

# BÁO CÁO THỰC HÀNH

Môn học: Quản trị mạng và hệ thống

Lab 4: Triển khai Active Directory trên Windows Server

Nhóm: 13

## 1. THÔNG TIN CHUNG:

Lớp: NT132.P12.ANTT.2

STT	Họ và tên	MSSV	Email
1	Hồ Diệp Huy	22520541	22520541@gm.uit.edu.vn
2	Đặng Đức Tài	22521270	22521270@gm.uit.edu.vn
3	Mai Nguyễn Nam Phương	22521164	22521164@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:

STT	Nội dung	Tình trạng	Trang
1	Xây dựng mô hình Workgroup	100%	2
2	Triển khai Active Directory và xây dựng mô hình Domain	100%	10
3	Xây dựng mô hình Additional Domain Controller cho dịch vụ Active Directory	100%	21
4	Xây dựng mô hình Read-only Domain Controller	100%	32
Điểm tự đánh giá			10/10

Phần bên dưới của báo cáo này là tài liệu báo cáo chi tiết của nhóm thực hiện

# BÁO CÁO CHI TIẾT

## Bài 1: Xây dựng mô hình Workgroup

**Yêu cầu 1.1** Tìm hiểu và trả lời câu hỏi sau:

1. Mô hình Workgroup hoạt động như thế nào?
2. Trình bày ưu và nhược điểm của mô hình Workgroup.

### 1. Mô hình Workgroup hoạt động như thế nào?

Trong mô hình Workgroup, các máy tính hoạt động bình đẳng theo cơ chế (peer-to-peer), chia sẻ tài nguyên với nhau nhưng quản lý độc lập. Không có máy chủ trung tâm nên dễ triển khai và chi phí thấp, nhưng việc bảo mật và quản lý phức tạp hơn khi quy mô mạng mở rộng.

### 2. Trình bày ưu và nhược điểm của mô hình Workgroup.

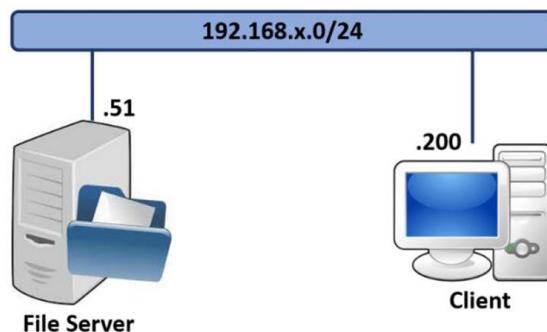
**Ưu điểm:** Workgroups không yêu cầu máy tính chạy trên hệ điều hành Windows Server để tập trung hóa thông tin bảo mật; workgroups thiết kế và hiện thực đơn giản và không yêu cầu lập kế hoạch có phạm vi rộng và quản trị như domain yêu cầu; workgroups thuận tiện đối với nhóm có số máy tính ít và gần nhau ( $\leq 10$  máy).

**Nhược điểm:** Mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập; bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi mật khẩu hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong Workgroup, nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó; việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng.

## Lab 4: Triển khai Active Directory trên Windows Server

**Yêu cầu 1.2** Xây dựng mô hình Workgroup để chia sẻ file như bên dưới.

Mô hình cần xây dựng:



Thông tin các máy:

Tên máy	Hệ điều hành	Địa chỉ IP
File Server	Windows Server 2016	192.168.13.51/24
Client	Windows 10	192.168.13.200/24

- Thông tin File Server:

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::a15c:cece:f8b3:666%6
  IPv4 Address . . . . . : 192.168.13.51
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.13.2

Tunnel adapter Teredo Tunneling Pseudo-Interface:

  Connection-specific DNS Suffix . :
  IPv6 Address . . . . . : 2001:0:2851:782c:1c7d:3c89:3f57:f2cc
  Link-local IPv6 Address . . . . . : fe80::1c7d:3c89:3f57:f2cc%11
  Default Gateway . . . . . : ::

Tunnel adapter isatap.{6E0421C6-13B1-481C-99E0-6D9475A3F602}:

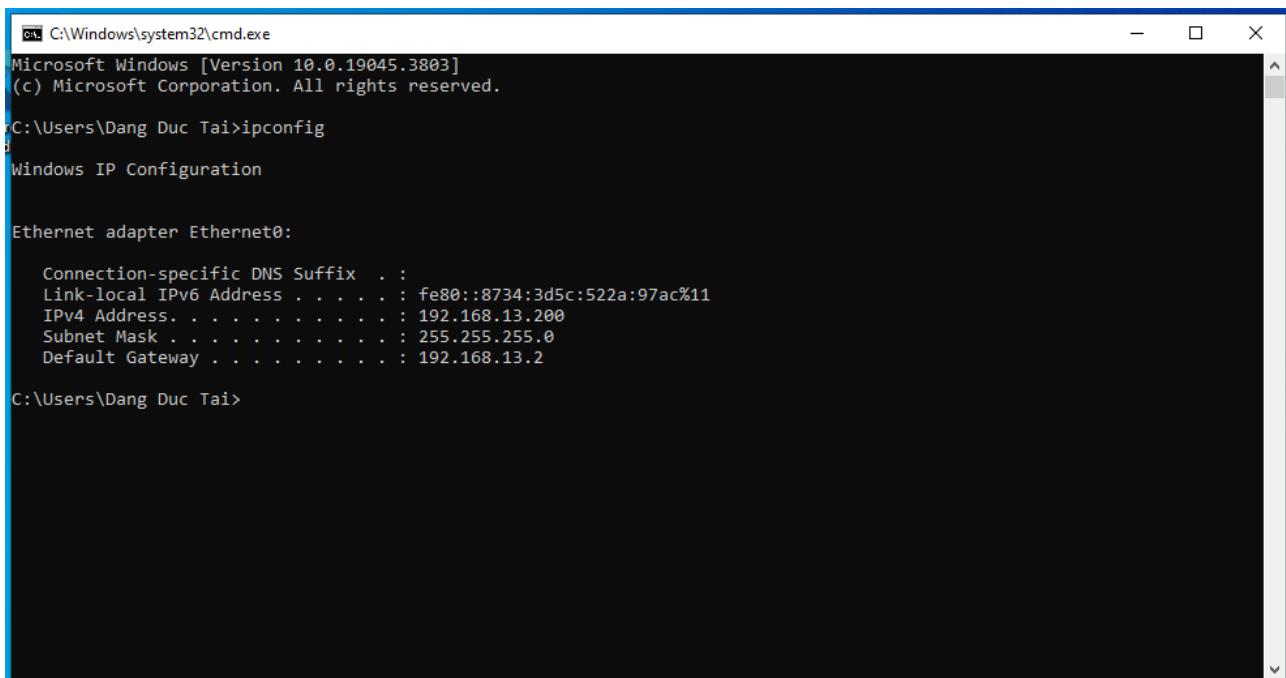
  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

C:\Users\Administrator>

```

## Lab 4: Triển khai Active Directory trên Windows Server

- Thông tin Client:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Đặng Đức Tài>ipconfig

Windows IP Configuration

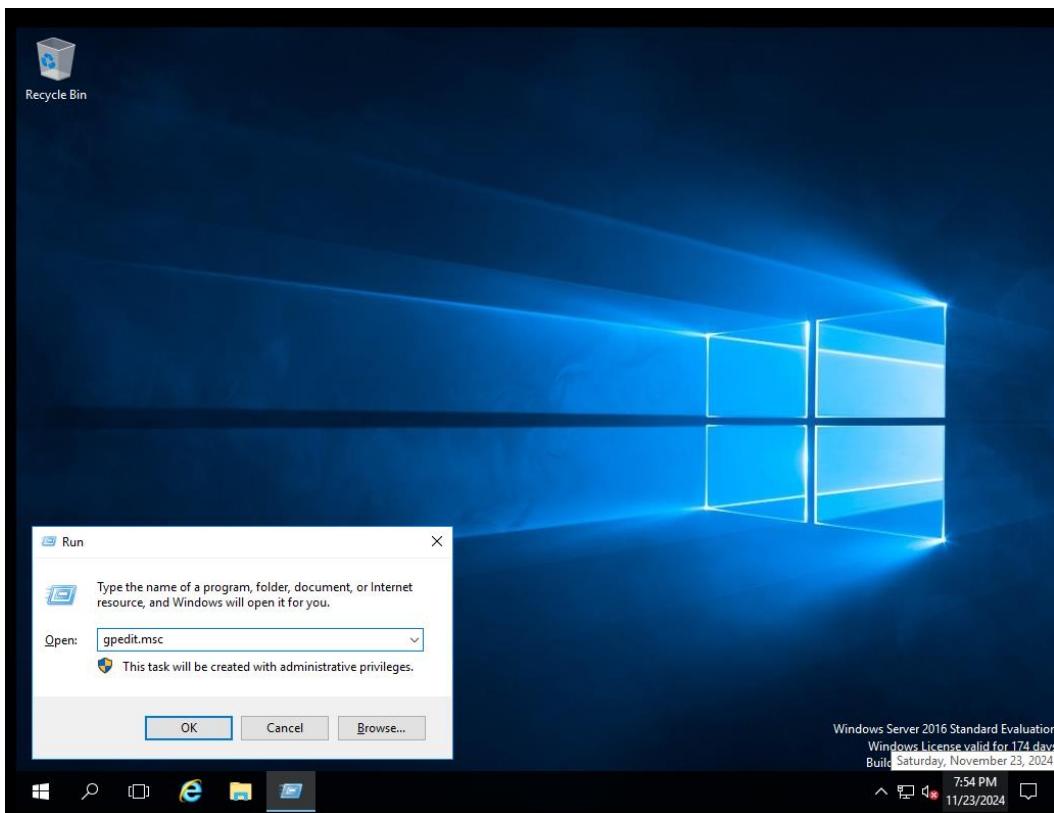
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::8734:3d5c:522a:97ac%11
IPv4 Address. . . . . : 192.168.13.200
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.13.2

C:\Users\Đặng Đức Tài>
```

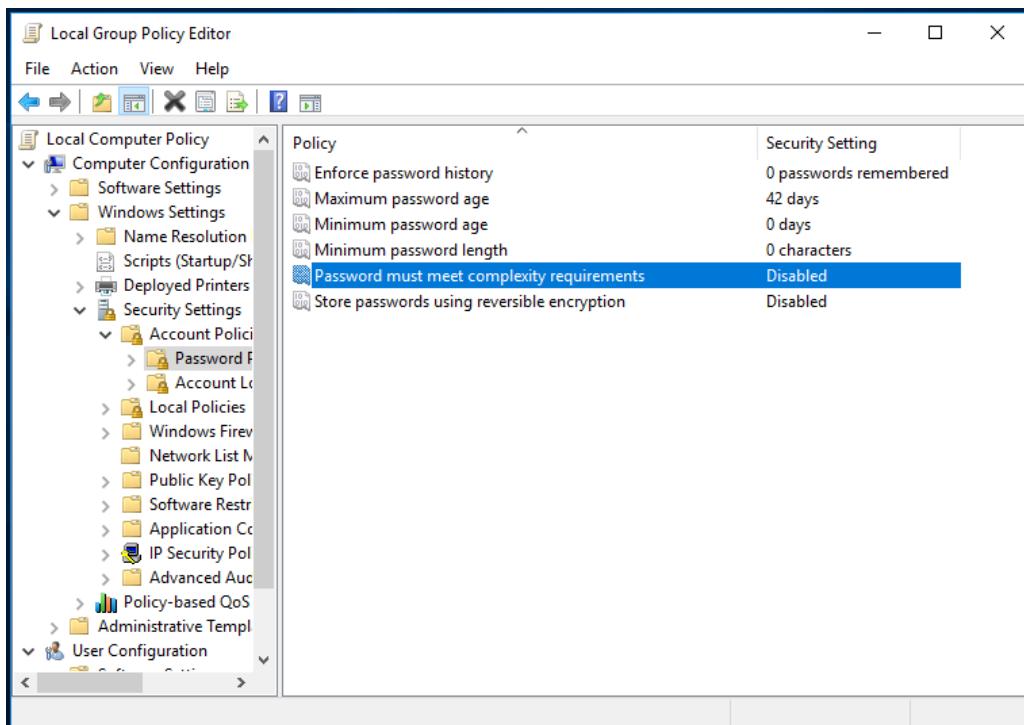
- Phía File Server: Thực hiện cấu hình chính sách mật khẩu

+ Sử dụng tổ hợp phím Win + R để mở hộp thoại Run, gõ lệnh gpedit.msc:

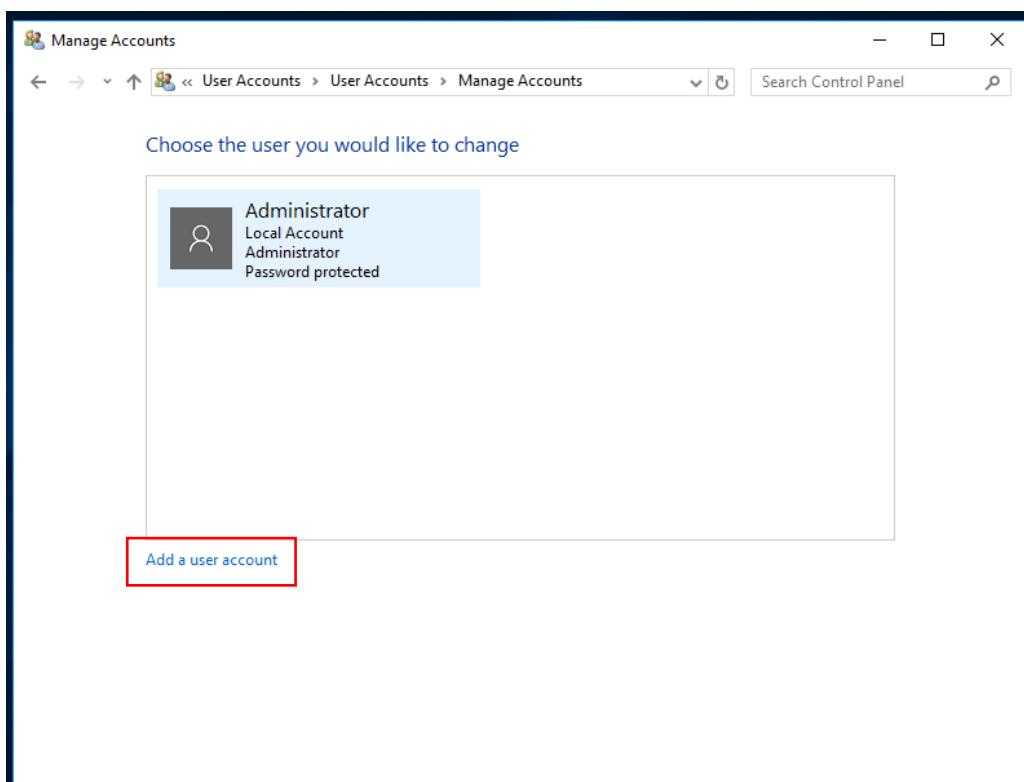


## Lab 4: Triển khai Active Directory trên Windows Server

- + Chính sửa chính sách tại **Windows Settings > Security Settings > Account Policies > Password Policy**. Tại mục **Password must meet complexity requirements**, thay đổi thành **Disabled**:

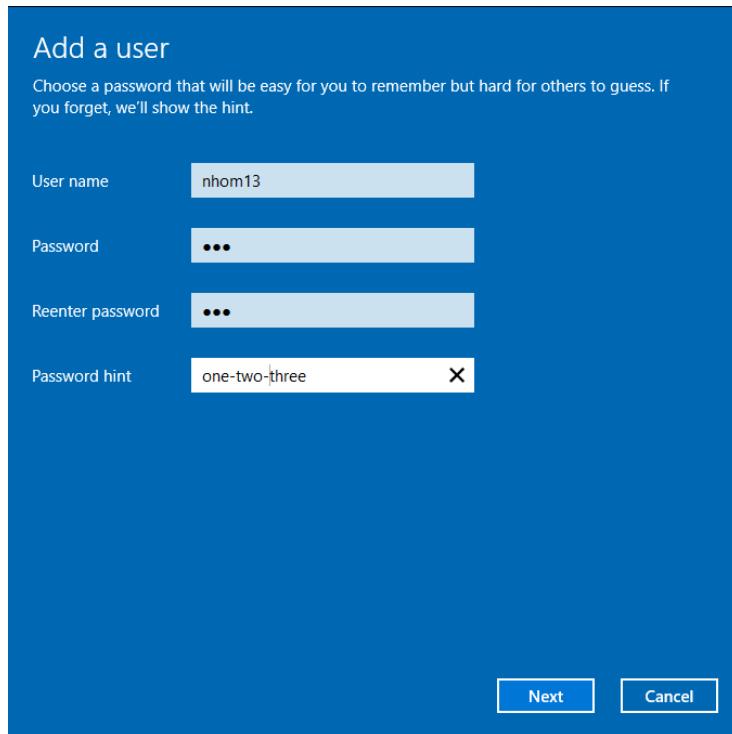


- Trên máy chủ File Server, tạo tài khoản **nhom13** có mật khẩu là **123**. Vào tại **Control Panel > User Accounts > Manage Another Accounts > Add a user account**:

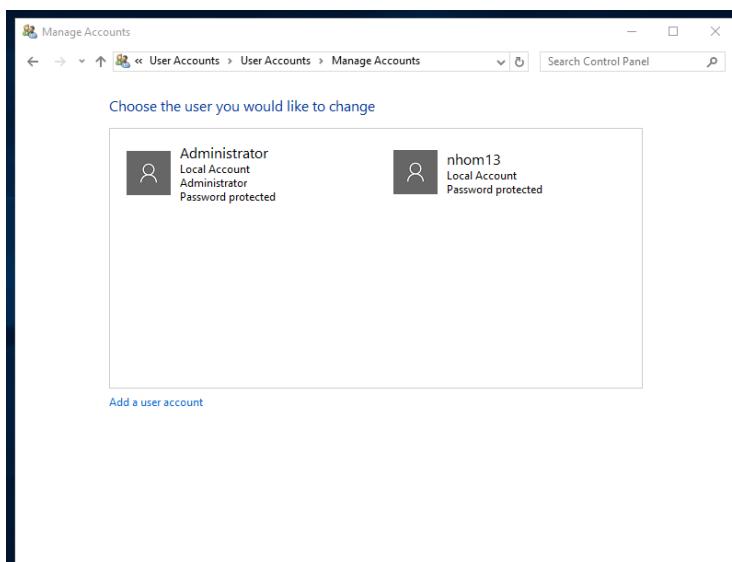


## Lab 4: Triển khai Active Directory trên Windows Server

- Nhập đầy đủ thông tin và ấn **Next**:



- Sau khi tạo thành công:

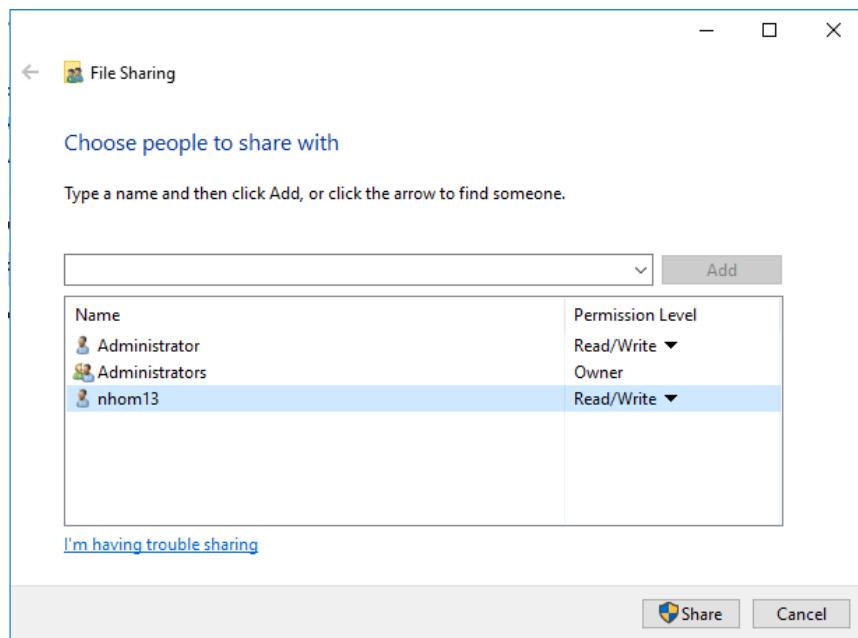


- Trên ổ đĩa C:\ của File Server, tạo 1 thư mục folder13 để chia sẻ dữ liệu:

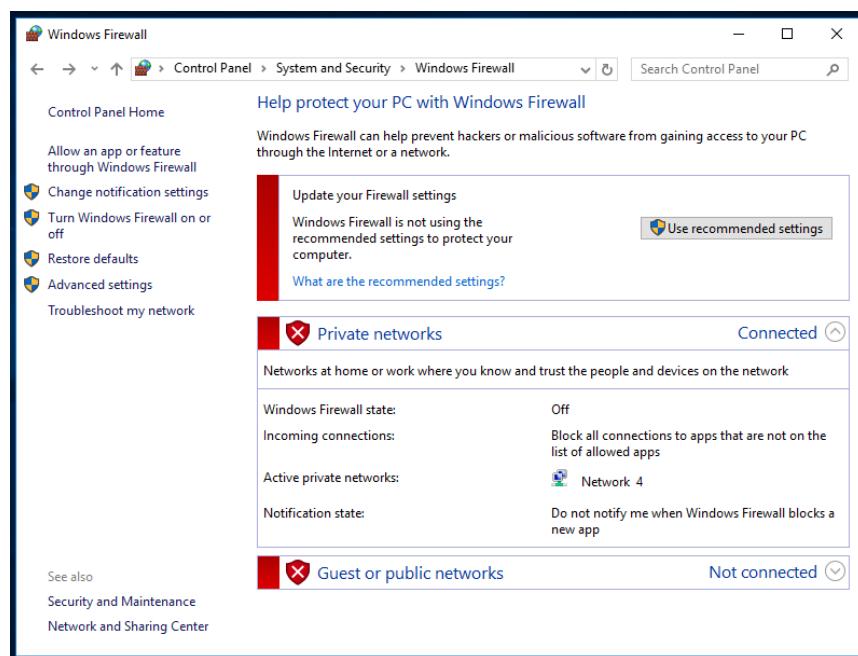
nhom13	11/17/2024 11:22 ...	File folder
PerfLogs	7/16/2016 6:23 AM	File folder
Program Files	11/17/2024 10:33 ...	File folder
Program Files (x86)	7/16/2016 6:23 AM	File folder
Users	11/17/2024 10:33 ...	File folder
Windows	11/17/2024 10:32 ...	File folder

## Lab 4: Triển khai Active Directory trên Windows Server

- Nhấp chuột phải vào tên thư mục **folder13**, chọn **Share with > Specific people...**. Thực hiện phân quyền chia sẻ trên thư mục này để user **nhom13** có quyền Read/Write.

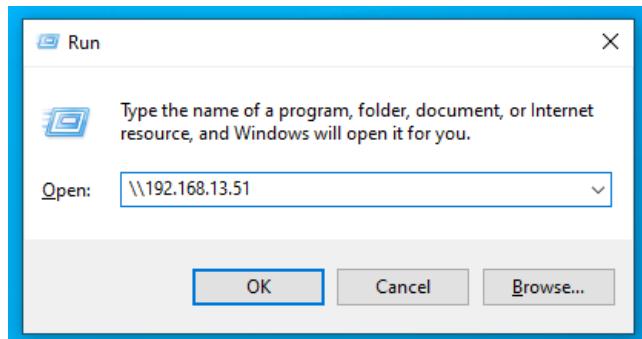


- Tắt Firewall trên File Server tại **Control Panel > System and Security > Windows Firewall > Turn Windows Firewall on or off:**



## Lab 4: Triển khai Active Directory trên Windows Server

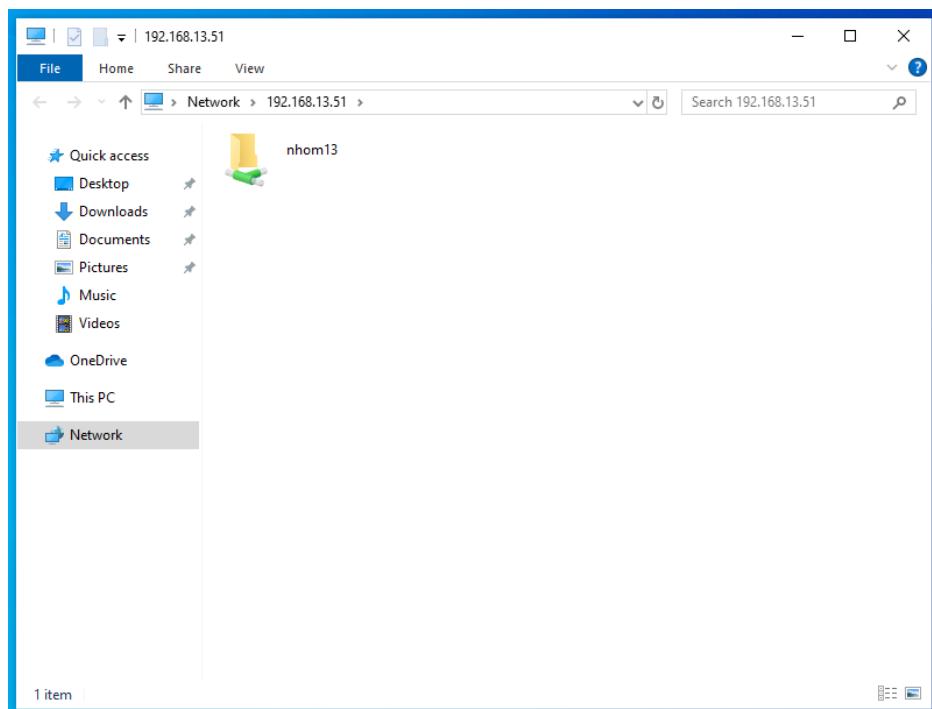
- Từ máy Client, kết nối vào máy chủ File Server. Vào Run, gõ địa chỉ IP của máy File Server:



- Đăng nhập bằng tài khoản máy Client không thành công:



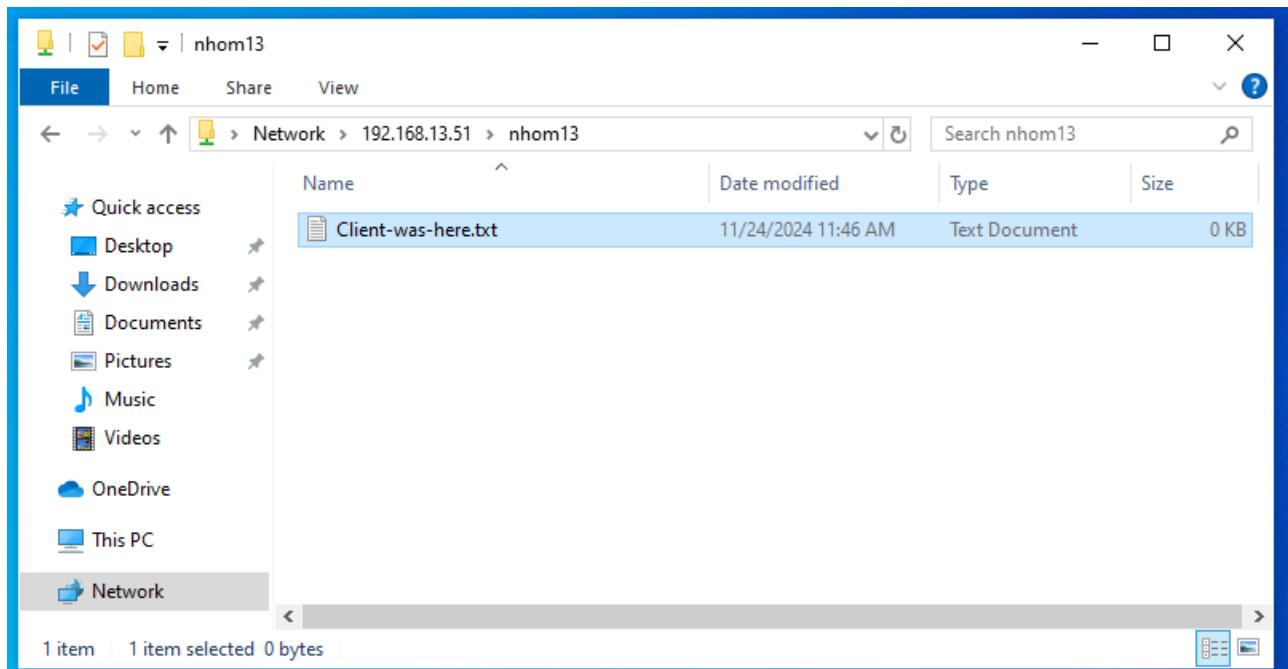
- Đăng nhập thành công bằng tài khoản **nhom13**:



## Lab 4: Triển khai Active Directory trên Windows Server

- Nguyên nhân: Khi thực hiện cấu hình quyền truy cập đối với folder13, ta chỉ cho phép một số user được phép truy cập và kèm theo một số quyền bên trong. User nhom13 có quyền Read/Write (Đọc/Ghi). Khi thực hiện truy cập bằng tài khoản nhom13, ta đang đóng vai trò là user trên File Server để truy cập vào folder13, chính vì thế ta hoàn toàn có thể truy cập vào folder13. Còn với user trên Client, do user này không được cấp quyền truy cập vào folder13, chính vì thế nên ta không thể thực hiện truy cập vào folder13.

- Tạo một file Client-was-here.txt:



- Do user nhom13 có quyền Read/Write nên được quyền tạo mới một file mới kí trong folder13 và ghi nội dung vào đó.

## Lab 4: Triển khai Active Directory trên Windows Server

### Bài 2: Triển khai Active Directory và xây dựng mô hình Domain

**Yêu cầu 2.1.** Tìm hiểu và trả lời câu hỏi sau:

1. Active Directory trong Windows là gì?
2. So sánh mô hình Domain và Workgroup?

#### 1. Active Directory trong Windows là gì?

Active Directory (AD) là một dịch vụ thư mục được phát triển bởi Microsoft, được ứng dụng chủ yếu trong các mạng sử dụng Windows Domain. Đây là một tập hợp các dịch vụ và quy trình được tích hợp trong hệ điều hành Windows Server.

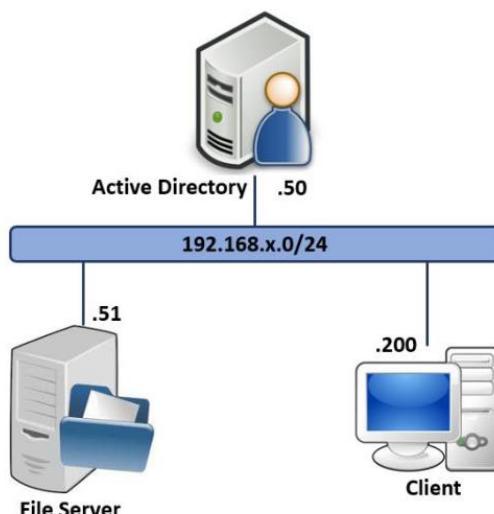
#### 2. So sánh mô hình Domain và Workgroup?

Domain	Workgroup
<ul style="list-style-type: none"> <li>- Quản trị viên mạng sử dụng một haowcj nhiều máy tính làm máy chủ và cung cấp tất cả các truy cập, quyền bảo mật cho tất cả các máy tính khác trong mạng.</li> <li>- Domain là một dạng của mạng máy tính, trong đó máy tính, máy in và tài khoản người dùng được đăng ký trong cơ quan sở dữ liệu trung tâm.</li> <li>- Nó có các máy chủ xác thực tập trung quy định quy tắc xác thực.</li> <li>- Nếu người dùng có tài khoản trong miền thì người dùng có thể đăng nhập vào bất kỳ máy tính nào trong miền.</li> <li>- Người dùng miền phải cung cấp thông tin đăng nhập bảo mật bất cứ khi nào họ truy cập mạng miền.</li> <li>- Trong một miền, máy tính có thể nằm trên một mạng cục bộ khác.</li> <li>- Trong một miền, hàng nghìn máy tính có thể được kết nối.</li> </ul>	<ul style="list-style-type: none"> <li>- Tất cả máy tính đều tương đương với nhau và không máy tính nào có quyền kiểm soát máy tính nào.</li> <li>- Trong một nhóm làm việc, mỗi máy tính duy trì cơ sở dữ liệu riêng của nó.</li> <li>- Mỗi máy tính có quy tắc xác thực riêng cho mỗi tài khoản người dùng.</li> <li>- Mỗi máy tính đã thiết lập tài khoản người dùng. Nếu người dùng có tài khoản trên máy tính đó thì chỉ người dùng mới có thể truy cập máy tính.</li> <li>- Nhóm làm việc không ràng buộc với bất kỳ sự cho phép bảo mật nào hoặc yêu cầu bất kỳ mật khẩu nào.</li> <li>- Tất cả máy tính phải trên cùng một mạng cục bộ.</li> <li>- Trong một nhóm làm việc, có thể chỉ có 20 máy tính được kết nối.</li> </ul>

## Lab 4: Triển khai Active Directory trên Windows Server

**Yêu cầu 2.2.** Xây dựng mô hình Domain như bên dưới.

Mô hình cần xây dựng:



Tên máy	Hệ điều hành	Địa chỉ IP	DNS Server
File Server	Windows Server 2016	192.168.13.51/24	192.168.13.50
Active Directory	Windows Server 2016	192.168.13.50/24	192.168.13.50
Client	Windows 10	192.168.13.200/24	192.168.13.50

- File Server:

```

C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : s1
Primary Dns Suffix . . . . . : nhom13.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : nhom13.local

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-16-39-BE
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9574:b9bb:6a6d:be09%15(Preferred)
IPv4 Address. . . . . : 192.168.13.51(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.13.2
DHCPv6 IAID . . . . . : 50334761
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-D4-9B-F3-00-0C-29-16-39-BE
DNS Servers . . . . . : 192.168.13.50
NetBIOS over Tcpip. . . . . : Enabled
  
```

## Lab 4: Triển khai Active Directory trên Windows Server

- Active Directory:

```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

Host Name . . . . . : WIN-TVMOINEF3V4
Primary Dns Suffix . . . . . : nhom13.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : nhom13.local

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : Intel(R) 82574L Gigabit Network Connection
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-00-16-07
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::95f6:d1b8:69aa:4b73%6(Preferred)
IPv4 Address. . . . . : 192.168.13.50(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.13.2
DHCPv6 IAID . . . . . : 33557545
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-D4-7B-AA-00-0C-29-00-16-07
DNS Servers . . . . . : ::1
                                         192.168.13.50
NetBIOS over Tcpip. . . . . : Enabled
```

- Client:

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Dang Duc Tai>ipconfig /all

Windows IP Configuration

Host Name . . . . . : s2
Primary Dns Suffix . . . . . : nhom13.local
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : nhom13.local

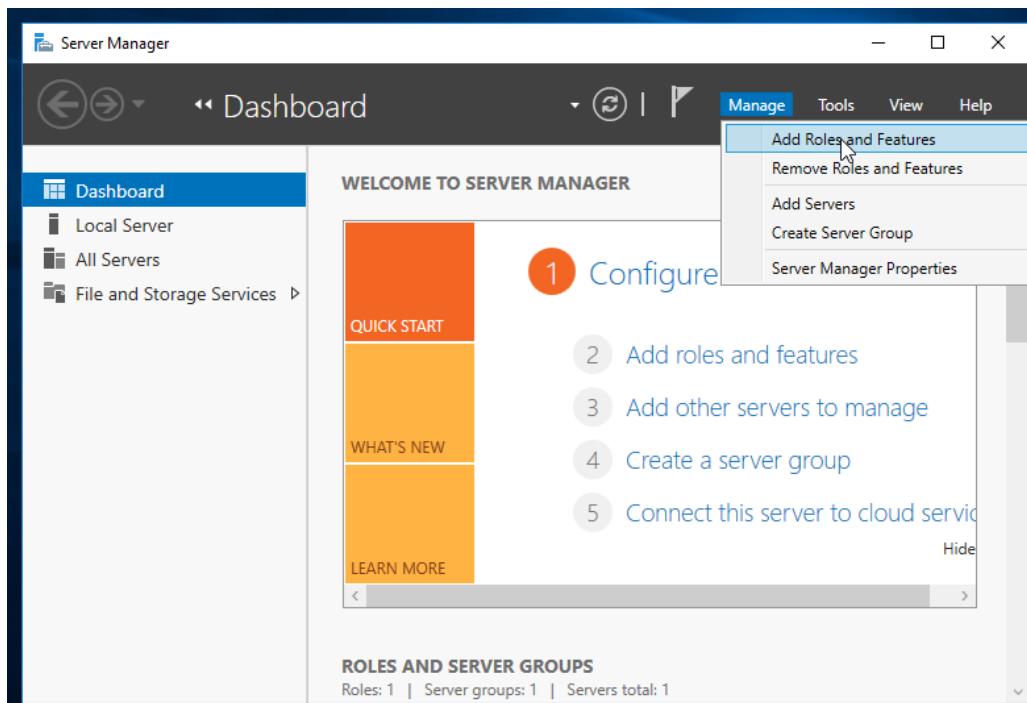
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . . . . . : Intel(R) 82574L Gigabit Network Connection
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-CD-C2-AF
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::8734:3d5c:522a:97ac%11(Preferred)
IPv4 Address. . . . . : 192.168.13.200(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.13.2
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-CD-6C-D6-00-0C-29-CD-C2-AF
DNS Servers . . . . . : 192.168.13.50
NetBIOS over Tcpip. . . . . : Enabled
```

## Lab 4: Triển khai Active Directory trên Windows Server

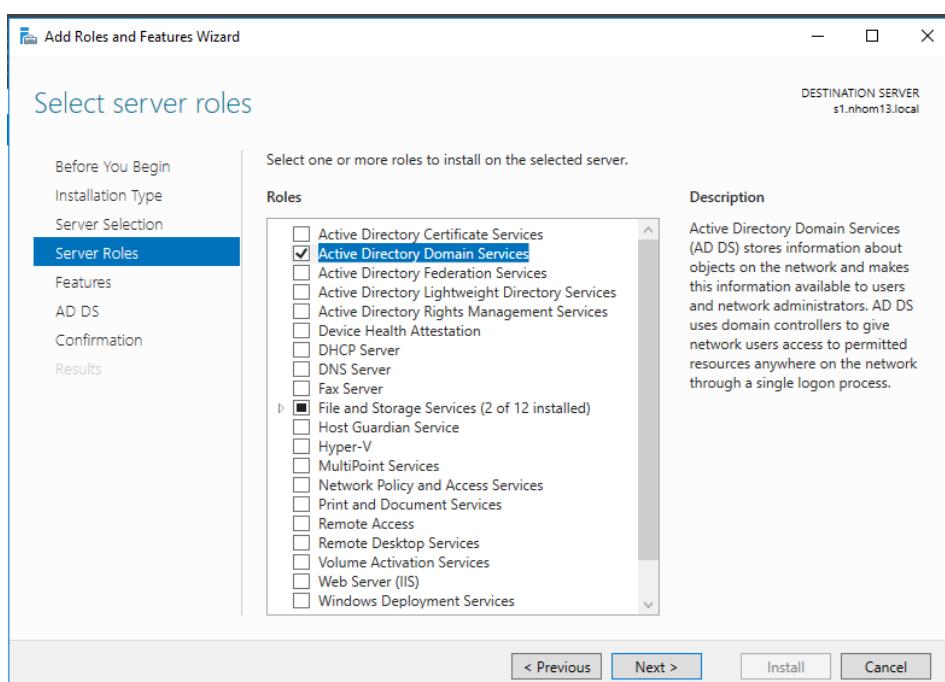
- Cài đặt Active Directory Domain Service trên máy Active Directory :

+ Vào Server Manager > Manage > Add Roles and Features:



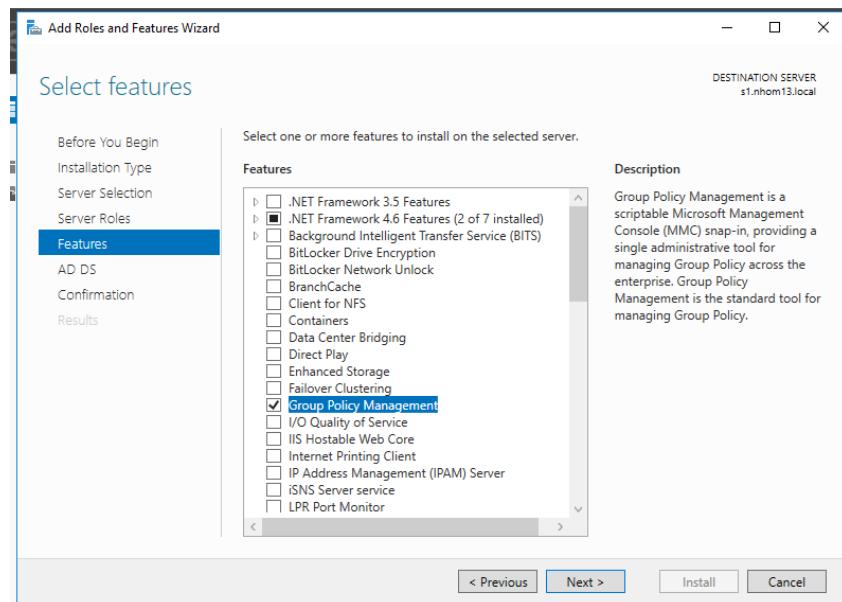
+ Chọn Next tại các bước Before You Begin, Installation Type, Server Selection.

+ Tại bước Server Roles, chọn Active Directory Domain Services.



## Lab 4: Triển khai Active Directory trên Windows Server

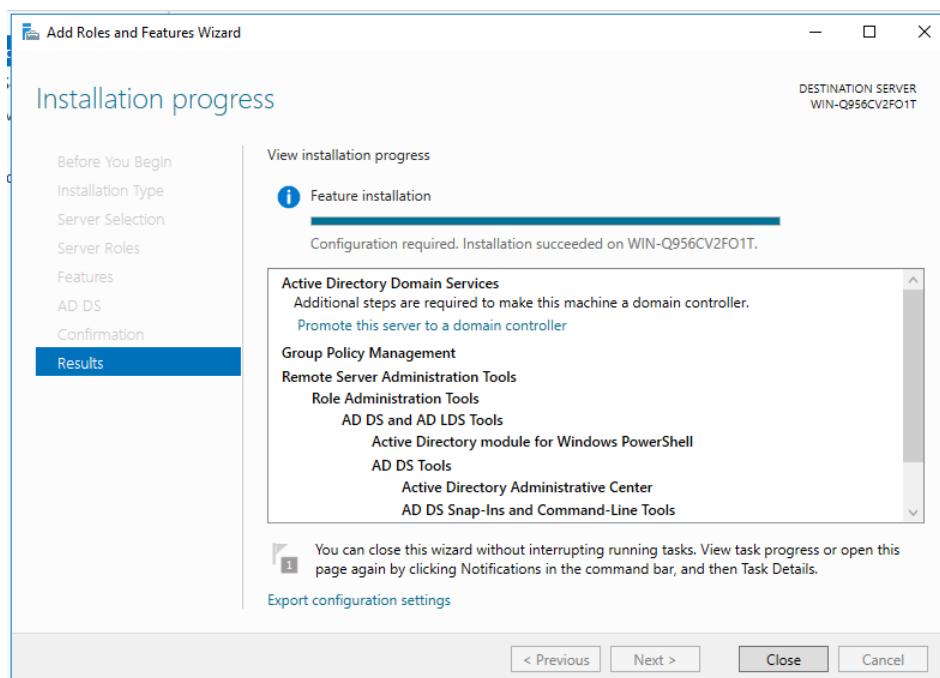
+ Ở bước **Features**, chọn **Group Policy Management**.



+ Ở bước **AD DS**, chọn **Next**.

+ Ở bước **Confirmation**, xác nhận lại thông tin và chọn **Install**.

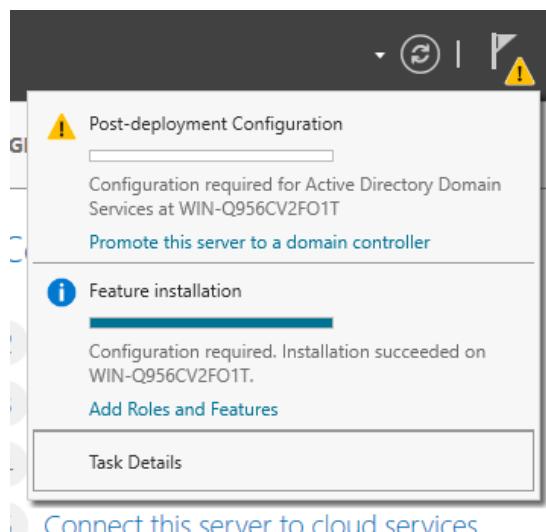
+ Chờ quá trình cài đặt hoàn thành và chọn **Close** để kết thúc.



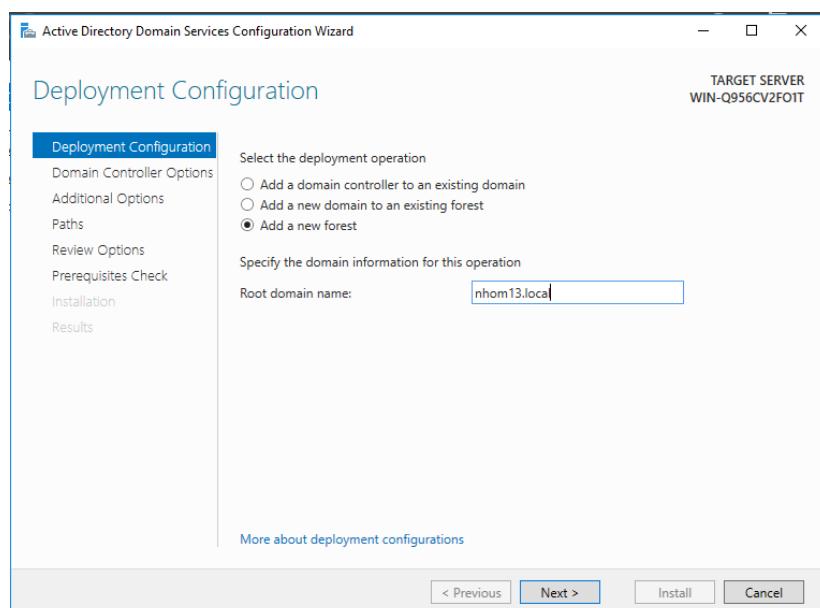
- Nâng cấp máy chủ Active Directory lên **Domain Controller**:

+ Vào **Server Manager** sẽ thấy biểu tượng cảnh báo, nhấn vào và chọn **Promote this server to a domain controller**.

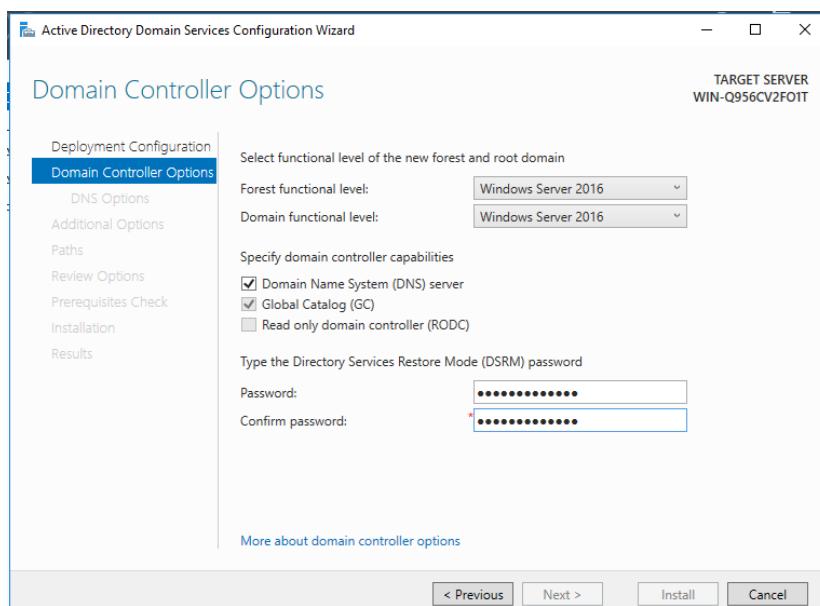
## Lab 4: Triển khai Active Directory trên Windows Server



+ Chọn **Add new forest** và gõ domain **nhom13.local** vào mục Root domain.

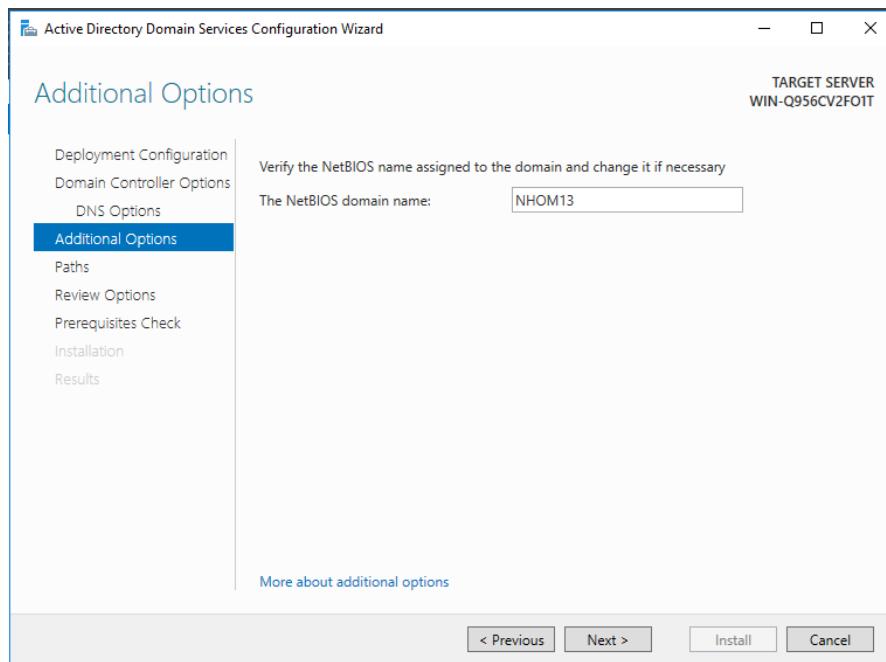


+ Tiếp theo, thiết lập **DSRM password** và các thiết lập như bên dưới.

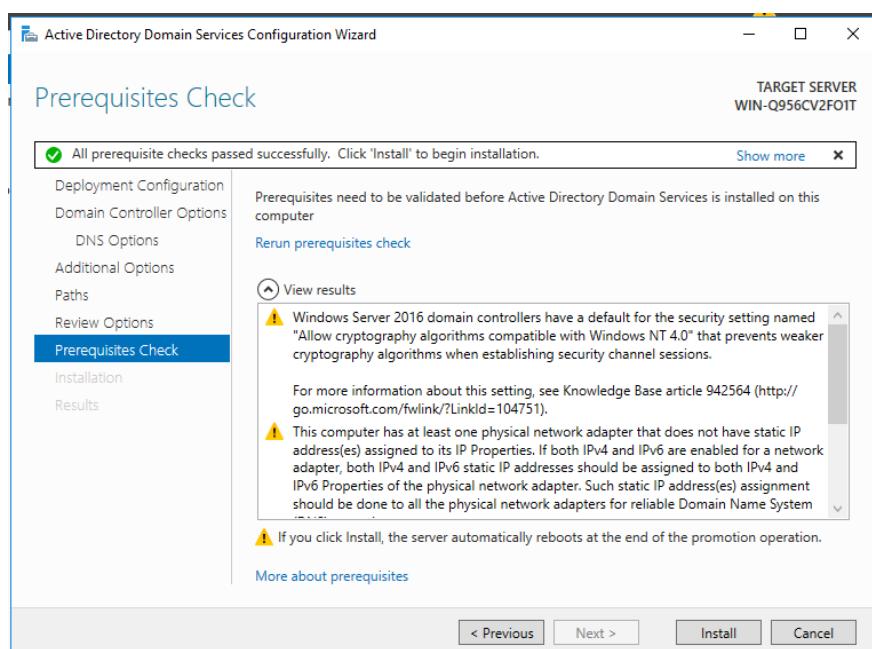


## Lab 4: Triển khai Active Directory trên Windows Server

- + Thiết lập NetBIOS domain name



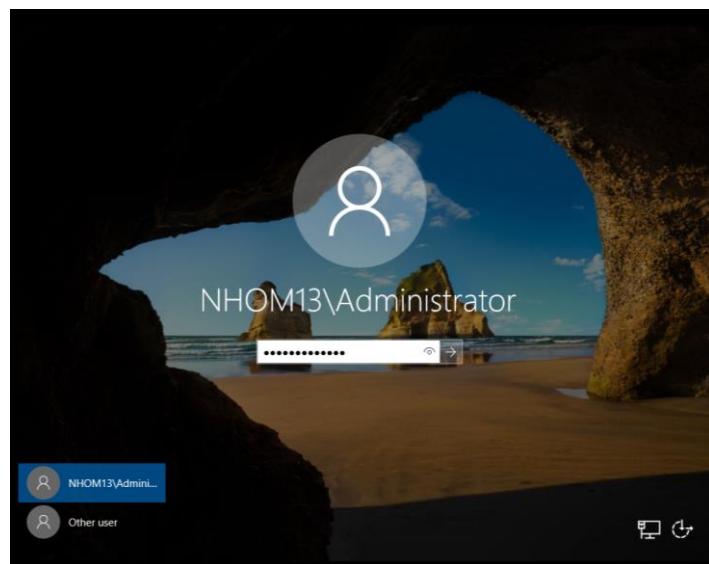
- + Giữ nguyên các tùy chỉnh mặc định ở mục **Paths**.
- + Thực hiện bước **Prerequisites Check** hoàn thành, sau đó chọn **Install** và chờ quá trình nâng cấp hoàn tất.



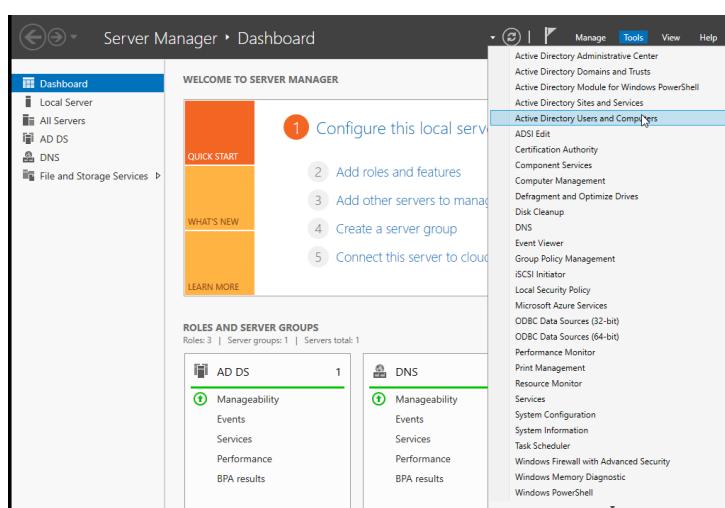
- + Sau khi hoàn tất quá trình này, máy chủ Active Directory sẽ khởi động lại và hoàn tất quá trình nâng cấp thành Domain Controller.
- Tạo user trong domain Bước này tạo 2 user fileadmin và user1 trong domain để sử dụng khi thêm File Server và Client vào domain ở các bước sau.

## Lab 4: Triển khai Active Directory trên Windows Server

+ Đăng nhập vào máy chủ Active Directory với tài khoản NHOM13\Administrator (tài khoản trong domain).



+ Vào Server Manager > Tools > Active Directory Users and Computers.



+ Trong **nhom13.local > Users**, nhấp chuột phải trong khung hiển thị các user, chọn **New > User** và nhập thông tin user muốn tạo.

**New Object - User**

Create in: nhom13.local/Users

First name:	File Admin	Initials:	<input type="text"/>
Last name:	<input type="text"/>		
Full name:	File Admin		
User logon name:	<input type="text"/> fileadmin	@nhom13.local	<input type="button" value="▼"/>
User logon name (pre-Windows 2000):	NHOM13\	fileadmin	<input type="button" value=""/>

**< Back** **Next >** **Cancel**

**New Object - User**

Create in: nhom13.local/Users

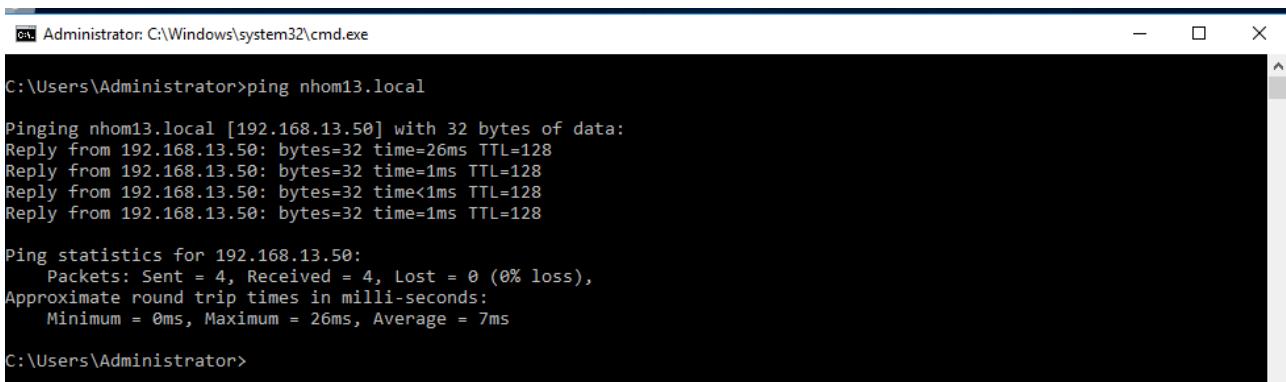
First name:	user1	Initials:	<input type="text"/>
Last name:	<input type="text"/>		
Full name:	user1		
User logon name:	<input type="text"/> user1	@nhom13.local	<input type="button" value="▼"/>
User logon name (pre-Windows 2000):	NHOM13\	user1	<input type="button" value=""/>

**< Back** **Next >** **Cancel**

## Lab 4: Triển khai Active Directory trên Windows Server

- Thêm File Server vào **File Server** domain đã tạo.

+ Trên máy, kiểm tra kết nối đến domain.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping nhom13.local

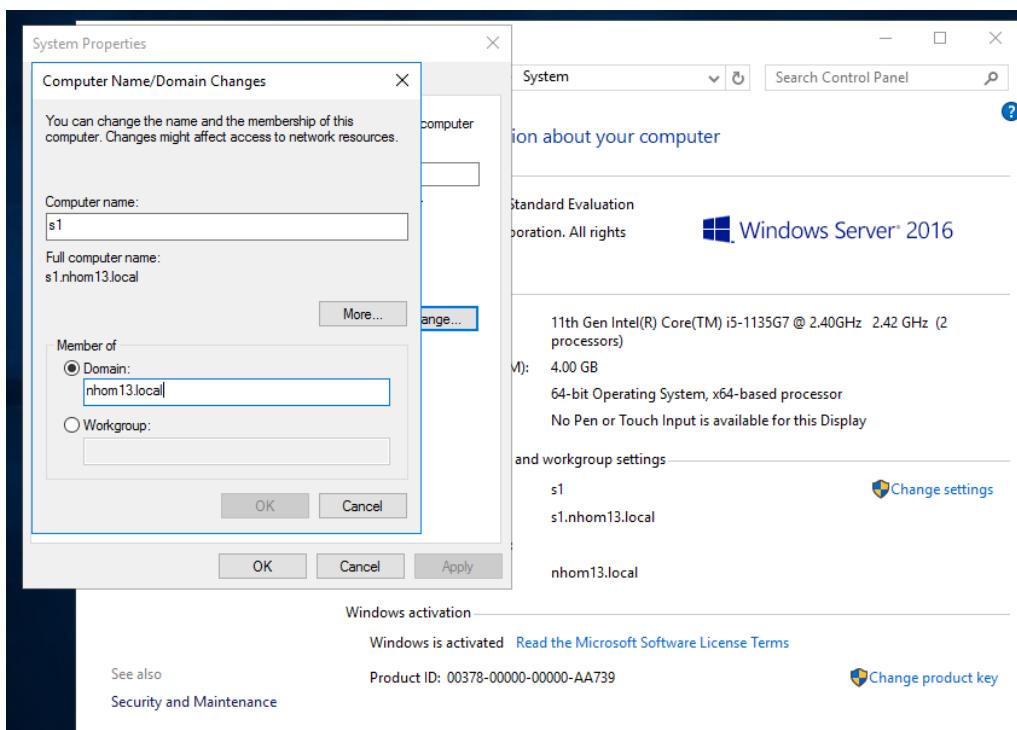
Pinging nhom13.local [192.168.13.50] with 32 bytes of data:
Reply from 192.168.13.50: bytes=32 time=26ms TTL=128
Reply from 192.168.13.50: bytes=32 time=1ms TTL=128
Reply from 192.168.13.50: bytes=32 time<1ms TTL=128
Reply from 192.168.13.50: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.13.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 26ms, Average = 7ms

C:\Users\Administrator>
```

+ Vào mục **System** trong **Control Panel**, sau đó sẽ xuất hiện ô cửa sổ **Settings**, chọn **Advanced system settings**.

+ Trong cửa sổ **System Properties**, tab **Computer Name**, chọn **Change**. Sau đó tại trường **Member of**, chọn **Domain** và nhập tên domain muốn tham gia



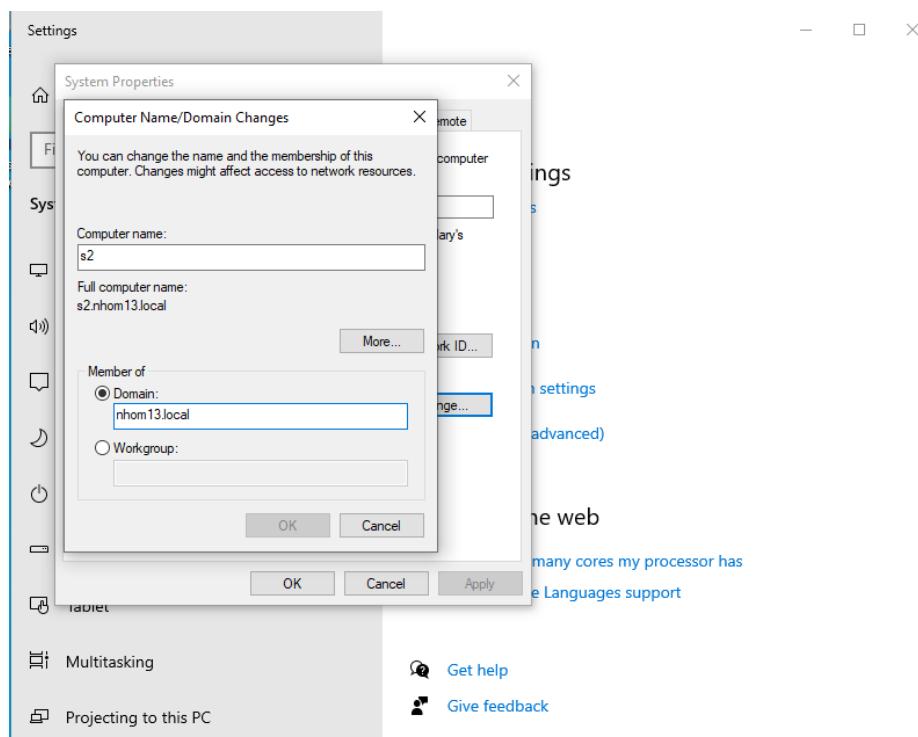
+ Sử dụng tài khoản tương ứng đã tạo trên Active Directory ở bước 3 để xác thực.

+ Xác thực thành công thì File Server sẽ được thêm vào domain.

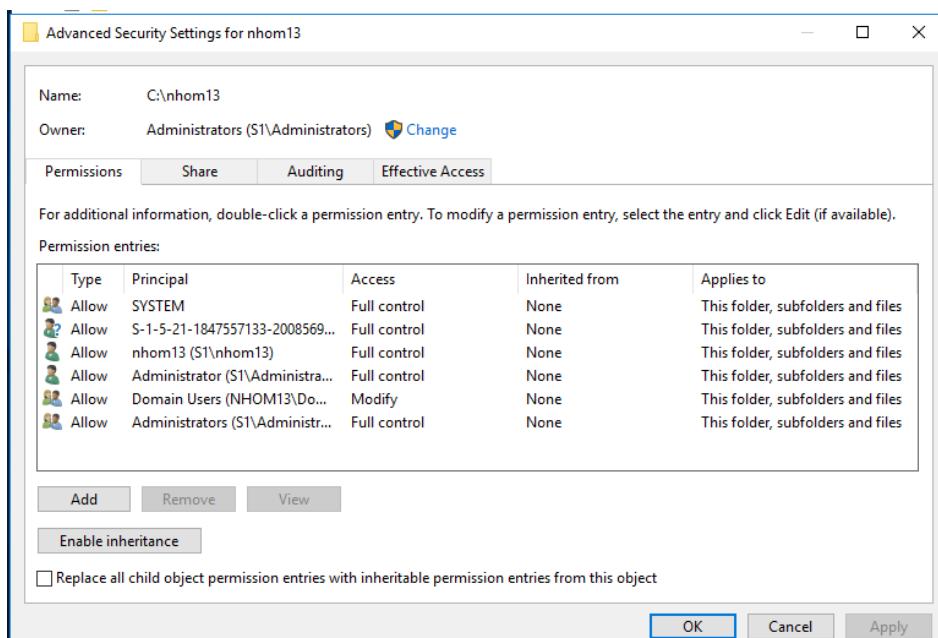
+ Sau khi quá trình này hoàn tất, tiến hành khởi động lại File Server.

## Lab 4: Triển khai Active Directory trên Windows Server

- Thêm máy client vào domain đã tạo (Tương tự các bước đối với File Server):

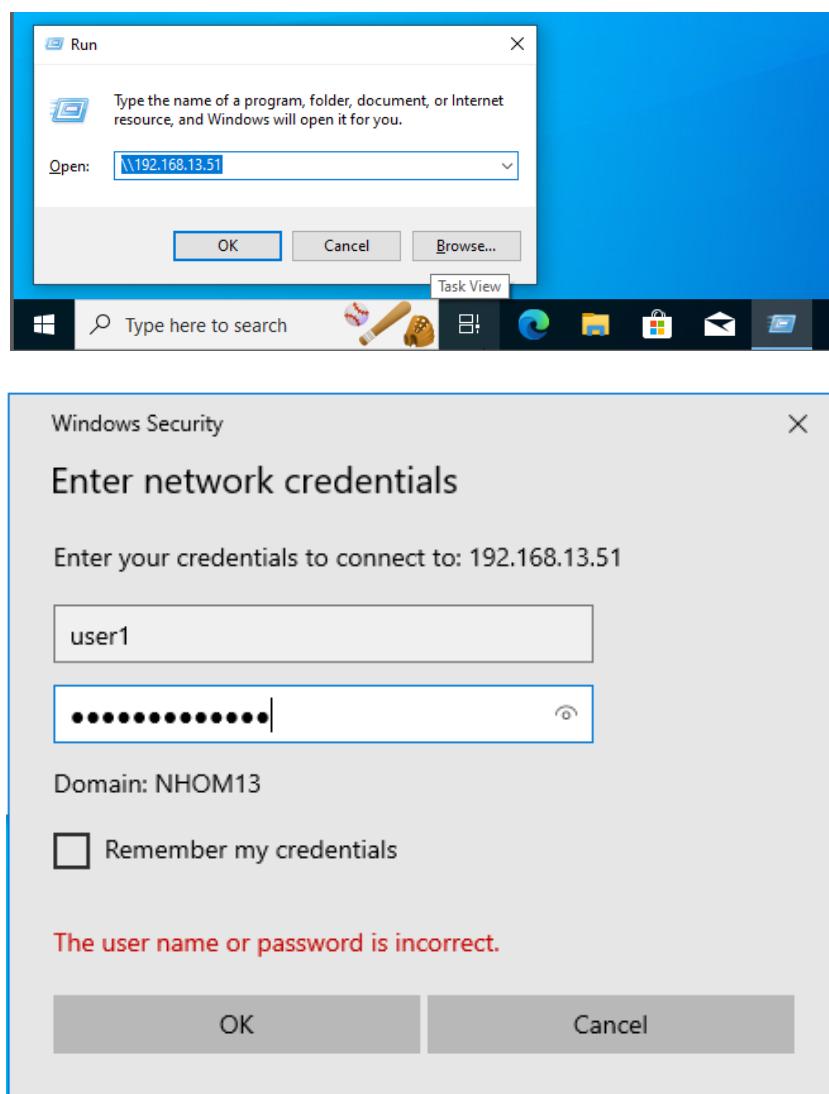


- Phân quyền và chia sẻ file từ File Server. Đăng nhập lại vào File Server và thực hiện phân quyền lại folder13 của File Server. Lưu ý: việc phân quyền có thể yêu cầu cần xác thực với 1 tài khoản user có quyền administrator trong domain (ví dụ administrator của AD).

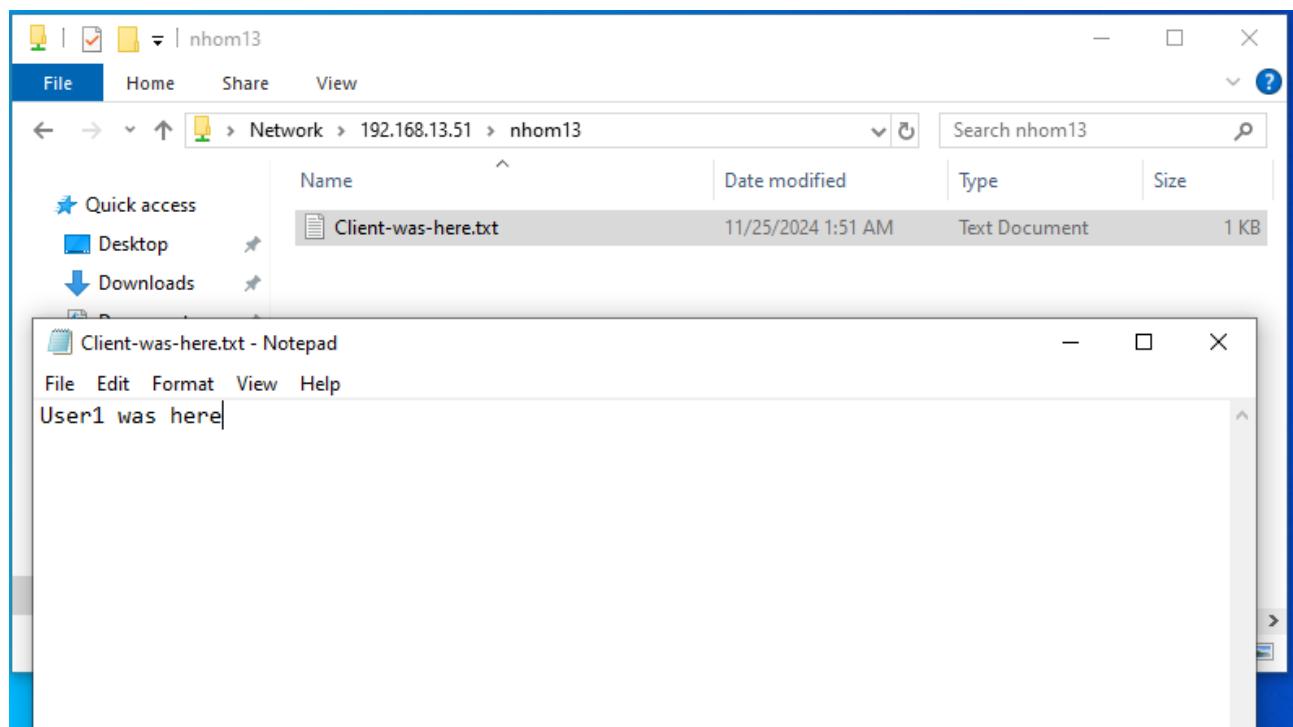


- Tại máy Client, đăng nhập với tài khoản NHOM13\user1 (tài khoản trong domain).
- Sau khi đăng nhập, trên Client vào Run và kết nối vào File Server. Kiểm tra các thao tác đọc, ghi dữ liệu tại thư mục này folder13 (giống với bài 1).

## Lab 4: Triển khai Active Directory trên Windows Server



- Thử sửa file Client-was-here.txt:



## Lab 4: Triển khai Active Directory trên Windows Server

- Trong Workgroup, mọi thứ phải được cấu hình thủ công và xác thực cục bộ, khiến việc quản lý trở nên khó khăn khi quy mô mạng lớn hơn. Trong Domain, việc quản lý tập trung và xác thực qua DC giúp đơn giản hóa việc quản lý và tăng cường bảo mật, đặc biệt khi làm việc với nhiều máy và nhiều người dùng.

### Bài 3: Xây dựng mô hình Additional Domain Controller cho dịch vụ Active Directory

**Yêu cầu 3.1.** Sinh viên hãy tìm hiểu và trả lời câu hỏi:

1. Additional Domain Controller (ADC) là gì?
2. Mô hình ADC hoạt động như thế nào?
3. Khi nào cần sử dụng ADC?

#### 1. Additional Domain Controller (ADC) là gì?

- Additional Domain Controller là một công cụ quan trọng dùng để cân bằng việc sử dụng giữa các domain controller hiện có. Các ADC cũng đóng vai trò trong việc có thể được dùng để xác thực lỗi, giúp cho các hoạt động kinh doanh của bạn được suôn sẻ hơn.

#### 2. Mô hình ADC hoạt động như thế nào?

- ADC sao chép thông tin từ Primary Domain Controller (PDC) và có thể được sử dụng để xác thực người dùng và máy tính nếu PDC không khả dụng.

- ADC hoạt động theo cách sau:

+ PDC sao chép thông tin AD của nó lên ADC theo lịch trình định kỳ

+ ADC lưu trữ thông tin AD được sao chép từ PDC

+ Nếu PDC bị lỗi, ADC có thể được sử dụng để xác thực người dùng và máy tính

- Điều này giúp đảm bảo rằng người dùng và máy tính vẫn có thể truy cập vào các tài nguyên miễn ngay cả khi có sự cố. ADC cũng có thể được sử dụng để cân bằng tải cho AD.

#### 3. Khi nào cần sử dụng ADC?

- Khi cần cân bằng tải cho hệ thống AD, cải thiện hiệu suất và giảm thời gian ngừng hoạt động.

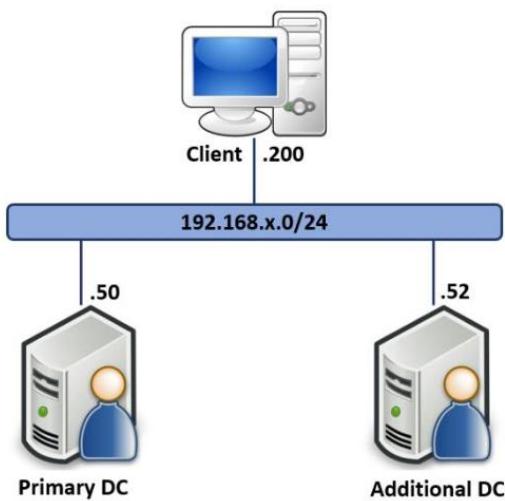
- Bảo vệ AD khỏi những kẻ tấn công bằng cách cung cấp một bản sao dự phòng của dữ liệu.

- Cân tăng khả năng chịu lỗi cho hệ thống AD.

## Lab 4: Triển khai Active Directory trên Windows Server

**Yêu cầu 3.2.** Sinh viên triển khai mô hình Additional Domain Controller theo yêu cầu bên dưới.

Mô hình cần xây dựng:



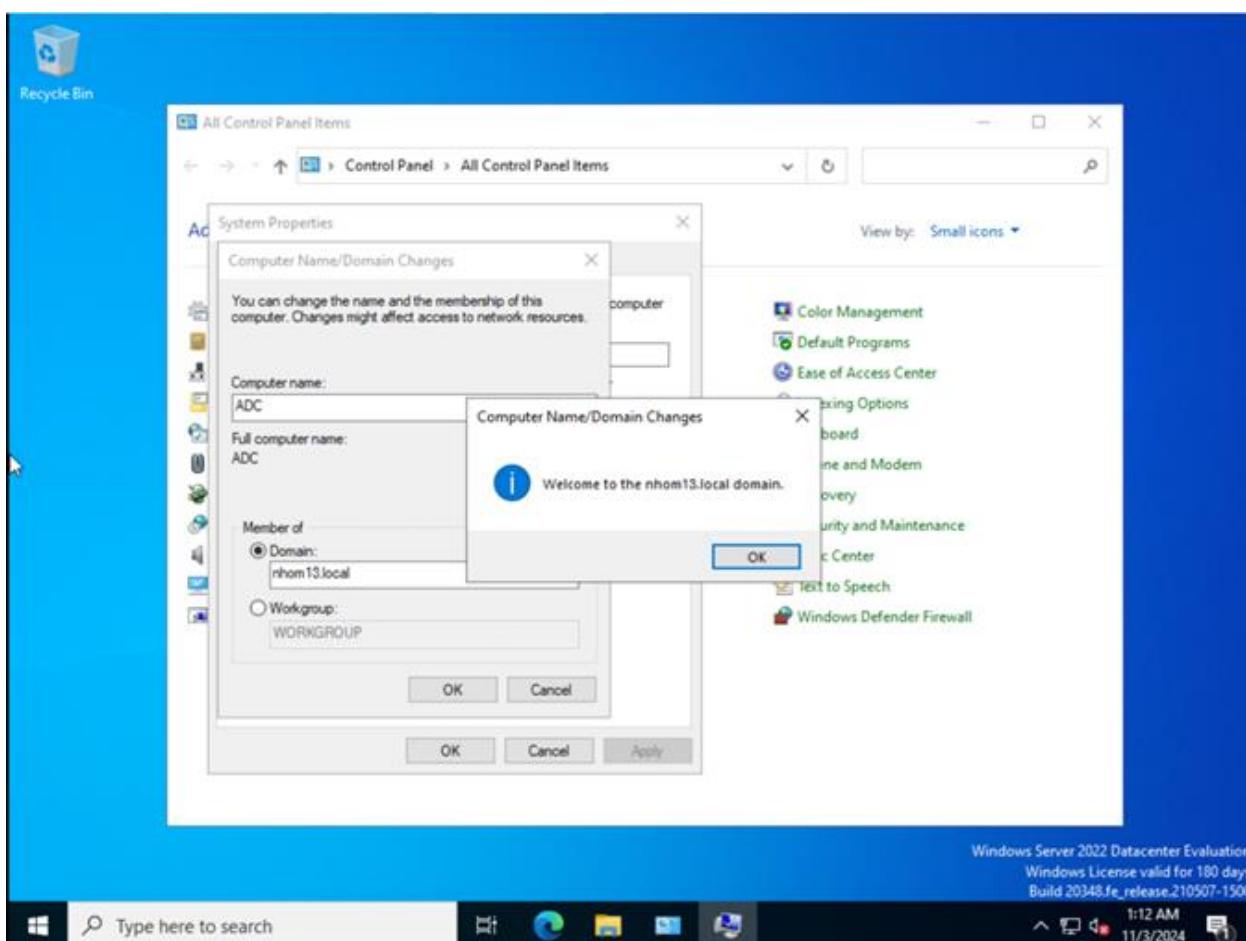
- Thông tin các máy như sau:

Tên máy	Hệ điều hành	Địa chỉ IP	DNS Server
Additional DC	Windows Server 2022	192.168.13.52/24	192.168.13.50 192.168.13.52
Primary DC	Windows Server 2022	192.168.13.50/24	192.168.13.50 192.168.13.52
Client	Windows 10 Pro	192.168.13.200/24	192.168.13.50 192.168.13.52

- Triển khai mô hình **Additional Domain Controller (ADC)** với thông tin trên.

+ Trước tiên ta thực hiện cấu hình lại DNS cho phù hợp với yêu cầu đề bài, tiếp đó ta thêm máy ADC vào domain nhom13.local

## Lab 4: Triển khai Active Directory trên Windows Server



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping nhom13.local

Pinging nhom13.local [192.168.13.50] with 32 bytes of data:
Reply from 192.168.13.50: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.13.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

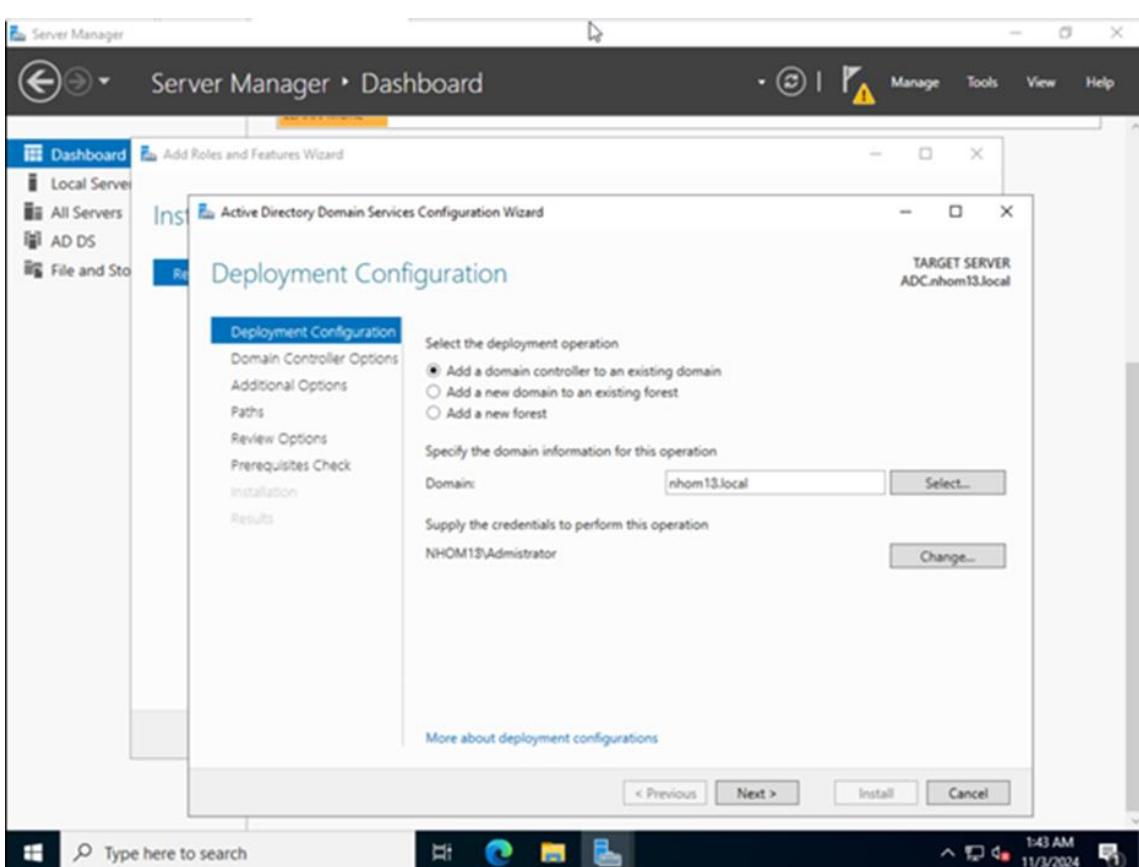
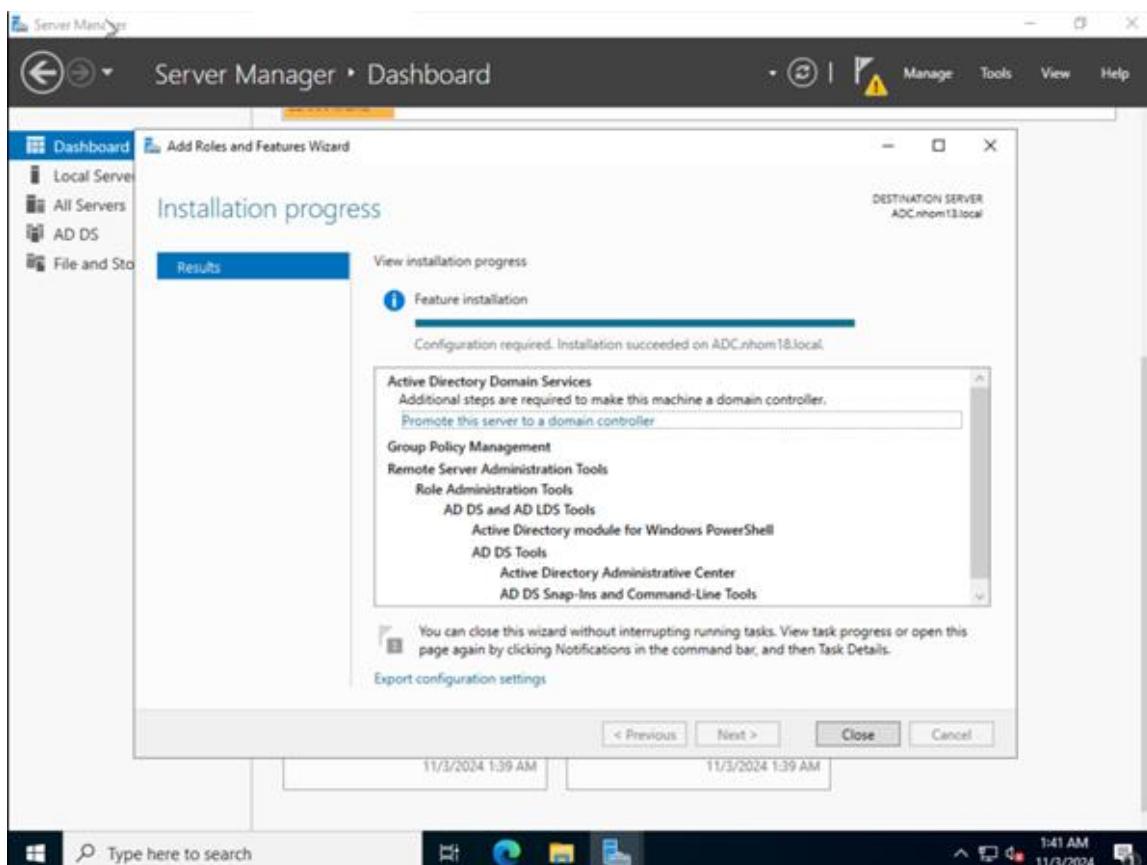
C:\Users\Administrator>
```

The screenshot shows a command-line window titled 'Administrator: C:\Windows\system32\cmd.exe'. The user has run the 'ping' command to the IP address 192.168.13.50. The output shows four successful replies with a minimum time of 1ms, maximum time of 1ms, and an average of 1ms. The status bar at the bottom indicates the server is running Windows Server 2022 Datacenter Evaluation with a valid license for 180 days.

## Lab 4: Triển khai Active Directory trên Windows Server

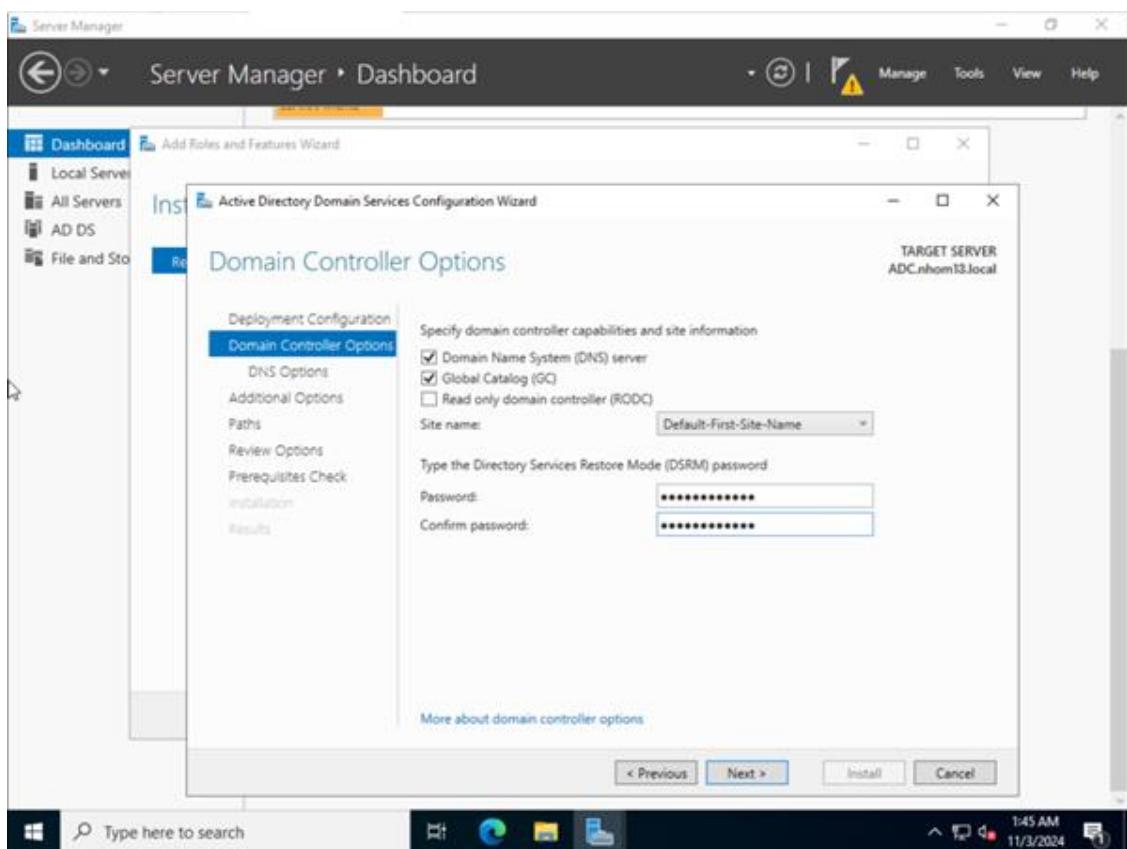
- Tiếp theo ta sẽ cấu hình máy thành ADC:

+ Bắt đầu cài đặt như yêu cầu 2 nhưng ở phần nâng cấp thành AD sẽ có khác biệt, ta chọn domain là nhom13.local, sau đó nhập username và password.

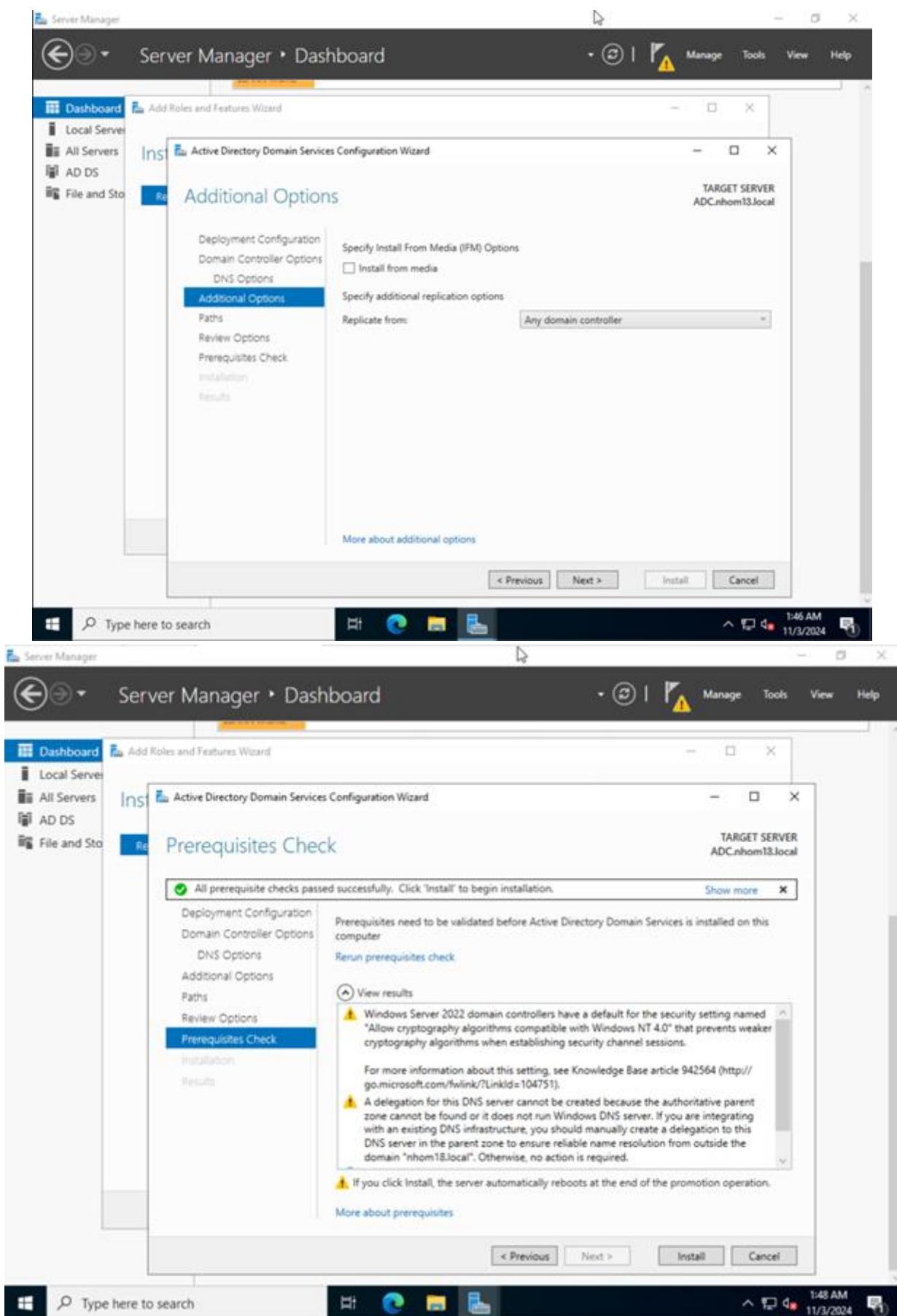


## Lab 4: Triển khai Active Directory trên Windows Server

+ Tại Domain controller options ta thực hiện cấu hình password cho DSRM.



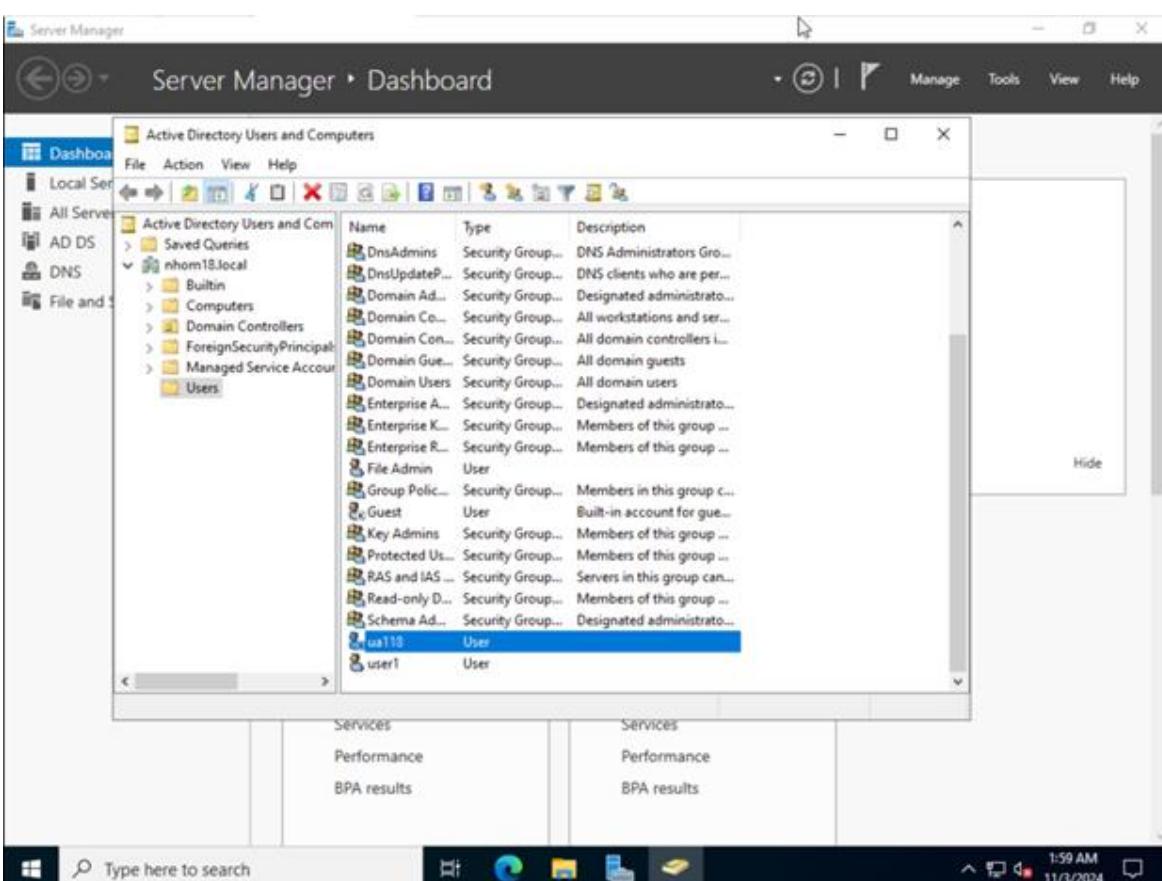
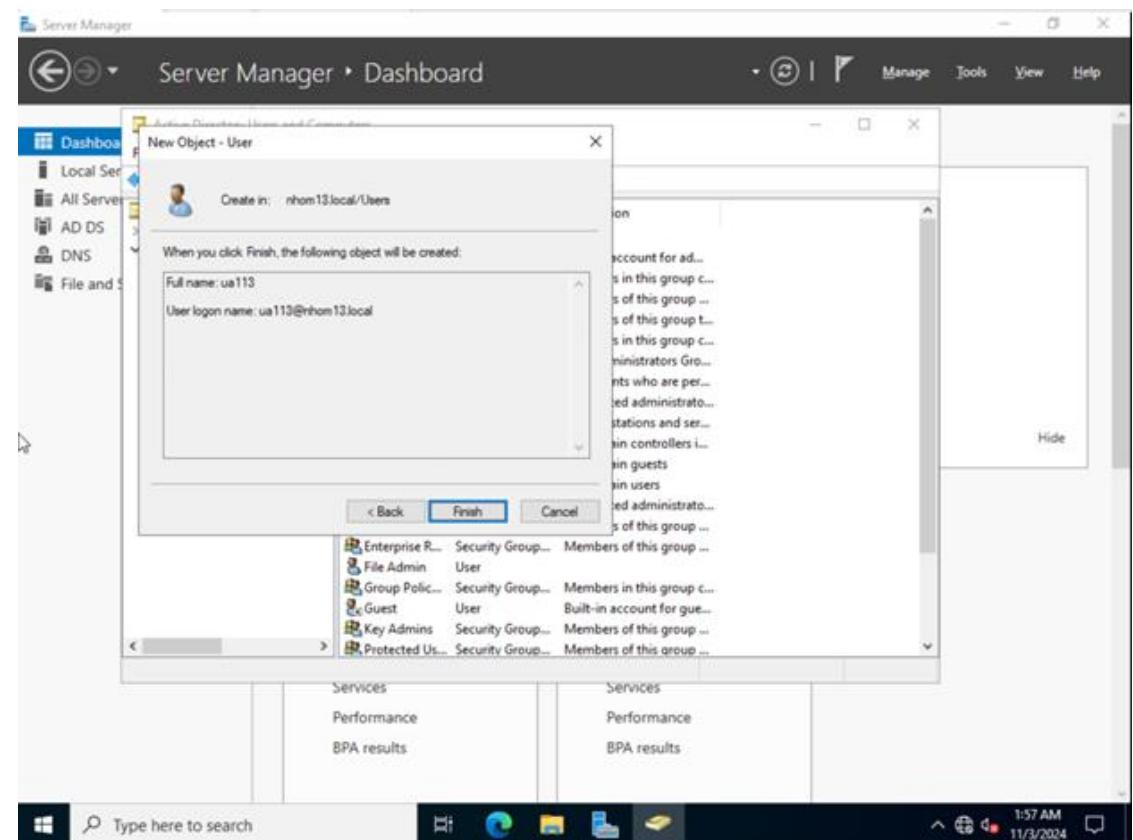
## Lab 4: Triển khai Active Directory trên Windows Server



- + Sau khi thực hiện bước cấu hình trên, máy sẽ tự động khởi động lại.
- Thực hiện các công việc sau và kiểm tra kết quả.

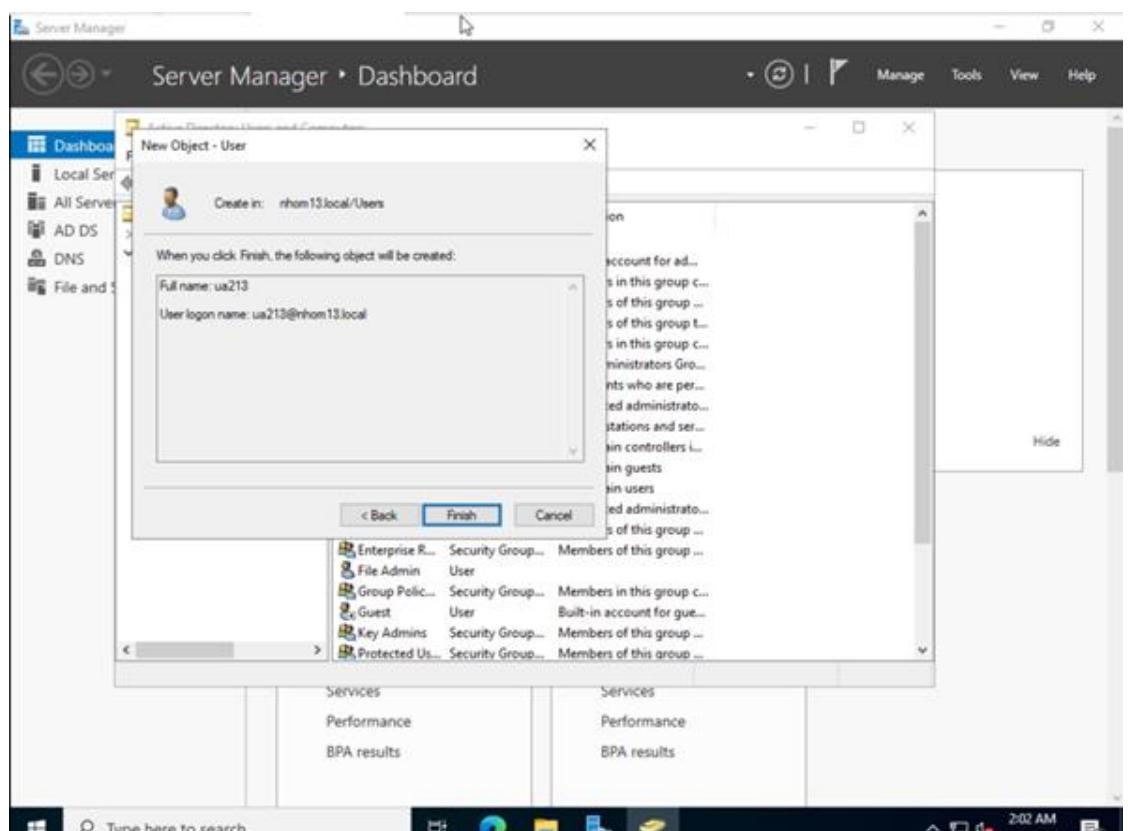
## Lab 4: Triển khai Active Directory trên Windows Server

- + Tạo user **ua113** trên Primary DC. Kiểm tra thông tin user này trên Additional DC.

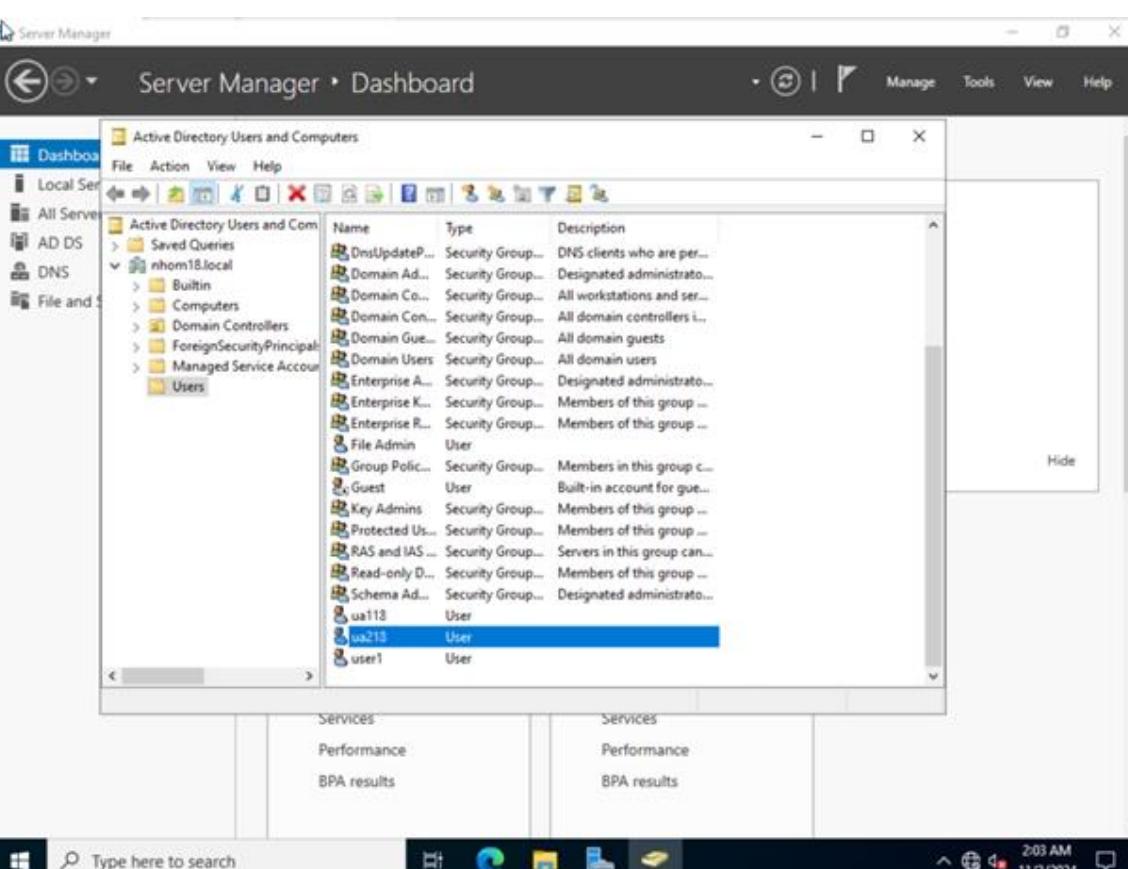


## Lab 4: Triển khai Active Directory trên Windows Server

- + Tạo user **ua213** trên Additional DC. Kiểm tra thông tin user này trên Primary DC.



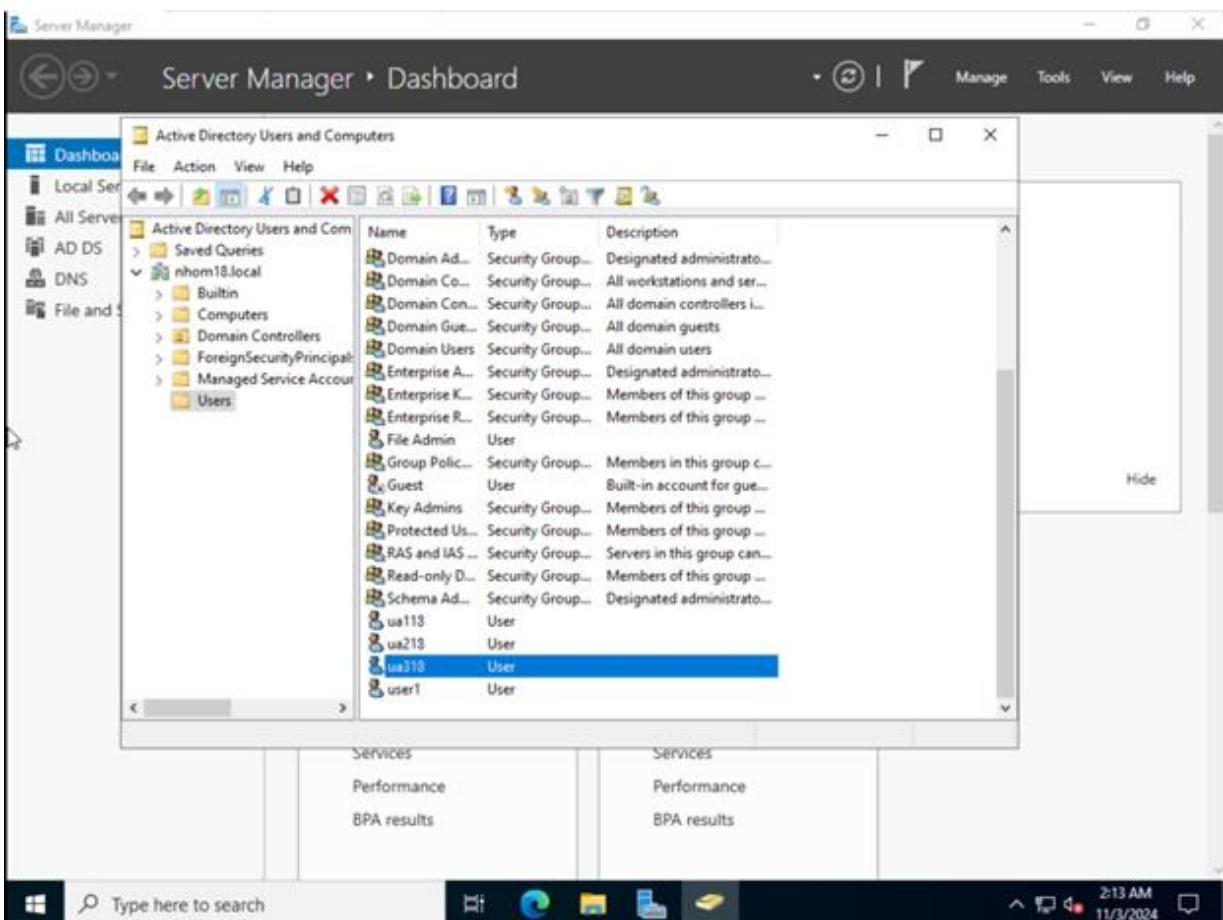
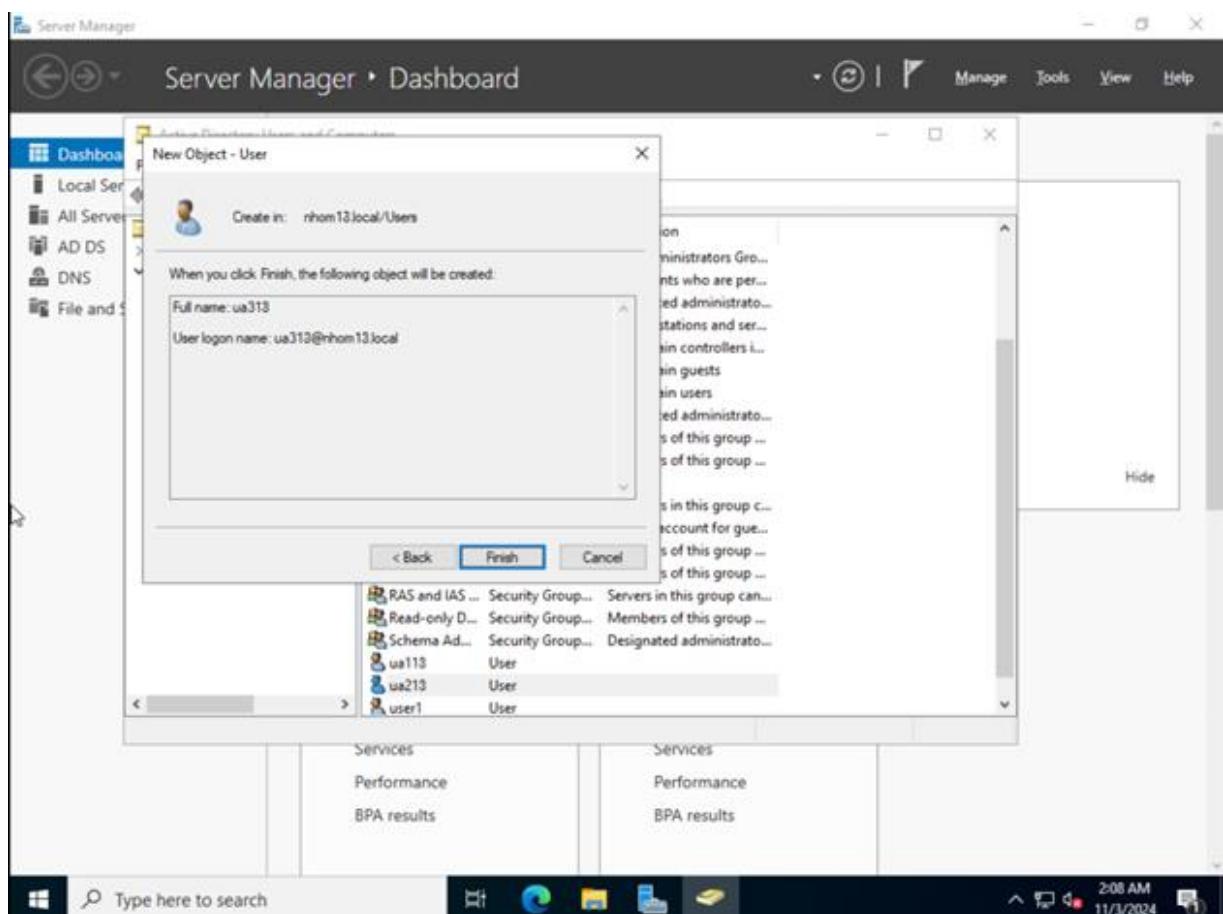
The screenshot shows the Windows Server Manager Dashboard. A modal window titled "New Object - User" is open, prompting for a full name ("ua213") and a logon name ("ua213@nhom13.local"). Below the input fields is a list of security groups: Enterprise R..., Security Group..., Members of this group ...; File Admin..., User; Group Policy..., Security Group..., Members in this group c...; Guest, User, Built-in account for gue...; Key Admins, Security Group..., Members of this group ...; Protected Us..., Security Group..., Members of this group ... . At the bottom of the modal are "Back", "Finish", and "Cancel" buttons. The main dashboard below shows sections for Services, Performance, and BPA results.

The screenshot shows the Active Directory Users and Computers console under the "Active Directory Users and Computers" section. The left navigation pane shows the tree structure: Active Directory Users and Computers > nhom13.local > Users. The right pane displays a list of users and groups. The user "ua213" is highlighted in blue, indicating it was recently selected or created. Other users listed include ua113, user1, and user2. The bottom of the screen shows the Windows taskbar with the date and time as 11/3/2024 at 2:03 AM.

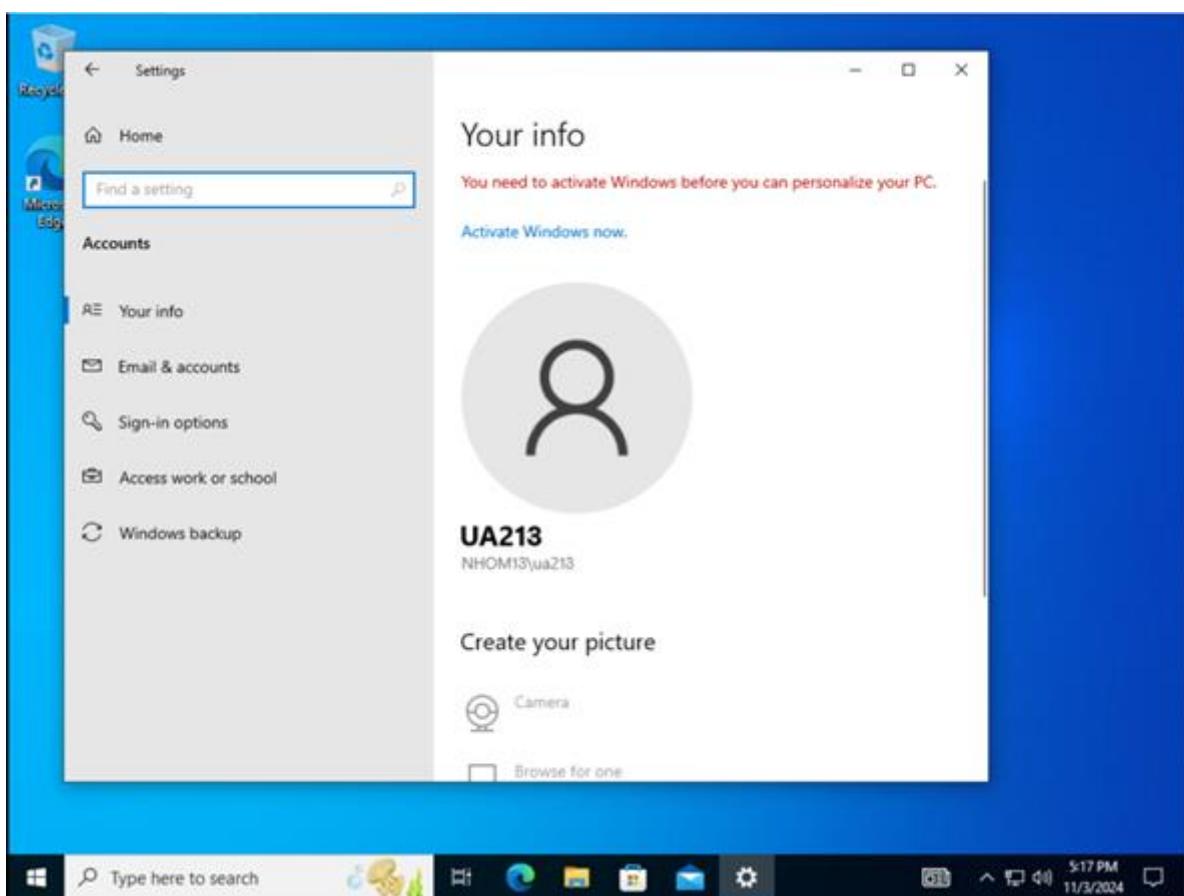
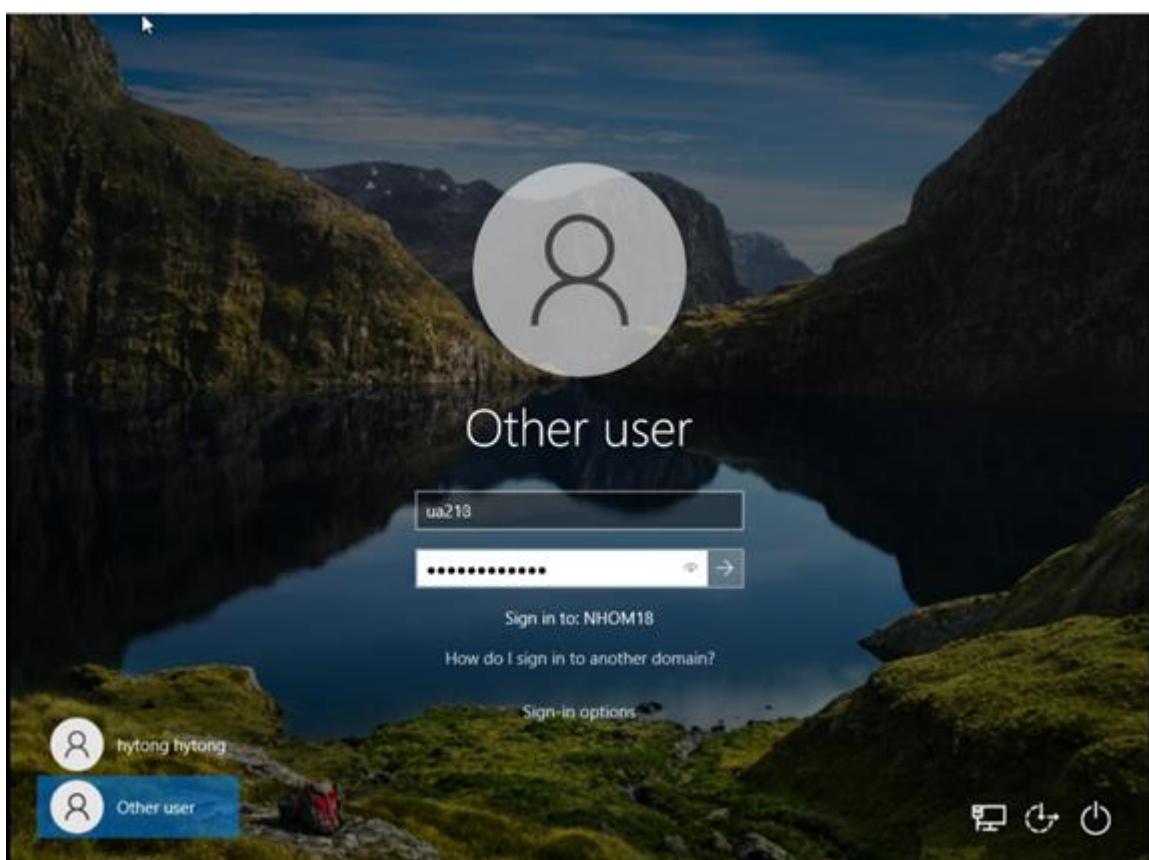
- + Tắt máy Primary DC, thêm user **ua313** trên Additional DC. Sau đó mở lại Primary DC và kiểm tra thông tin user này trên Primary DC.

## Lab 4: Triển khai Active Directory trên Windows Server



+ Tắt máy Primary DC, login ua213 trên máy Client. Giải thích kết quả.

## Lab 4: Triển khai Active Directory trên Windows Server



---

#### Lab 4: Triển khai Active Directory trên Windows Server

*Giải thích:* Ta thấy rằng, khi PDC đăng ở trạng thái không hoạt động thì tài khoản ua213 vẫn có thể đăng nhập được trên máy Client, điều này đồng nghĩa với việc ADC đã thay PDC thực hiện đăng nhập trong khi PDC không hoạt động

**Bài 4: Xây dựng mô hình Read-Only Domain Controller**

**Yêu cầu 4.1** Sinh viên hãy tìm hiểu và trả lời câu hỏi:

1. Read-Only Domain Controller (RODC) là gì?
2. Mô hình RODC hoạt động như thế nào?
3. Khi nào cần sử dụng RODC?
4. So sánh sự khác nhau giữa mô hình ADC và mô hình RODC?

**1. Read-Only Domain Controller (RODC) là gì?**

- Read Only Domain Controller (RODC) là một loại Domain Controller (DC) trong hệ thống Windows Domain. RODC sẽ được thiết kế để triển khai trong các vị trí có môi trường không đảm bảo về bảo mật, như các chi nhánh, văn phòng nhỏ hoặc các môi trường có nguy cơ bị tấn công.

**2. Mô hình RODC hoạt động như thế nào?**

- Read Only Domain Controller (RODC) sẽ hoạt động theo các nguyên tắc sau:
  - + Tạo bản sao dữ liệu Active Directory (AD)
  - + Xác thực và ủy quyền địa phương
  - + Replikasi dữ liệu từ PCD
  - + Ghi nhận các yêu cầu ghi dữ liệu
  - + Bảo vệ dữ liệu tối đa

**3. Khi nào cần sử dụng RODC?**

- Chi nhánh văn phòng hoặc địa điểm từ xa không đáng tin cậy - Mạng có kết nối chậm hoặc không ổn định
- Khi muốn giảm tải cho Domain Controller chính
- Bảo vệ dữ liệu mật khẩu nhạy cảm
- Khi yêu cầu truy cập chỉ đọc với dữ liệu Active Directory
- Đáp ứng nhu cầu quản lý tập trung và giám sát quyền hạn

**4. So sánh sự khác nhau giữa mô hình ADC và mô hình RODC?**

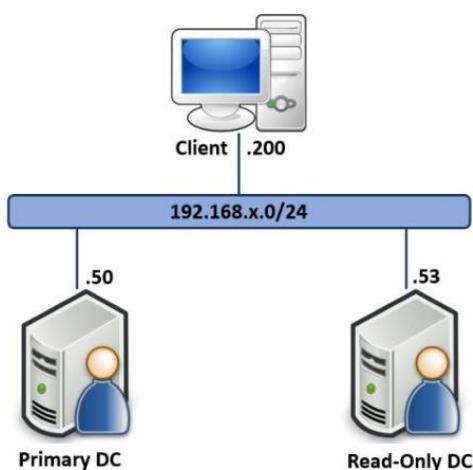
ADC (Additional Domain Controller)	RODC (Read-Only Domain Controller)
Sao lưu dữ liệu đầy đủ từ Domain Controller chính	Sao lưu dữ liệu chỉ đọc, không có khả năng ghi

#### Lab 4: Triển khai Active Directory trên Windows Server

Có thể ghi, tạo, xóa, chỉnh sửa đối tượng trong AD	Chỉ đọc, không thể chỉnh sửa dữ liệu
Có nguy cơ bảo mật cao hơn do có khả năng ghi và thay đổi dữ liệu	Bảo mật cao hơn, thích hợp cho môi trường không đáng tin cậy
Thực hiện chuyển đổi dữ liệu đầy đủ giữa các Domain Controller	Chỉ đồng bộ dữ liệu cần thiết từ Domain Controller chính
Thực hiện đầy đủ xác thực người dùng và máy tính	Chỉ thực hiện xác thực được ủy quyền, không hoàn chỉnh như ADC
Lưu trữ đầy đủ mật khẩu và thông tin xác thực	Không lưu mật khẩu mặc định, có thể tùy chọn lưu một phần mật khẩu
Dành cho các mạng tin cậy cao, ví dụ như văn phòng chính	Dành cho các mạng tin cậy cao, ví dụ như văn phòng chính
Có thể khôi phục lại các thay đổi từ dữ liệu khác	Không thể khôi phục, vì không thực hiện các thay đổi dữ liệu
Toàn quyền truy cập vào dữ liệu AD	Chỉ có quyền truy cập hạn chế, chỉ đọc
Đồng bộ tức thời với Domain Controller chính	Đồng bộ có thể chậm hơn do chỉ tải dữ liệu cần thiết

**Yêu cầu 4.2** Sinh viên triển khai mô hình Read-Only Domain Controller theo yêu cầu bên dưới.

#### Mô hình cần xây dựng:

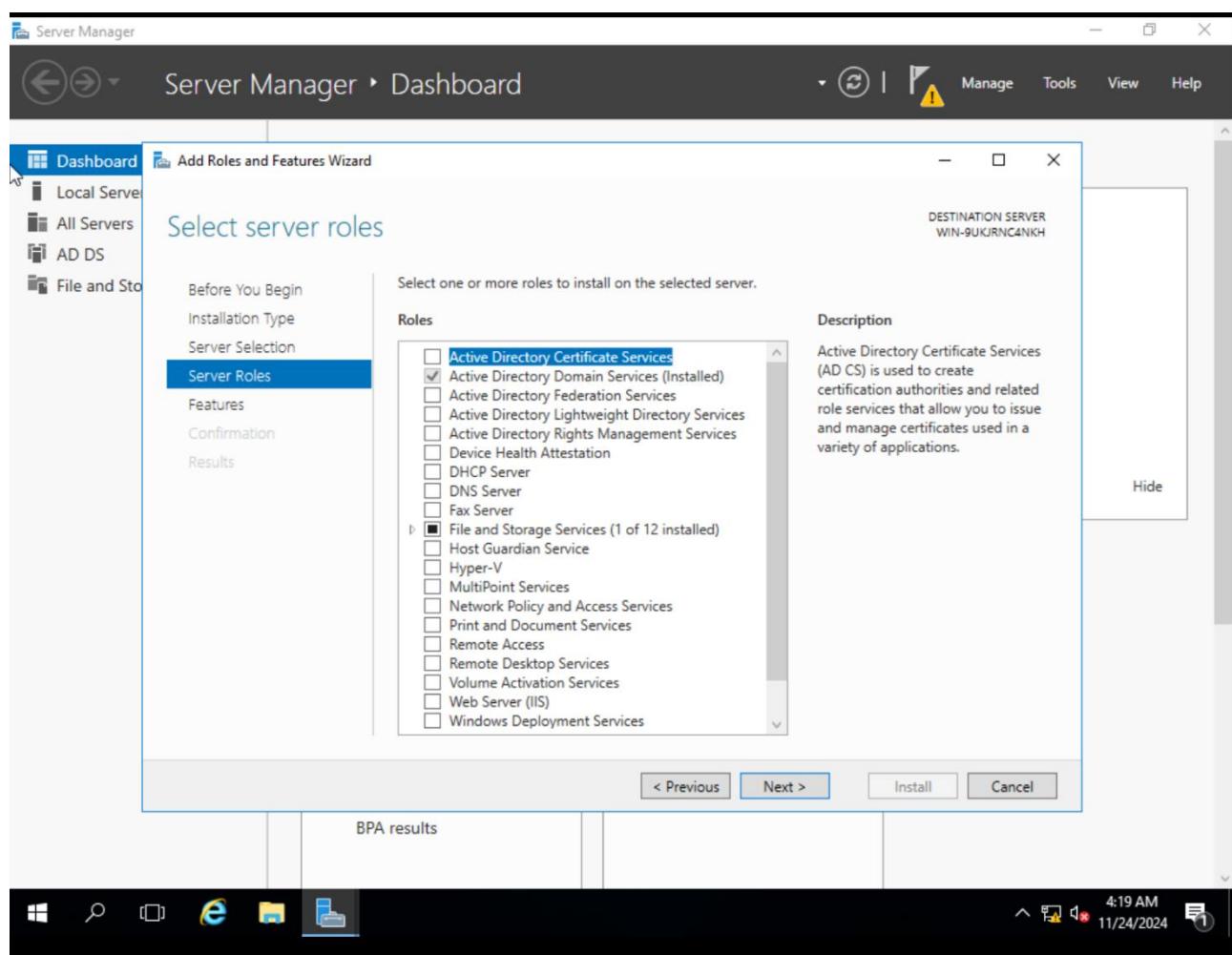


## Lab 4: Triển khai Active Directory trên Windows Server

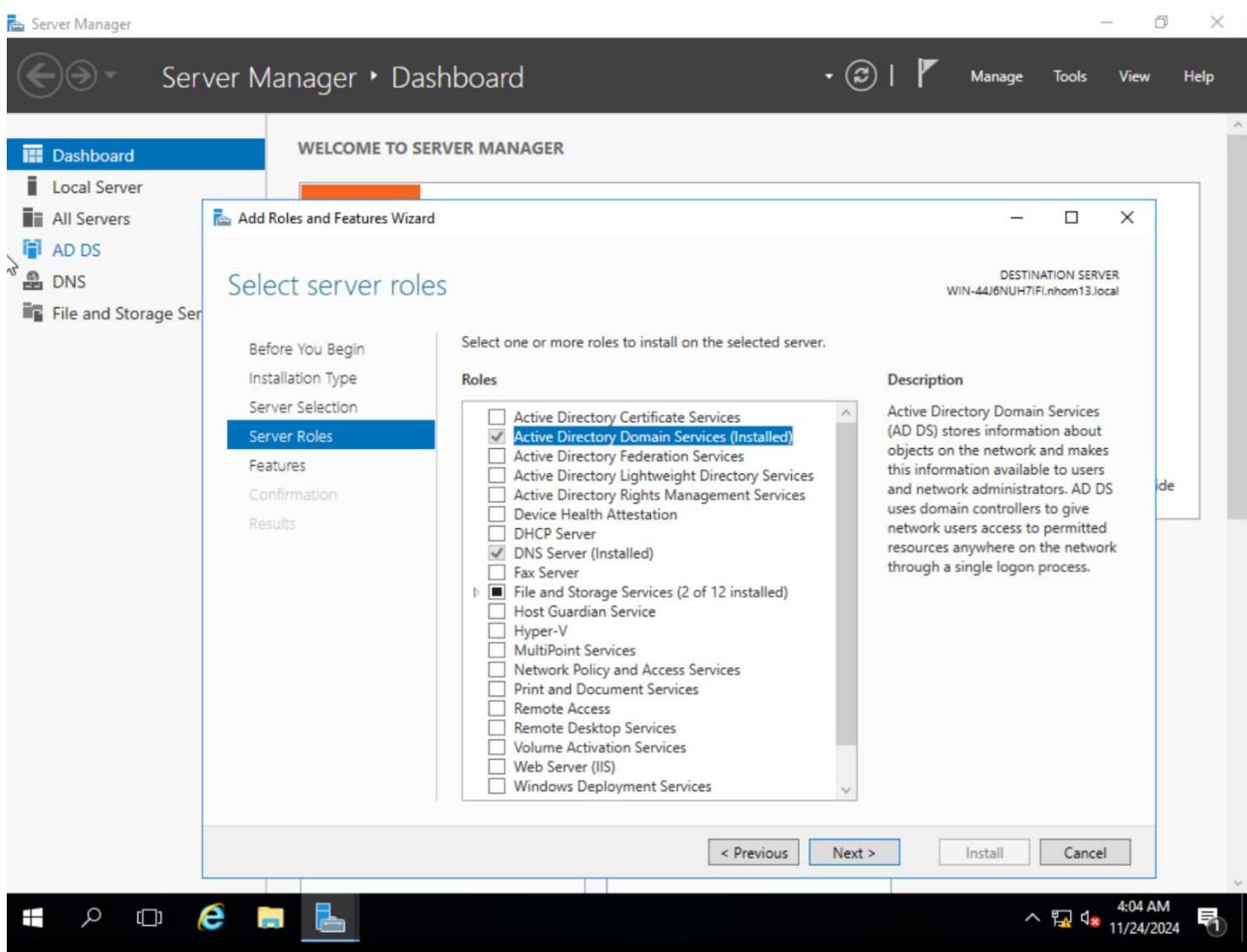
- Thông tin các máy như sau:

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 10	192.168.13.200/24	192.168.13.53
			192.168.13.50
Primary DC	Windows Server 2016	192.168.13.50/24	192.168.13.53
			192.168.13.50
Read-Only DC	Windows Server 2016	192.168.13.53/24	192.168.13.53
			192.168.13.50

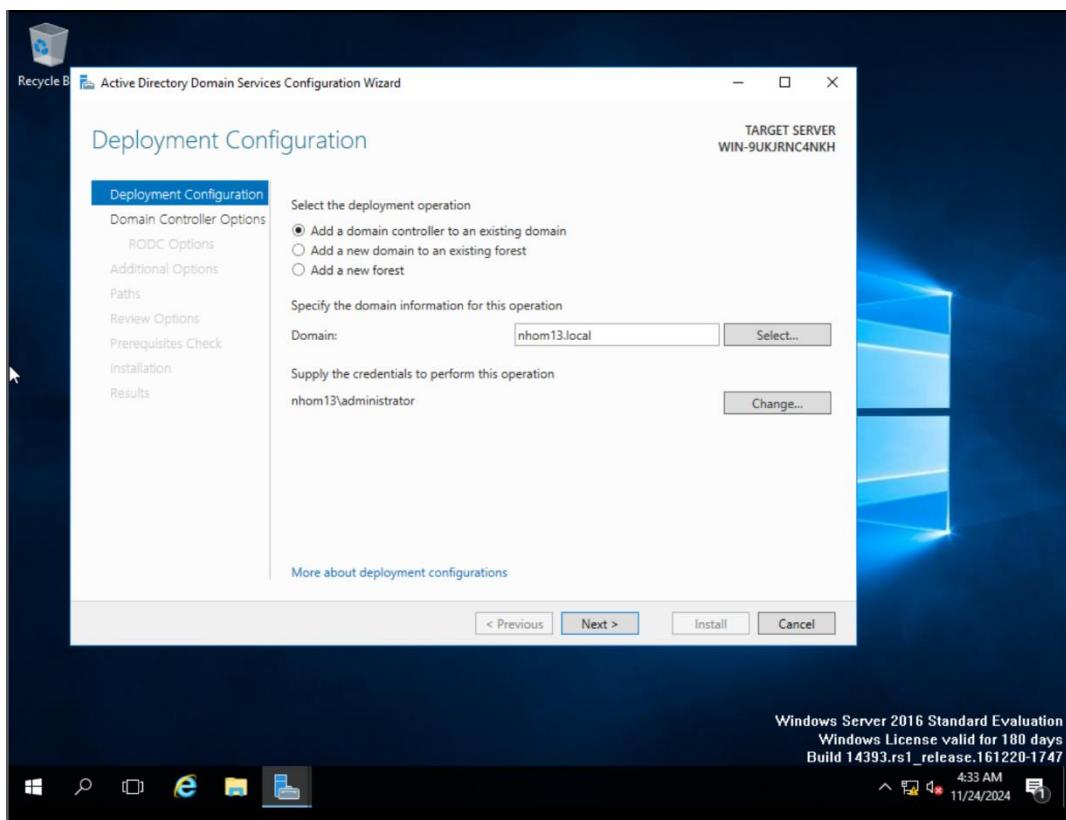
- Cài đặt role trên RODC và PDC:



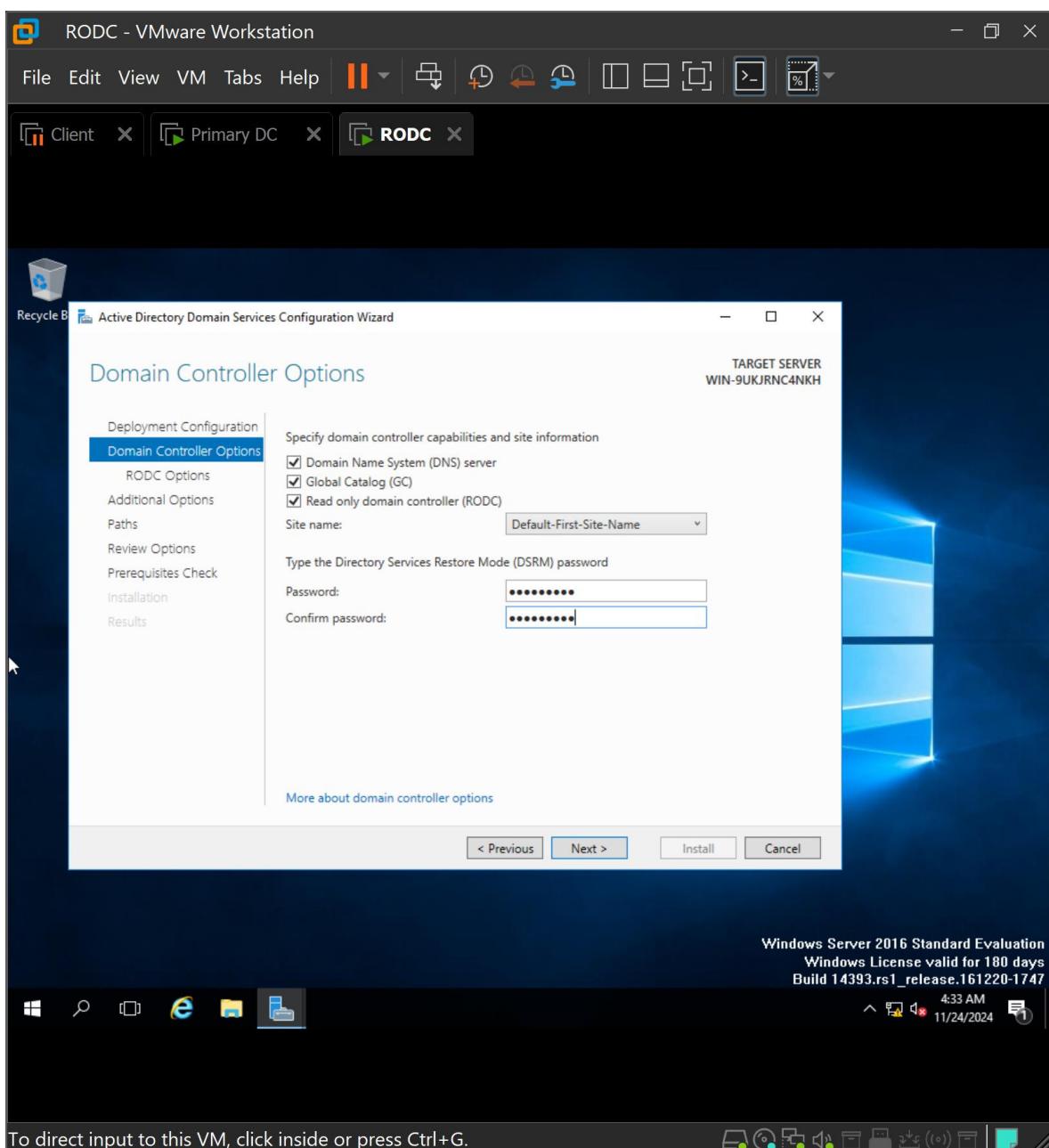
## Lab 4: Triển khai Active Directory trên Windows Server



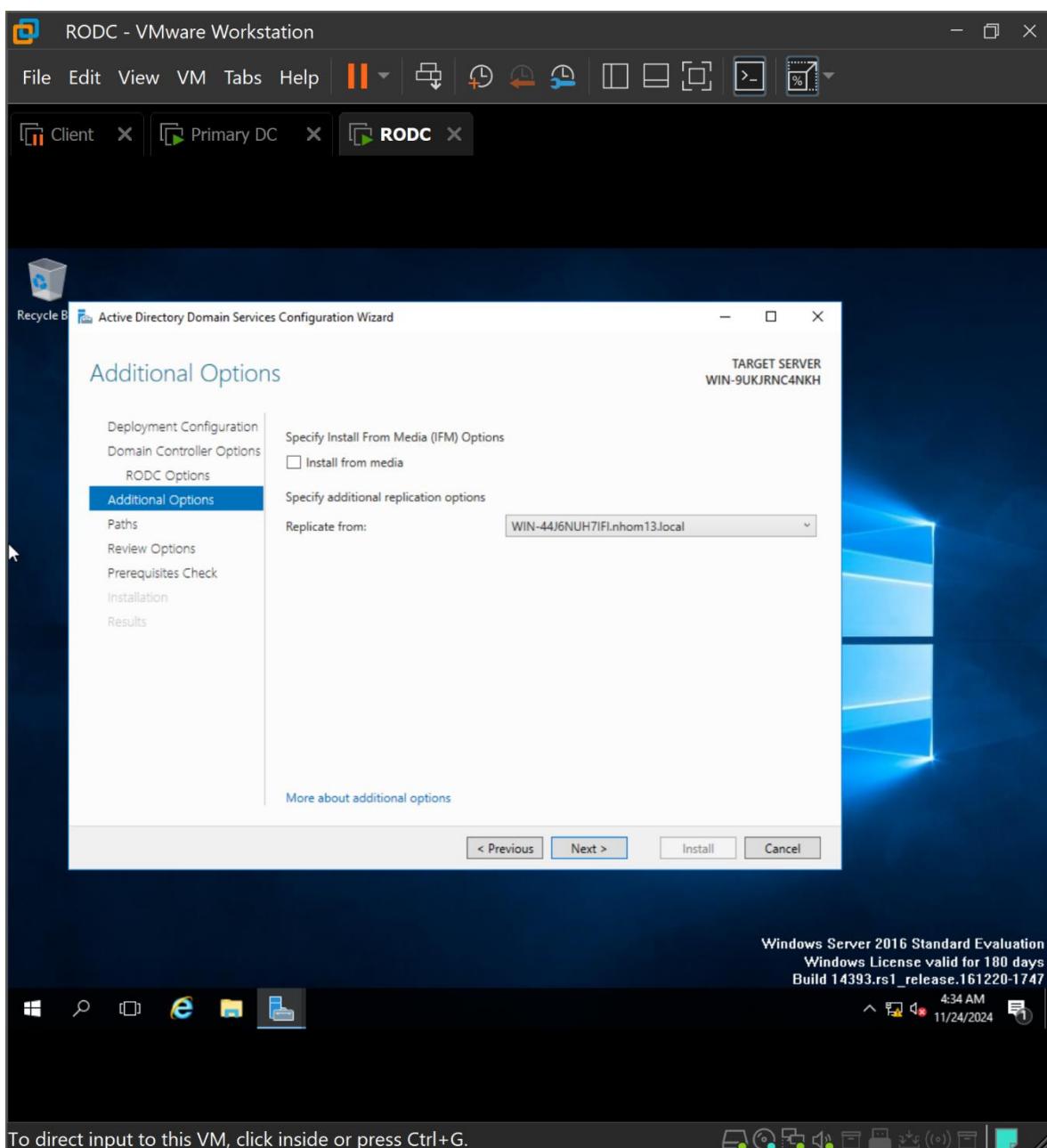
- Chính trên RODC:



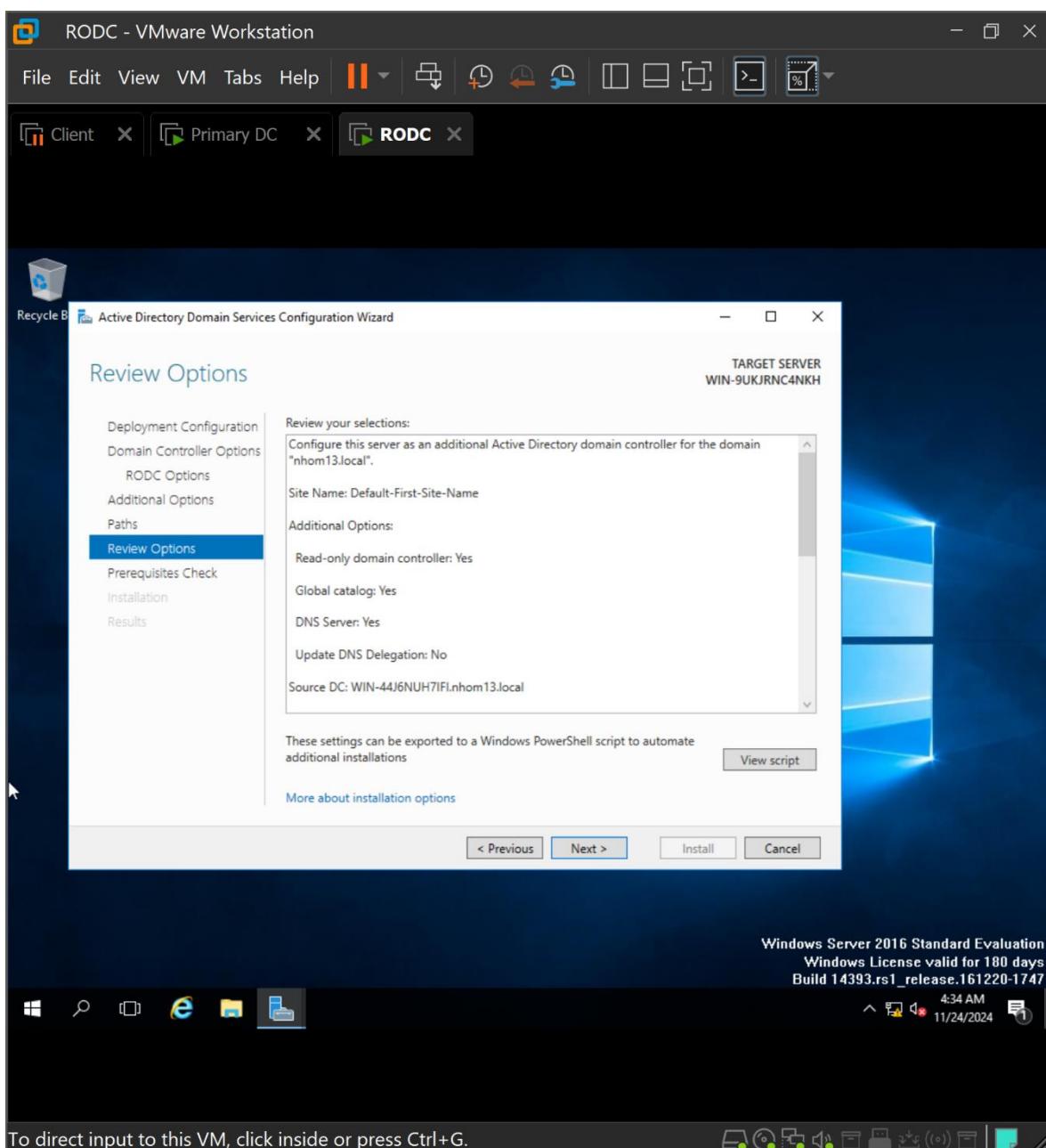
## Lab 4: Triển khai Active Directory trên Windows Server



## Lab 4: Triển khai Active Directory trên Windows Server

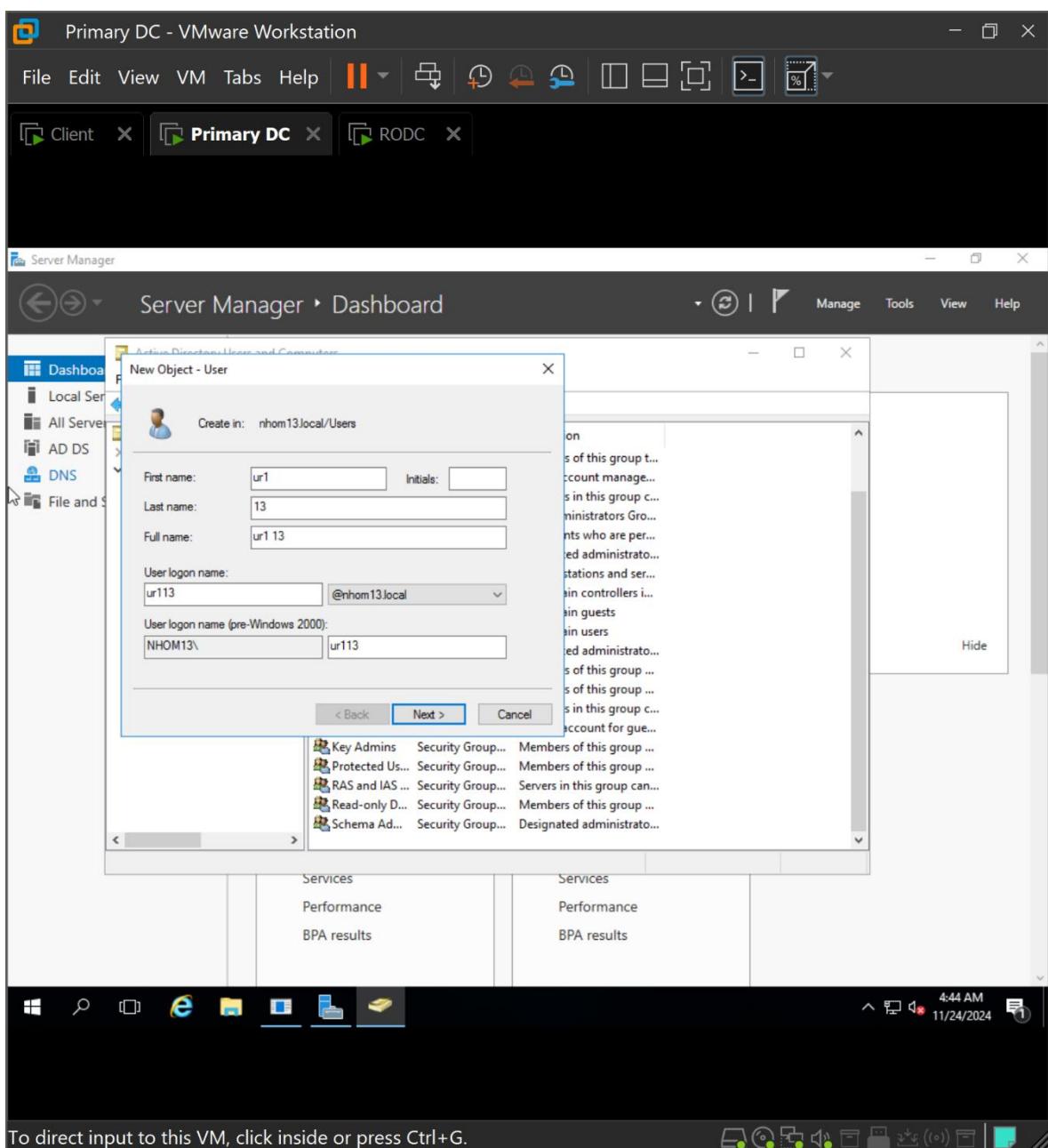


## Lab 4: Triển khai Active Directory trên Windows Server

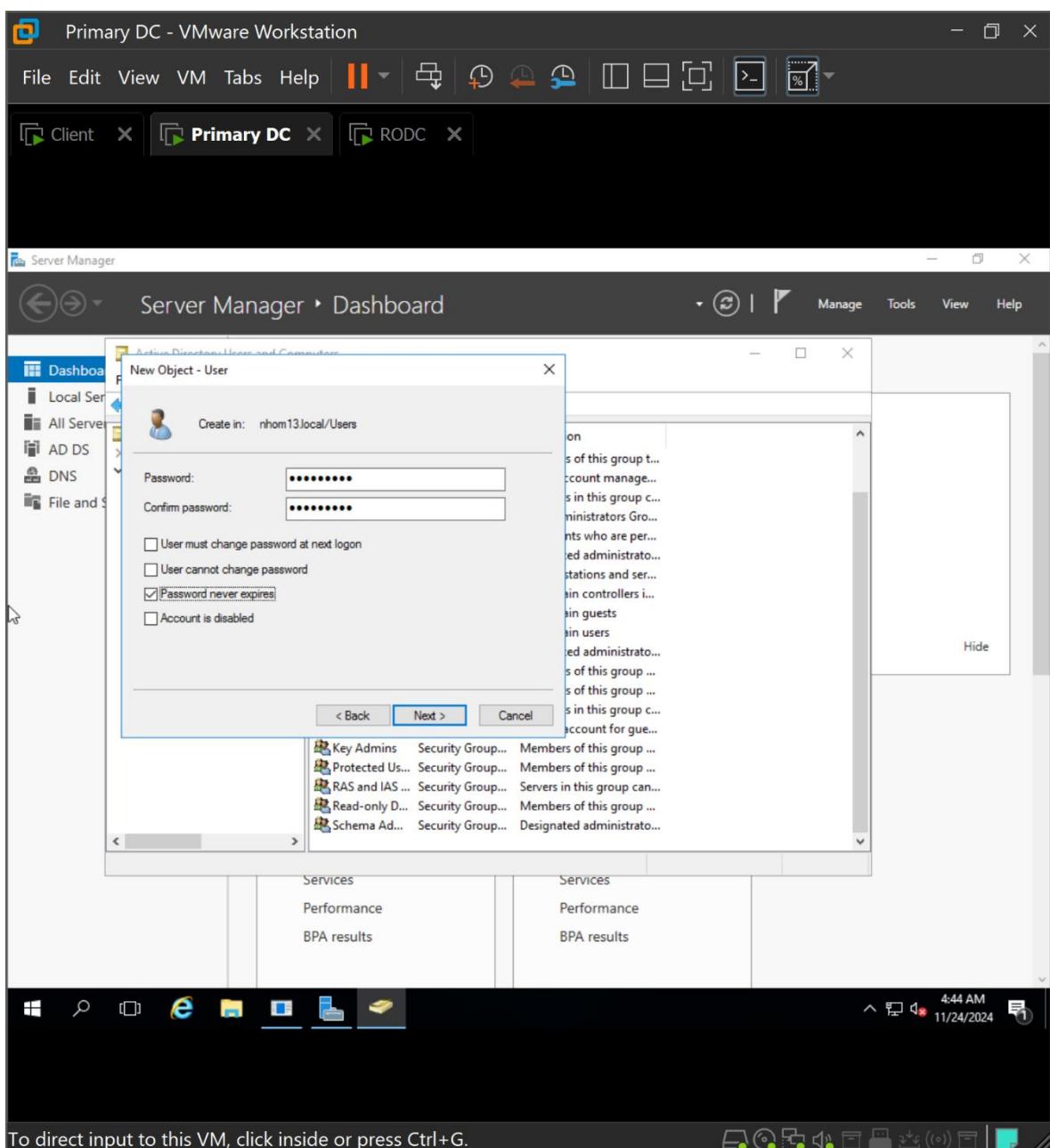


- Tạo ur113 trên PDC

## Lab 4: Triển khai Active Directory trên Windows Server

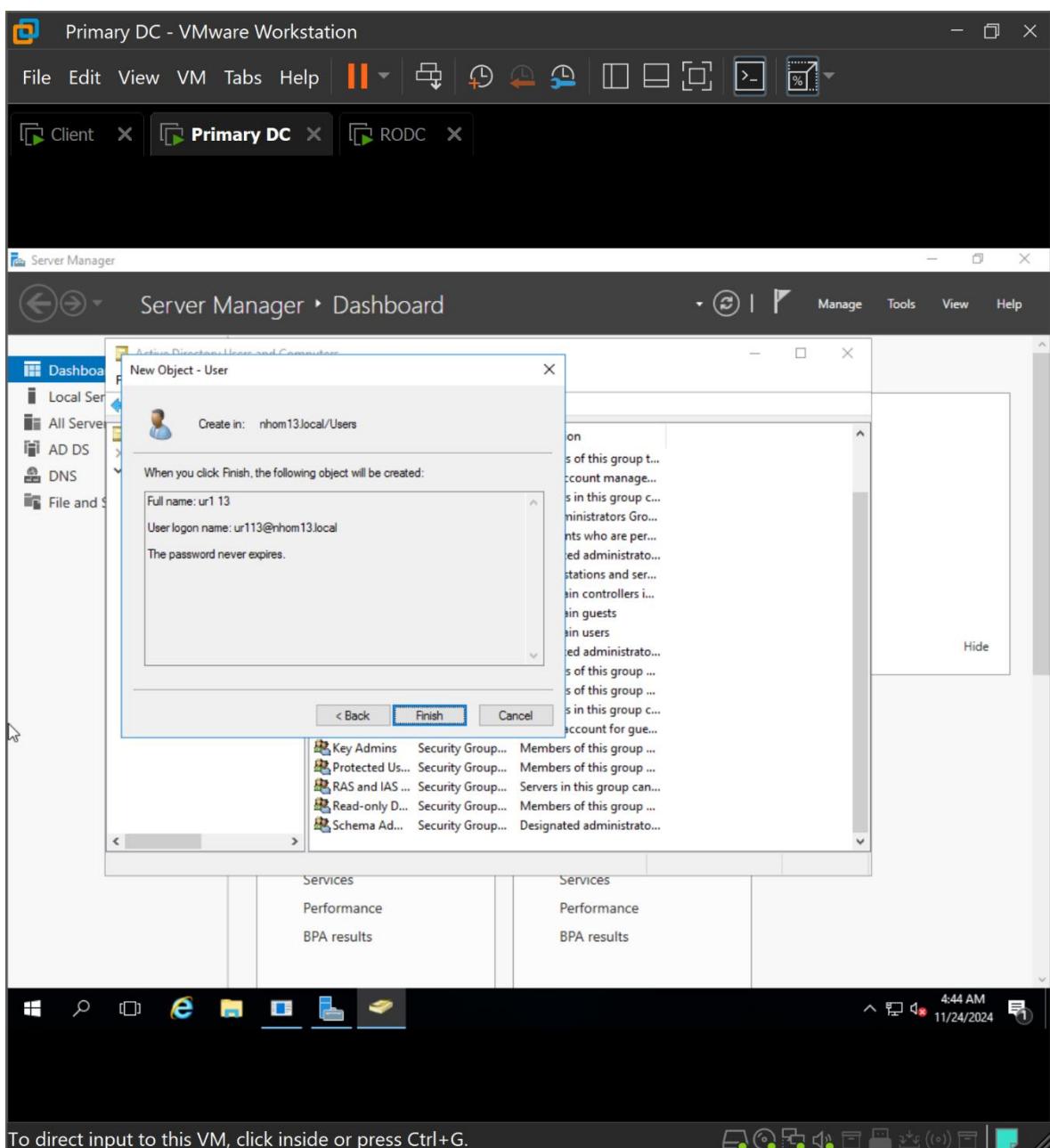


## Lab 4: Triển khai Active Directory trên Windows Server



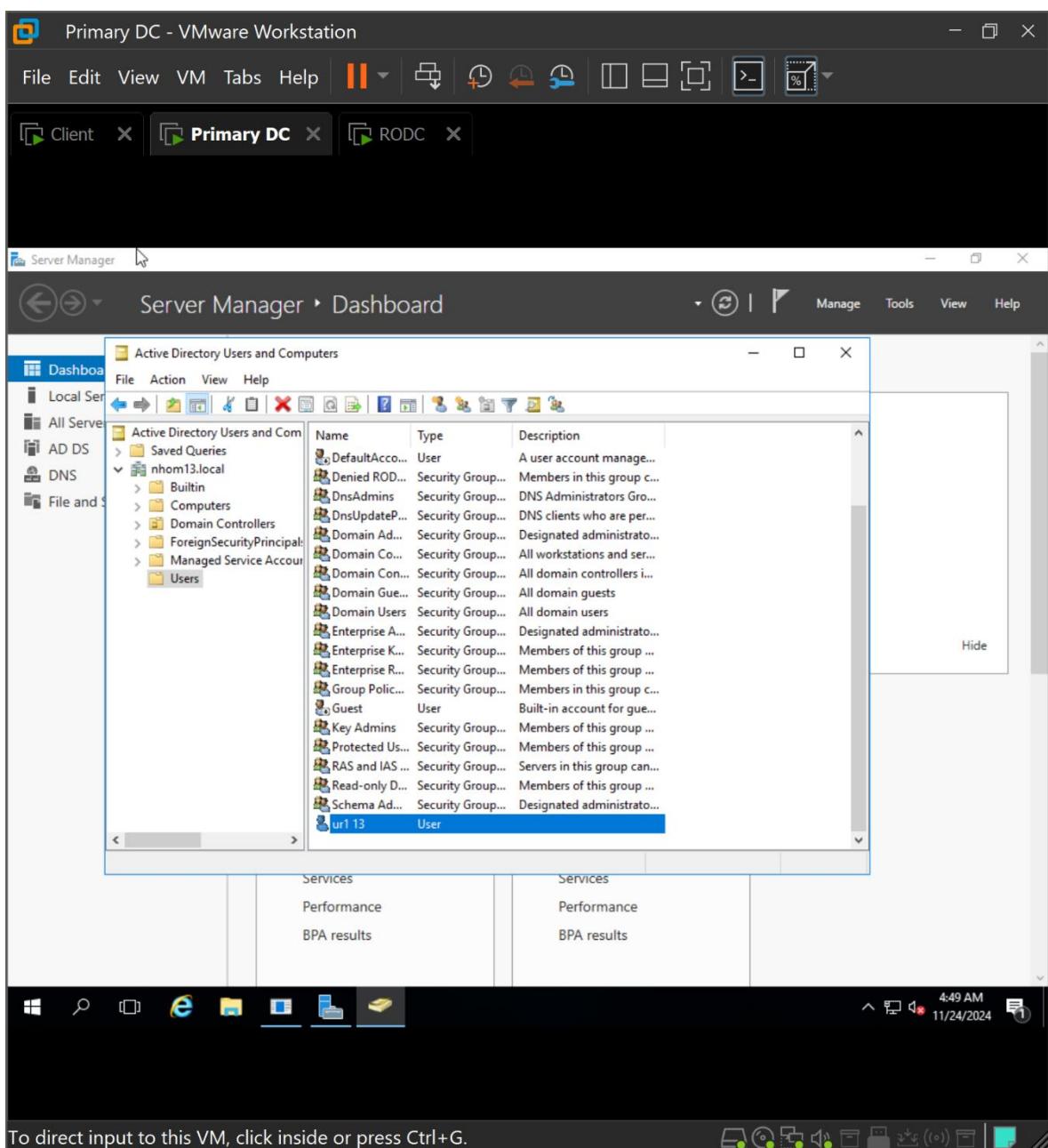
To direct input to this VM, click inside or press Ctrl+G.

## Lab 4: Triển khai Active Directory trên Windows Server



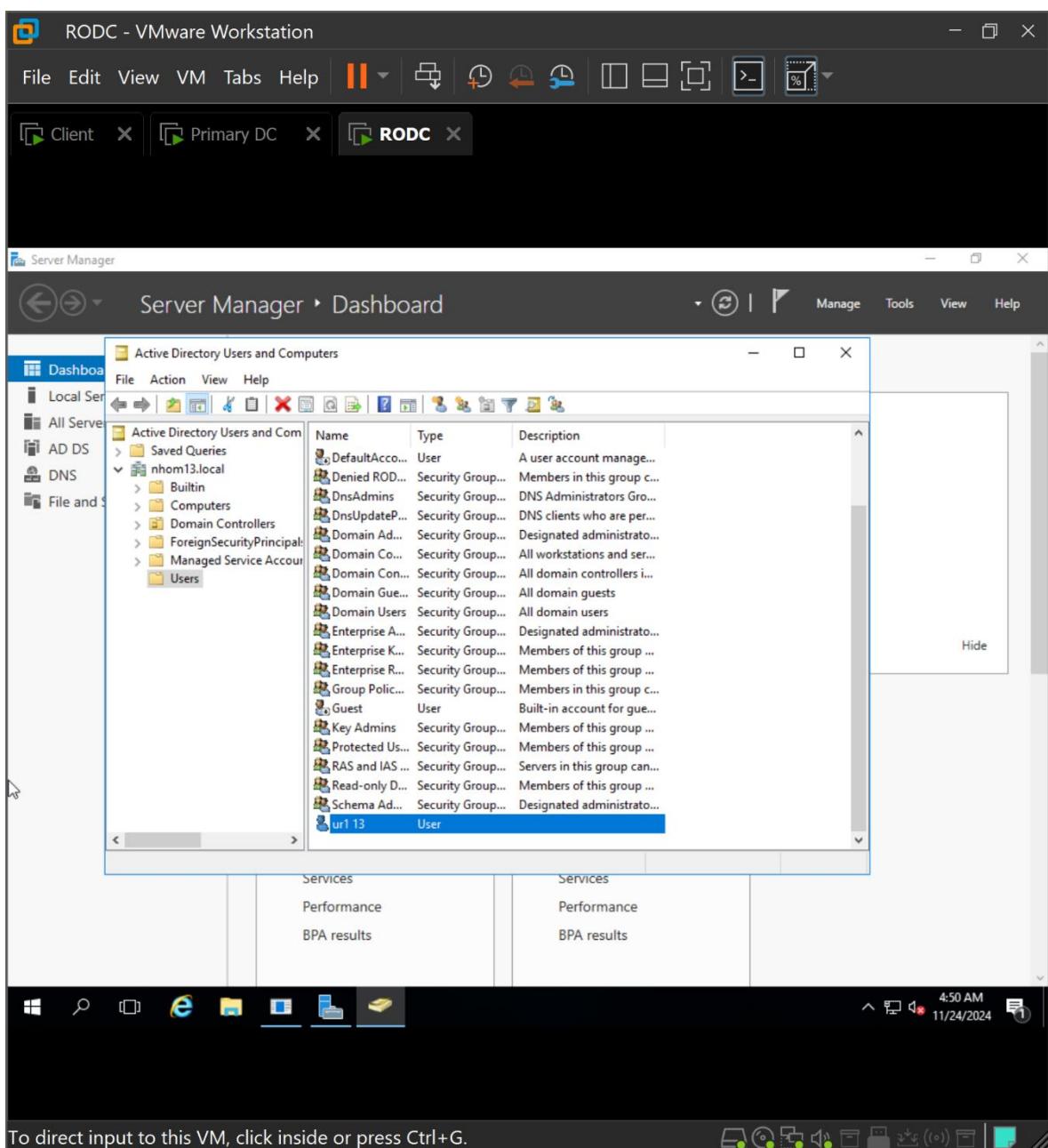
To direct input to this VM, click inside or press Ctrl+G.

## Lab 4: Triển khai Active Directory trên Windows Server



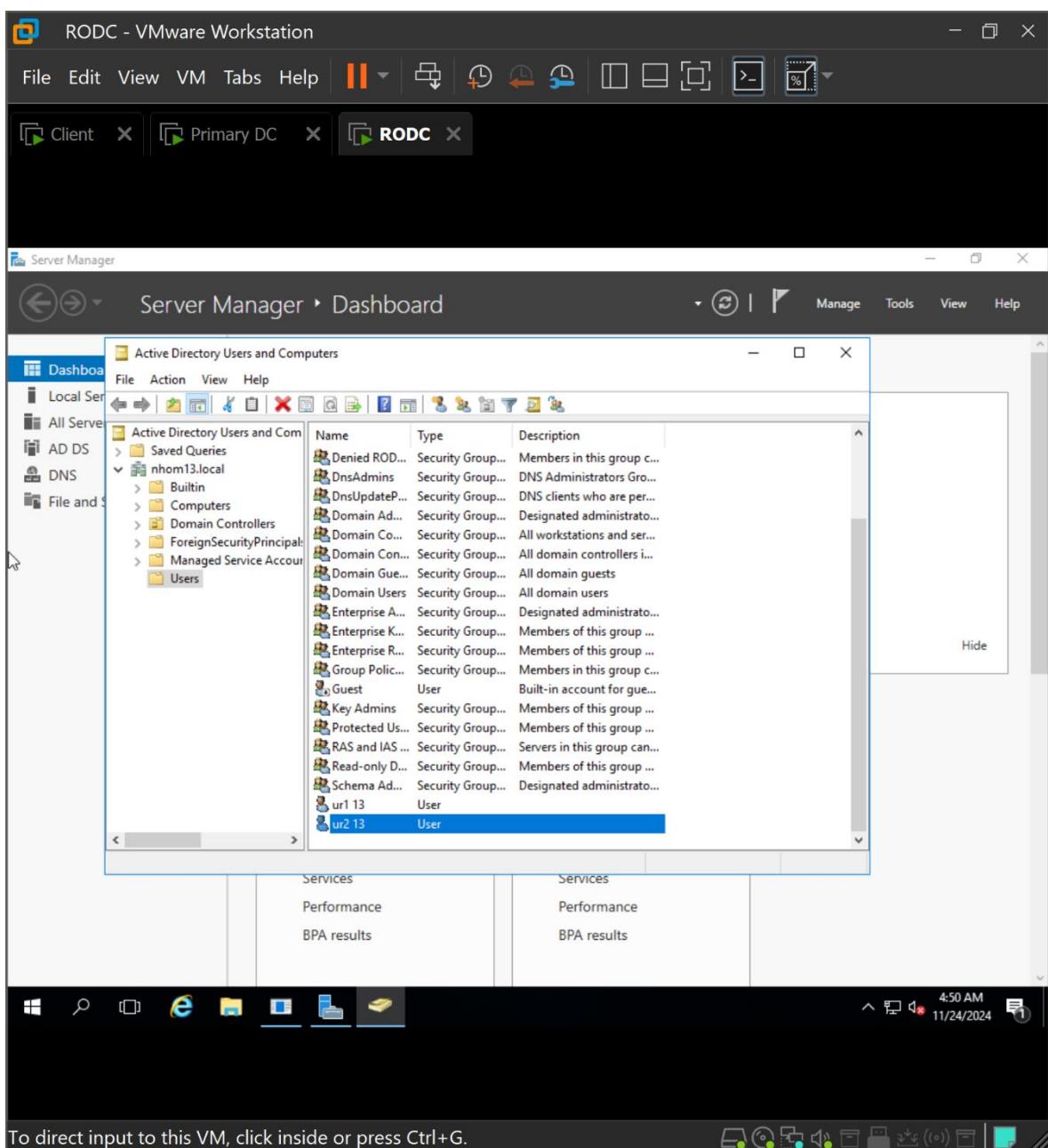
- Kiểm tra trên RODC:

## Lab 4: Triển khai Active Directory trên Windows Server



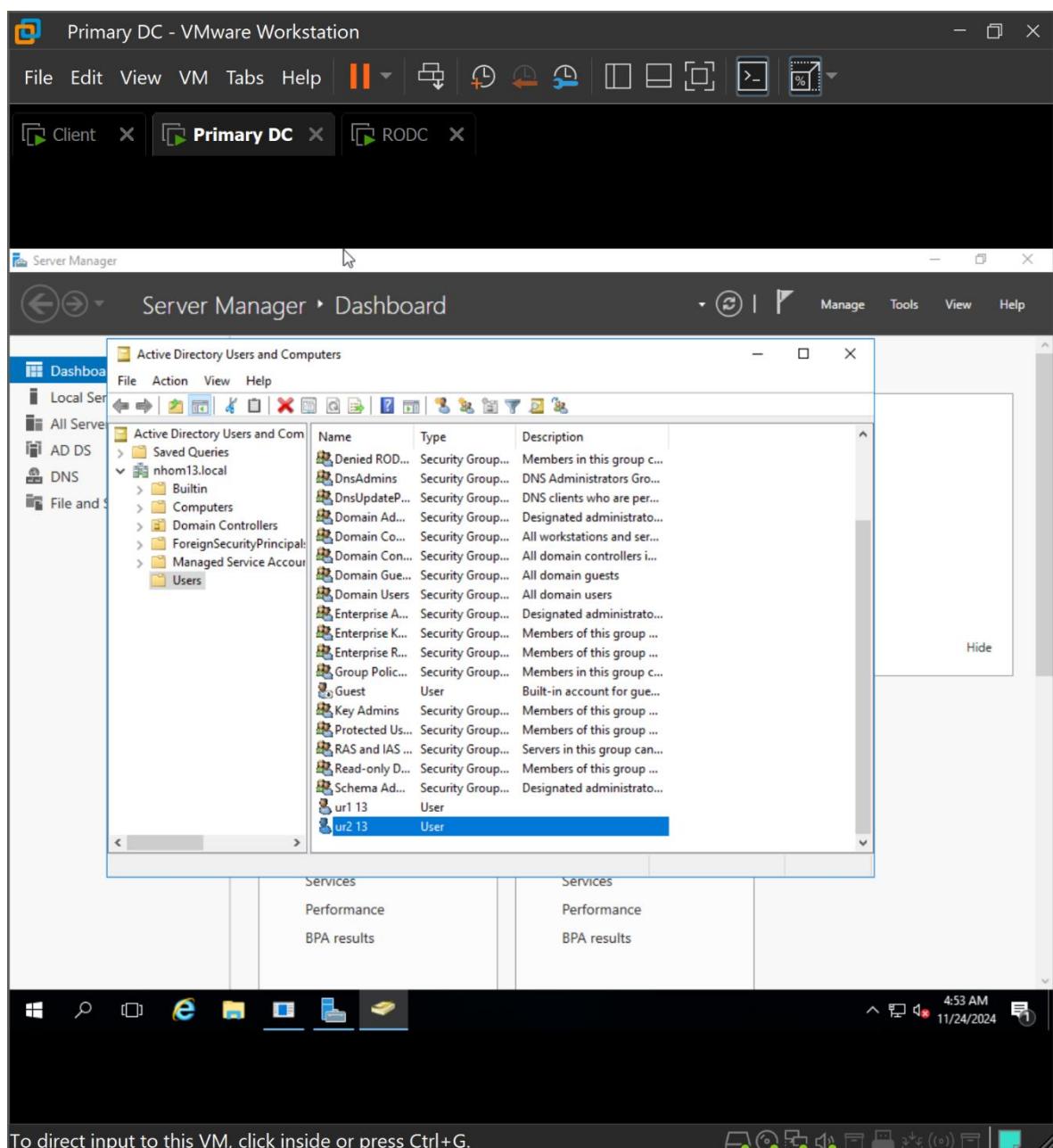
- Tạo ur213 trên RODC:

## Lab 4: Triển khai Active Directory trên Windows Server



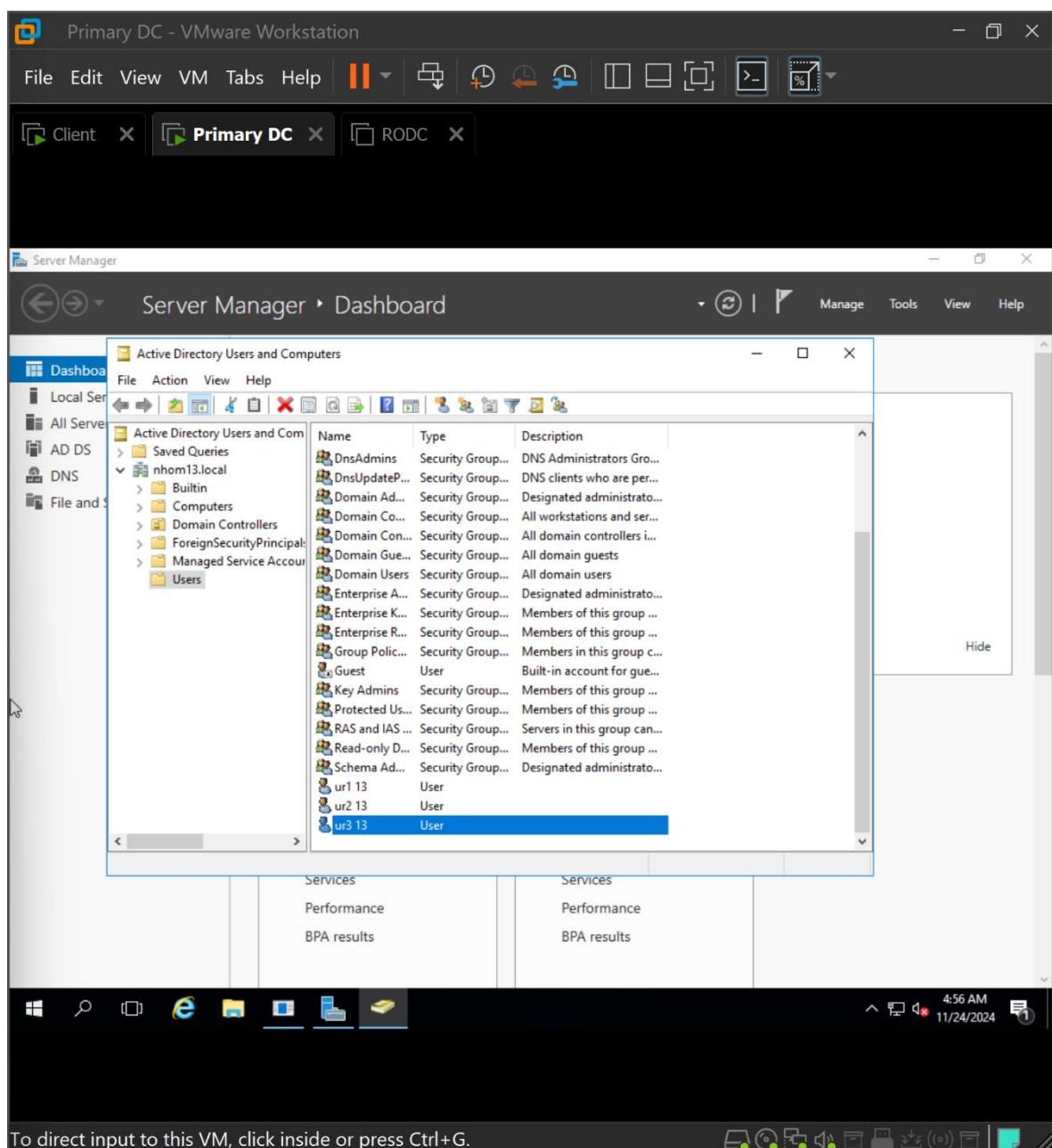
- Kiểm tra trên PDC:

## Lab 4: Triển khai Active Directory trên Windows Server



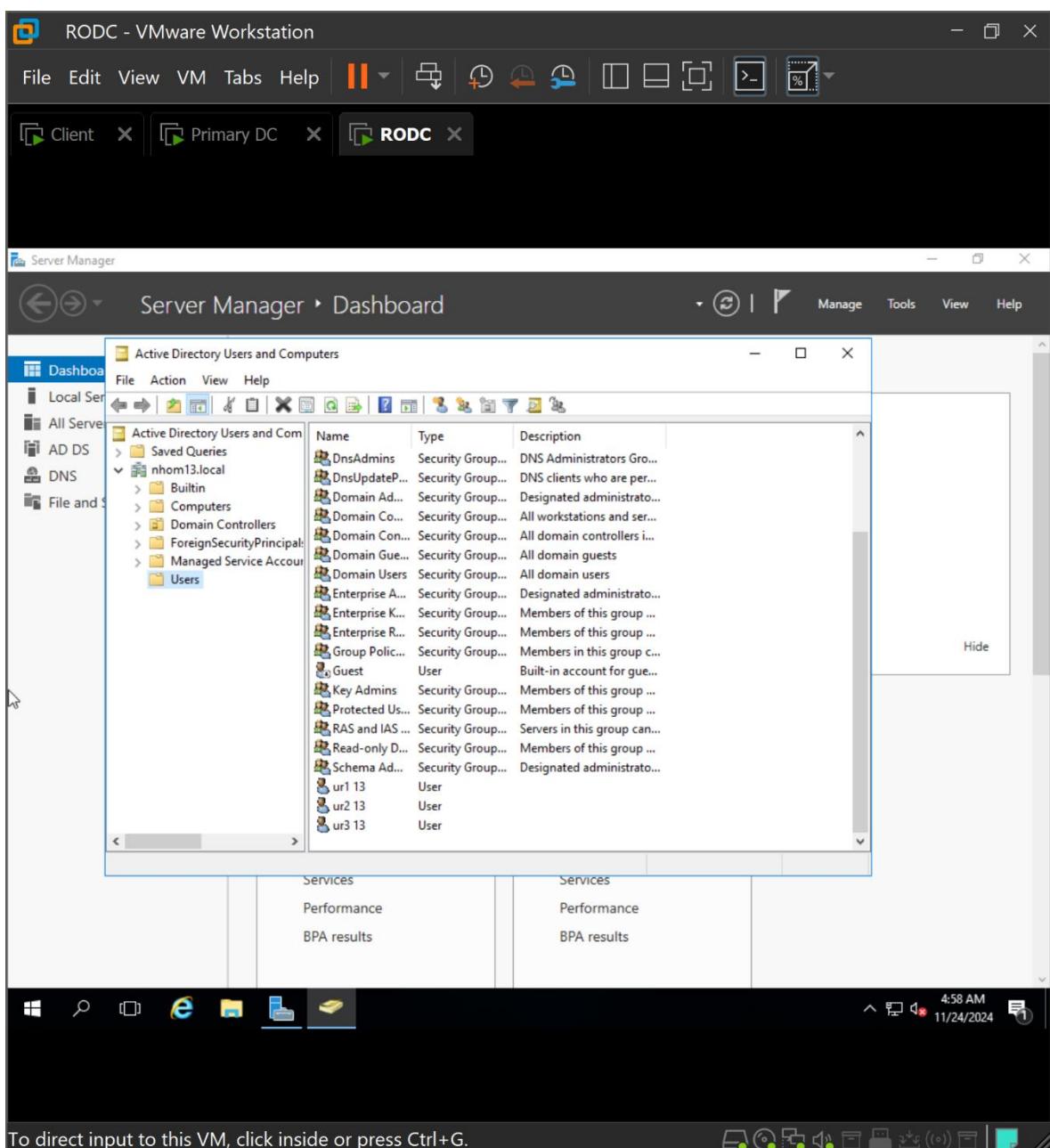
- Tắt RODC và tạo ur313 trên PDC:

## Lab 4: Triển khai Active Directory trên Windows Server



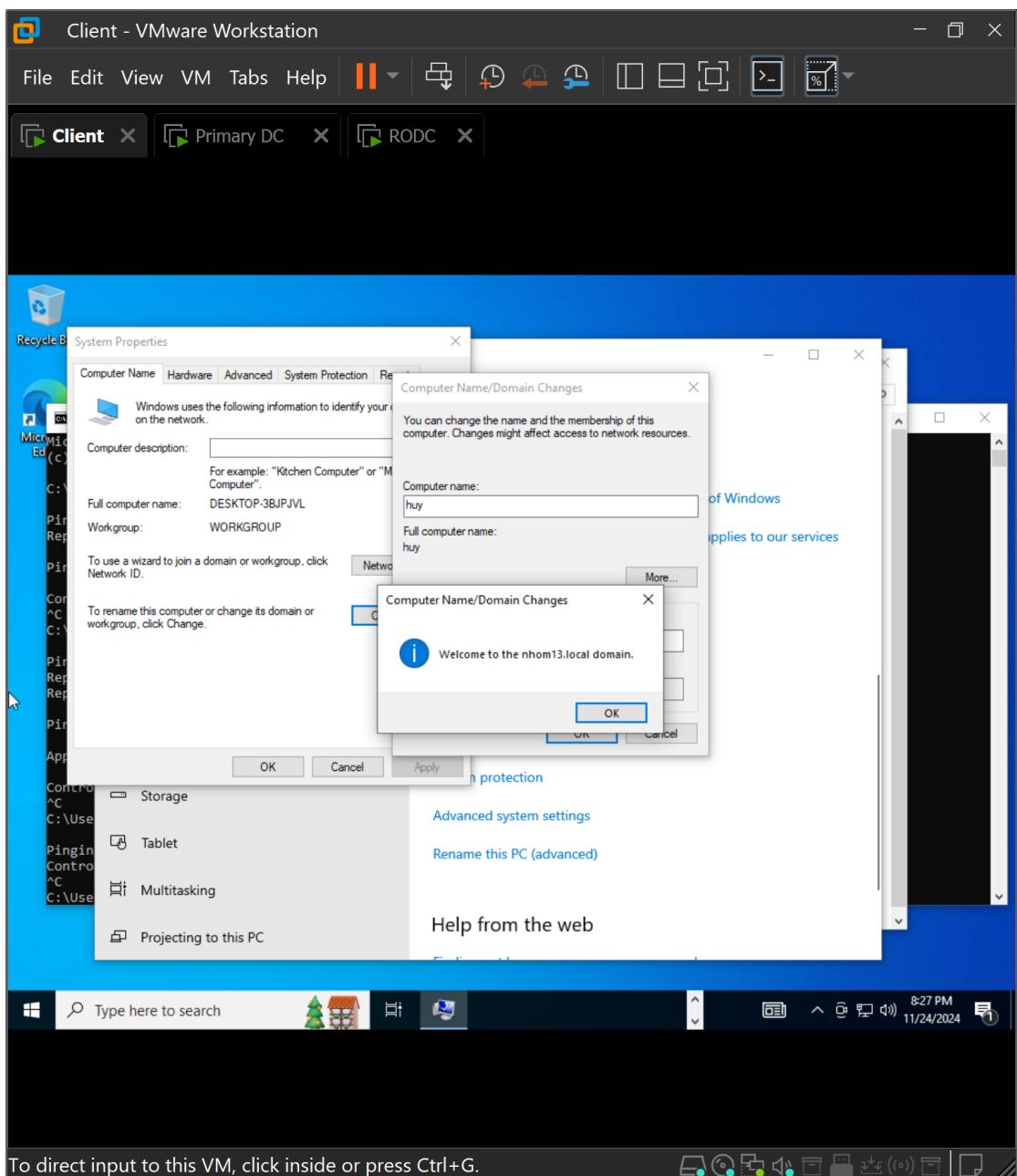
- Mở RODC và kiểm tra ur313:

## Lab 4: Triển khai Active Directory trên Windows Server



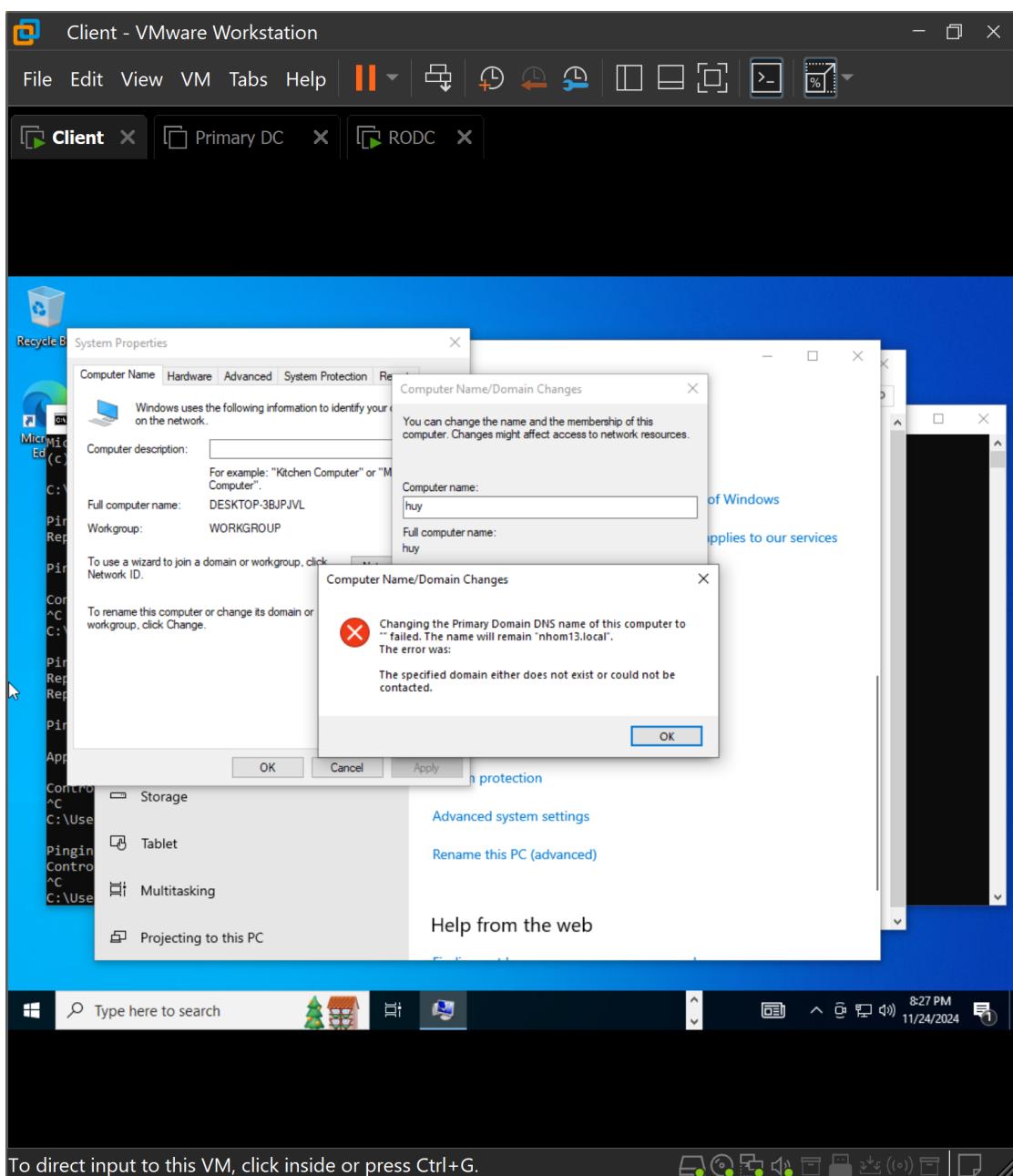
- Đăng nhập ur213 trên client

## Lab 4: Triển khai Active Directory trên Windows Server



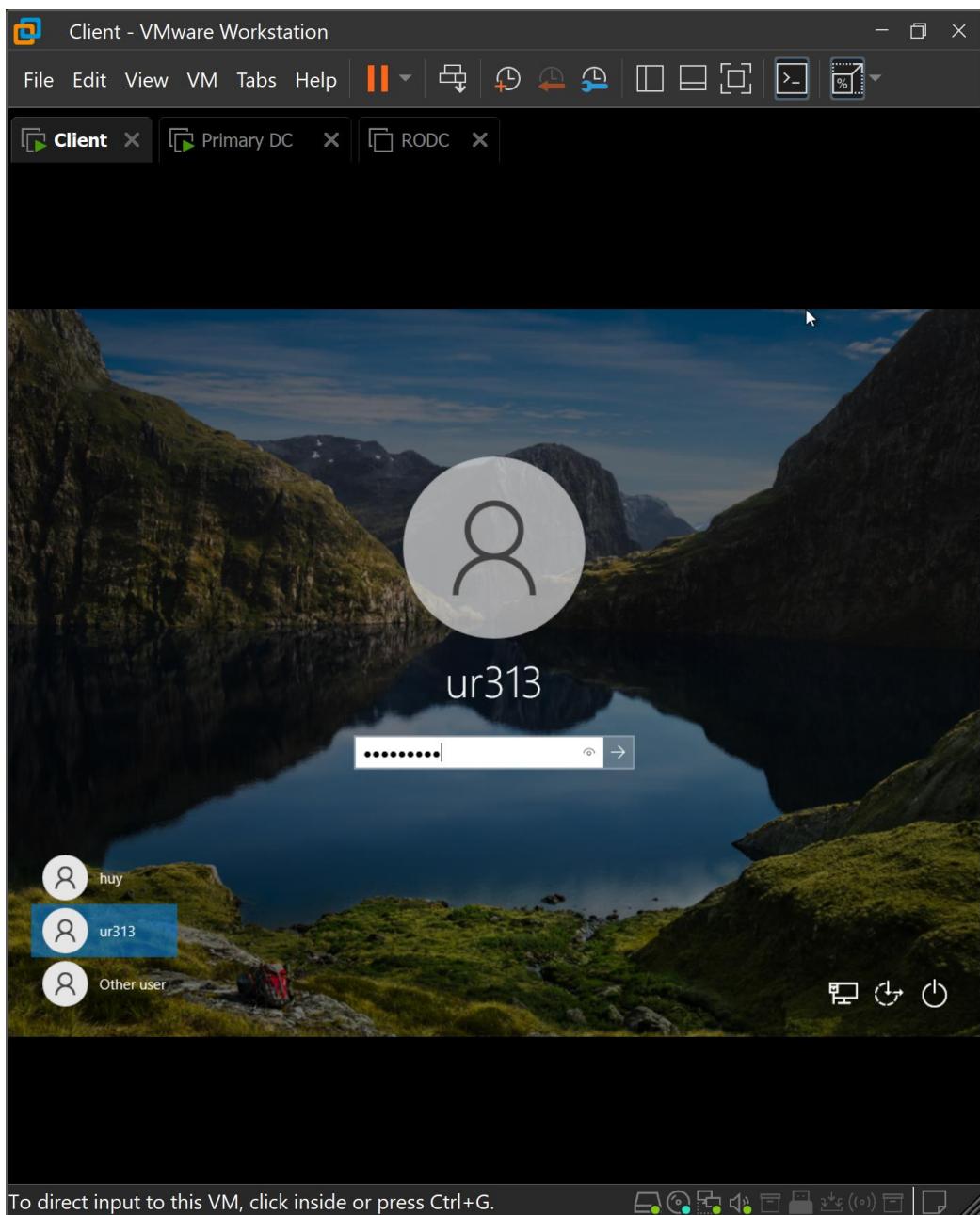
- Tắt PDC và đăng nhập ur213 trên client --> Không được.

## Lab 4: Triển khai Active Directory trên Windows Server

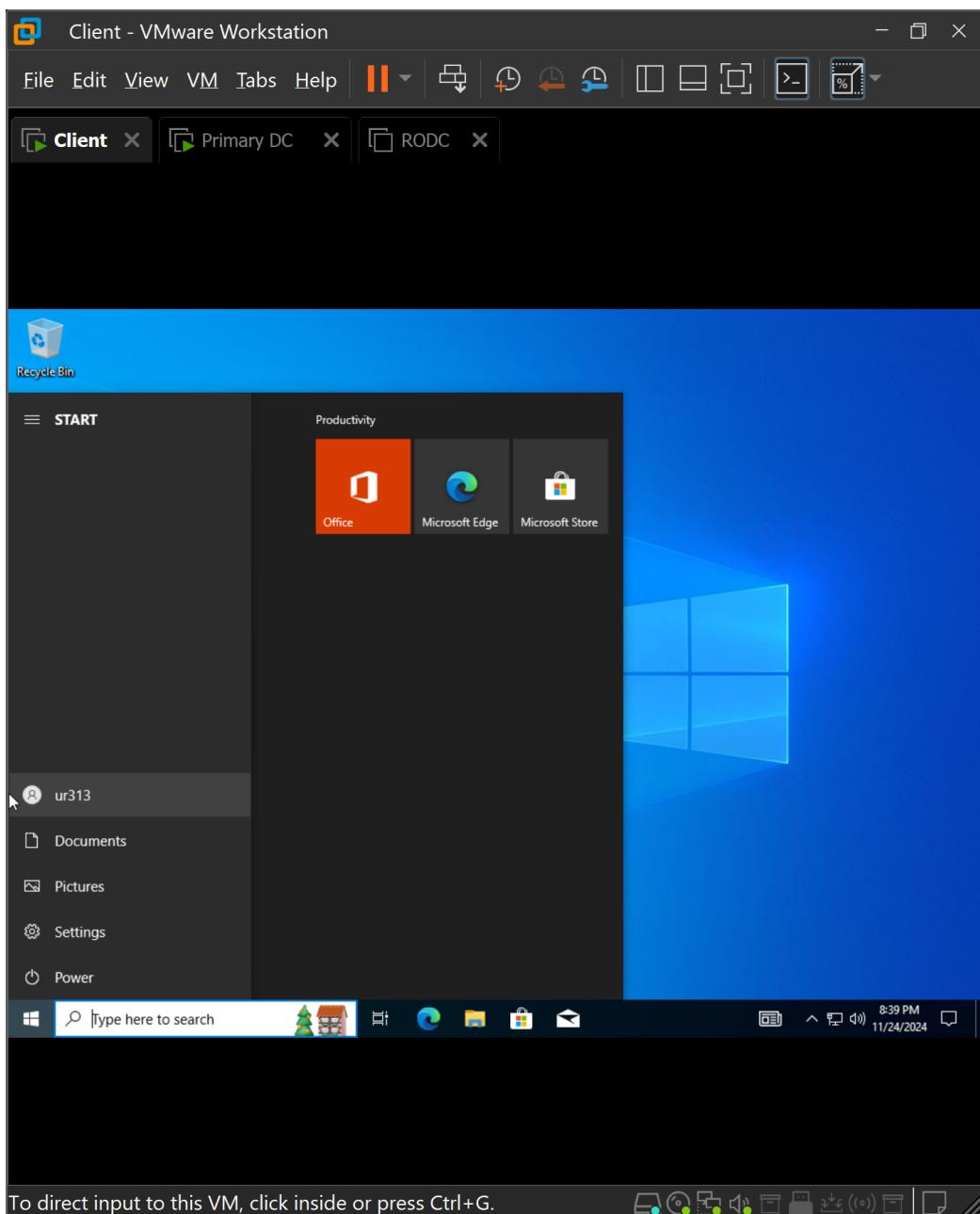


- Giải thích: Vì ur213 được tạo trên RODC mà RODC chỉ có quyền đọc nên những thay đổi trên Active Directory thông qua RODC sẽ không có tác dụng.
- Tắt RODC và đăng nhập vào ur313 bằng client:

## Lab 4: Triển khai Active Directory trên Windows Server



## Lab 4: Triển khai Active Directory trên Windows Server



- Giải thích: Vì ur313 được tạo trên PDC, RODC sẽ đọc và kiểm tra trên Active Directory.

----- HẾT -----