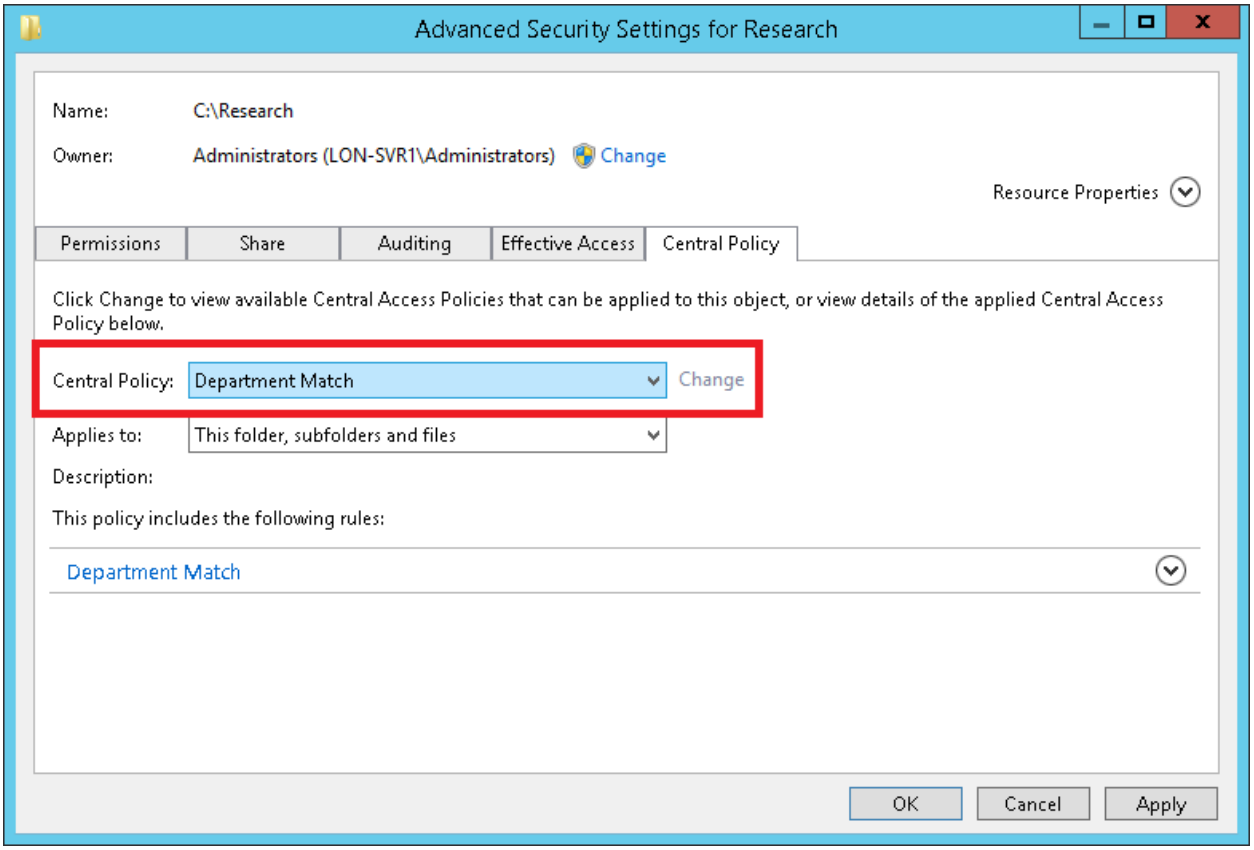
6. Trong **File Explorer,** chuột phải thư mục **Research**, chọn **Properties**.




7. Hộp thoại **Research Properties**, qua tab **Security**, chọn **Advanced**.



8. Cửa sổ **Advanced Security Settings for Research**, qua tab **Central Policy**, chọn **Change**. Bung ô **Central Policy**, chọn **Department Match**, chọn **OK** 2 lần.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai DAC thành công.**

## Bài tập 3: Cấu hình Access-Denied Assistance và kiểm tra DAC.

Bước cuối cùng, để giúp người dùng hiểu được các thông báo lỗi mà họ nhận được và cho phép họ yêu cầu truy cập tự động, bạn sẽ cấu hình chức năng Access-Denied Assistance. Ngoài ra, để đảm bảo rằng các thiết lập DAC được cấu hình đúng, bạn sẽ kiểm tra DAC bằng cách truy cập vào các dữ liệu bằng quyền của nhiều người dùng và máy tính khác nhau.

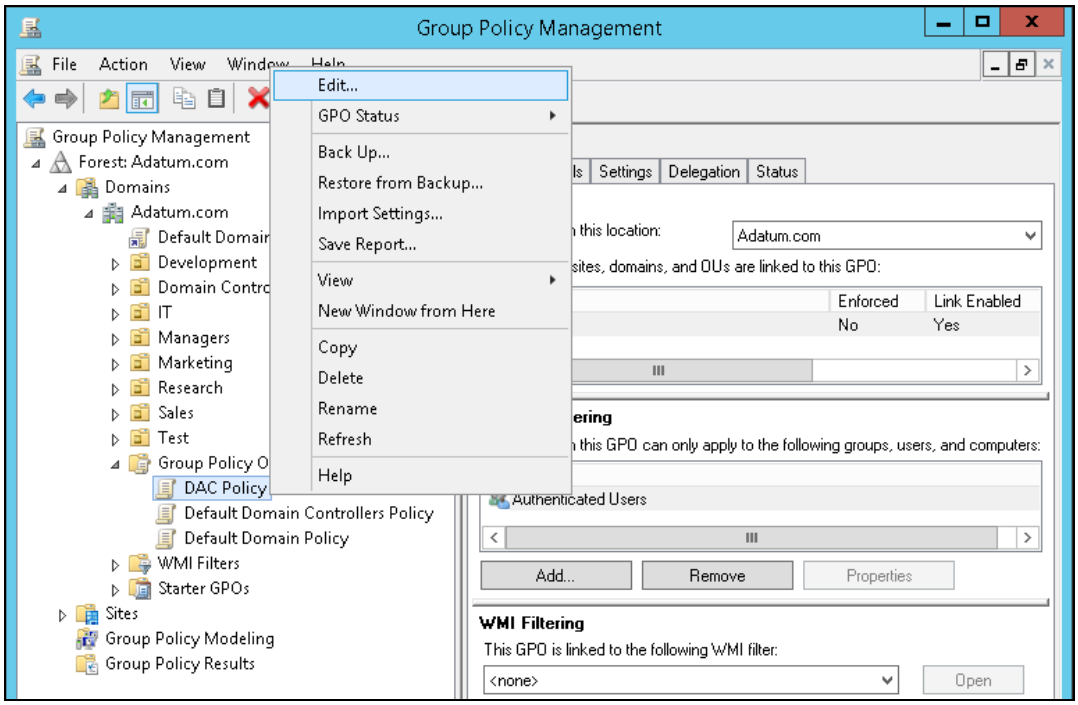
❖ **Bài thực hành bao gồm các bước:**

1. Cấu hình Access-Denied Assistance.
2. Kiểm tra chức năng DAC.
3. Kiểm tra quyền bằng Effective Permissions

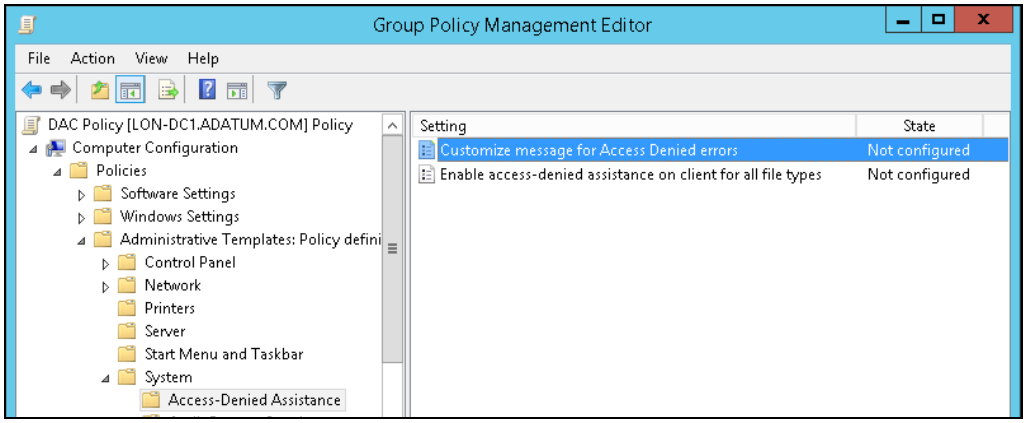
❖ **Thực hành:**

### Bước 1: Cấu hình Access-Denied Assistance.

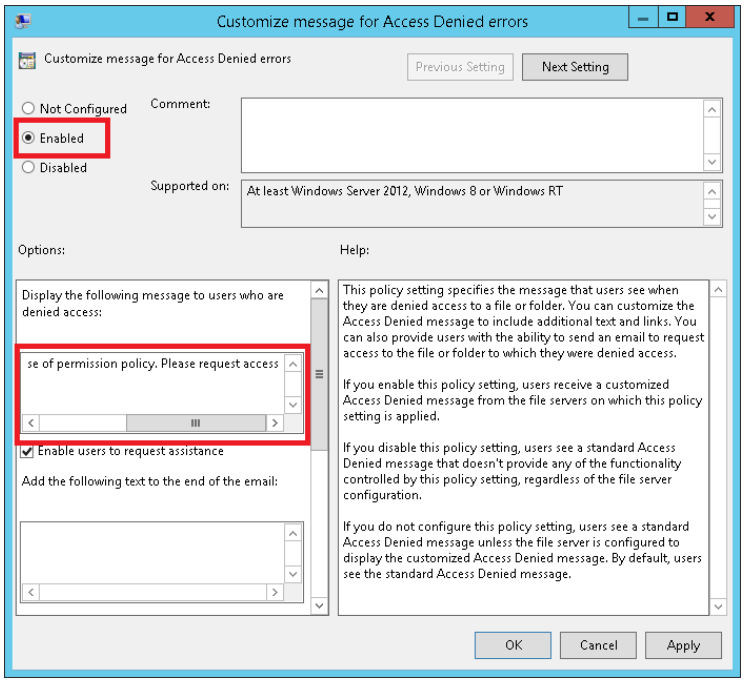
1. Qua máy **LON-DC1**. Trong **Server Manager**, bung menu **Tools**, mở **Group Policy Management**. Bung **Forest: Adatum.com**, bung **Domains**, bung **Adatum.com**, chọn **Group Policy Objects**. Chuột phải **DAC Policy**, chọn **Edit**.



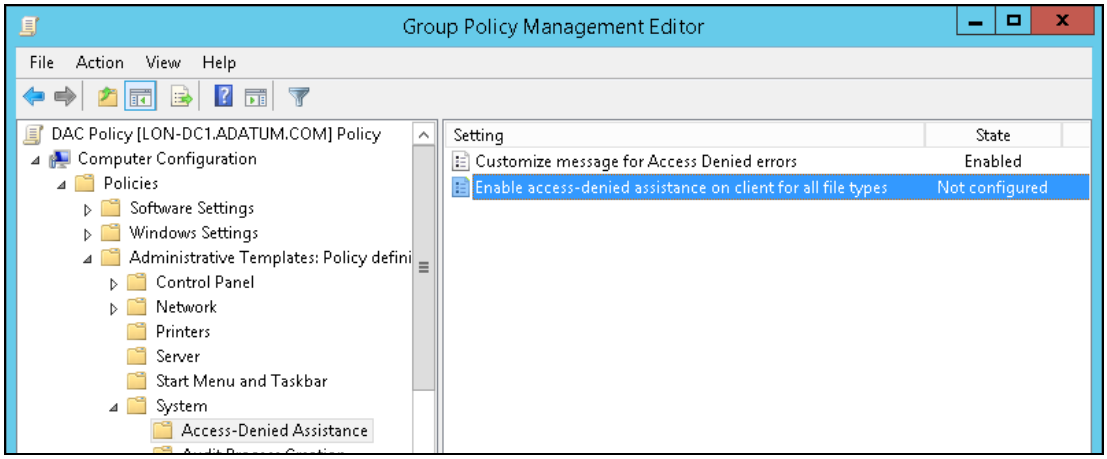
2. Cửa sổ **Group Policy Management** , bung **Computer Configuration**, bung **Policies**, bung **Administrative Templates**, bung **System**, chọn **Access-Denied Assistance**, nhấp đôi chuột lên policy **Customize Message for Access Denied errors**.



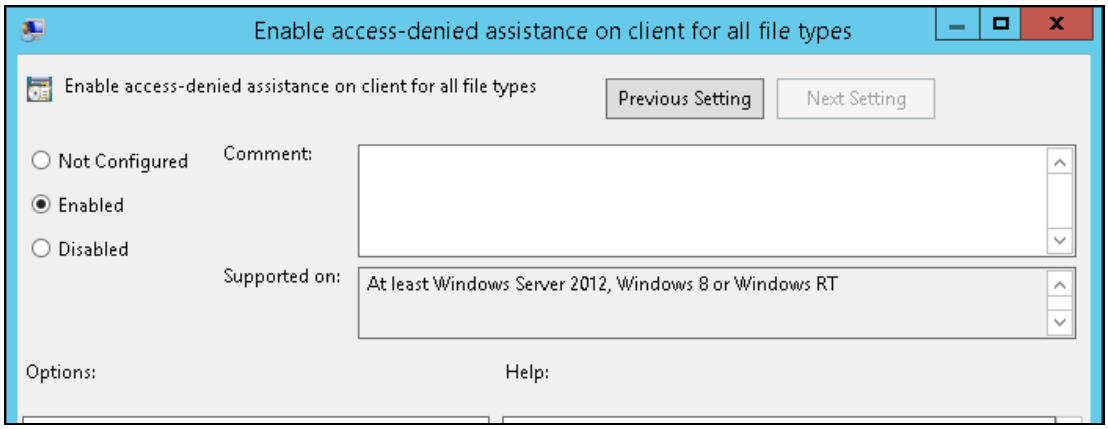

3. Cửa sổ **Customize Message for Access Denied errors**, chọn **Enabled**. Trong ô **Display the following message to users who are denied access**, nhập ***You are denied access because of permission policy. Please request access***. Đánh dấu chọn **Enable users to request assistance**, chọn **OK**.



4. Nhấp đôi chuột lên policy **Enable access-denied assistance on client for all file types**

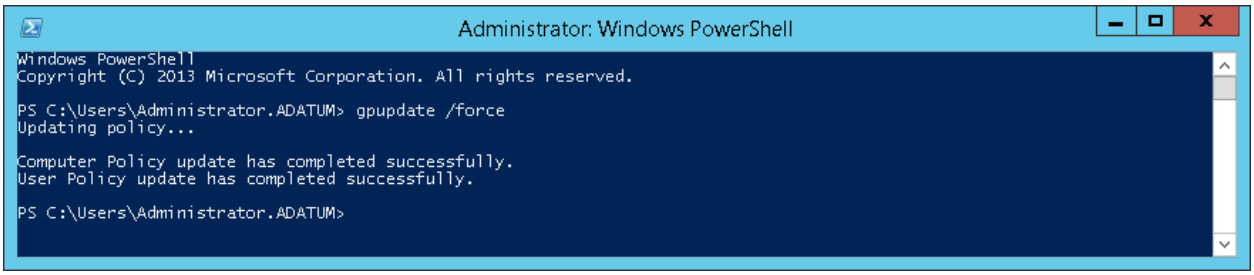



5. Cửa sổ **Enable access-denied assistance on client for all file types**, chọn **Enabled**, và chọn **OK**.




6. Tắt **Group Policy Management Editor** và **Group Policy Management Console**.

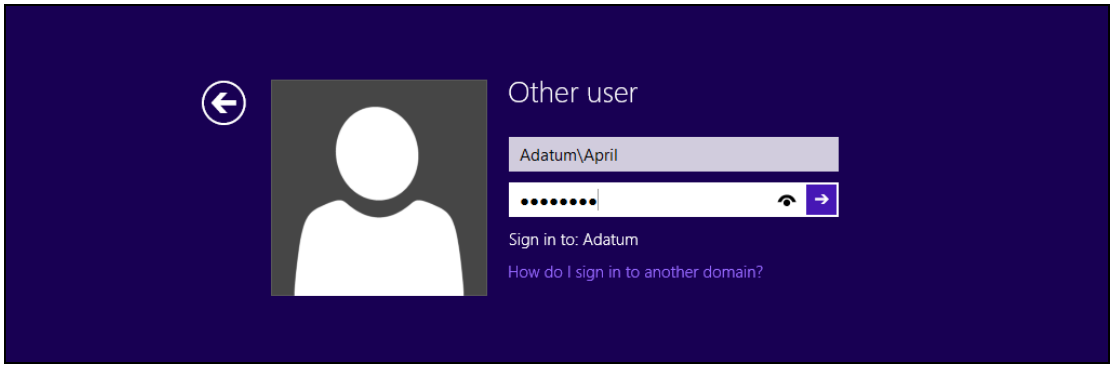
7. Qua máy **LON-SVR1**. Mở **Windows PowerShell,** gõ lệnh: **gpupdate /force**



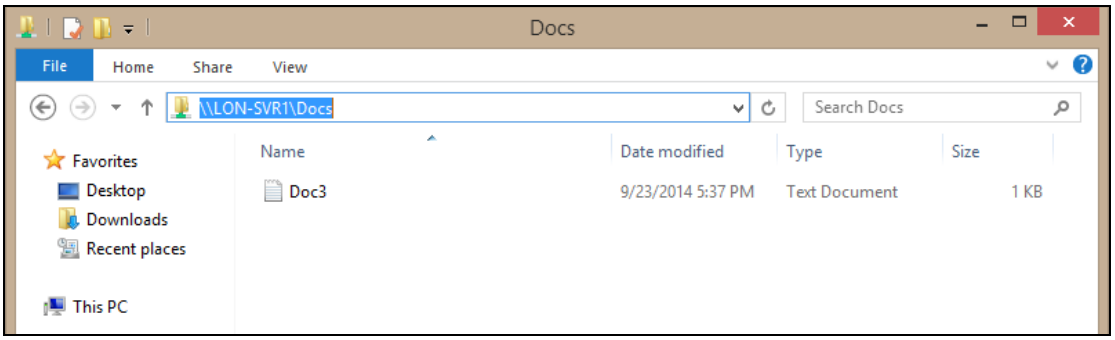
## Bước 2: Kiểm tra chức năng DAC.

1. Restart máy **LON-CL1**.

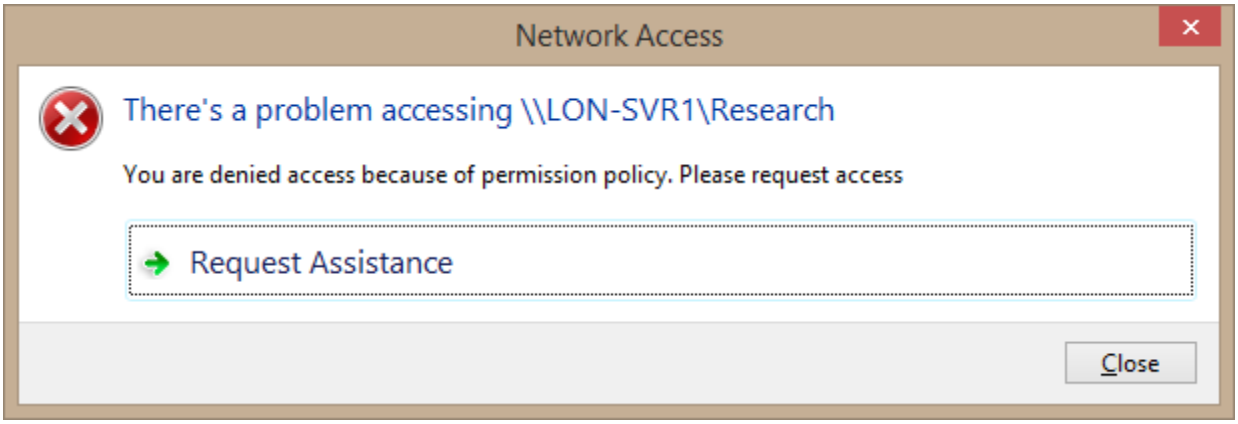
2. Sign in vào **LON-CL1** bằng **Adatum\April** với password **Pa$$w0rd**.




3. Mở **File Explorer,** truy cập**\\LON-SVR1\Docs.** Kiểm tra chỉ có quyền truy cập file **Doc3**.



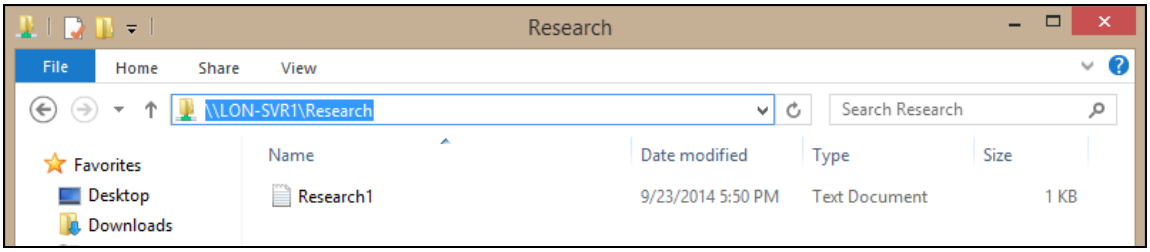

4. Trong **File Explorer**, truy cập **\\LON-SVR1\Research**. Kiểm tra truy cập thất bại. Chọn **Request Assistance**. Xem xét các lựa chọn, và chọn **Close**.



5. Sign out và Sign in vào máy **LON-CL1** bằng **Adatum\Allie** với password **Pa$$w0rd**.



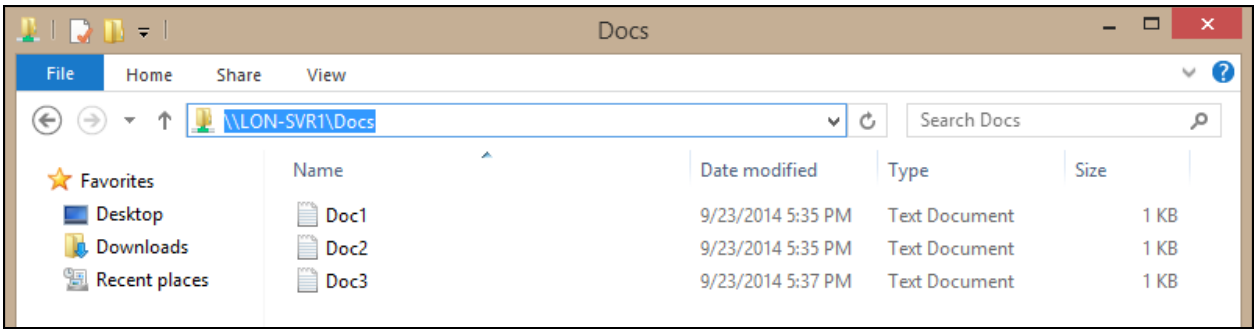

6. Mở **File Explorer,** truy cập **\\LON-SVR1\Research**. Kiểm tra truy cập thành công, bởi vì **Allie** là thành viên của **Research Department** .




7. Sign out và Sign in vào máy **LON-CL1** bằng **Adatum\Aidan** với password **Pa$$w0rd**.



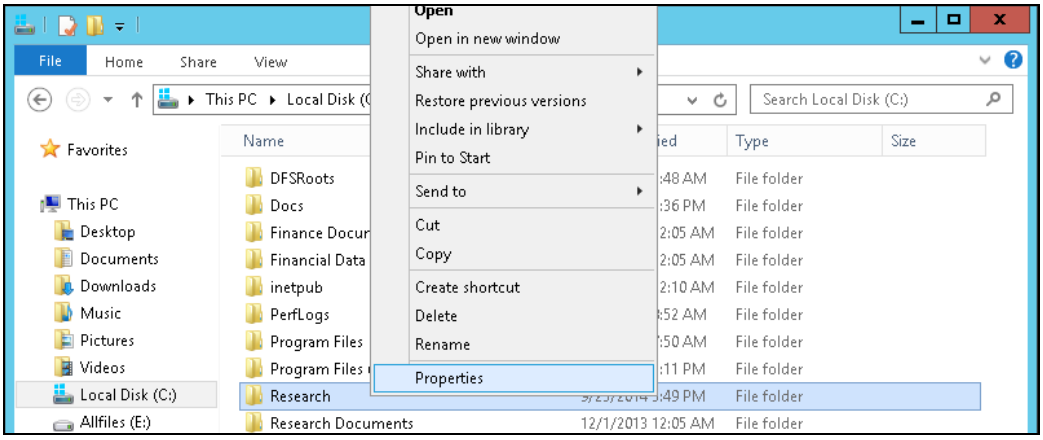

8. Mở **File Explorer**, truy cập **\\LON-SVR1\Docs**. Kiểm tra truy cập thành công tất cả các file trong thư mục **Docs**, bởi vì **Aidan** là thành viên của **Managers Department** và máy tính dang sử dụng là thành viên của group **ManagersWKS**



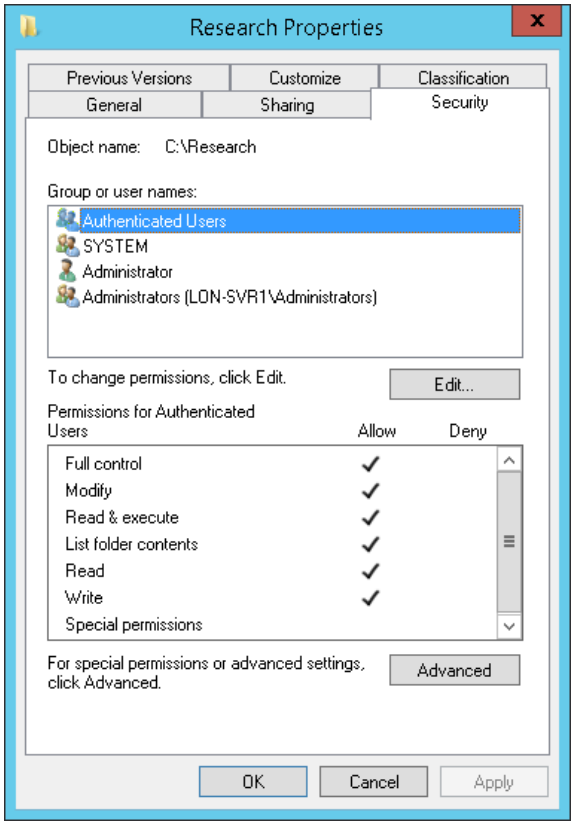
## Bước 3: Kiểm tra quyền bằng Effective Permissions.

1. Qua máy **LON-SVR1**.

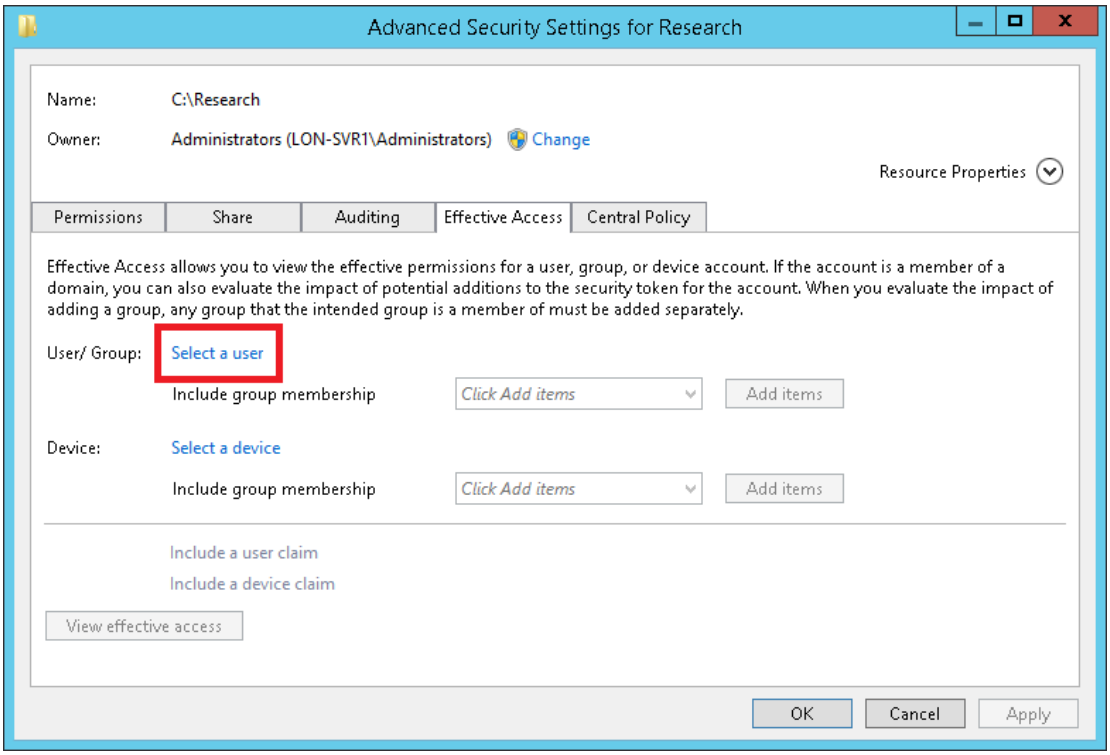
2. Mở **File Explorer**, vào ổ **C:**, chuột phải folder **Research**, chọn **Properties**.



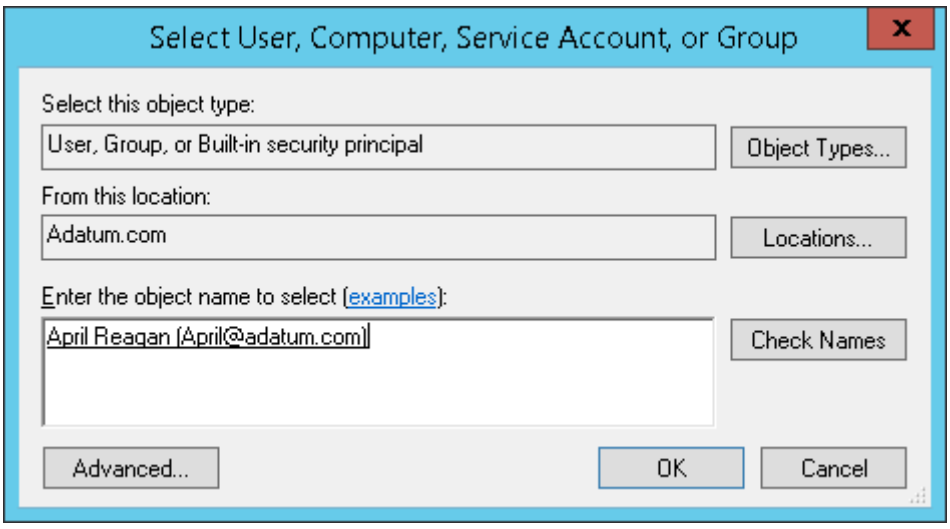

3. Hộp thoại **Research Properties**, qua tab **Security**, chọn **Advanced.**



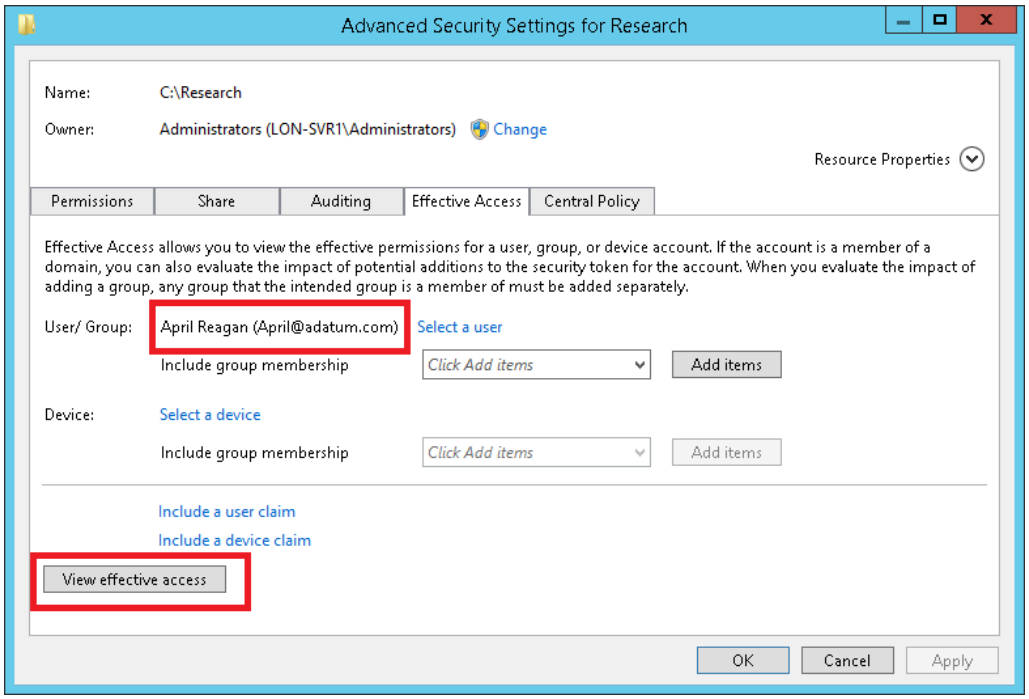
4. Qua tab **Effective Access**, chọn **select a user**.



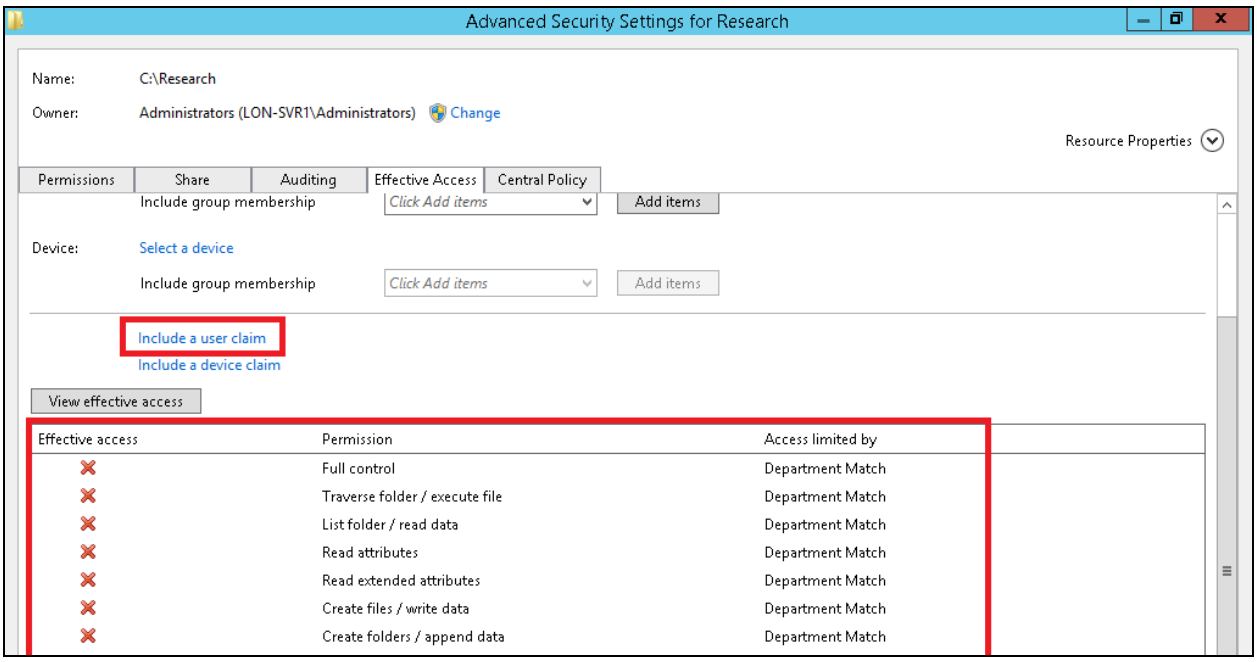

5. Hộp thoại **Select User, Computer, Service Account, or Group**, nhập **April**, chọn **Check Names**, chọn **OK**.



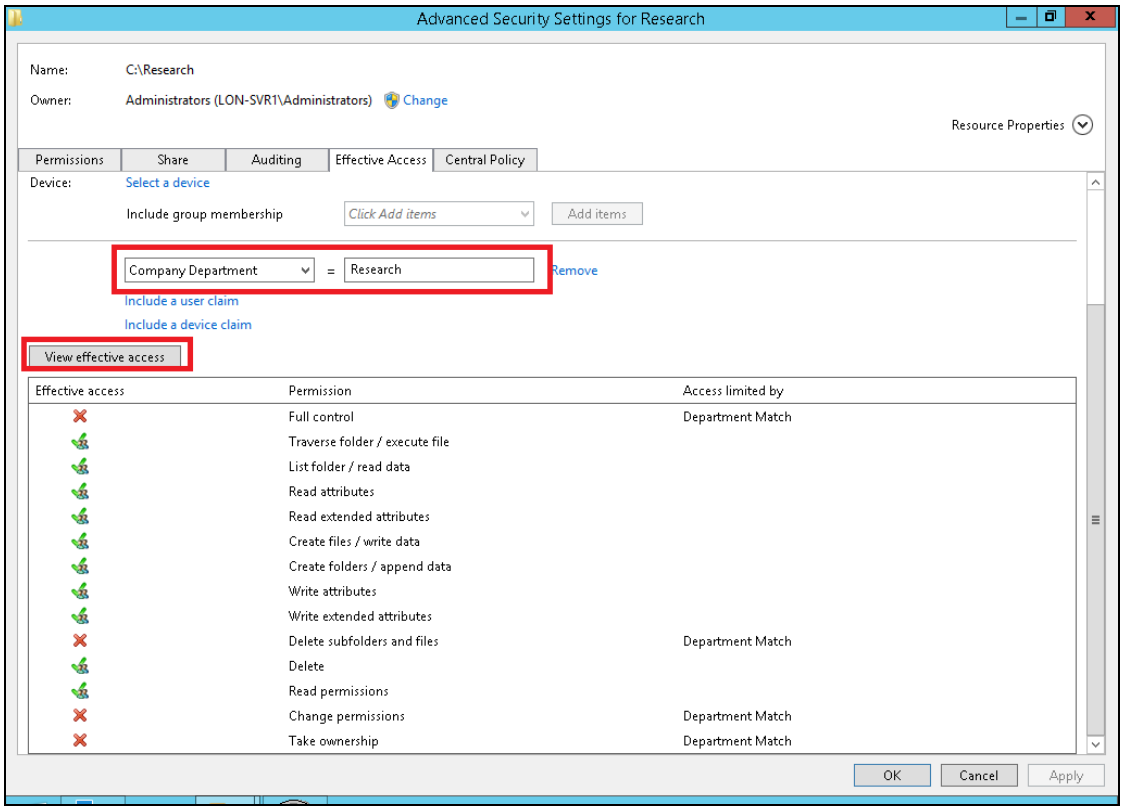
6. Chọn **View effective access**.




7. Kiểm tra user **April** không có quyền truy cập folder. Chọn **Include a user claim**.



8. Bung ô chọn, chọn **Company Department**, trong ô **Value**, nhập **Research**, chọn **View Effective access**. Kiểm tra user **April** có quyền truy cập folder.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình thành công chức năng Access-Denied Assistance và kiểm tra chức năng DAC.**

## 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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiện bước 2 và 3 cho máy ảo **20414C-LON-SVR1** và **20414C-LON-CL1.**

# Bài 12: Triển khai chức năng Work Folder

## I. Mục tiêu:

- Triển khai cơ sở hạ tầng cho Work Folders.
- Cấu hình AD FS và Web Application Proxy để hỗ trợ người dùng bên ngoài hệ thống truy cập Work Folder.
- Kiểm tra chức năng Work Folders.

## II. Kịch bản và yêu cầu tổng quan:

Công ty A. Datum có các nhân viên bán hàng và một số người sử dụng nói chung làm việc từ xa bằng các loại thiết bị cá nhân khác nhau. Các nhân viên này có yêu cầu được truy cập dữ liệu lưu trữ trên File Server bằng các thiết bị cá nhân của họ dù đang ở bất kỳ nơi nào.

Để đáp ứng nhu cầu trên, bạn sẽ cấu hình chức năng Work Folders để cho phép người dùng truy cập dữ liệu của họ mọi lúc và mọi nơi.

## III. Mô hình thực hành gồm các máy:

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-DC1**<br>**20414C-LON-SVR1**<br>**20414C-LON-SVR2**<br>**20414C-LON-CL1**<br>**20414C-LON-CL2** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**IV. Chuẩn bị:**

1. Trên máy **LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.

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

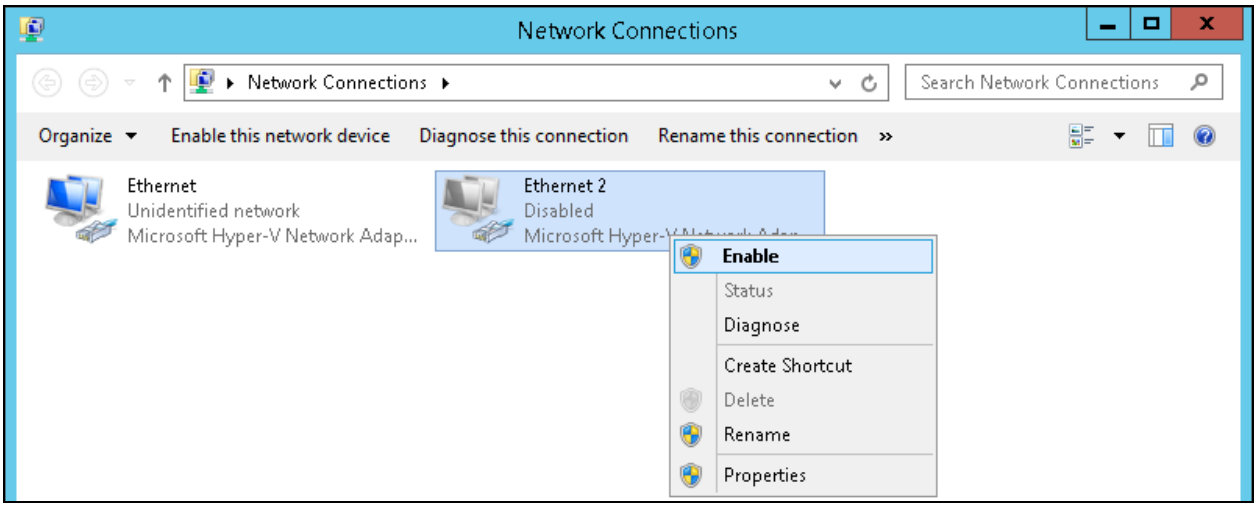
3. Logon vào máy **20414C-LON-DC1** với thông tin sau:

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

4. Thực hiên từ bước 1 đến 3 cho các máy ảo còn lại**.** Không sign in vào máy **LON-CL1** và **LON-CL2** cho đến khi có yêu cầu.

5. Trên máy **LON-SVR2**, chuột phải **Start** menu, mở **Network Connections**.

6. Trong cửa sổ **Network Connections**, chuột phải lên card **Ethernet 2**, chọn **Enable**.



**V. Thực hành:**

*Thời gian thực hành: 60 phút*

## Bài tập 1: Triển khai cơ sở hạ tầng cho Work Folders.

Công việc đầu tiên trong việc triển khai Work Folders là tạo Sync Server Share trên máy File Server đang có của bạn.

❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt Work Folders và cấu hình SSL Certificate
2. Tạo Share Folder cho Work Folders
3. Cấu hình và triển khai Work Folders

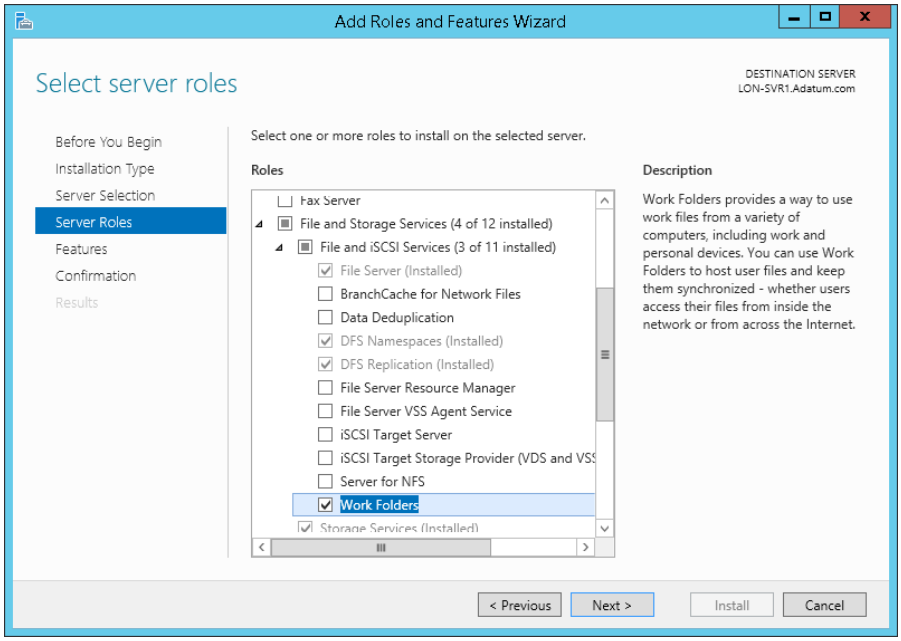
❖ **Thực hiện:**

### Bước 1: Cài đặt Work Folders và cấu hình SSL Certificate

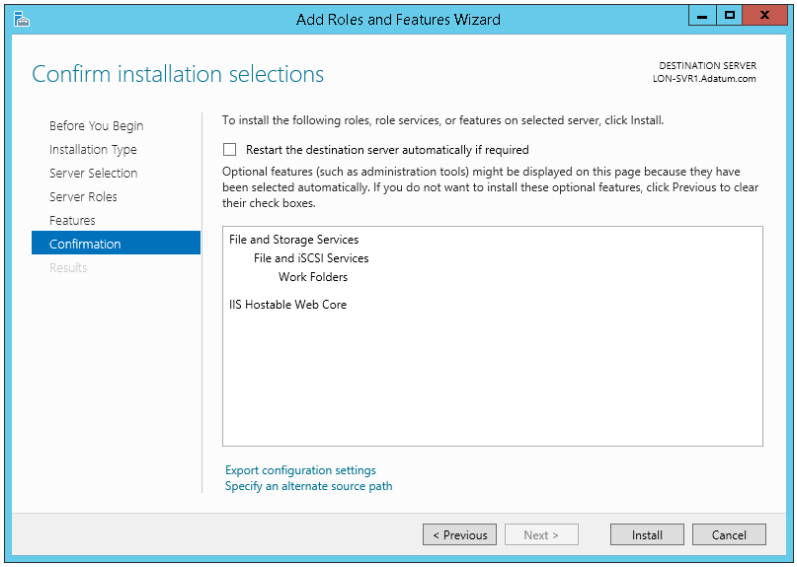
1. Trên máy **LON-SVR1.** Trong **Server Manager**, chọn **Add roles and features**.

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

3. Cửa sổ **Select server roles**, bung **File and Storage Services**, bung **File and iSCSI Services**, đánh dấu chọn **Work Folders**, chọn **Add Features**, chọn **Next** 2 lần.

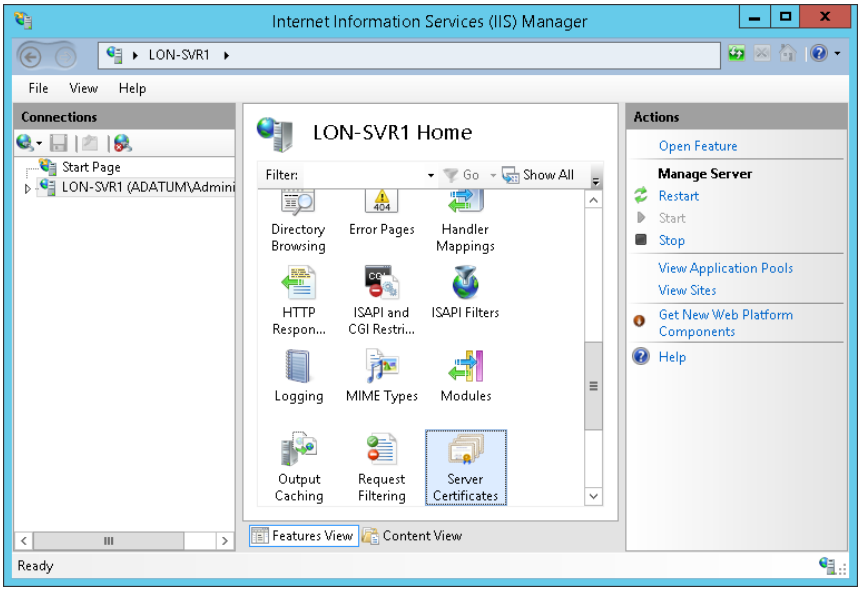


4. Cửa sổ **Confirm installation selection**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close.**

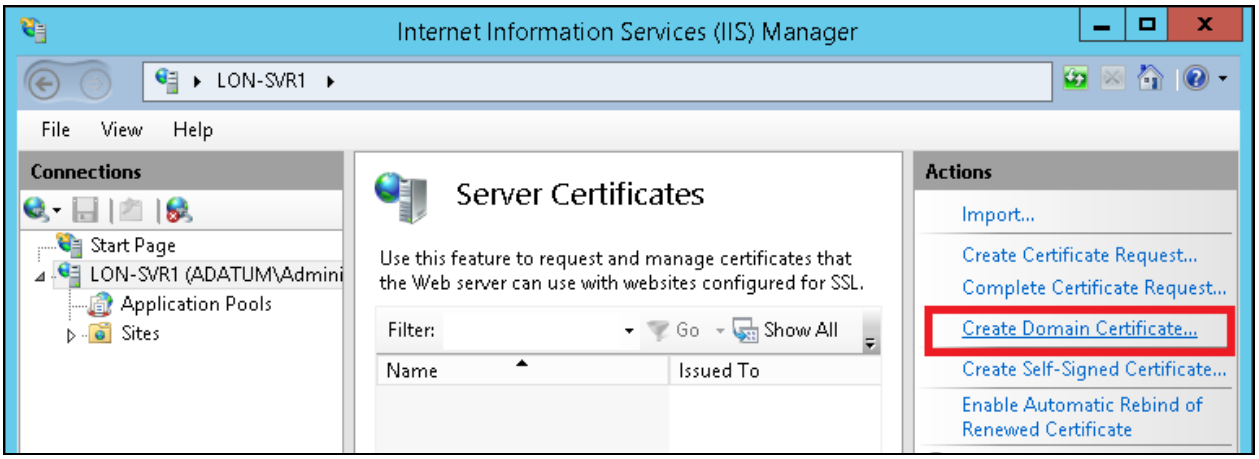



5. Trong **Server Manager,** bung menu **Tools**, mở **Internet Information Services (IIS) Manager**. Hộp thoại thông báo, chọn **No.**

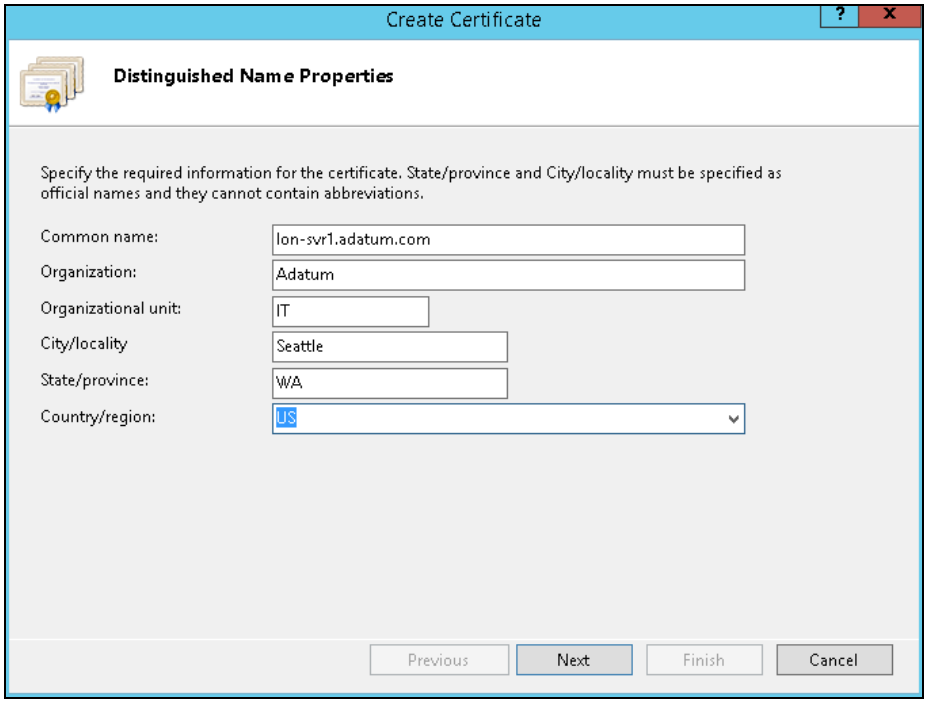
6. Trong cửa sổ **Internet Information Services (IIS) Manager**, chọn **LON-SVR1**, nhấp đôi chuột **Server Certificates**.



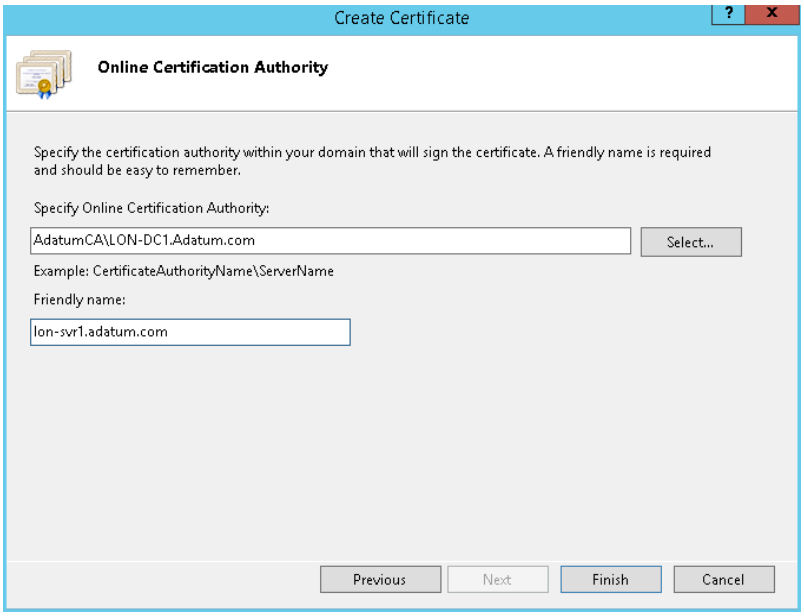
7. Cửa sổ **Actions**, chọn **Create Domain Certificate**.



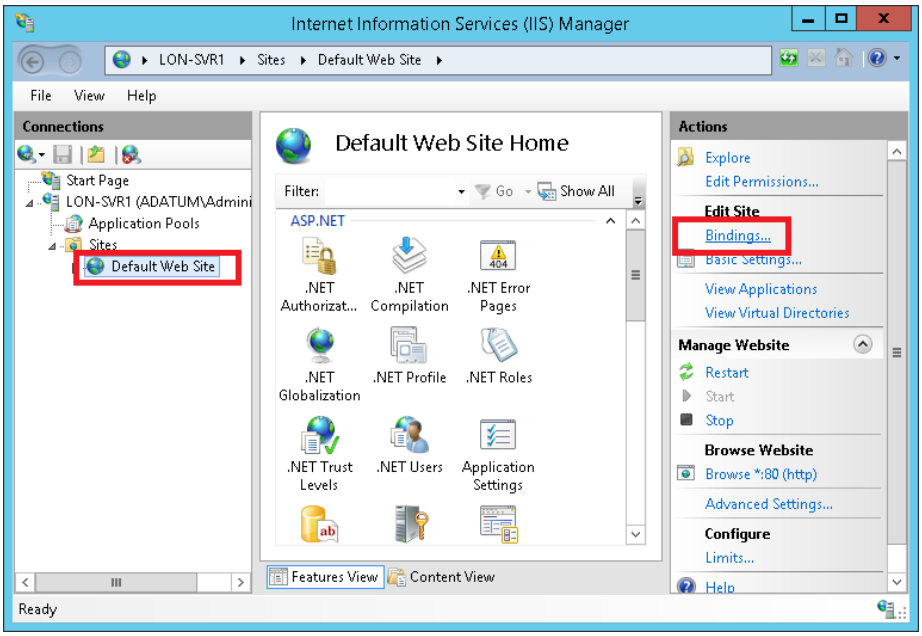

8. Cửa sổ **Create Certificate**, nhập thông tin như hình bên dưới, và chọn **Next**.



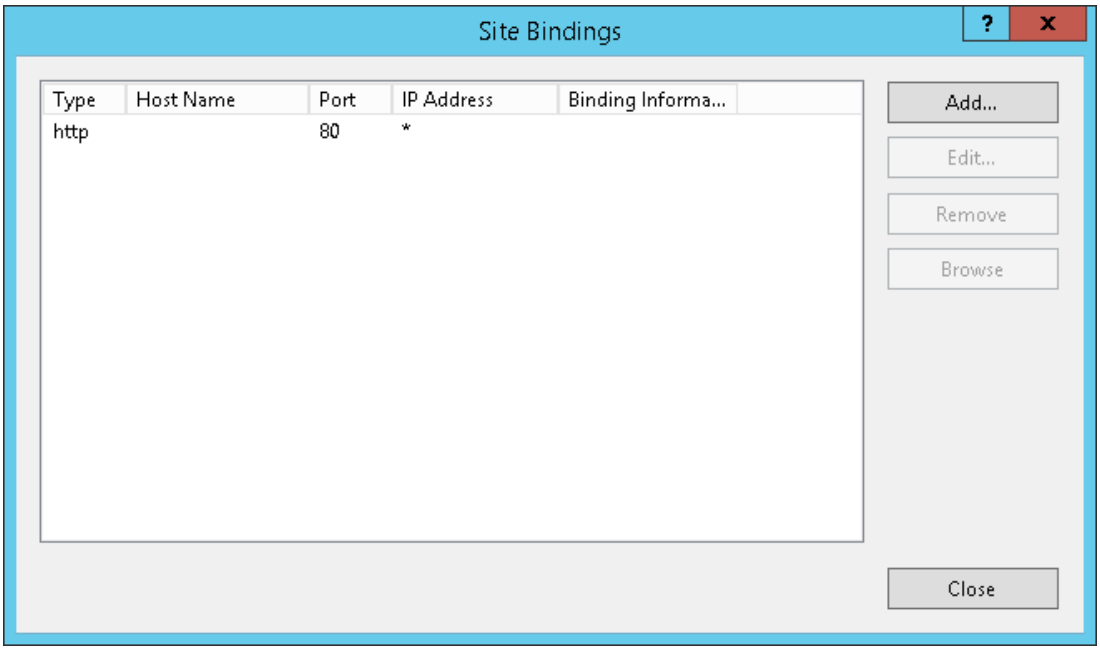
9. Cửa sổ **Online Certification Authority**, chọn **Select**, cửa sổ **Select Certification Authority,** chọn **AdatumCA,** chọn **OK**. Trong ô **Friendly name**, nhập **lon-svr1.adatum.com ,**và chọn **Finish**



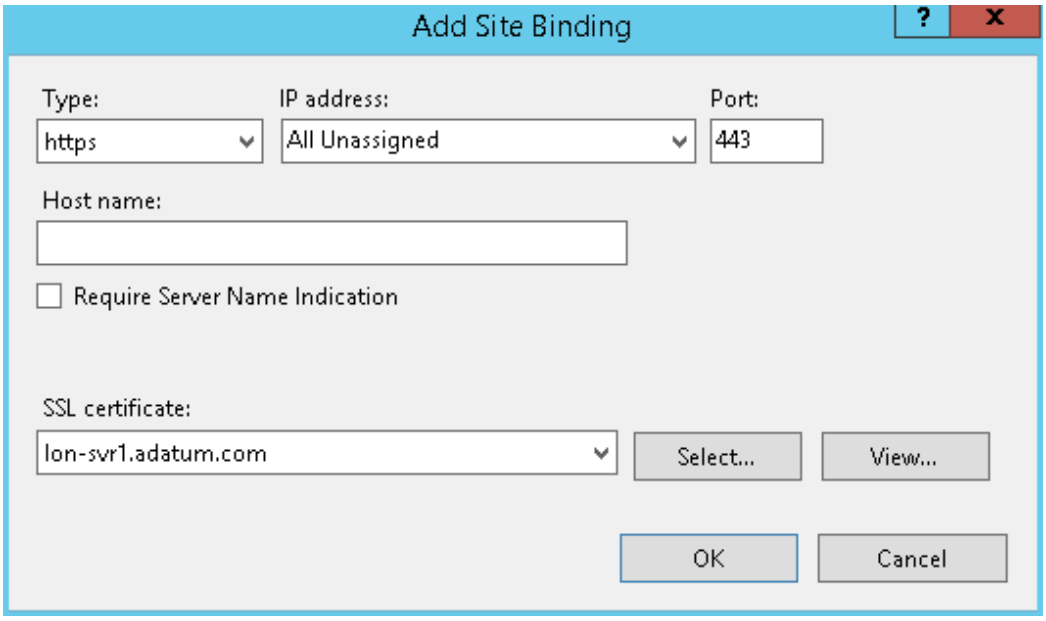

10. Trong cửa sổ **IIS**, bung **Sites**, chọn **Default Web Site**, chọn **Bindings**



11. Hộp thoại **Site Bindings**, chọn **Add…**.



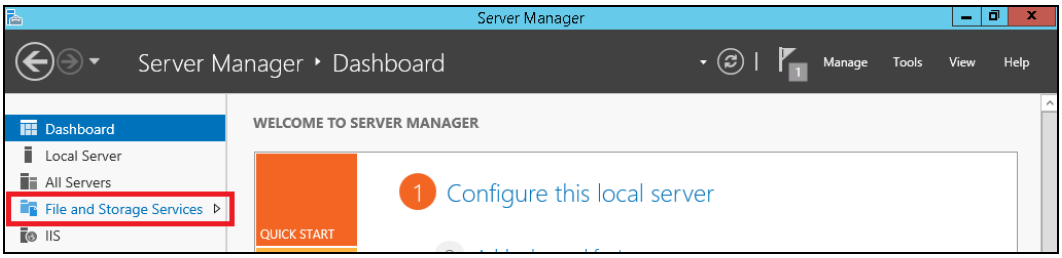

12. Hộp thoại **Add Site Binding**, bung **Type**, chọn **https**, bung ô **SSL certificate** chọn **lon-svr1.adatum.com**, chọn **OK**, và chọn **Close**.



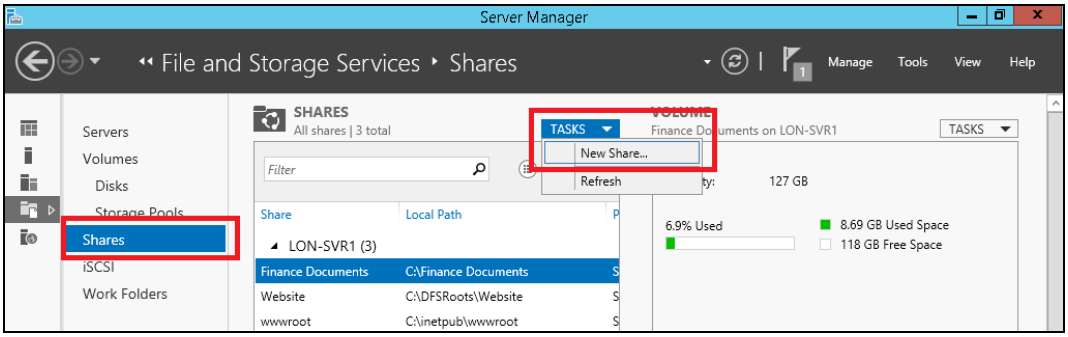

13. Tắt cửa sổ **Internet Information Services (IIS) Manager**.

## Bước 2: Tạo Share Folder cho Work Folders

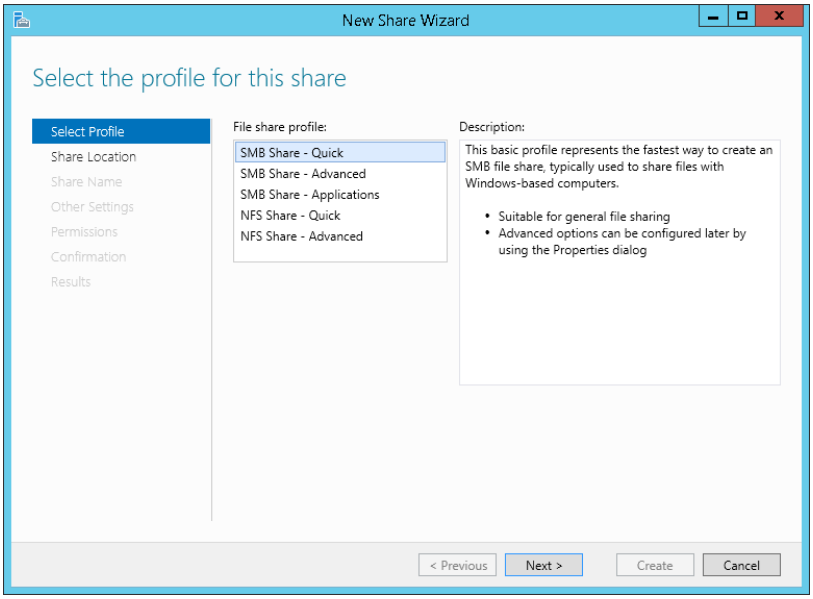
1. Trên máy **LON-SVR1**, trong **Server Manager**, mở **File and Storage Services**.



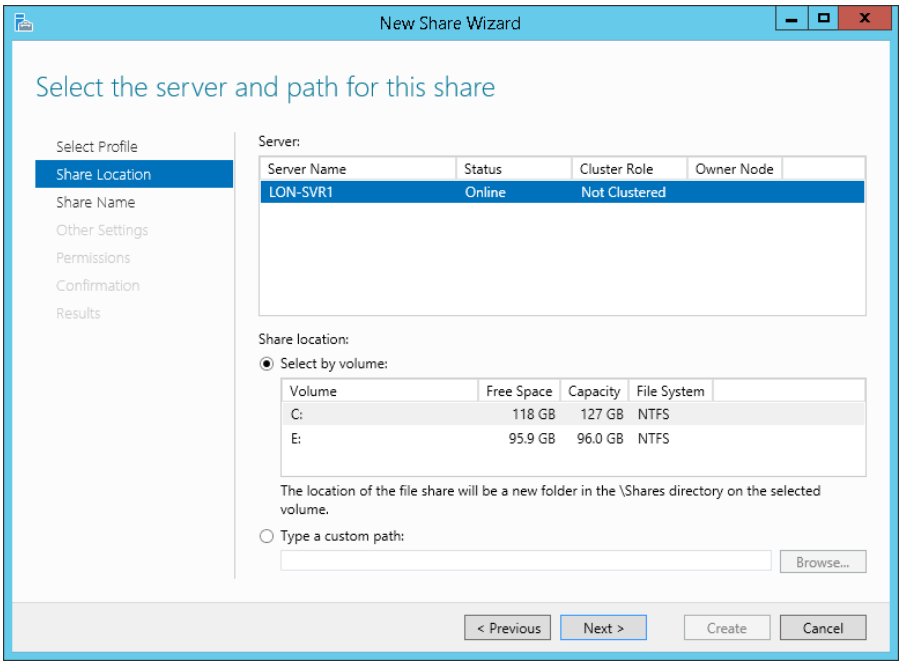

2. Cửa sổ **File and Storage Services**, chọn **Shares**, trong phần **SHARES**, bung **Tasks**, chọn **New Share….**



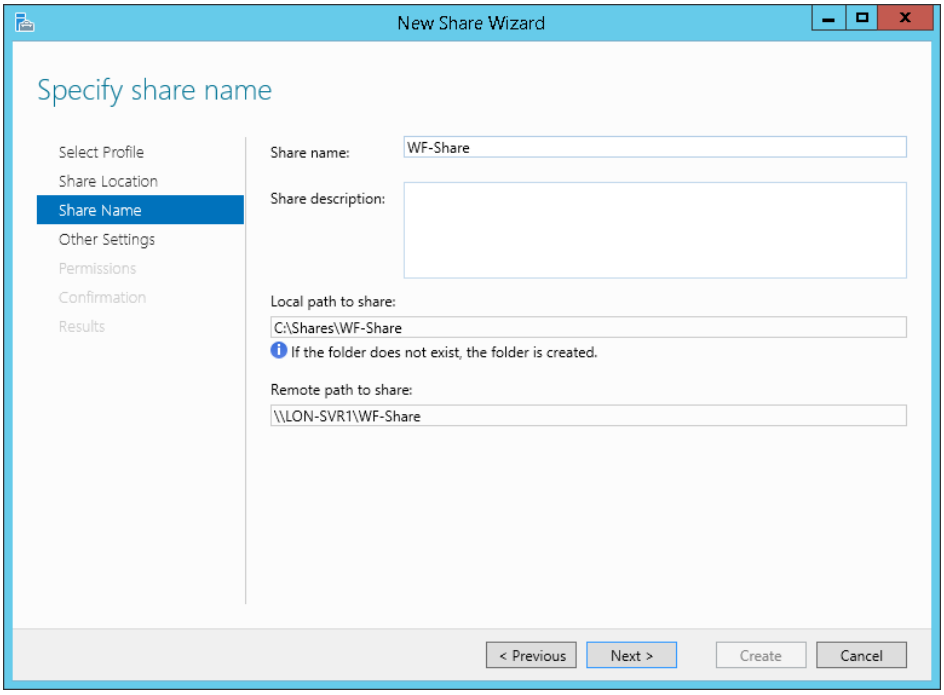

3. Cửa sổ **Select the profile for this share**, chọn **SMB Share – Quick**, và chọn **Next**.



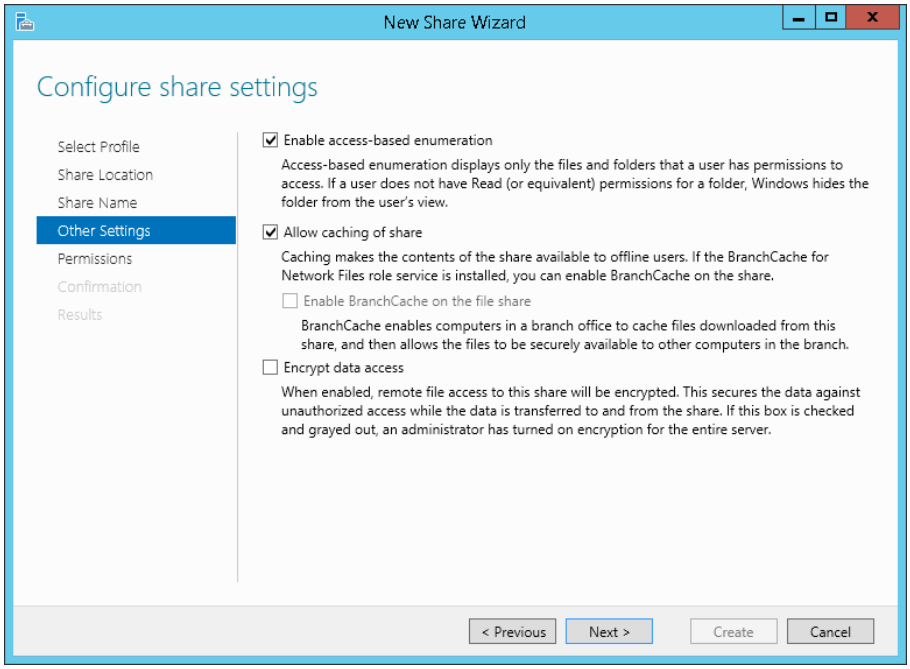
4. Cửa sổ **Select the server and path for this share**, chọn **Next**.



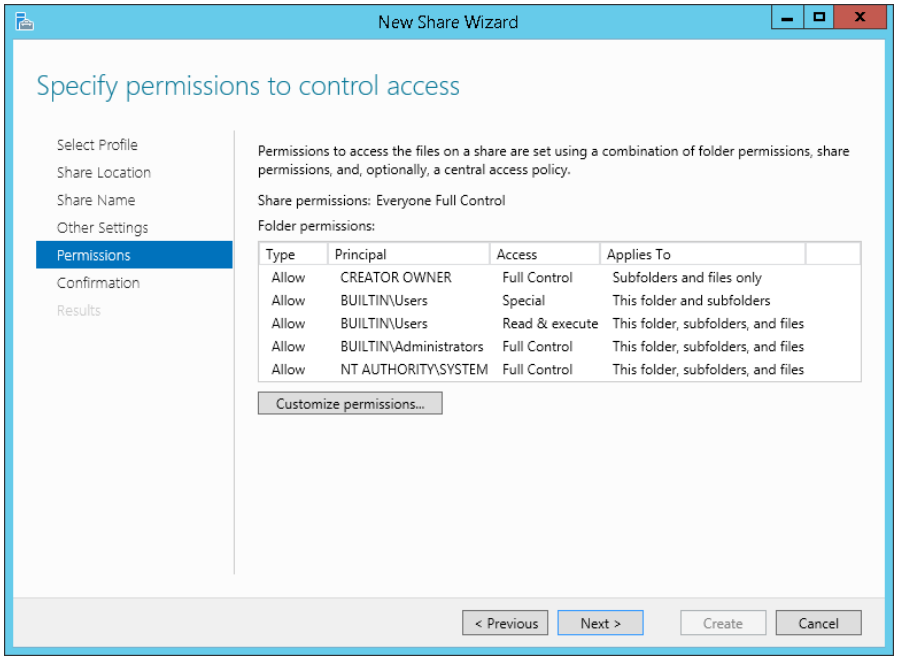

5. Cửa sổ **Specify share name**, trong ô **Share name**, nhập **WF-Share**, và chọn **Next**.



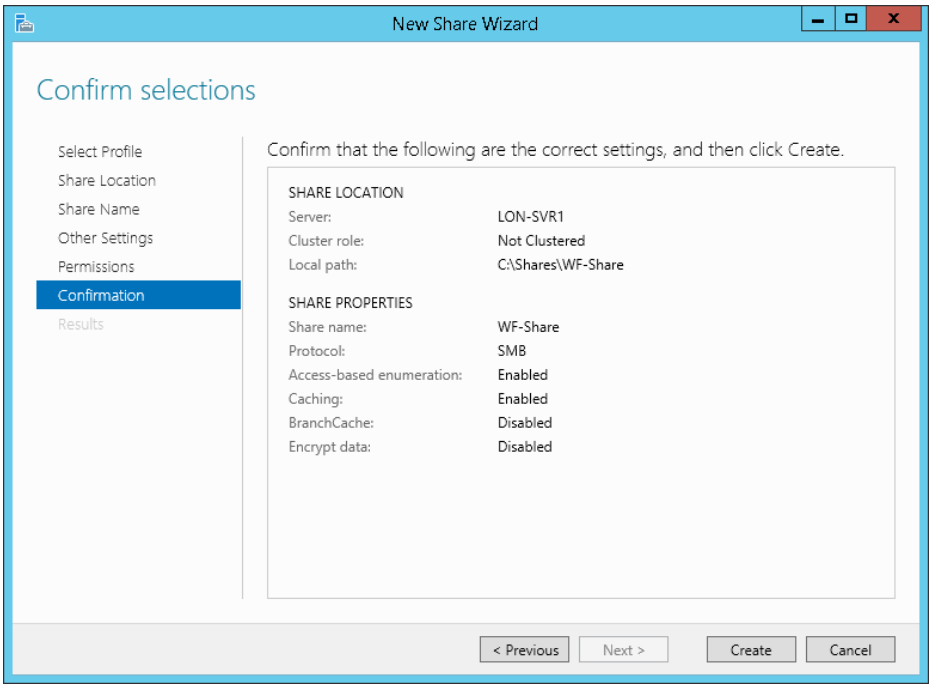
6. Cửa sổ **Configure share settings**, đánh dấu chọn **Enable access - based enumeration**, , và chọn **Next**.



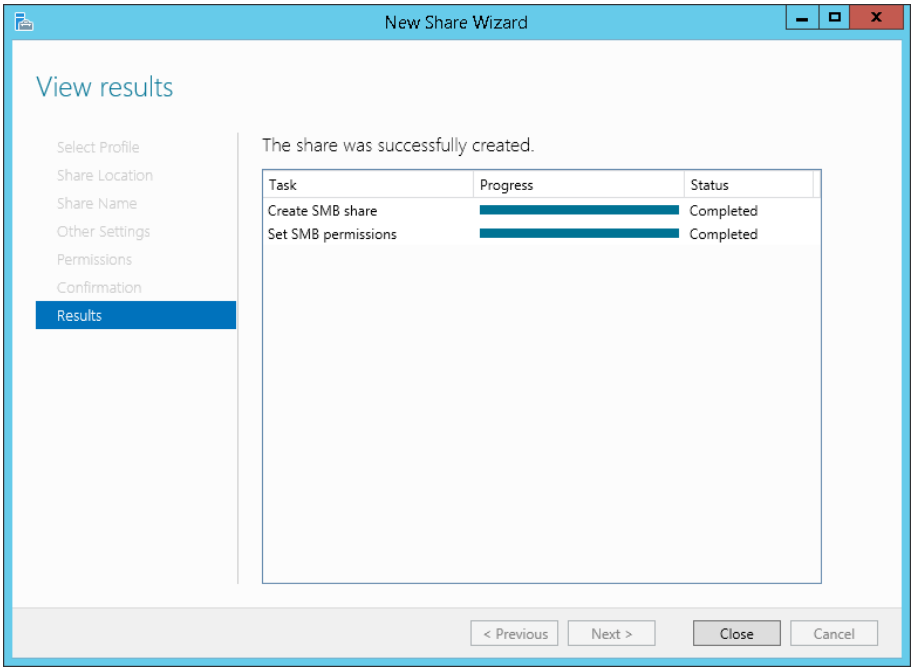

7. Cửa sổ **Specify permissions to control access**, chọn **Next**.



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

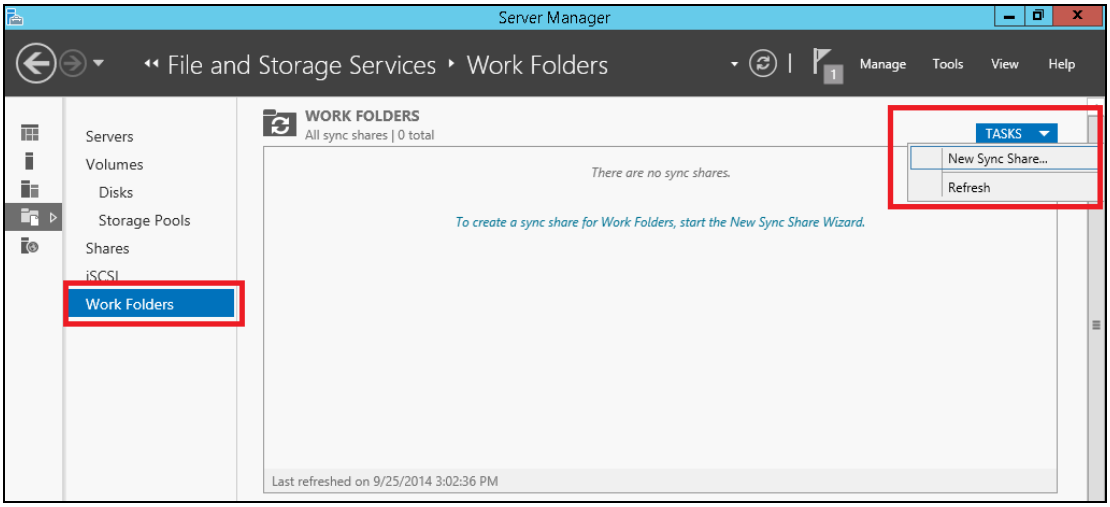



9. Cửa sổ **View results**, chọn **Close**.



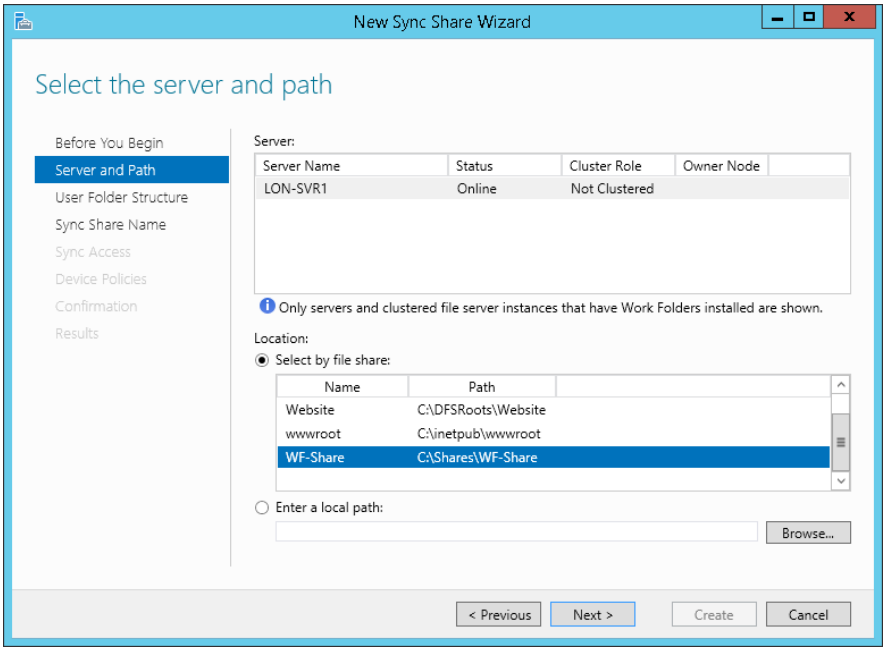
## Bước 3: Cấu hình và triển khai Work Folders

1. Trên máy **LON-SVR1**, trong **Server Manager**, chọn **File and Storage Services**, và chọn **Work Folders**, trong phần **WORK FOLDERS**, bung **TASKS**, chọn **New Sync Share….**

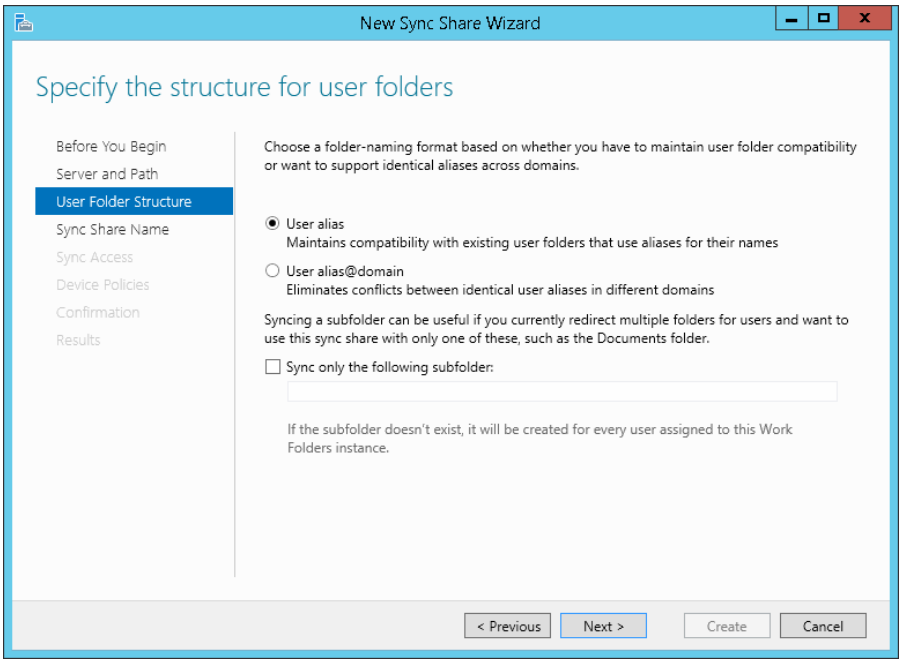



2. Cửa sổ **Before You Begin**, chọn **Next**.

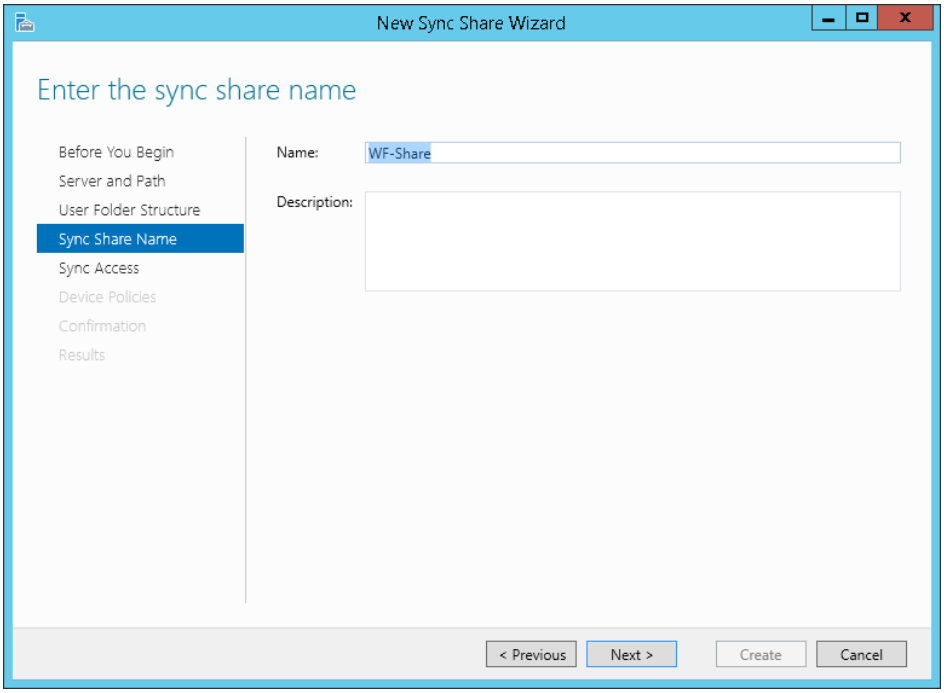
3. Cửa sổ **Select the server and path**, chọn **Select by file share**, chọn **WF-Share**, và chọn **Next**.



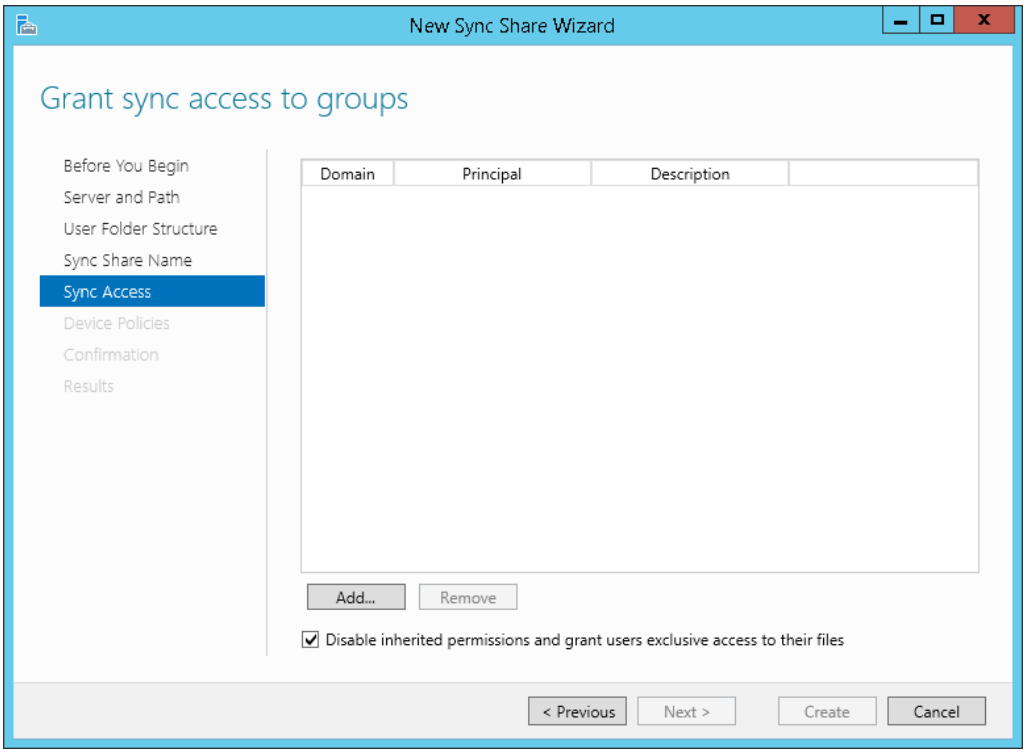
4. Cửa sổ **Specify the structure for user folders**, chọn **User alias**, chọn **Next**.



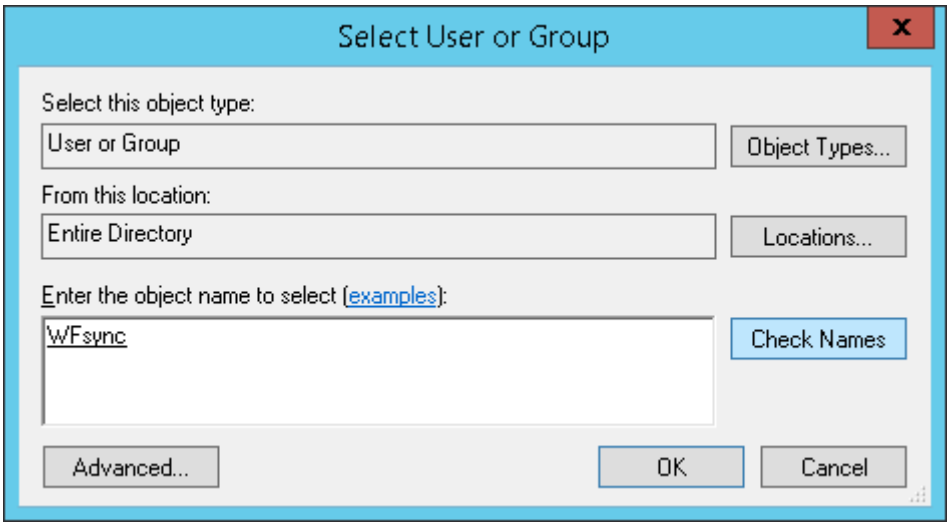

5. Cửa sổ **Enter the sync share name**, chọn **Next**.



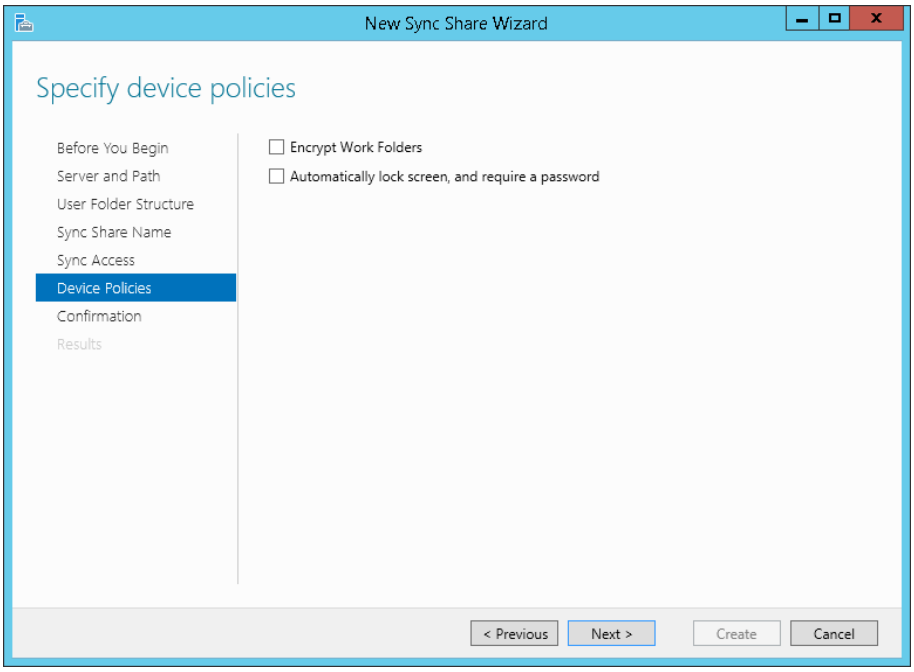
6. Cửa sổ **Grant sync access to groups**, chọn **Add**.



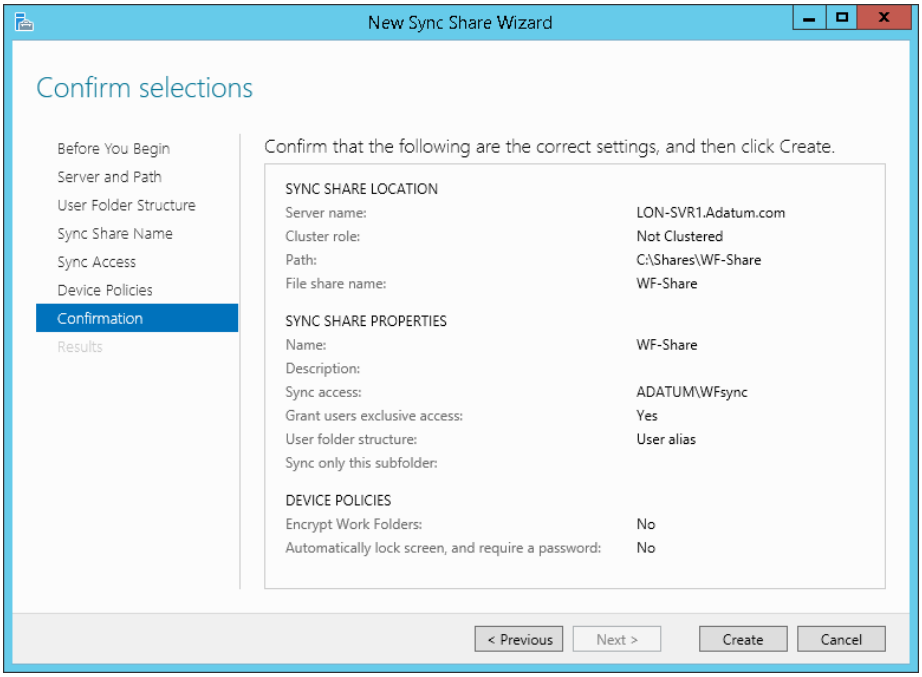

7. Hộp thoại **Select User or Group**, nhập **WFsync**, chọn **Check Names**, chọn **OK**, và chọn **Next.**



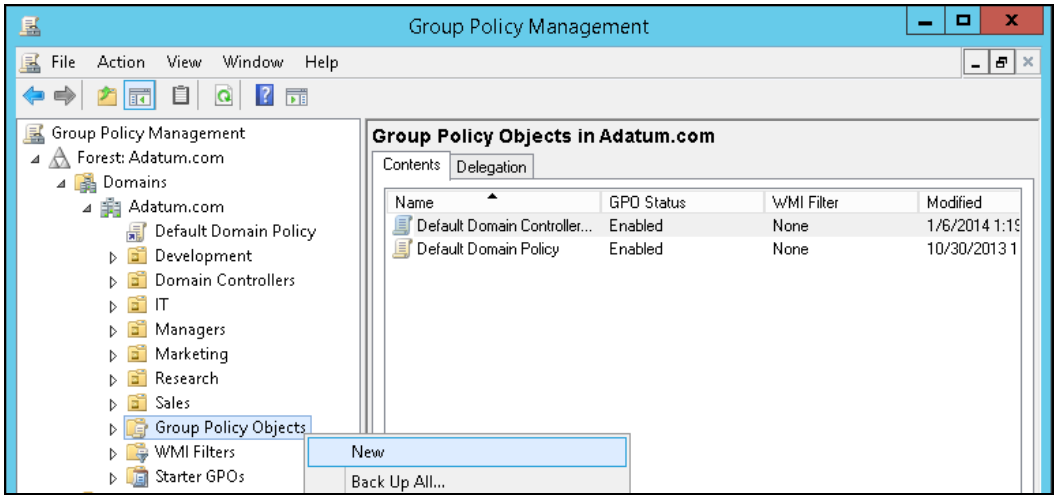
8. Cửa sổ **Specify device policies**, bỏ dấu chọn cả 2 ô, chọn **Next**.



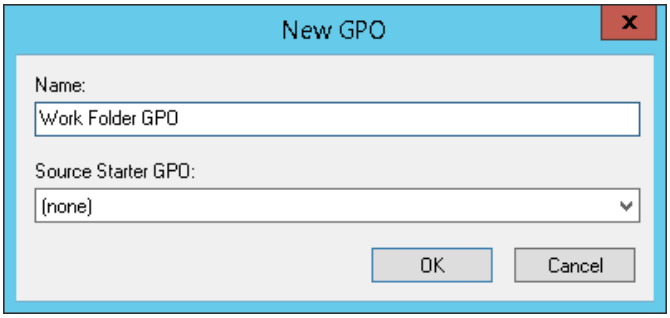

9. Cửa sổ **Confirm selections**, chọn **Create**. Sau khi tạo thành công, chọn **Close**.



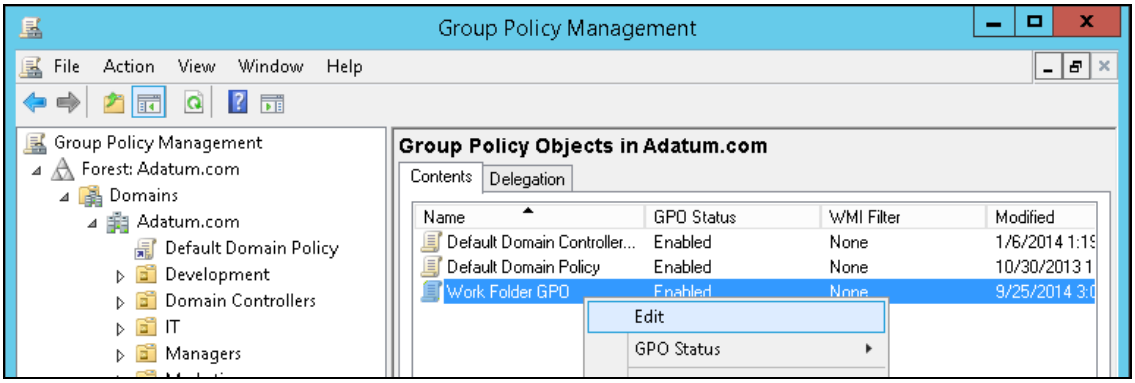
10. Qua máy **LON-DC1**. Trong **Server Manager**, bung menu **Tools**, mở **Group Policy Management**, bung **Forest: Adatum.com,** bung **Domains,** bung **Adatum.com**, chuột phải **Group Policy Objects**, chọn **New**.



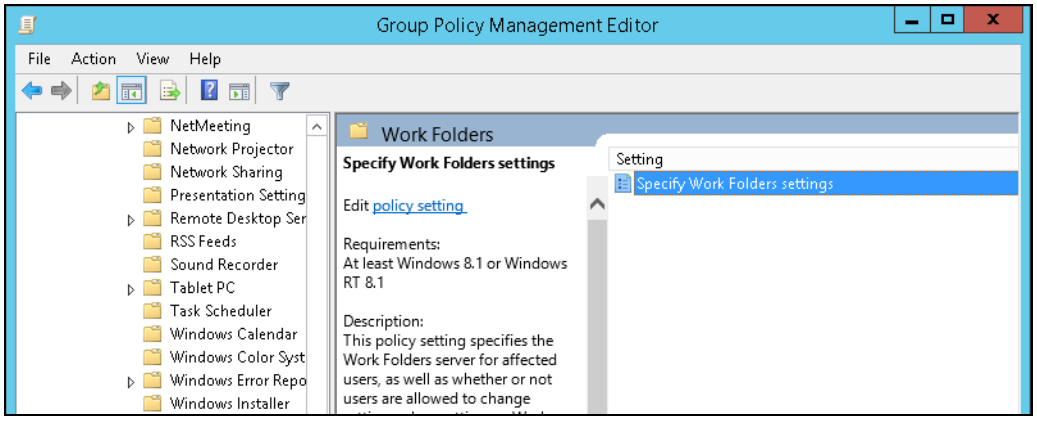

11. Hộp thoại **New GPO**, nhập **Work Folders GPO** vào ô **Name**, chọn **OK**.



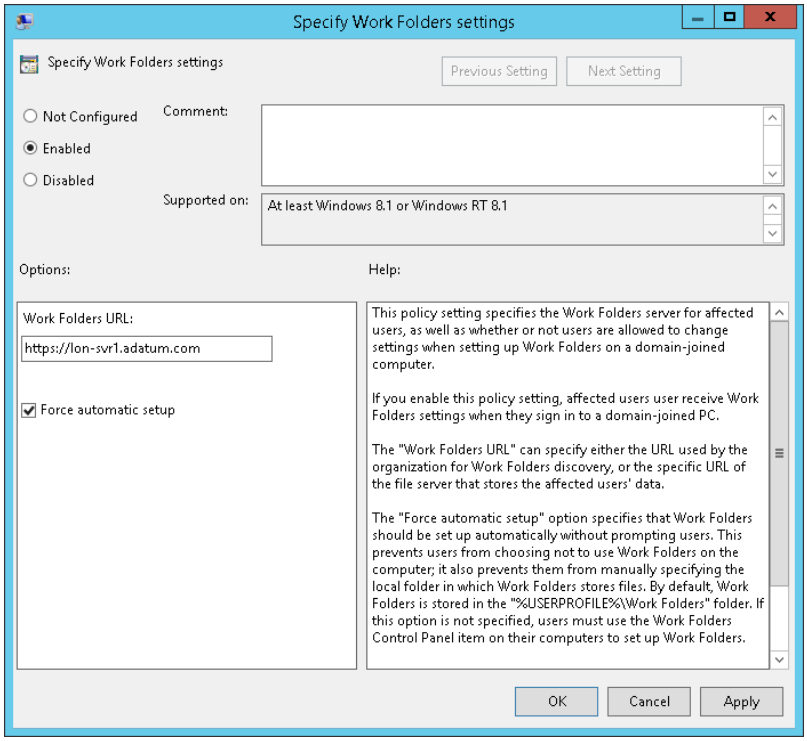

12. Chuột phải **Work Folders GPO**, chọn **Edit**.



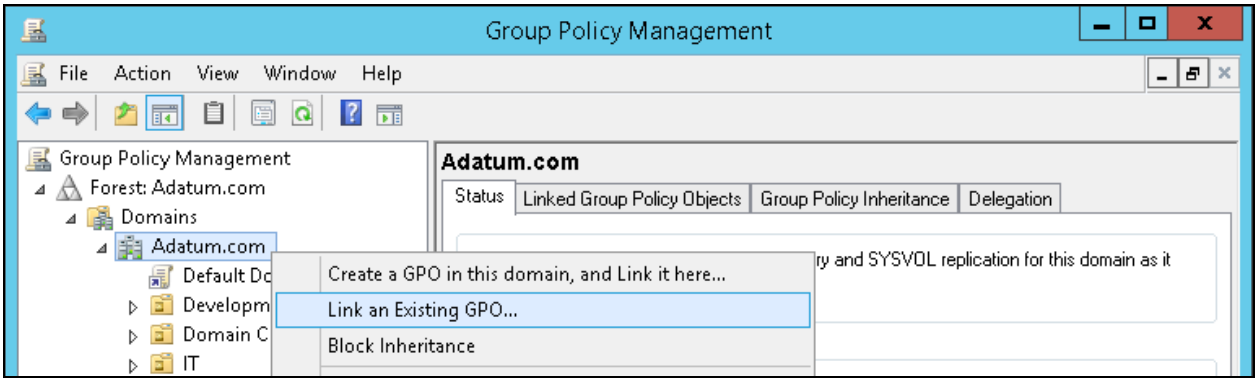
13. Trong cửa sổ **Group Policy Management Editor**, bung **User Configuration,** bung **Policies,** bung **Administrative Templates,** bung **Windows Components**, chọn **Work Folders**, nhấp đôi chuột policy **Specify Work Folders settings**



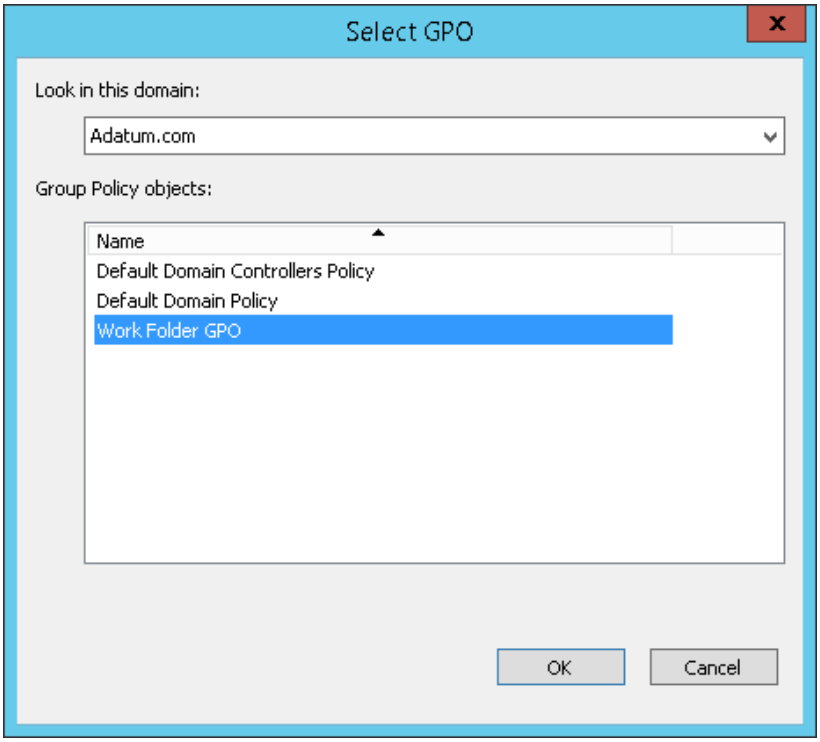

14. Cửa sổ **Specify Work Folders settings**, chọn **Enabled**. Trong ô **Work Folders URL**, nhập **https://lon-svr1.adatum.com**, đánh dấu chọn **Force automatic setup**, chọn **OK**, và tắt **Group Policy Management Editor**.



15. Cửa sổ **Group Policy Management Console**, chuột phải domain **Adatum.com**, chọn **Link an Existing GPO…**.




16. Hộp thoại **Select GPO**, chọn **Work Folders GPO**, và chọn **OK**. Tắt cửa sổ **Group Policy Management Console**.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công sở hạ tầng cho Work Folders.**

## Bài tập 2: Cấu hình AD FS và Web Application Proxy để hỗ trợ người dùng bên ngoài hệ thống truy cập Work Folder.

Để hỗ trợ người dùng khi làm việc bên ngoài hệ thống truy cập Work Folder bằng các thiết bị cá nhân của họ, bạn cần phải triển khai AD FS và Web Application Proxy. Bạn sẽ cấu hình Web Application Proxy để công bố Work Folder trên LON-SVR1 cho phép người dùng bên ngoài truy cập bằng tên wf.adatum.com.

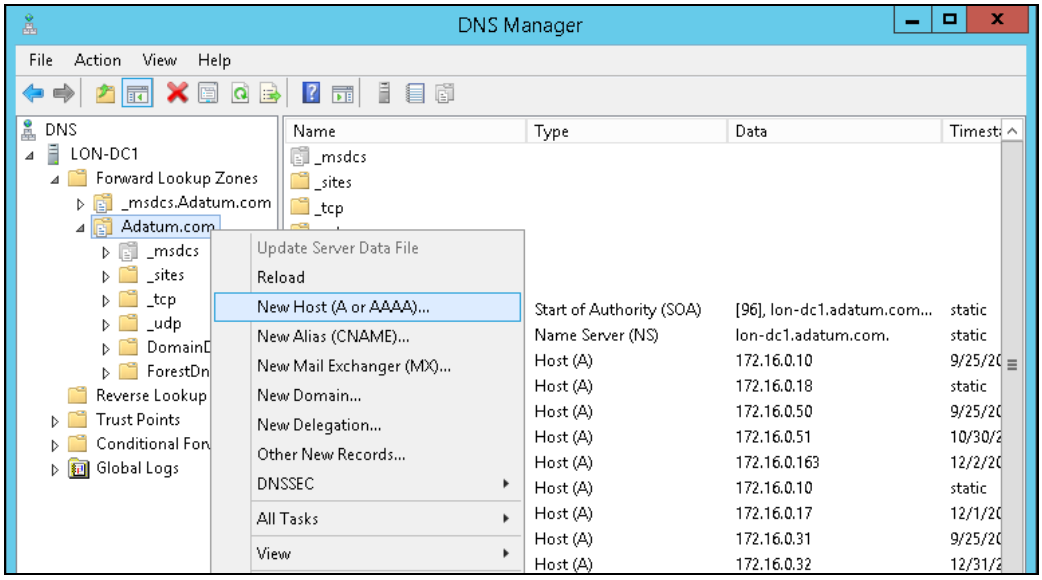
❖ **Bài thực hành bao gồm các bước:**

1. Cài đặt AD FS
2. Cấu hình AD FS
3. Cài đặt Web Application Proxy
4. Cấu hình Web Application Proxy
5. Công bố Work Folders thông qua Web Application Proxy

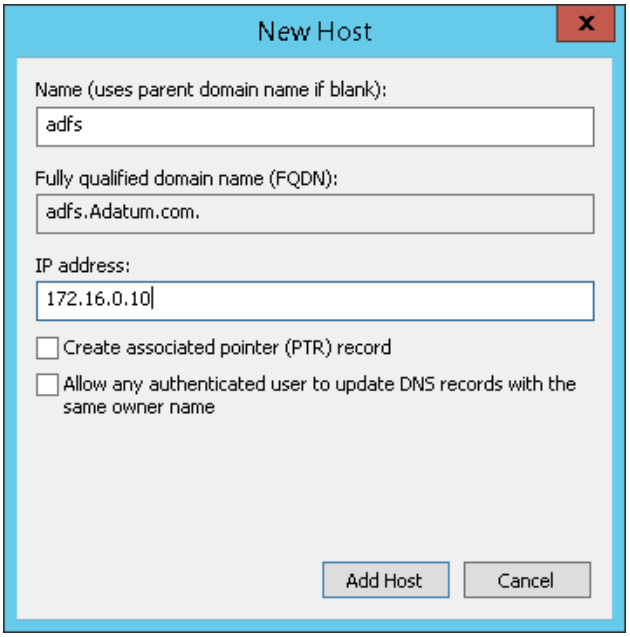
❖ **Thực hiện:**

### Bước 1: Cài đặt AD FS

1. Trên máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **DNS**. Bung **LON-DC1**, bung **Forward Lookup Zones**, chuột phải **Adatum.com**, chọn **New Host (A or AAAA)**.

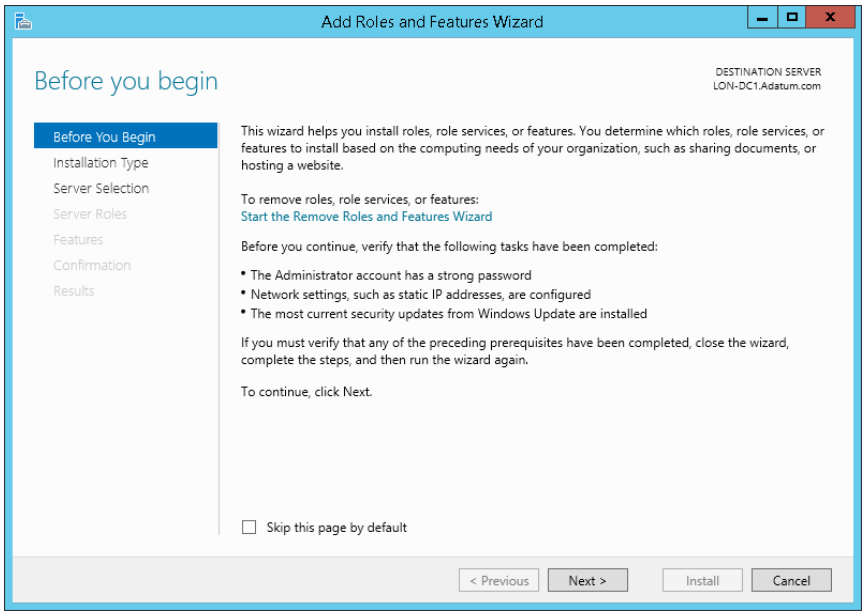


2. Hộp thoại **New Host**, trong ô **Name**, nhập **adfs**, trong ô **IP address**, nhập **172.16.0.10**, chọn **Add Host**, chọn **OK**, và chọn **Done**. Tắt cửa sổ DNS Manager.

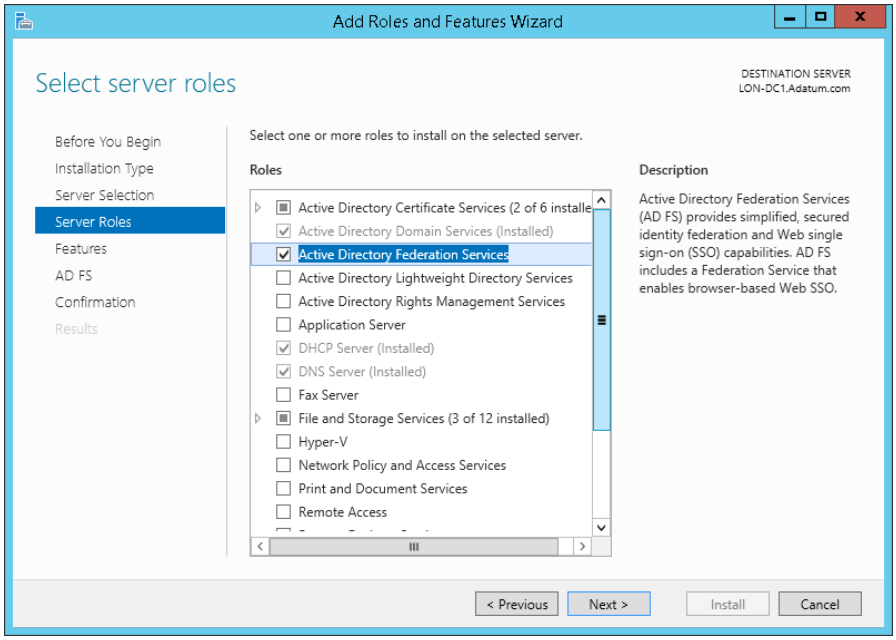



3. Trong **Server Manager**, chọn **Add Roles and Features**.

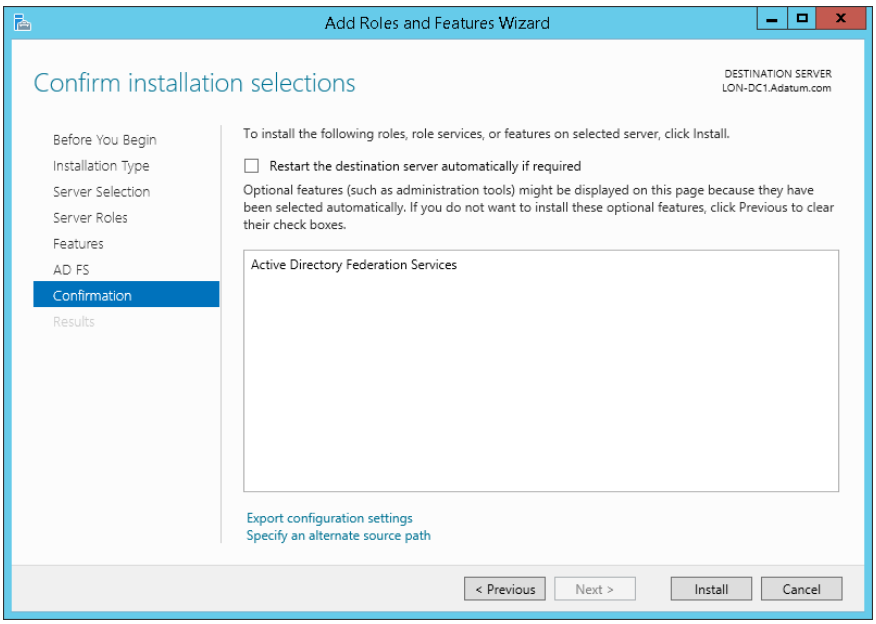
4. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.



5. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Federation Services**, và chọn **Next** 3 lần.

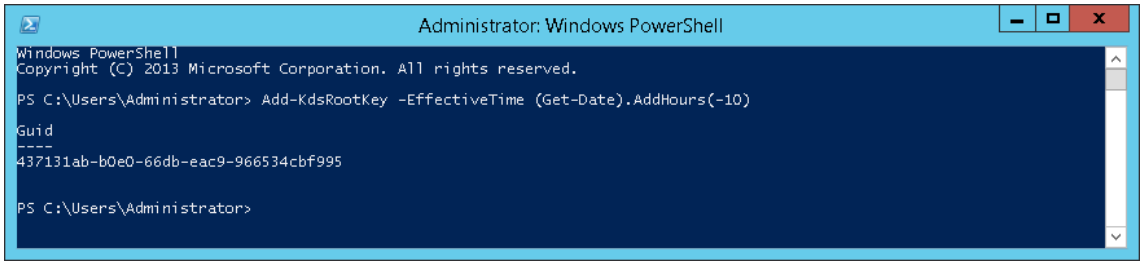



6. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.



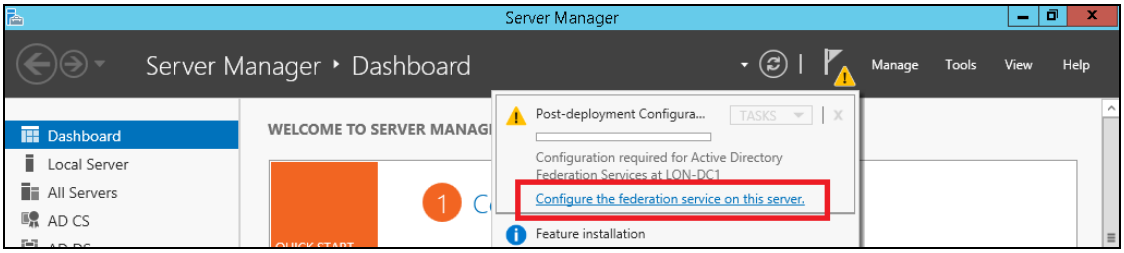
7. Mở **Windows PowerShell**, gõ lệnh:

**Add-KdsRootKey – EffectiveTime (Get-Date).AddHours(-10)**

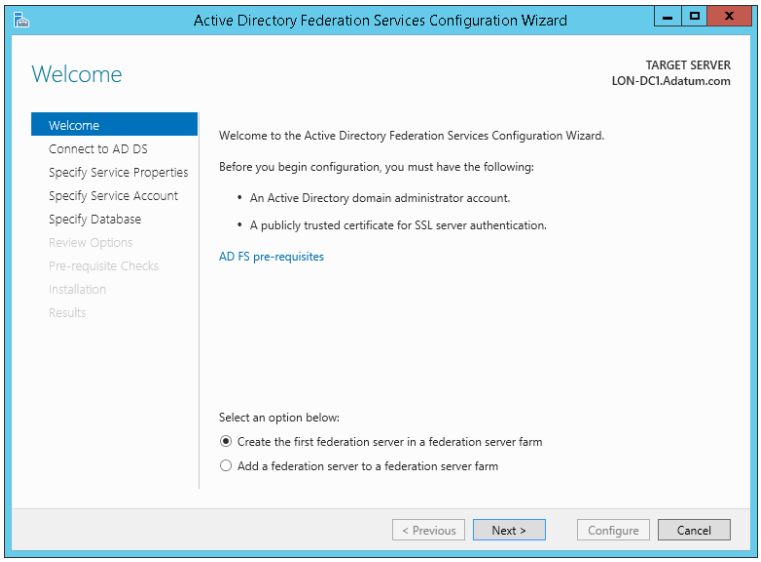



## Bước 2: Cấu hình AD FS

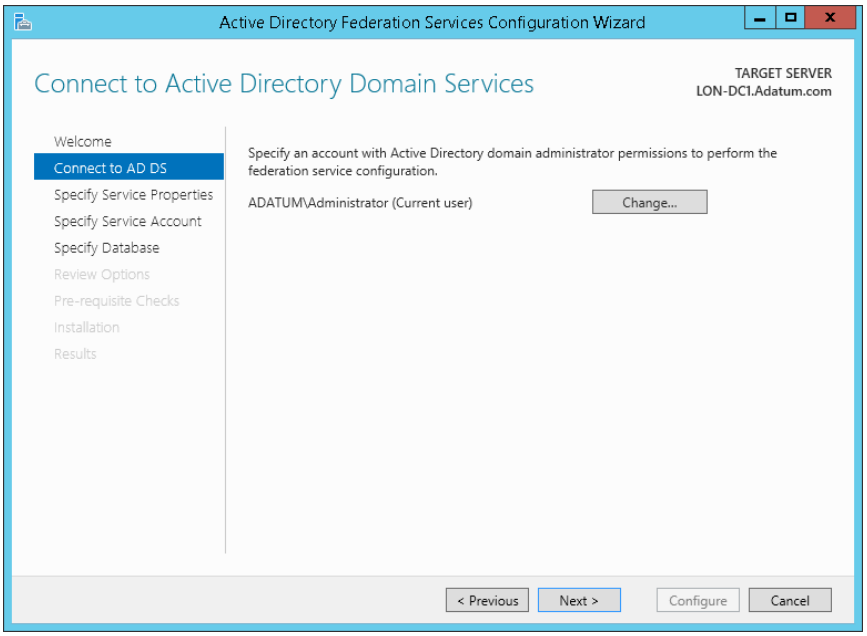
1. Trên máy **LON-DC1**, trong **Server Manager**, chọn biểu tượng **Notifications** màu vàng, chọn **Configure the federation service on this server**.



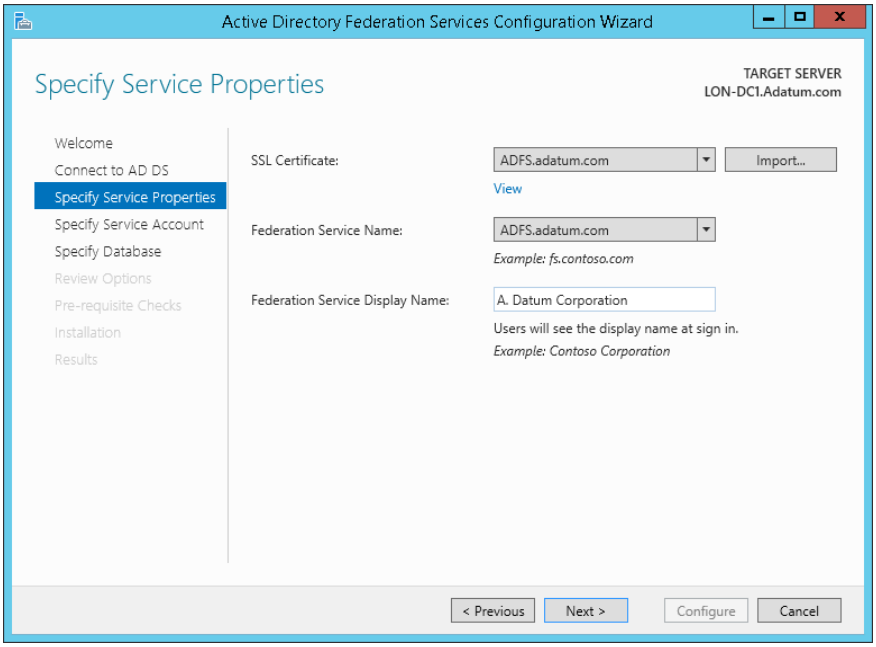

2. Cửa sổ **Welcome**, chọn **Create the first federation server in a federation server farm**, và chọn **Next**.



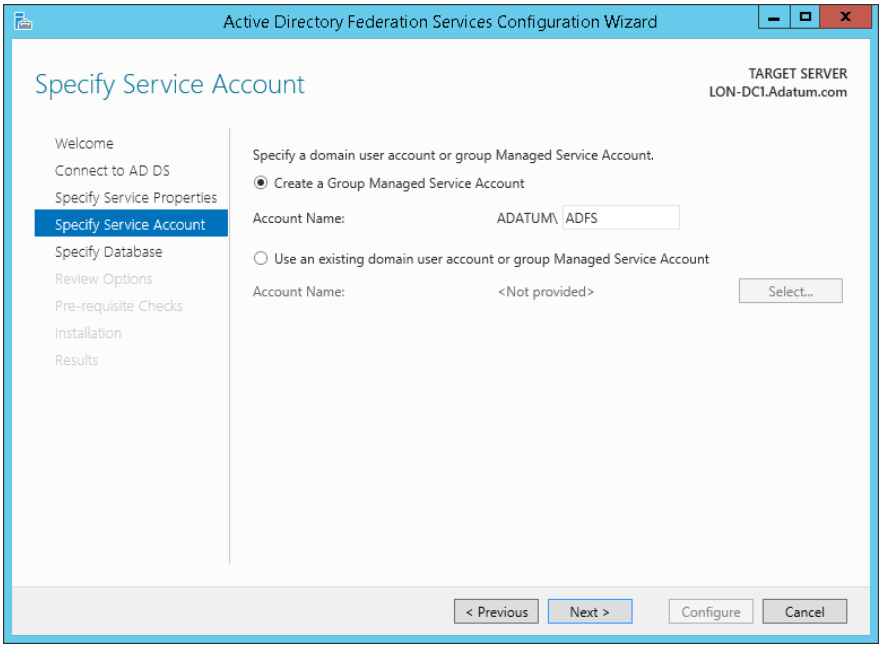
3. Cửa sổ **Connect to Active Directory Domain Services**, chọn **Next**.



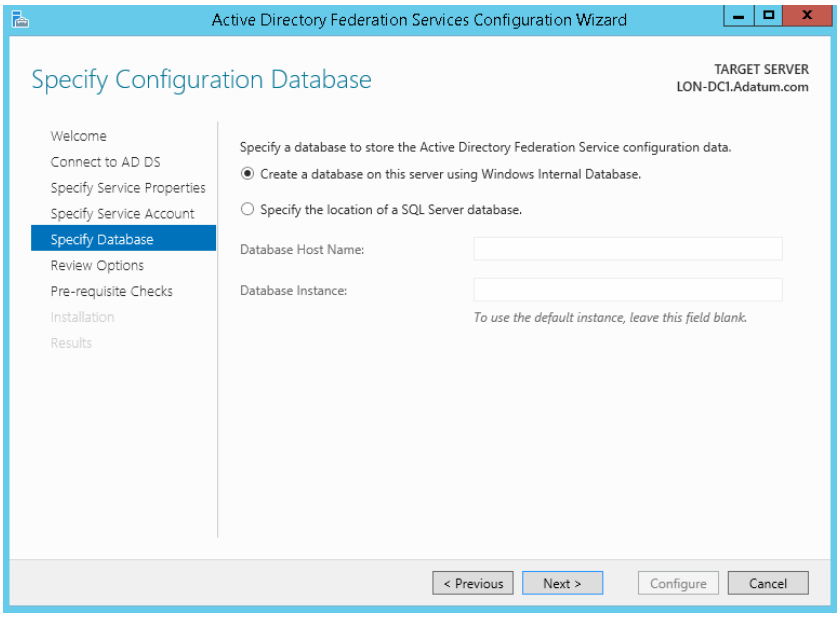

4. Cửa sổ **Specify Service Properties**, bung ô **SSL Certificate**, chọn **ADFS.adatum.com**. Trong ô **Federation Service Display Name**, nhập **A. Datum Corporation**, và chọn **Next**.



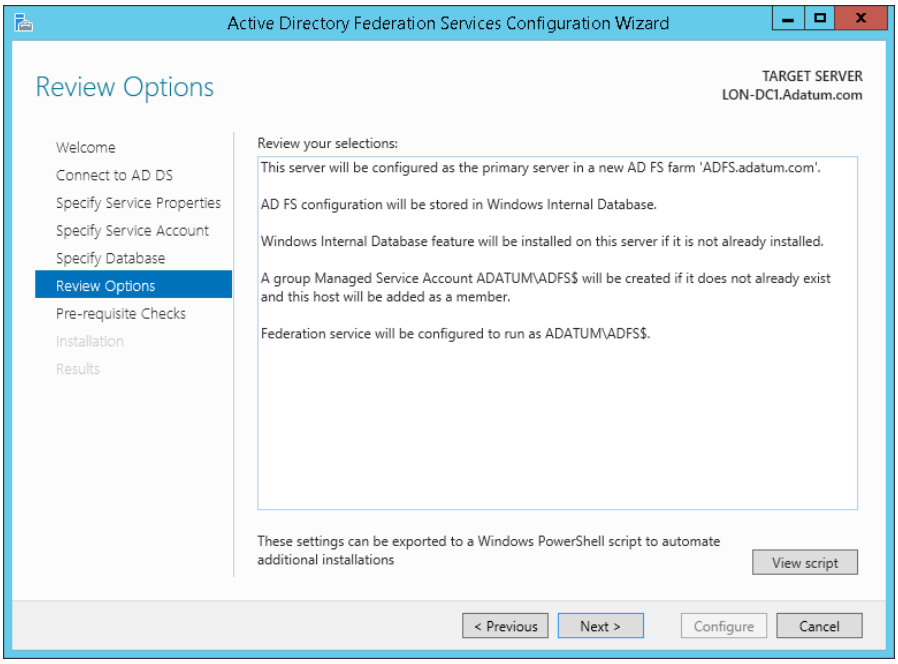
5. Cửa sổ **Specify Service Account**, chọn **Create a Group Managed Service Account**, trong ô **Account Name**, nhập **ADFS**, và chọn **Next**.



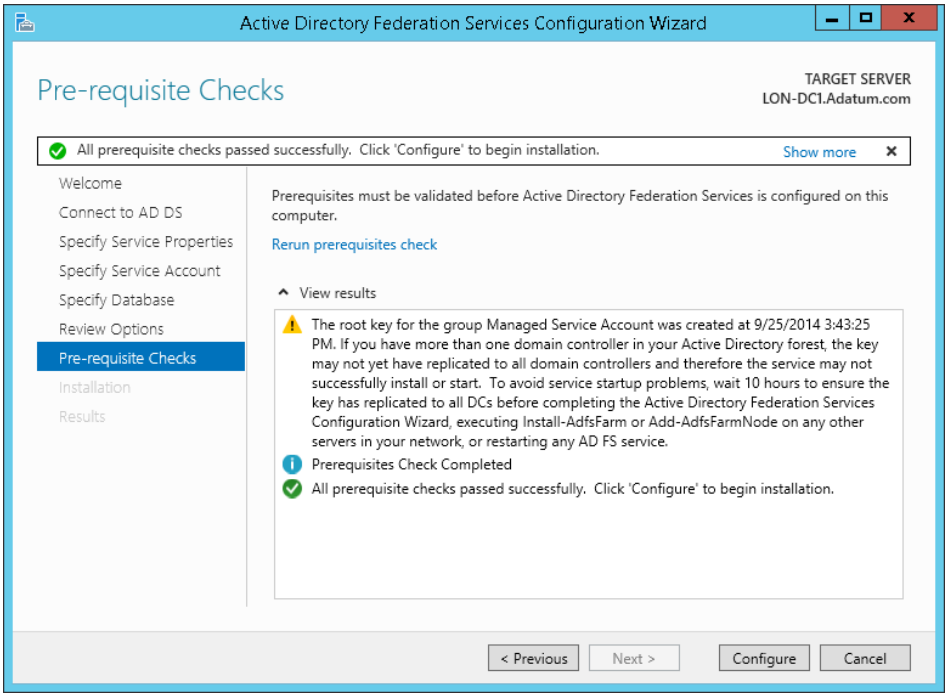

6. Cửa sổ **Specify Configuration Database**, chọn **Create a database on this server using Windows Internal Database**, và chọn **Next**.



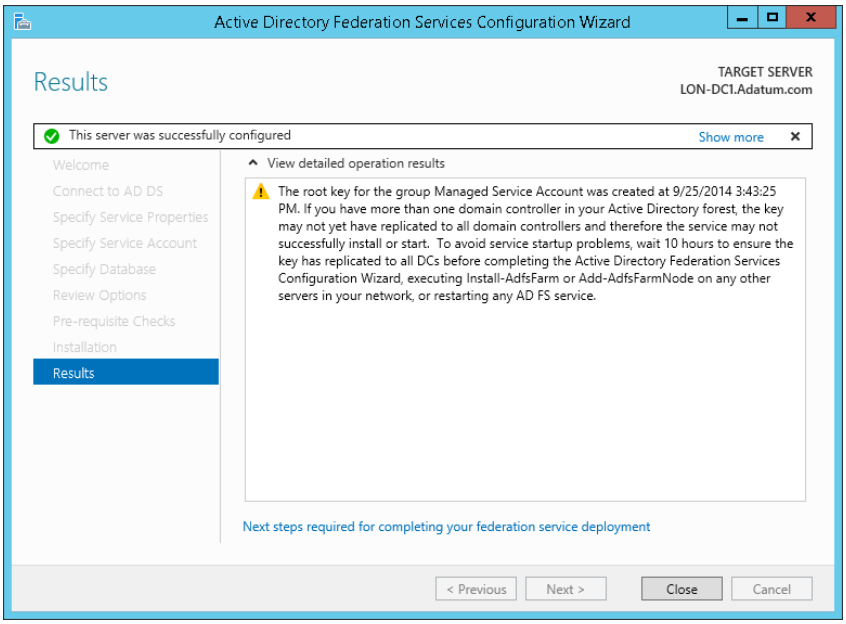
7. Cửa sổ **Review Options**, chọn **Next**.




8. Cửa sổ **Pre-requisite Checks**, chọn **Configure**.



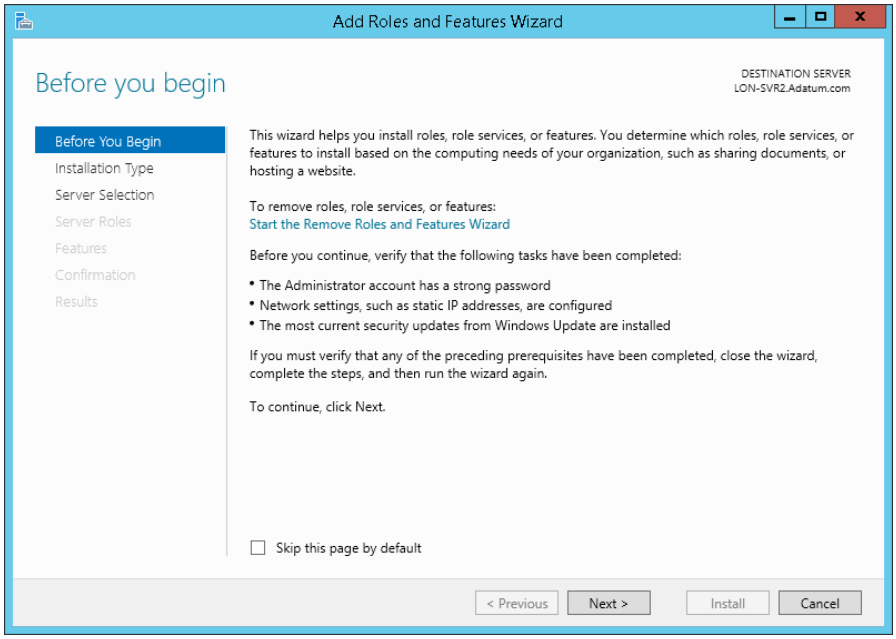
9. Cửa sổ **Results**, chọn **Close**.



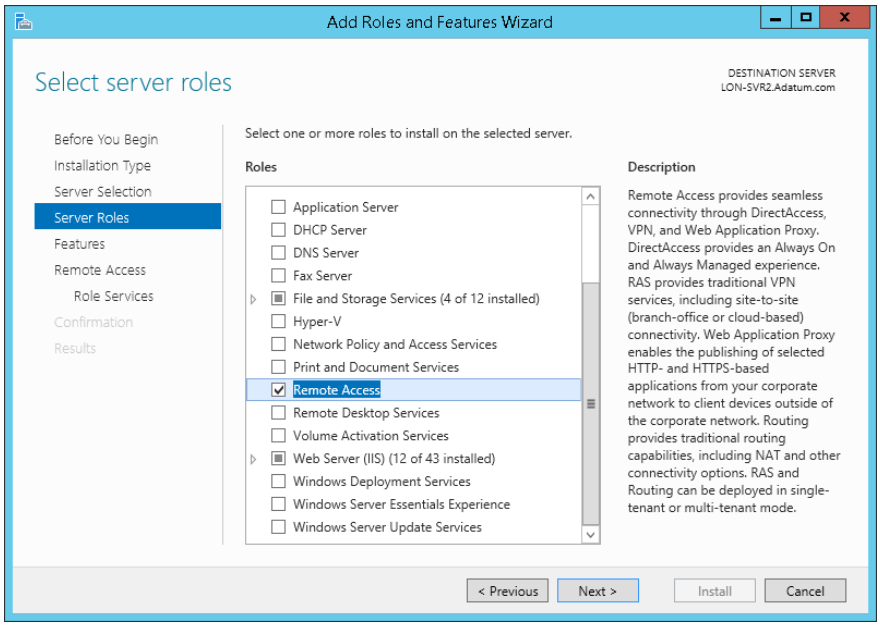

## Bước 3: Cài đặt Web Application Proxy

1. Qua máy **LON-SVR2**, trong **Server Manager**, chọn **Add Roles and Features**.

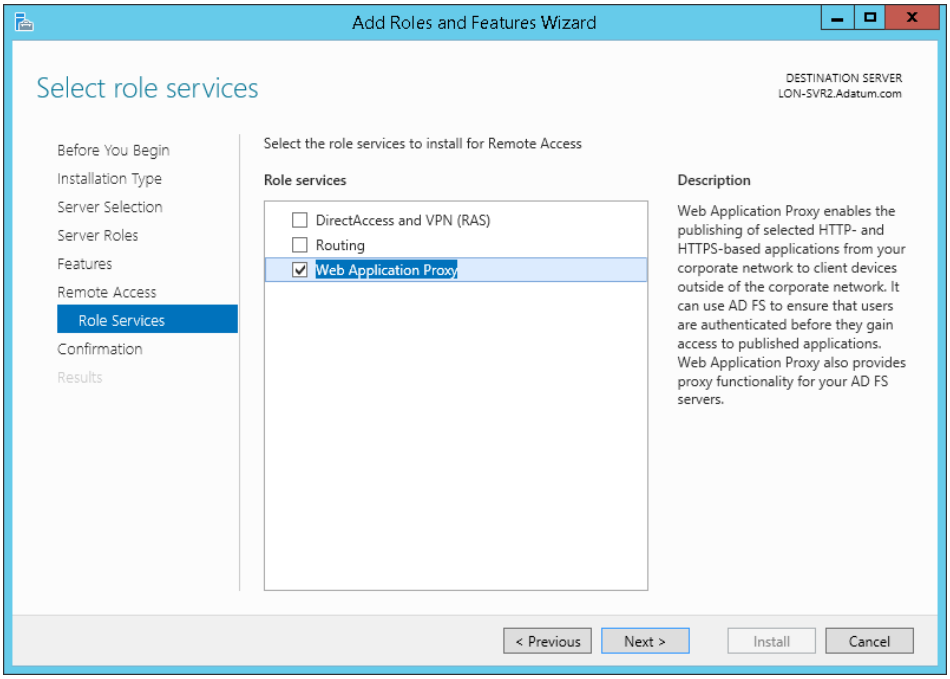
2. Cửa sổ **Before You Begin**, chọn **Next** 3 lần.



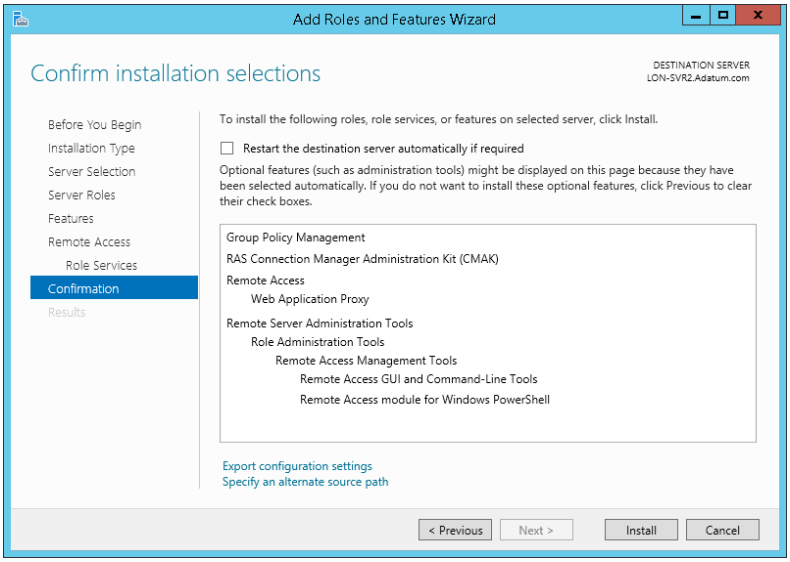
3. Cửa sổ **Select server roles**, đánh dấu chọn **Remote Access**, chọn **Next** 3 lần.




4. Cửa sổ **Select role services**, đánh dấu chọn **Web Application Proxy**, chọn **Add Features,** và chọn **Next.**



5. Cửa sổ **Confirm installation selections**, chọn **Install**. Sau khi cài đặt thành công, chọn **Close**.

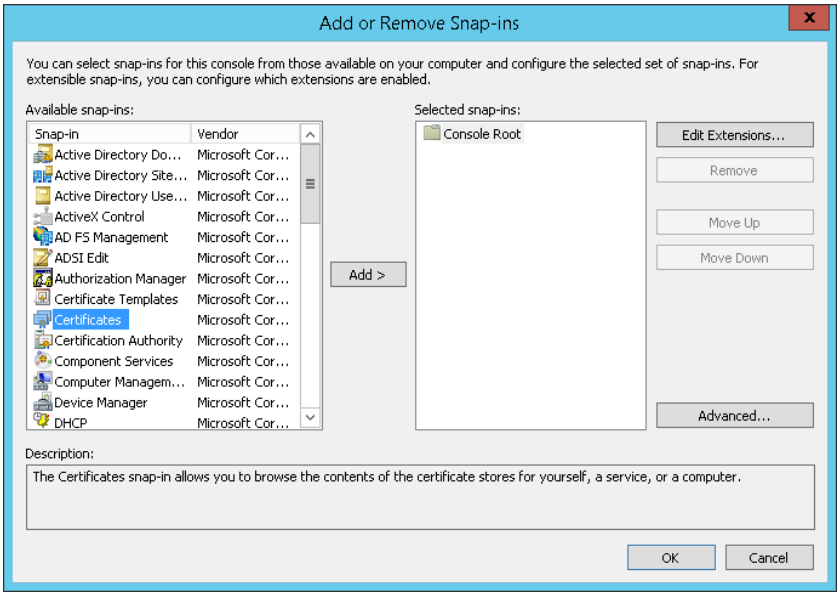



## Bước 4: Cấu hình Web Application Proxy

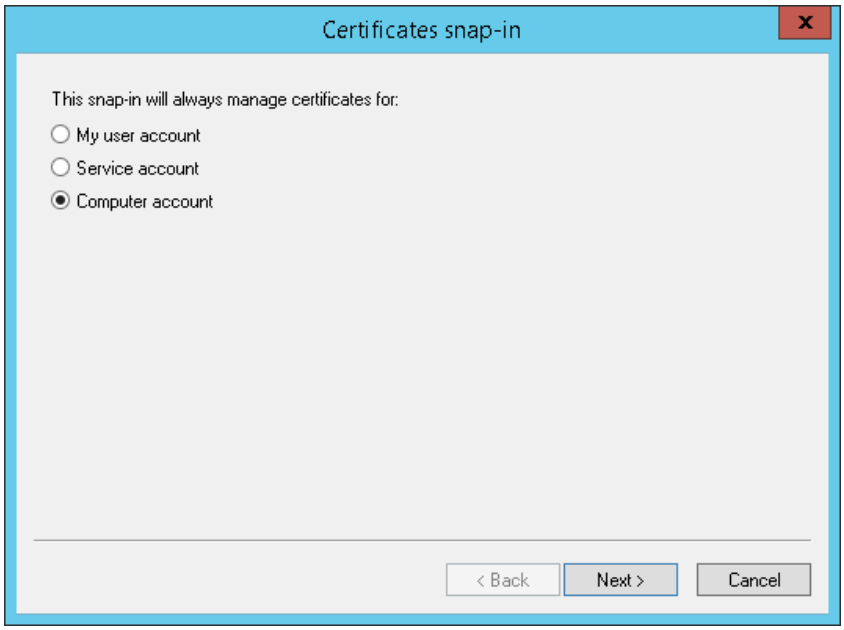
1. Qua máy **LON-DC1.**

2. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.

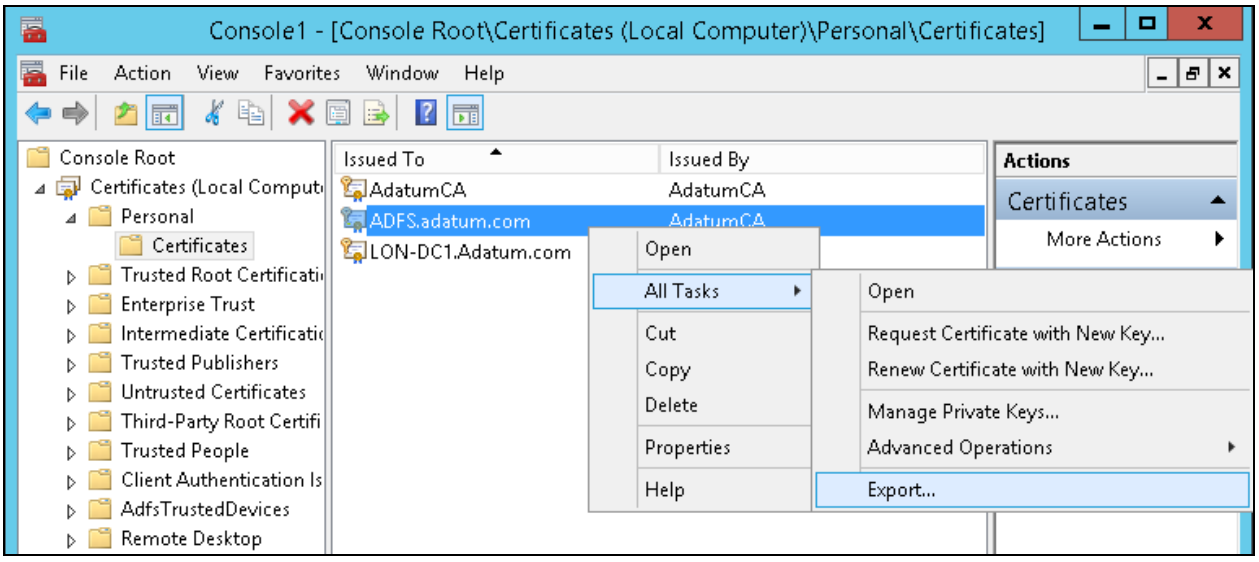
3. Cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**., chọn **Add.**



4. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**. Cửa sổ **Select Computer,** chọn **Local Computer (the computer this console is running on)**, chọn **Finish**, và chọn **OK**.

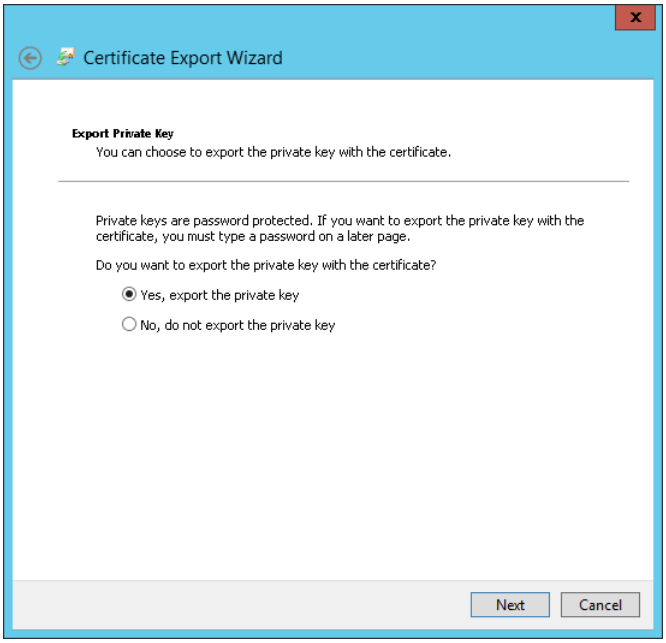



5. Trong cửa sổ **MMC**, bung **Certificates (Local Computer)**, bung **Personal**, chọn **Certificates**. Chuột phải **ADFS.adatum.com**, bung **All Tasks**, chọn **Export**.

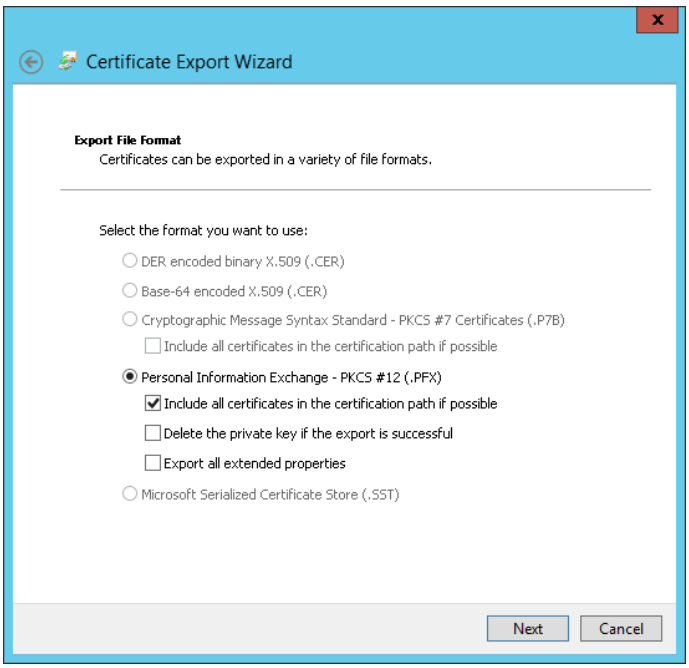


6. Cửa sổ **Welcome**, chọn **Next**.

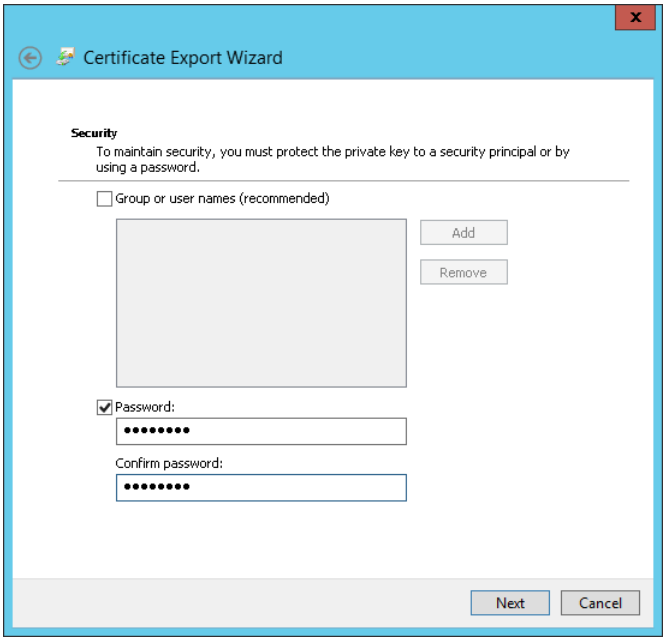
7. Cửa sổ **Export Private Key**, chọn **Yes, export the private key**, và chọn **Next**.



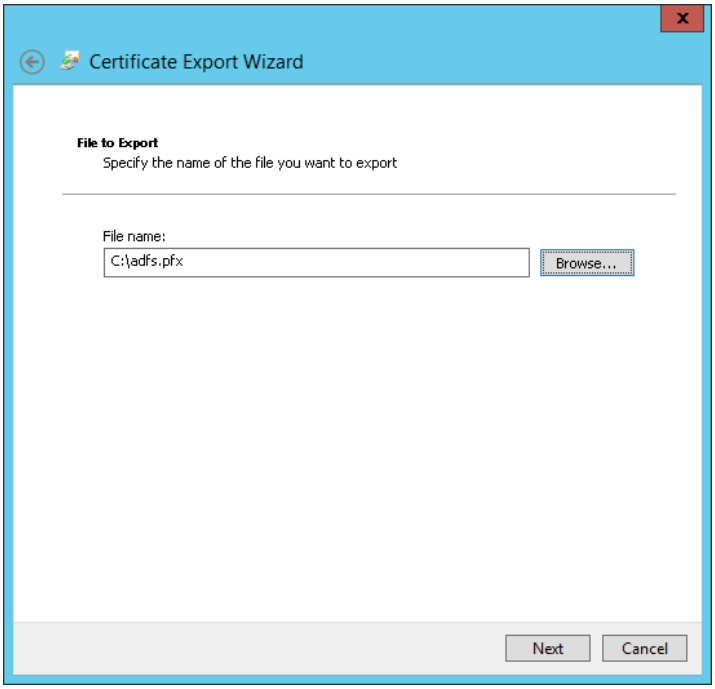

8. Cửa sổ **Export File Format**, chọn **Next**.



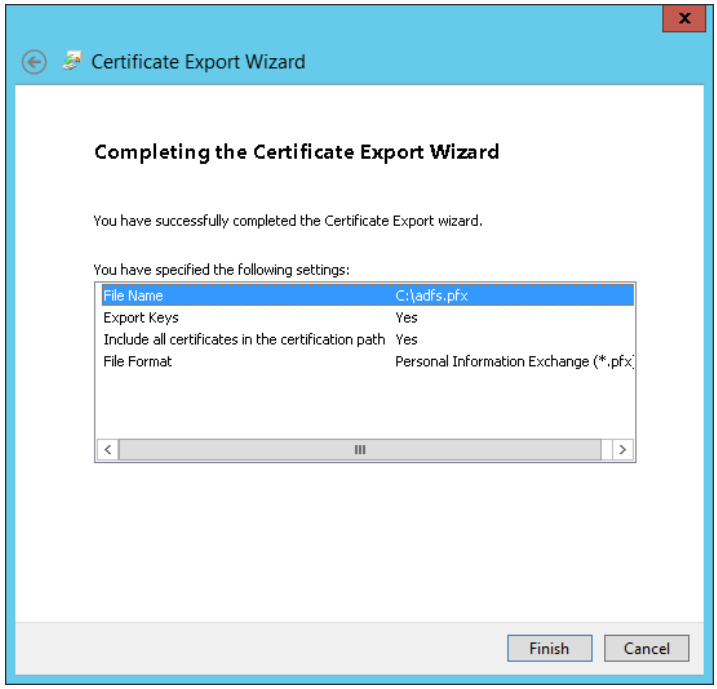
9. Cửa sổ **Security**, đánh dấu chọn **Password**. Nhập **Pa$$w0rd** vào ô **Password** và **Confirm password**, chọn **Next**.




10. Cửa sổ **File to Export**, trong ô **File name**, nhập **C:\adfs.pfx**, và chọn **Next**.



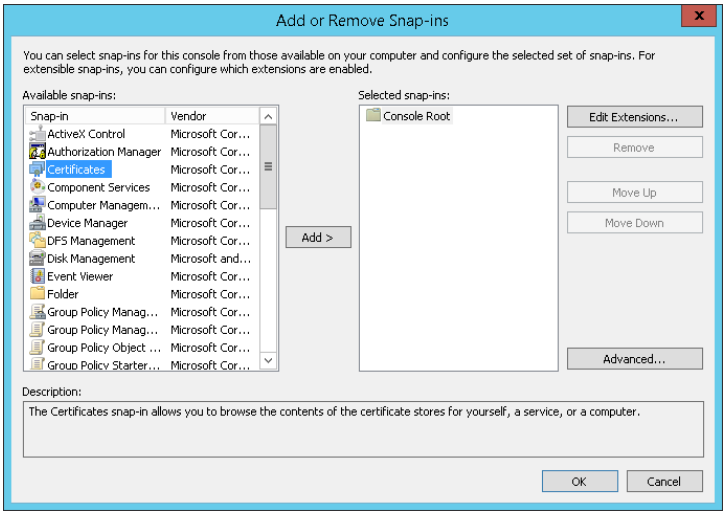
11. Cửa sổ **Completing the Certificate Export Wizard**, chọn **Finish**, và chọn **OK.** Tắt **Console1**, chọn **No**.



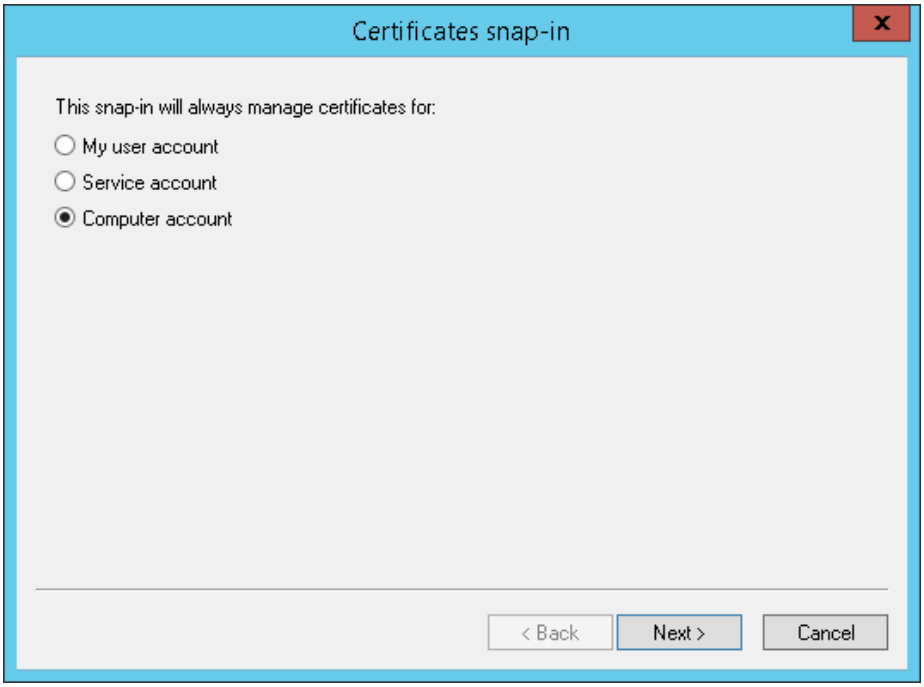

12. Qua máy **LON-SVR2**.

13. Mở **MMC**, bung menu **File**, chọn **Add/Remove Snap-in**.

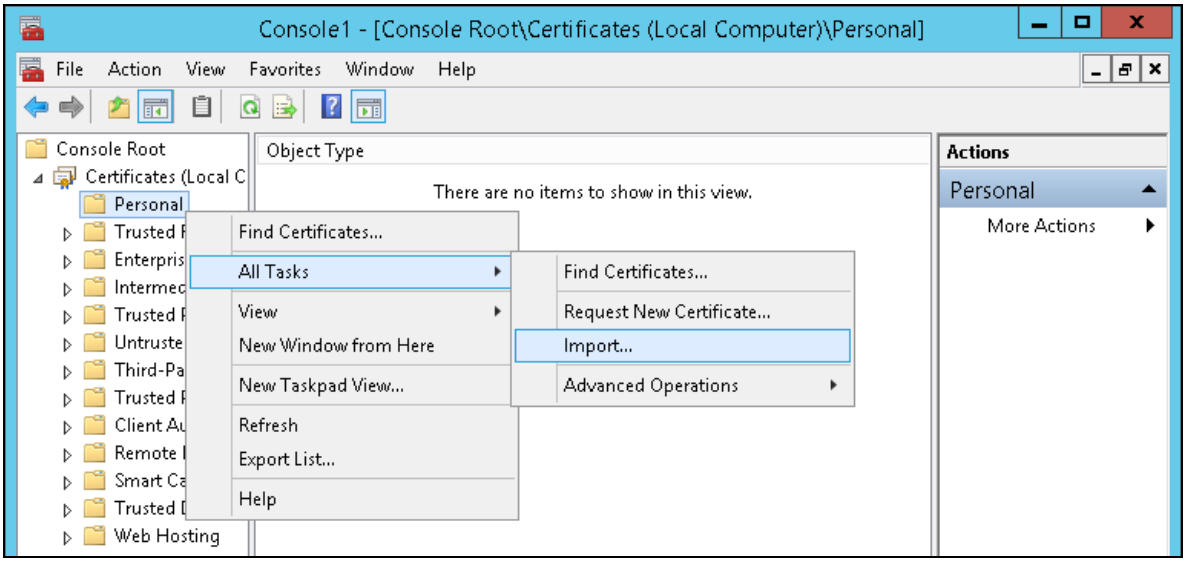
14. Cửa sổ **Add or Remove Snap-ins**, chọn **Certificates**, chọn **Add**.



15. Cửa sổ **Certificates snap-in**, chọn **Computer account**, chọn **Next**. Cửa sổ **Select Computer**, chọn **Finish**, và chọn **OK**.

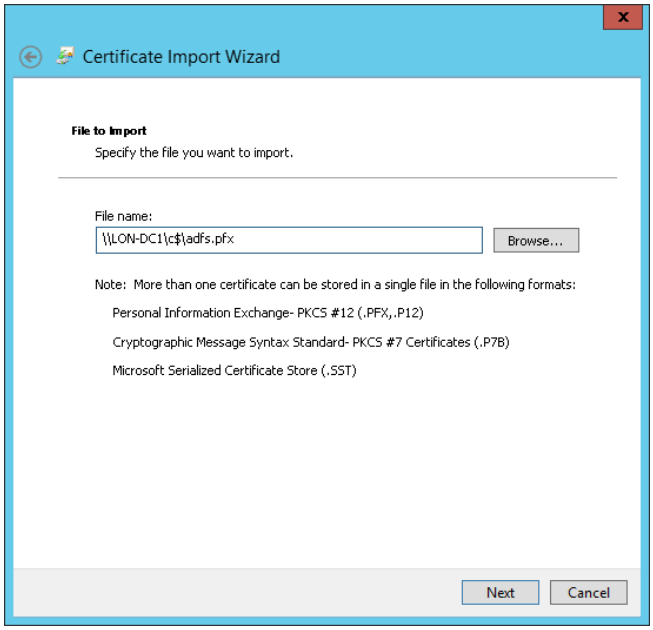



16. Trong cửa sổ **MMC**, bung **Certificates (Local Computer)**, chuột phải **Personal**, bung **All Tasks**, chọn **Import**.

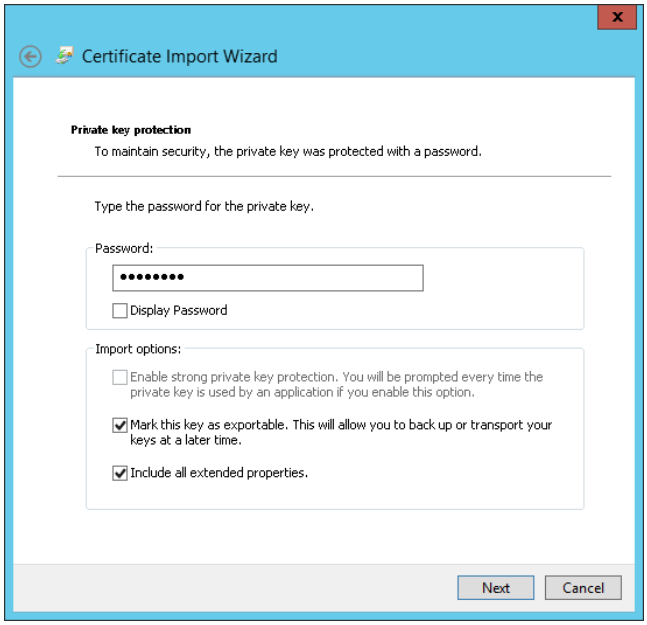


17. Cửa sổ **Welcome**, chọn **Next**.

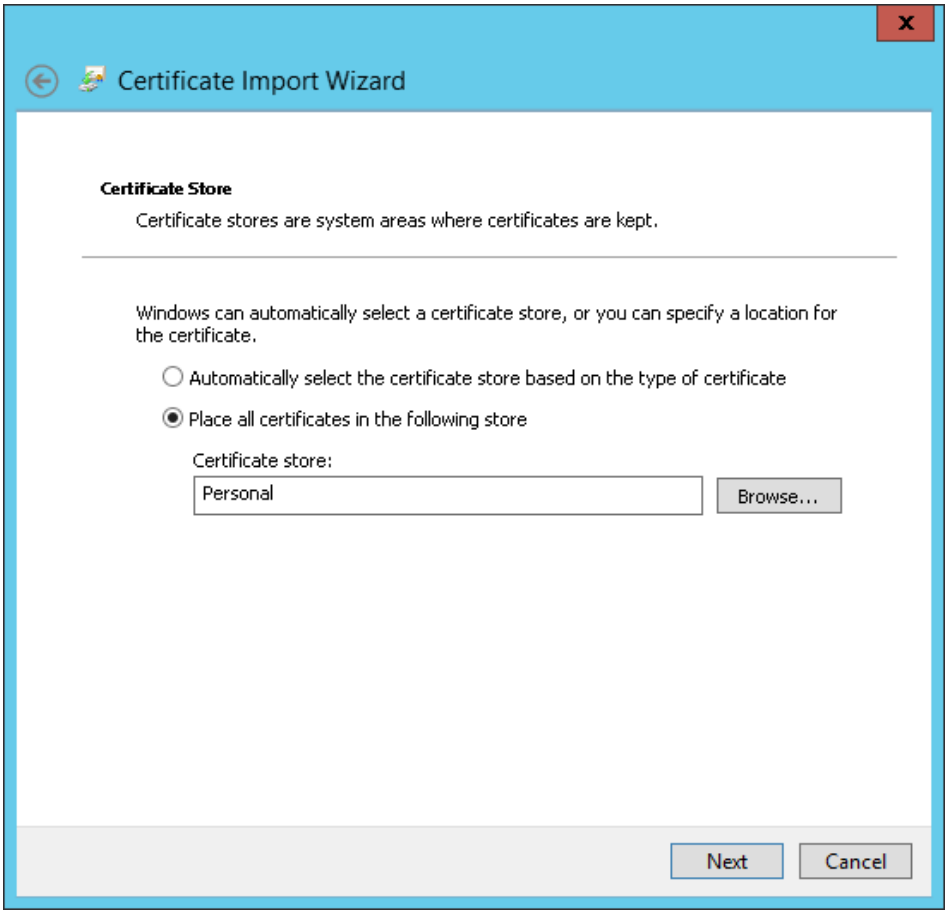
18. Cửa sổ **File to Import**, trong ô **File name**, nhập **\\LON-DC1\c$\adfs.pfx**, chọn **Next**.



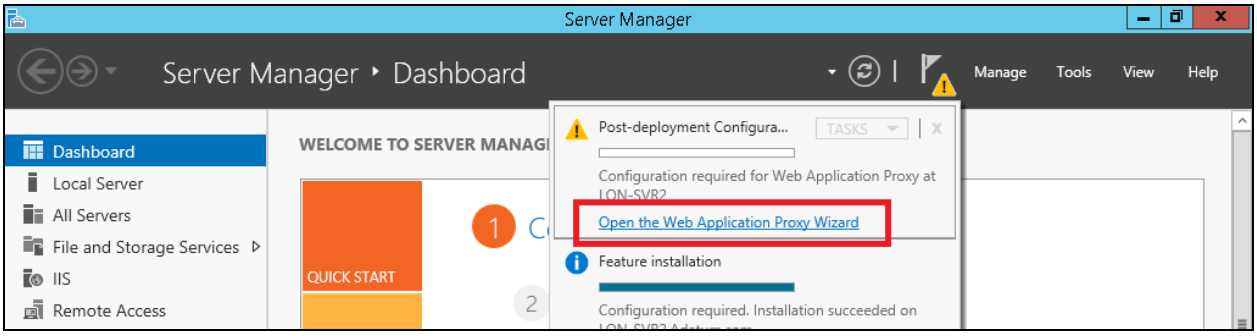

19. Cửa sổ **Private key protection**, trong ô **Password**, nhập **Pa$$w0rd**, đánh dấu chọn **Mark this key as exportable**, chọn **Next**.



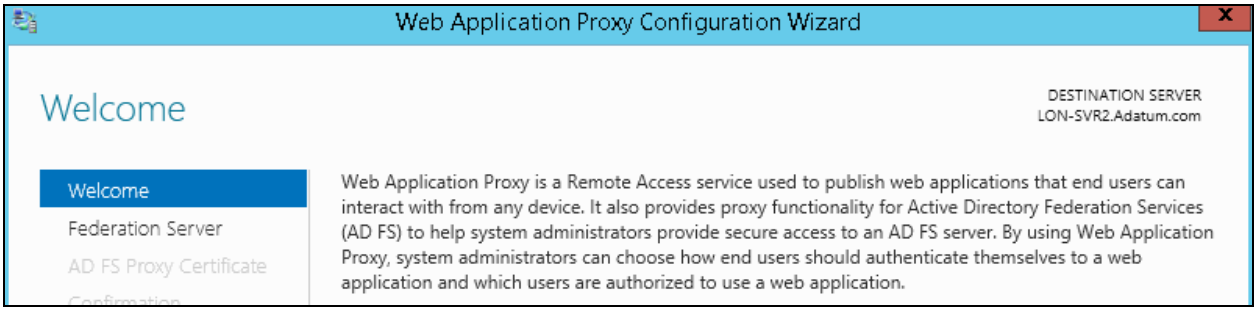
20. Cửa sổ **Certificate Store**, chọn **Next**, chọn **Finish**, và chọn **OK.** Tắt cửa sổ **Console1,** chọn **No.**




21. Trên máy **LON-SVR2**, trong **Server Manager**, chon biểu tượng **Notifications**, chọn **Open the Web Application Proxy Wizard**.

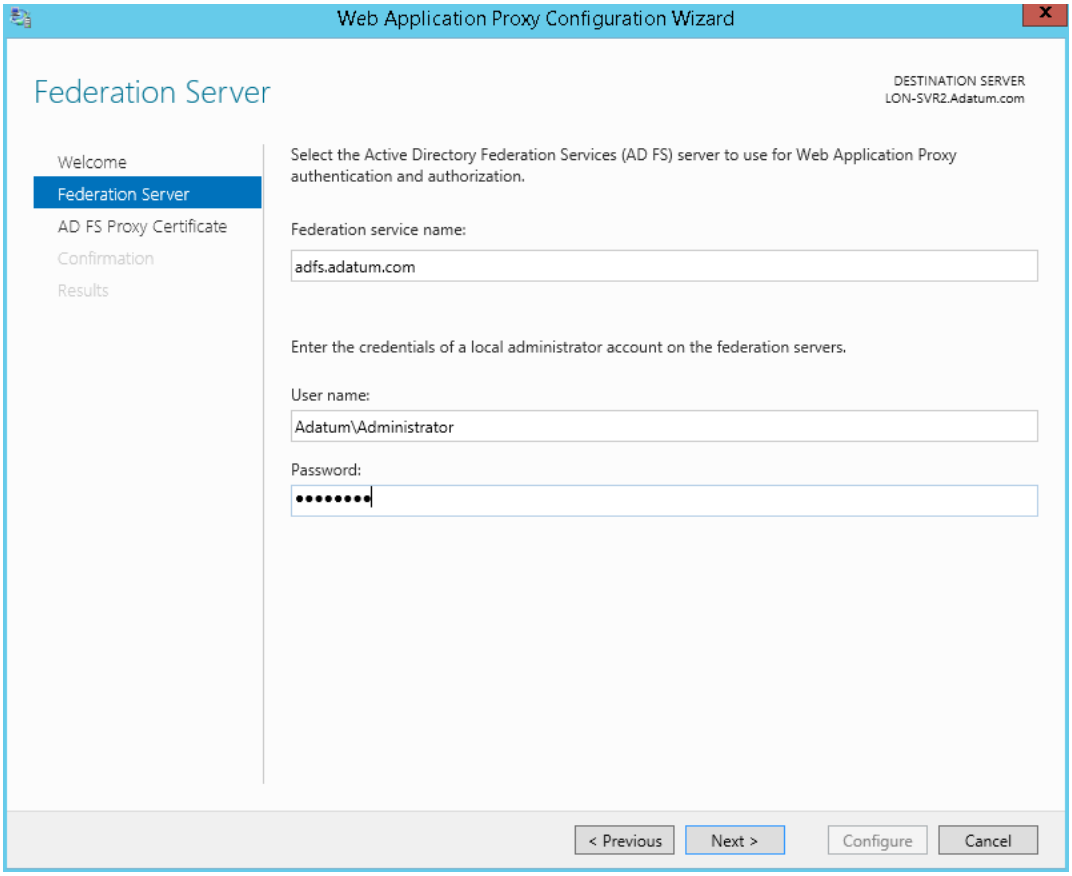


22. Cửa sổ **Welcome**, chọn **Next**.

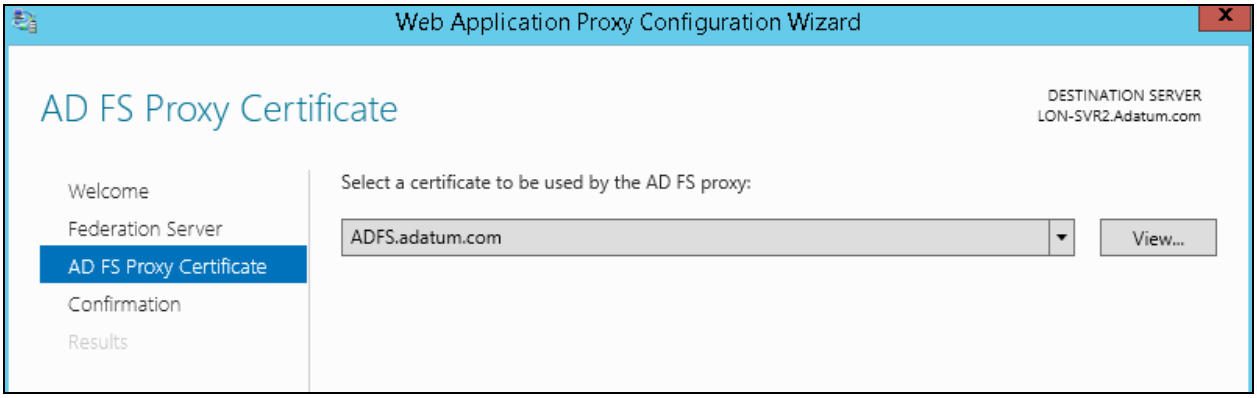



23. Cửa sổ **Federation Server**, nhập thông tin như bên dưới và chọn **Next**.

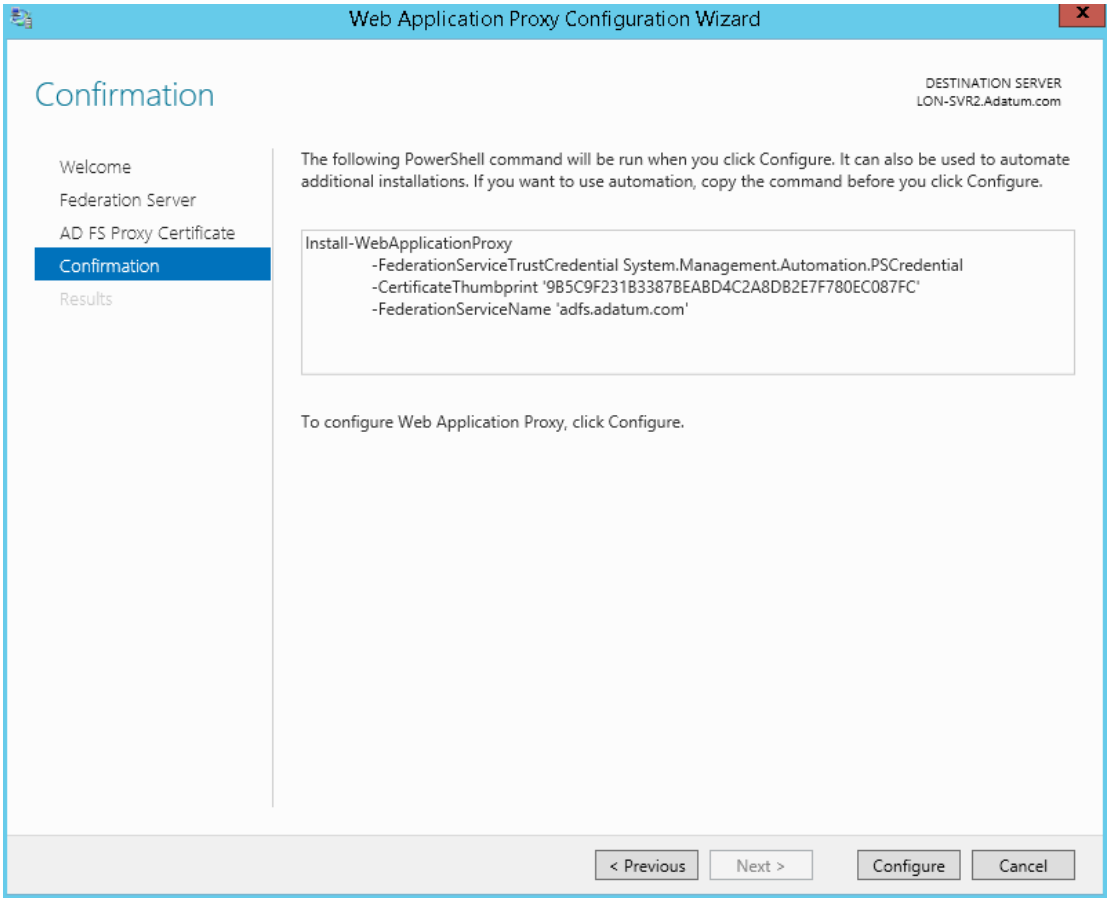
- Federation service name: **adfs.adatum.com**
- User name: **Adatum\Administrator**
- Password: **Pa$$w0rd**



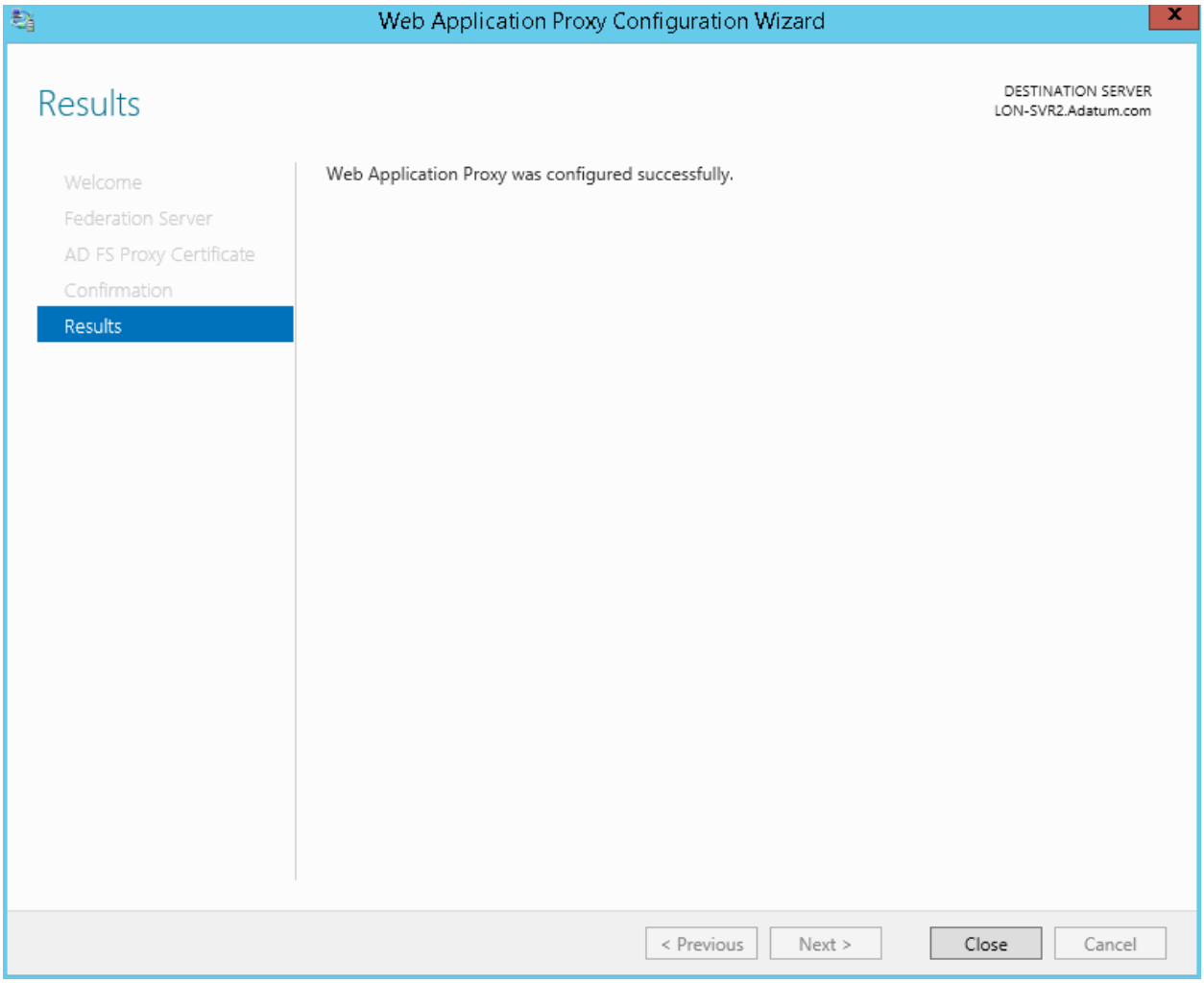
24. Cửa sổ **AD FS Proxy Certificate**, bung ô **Select a certificate to be used by the AD FS proxy**, chọn **ADFS.adatum.com**, và chọn **Next**.




25. Cửa sổ **Confirmation**, chọn **Configure**.

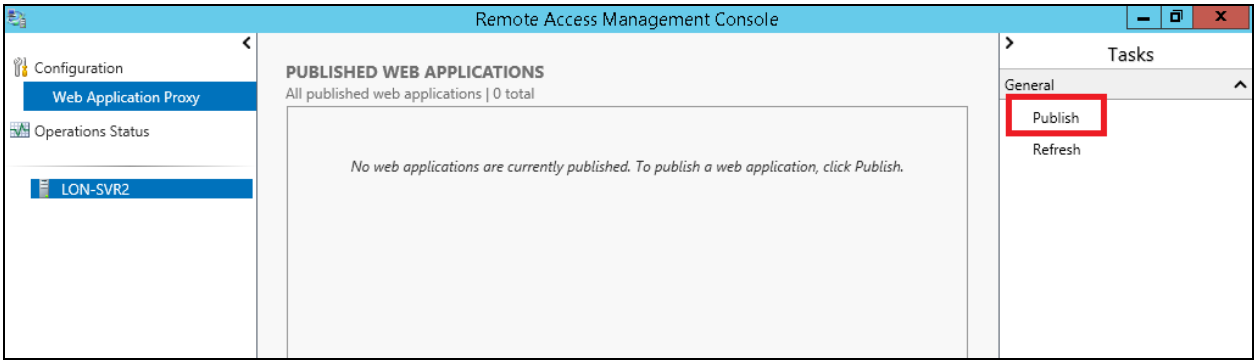


26. Cửa sổ **Results**, chọn **Close**.



## Bước 5: Công bố Work Folders thông qua Web Application Proxy

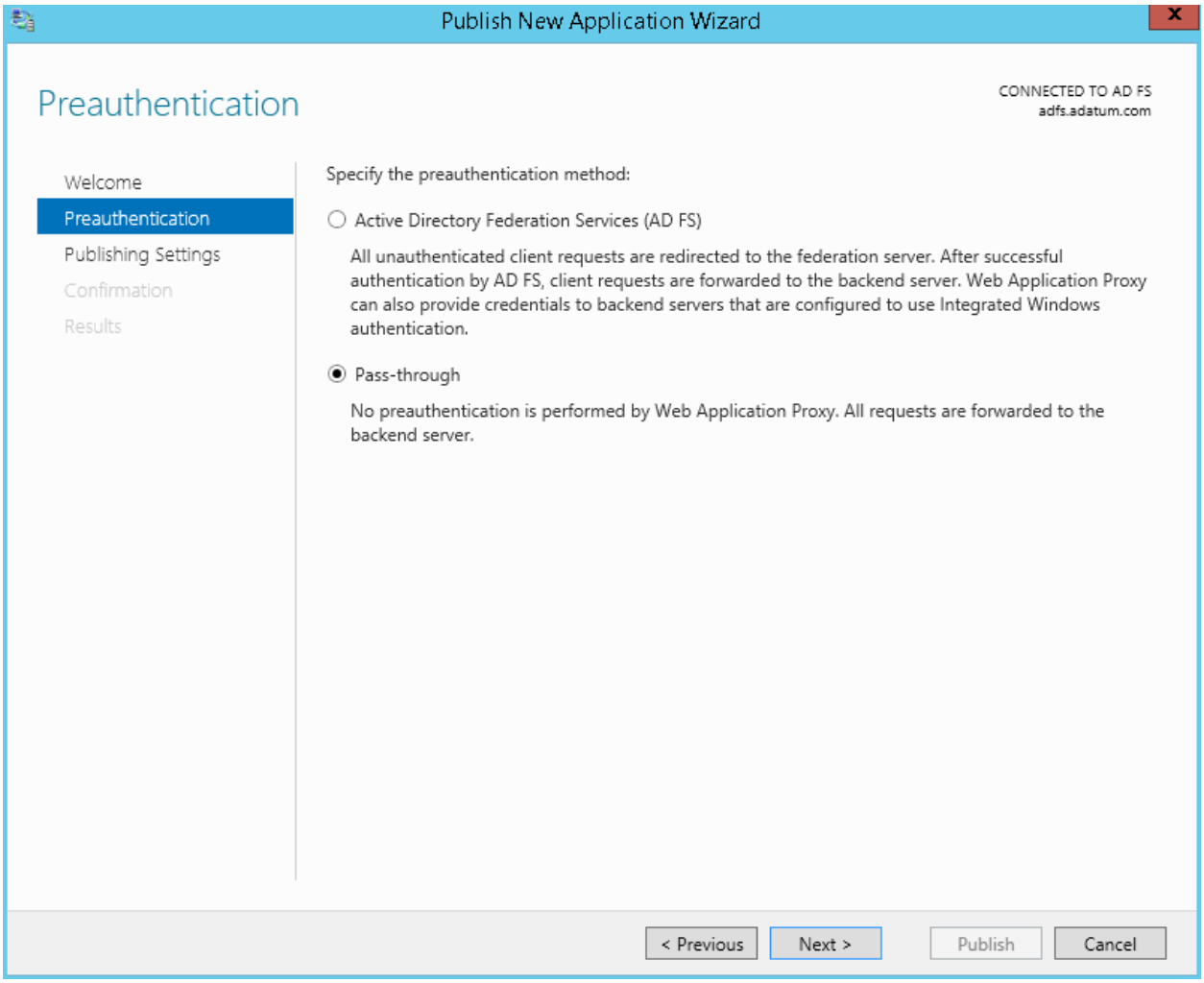
1. Trên máy **LON-SVR2**, trong cửa sổ **Remote Access Management Console**, chọn **Publish**.




2. Cửa sổ **Welcome**, chọn **Next**.

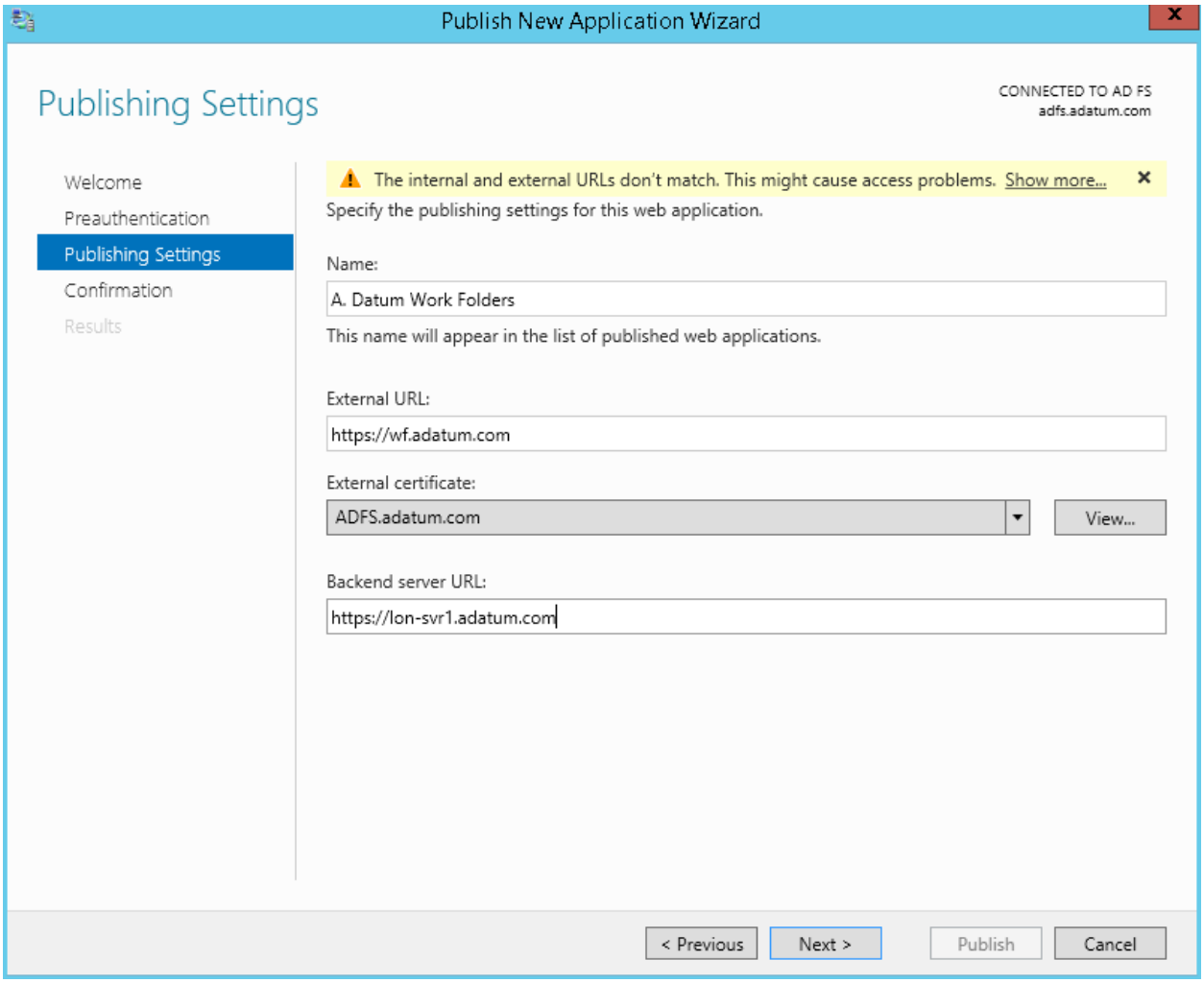


3. Cửa sổ **Preauthentication**, chọn **Pass-through**, và chọn **Next**.

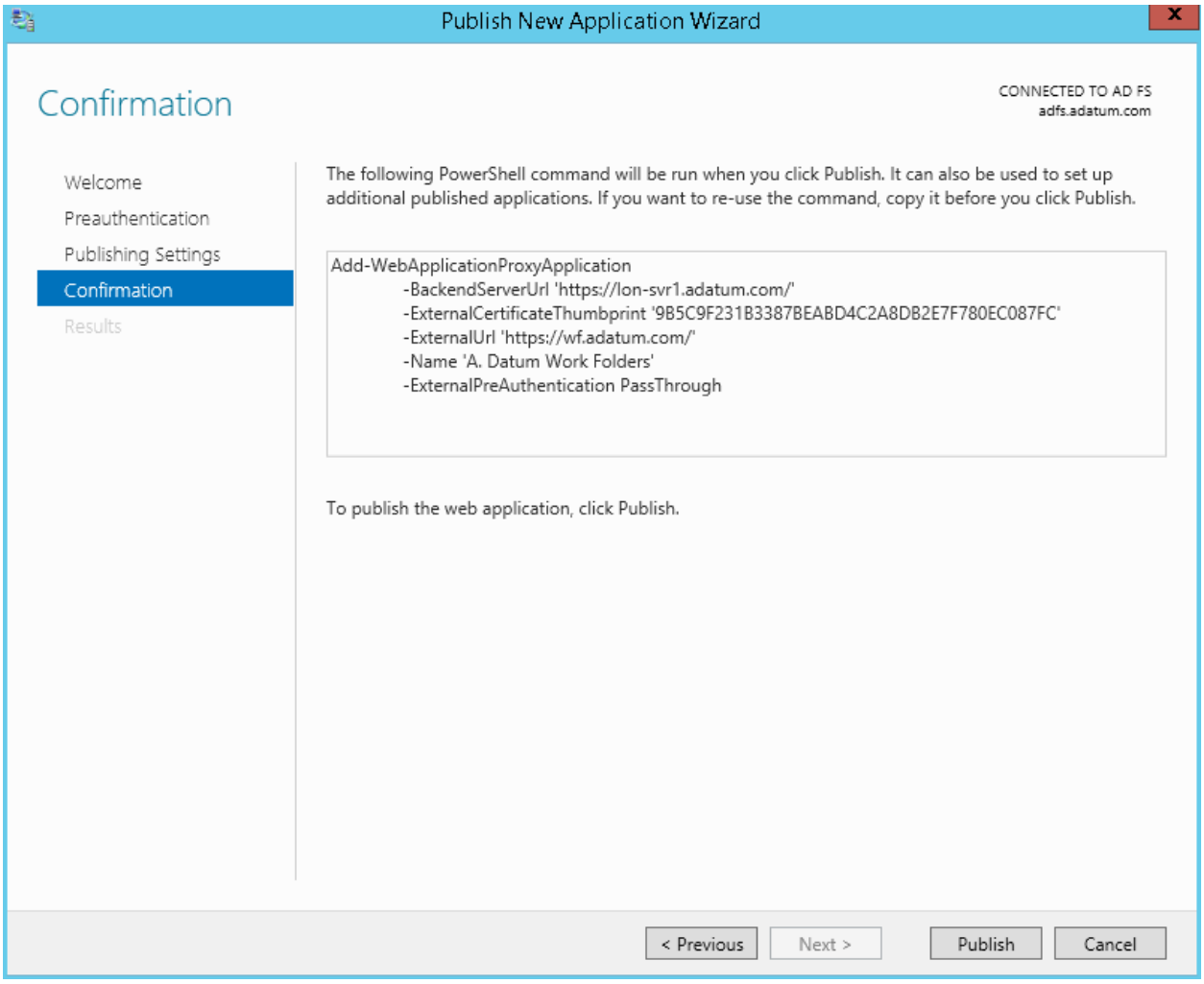


4. Cửa sổ **Publishing Settings**, khai báo thông tin như bên dưới và chọn **Next**.

- Name: **A. Datum Work Folders**
- External URL: **https://wf.adatum.com/**
- External certificate: **ADFS.adatum.com**
- Backend server URL: **https://lon-svr1.adatum.com/**



5. Cửa sổ **Confirmation**, chọn **Publish**. Sau khi publish thành công, chọn **Close.**




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã cấu hình AD FS và Publish Work Folders thông qua Web Application Proxy để hỗ trợ người dùng bên ngoài truy cập.**

## Bài tập 3: Kiểm tra chức năng Work Folders.

Để kiểm tra quyền truy cập vào Work Folders. Bạn sẽ sử dụng một máy client đã tham gia domain là LON-CL1, và một máy client chưa tham gia domain là LON-CL2. Máy LON-CL1 sẽ truy cập vào Work Folders mạng nội bộ bằng cách sử dụng tên nội bộ là lon-svr1.adatum.com. Máy LON-CL2 sẽ kết nối từ bên ngoài, thông qua Web Application Proxy bằng tên internet là wf.adatum.com.

❖ **Bài thực hành bao gồm các bước:**

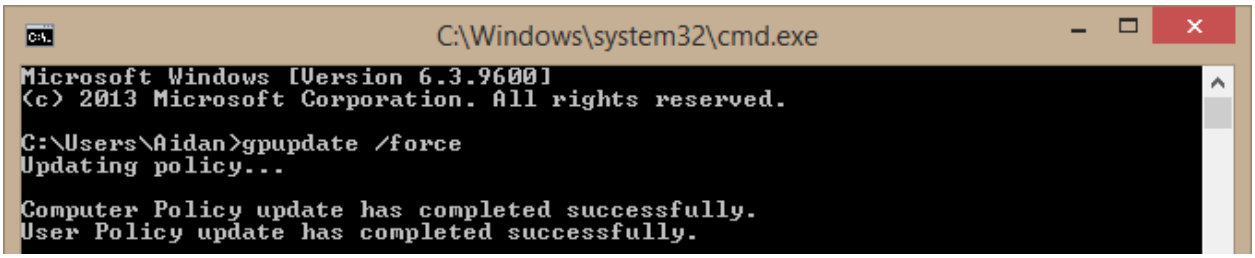
1. Truy cập Work Folders từ máy client đã tham gia domain.
2. Truy cập Work Folders từ máy client không tham gia domain.
3. Kiểm tra đồng bộ dữ liệu của Work Folders.

❖ **Thực hiện:**

### Bước 1: Truy cập Work Folders từ máy client đã tham gia domain.

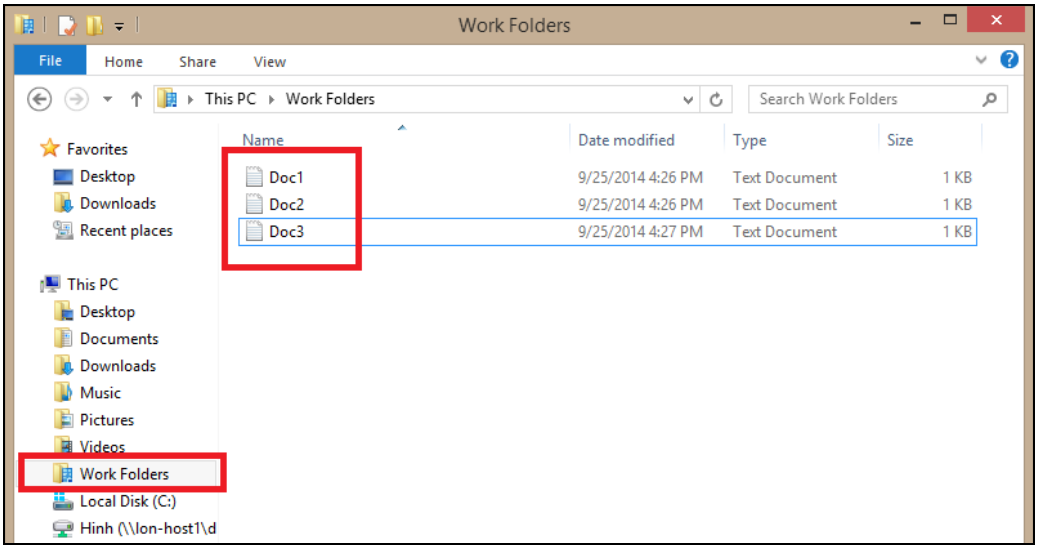
1. Sign in vào máy **LON-CL1** bằng **Adatum\Aidan** với password **Pa$$w0rd**.

2. Mở **Windows PowerShell,** gõ lệnh**: gpupdate /force**



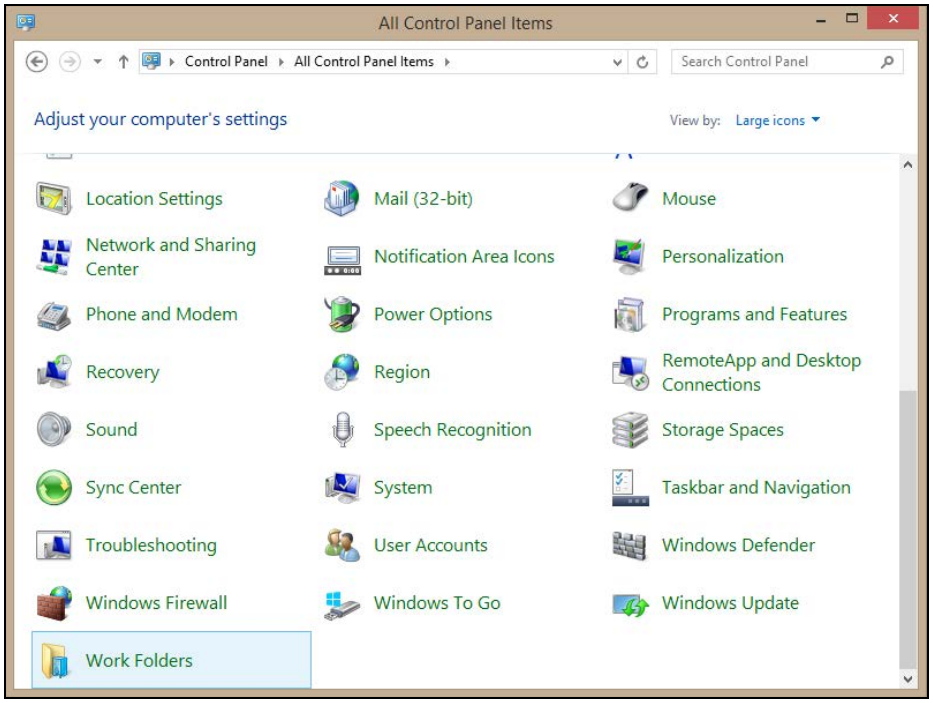

**Chú ý: Nếu gặp lỗi khi cập nhật Group Policy thì khởi động lại máy LON-CL1.**

3. Mở **File Explorer,** kiểm tra **Work Folders** đã được tạo. Vào **Work Folders** tạo 3 file text: **Doc1.txt, Doc2.txt và Doc3.txt**

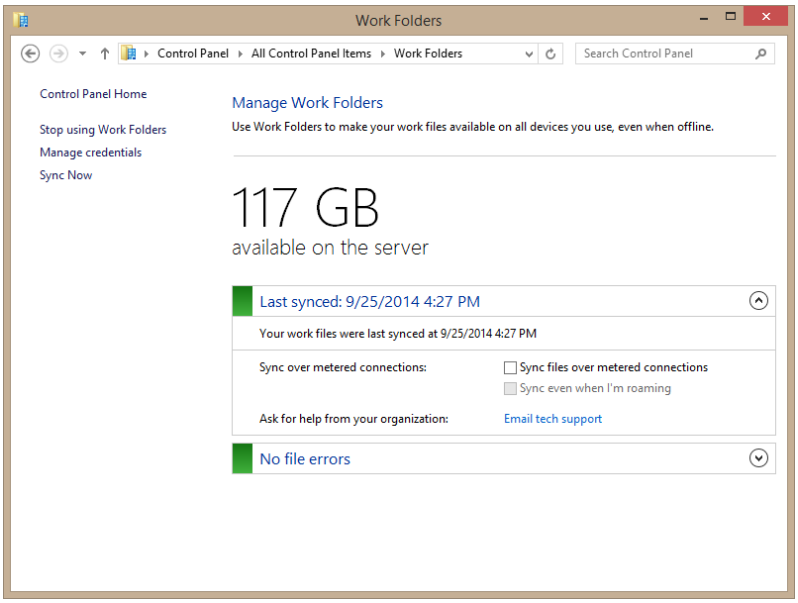



**Chú ý: Trên máy LON-CL1, Work Folders được tạo tự động thông qua Group Policy.**

4. Mở **Control Panel**, bung ô **View by**, chọn **Large icons,** chọn **Work Folders**.



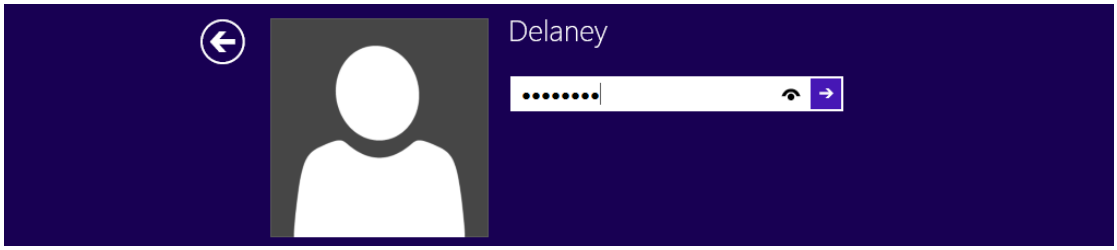
5. Kiểm tra Work Folders đã được cấu hình và đang hoạt động.



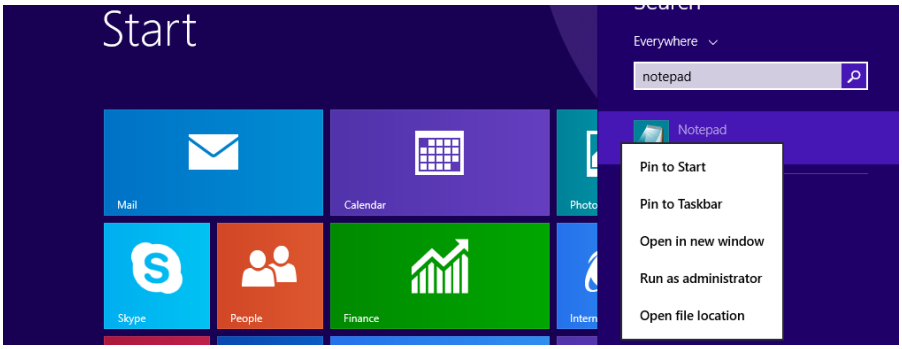

## Bước 2: Truy cập Work Folders từ máy client không tham gia domain.

1. Sign in vào máy **LON-CL2** bằng **Delaney** với password **Pa$$w0rd**.

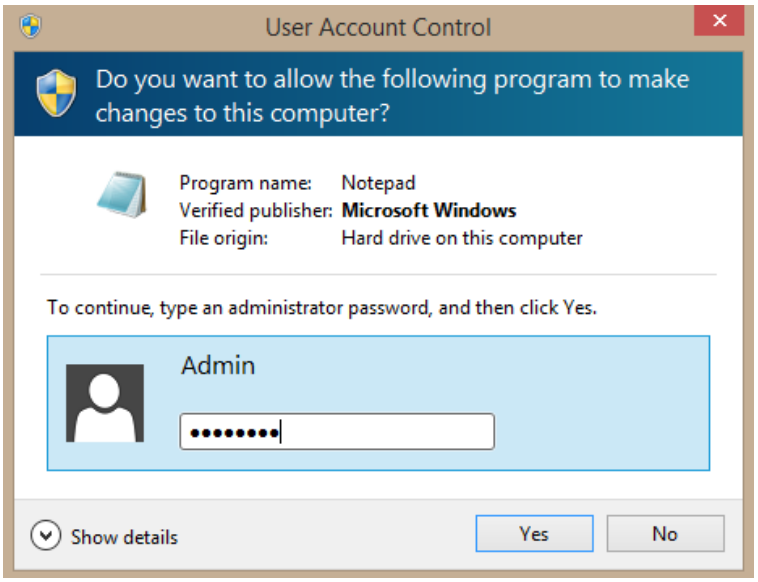
(Lưu ý: máy **LON-CL2** không tham gia domain **Adatum.com**)




2. Bung **Start** menu, gõ **Notepad**, chuột phải **Notepad**, chọn **Run as administrator**.

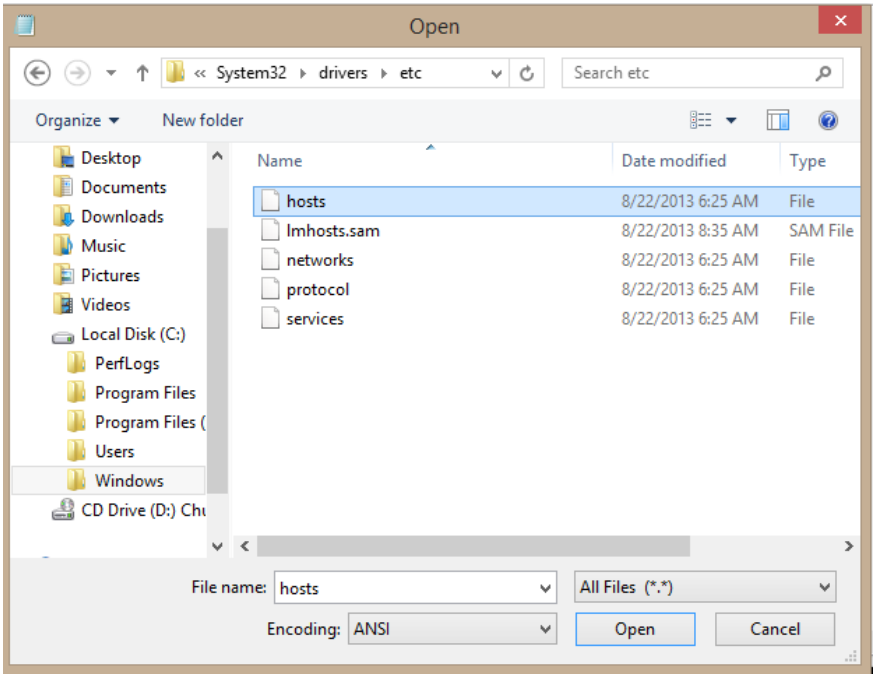


3. Hộp thoại **User Account Control**, nhập **Pa$$w0rd** vào ô **Password**, và chọn **Yes**.

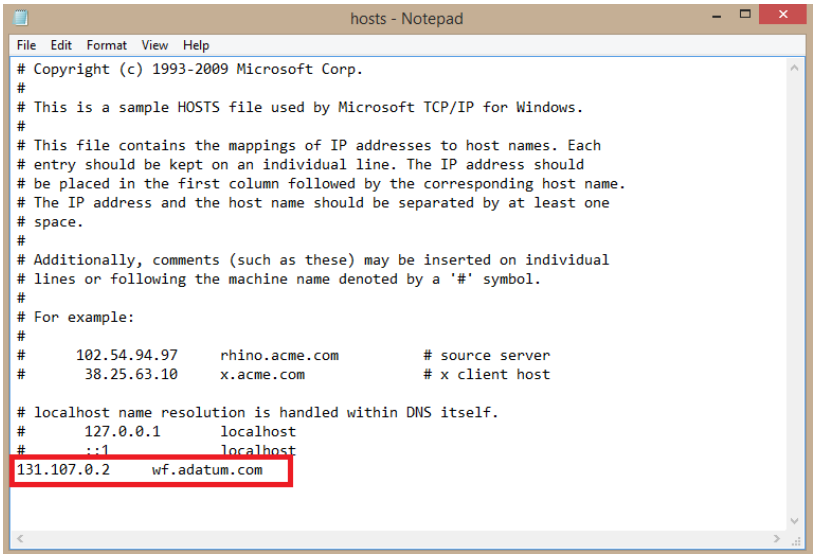



4. Trong cửa sổ **Notepad**, bung menu **File**, chọn **Open**.

5. Trỏ vào đường dẫn **C:\Windows\System32\Drivers\etc**, bung ô **File name**, chọn **All files**, chọn file **hosts,** và chọn **Open**.

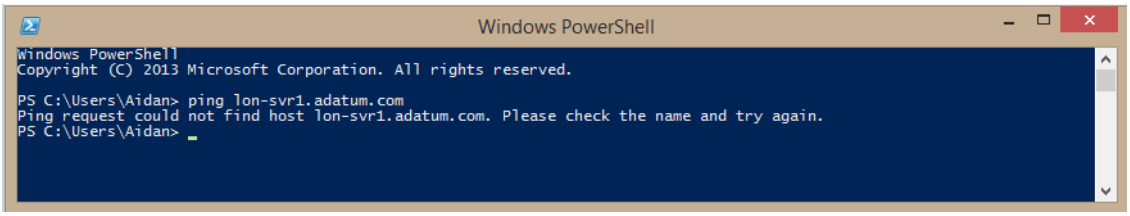


6. Trong file **hosts**, ở cuối trang, nhập thêm dòng **131.107.0.2 wf.adatum.com.** Bung menu **File**, chọn **Save**, tắt **Notepad**.



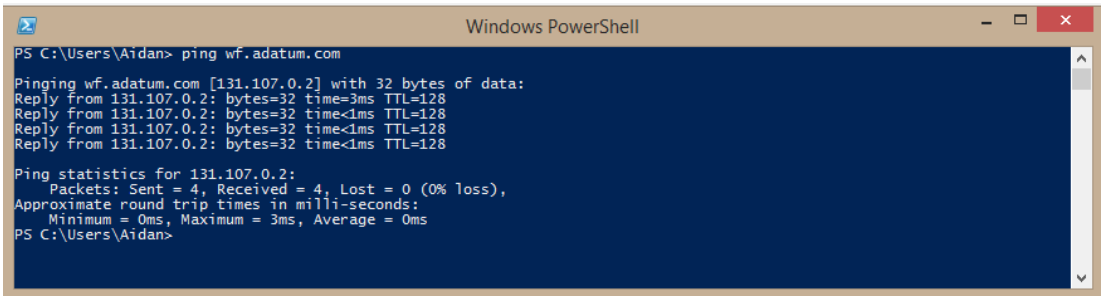

7. Mở **Windows PowerShell**, gõ lệnh **ping lon-svr1.adatum.com**

**Chú ý:** Không phân giải được tên **lon-svr1.adatum.com**, vì **LON-CL2** là máy client nằm bên ngoài hệ thống nên không thể truy cập bằng tên nội bô.

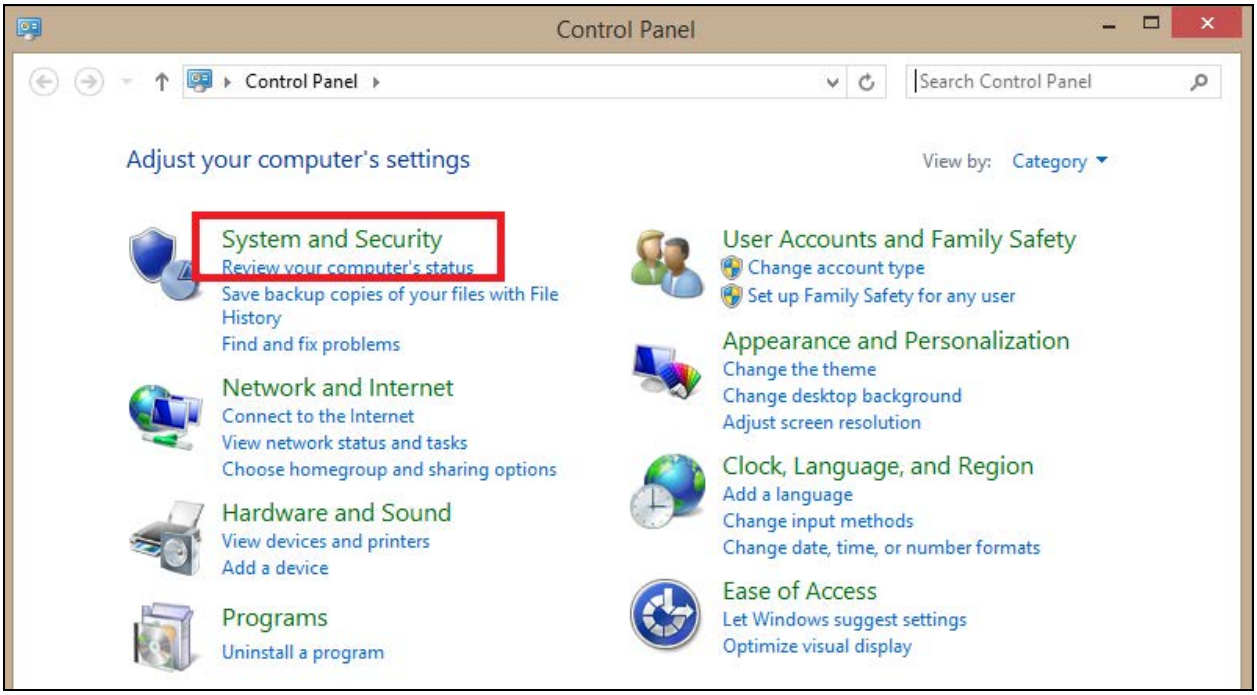



8. Trong **Windows PowerShell,** gõ lệnh **ping wf.adatum.com**

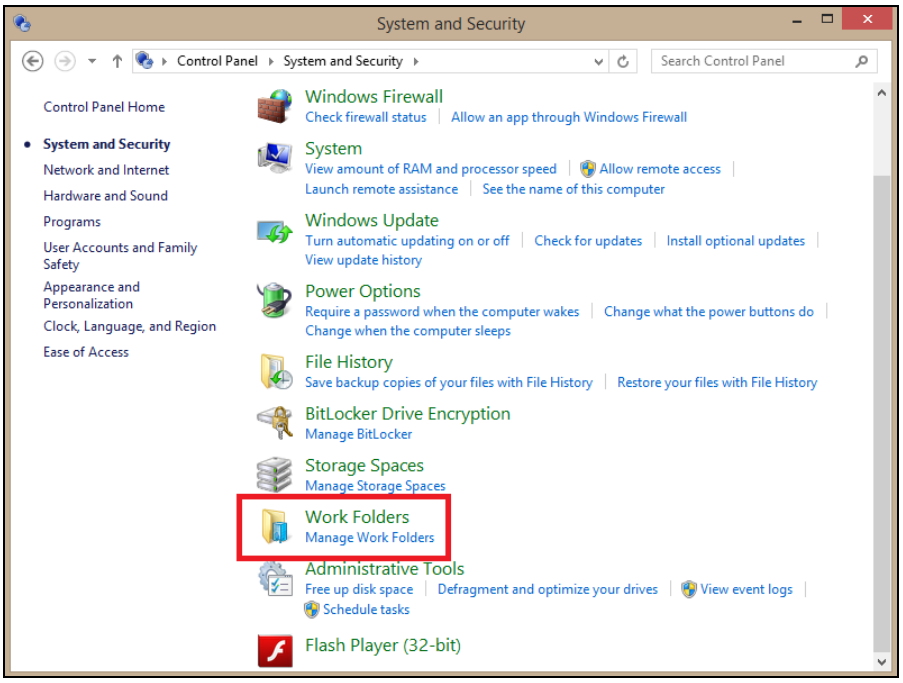
**Kiểm tra:** liên lạc thành công, và **wf.adatum.com** có địa chỉ **131.107.0.2**.



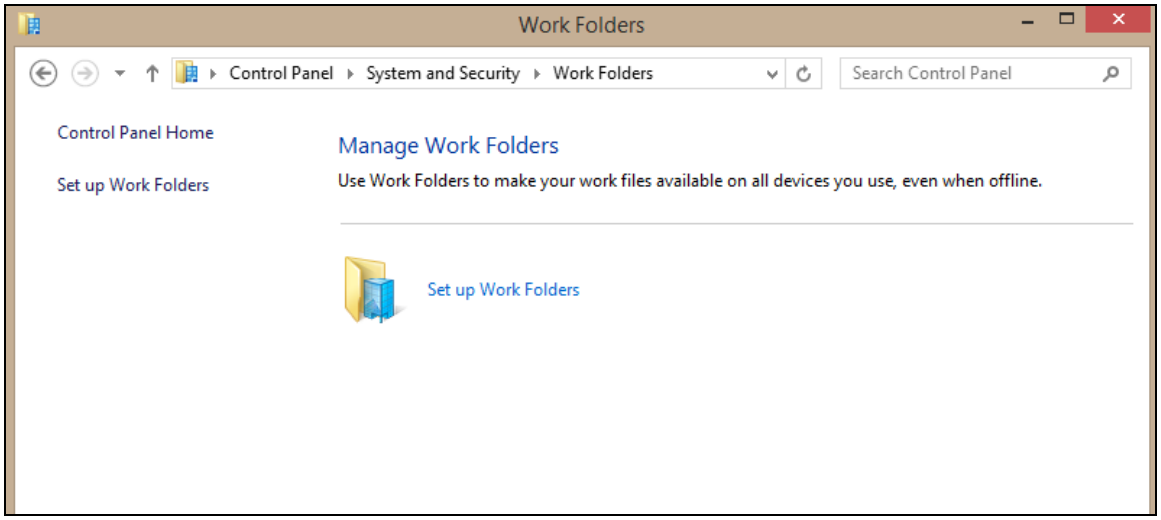
9. Mở **Control Panel**, chọn **System and Security**.



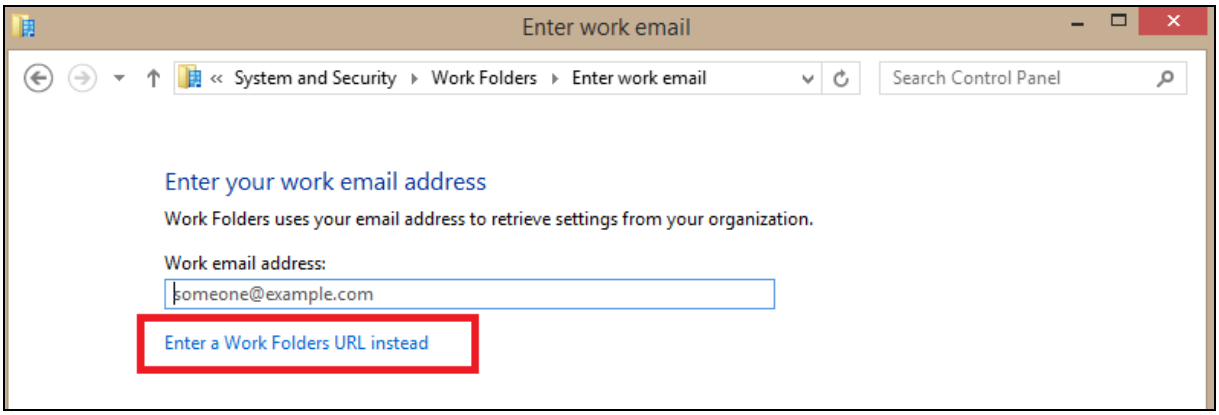

10. Trong **System and Security,** chọn **Work Folders**.



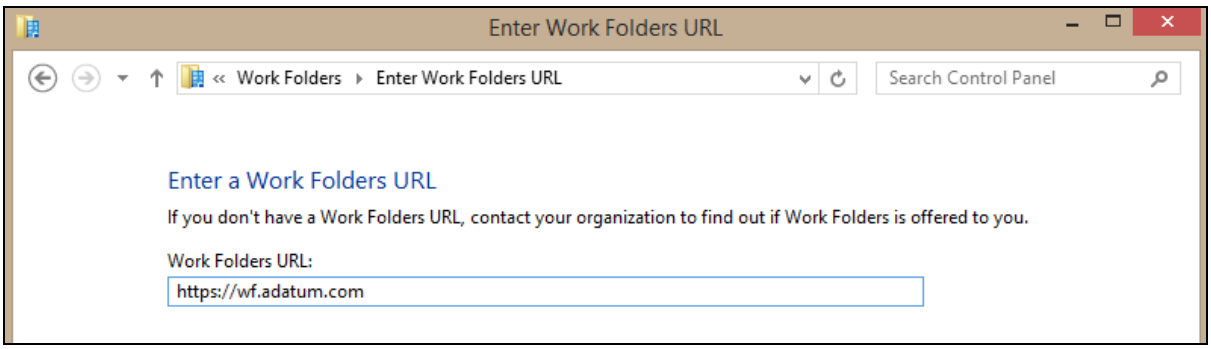
11. Cửa sổ **Work Folders,** chọn **Set up Work Folders**.



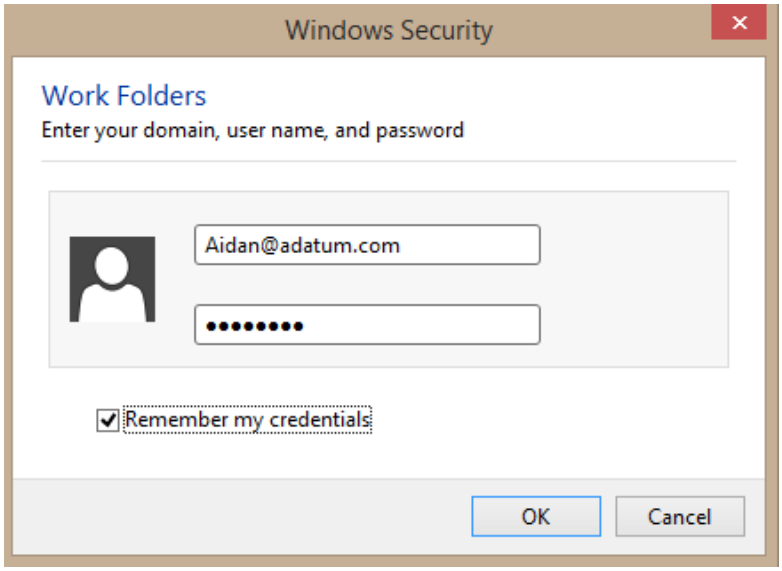

12. Cửa sổ **Enter your work email address**, chọn **Enter a Work Folders URL instead**



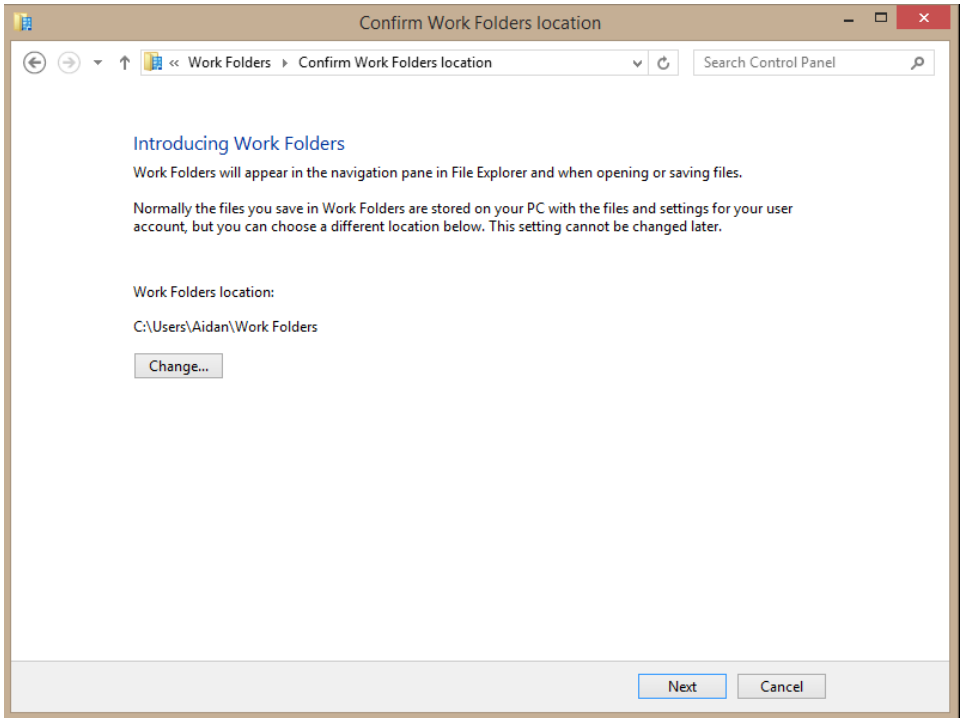

13. Trong ô **Work Folders URL**, nhập **https://wf.adatum.com**, chọn **Next**.



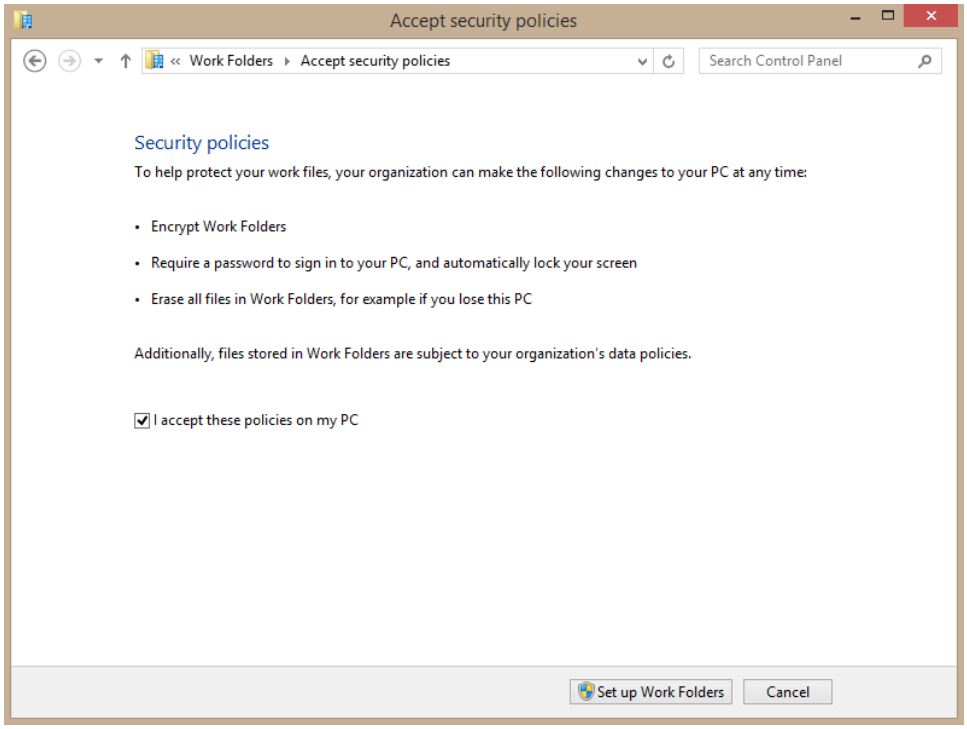
14. Hộp thoại **Windows Security**, trong ô **User name,** nhập **Aidan@adatum.com,** trong ô **Password**, nhập **Pa$$w0rd ,** đánh dấu chọn **Remember my credentials**, chọn **OK**.



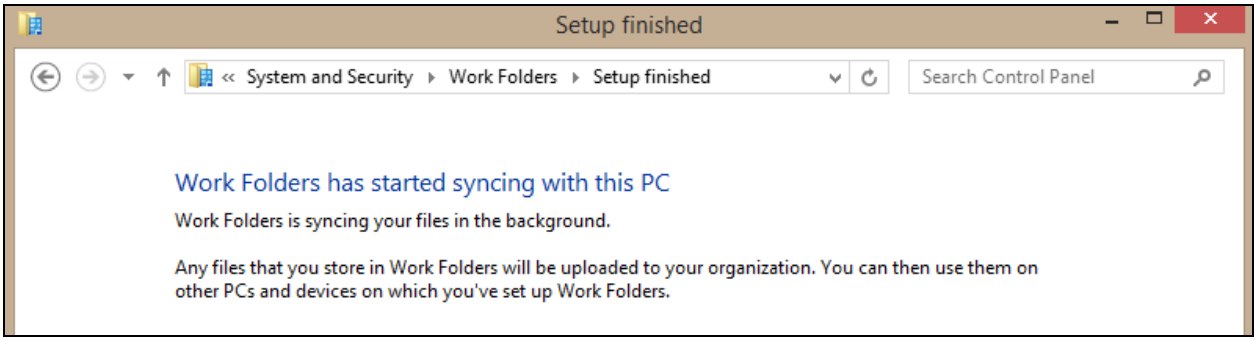

15. Cửa sổ **Introducing Work Folders**, chọn **Next**.



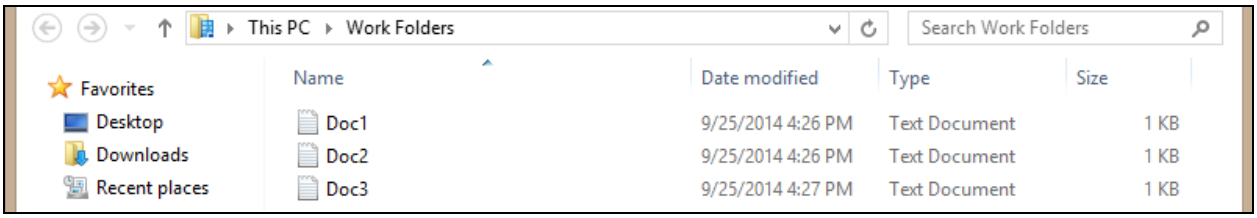
16. Cửa sổ **Security policies**, đánh dấu chọn **I accept these policies on my PC**, và chọn **Set up Work Folders**.




17. Cửa sổ **Work Folders has started syncing with this PC**, chọn **Close**.

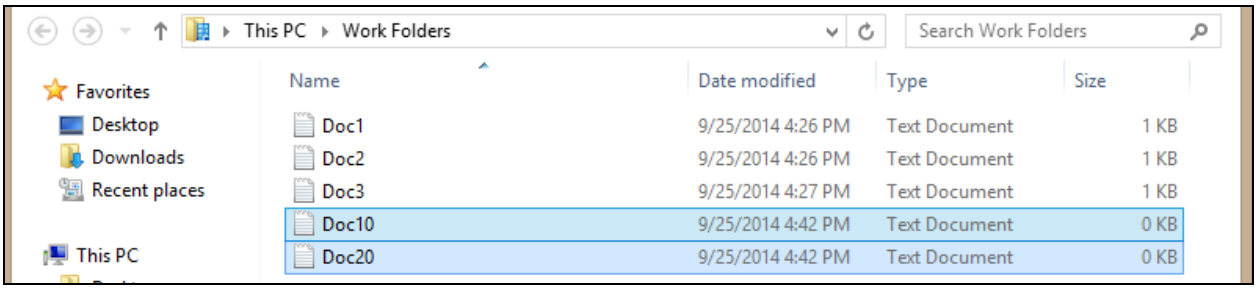


18. Trong **Work Folders**, Kiểm tra có file **Doc1.txt, Doc2.txt và Doc3.txt**.

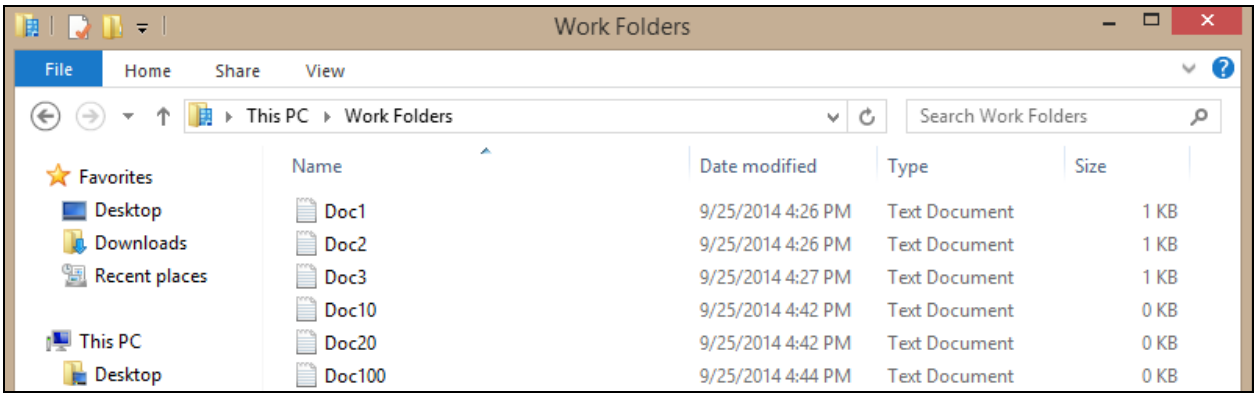



## Bước 3: Kiểm tra đồng bộ dữ liệu của Work Folders.

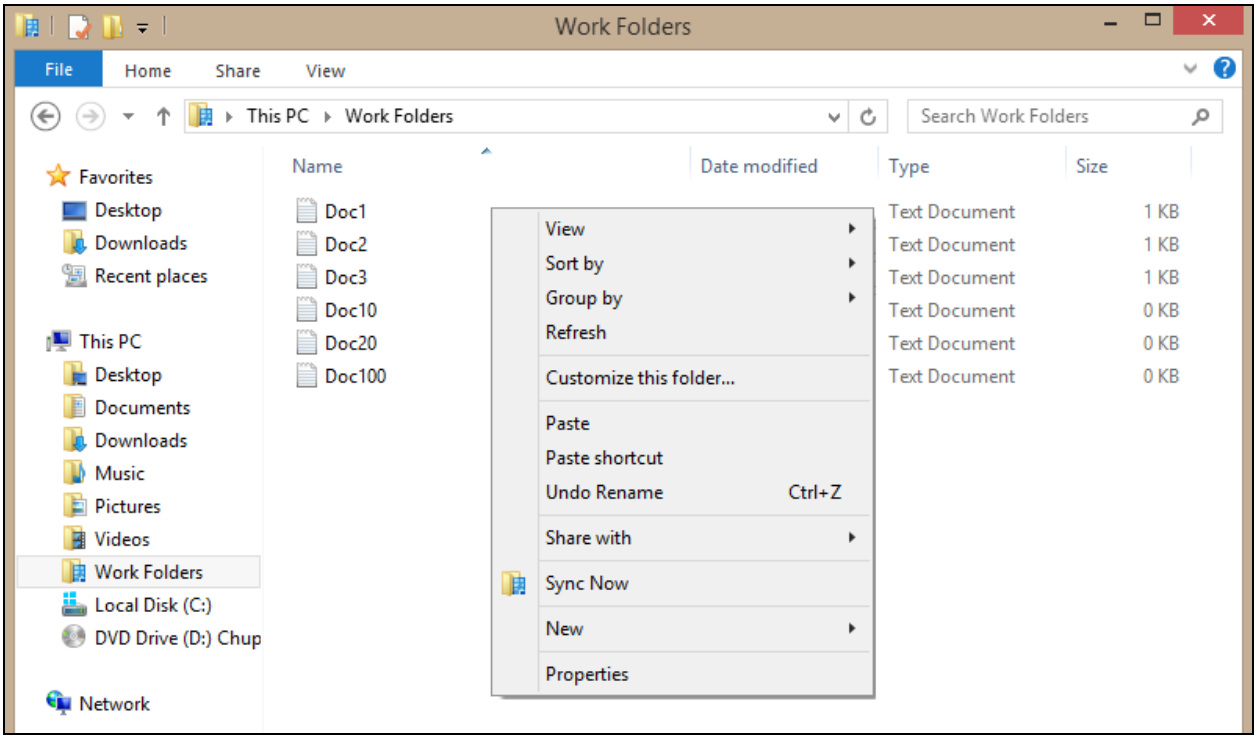
1. Trên máy **LON-CL2**, trong **Work Folders**, tạo thêm 2 file **Doc10.txt** và **Doc20.txt.**




2. Đợi khoảng 5 phút. Qua máy **LON-CL1**, mở **File Explorer,** chọn **Work Folders**. Kiểm tra có 2 file mới **Doc10.txt** và **Doc20.txt.** Sau đó tạo thêm file **Doc100.txt**



3. Đợi khoảng 5 phút. Qua máy **LON-CL2**. mở **File Explorer,** chọn **Work Folders**. Kiểm tra có file mới **Doc100.txt**. (**Chú ý:** Nếu chưa đồng bộ, chuột phải lên khoảng trắng chọn **Syns Now**)




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã kiểm tra truy cập thành công Work Folders từ một máy client trong nội bô (LON-CL1) và từ một máy client bên ngoài hệ thống (LON-CL2)**

**VI. 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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiện bước 2 và 3 cho các máy ảo còn lại.

# Bài 13: Triển khai Active Directory Rights Management Services (AD RMS)

**I. Mục tiêu:**

- Triển khai AD RMS cho người dùng nội bộ.
- Tích hợp AD RMS với Dynamic Access Control.
- Tích hợp AD RMS với hệ thống của đối tác.

**II. Kịch bản:**

Do tính chất công việc bí mật của nhóm nghiên cứu tại công ty A. Datum, bô phận an ninh mạng muốn triển khai thêm các chức năng bảo mật cho các tài liệu của nhóm nghiên cứu. Đặc biệt, bô phận an ninh mạng muốn đảm bảo người dùng trong và ngoài tổ chức không thể chia sẻ tài liệu bí mật trái phép.

Bạn cần lên kế hoạch triển khai giải pháp AD RMS để cung cấp chức năng bảo vệ tài liệu mà bộ phận an ninh mạng yêu cầu.

**III. Yêu cầu tổng quan:**

- Triển khai AD RMS cho công ty A. Datum và Trey Research.
- Người dùng phải sử quyền RMS trên các tài liệu bí mật của mình để chỉ định cho các người dùng khác có quyền đọc nội dung, sao chép nội dung, in hoặc là save as.
- AD RMS sẽ tự động bảo vệ tất cả các tài liệu bí mật của nhóm nghiên cứu.
- Chỉ có thành viên của nhóm Research và Managers mới được phép truy cập tài liệu bí mật.
- Tích hợp AD RMS với Dynamic Access Control.
- Cho phép người dùng của A. Datum và Trey Research có thể truy cập tài liệu RMS lẫn nhau.

**IV. Mô hình thực hành:**

| | |
|---|---|
| Máy ảo (VM) | **20414C-LON-DC1**<br>**20414C-LON-CL1**<br>**20414C-TREY-DC1**<br>**20414C-TREY-CL1** |
| User name | **Adatum\Administrator** |
| Password | **Pa$$w0rd** |

**V. Chuẩn bị:**

1. Trên máy **LON-HOST1**. Mở **Hyper-V® Manager**, chuột phải **20414C-LON-DC1**, chọn **Start**.
2. Nhấn chuột phải máy ảo **20413C-LON-DC1**, chọn **Connect**.
3. Logon vào máy **20414C-LON-DC1** với thông tin sau:
   - User name: **Adatum\Administrator**
   - Password: **Pa$$w0rd**
4. Thực hiên từ bước 1 đến 3 cho các máy ảo còn lại**.**
5. Logon vào máy **20414C-TREY-DC1** với thông tin sau:
   - User name: **TreyResearch\Administrator**
   - Password: **Pa$$w0rd**
6. Không logon vào máy **20414C-LON-CL1** và **20414C-TREY-CL1** cho đến khi có yêu cầu

**VI. Thực hành:**

*Thời gian thực hành: 60 phút*

## Bài tập 1: Triển khai AD RMS cho người dùng nội bộ.

Công việc đầu tiên của việc triển khai AD RMS cho A. Datum là triển khai AD RMS cho người dùng nội bộ. Cụ thể, bạn phải tạo một tài khoảng AD RMS Service, sau đó sẽ cài đặt và cấu hình RMS Server đầu tiên, bước tiếp theo bạn sẽ cấu hình các Rights Policy Templates và Exclusion Policies cho hệ thống.

❖ **Bài thực hành bao gồm các bước:**

1. Thực hiện các bước chuẩn bị để triển khai AD RMS.
2. Cài đặt và cấu RMS Server đầu tiên cho Adatum.com.
3. Cài đặt và cấu hình AD RMS cho forest TreyResearch.net.
4. Cấu hình AD RMS Templates.
5. Cấu hình AD RMS Exclusion Policies.
6. Kiểm tra kết quả.

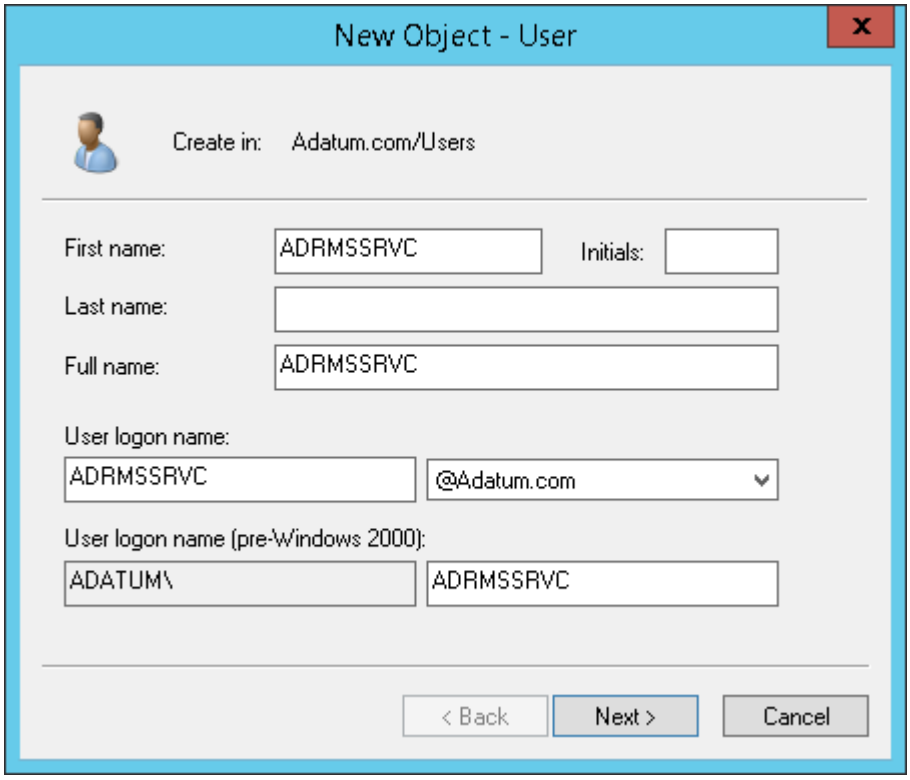
❖ **Thực hiện:**

**Bước 1: Thực hiện các bước chuẩn bị để triển khai AD RMS.**

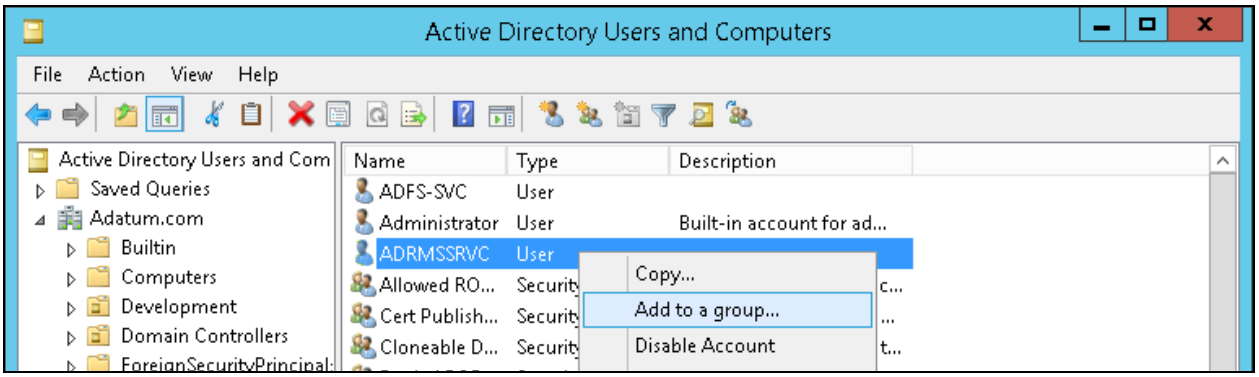
➢ **Tạo AD RMS Service account.**

1. Trên máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Active Directory Users and Computers**.

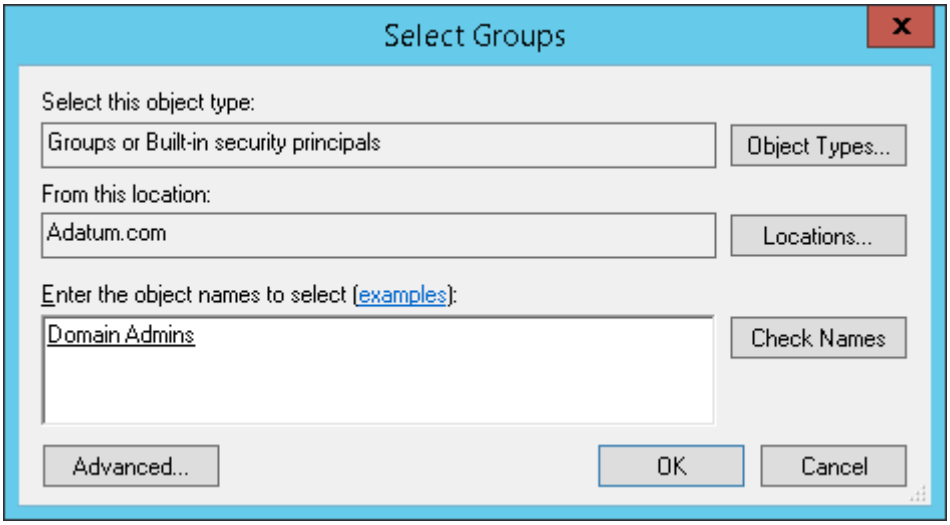
2. Trong cửa sổ **Active Directory Users and Computers,** bung **Adatum.com**, vào mục **Users**, tạo một user mới đặt tên **ADRMSSRVC** có password là **Pa$$w0rd** (Bỏ trắng dấu chọn **User must change password at next logon**)



3. Chuột phải user **ADRMSSRVC**, chọn **Add to a group**.

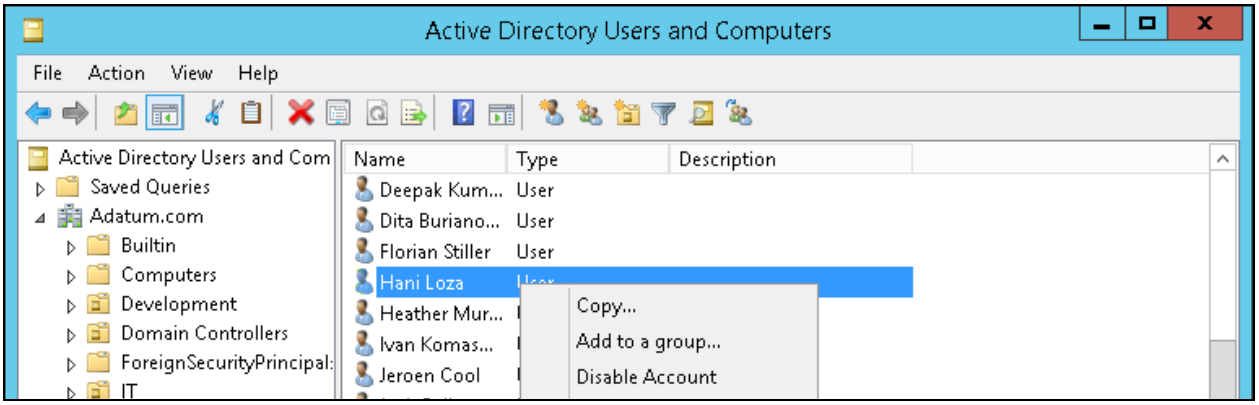



4. Hộp thoại **Select Groups**, nhập **Domain Admins**, và chọn **OK**.

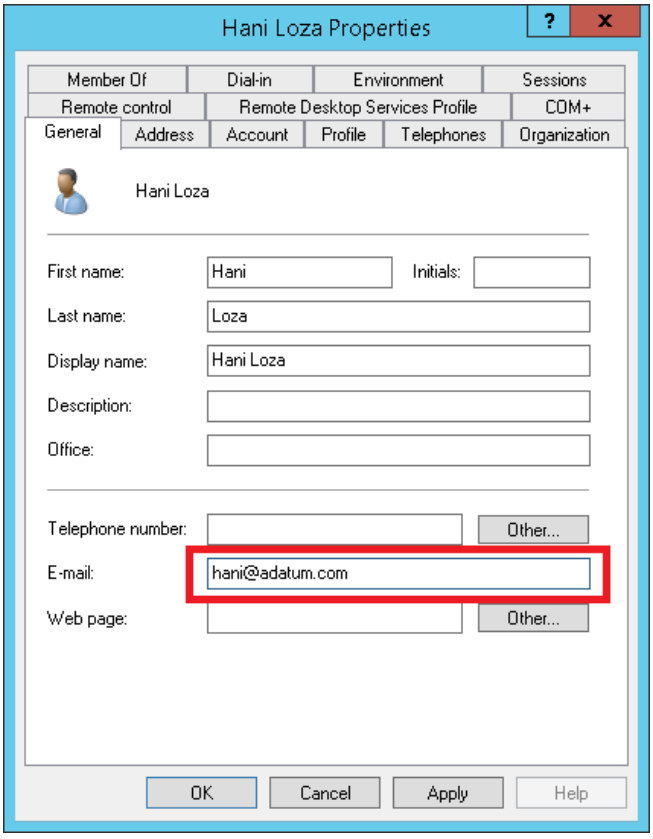


➢ **Khai báo địa chỉ email cho các Users**

1. Trong cửa sổ **Active Directory Users and Computers,** vào OU **Research,** chuột phải user **Hani Loza**, chọn **Properties.**



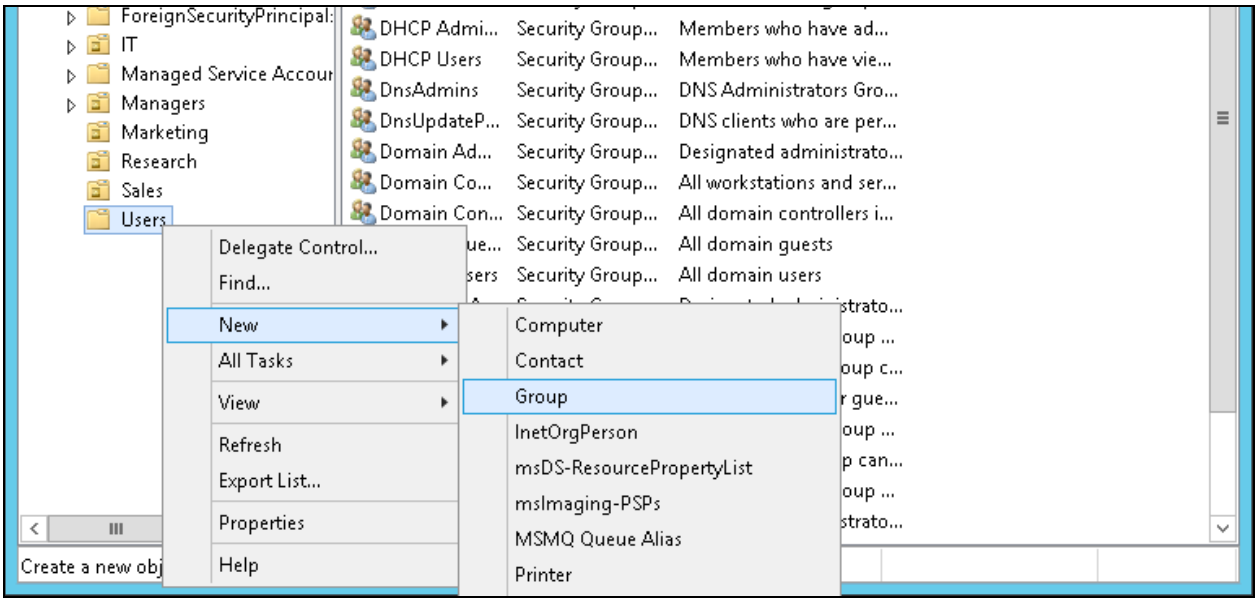

2. Hộp thoại **Properties**, trong ô **E-mail**, nhập **hani@adatum.com**, và chọn **OK**.



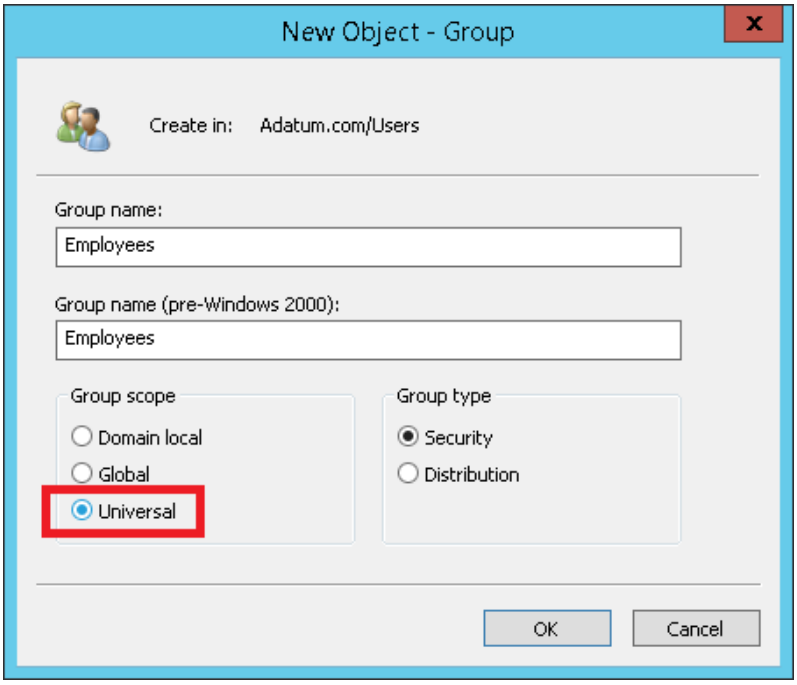
3. Tương tự, khai báo địa chỉ email cho các user theo thông tin trong bảng bên dưới:

| OU/Container | Users | Email |
|---|---|---|
| Development | Toni Poe | toni@adatum.com |
| Sales | Limor Henig | limor@adatum.com |
| Marketing | Stuart Glasson | stuart@adatum.com |

4. Trong cửa sổ **Active Directory Users and Computers**, chuột phải **Users**, chọn **New**, chọn **Group**.

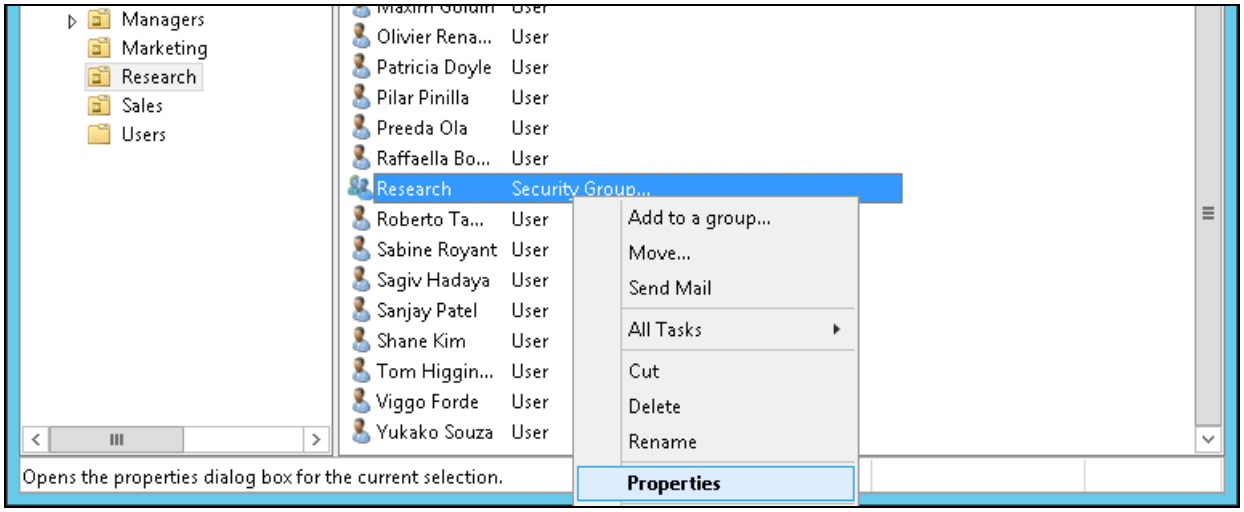


5. Hộp thoại **New Object – Group**, trong ô **Group Name**, nhập **Employees**, trong **Group Scope**, chọn **Universal**, và chọn **OK**.

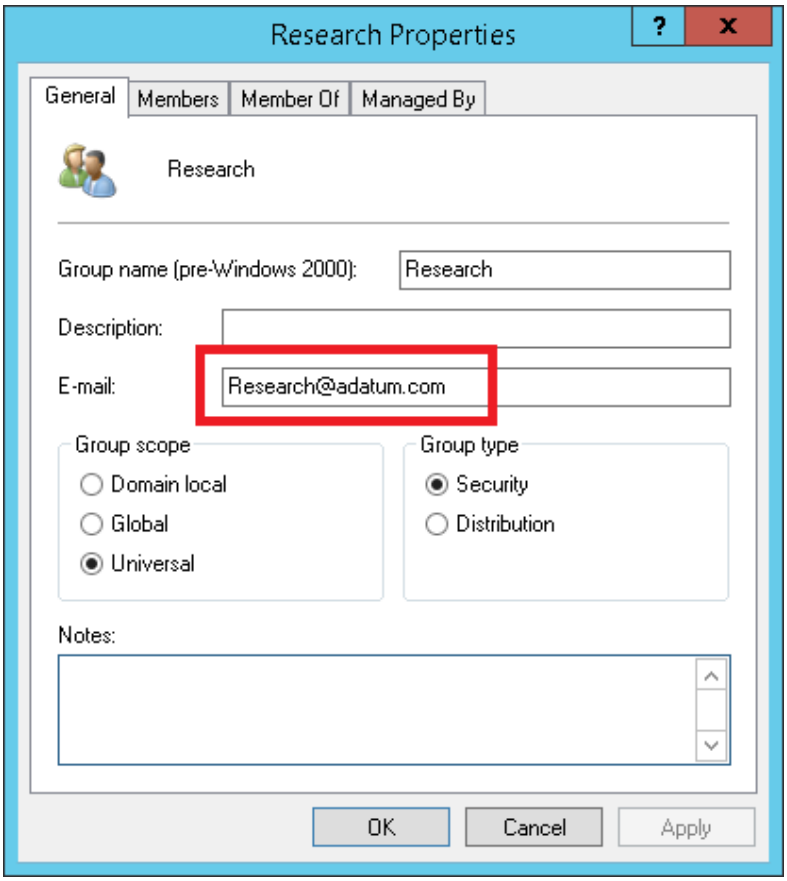



➢ **Khai báo địa chỉ email cho các Group**

1. Trong cửa sổ **Active Directory Users and Computers**, vào OU **Research**, chuột phải lên group **Research,** chọn **Properties.**



2. Hộp thoại **Properties**, trong ô **E-mail**, nhập **Research@adatum.com**, chọn **OK**.

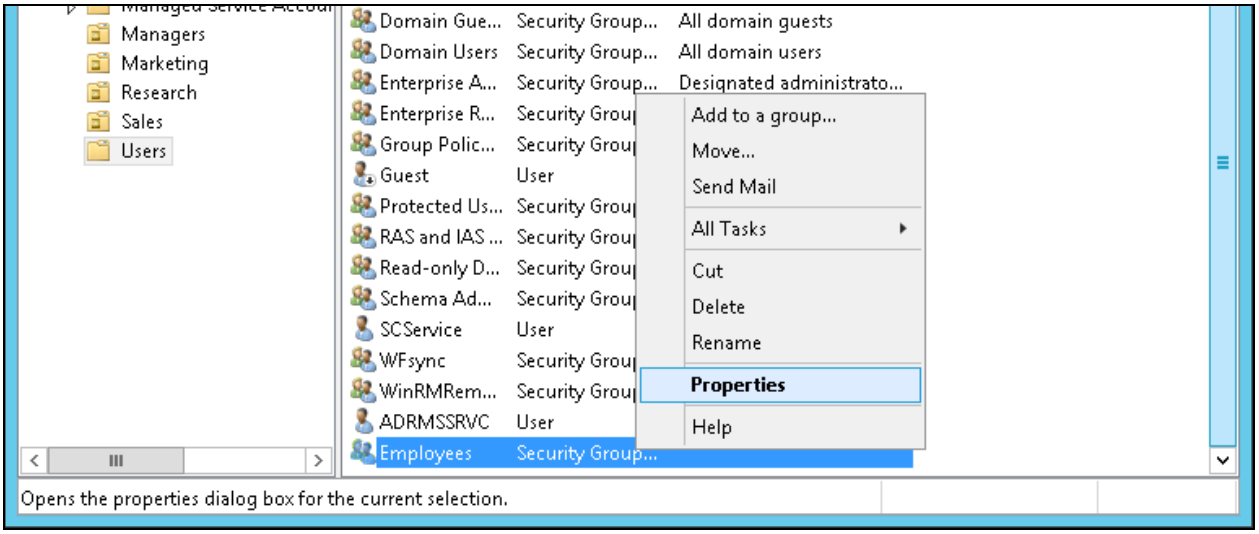



3. Tương tự, khai báo địa chỉ email cho các group theo thông tin trong bảng bên dưới:

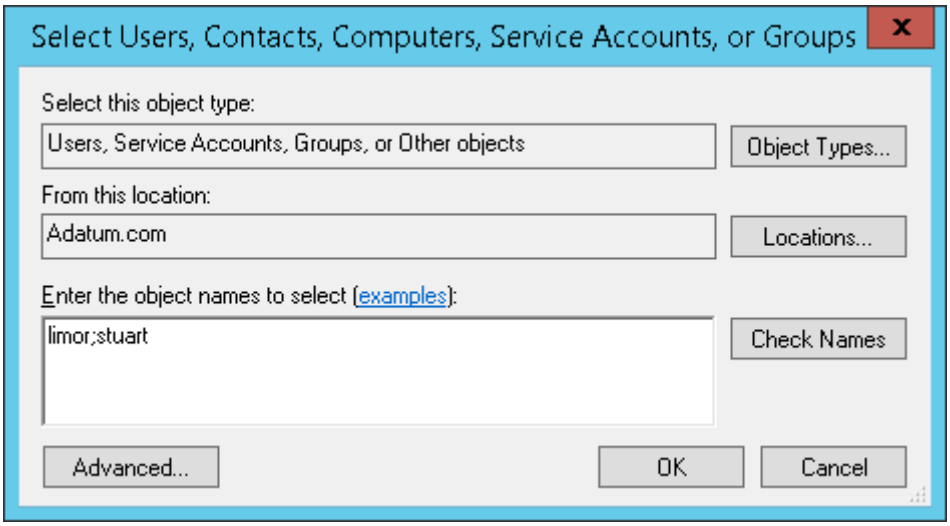
| OU/Container | Group | Email |
|---|---|---|
| Managers | Managers | Managers@adatum.com |
| Users | Employees | Employees@adatum.com |

➢ **Cho user accounts làm thành viên của group.**

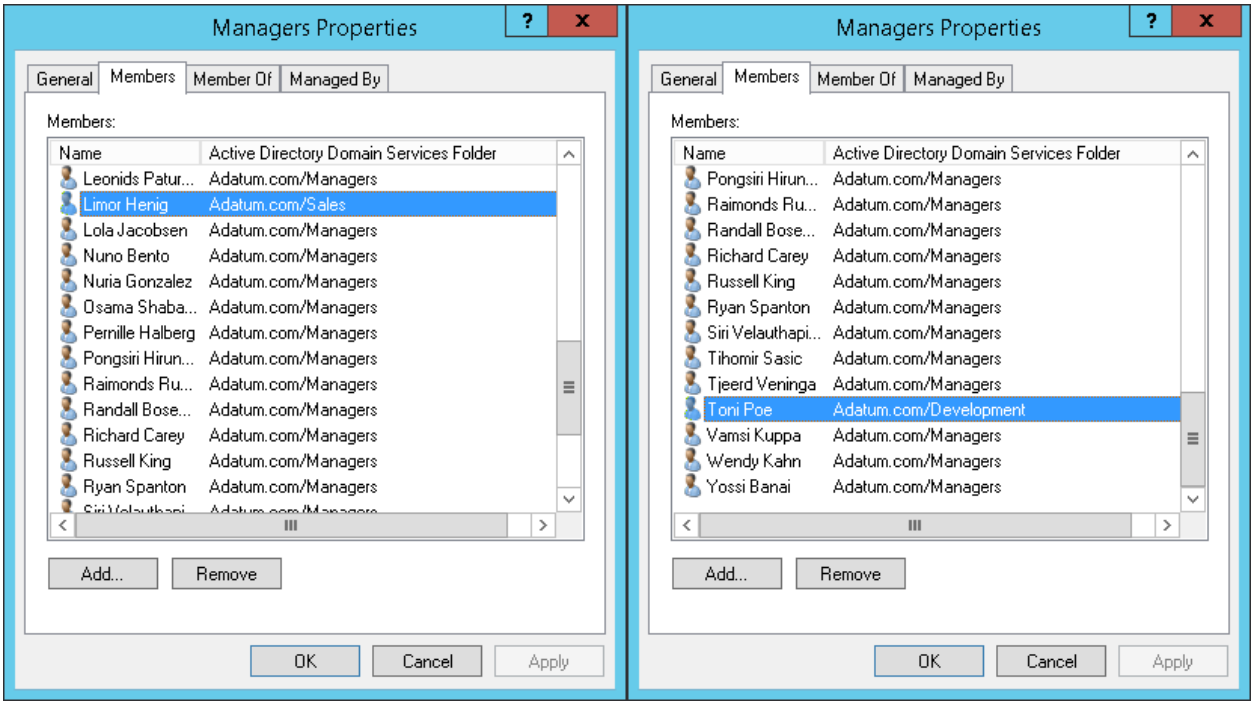
1. Trong cửa sổ **Active Directory Users and Computers**, vào mục **Users**, chuột phải lên group **Employees**, chọn **Properties.**




2. Trong hộp thoại **Properties** , qua tab **Members**, chọn **Add**. Hộp thoại **Select Users...**, nhập **limor;stuart**, chọn **Check Names**, và chọn **OK** 2 lần.

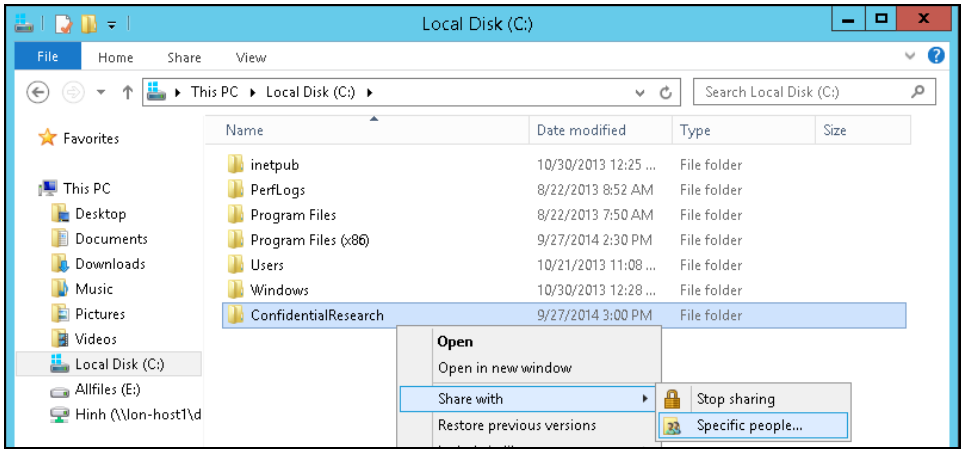


3. Lặp lại bước 1 và 2 để đưa 2 user **Limor Henig** và **Toni Poe** vào làm thành viên của group **Managers**.

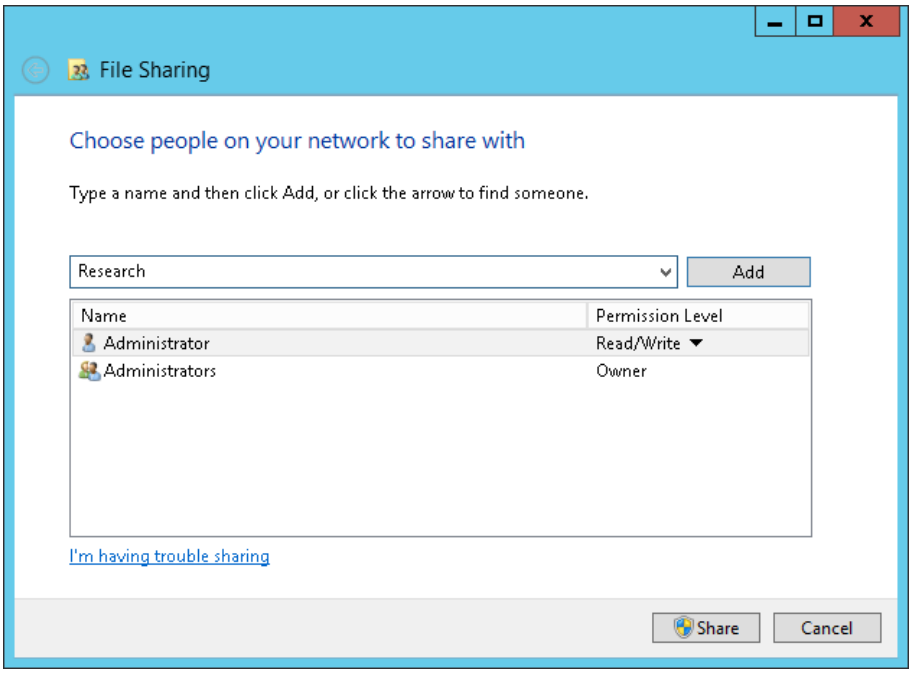



➢ **Tạo Shared Folders trên máy LON-DC1**

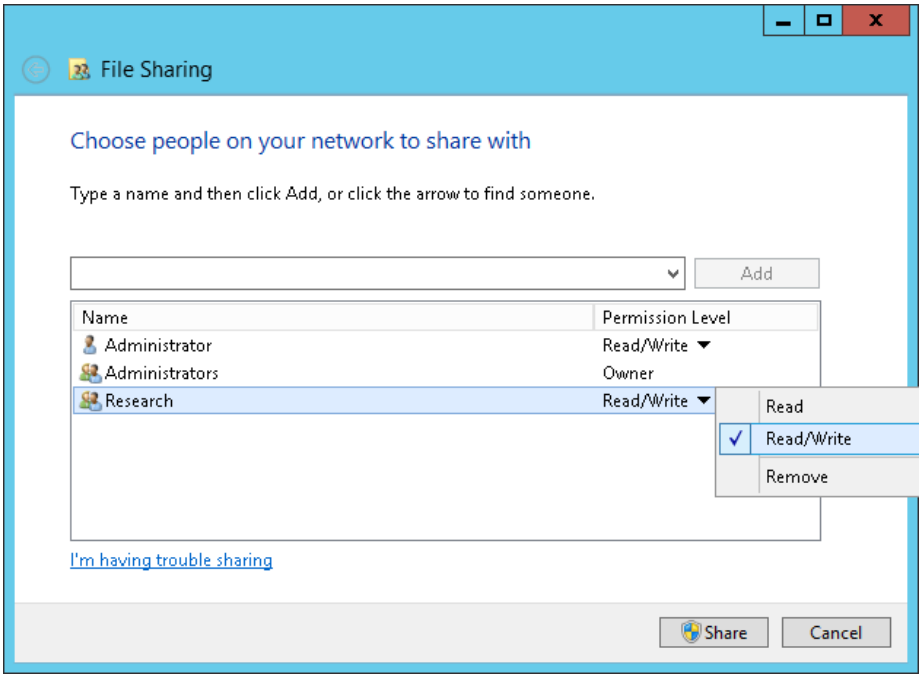
1. Trên máy **LON-DC1**, mở **File Explorer**, vào ổ **Local Disk (C:)**. Tạo một thư mục mới tên **ConfidentialResearch**. Chuột phải lên thư mục **ConfidentialResearch**, bung **Share with**, chọn **Specific people**.



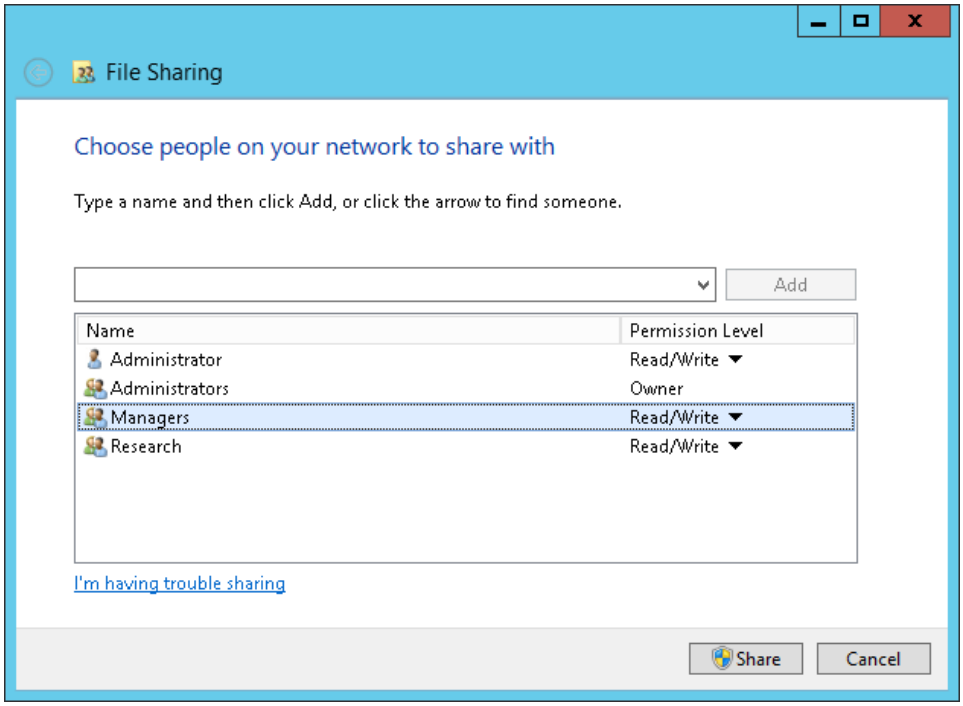
2. Cửa sổ **File Sharing**, nhập **Research**, chọn **Add**.




3. Chọn group **Research,** bung ô **Permission Level,** chọn **Read/Write**.

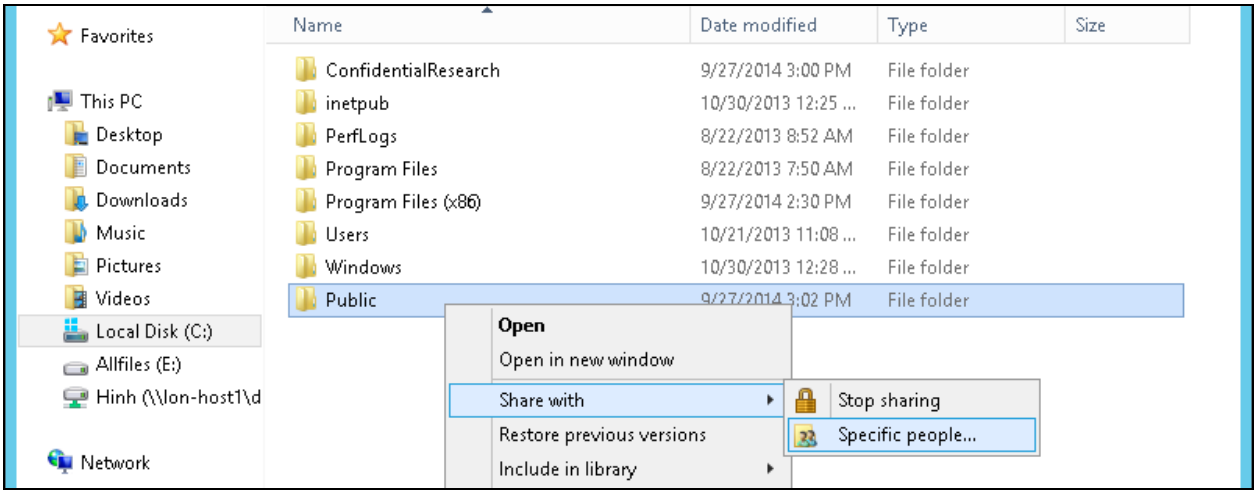


4. Lặp lại bước 2 và 3 để cấp quyền cho group **Managers** là **Read/Write.** Sau đó chọn **Share**, và chọn **Done**.

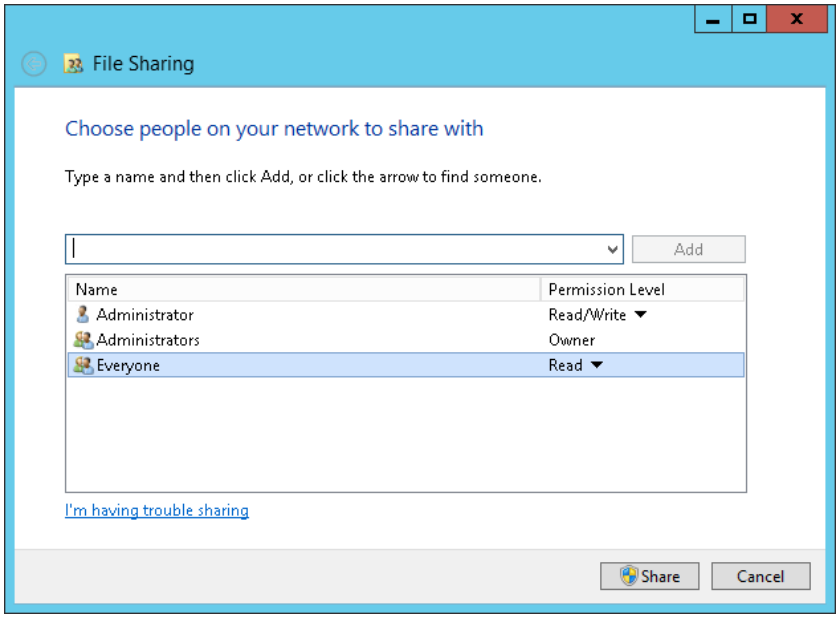



➢ **Tạo Share folder trên máy LON-DC1 để lưu trữ AD RMS Templates**

1. Trên máy **LON-DC1**, mở **File Explorer**, trong ổ **C**: Tạo một thư mục mới tên **Public**. Chuột phải lên thư mục **Public**, bung **Share with**, chọn **Specific people**.



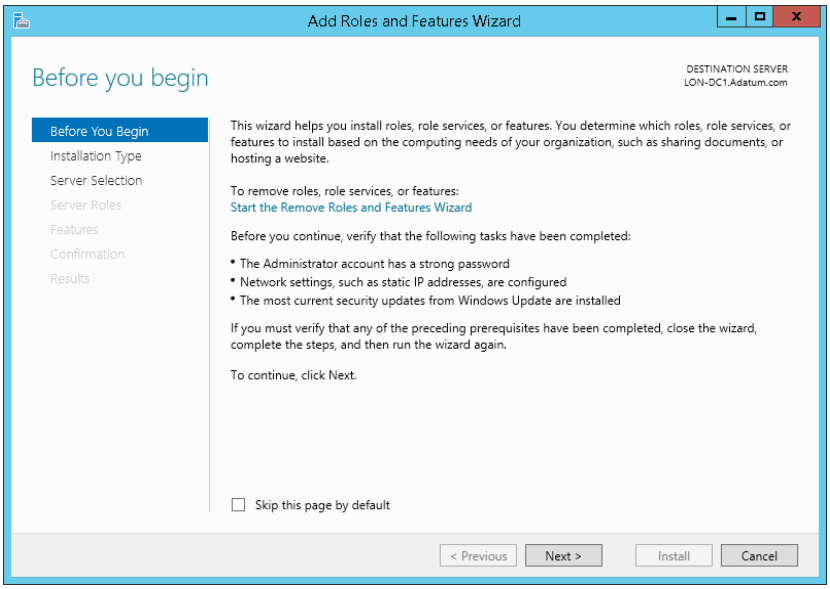
2. Chọn group **Everyone,** bung ô **Permission Level,** chọn **Read**. Chọn **Share**, và chọn **Done**.



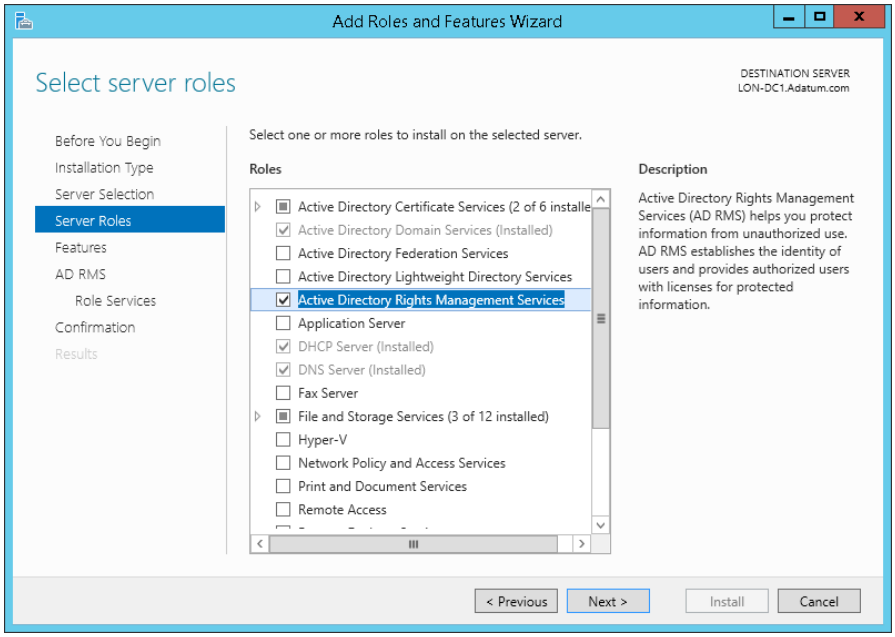

## Bước 2: Cài đặt và cấu RMS Server đầu tiên cho Adatum.com.

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

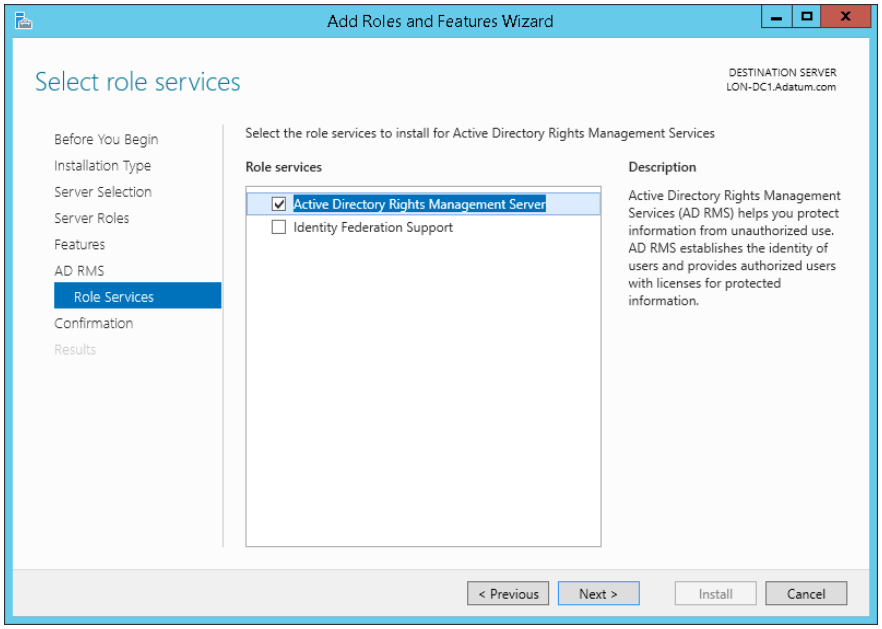
2. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



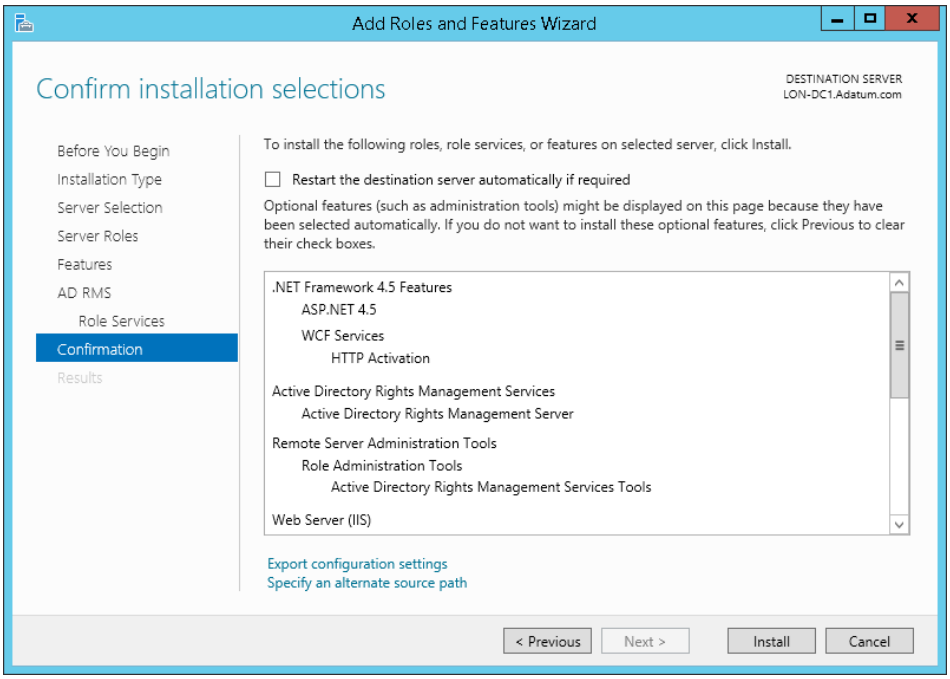
3. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Rights Management Services**, chọn **Add Features**, chọn **Next** 3 lần.



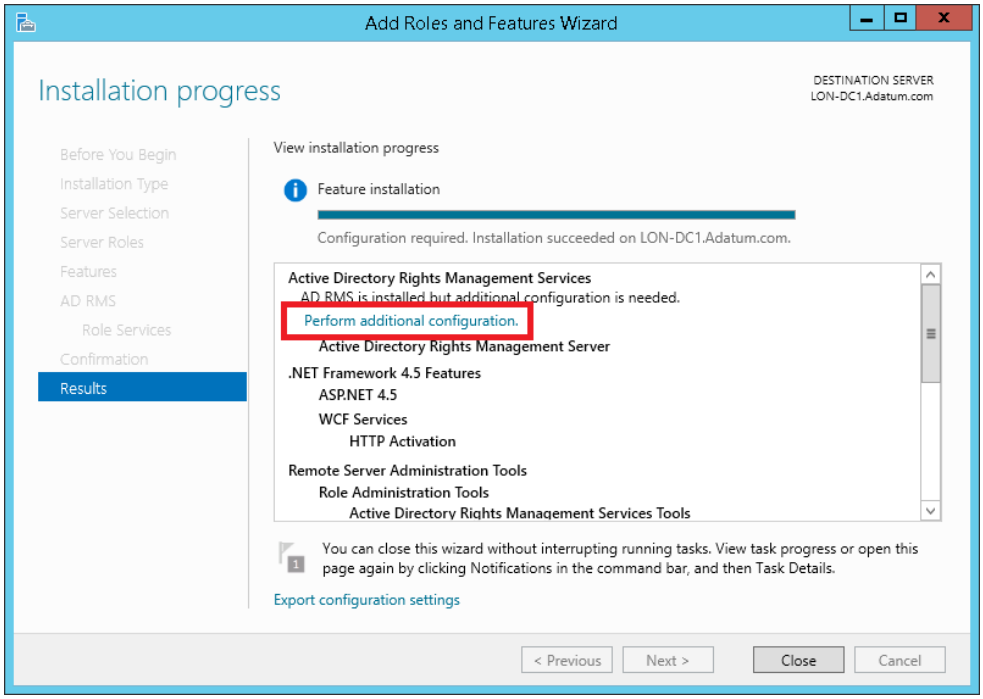

4. Cửa sổ **Select role services**, kiểm tra có đánh dấu chọn **Active Directory Rights Management Server**, chọn **Next**.



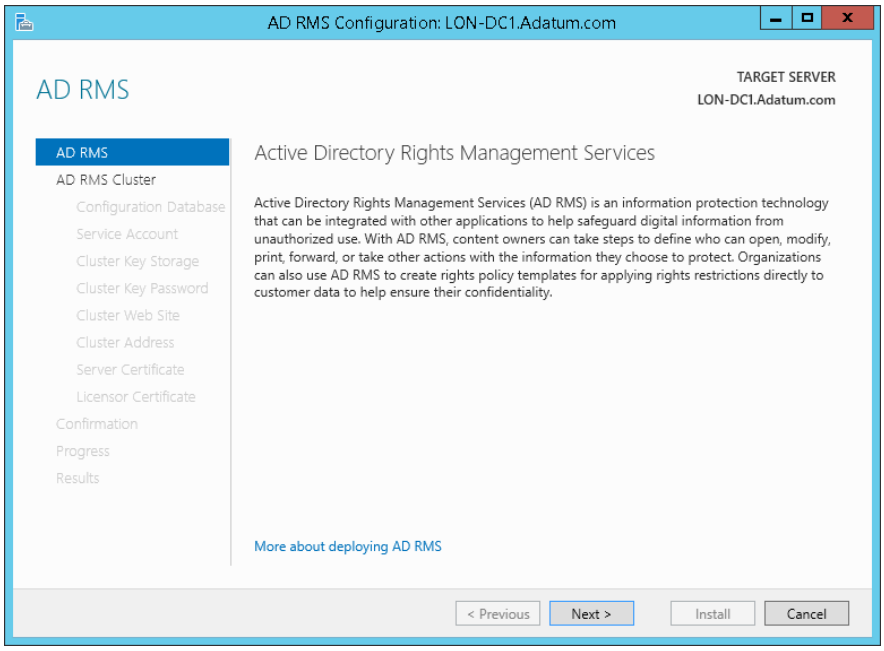
5. Cửa sổ **Confirm installation selections**, chọn **Install.**



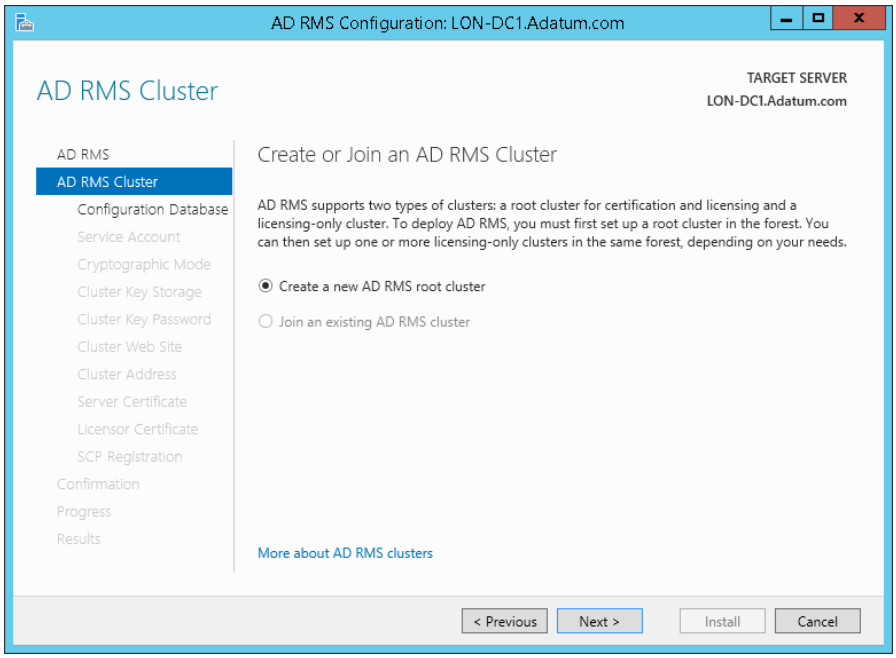

6. Cửa sổ **Installation progress,** chọn **Perform additional configuration**.



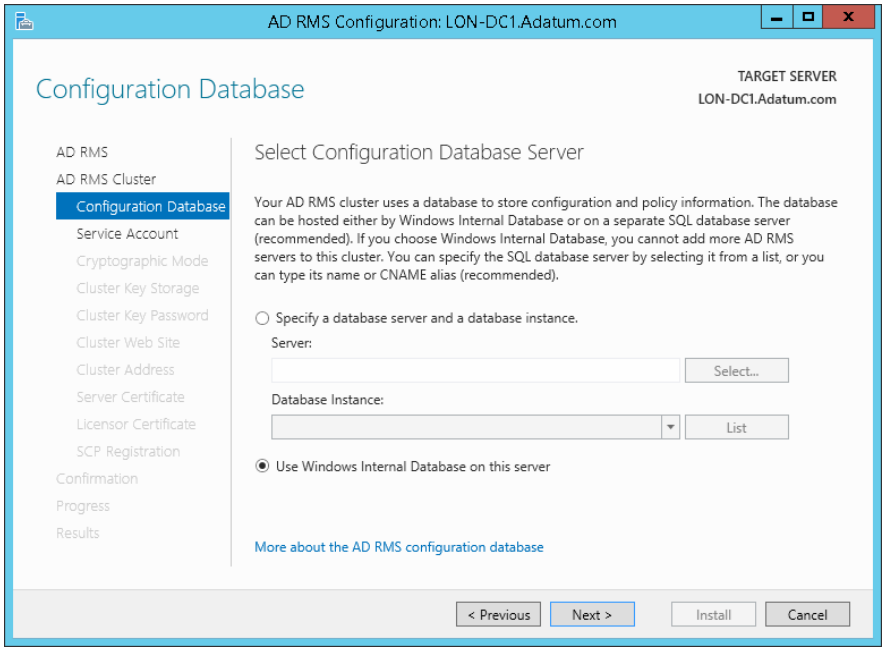
7. Cửa sổ **Active Directory Rights Management Services**, chọn **Next**.



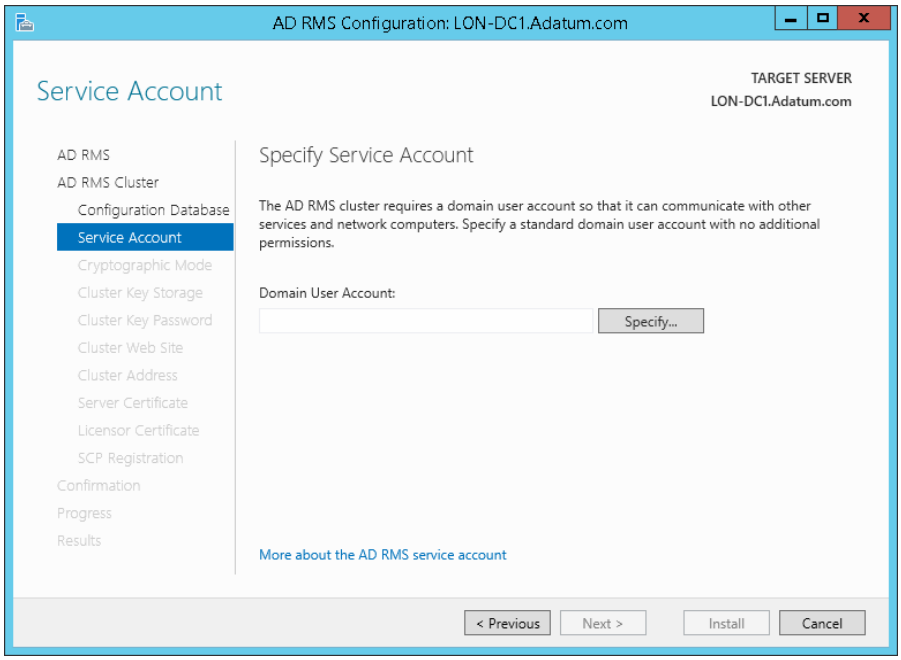

8. Cửa sổ **Create or Join an AD RMS Cluster**, chọn **Create a new AD RMS root cluster**, và chọn **Next**.



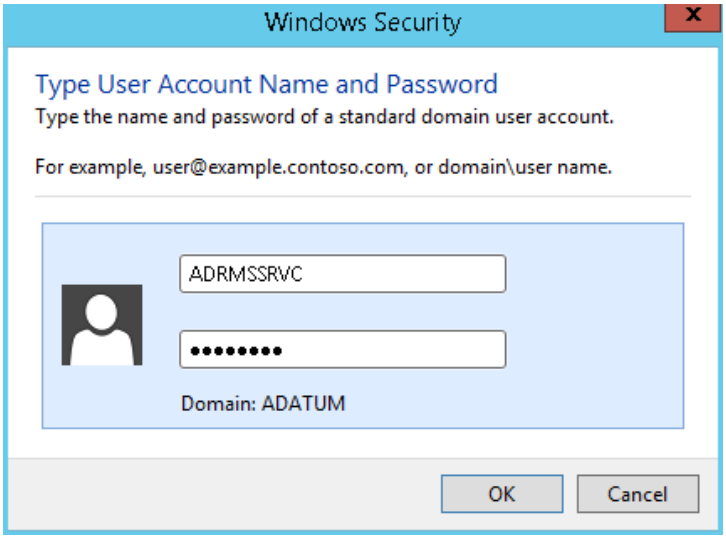
9. Cửa sổ **Select Configuration Database Server**, chọn **Use Windows Internal Database on this server**, và chọn **Next**.



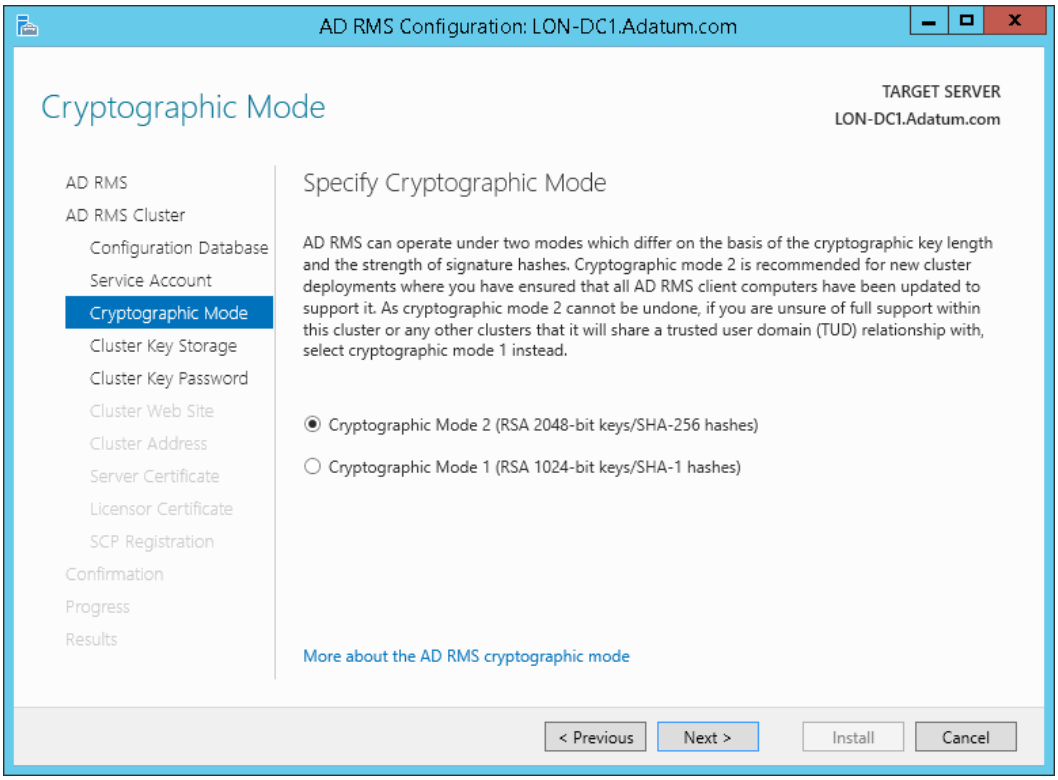

10. Cửa sổ **Specify Service Account**, , chọn **Specify.**



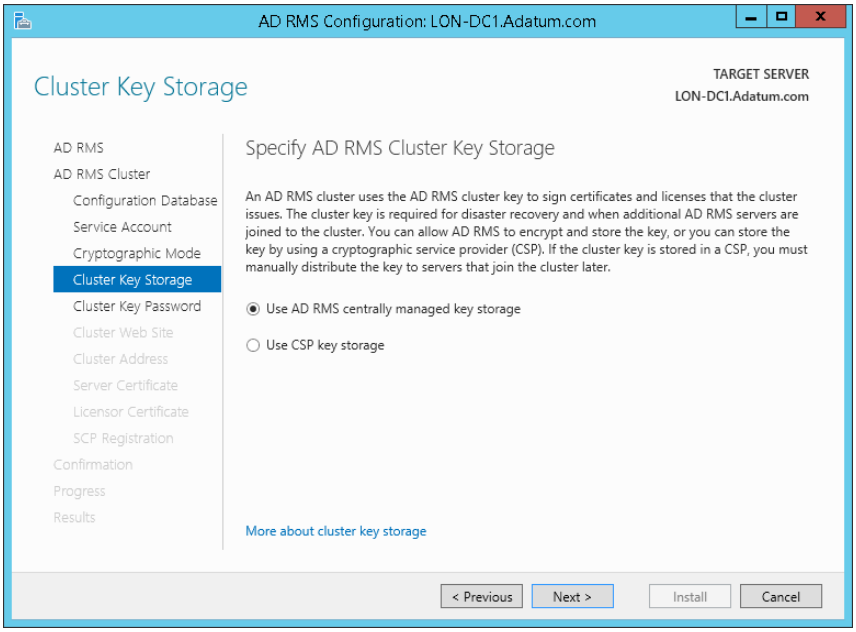
11. Hộp thoại **Windows Security**, trong ô **User name**nhập **ADRMSSRVC,** trong ô **Password** nhập **Pa$$w0rd**, và chọn **OK**. Và chọn **Next.**



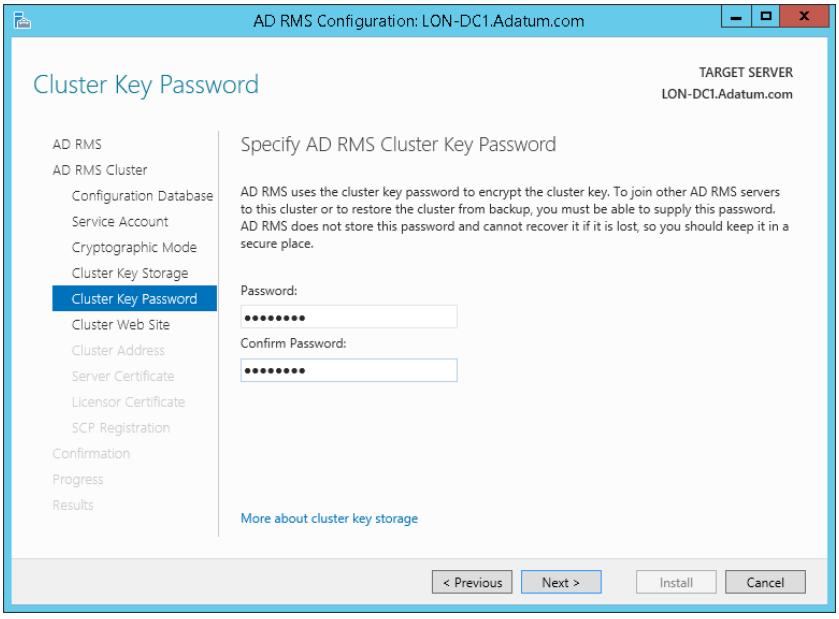

12. Cửa sổ **Cryptographic Mode**, chọn **Cryptographic Mode 2**, và chọn **Next**.



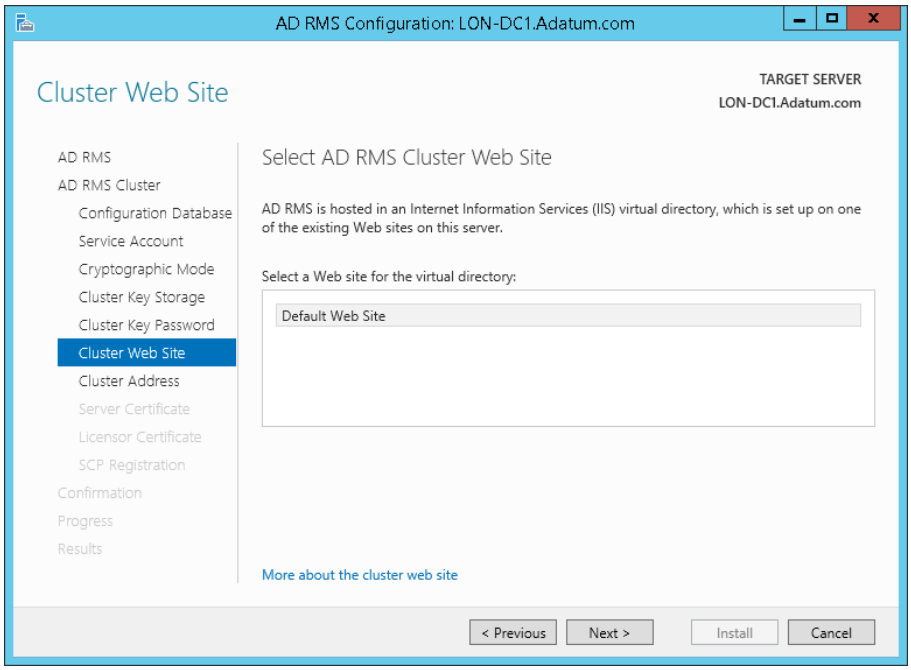
13. Cửa sổ **Cluster Key Storage**, chọn **Use AD RMS centrally managed key storage**, và chọn **Next**.



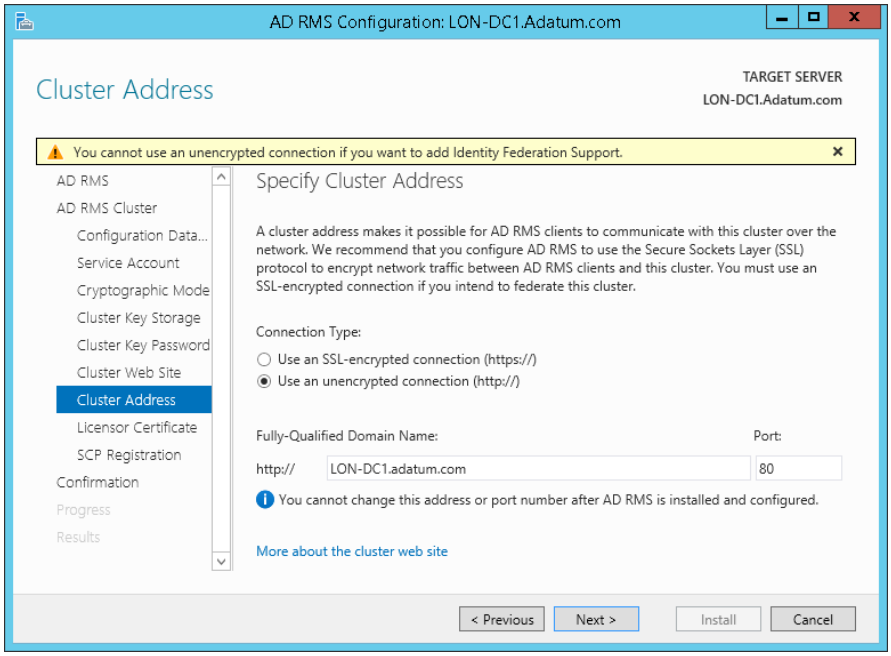

14. Cửa sổ **Cluster Key Password**, nhập **Pa$$w0rd** vào ô **Password** và **Confirm Password**, và chọn **Next**.



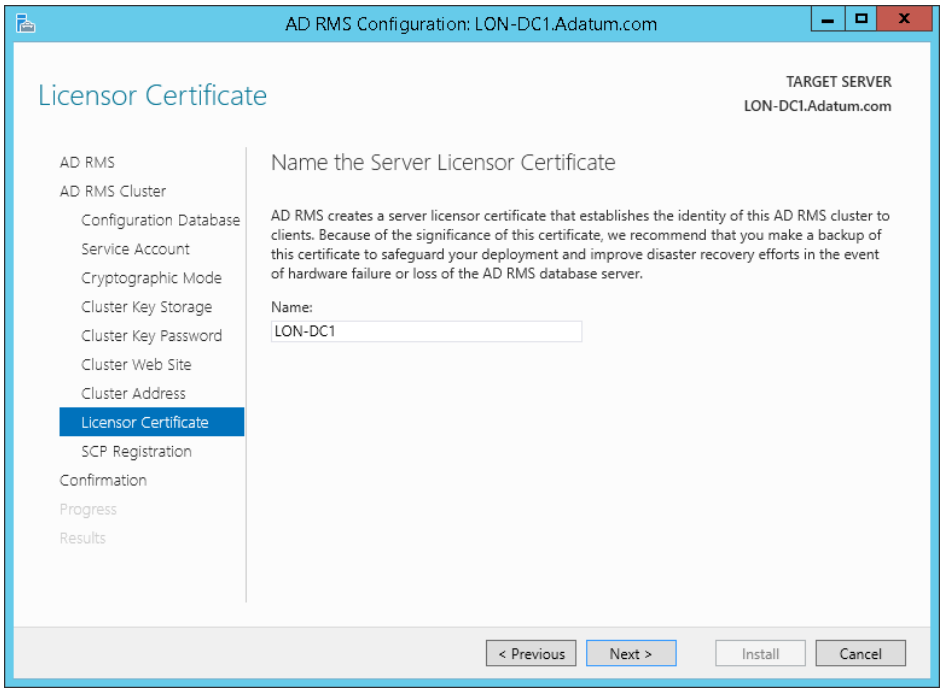
15. Cửa sổ **Cluster Web Site**, chọn **Default Web Site**, và chọn **Next**.



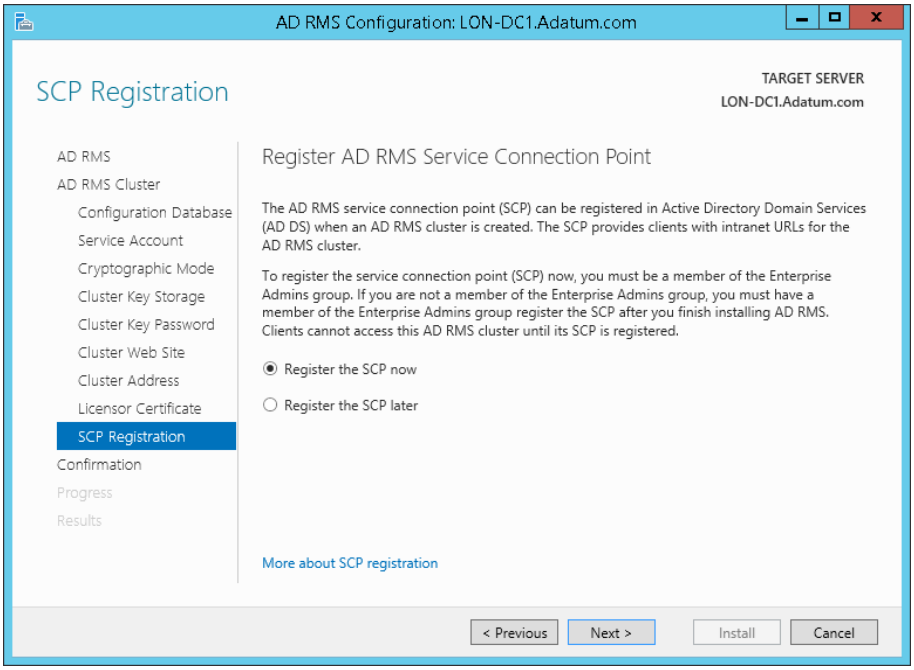

16. Cửa sổ **Cluster Address**, chọn **Use an unencrypted connection (http://)**, trong ô **Fully Qualified Domain Name**, nhập **LON-DC1.adatum.com**, và chọn **Next**.



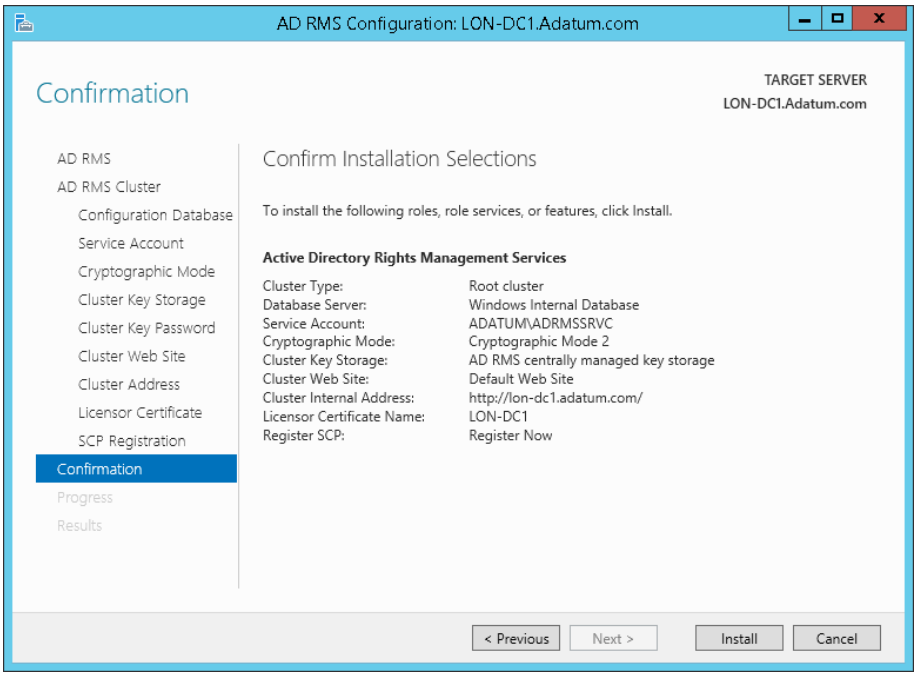
17. Cửa sổ **Licensor Certificate**, chọn **Next**.



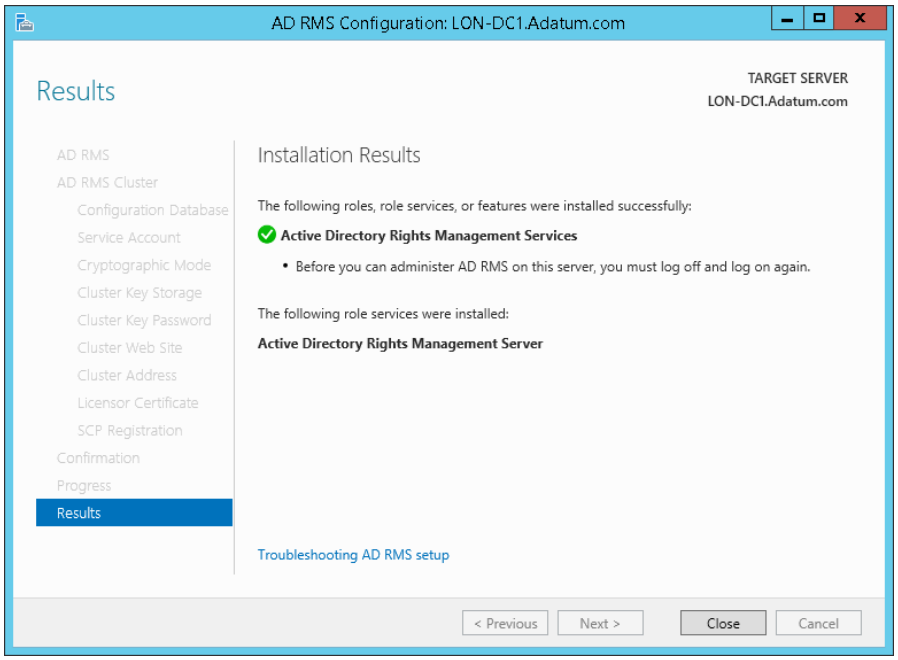

18. Cửa sổ **SCP Registration**, chọn **Register the SCP now**, và chọn **Next**.



19. Cửa sổ **Confirmation**, chọn **Install**.



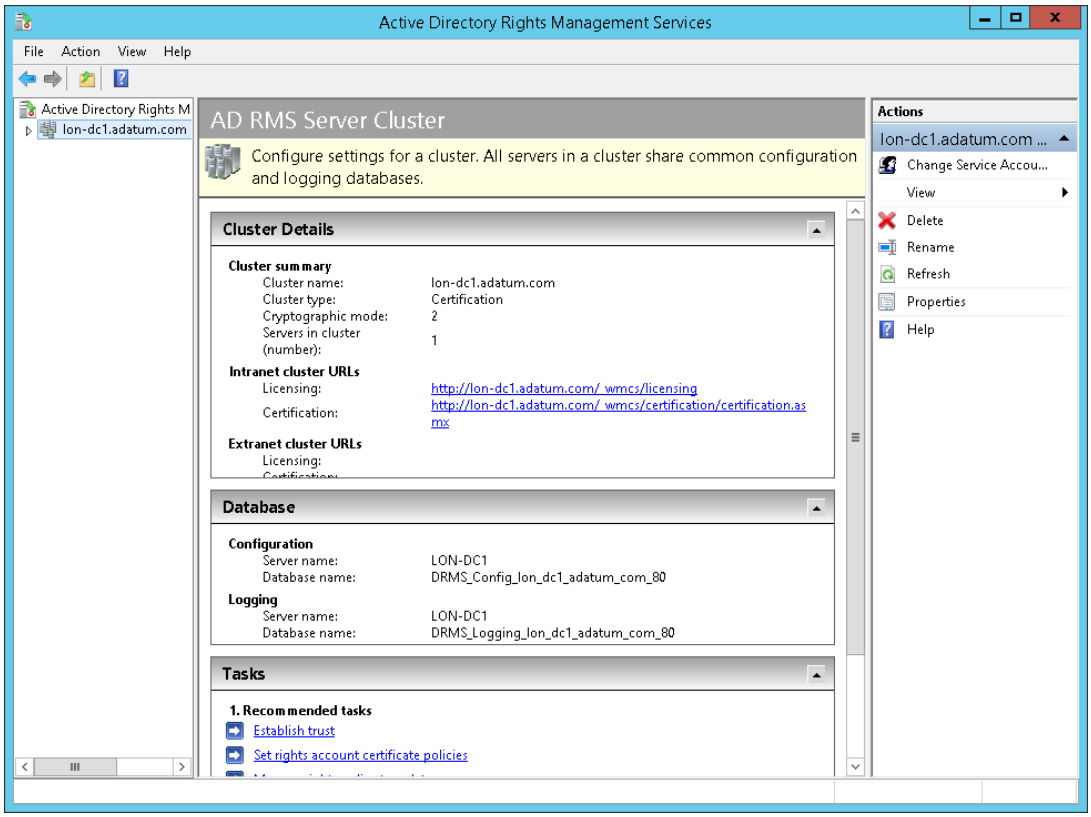

20. Sau khi cấu hình thành công, chọn **Close** 2 lần.



21. Sign out máy **LON-DC1**, và sign in bằng **Adatum\Administrator** với password **Pa$$w0rd** để cập nhật security token. (**Lưu ý:** Đây là bước bắt buộc)




22. Trong **Server Manager**, bung **Tools**, mở **Active Directory Rights Management Services**. Kiểm tra không có thông báo lỗi.

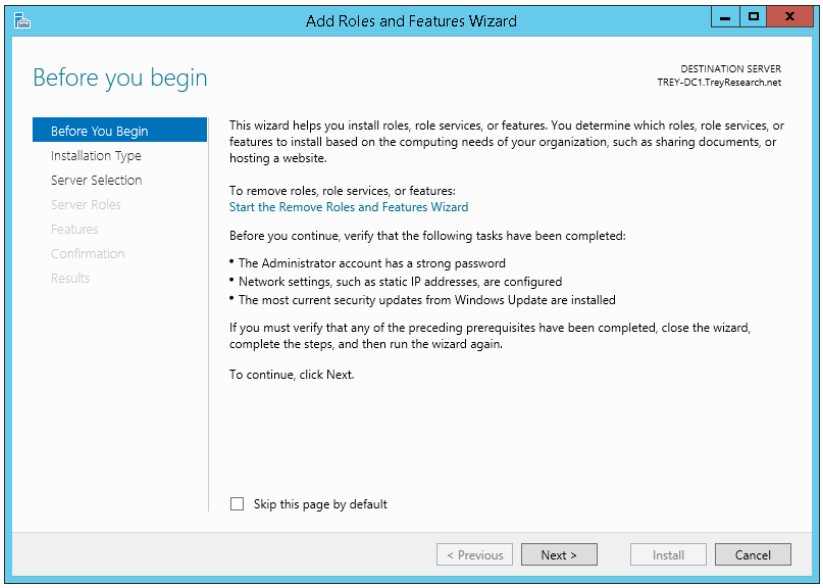



23. Tắt cửa sổ **Active Directory Rights Management Services**.

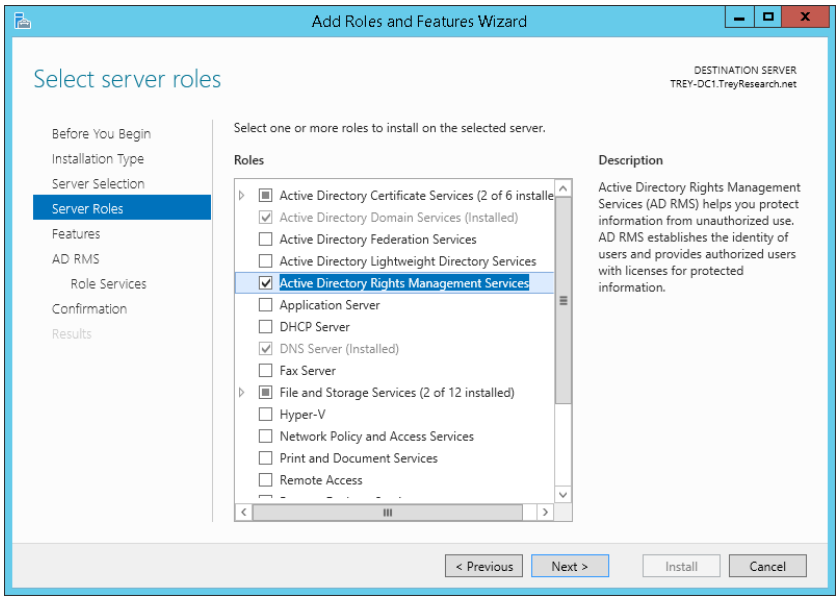
## Bước 3: Cài đặt và cấu hình AD RMS cho forest TreyResearch.net.

1. Qua máy **TREY-DC1**, trong **Server Manager**, chọn **Add roles and features**.

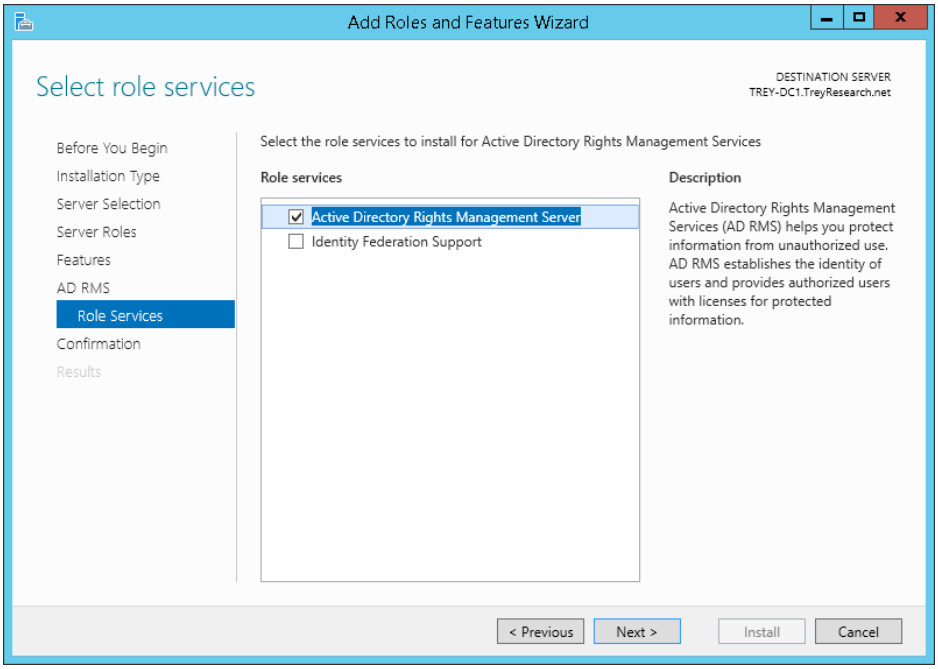
2. Cửa sổ **Before you begin**, chọn **Next** 3 lần.



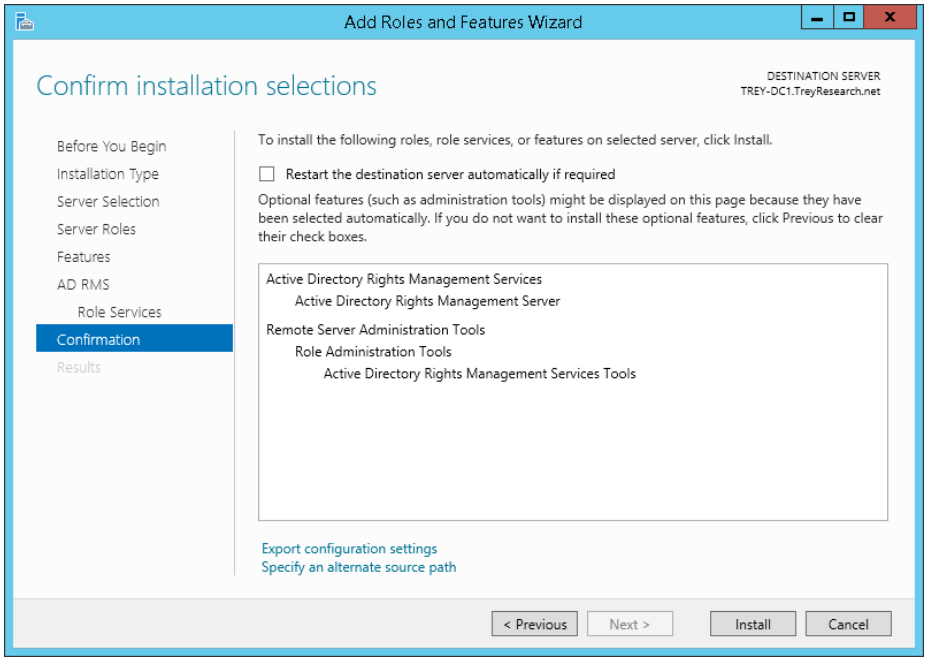

3. Cửa sổ **Select server roles**, đánh dấu chọn **Active Directory Rights Management Services**, chọn **Add Features**, chọn **Next** 3 lần.



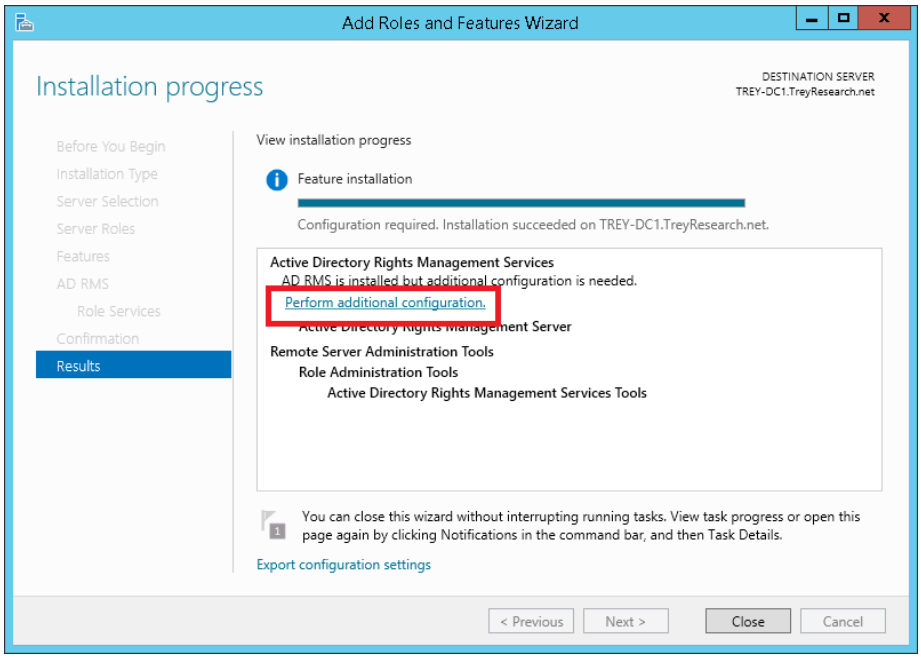
4. Cửa sổ **Select role services**, kiểm tra có đánh dấu chọn **Active Directory Rights Management Server**, chọn **Next**.



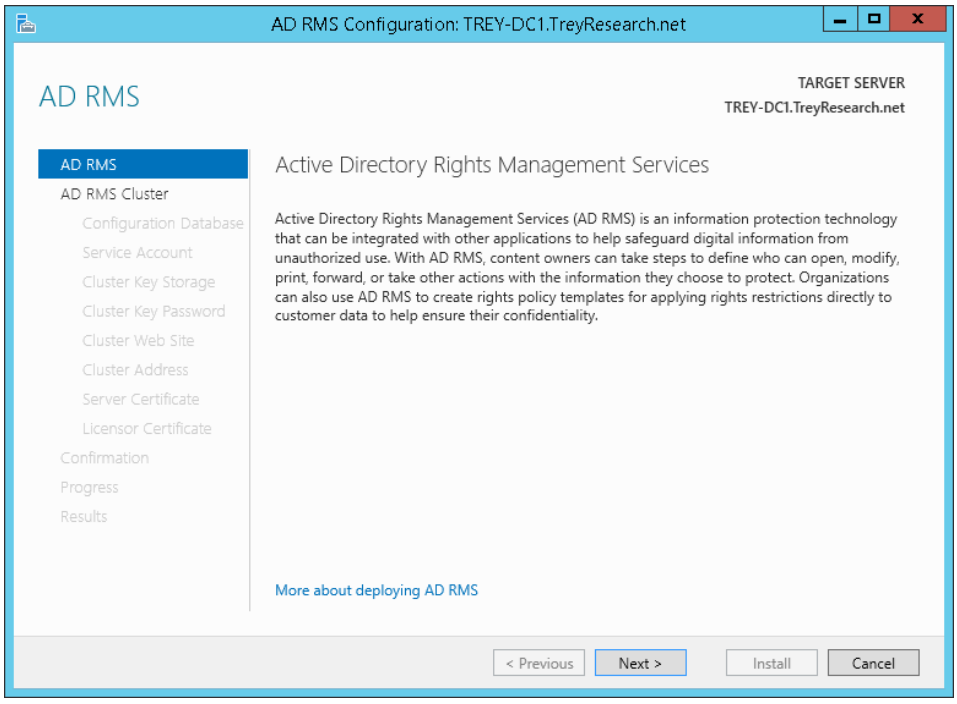

5. Cửa sổ **Confirm installation selections**, chọn **Install.**



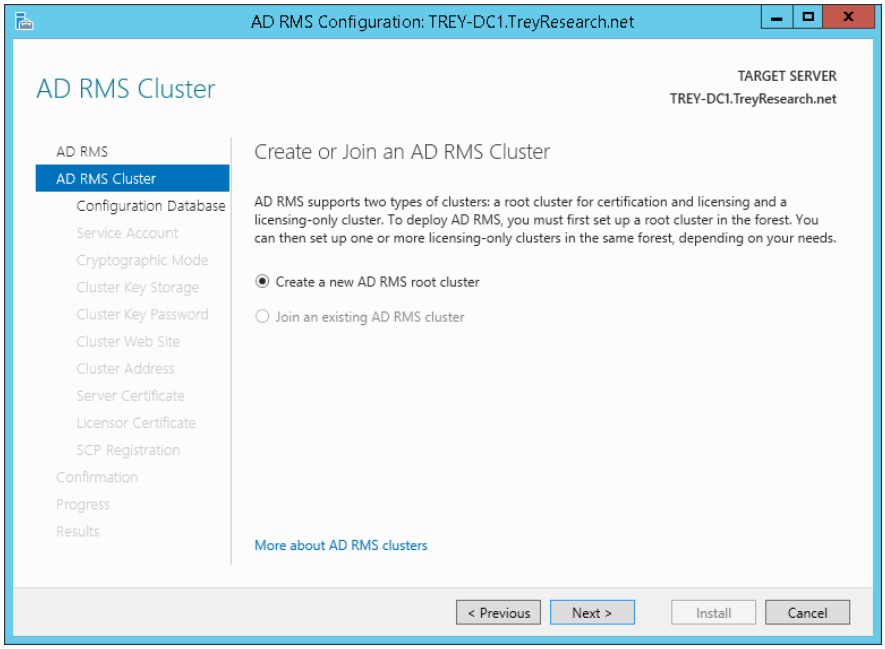
6. Cửa sổ **Installation progress,** chọn **Perform additional configuration**.



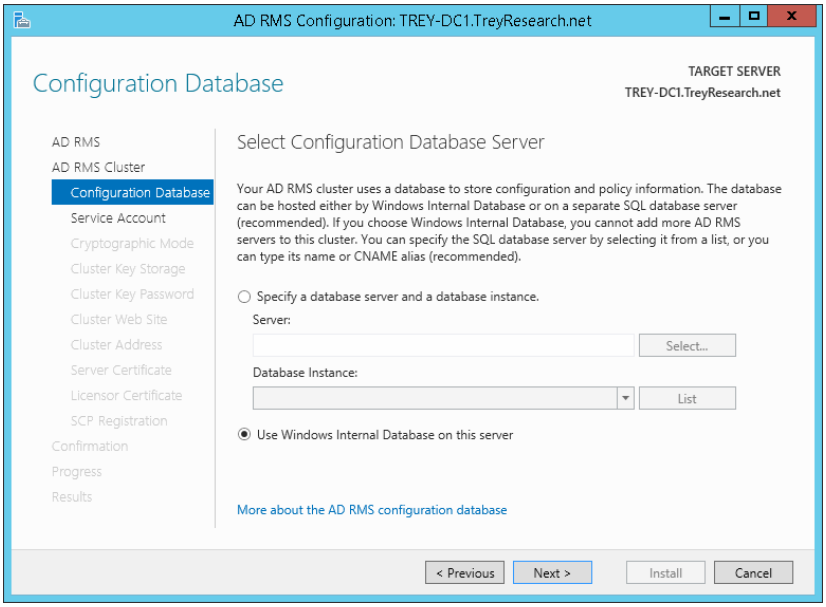

7. Cửa sổ **Active Directory Rights Management Services**, chọn **Next**.



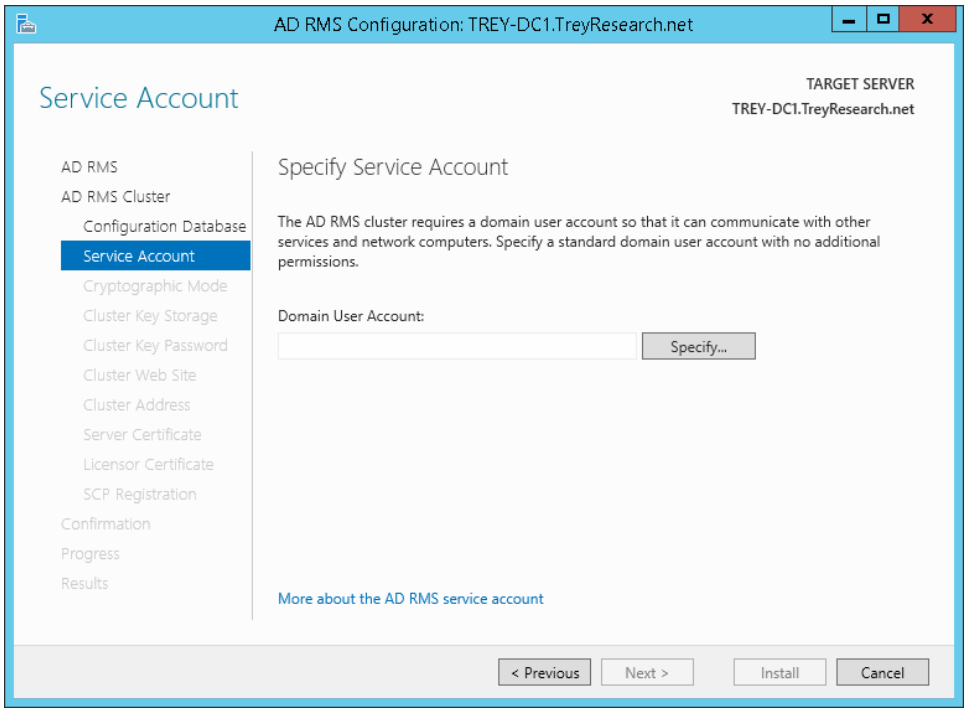
8. Cửa sổ **Create or Join an AD RMS Cluster**, chọn **Create a new AD RMS root cluster**, và chọn **Next**.



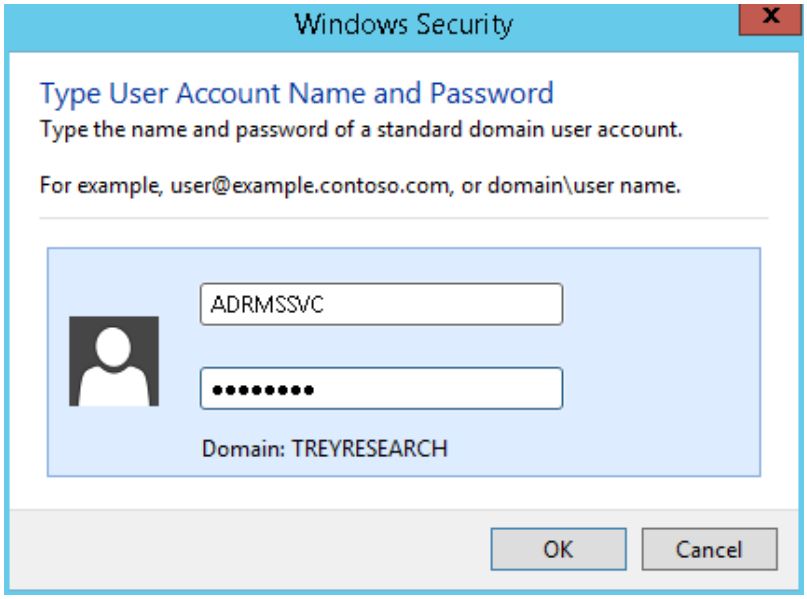

9. Cửa sổ **Select Configuration Database Server**, chọn **Use Windows Internal Database on this server**, và chọn **Next**.



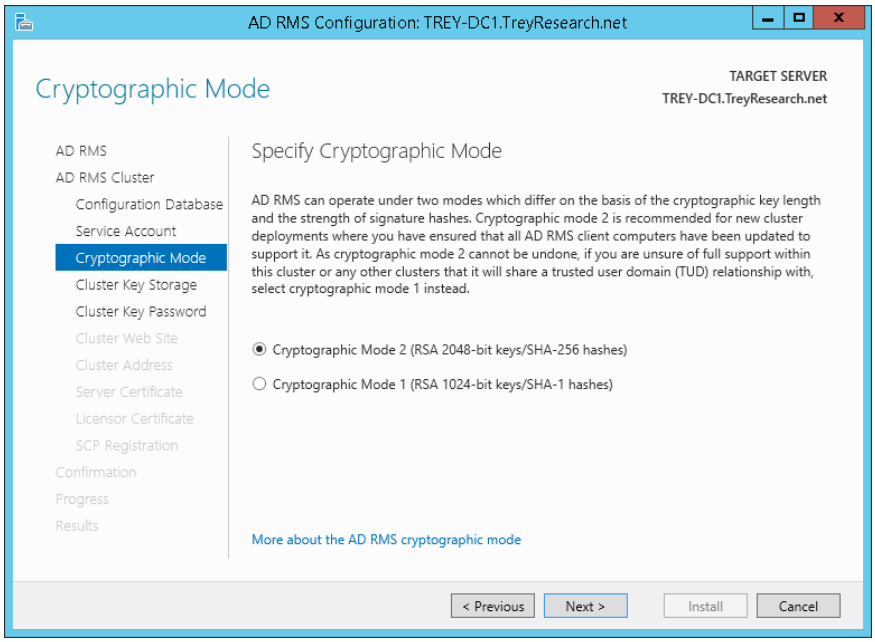
10. Cửa sổ **Specify Service Account**, , chọn **Specify.**



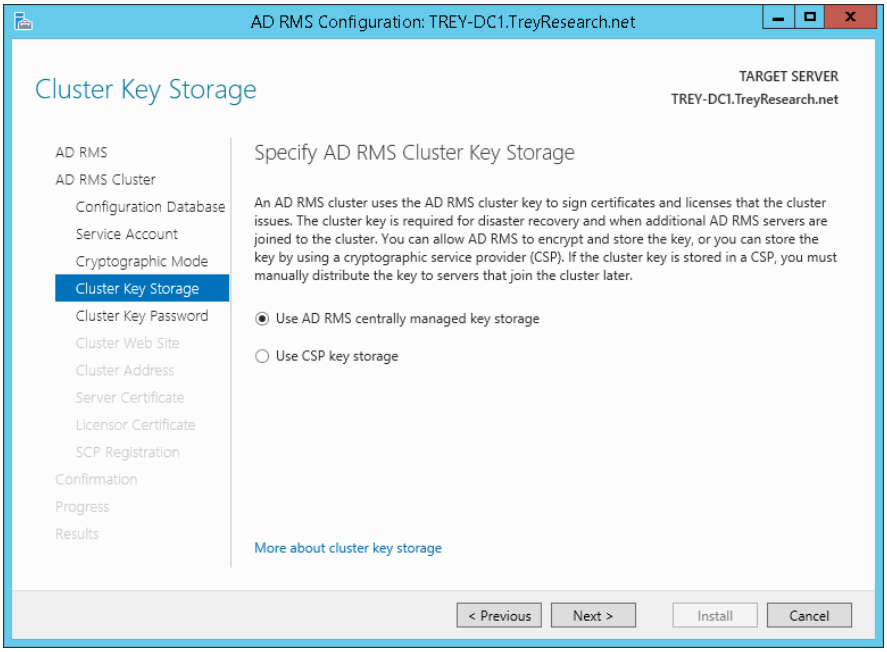

11. Hộp thoại **Windows Security**, trong ô **User name**nhập **ADRMSSVC,** trong ô **Password** nhập **Pa$$w0rd**, và chọn **OK**. Và chọn **Next.**



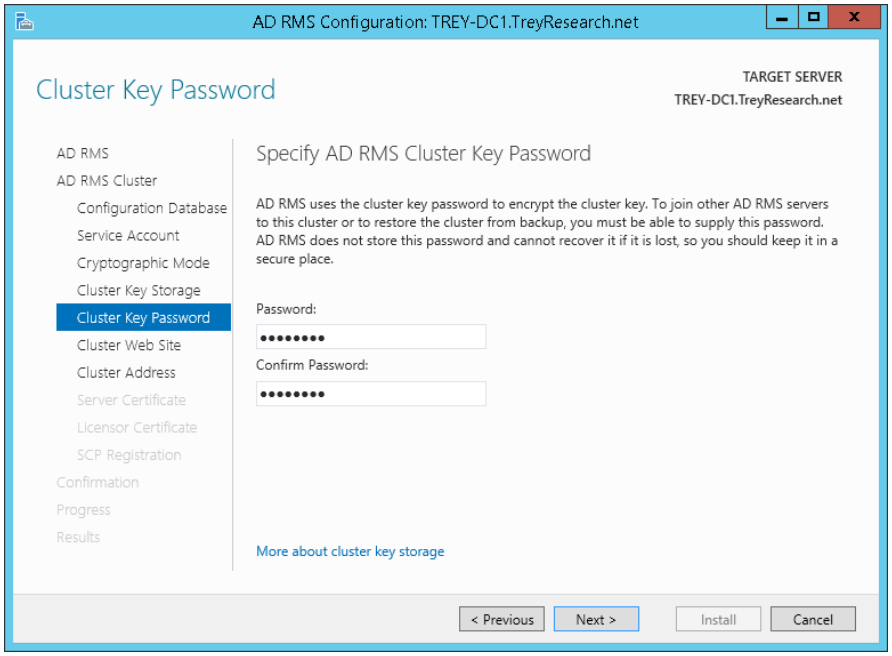
12. Cửa sổ **Cryptographic Mode**, chọn **Cryptographic Mode 2**, và chọn **Next**.



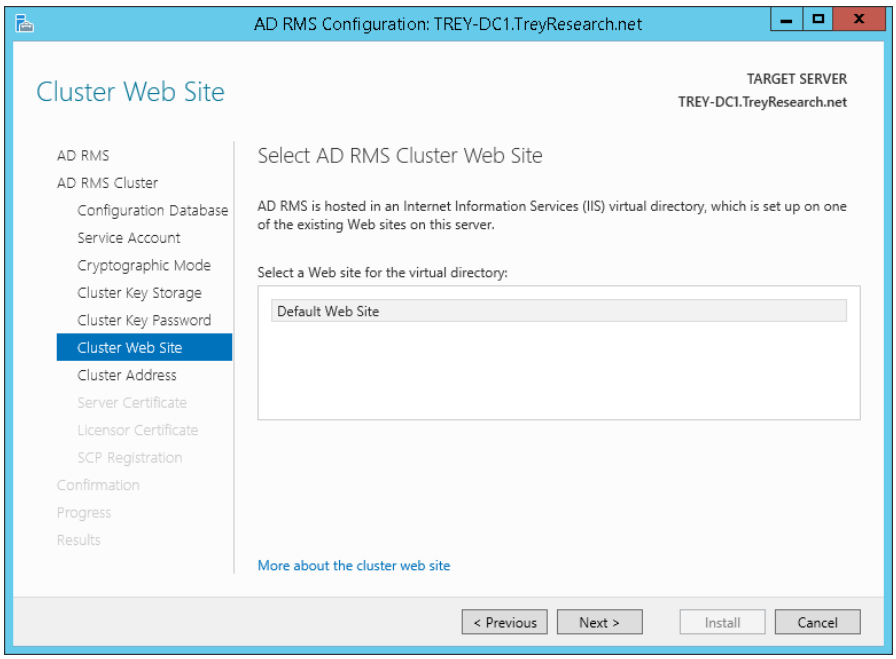

13. Cửa sổ **Cluster Key Storage**, chọn **Use AD RMS centrally managed key storage**, và chọn **Next**.



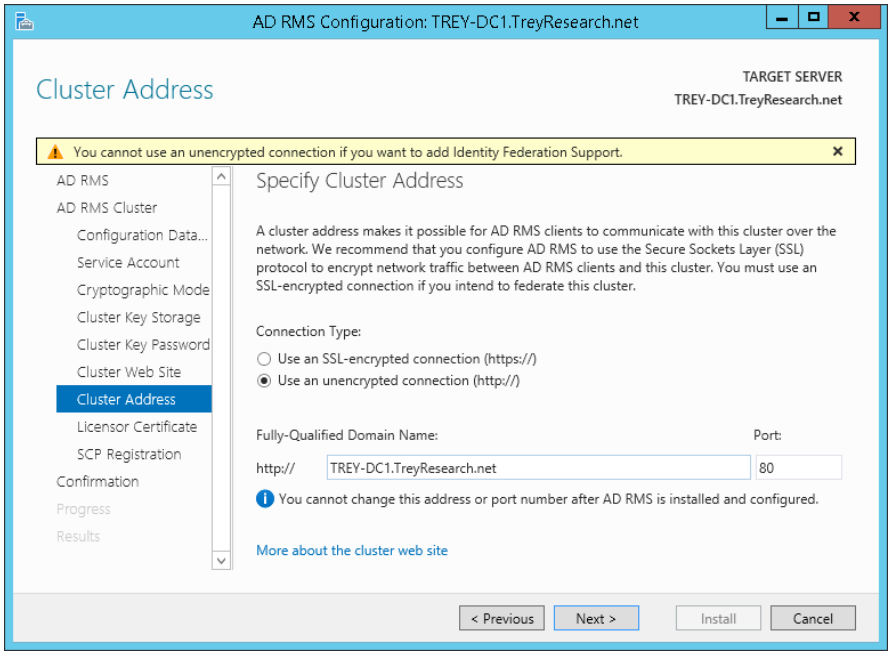
14. Cửa sổ **Cluster Key Password**, nhập **Pa$$w0rd** vào ô **Password** và **Confirm Password**, và chọn **Next**.



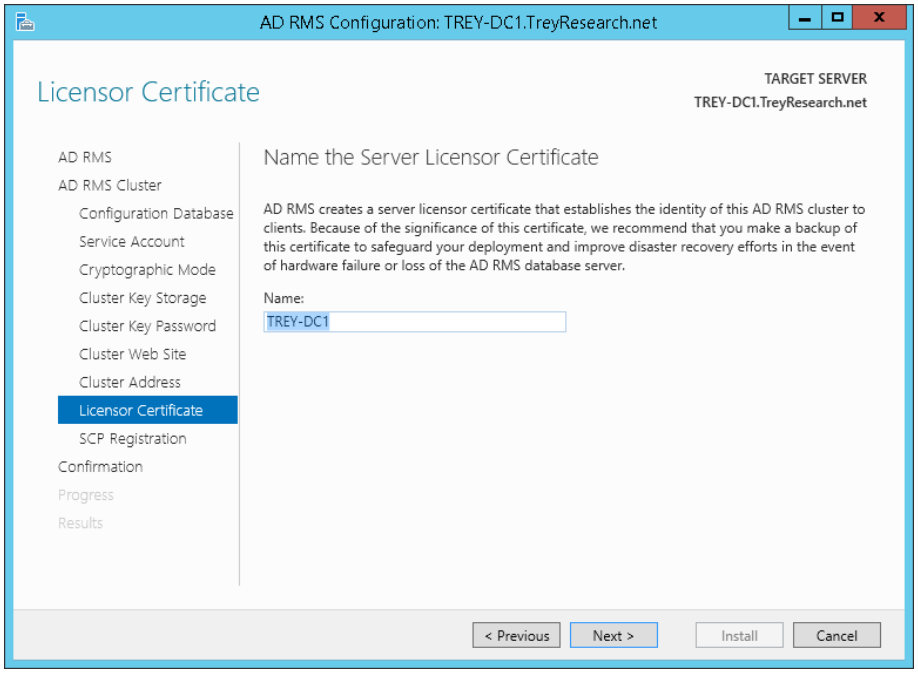

15. Cửa sổ **Cluster Web Site**, chọn **Default Web Site**, và chọn **Next**.



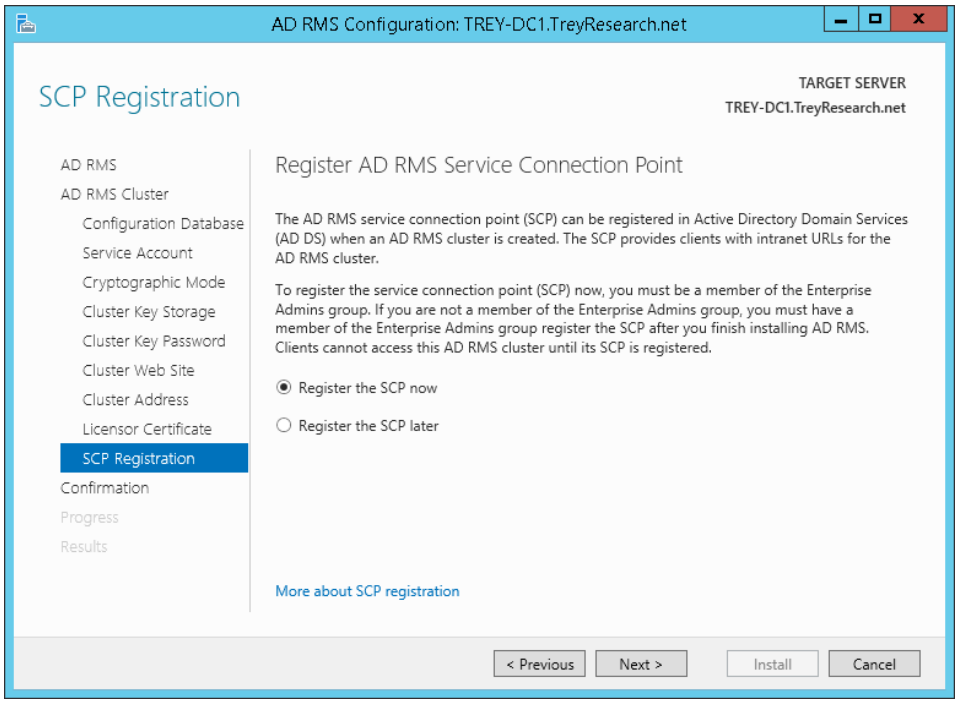
16. Cửa sổ **Cluster Address**, chọn **Use an unencrypted connection (http://)**, trong ô **Fully Qualified Domain Name**, nhập **TREY-DC1.TreyResearch.net**, và chọn **Next**.



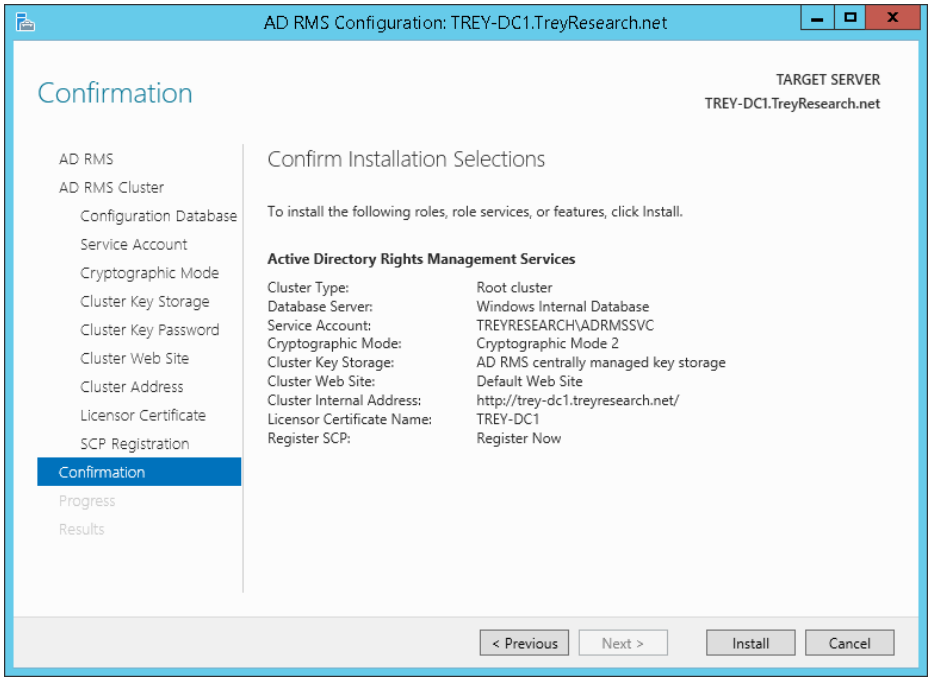

17. Cửa sổ **Licensor Certificate**, chọn **Next**.



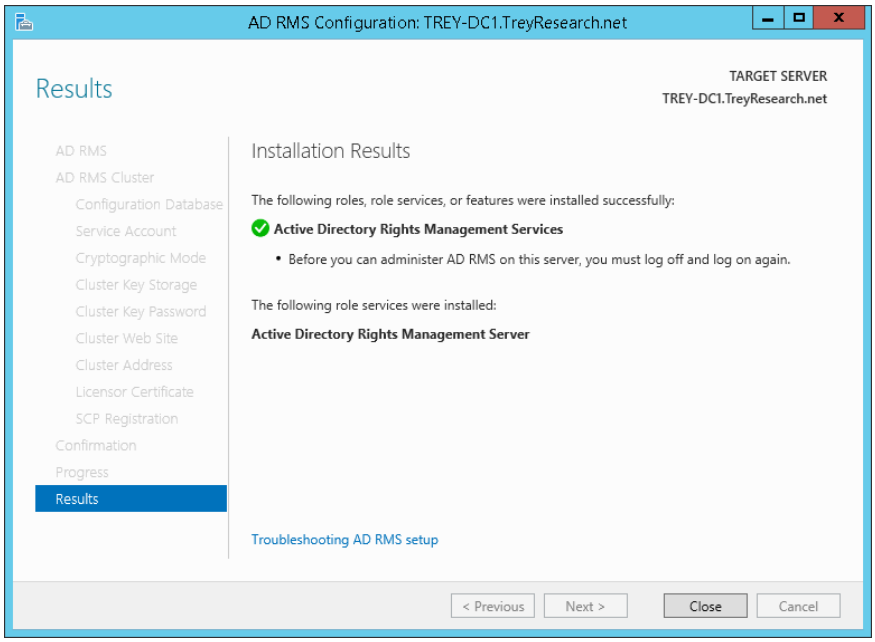
18. Cửa sổ **SCP Registration**, chọn **Register the SCP now**, và chọn **Next**.




19. Cửa sổ **Confirmation**, chọn **Install**.

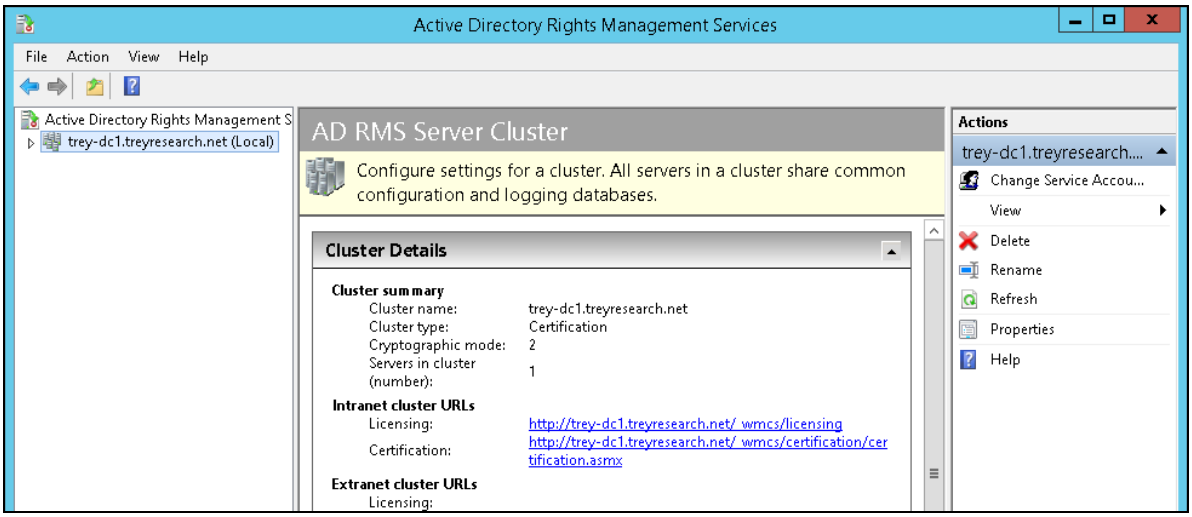


20. Sau khi cấu hình thành công, chọn **Close** 2 lần.




21. Sign out máy **TREY-DC1**, và sign in lại bằng **Treyresearch\Administrator** với password **Pa$$w0rd** để cập nhật security token.

22. Trong **Server Manager**, bung **Tools**, mở **Active Directory Rights Management Services**. Kiểm tra không có thông báo lỗi.

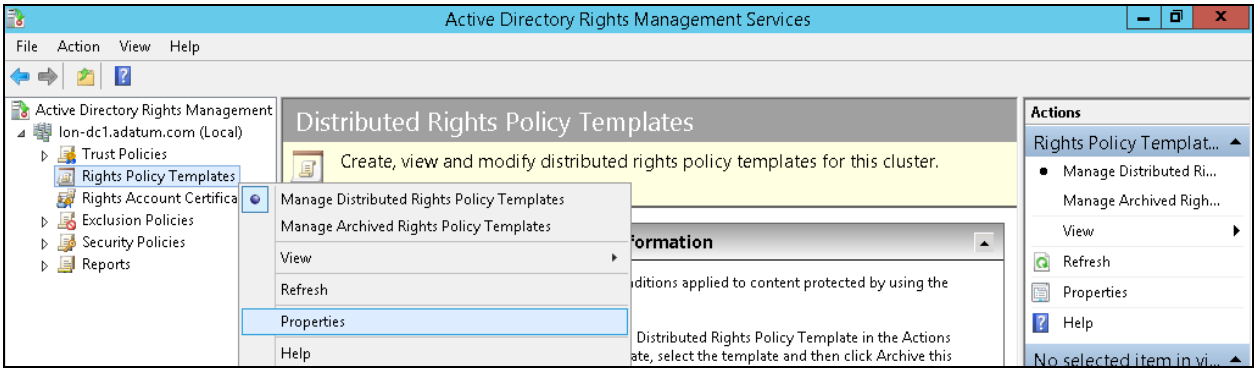



23. Tắt cửa sổ **Active Directory Rights Management Services**.

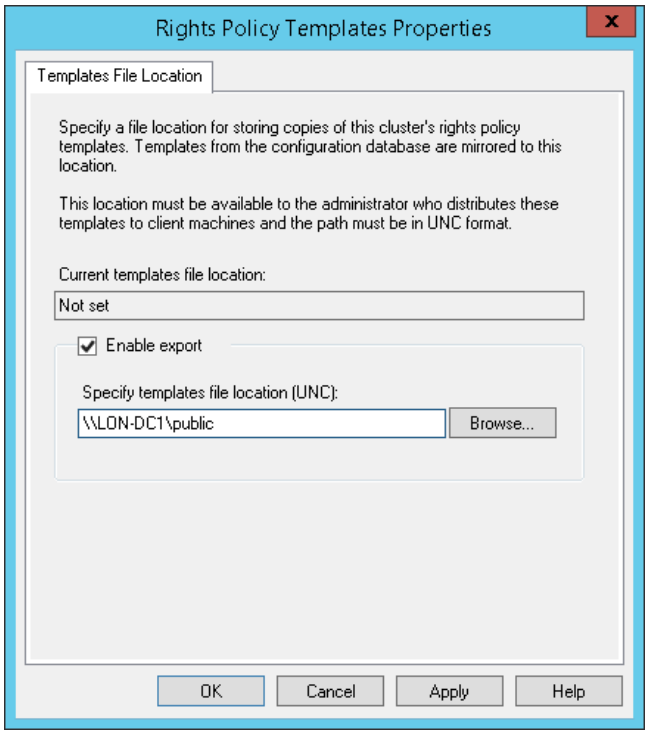
## Bước 4: Cấu hình AD RMS Templates.

➢ **Tạo AD RMS Rights Policy Template**

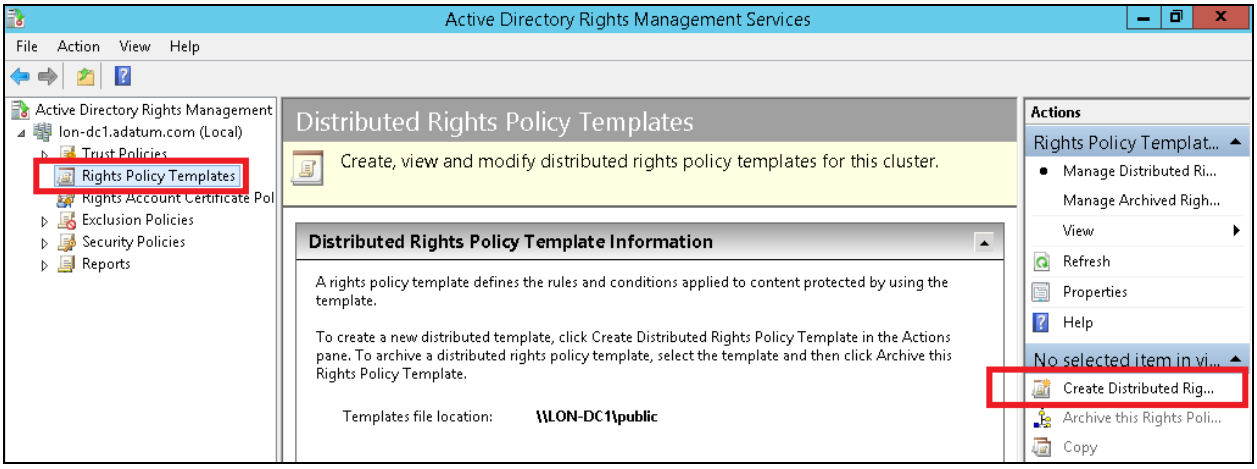
1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Active Directory Rights Management Services**, bung **lon-dc1.adatum.com**, chọn và chuột phải **Rights Policy Templates**, chọn **Properties**.



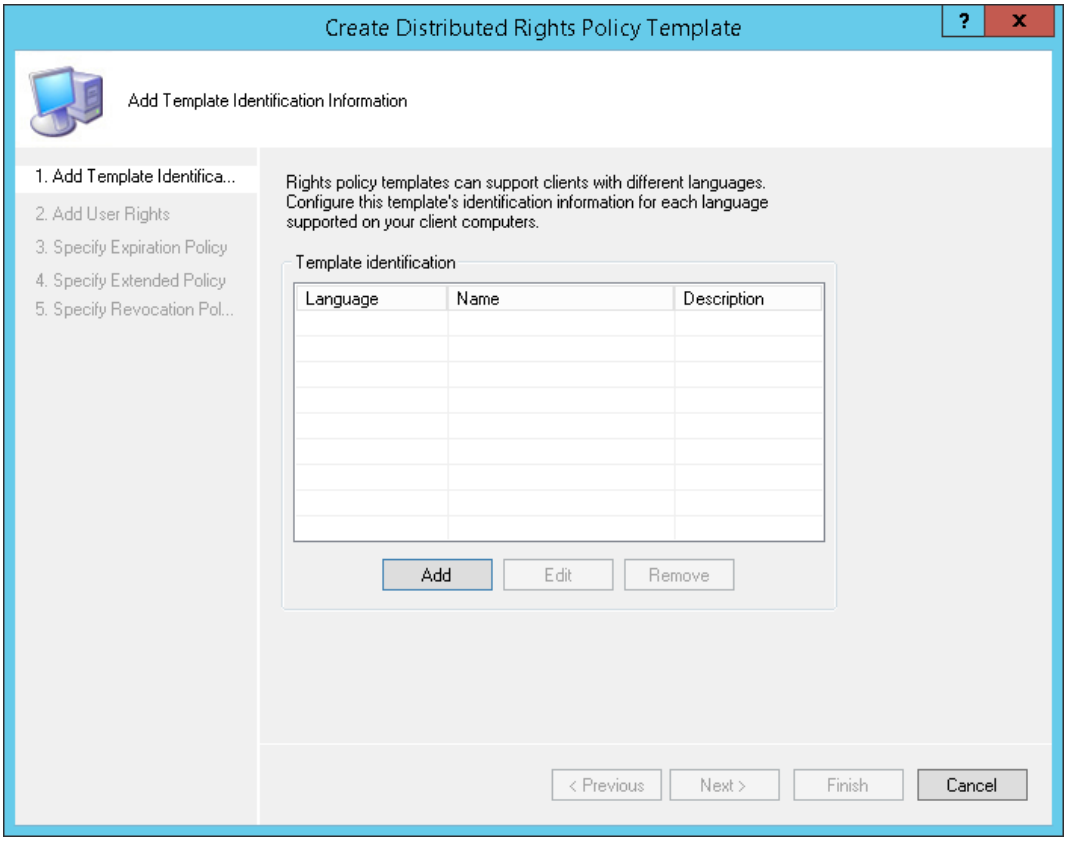

2. Hộp thoại **Rights Policy Templates Properties**, đánh dấu chọn **Enable export**, trong ô **Specify templates file location (UNC)**, nhập **\\LON-DC1\public**, chọn **OK**.



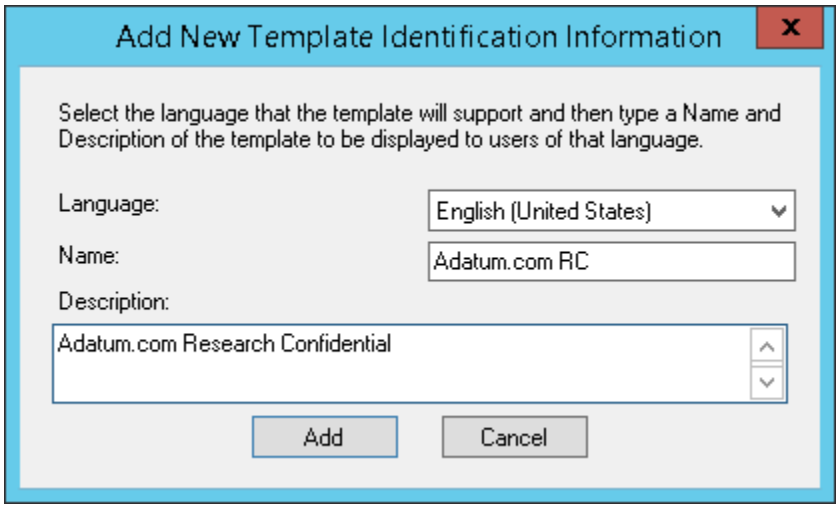
3. Chọn **Rights Policy Templates,** trong cửa sổ **Actions**, chọn **Create Distributed Rights Policy Template**.



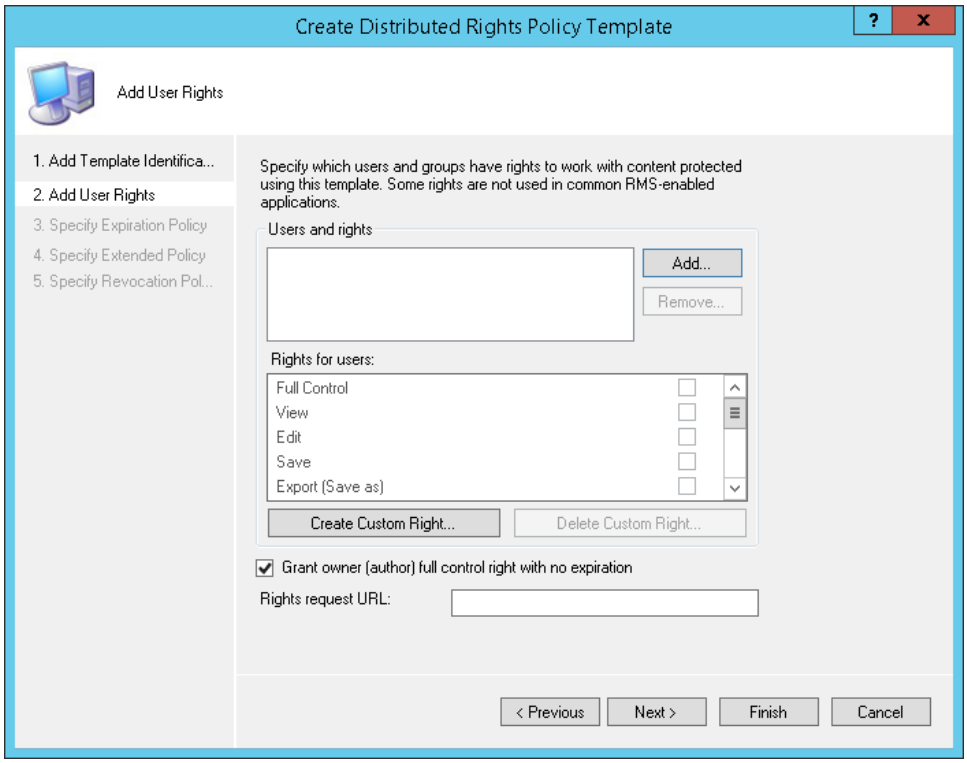

4. Cửa sổ **Add Template Identification Information**, chọn **Add**.



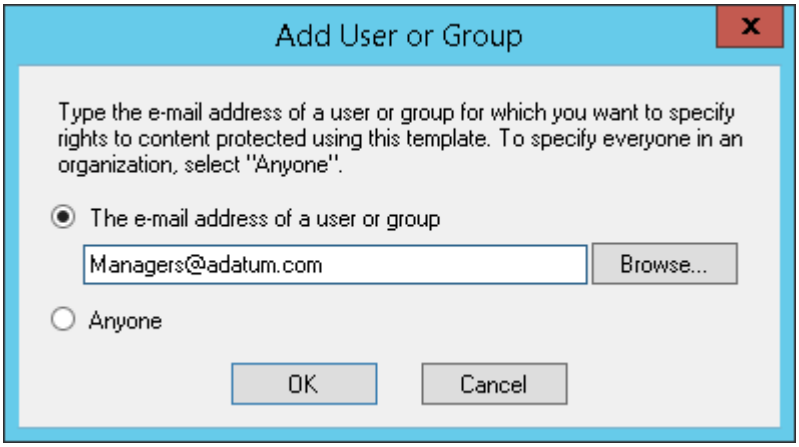
5. Hộp thoại **Add New Template Identification Information**, bung ô **Language**, chọn **English (United States)**, trong ô **Name**, nhập **Adatum.com RC**, trong ô **Description**, nhập **Adatum.com Research Confidential**, chọn **Add**, và chọn **Next**.



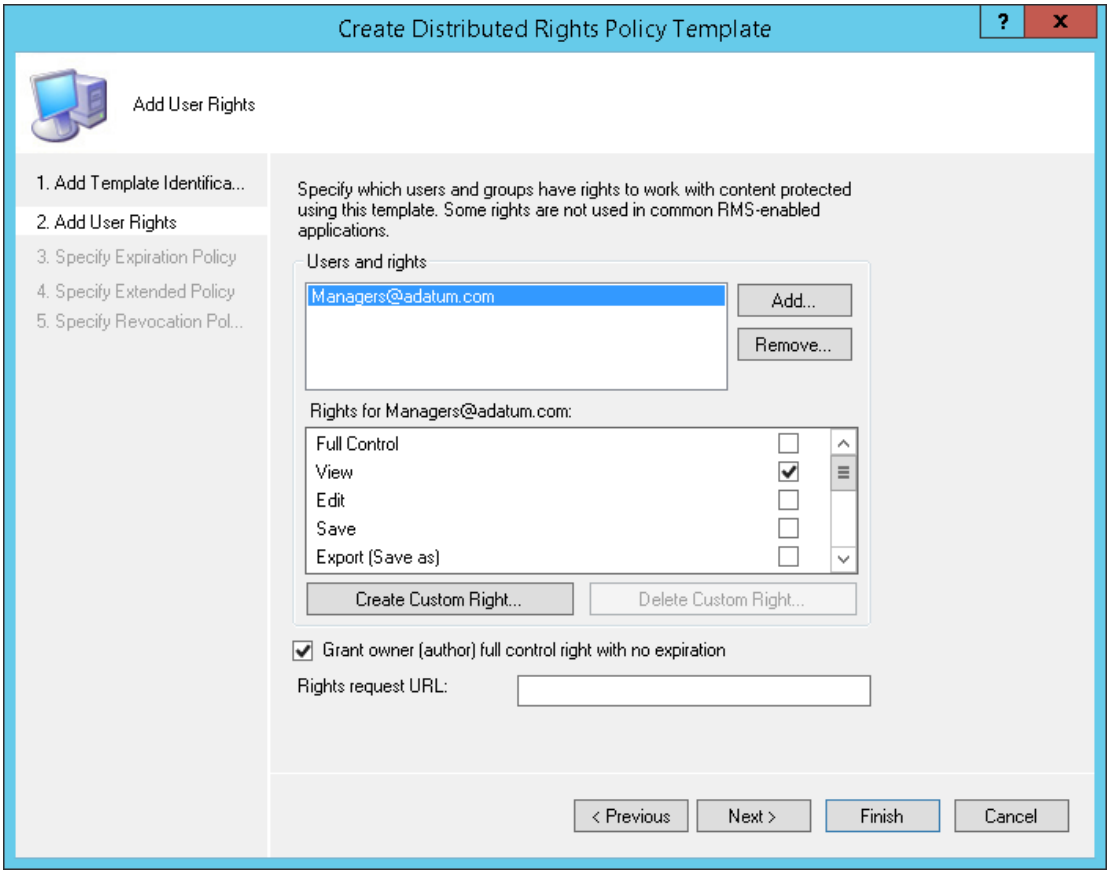

6. Cửa sổ **Add User Rights**, chọn **Add**.



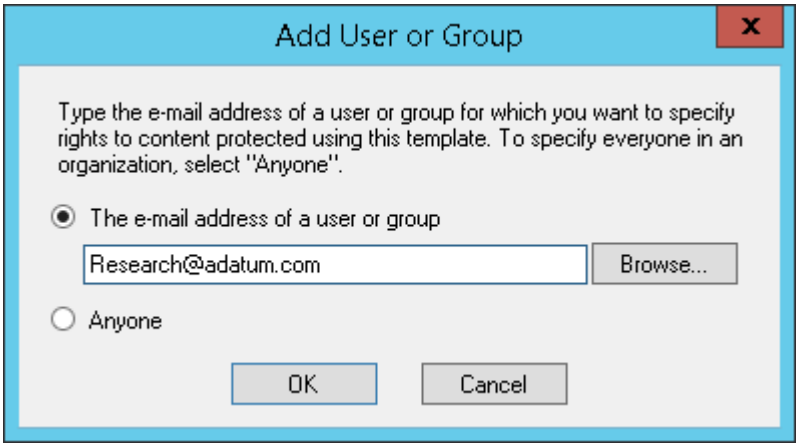
7. Hộp thoại **Add User or Group**, chọn **The e-mail address of a user or group**, nhập **Managers@adatum.com**, chọn **OK**.



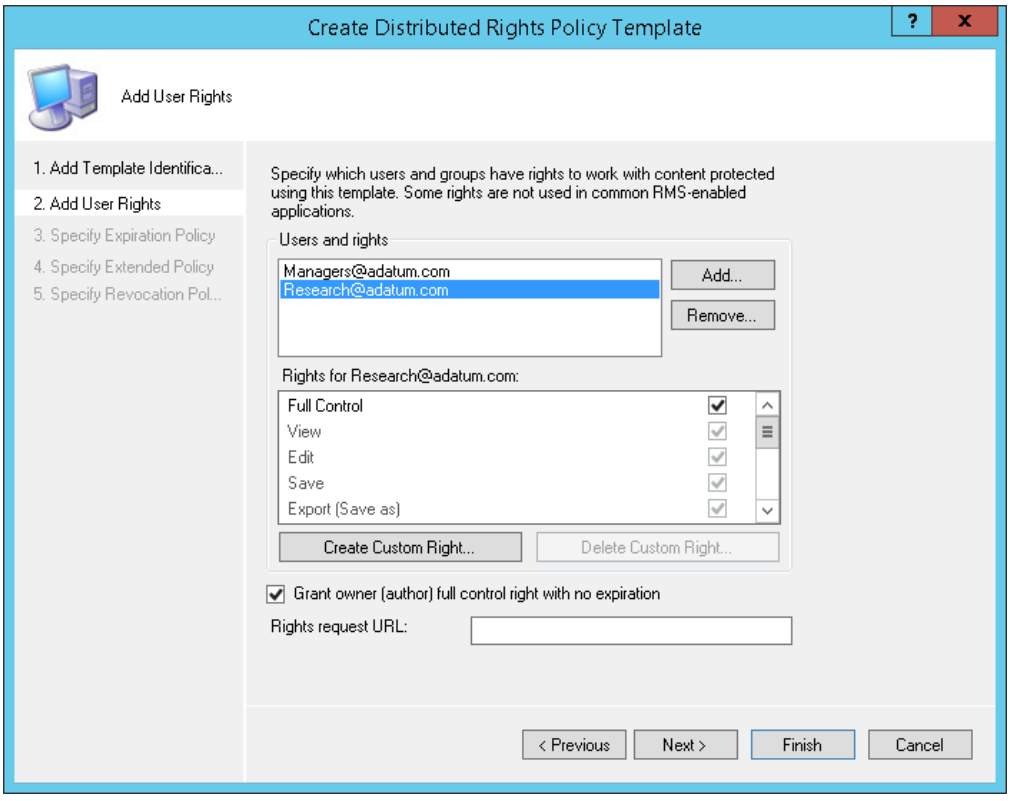

8. Cửa sổ **Add User Rights,** đánh dấu chọn ô **View**, và chọn **Add.**



9. Hộp thoại **Add User or Group**, chọn **The e-mail address of a user or group**, nhập **research@adatum.com**, và chọn **OK**.




10. Cửa sổ **Add User Rights,** chọn **research@adatum.com,** đánh dấu chọn **Full Control,** và chọn **Finish**.



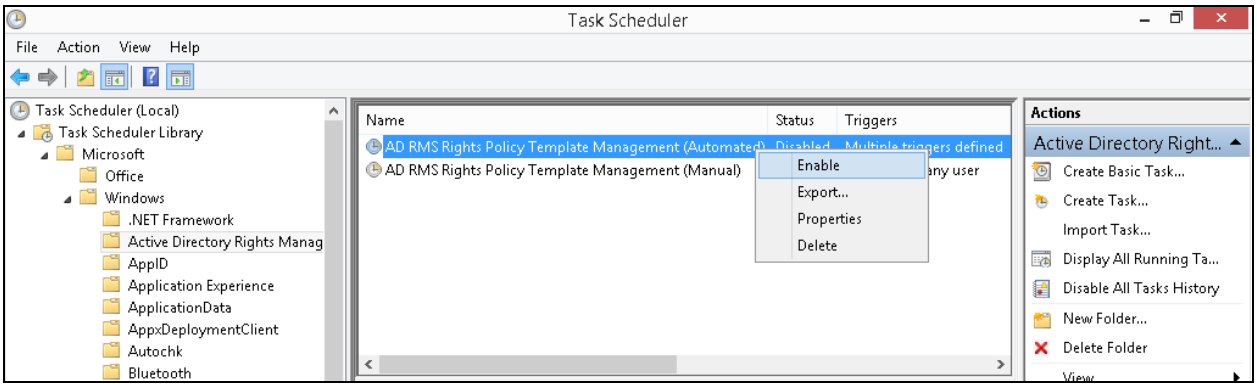
➢ **Bật Automated Scheduled Task**

1. Sign in vào máy **LON-CL1** bằng **Adatum\Administrator** với password **Pa$$w0rd**.

2. Trong giao diện **Start**, gõ **Schedule tasks**, chọn biểu tượng **Schedule tasks**.



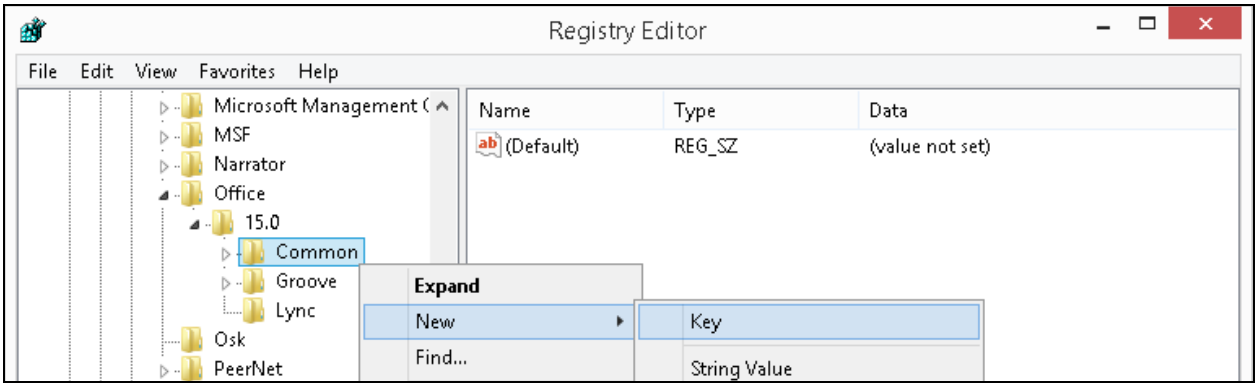

3. Trong cửa sổ T**asks Schedule,** bung **Task Scheduler Library**, bung **Microsoft**, bung **Windows**, chọn **Active Directory Rights Management Services Client**. Chuột phải **AD RMS Rights Policy Template Management (Automated)**, chọn **Enable**.



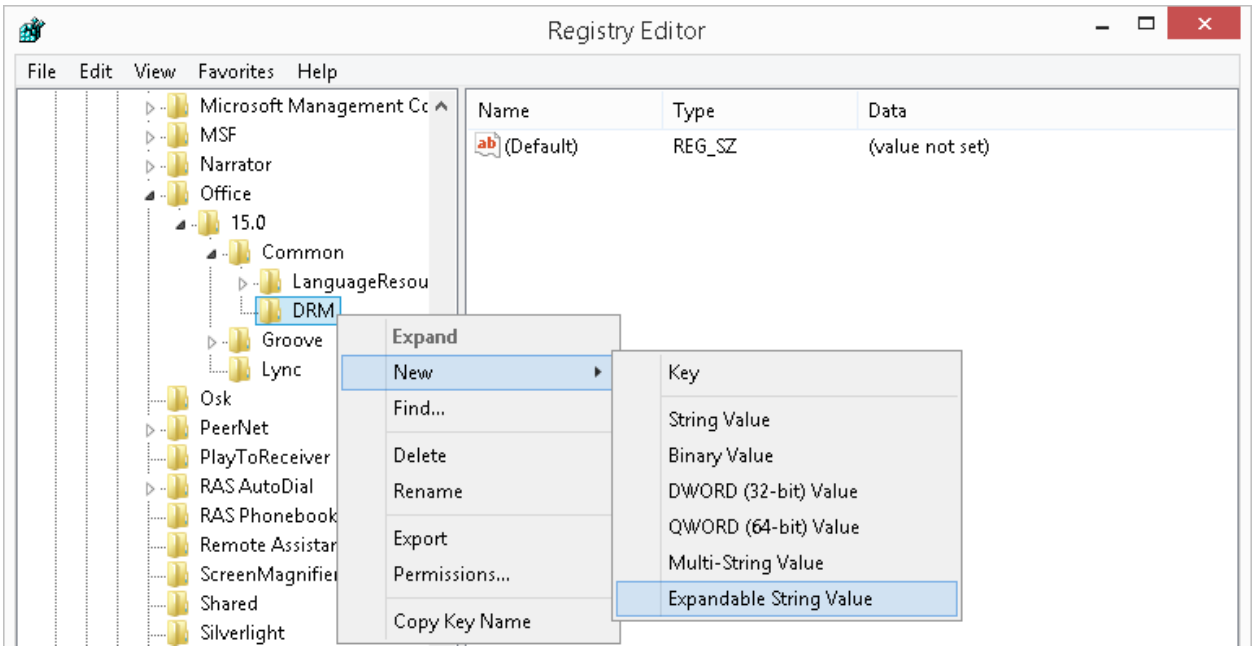

4. Tắt cửa sổ **Task Scheduler**.

5. Chuột phải **Start** menu, chọn **Run**, gõ **regedit.exe**, chọn **OK**.

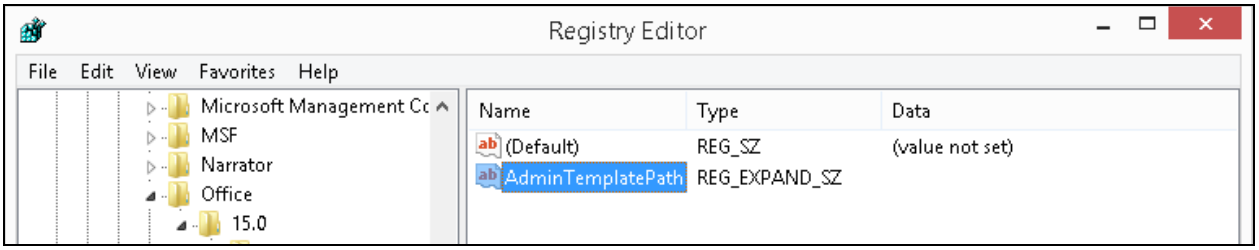
6. Trong cửa sổ Registry Editor, vào đường dẫn: **HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Common\.** Chuột phải **Common,** bung **New**, chọn **Key**.



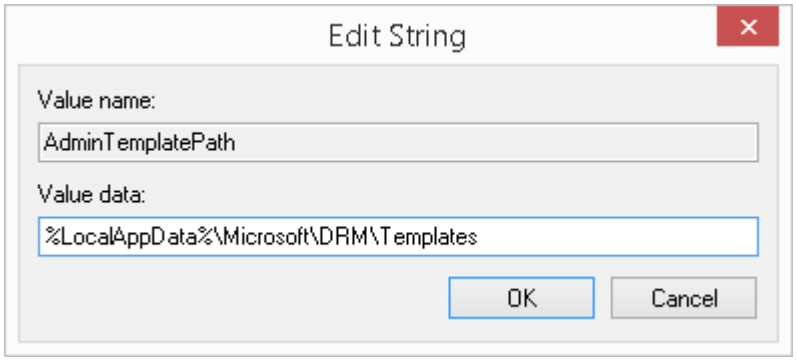

7. Đặt tên cho key mới là **DRM**, chuột phải **DRM**, bung **New**, chọn **Expandable String Value**.



8. Đặt tên cho Expandable String Value là **AdminTemplatePath**. Nhấp đôi chuột mở **AdminTemplatePath.**

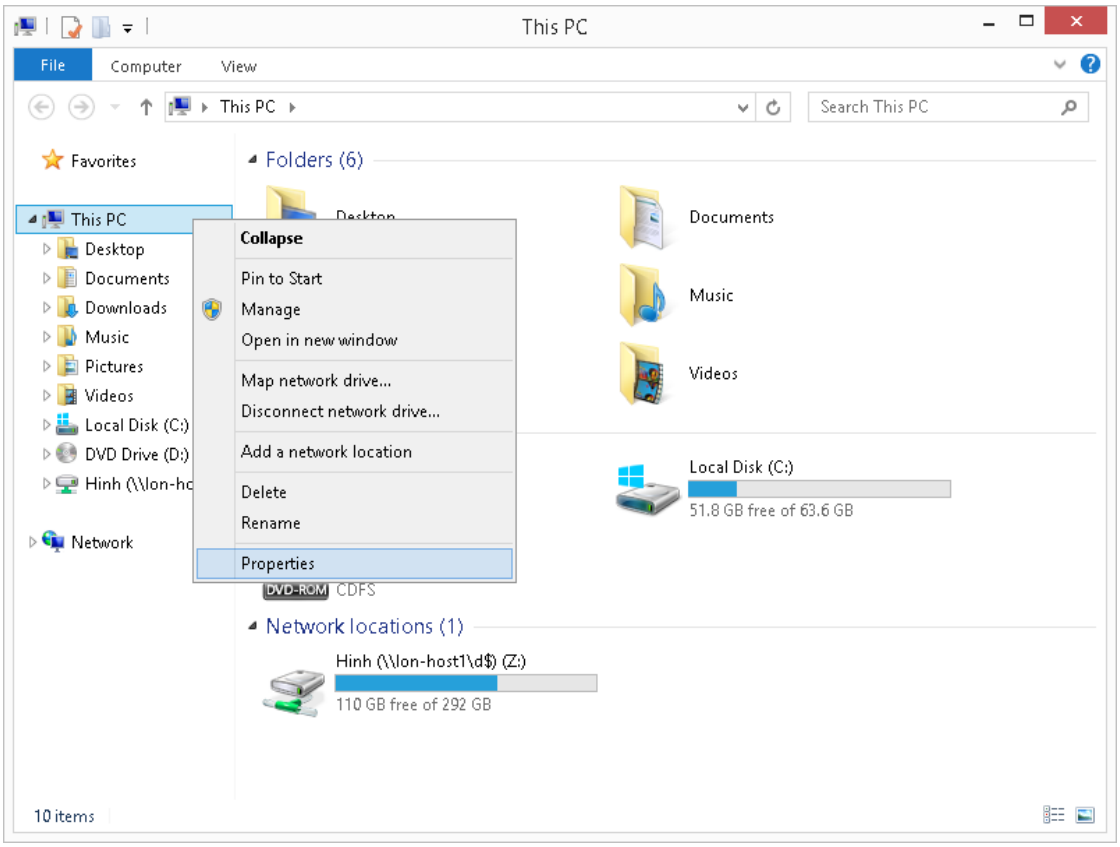



9. Hộp thoại **Edit String**, trong ô **Value data**, nhập **%LocalAppData%\Microsoft\DRM\Templates**, và chọn **OK**.

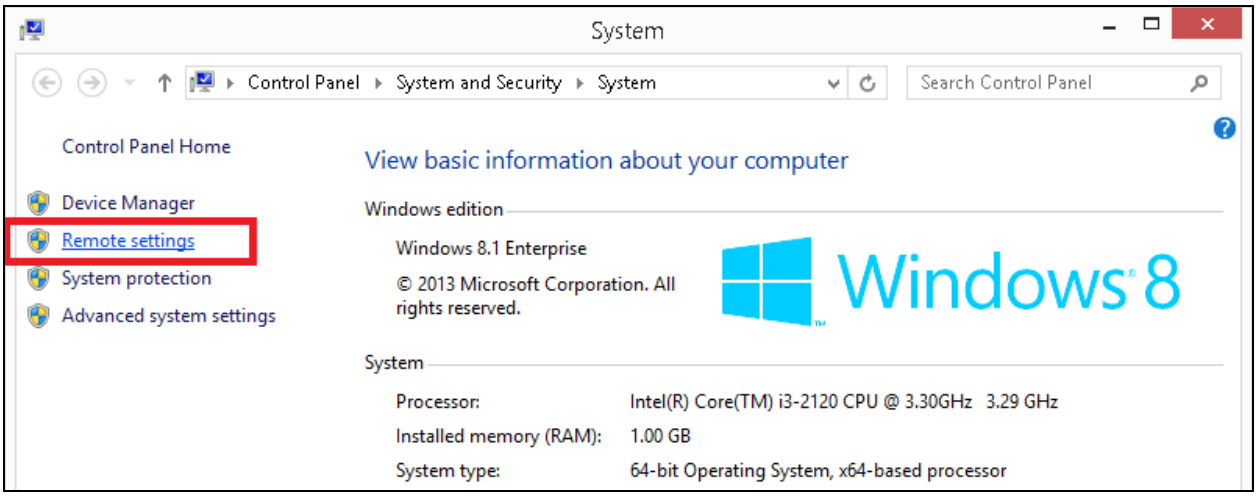



10. Tắt cửa sổ **Registry Editor**.

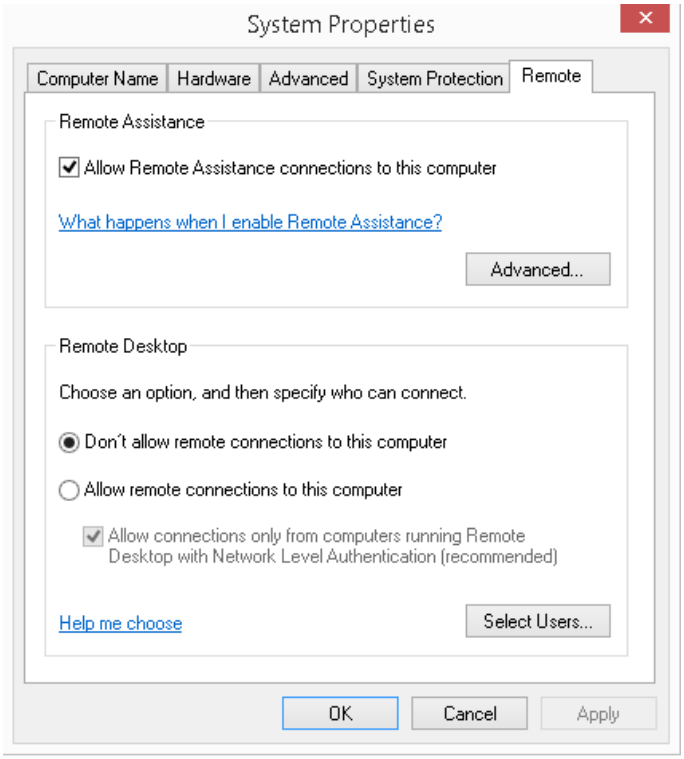
11. Mở **File Explorer**, chuột phải **This PC**, chọn **Properties.**



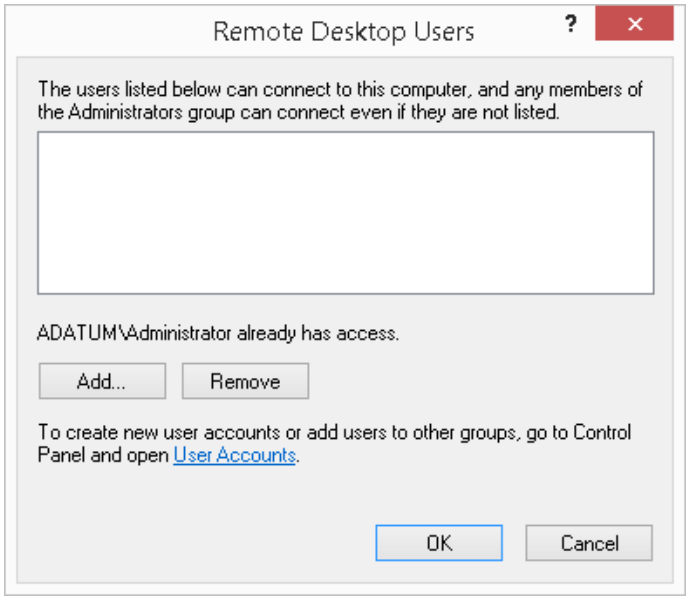

12. Cửa sổ **System**, chọn **Remote settings**.



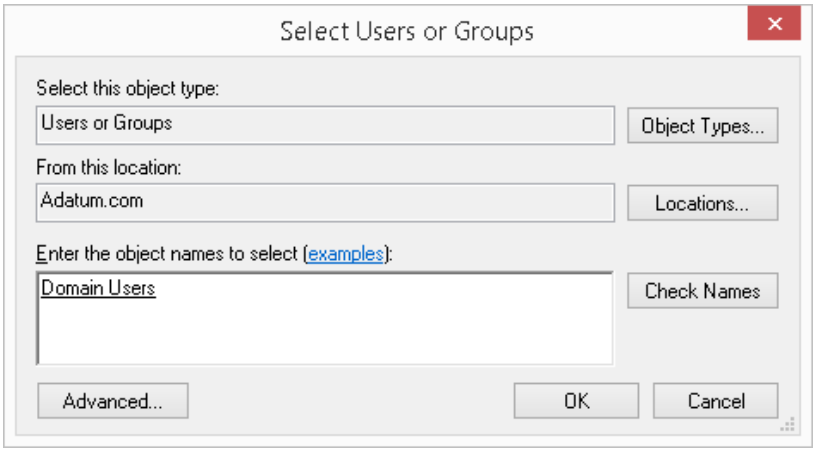
13. Cửa sổ **System Properties**, chọn **Select Users**.




14. Hộp thoại **Remote Desktop Users**, chọn **Add**.



15. Hộp thoại **Select Users or Groups**, trong ô **Enter the object names to select**, nhập **Domain Users**, và chọn **OK** 3 lần.



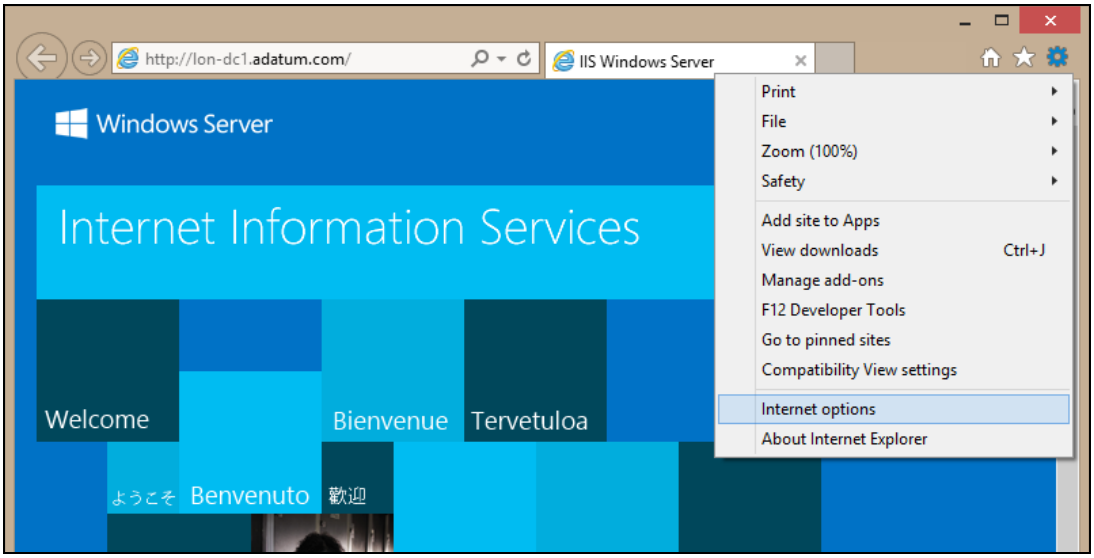

16. Sign out máy **LON-CL1**.

## Bước 5: Cấu hình AD RMS Exclusion Policies.

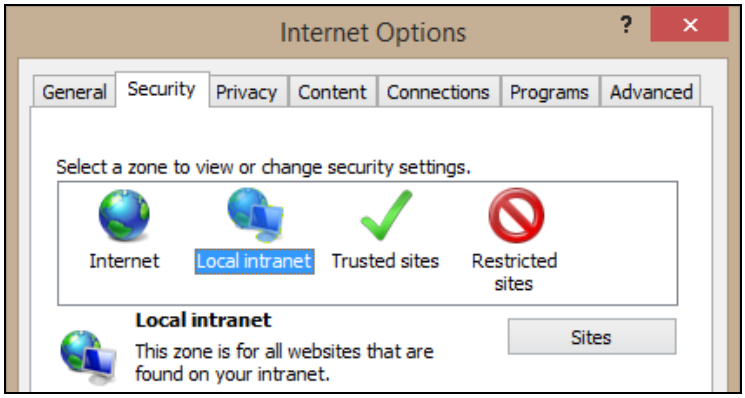
➢ **Tạo Rights Account Certificates (RAC) cho user Toni Poe**

1. Trên máy **LON-CL1**, sign in bằng **Adatum\Toni** với password **Pa$$w0rd**.

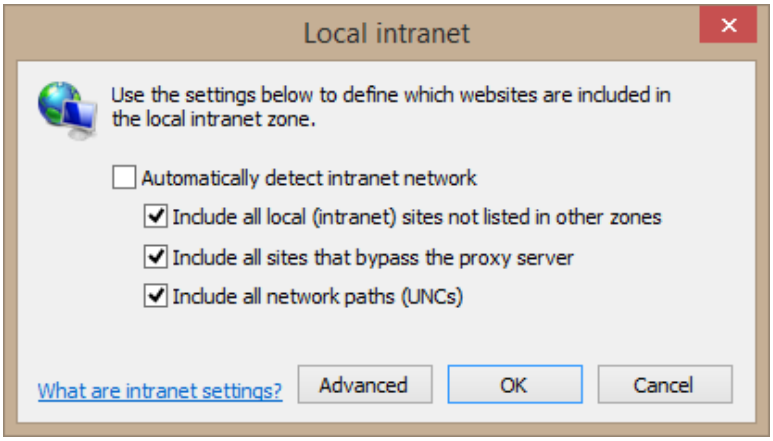
2. Mở **Internet Explorer**, truy cập **http://lon-dc1.adatum.com**. Bung biểu tượng **Tools**, chọn **Internet options**.



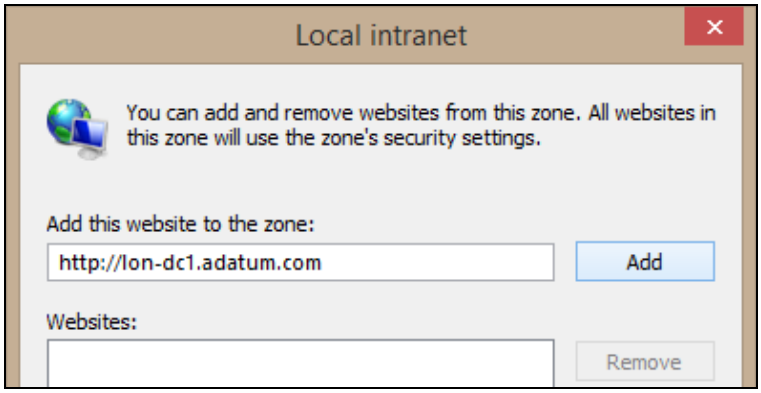
3. Cửa sổ **Internet options**, qua tab **Security**, chọn **Local intranet**, chọn **Sites**.




4. Hộp thoại **Local intranet**, chọn **Advanced**

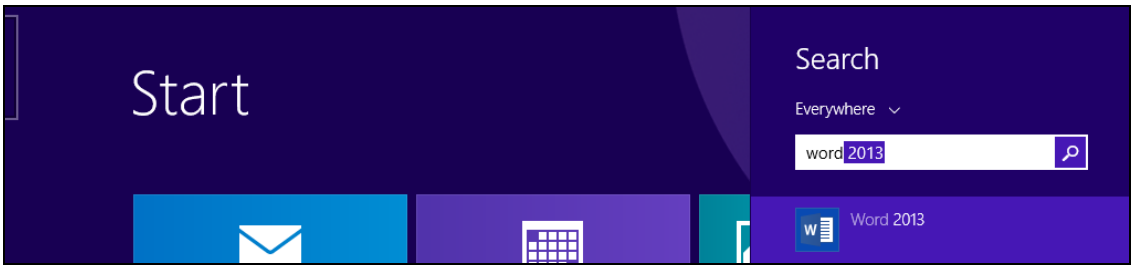



5. Trong ô **Add this website to the zone**, nhập **http://LON-DC1.adatum.com**, chọn **Add**, chọn **Close**, và chọn **OK** 2 lần.

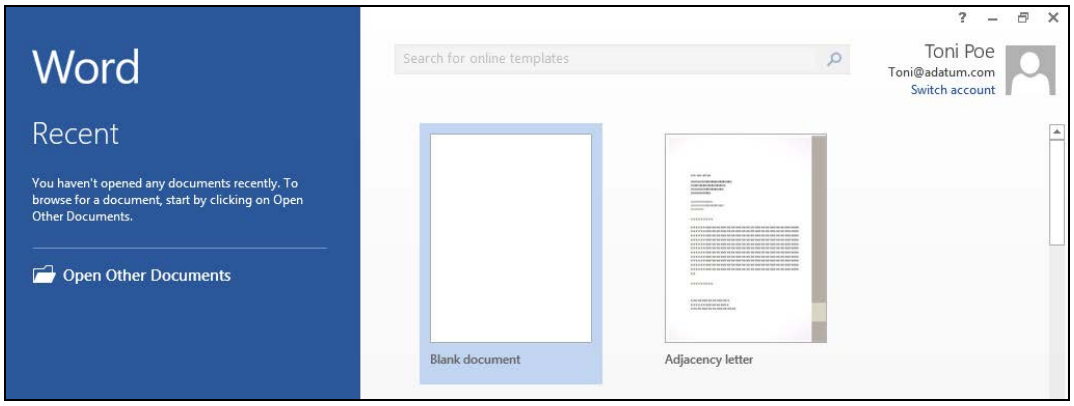


6. Tắt cửa sổ **Internet Explorer**.

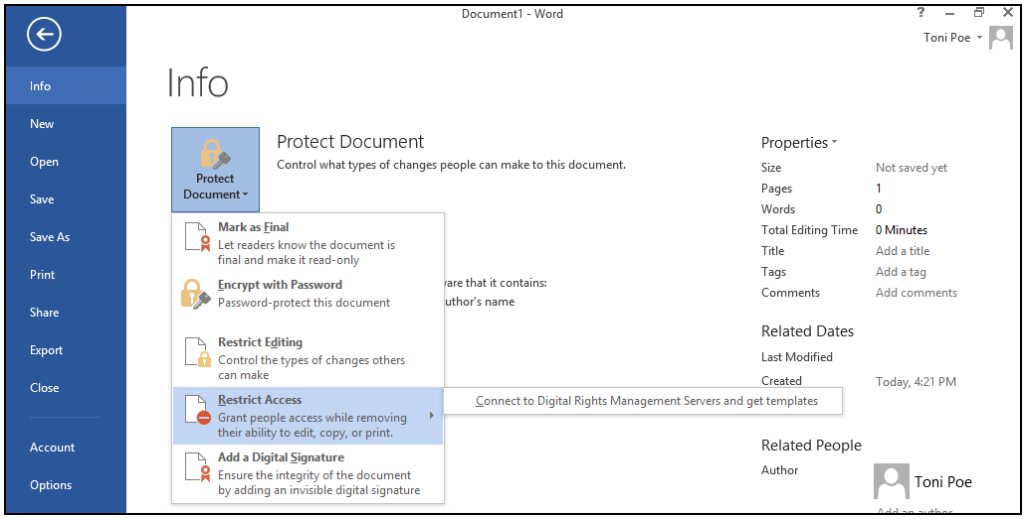
7. Bung **Start** menu, gõ **Word**, chọn **Word 2013**.



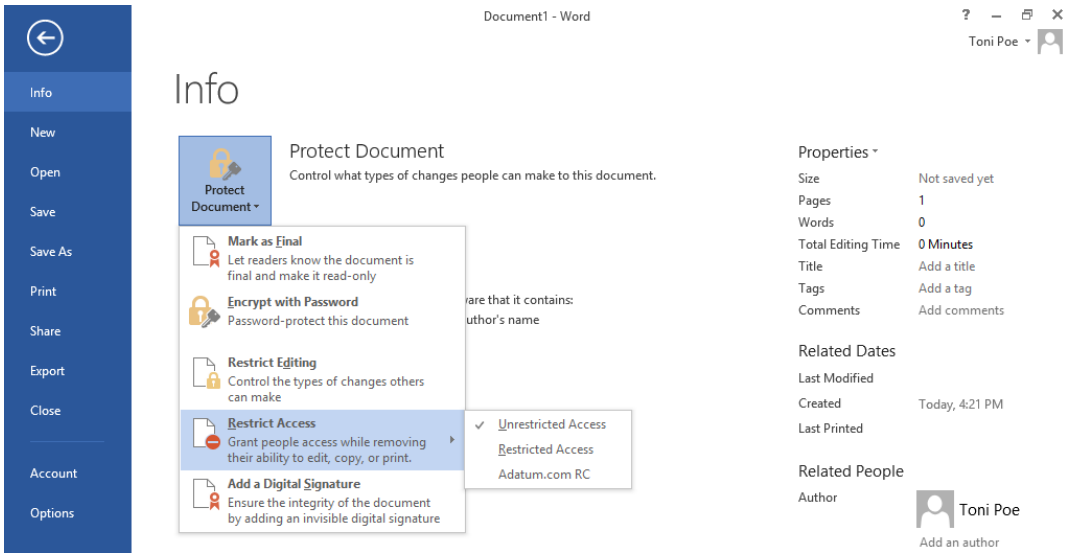

8. Tắt tất cả cửa sổ welcome của Office, trong cửa sổ Word, chọn **Blank document**.



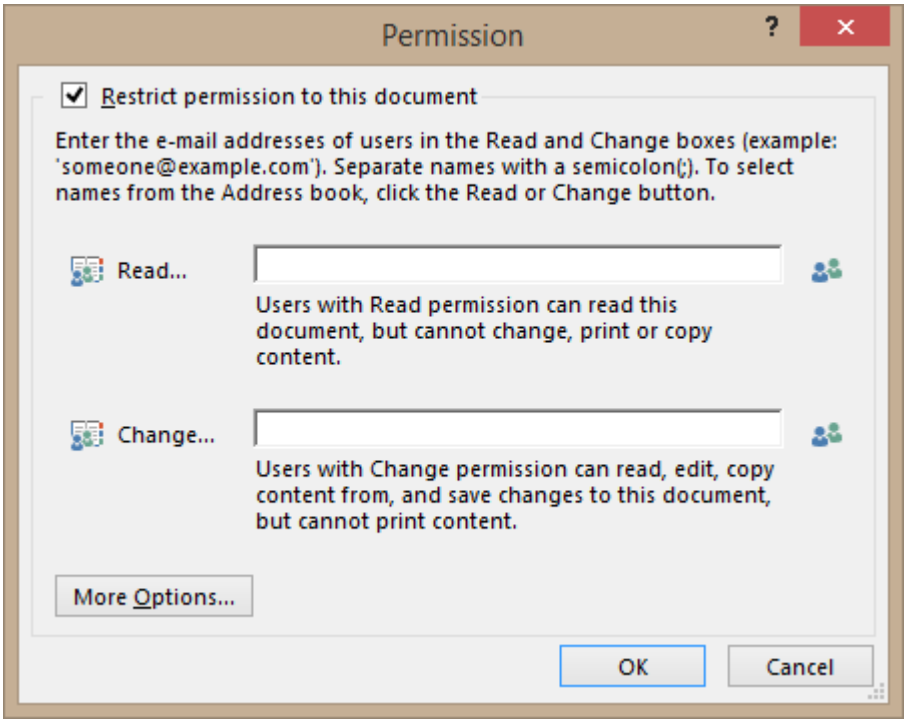

9. Trong cửa sổ Word, vào tab **File**, trong **Info**, chọn **Protect Document**, chọn **Restrict Access,** và chọn **Connect to Digital Rights Management Servers and get templates.**



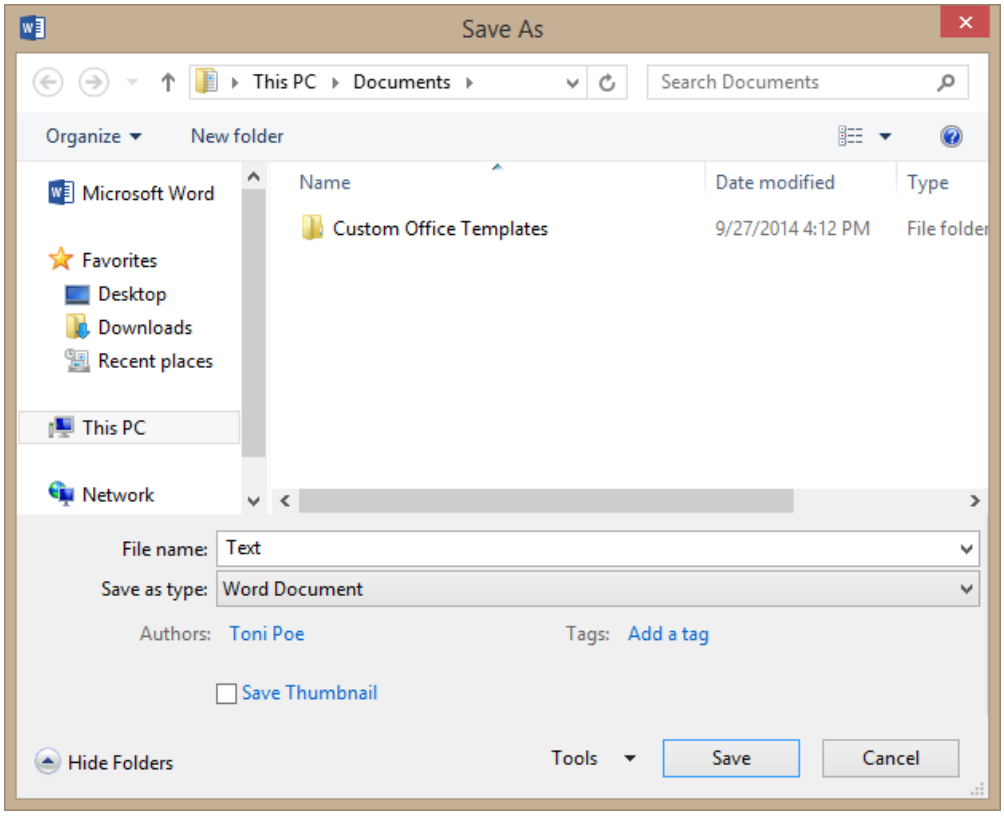
10. Chọn **Protect Document**, chọn **Restrict Access,** và chọn **Restricted Access.**




11. Hộp thoại **Permission**, đánh dấu chọn **Restrict permission to this document**, và chọn **OK**.

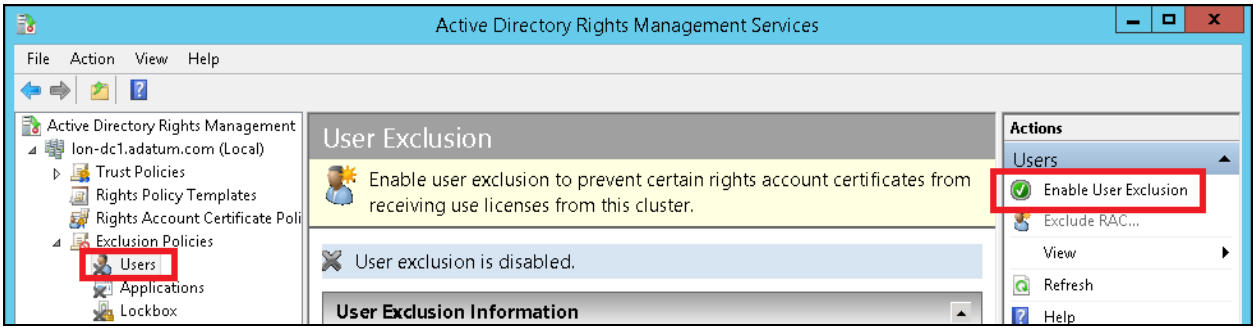


12. Save file word vào **Documents**, đặt tên là **Text.docx.** Tắt tất cả cửa sổ, và sign out máy **LON-CL1**.

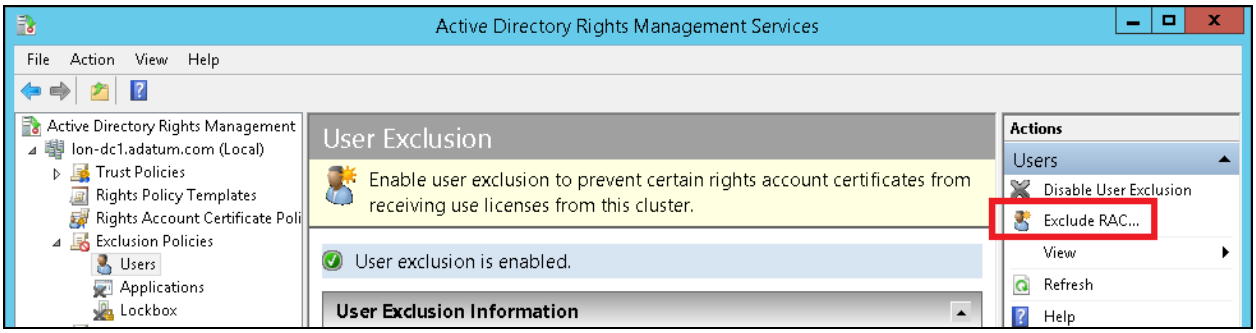



➢ **Loại trừ Rights Account Certificates (RAC)**

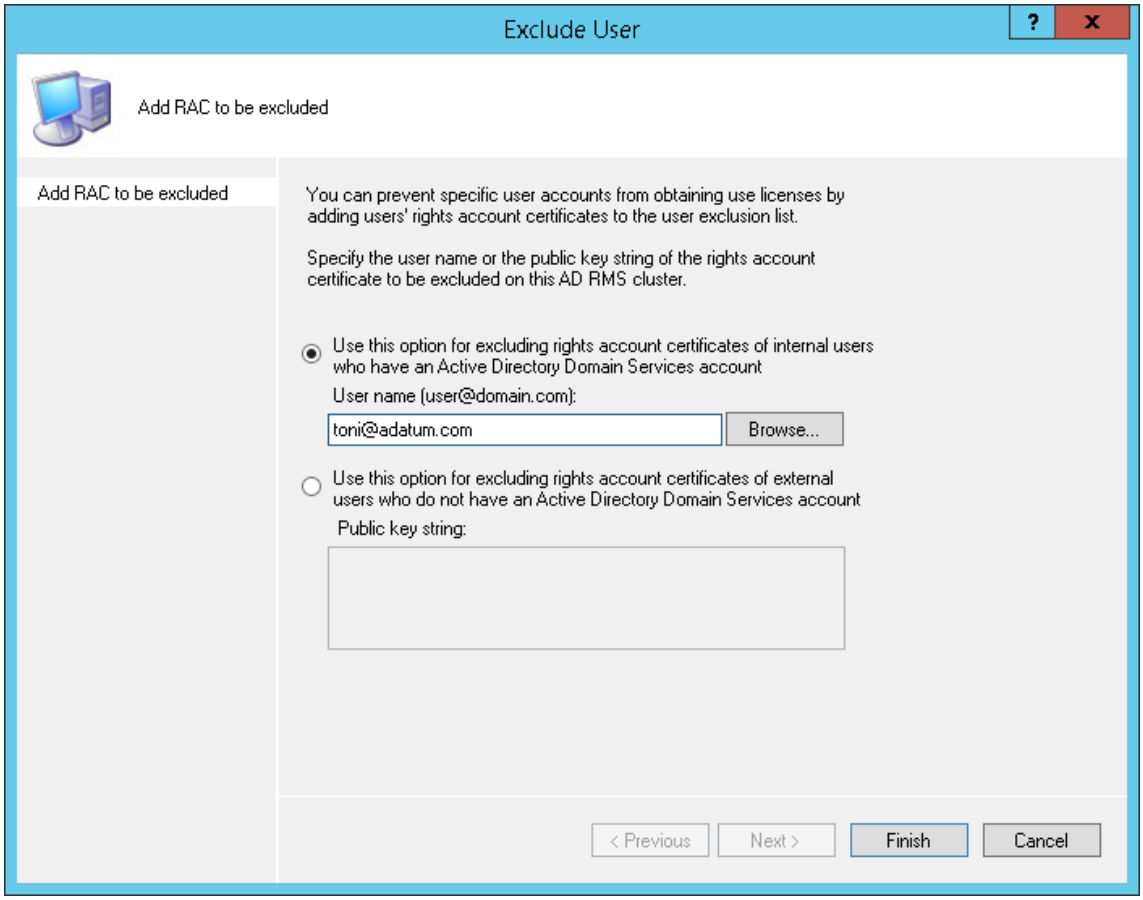
1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Active Directory Rights Management Services**. Bung **lon-dc1.adatum.com**, bung **Exclusion policies**, chọn **Users**, chọn **Enable User Exclusion**.



2. Trong cửa sổ **Actions**, chọn **Exclude RAC**.




3. Cửa sổ **Add RAC to be excluded**, chọn **Use this option for excluding rights accounts certificates of internal users who have an Active Directory Domain Services account**, nhập **toni@adatum.com**, chọn **Finish**.



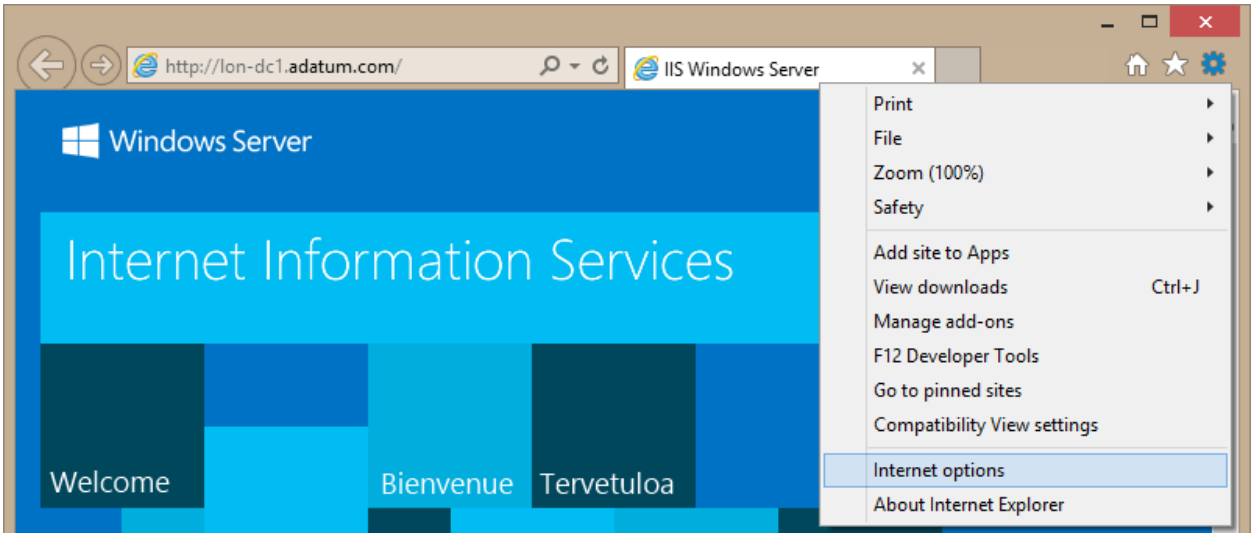
**Bước 6: Kiểm tra kết quả.**

➢ **Add AD RMS cluster vào Local Intranet security zone**

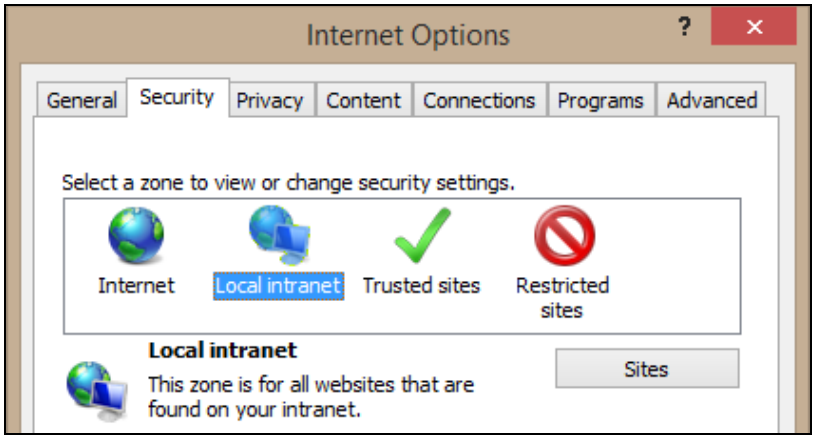
1. Sign in vào máy **LON-CL1** bằng **Adatum\Hani** với password **Pa$$w0rd**.



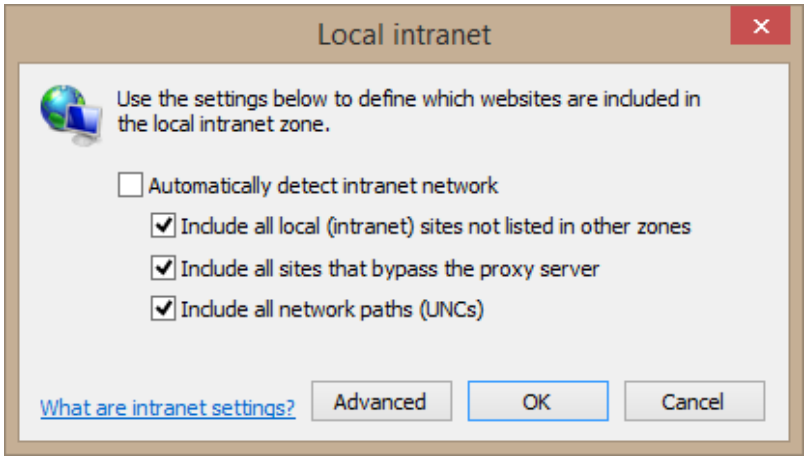

2. Mở **Internet Explorer**, bung biểu tượng **Tools**, chọn **Internet options**.



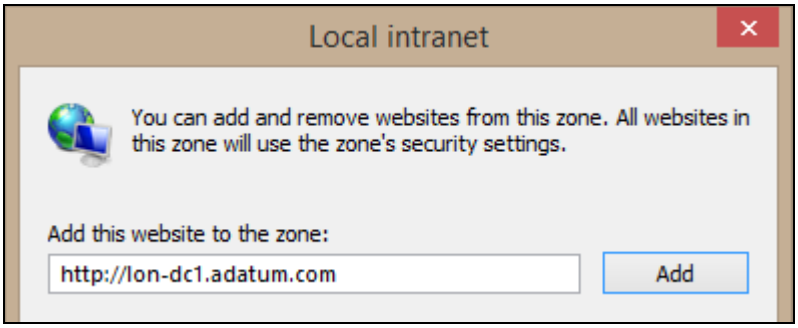
3. Cửa sổ **Internet options**, qua tab **Security**, chọn **Local intranet**, chọn **Sites**.




4. Hộp thoại **Local intranet**, chọn **Advanced**




5. Trong ô **Add this website to the zone**, nhập **http://LON-DC1.adatum.com**, chọn **Add**, chọn **Close**, và chọn **OK** 2 lần.



6. Tắt cửa sổ **Internet Explorer**.

7. Sign out máy **LON-CL1**.

8. Lặp lại từ bước 1 tới 7 cho user **Adatum\Limor**.

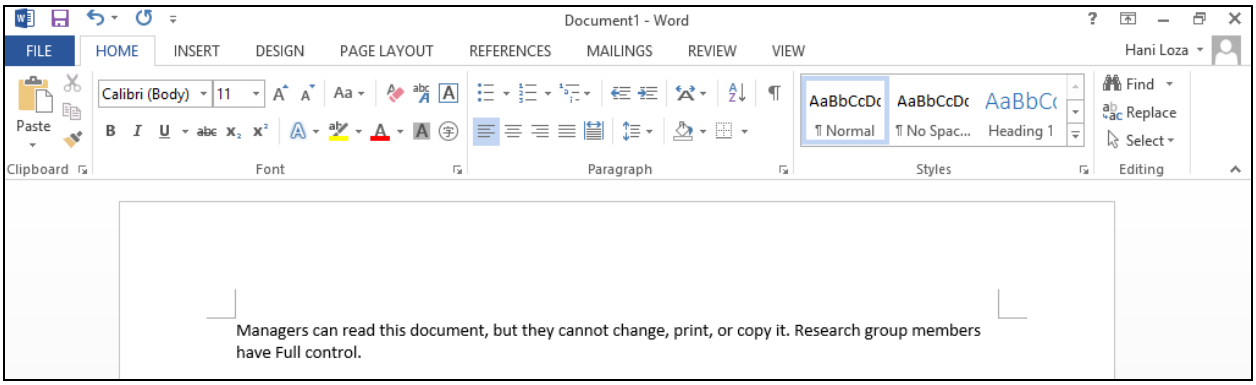
➢ **Gán quyền RMS trên tài liệu Microsoft Word.**

1. Sign in vào máy **LON-CL1** bằng **Adatum\Hani** với a password of **Pa$$w0rd**.

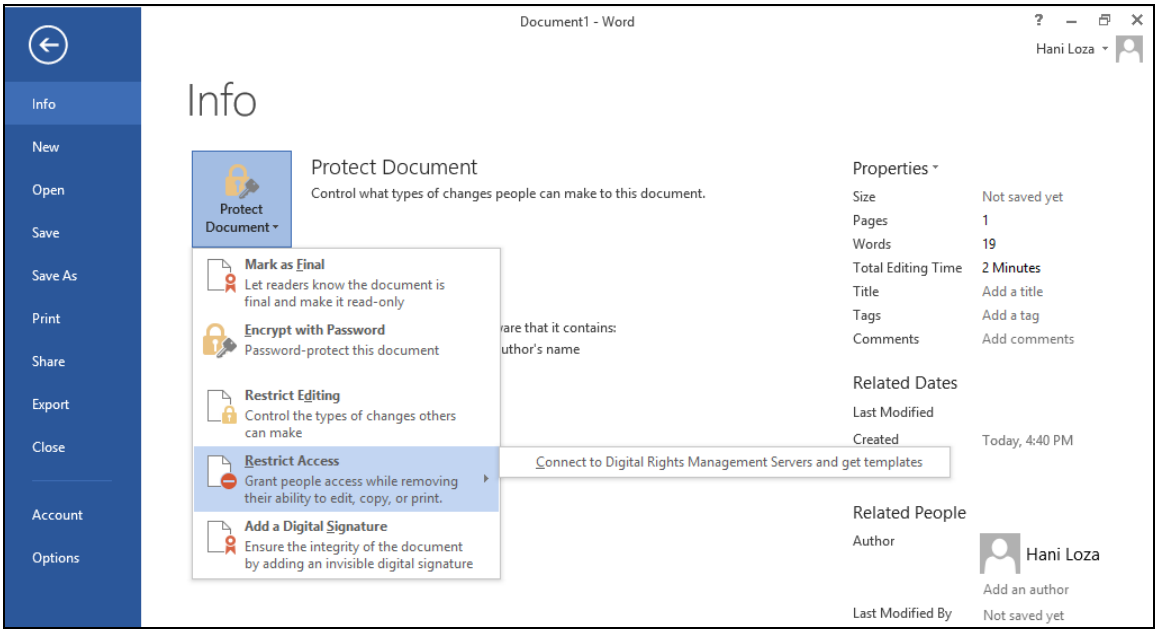
2. Trong giao diện **Start**, gõ **Word**, và mở **Word 2013**. (Tắt tất cả cửa sổ Welcome của Microsoft Office nếu có)



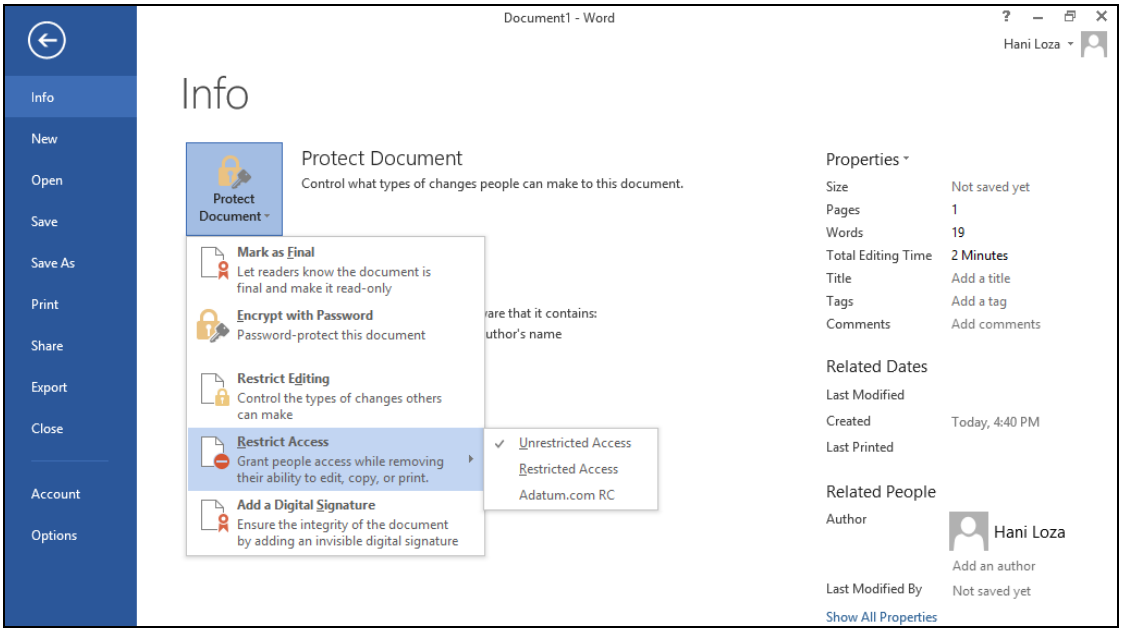

3. Trong cửa sổ **Word**, chọn **Blank document**. Nhập nội dung **Managers can read this document, but they cannot change, print, or copy it. Research group members have Full control**.



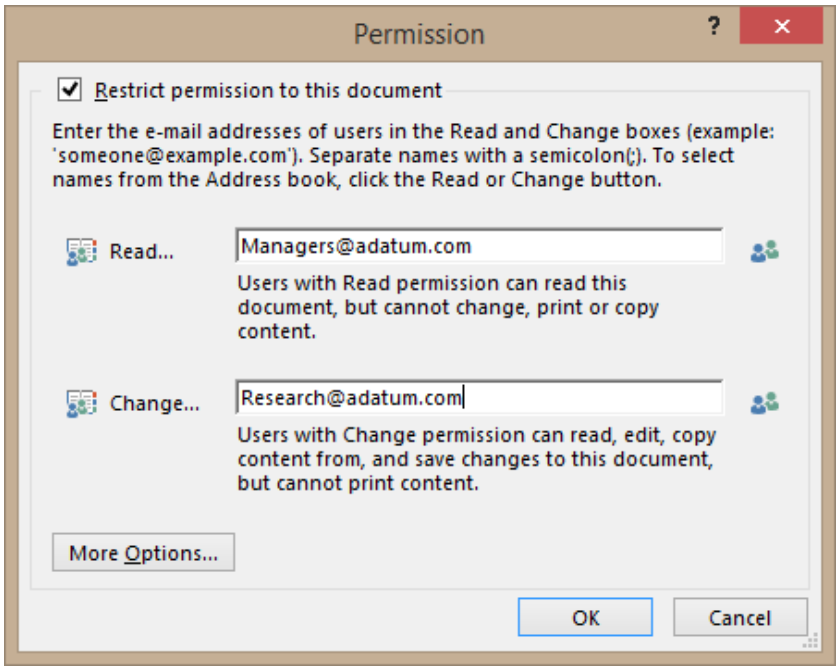
4. Trong cửa sổ **Word** , chọn tab **File**, trong trang **Info**, chọn **Protect Document**, chọn **Restrict Access**, và chọn **Connect to Digital Rights Management Servers**.



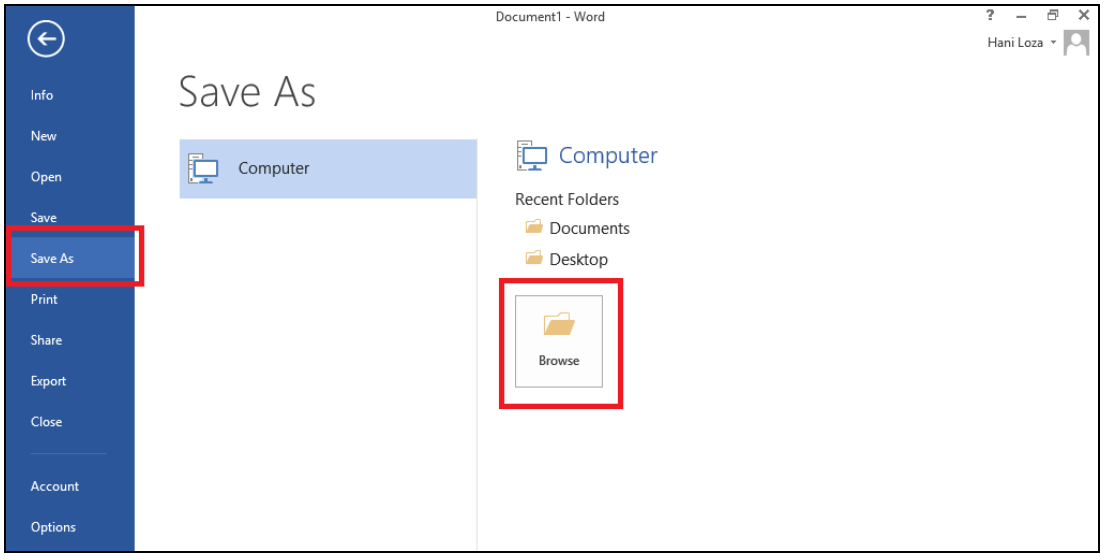

5. Trong trang **Info**, chọn **Protect Document**, chọn **Restrict Access**, và chọn **Restricted Access.**



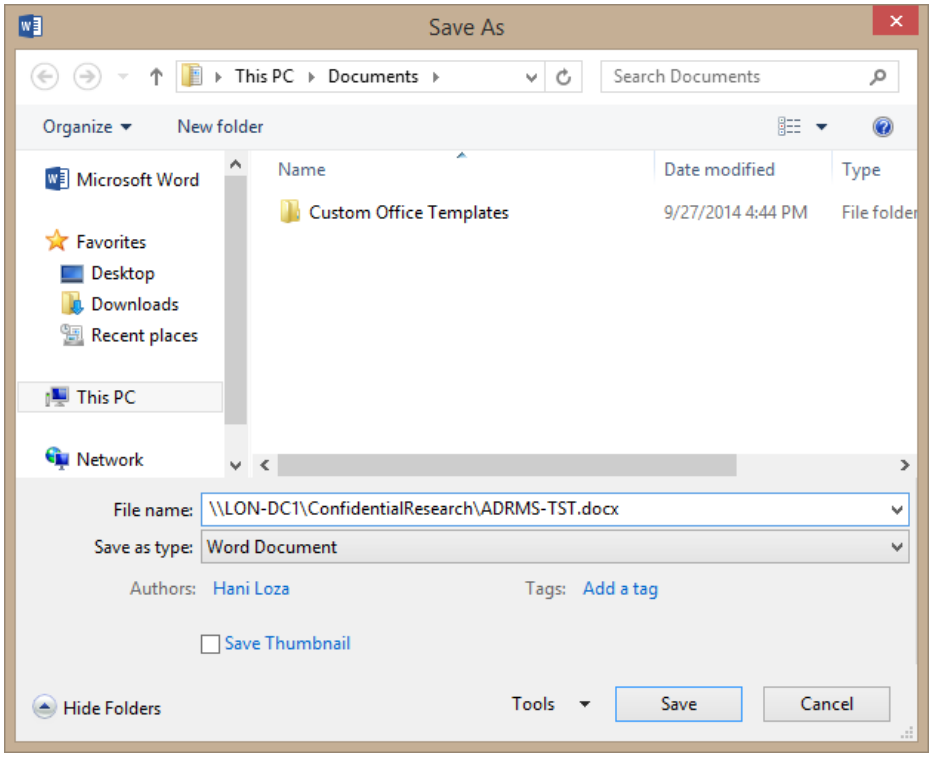
6. Hộp thoại **Permissions**, đánh dấu chọn **Restrict permission to this document**, trong ô **Read**, nhập **Managers@adatum.com**, trong ô **Change**, nhập **research@adatum.com**, chọn **OK.**




7. Trong menu **File**, chọn **Save As**, và chọn **Browse**.



8. Hộp thoại **Save As**, trong ô **File name**, nhập **\\LON-DC1\ConfidentialResearch\ADRMS-TST.docx**, và chọn **Save**.

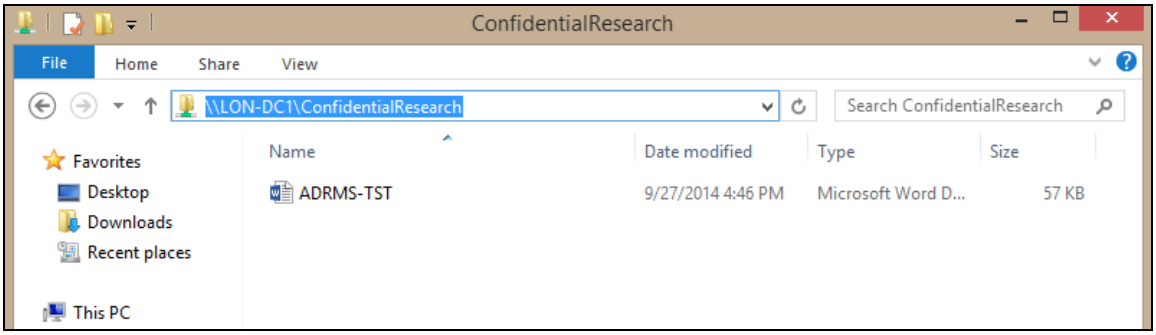



9. Tắt **Microsoft Word**, và sign out máy **LON-CL1**.

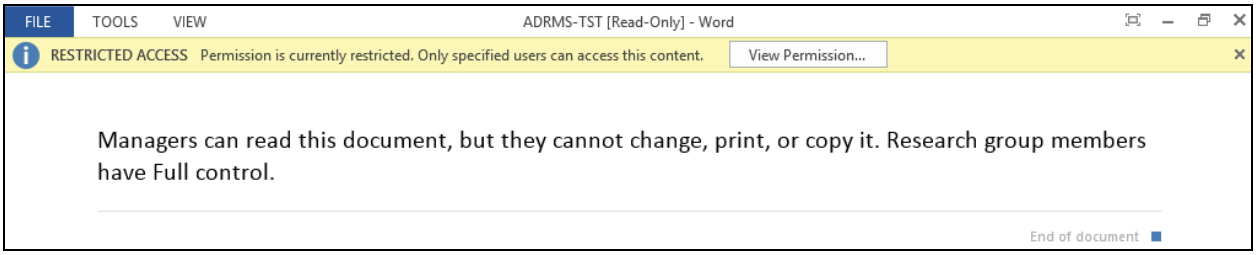
➢ **Kiểm tra quyền trên tài liệu.**

1. Sign in vào máy **LON-CL1** bằng **ADATUM\limor** với password **Pa$$w0rd**.

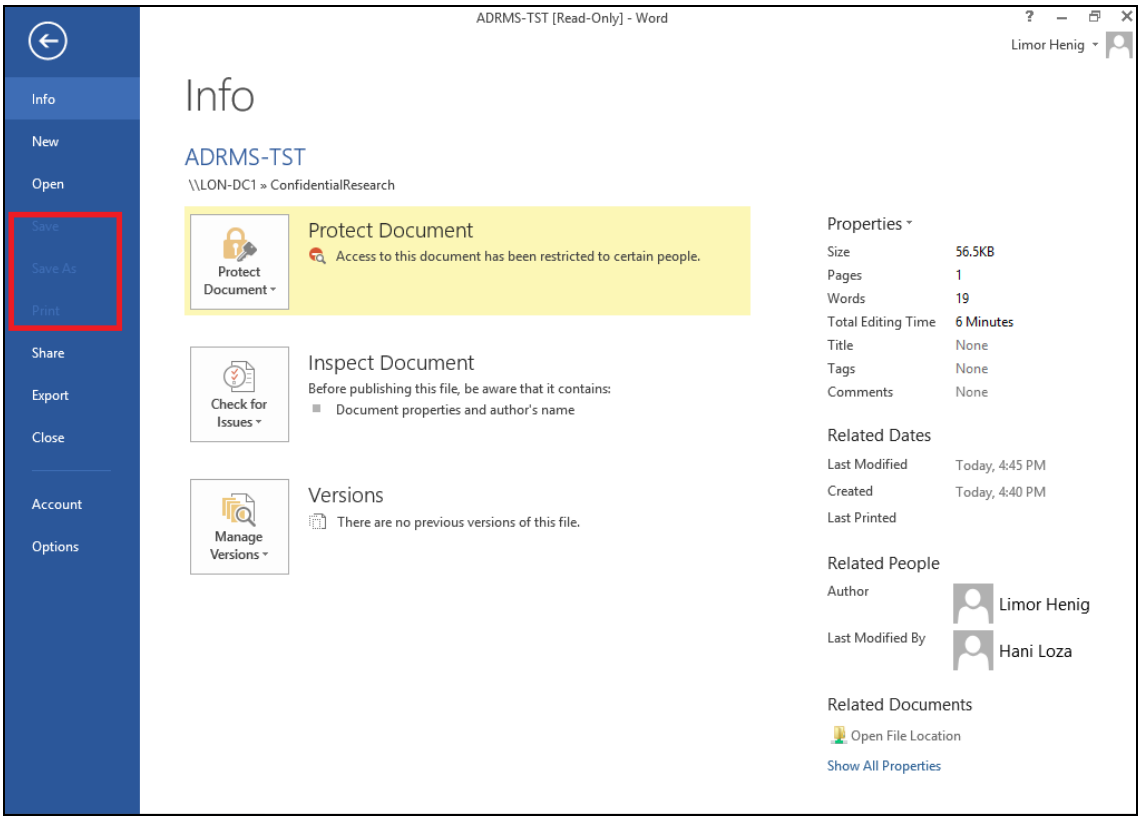
2. Mở **File Explorer**, truy cập **\\LON-DC1\ConfidentialResearch**. Mở file **ADRMS-TST.docx**. (Tắt tất cả cửa sổ Welcome của Microsoft Office nếu có)



3. Trong file Word, chú ý thanh thông báo Restricted Access màu vàng: **Permission is currently restricted. Only specified users can access this content**. Kiểm tra user **limor** không có quyền copy nội dung của tài liệu.




4. Chọn tab **File**, Kiểm tra user **limor** không có quyền **Print và Save As**.




5. Tắt **Microsoft Word** và sign out máy **LON-CL1.**

**Kết quả: Sau khi hoàn thành bài tập này, bạn đã triển khai thành công AD RMS hỗ trợ cho người dùng nội bộ bảo vệ các tài liệu quan trọng.**

## Bài tập 2: Tích hợp AD RMS với hệ thống của đối tác.

Sau khi triển khai AD RMS cho A. Datum. Công việc tiếp theo là bạn phải tích hợp AD RMS của Adatum.com và TreyResearch.net để hỗ trợ người dùng của hai hệ thống có thể truy cập tài liệu RMS lẫn nhau.

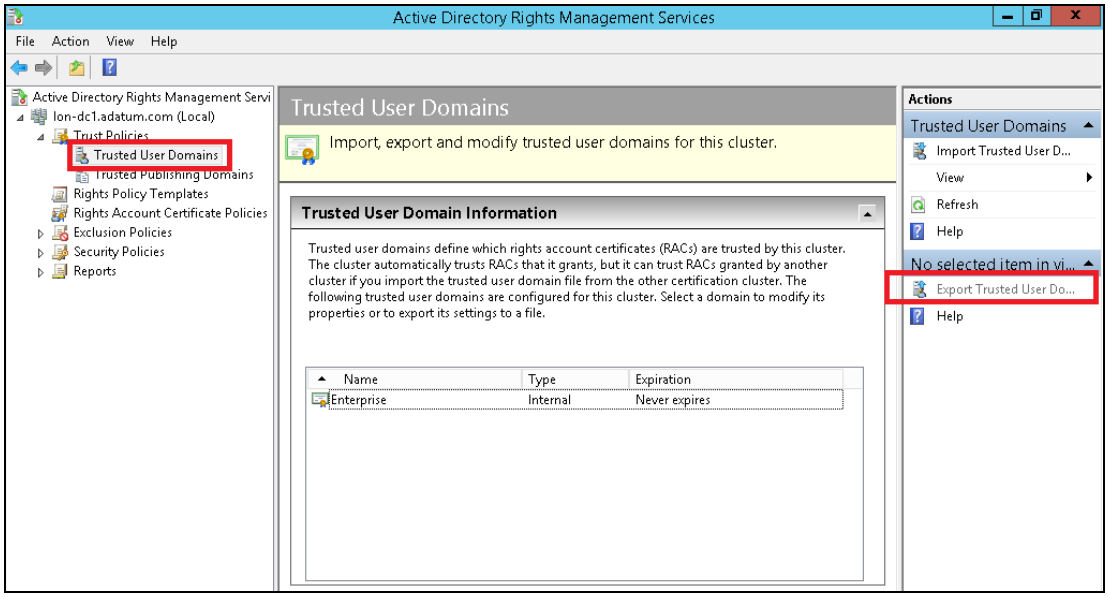
❖ **Bài thực hành bao gồm các bước:**

1. Export Trusted User Domain Policy.
2. Export Trusted Publishing Domain Policy.
3. Import Trusted User Domain Policy của domain đối tác.
4. Import Trusted Publishing Domain Policy của domain đối tác.
5. Cấu hình cho phép Anonymous truy cập AD RMS Licensing Server.
6. Kiểm tra người dùng truy cập tài liệu.

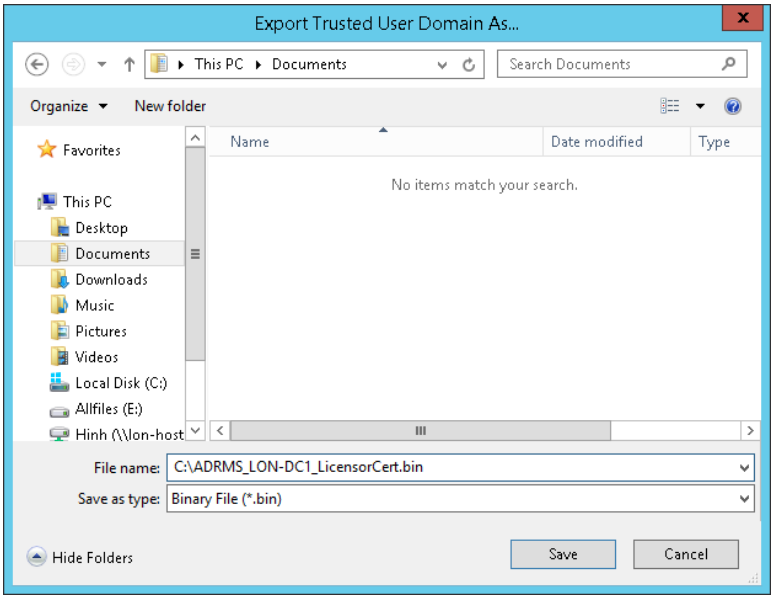
❖ **Thực hiện:**

### Bước 1: Export Trusted User Domain Policy.

1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Active Directory Rights Management Services**. Bung **lon-dc1.adatum.com**, bung **Trust Policies**, chọn **Trusted User Domains,** chọn **Enterprise**, chọn **Export Trusted User Domain**.



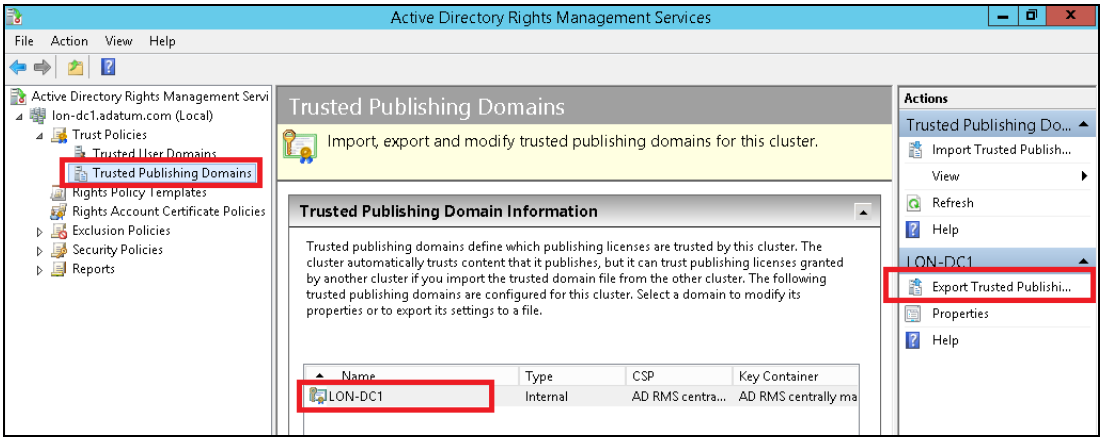
2. Hộp thoại **Export Trusted User Domain As**, trong ô **File name**, nhập **C:\ADRMS_LON-DC1_LicensorCert.bin**, chọn **Save**.



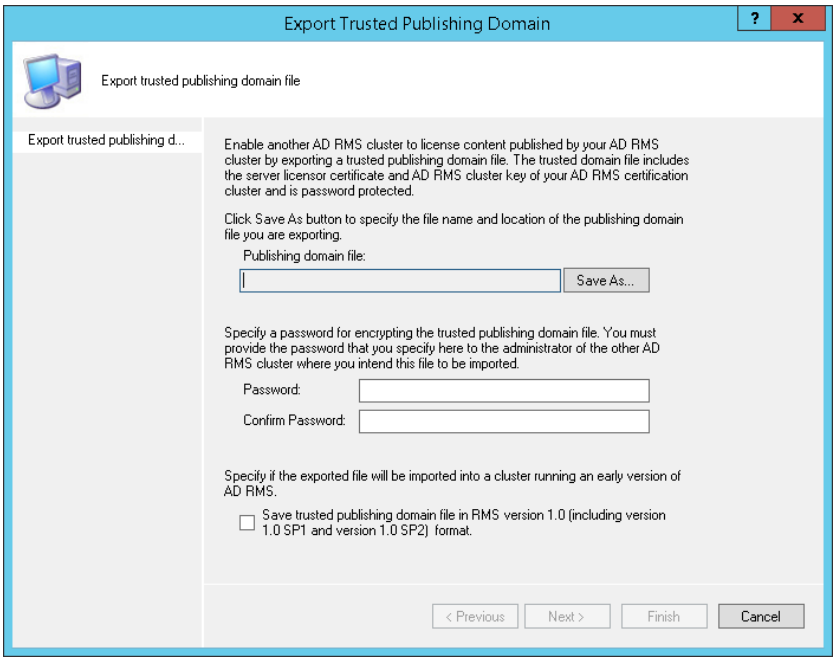

3. Qua máy **TREY-DC1**, lập lại bước 1 và 2 để export **Trusted User Domain** thành file **C:\ADRMS_TREY-DC1_LicensorCert.bin.**

## Bước 2: Export Trusted Publishing Domain Policy.

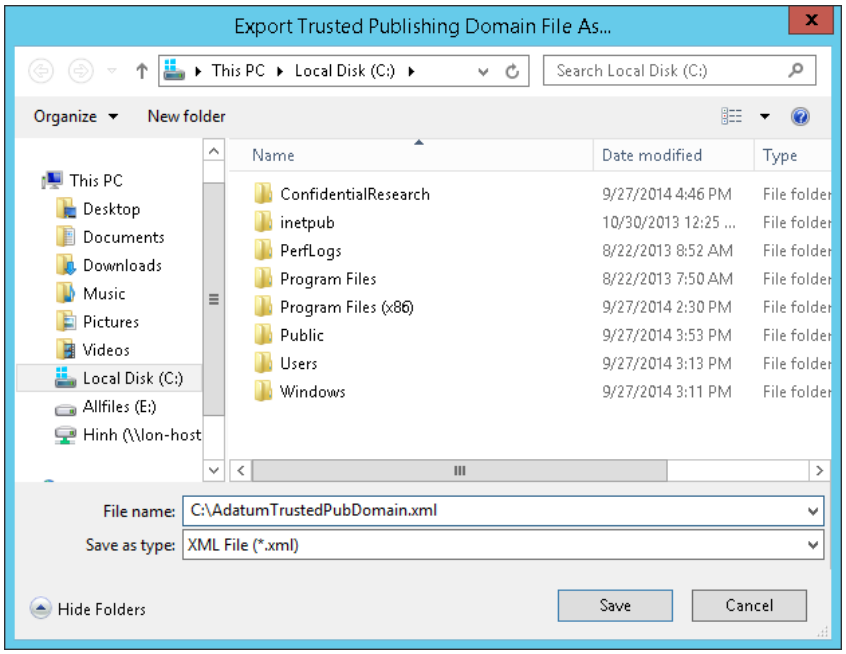
1. Qua máy **LON-DC1**, trong cửa sổ **Active Directory Rights Management Services**, bung **lon-dc1.adatum.com**, bung **Trust Policies**, chọn **Trusted Publishing Domains**, chọn **LON-DC1**, và chọn **Export Trusted Publishing Domain**.



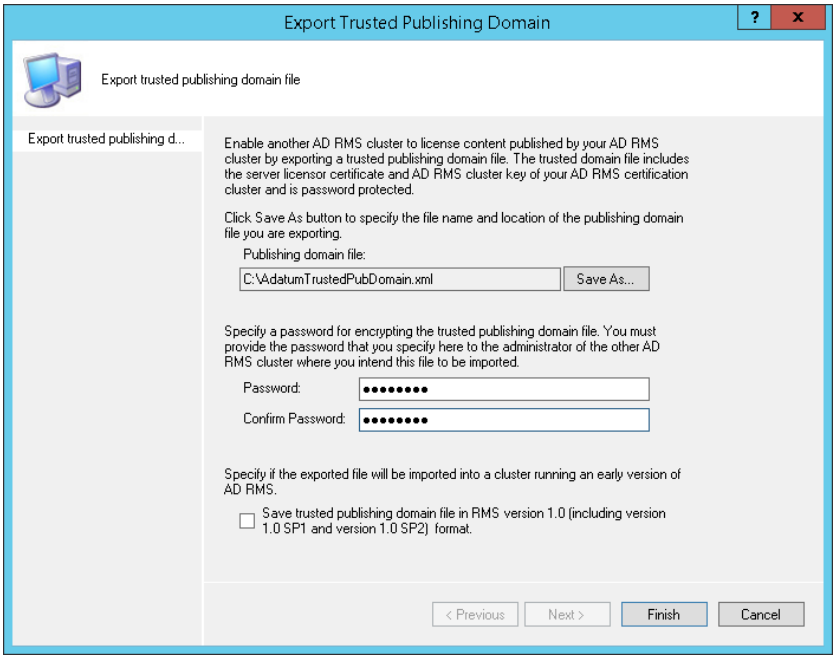
2. Hộp thoại **Export Trusted Publishing Domain**, chọn **Save As**.




3. Hộp thoại **Export Trusted Publishing Domain File As**, trong ô **File name,** nhập **C:\AdatumTrustedPubDomain.xml**, chọn **Save**.



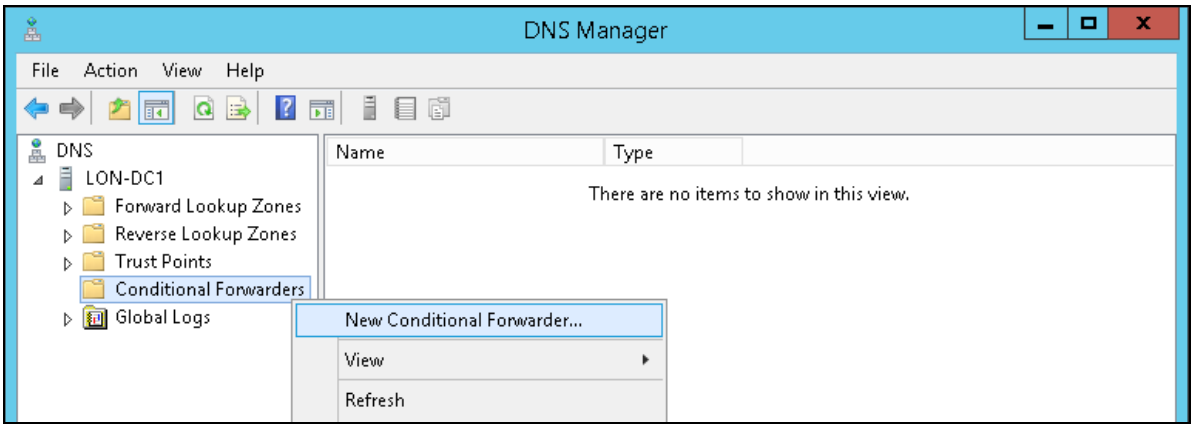
4. Hộp thoại **Export Trusted Publishing Domain**, trong ô **Password** và **Confirm password**, nhập **Pa$$w0rd**, chọn **Finish**.




5. Qua máy **TREY-DC1**, lập lại từ bước 1 đến 4 để export **Trusted Publishing Domain** thành file **C:\TreyTrustedPubDomain.xml** với password là **Pa$$word**.

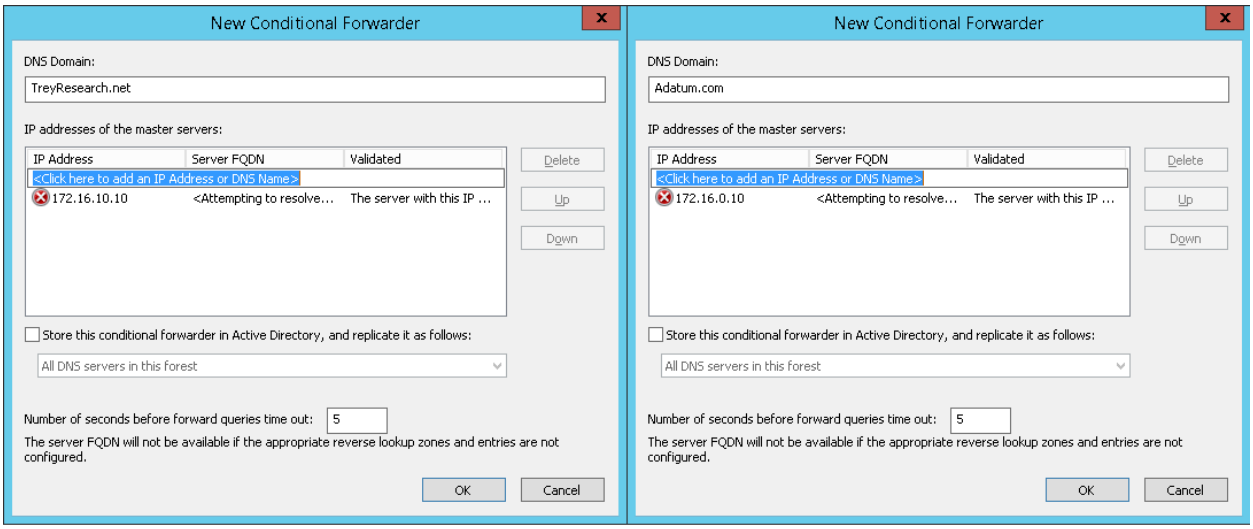
**Bước 3: Import Trusted User Domain Policy của domain đối tác.**

1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **DNS**, bung **LON-DC1**, chọn và chuột phải **Conditional Forwarders**, chọn **New Conditional Forwarder**.

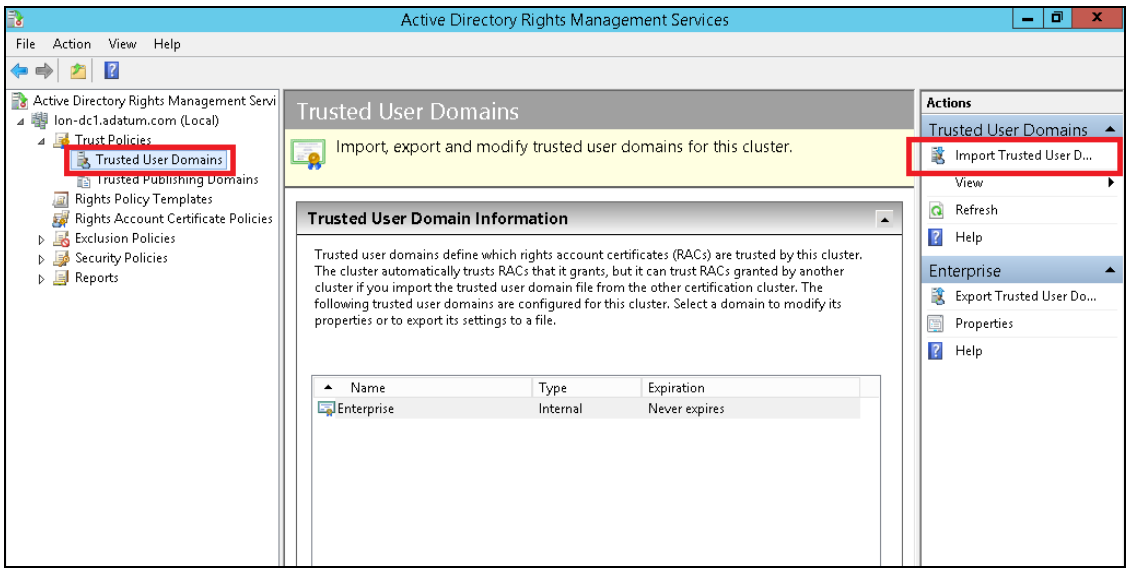


2. Hộp thoại **New Conditional Forwarder**, trong ô **DNS Domain**, nhập **TreyResearch.net**, trong ô **IP addresses of the master servers**, nhập **172.16.10.10**, nhấn **Enter**, chọn **OK**.

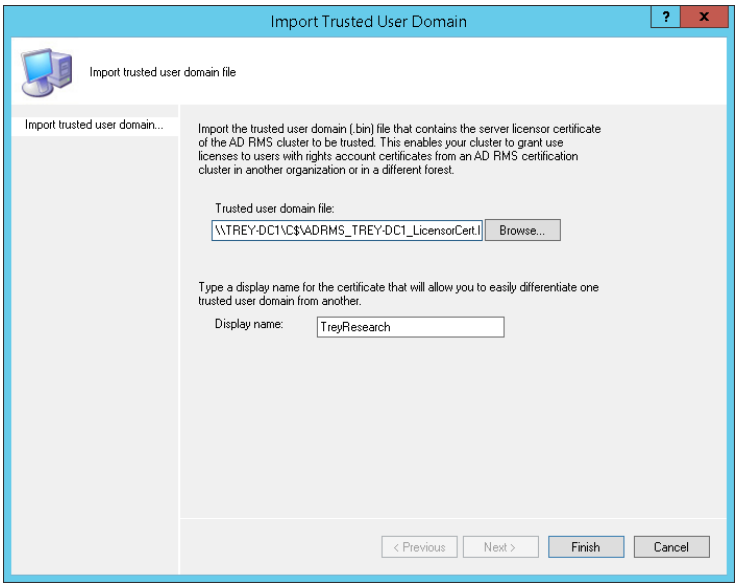
3. Qua máy **TREY-DC1**, Lặp lại bước 1 và 2 để cấu hình **Conditional Forwarder** với domain **Adatum.com** có **IP Address of the master servers** là **172.16.0.1**



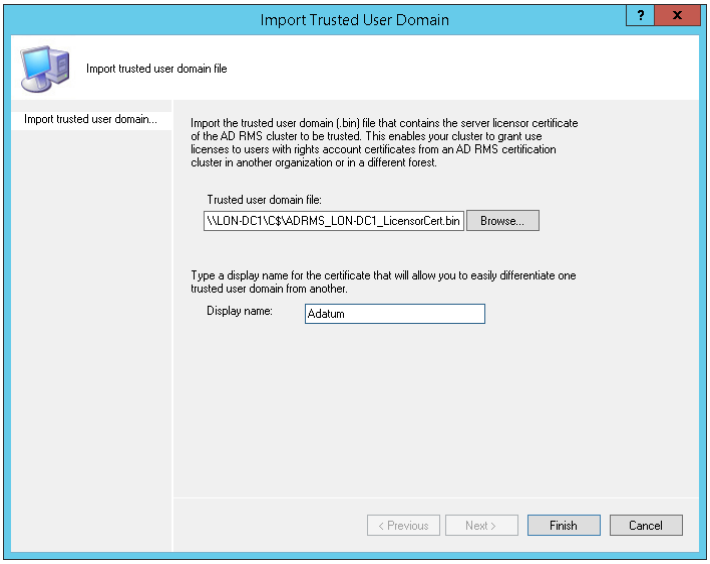

4. Qua máy **LON-DC1**, trong cửa sổ **Active Directory Rights Management Services**, bung **lon-dc1.adatum.com**, bung **Trust Policies**, chọn **Trusted User Domains**, chọn **Import Trusted User Domain**.



5. Hộp thoại **Import Trusted User Domain,** trong ô **Trusted user domain file**, nhập **\\TREY-DC1\C$\ADRMS_TREY-DC1_LicensorCert.bin**, trong ô **Display name**, nhập **TreyResearch**, chọn **Finish**.

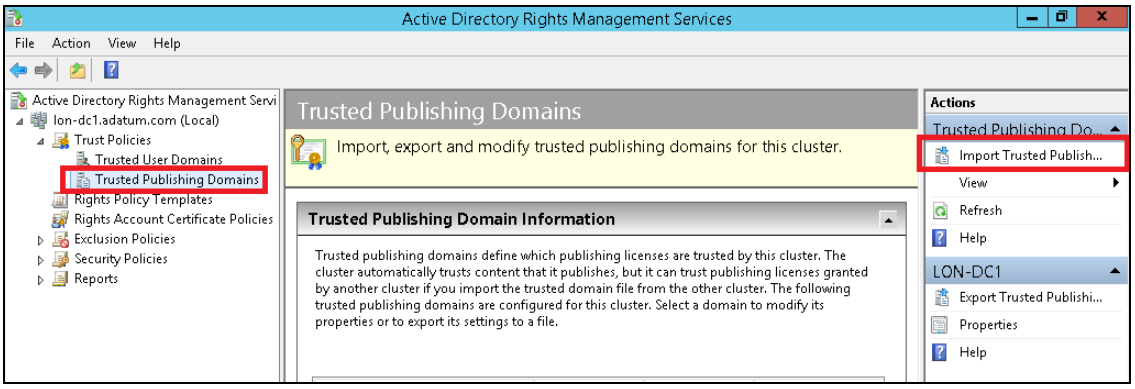



6. Qua máy **TREY-DC1**, Lặp lại bước 4 và 5 để import **Trusted User Domain** với **Trusted user domain file** là **\\LON-DC1\C$\ADRMS_LON-DC1_LicensorCert.bin** và **Display name** là **Adatum**.

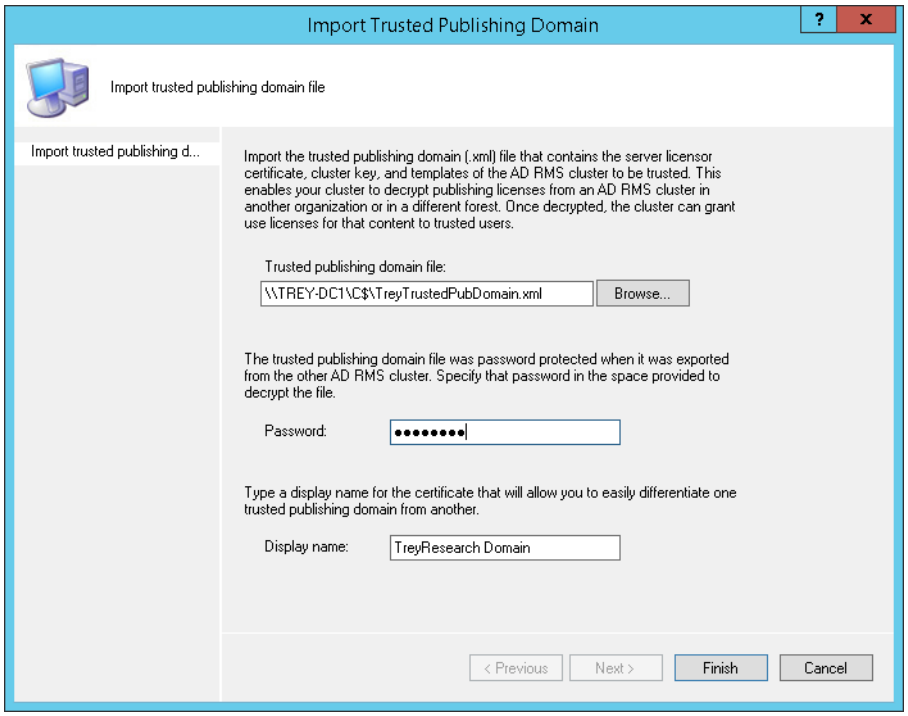


## Bước 4: Import Trusted Publishing Domain Policy của domain của đối tác.

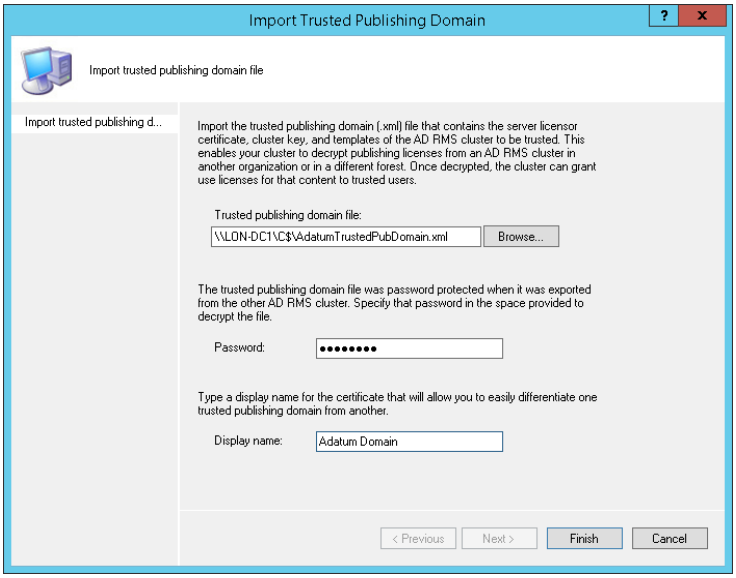
1. Qua máy **LON-DC1**, trong cửa sổ **Active Directory Rights Management Services**, bung **lon-dc1.adatum.com**, bung **Trust Policies**, chọn **Trusted Publishing Domains**, chọn **Import Trusted Publishing Domain**.




2. Hộp thoại **Import Trusted Publishing Domain** , trong ô **Trusted Publishing Domain file**, nhập **\\TREY-DC1\c$\TreyTrustedPubDomain.xml**, trong ô **Password** nhập **Pa$$w0rd**, trong ô **Display name**, nhập **TreyResearch Domain**, chọn **Finish**.

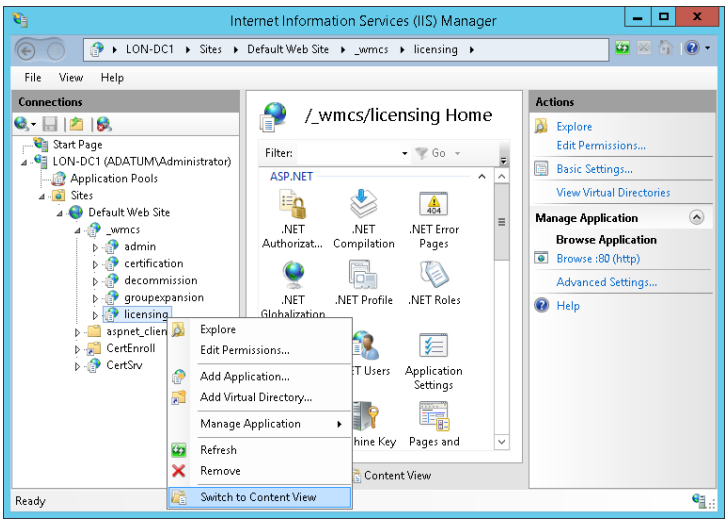


3. Qua máy **TREY-DC1**, Lặp lại bước 1 và 6 để import **Trusted Publishing Domain,** với **Trusted Publishing Domain file** là **\\LON-DC1\C$\AdatumTrustedPubDomain.xml** và **Display name** là **Adatum Domain**.

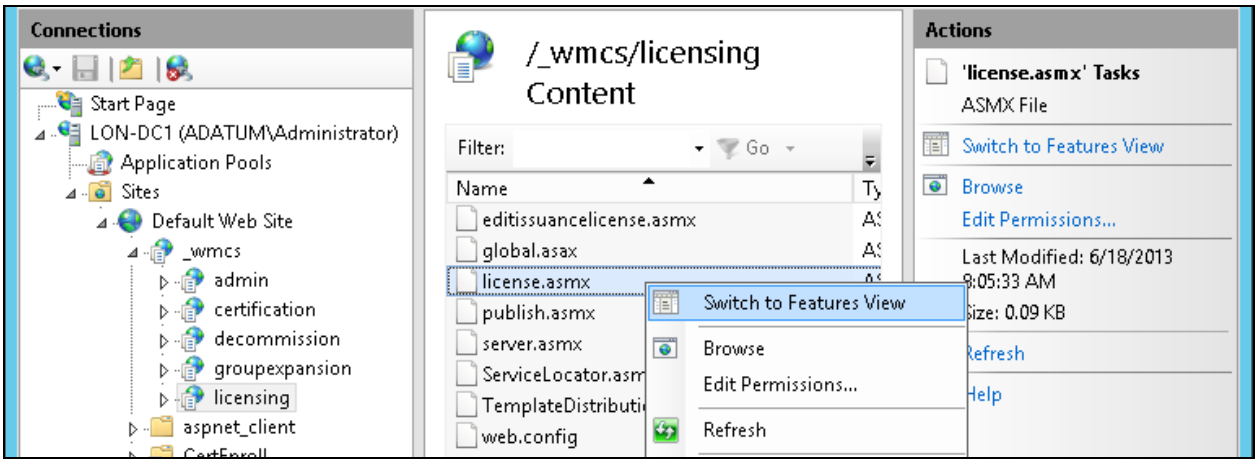



## Bước 5: Cấu hình cho phép Anonymous truy cập AD RMS Licensing Server.

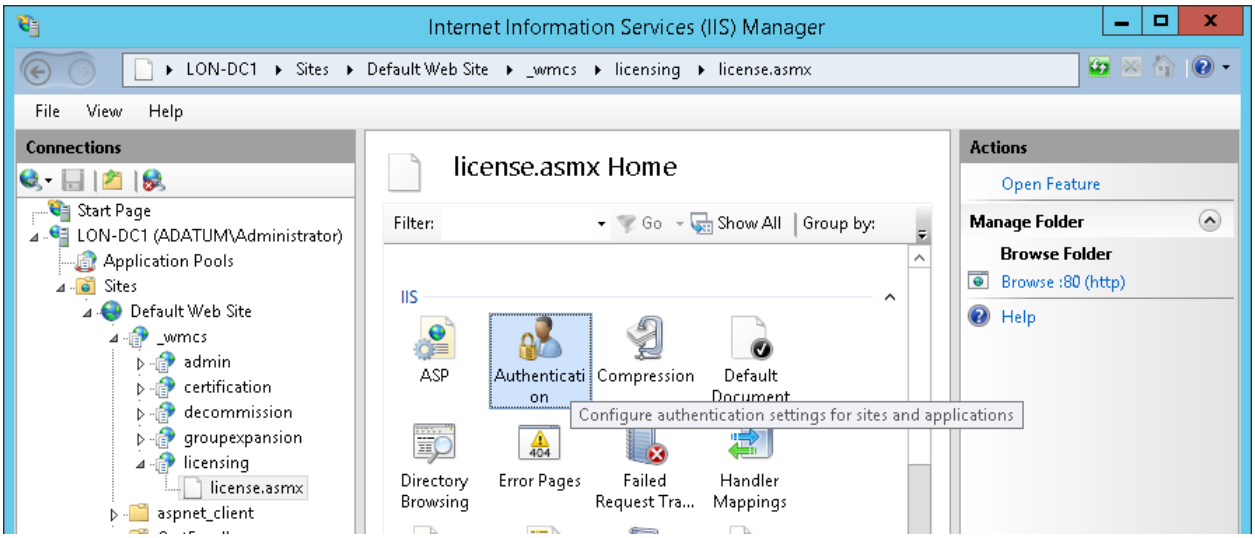
1. Qua máy **LON-DC1**, trong **Server Manager**, bung menu **Tools**, mở **Internet Information Services (IIS) Manager**, bung **LON-DC1,** bung **Sites,** bung **Default Web Site,** bung **_wmcs**, chọn và chuột phải **licensing**, chọn **Switch to Content View**.



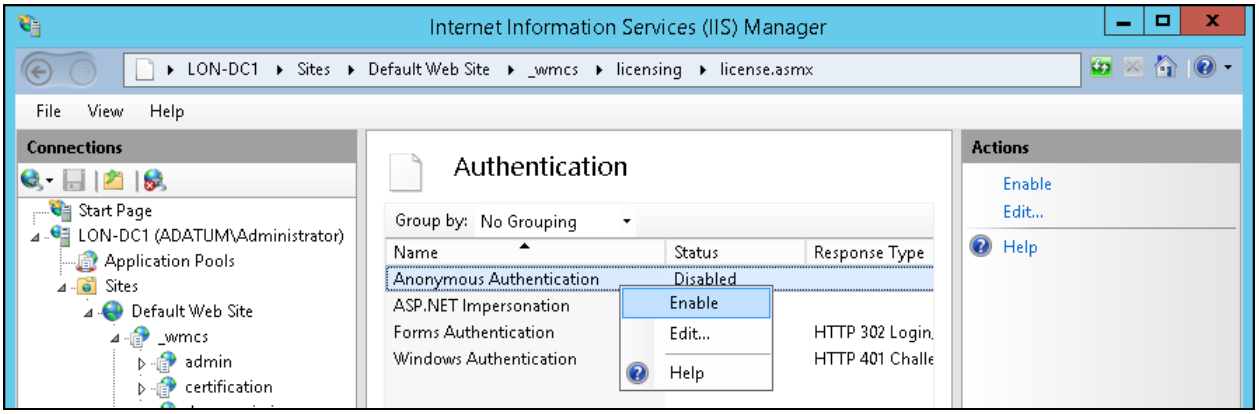
2. Trong cửa sổ giữa, chuột phải **license.asmx**, chọn **Switch to Features View**.



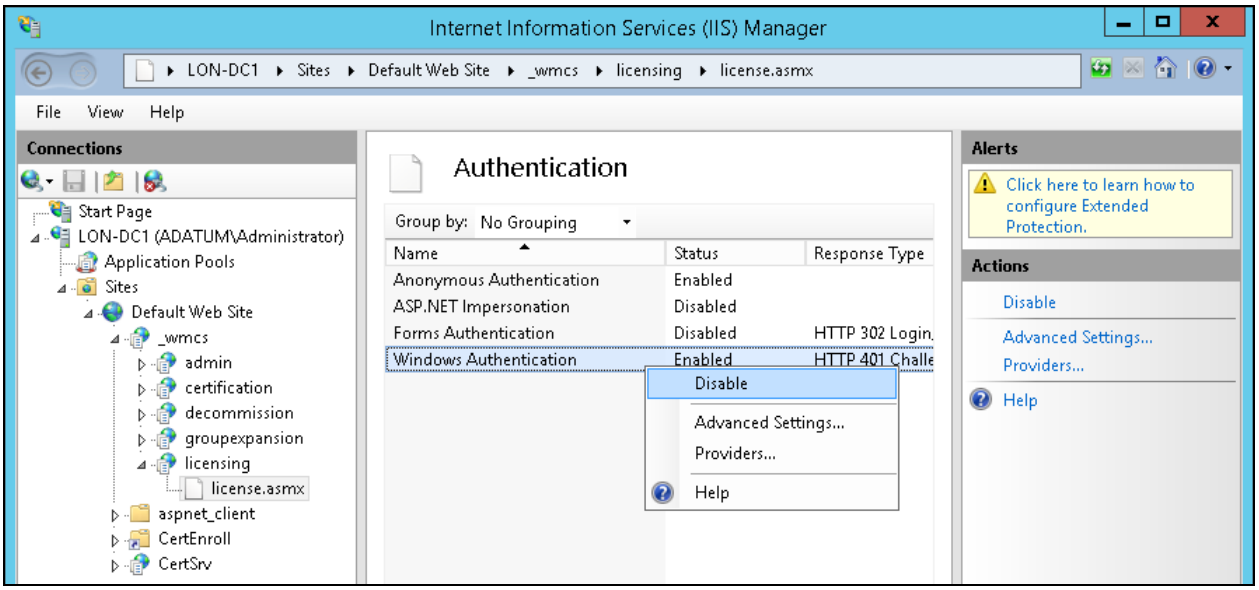

3. Trong cửa sổ giữa, nhấp đôi chuột **Authentication**.



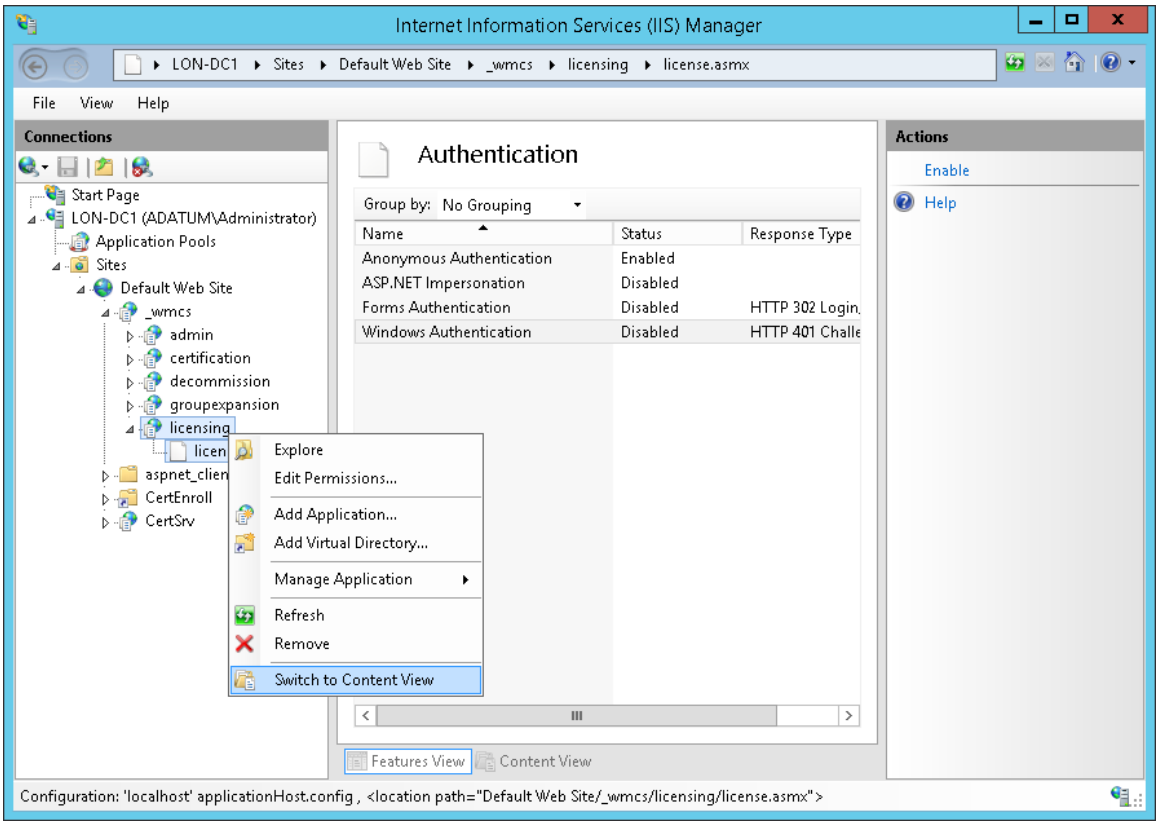
4. Chuột phải **Anonymous Authentication**, chọn **Enable**.



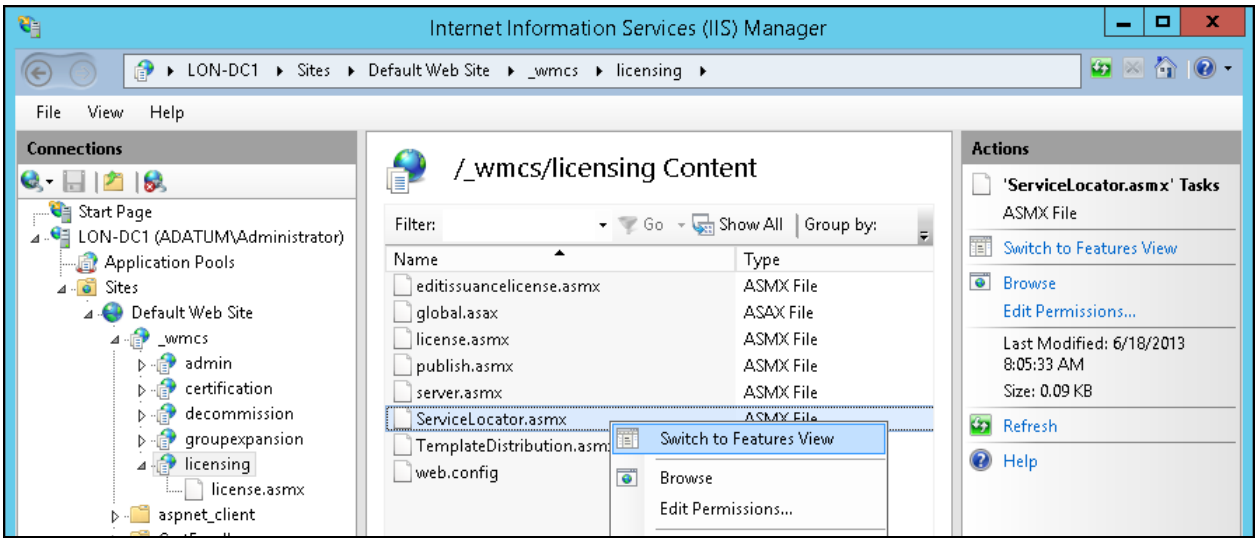

5. Chuột phải **Windows Authentication**, chọn **Disable**.



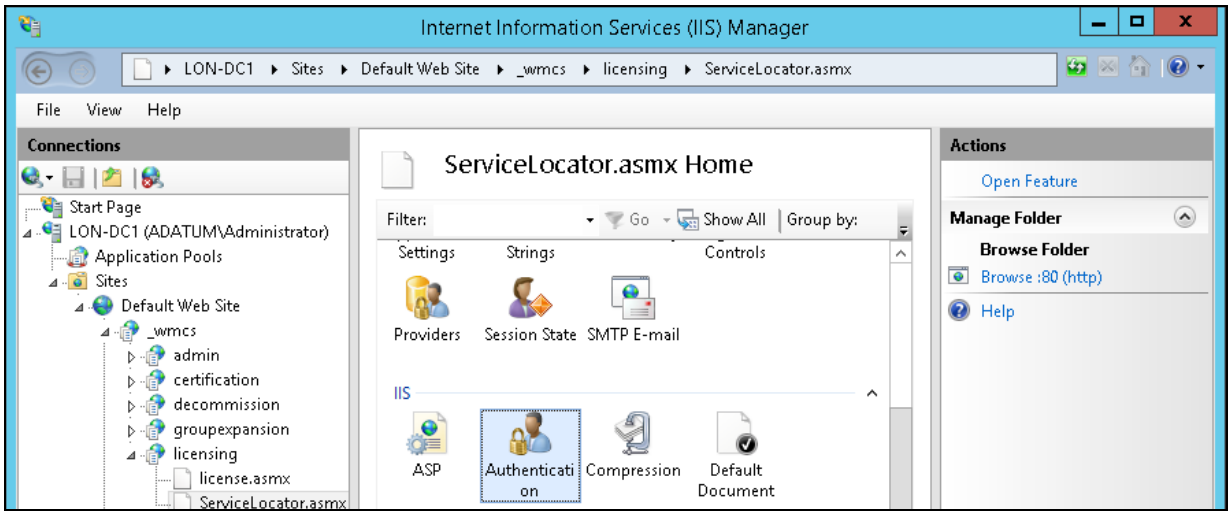
6. Chuột phải **licensing**, chọn **Switch to Content View**.



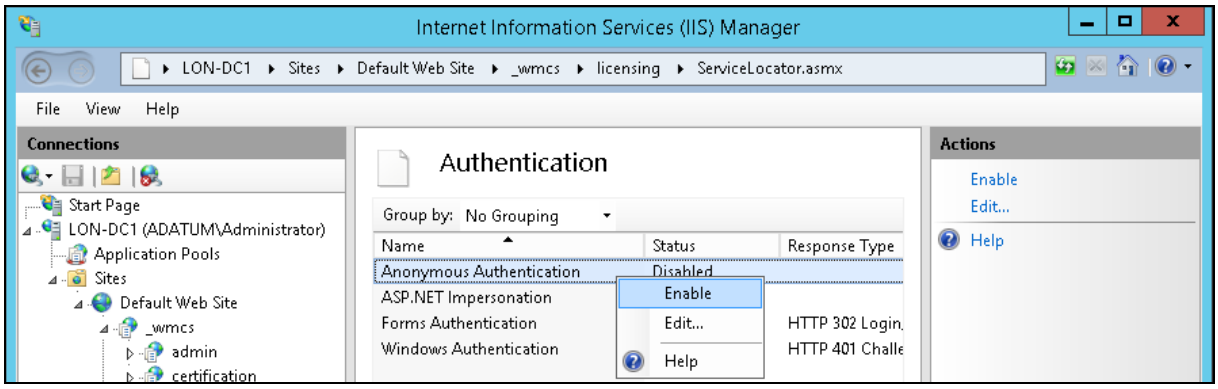

7. Chuột phải **ServiceLocator.asmx**, chọn **Switch to Features View**.



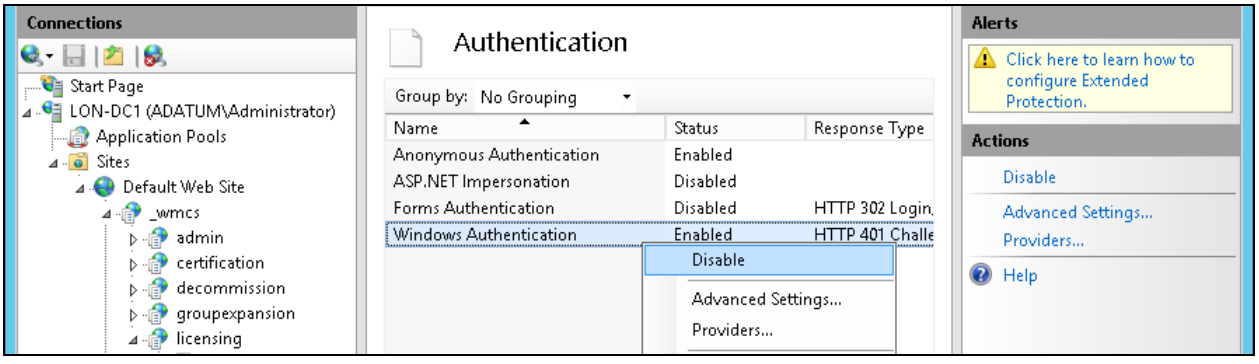
8. Nhấp đôi chuột **Authentication**.




9. Chuột phải **Anonymous Authentication**, chọn **Enable**.




10. Chuột phải **Windows Authentication**, chọn **Disable**.

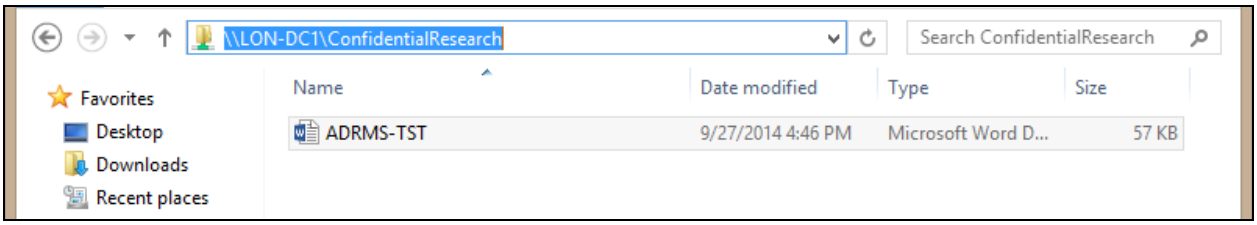



11. Tắt cửa sổ **Internet Information Services (IIS) Manager**.

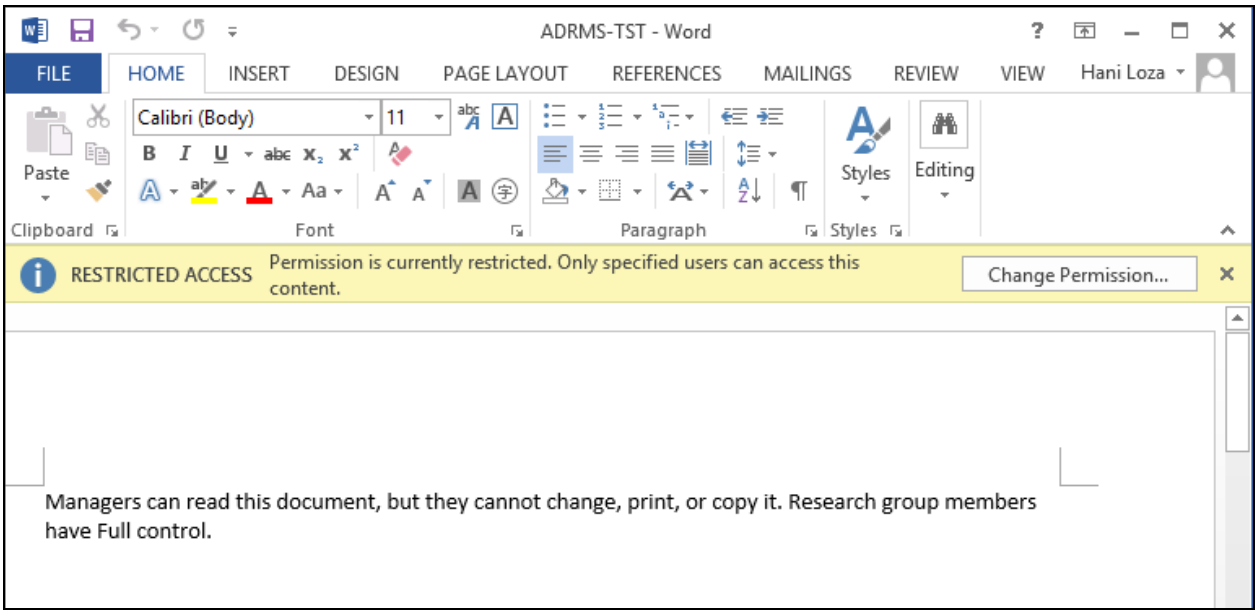
## Bước 6: Kiểm tra người dùng truy cập tài liệu.

1. Sign in vào máy **LON-CL1** bằng **Adatum\Hani** với password **Pa$$w0rd**.

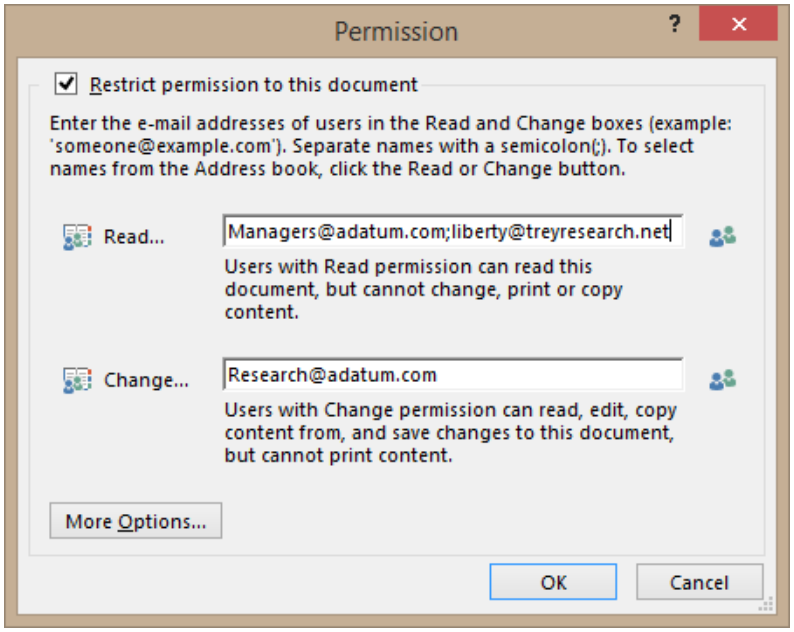
2. Mở File Explorer, truy cập **\\LON-DC1\ConfidentialResearch**, mở file **ADRMS-TST.docx**.




3. Trong file Word, trên thanh **Restricted Access** màu vàng, chọn **Change Permission**.

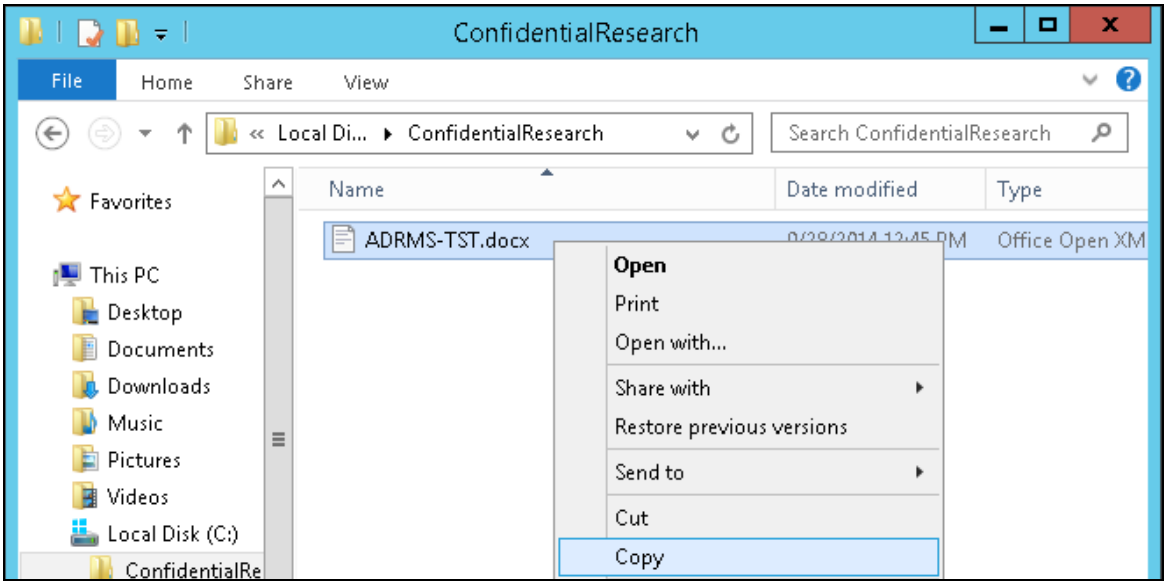


4. Hộp thoại **Permission**, trong ô **Read**, thêm dấu **;** vào phía sau **Managers@adatum.com**, và nhập thêm **liberty@treyresearch.net**, chọn **OK**.

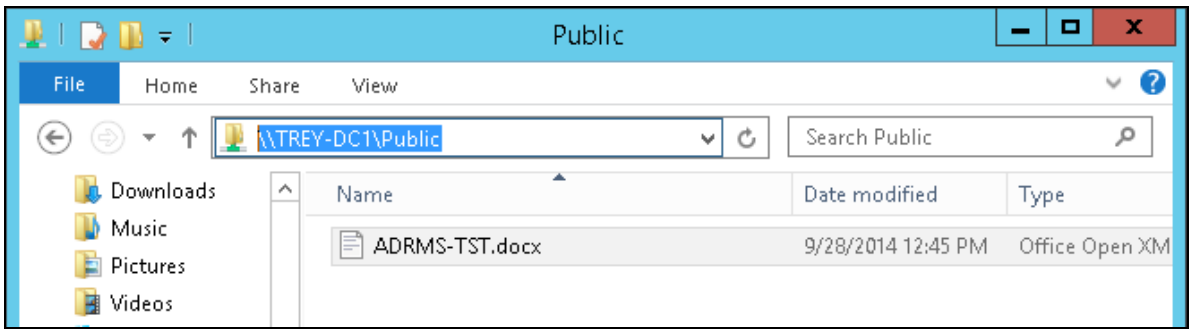



5. Save file **ADRMS-TST.docx**, tắt Microsoft Word, và sign out máy **LON-CL1**.

6. Qua máy **LON-DC1**, mở **File Explorer**, vào **C:\ConfidentialReseach**, copy file **ADRMS-TST.docx**

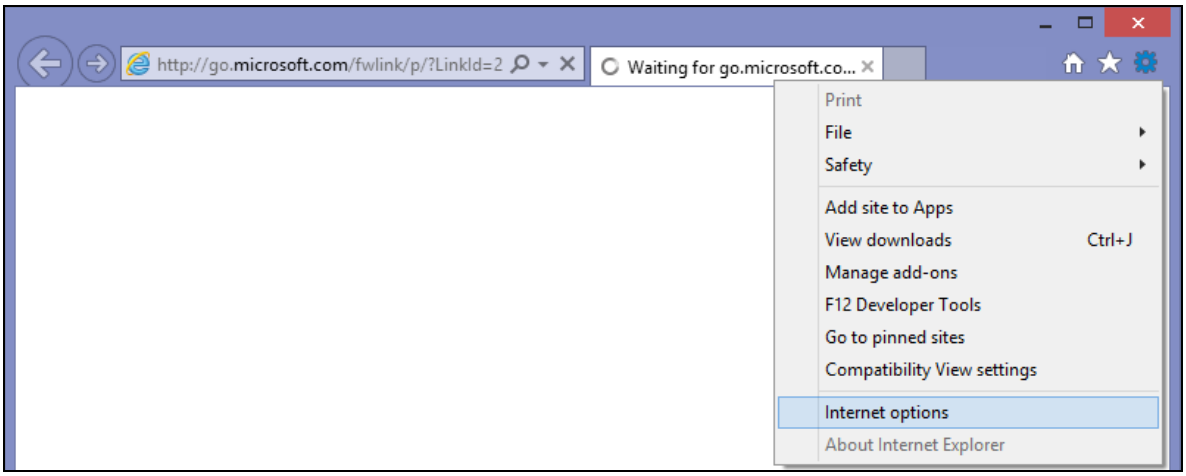


7. Truy cập **\\TREY-DC1\Public**, và chép file **ADRMS-TST.docx** vào.

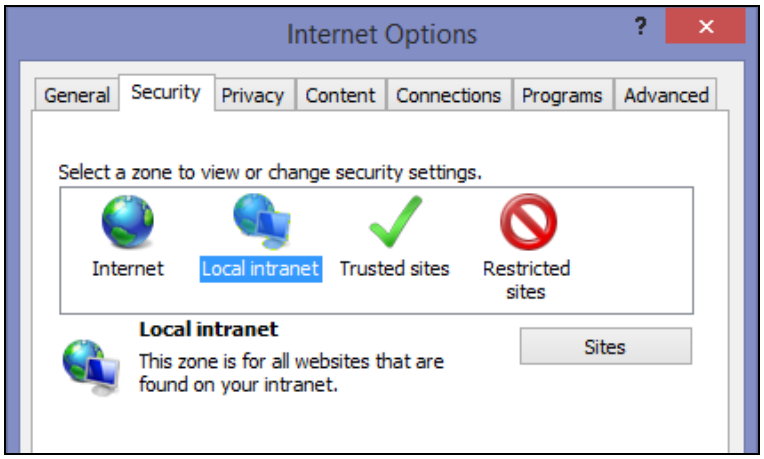



8. Sign in vào máy **TREY-CL1** bằng **TreyResearch\Liberty** với password **Pa$$w0rd**.

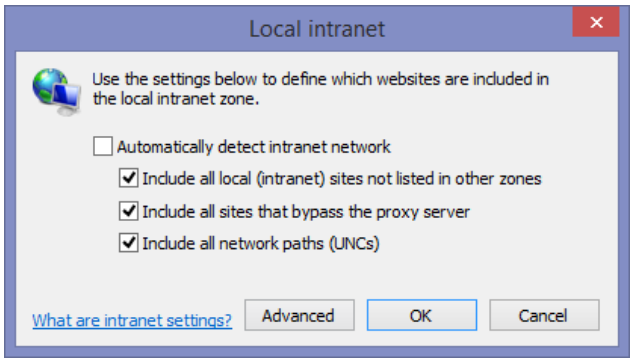
9. Mở **Internet Explorer**, bung biểu tượng **Tools**, chọn **Internet options**.



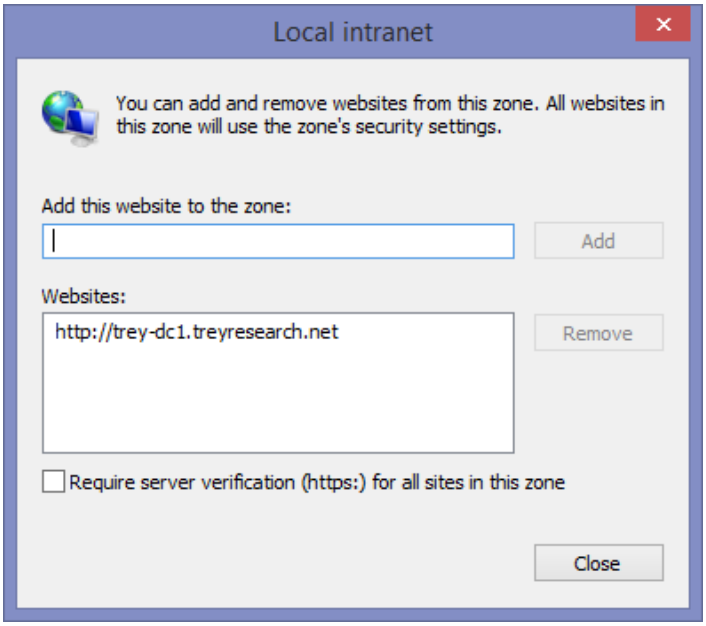

10. Hộp thoại **Internet options,** qua tab **Security**, chọn **Local intranet**, chọn **Sites**.



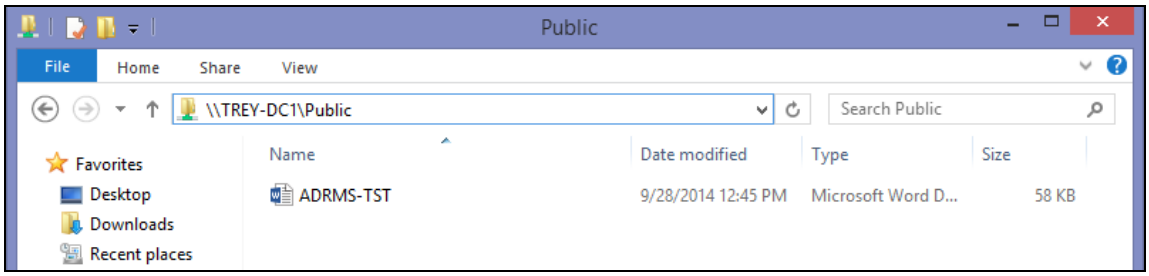
11. Hộp thoại **Local intranet**, chọn **Advanced**.



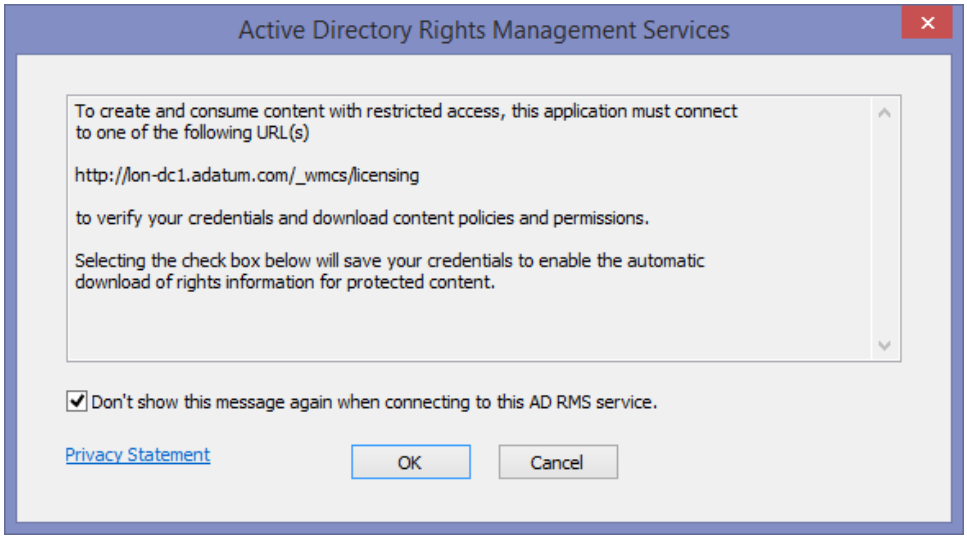

12. Trong ô **Add this website to the zone**, nhập **http://TREY-DC1.TreyResearch.net**, chọn **Add**, chọn **Close**, chọn **OK** 2 lần. Tắt cửa sổ **Internet Explorer.**



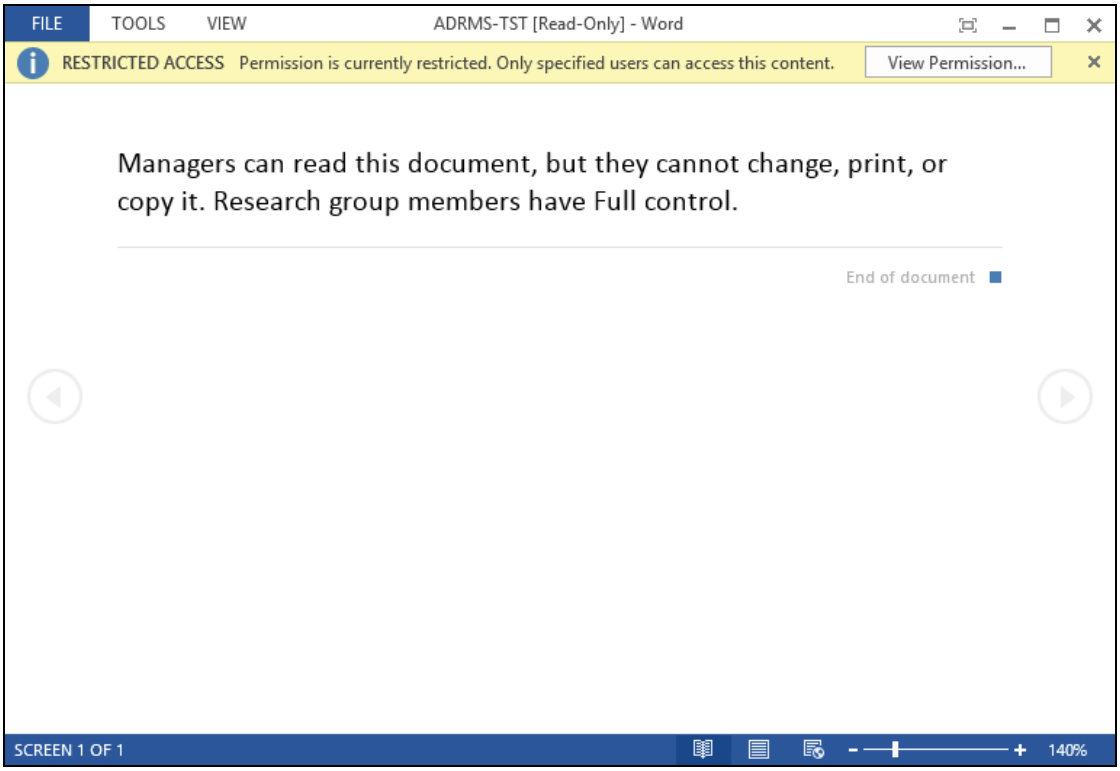

13. Mở File Explorer, truy cập **\\TREY-DC1\Public**, mở file **ADRMS-TST.docx**.



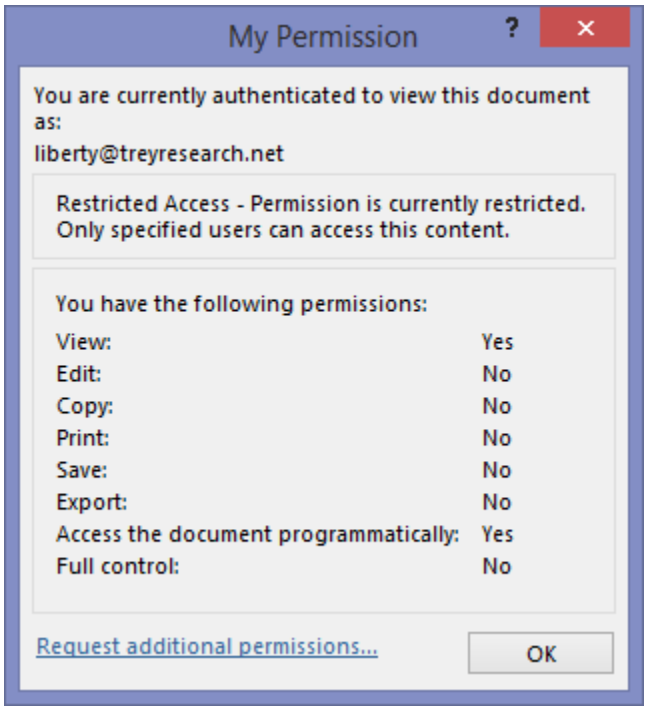
14. Hộp thoại **Active Directory Rights Management Services**, chọn **OK.** (Tắt tất cả cửa sổ Welcome của Microsoft Office nếu có)




15. Trong cửa sổ Word, trên thanh **Restricted Access** màu vàng, chọn **View Permission**.



16. Kiểm tra user **Liberty@treyresearch.net** chỉ có quyền đọc nội dung của tài liệu.




**Kết quả: Sau khi hoàn thành bài tập này, bạn đã tích hợp AD RMS của domain Adatum.com và TreyResearch.net để hỗ trợ người dùng của hai hệ thống có thể truy cập tài liệu RMS lẫn nhau.**

**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 **20414C-LON-DC1**, chọn **Revert**.
3. Trong hộp thoại **Revert Virtual Machine**, chọn **Revert**.
4. Thực hiện bước 2 và 3 cho các máy ảo còn lại.