

BÁO CÁO THỰC HÀNH

Môn học: Quản trị mạng và hệ thống

Lab 4: Setting up Active Directory in Windows Server

GVHD: Ngô Đức Hoàng Sơn

Nhóm 8

THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.P12.ANTT.2

STT	Họ và tên	MSSV	Email
1	Đinh Bạch Kiều Phương	21520406	21520406@gm.uit.edu.vn
2	Nguyễn Đăng Quỳnh Như	22521050	22521050@gm.uit.edu.vn
3	Nguyễn Phúc Nhi	22521041	22521041@gm.uit.edu.vn

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

BÁO CÁO CHI TIẾT

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

1. Mô hình Workgroup hoạt động như thế nào?

- Mô hình Workgroup:

+ Một nhóm các máy tính cùng chia sẻ các tài nguyên, là một nhóm logic các máy tính mà tất cả chúng có cùng tên nhóm. Ở phạm vi 1 mạng LAN có thể có nhiều nhóm làm việc Workgroup khác nhau cùng kết nối.

+ Các máy tính có quyền chia sẻ tài nguyên ngang nhau, không có các máy tính chuyên dụng làm nhiệm vụ cung cấp dịch vụ hay quản lý.

+ Mỗi máy tính đều được tạo riêng 1 useraccount. Khi đăng nhập vào bất kỳ máy nào trong 1 workgroup bạn phải có account của máy đó.

+ Tất cả các máy tính phải ở trong cùng 1 local network hoặc cùng subnet.

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

- Ưu điểm:

+ Không yêu cầu có Domain Controller.

+ Thiết kế và thực hiện đơn giản.

+ Phù hợp với mạng nhỏ (từ 10 – 20 máy).

- Nhược điểm:

+ Không phù hợp với mô hình lớn có hàng ngàn máy tính.

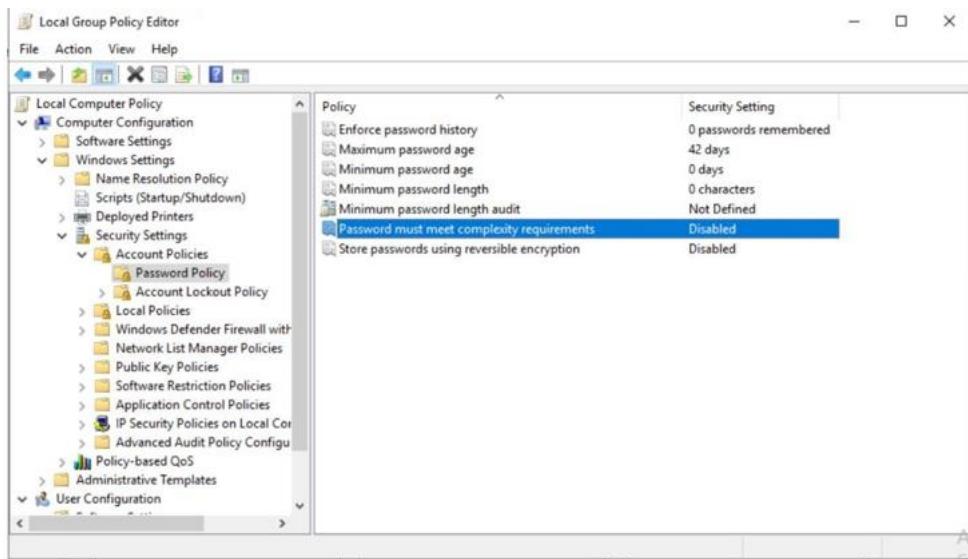
+ Khả năng bảo mật thấp, dễ bị xâm nhập.

+ Nếu như có bất kì sự thay đổi nào liên quan đến tài khoản đều cần thực hiện trên tất cả các máy tính trong nhóm làm việc.

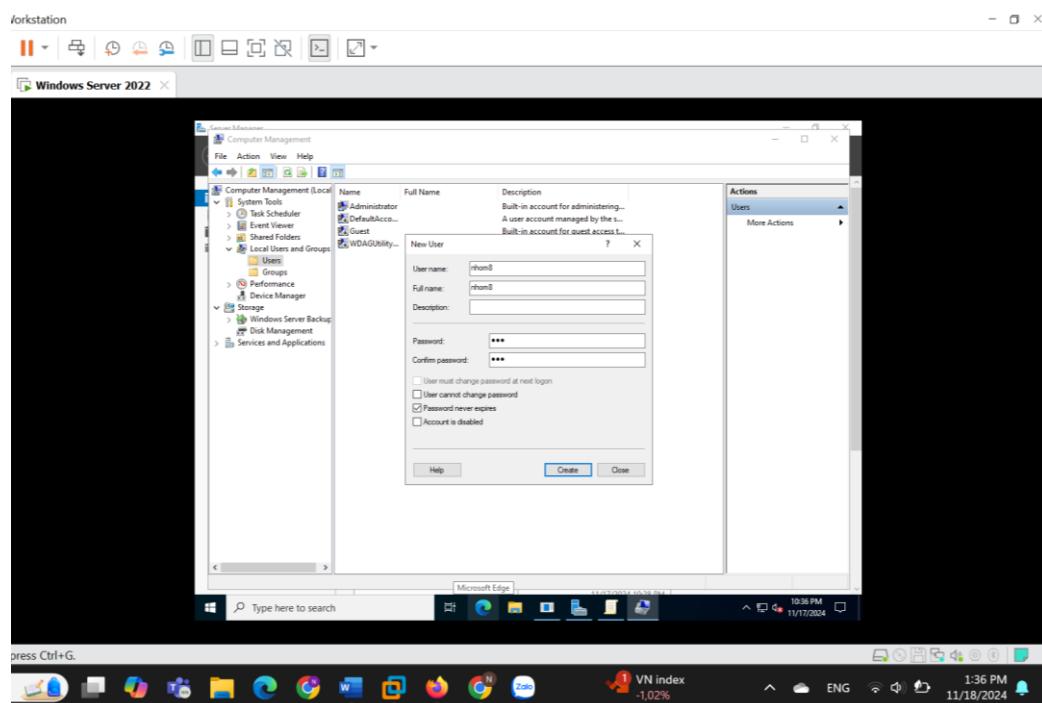
+ Việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng → không cho phép quản lý tập trung, dữ liệu bị phân tán.

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

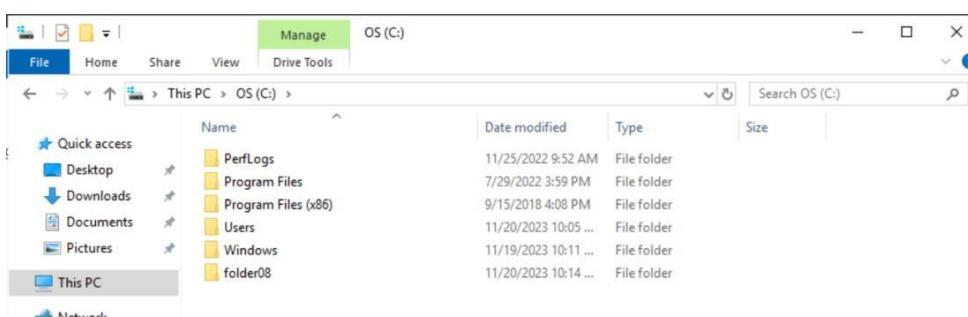
Bước 1: Cấu hình chính sách mật khẩu trên File Server



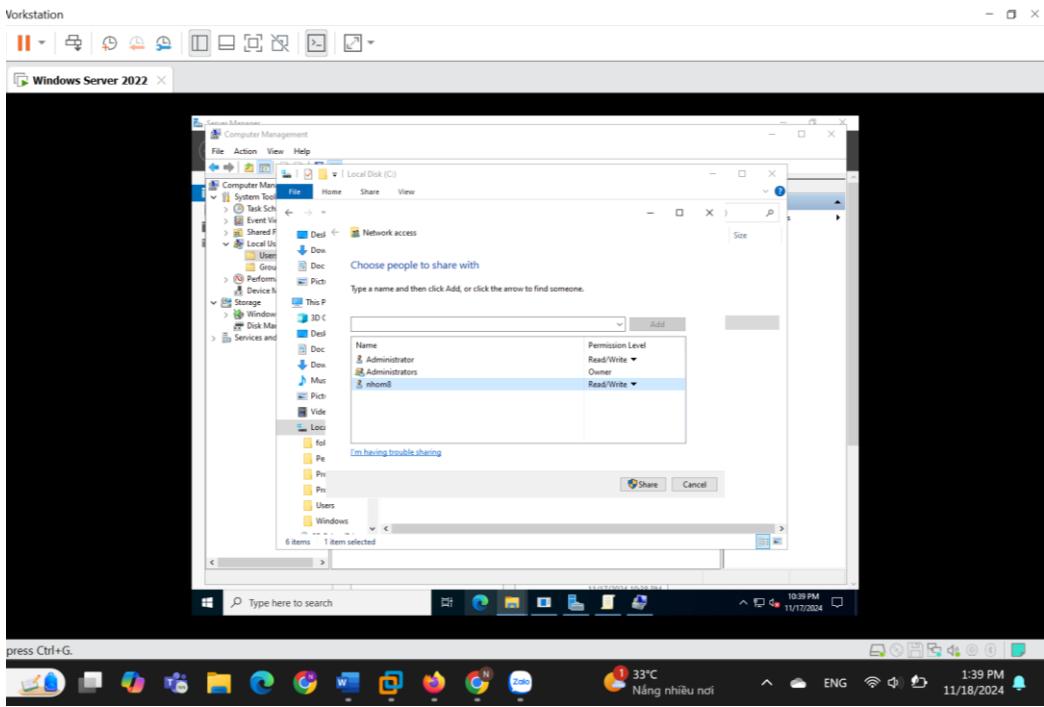
Bước 2: Trên máy chủ File Server, tạo tài khoản nhomX có mật khẩu là 123.



Bước 3: Trên ổ đĩa C:\ của File Server, tạo 1 thư mục folderX (X là thứ tự nhóm dạng 2 chữ số) để chia sẻ dữ liệu.

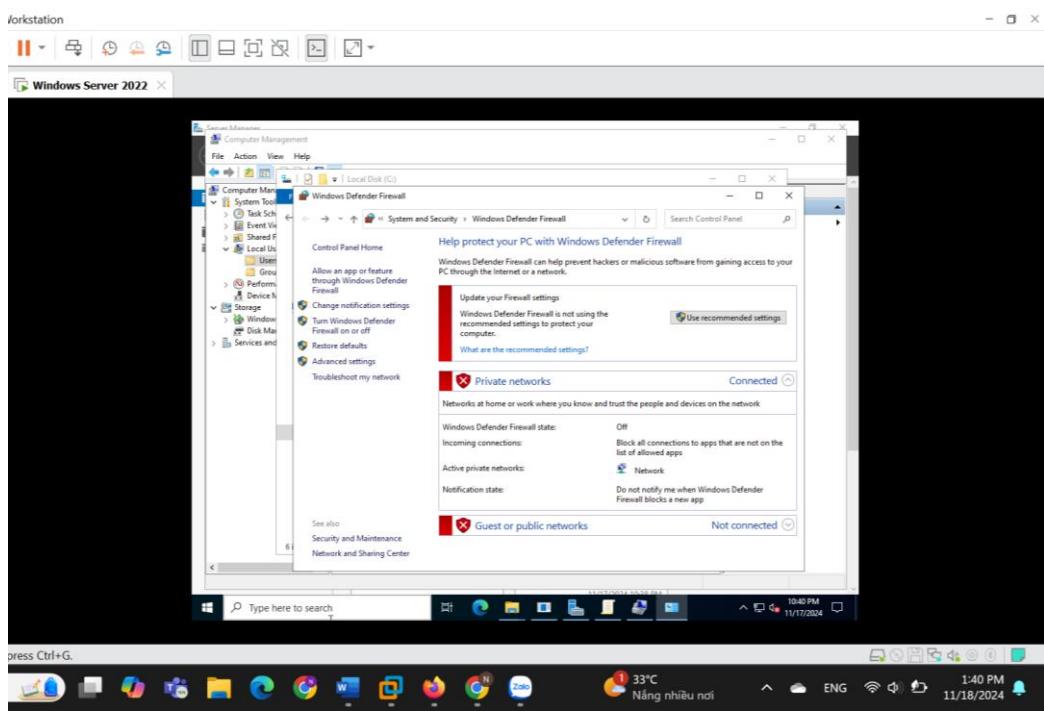


Bước 4: Nhấp chuột phải vào tên thư mục folderX, chọn Share with > Specific people... Thực hiện phân quyền chia sẻ trên thư mục này để user nhomX có quyền Read/Write.



Bước 5:

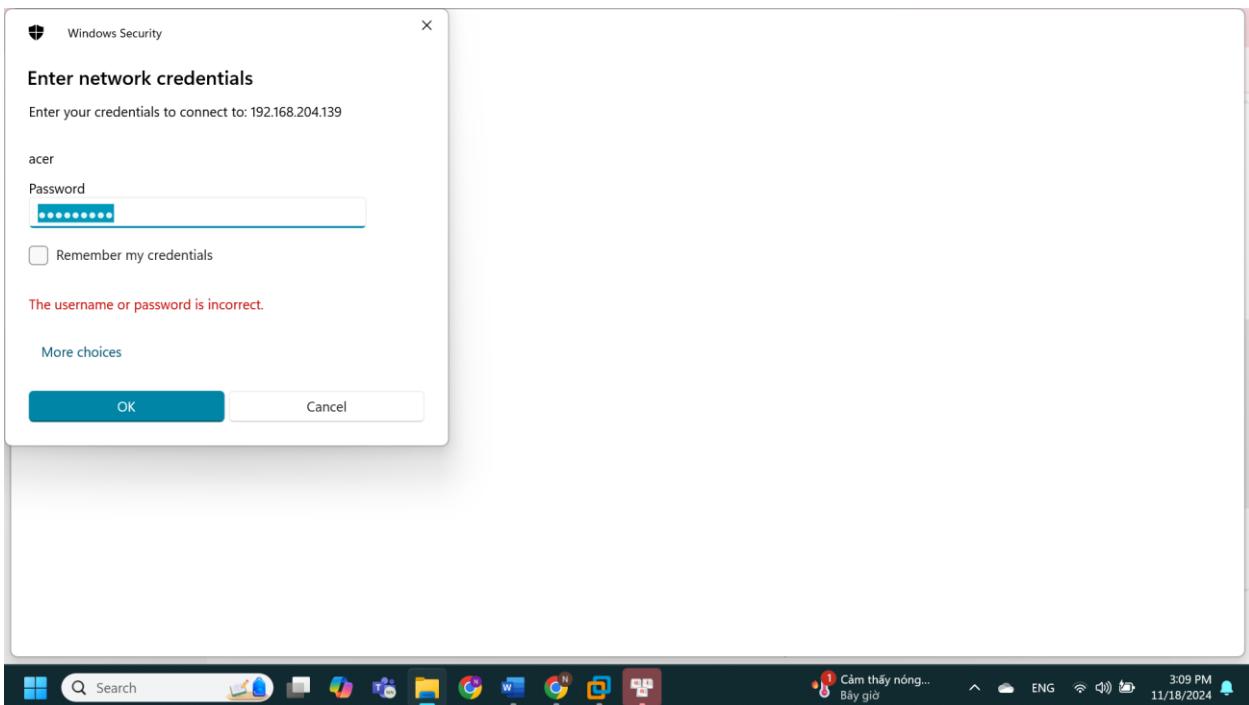
tạm thời tắt Firewall trên File Server trước khi kết nối ở Bước 5



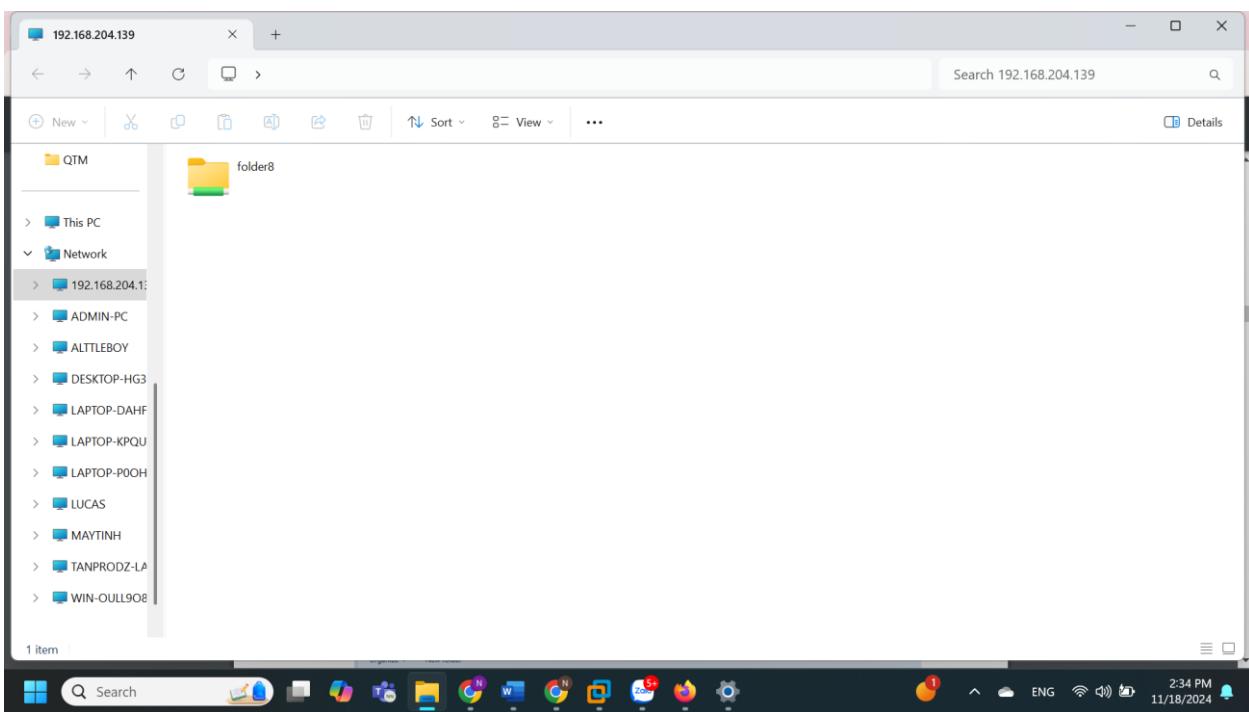
Bước 6: Nhập user xác thực để truy cập vào File Server

- Sử dụng tài khoản của máy Client và tài khoản của máy File Server (user nhom08)
- Khi truy cập File Server bằng tài khoản của máy Client

Khi truy cập File Server bằng tài khoản của máy Client: không thành công



Khi truy cập File Server bằng tài khoản user nhom08: thành công

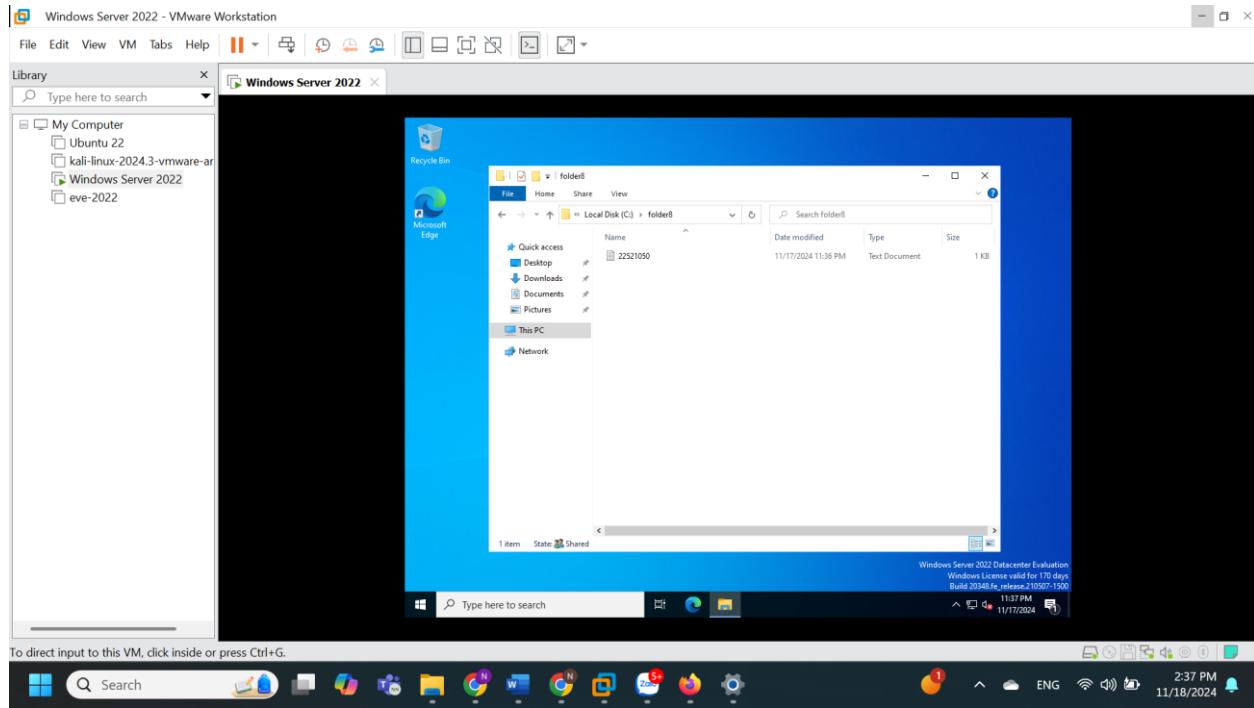


* Giải thích các kết quả:

++ TH1: Sử dụng tài khoản của máy Client: Kết quả là không kết nối được vì tài khoản của máy Client không nằm trong mô hình.

++ TH2: Sử dụng tài khoản của máy File Server: Kết quả là có thể kết nối, Read/Write được vào folder8. Vì đó là 1 tài khoản thuộc mô hình nên có quyền kết nối vào máy chủ và thực hiện quyền cho phép.

Bước 7 : tại đây em tạo 1 file 22521050.txt ở máy client (windows) thì ở file server cũng sẽ có file đó vừa được tạo ra



Thay đổi bên máy client cũng làm thay đổi bên file server

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?

Active Directory (AD) là một dịch vụ quản lý danh mục thư mục được phát triển bởi Microsoft để quản lý và lưu trữ thông tin liên quan đến tài khoản, máy tính, tài nguyên mạng và các đối tượng khác trong môi trường Windows.

2. So sánh mô hình Domain và Workgroup?

Tiêu chí	Domain	Workgroup
Quy mô	Dành cho mạng lớn (doanh nghiệp, tổ chức).	Phù hợp với mạng nhỏ (gia đình, văn phòng nhỏ).
Quản lý	Tập trung (qua Active Directory).	Phân tán (mỗi máy tính quản lý riêng lẻ).
Xác thực	Sử dụng máy chủ Domain Controller để xác thực người dùng.	Xác thực cục bộ trên từng máy tính trong Workgroup.
Tài khoản người dùng	Tài khoản người dùng được lưu trữ và quản lý tập trung trên máy chủ.	Tài khoản người dùng được lưu trữ trên từng máy tính riêng lẻ.
Bảo mật	Cao, nhờ cơ chế quản lý quyền và chính sách tập trung.	Thấp hơn, dễ bị lỗi bảo mật khi số lượng máy tăng lên.
Quyền truy cập tài nguyên	Quản lý tài nguyên (như máy in, thư mục chia sẻ) tập trung và có kiểm soát.	Chia sẻ tài nguyên đơn giản nhưng thiếu quản lý tập trung.
Hiệu năng mạng	Có thể hỗ trợ hàng nghìn thiết bị.	Hạn chế ở một số lượng thiết bị nhỏ, thường dưới 10 máy.

Cài đặt và bảo trì

Yêu cầu cài đặt và quản lý phức tạp hơn.

Dễ thiết lập và không yêu cầu phần mềm bổ sung.

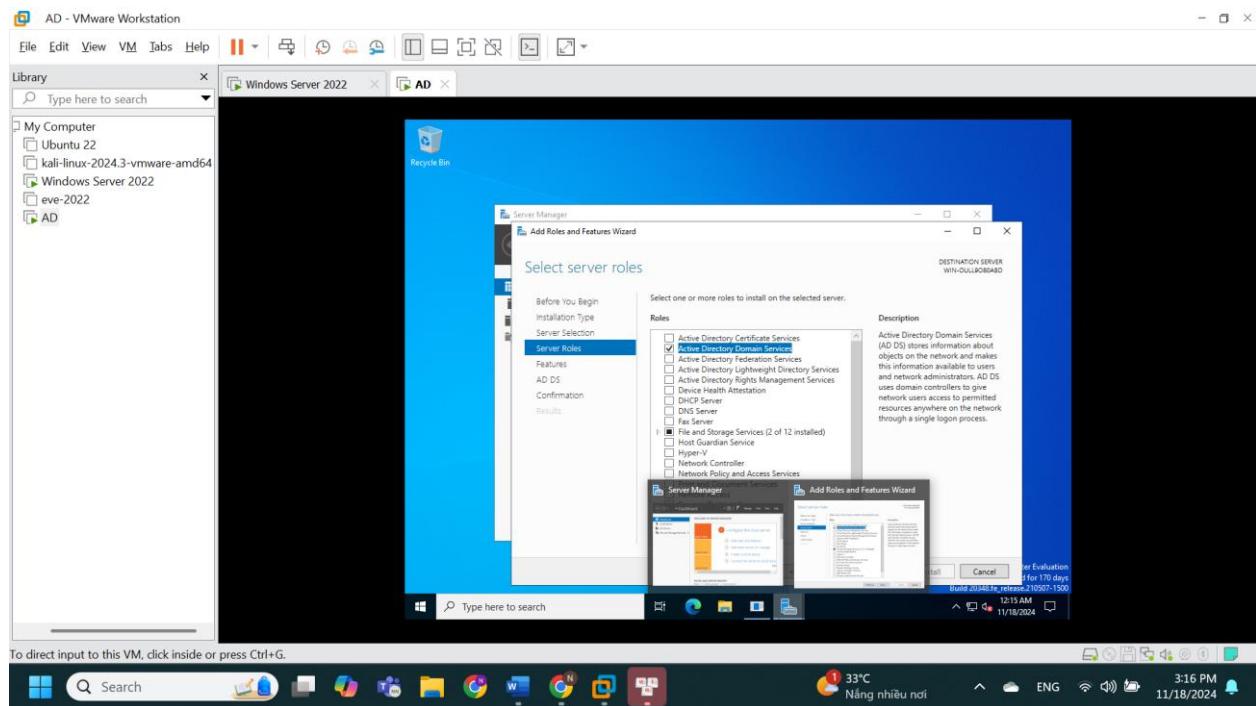
Yêu cầu 2.2. Xây dựng mô hình Domain như bên dưới.

Bước 1: Cài đặt Active Directory Domain Service trên máy Active Directory

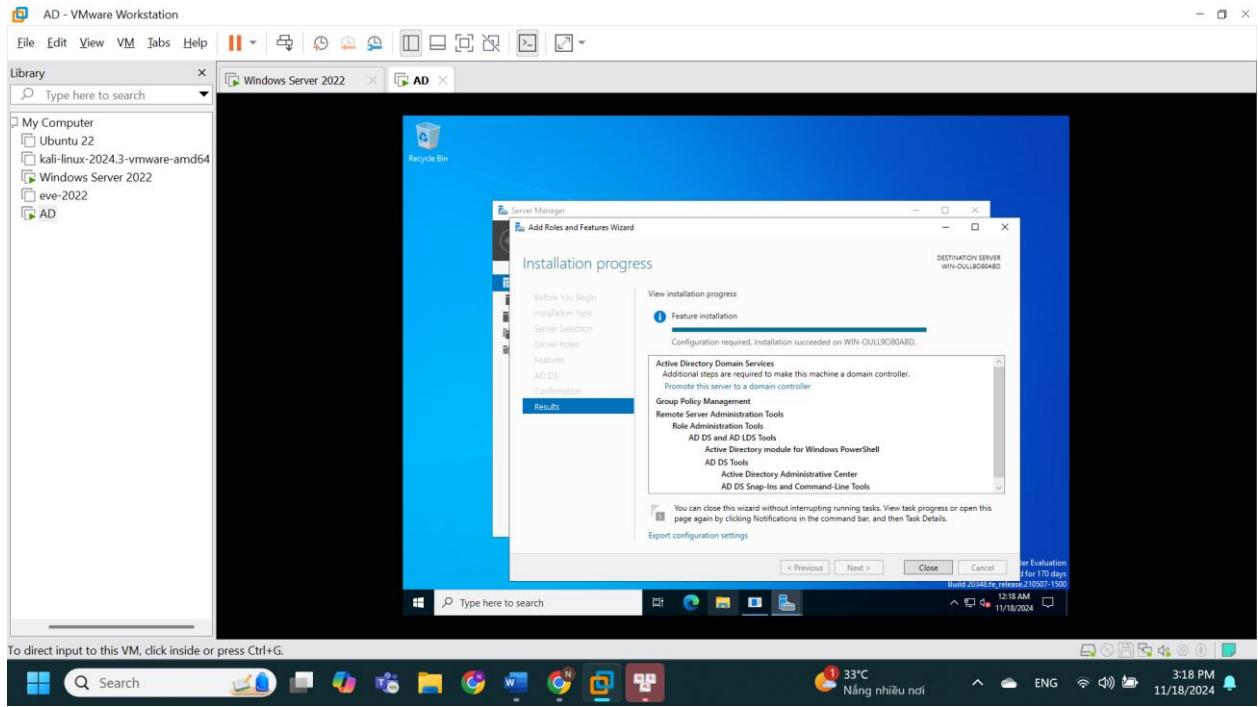
Vào Server Manager > Manage > Add Roles and Features.

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

Tại bước Server Roles, chọn Active Directory Domain Services.

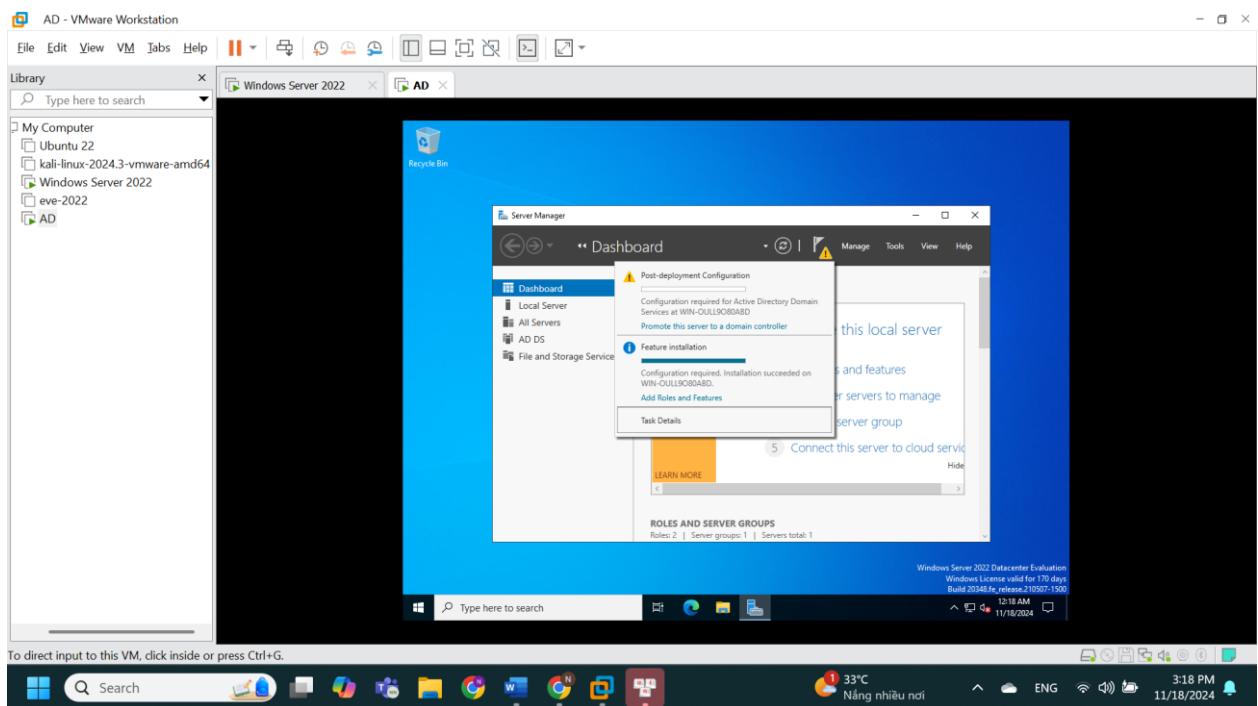


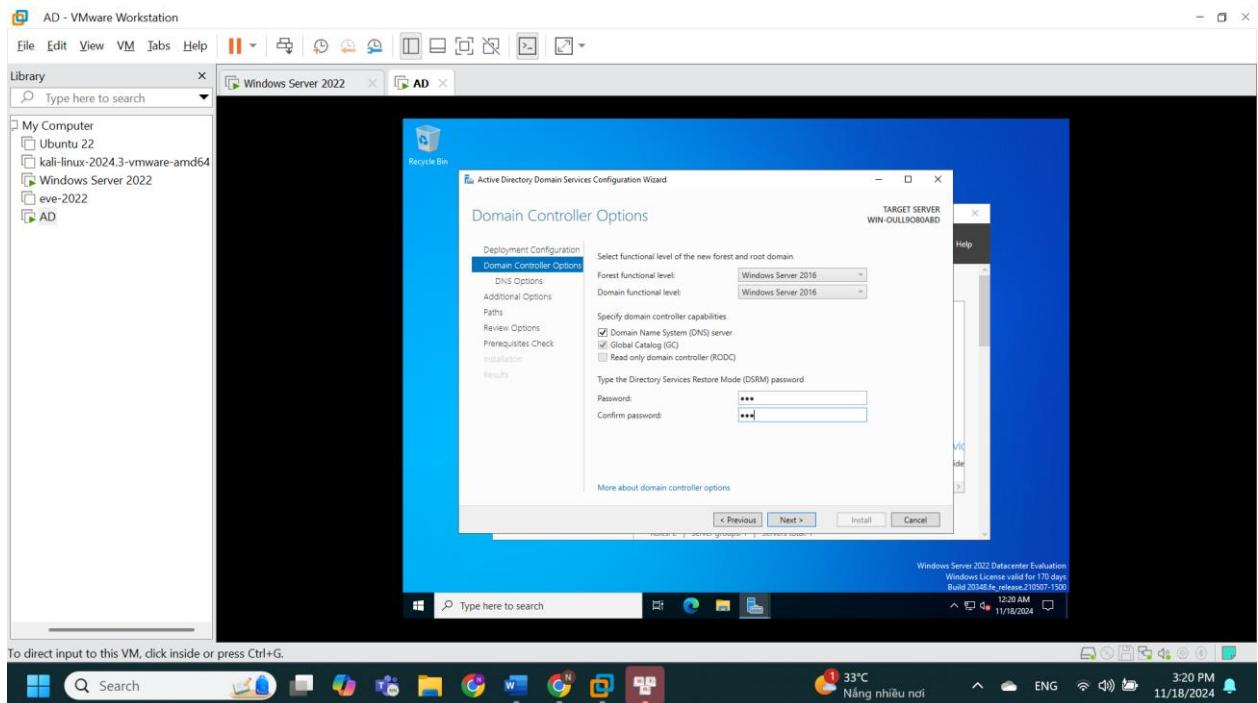
- Ở bước AD DS, chọn Next.
- Ở bước Confirmation, xác nhận lại thông tin và chọn Install.
- Chờ quá trình cài đặt hoàn thành và chọn Close để kết thúc.



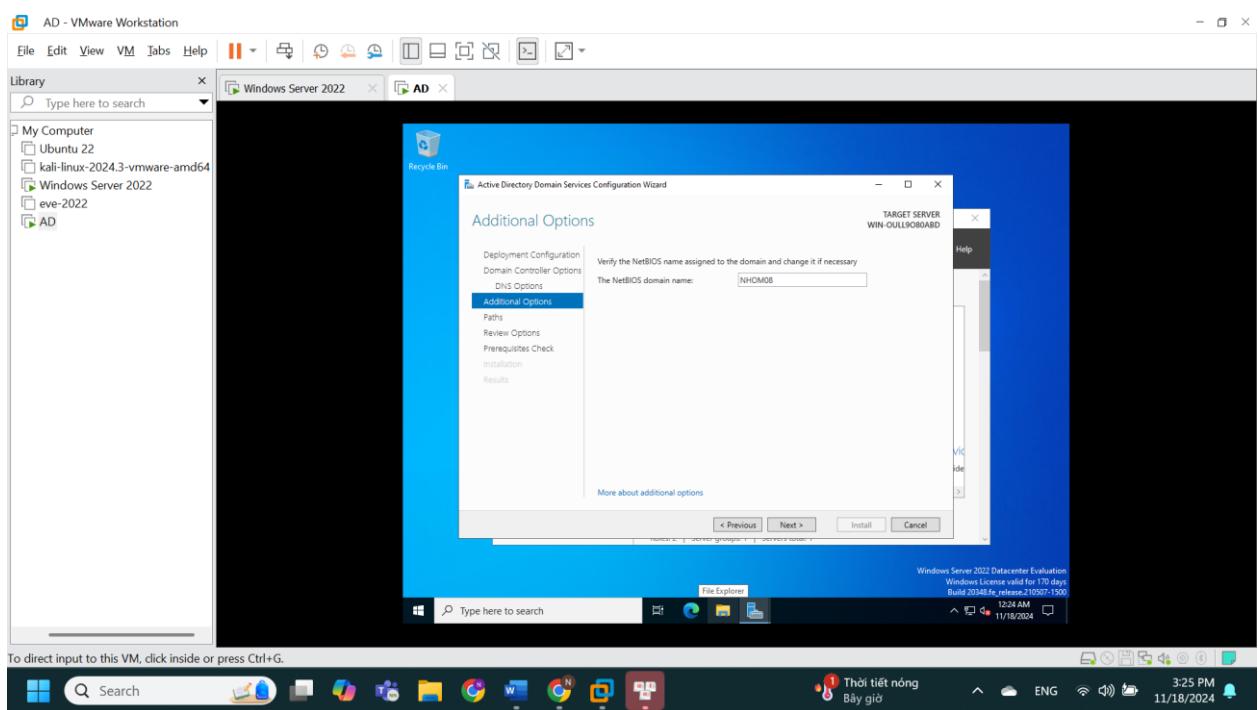
Bước 2: Nâng cấp máy chủ Active Directory lên Domain Controller

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

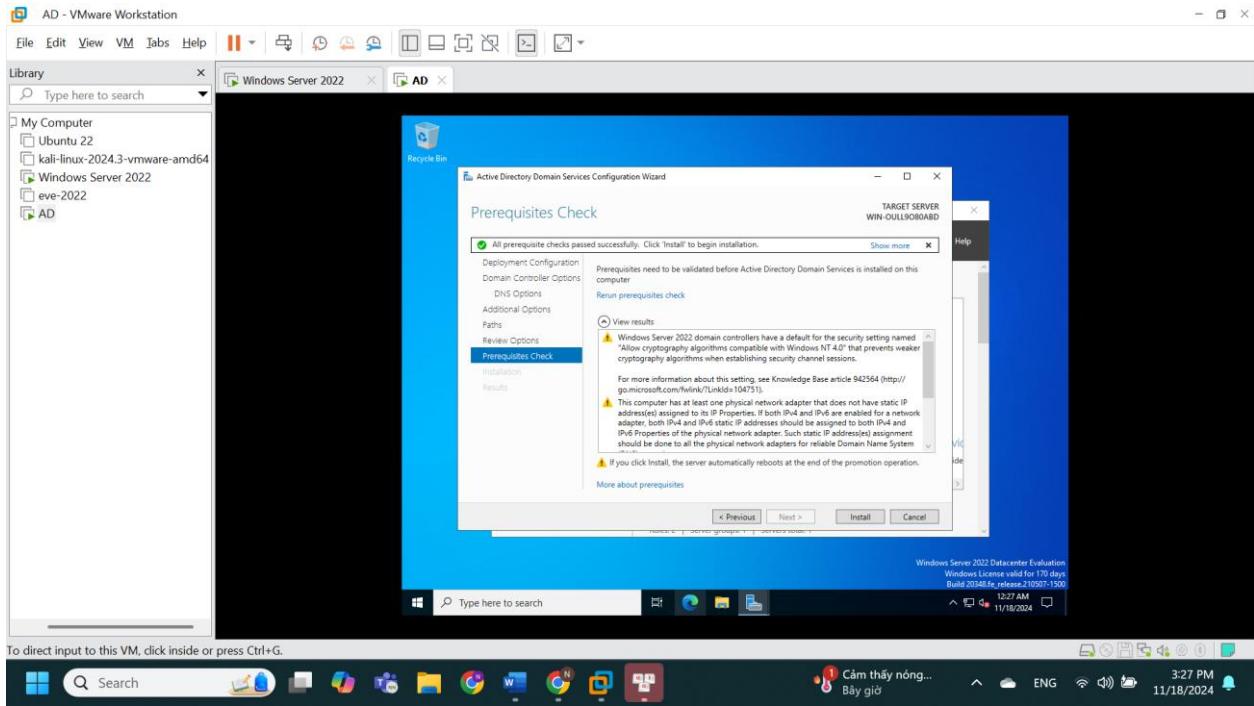




Thiết lập NetBIOS domain name



- Thực hiện bước Prerequisites Check hoàn thành, sau đó chọn Install và chờ quá trình nâng cấp hoàn tất.

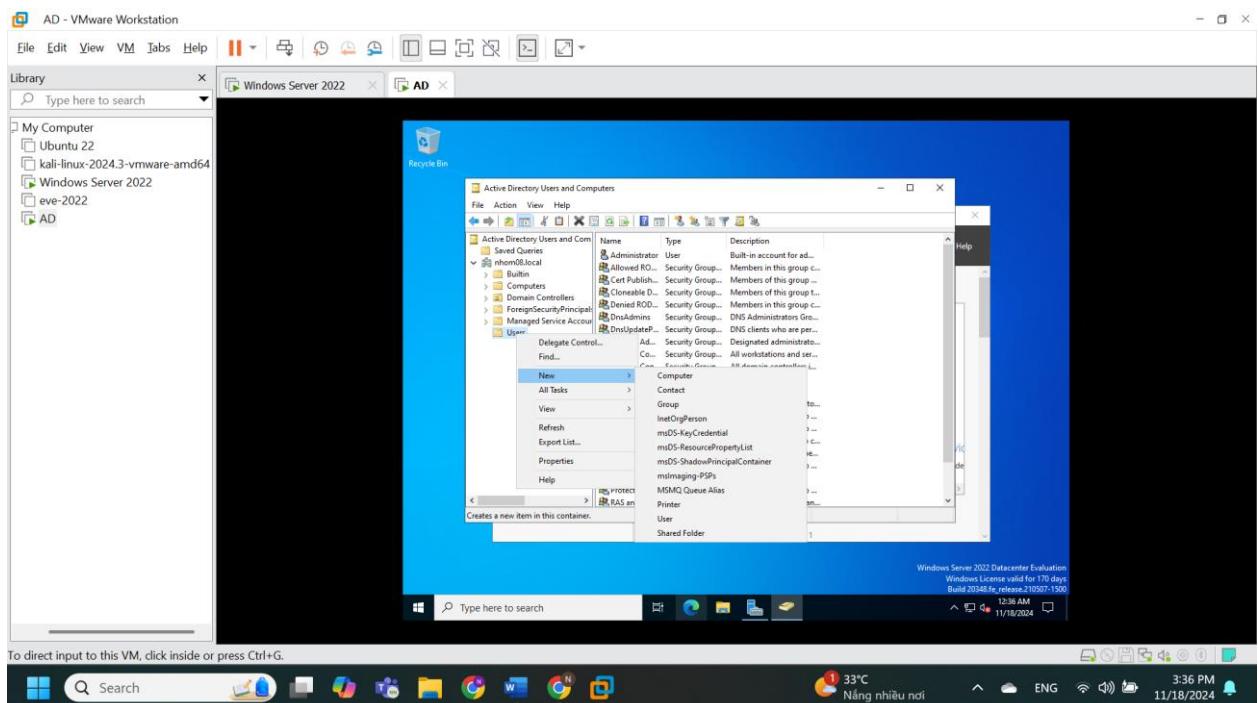
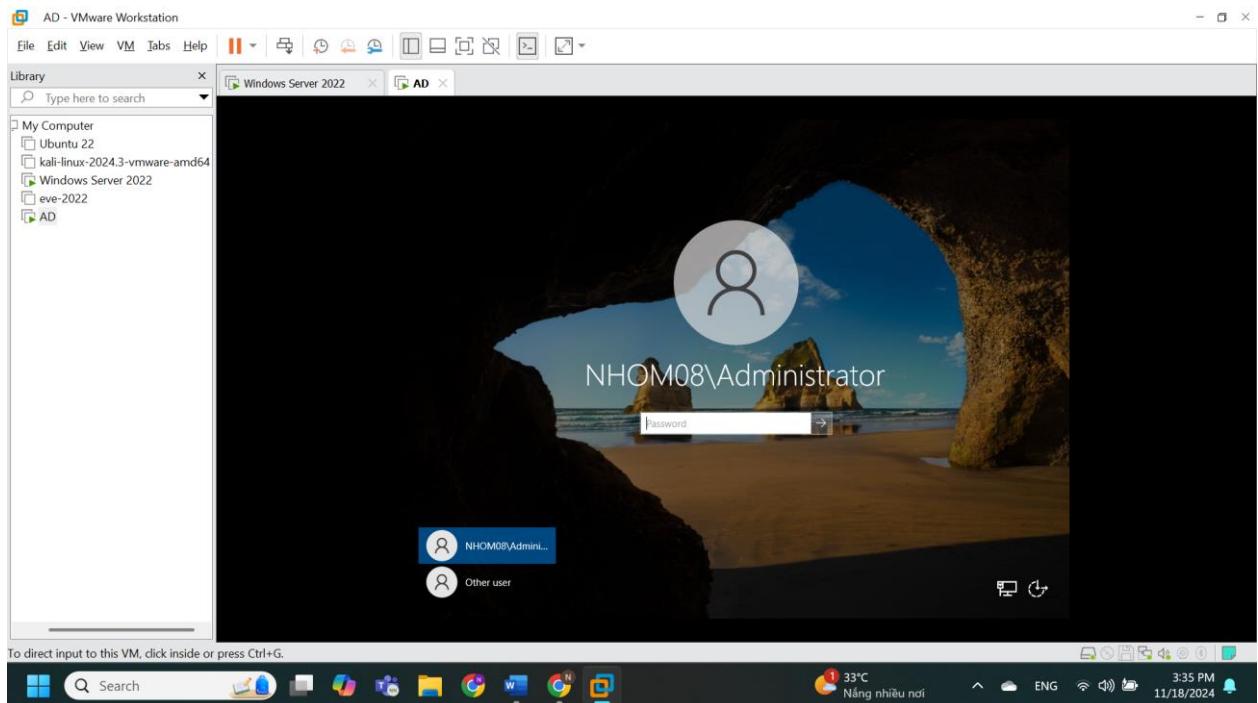


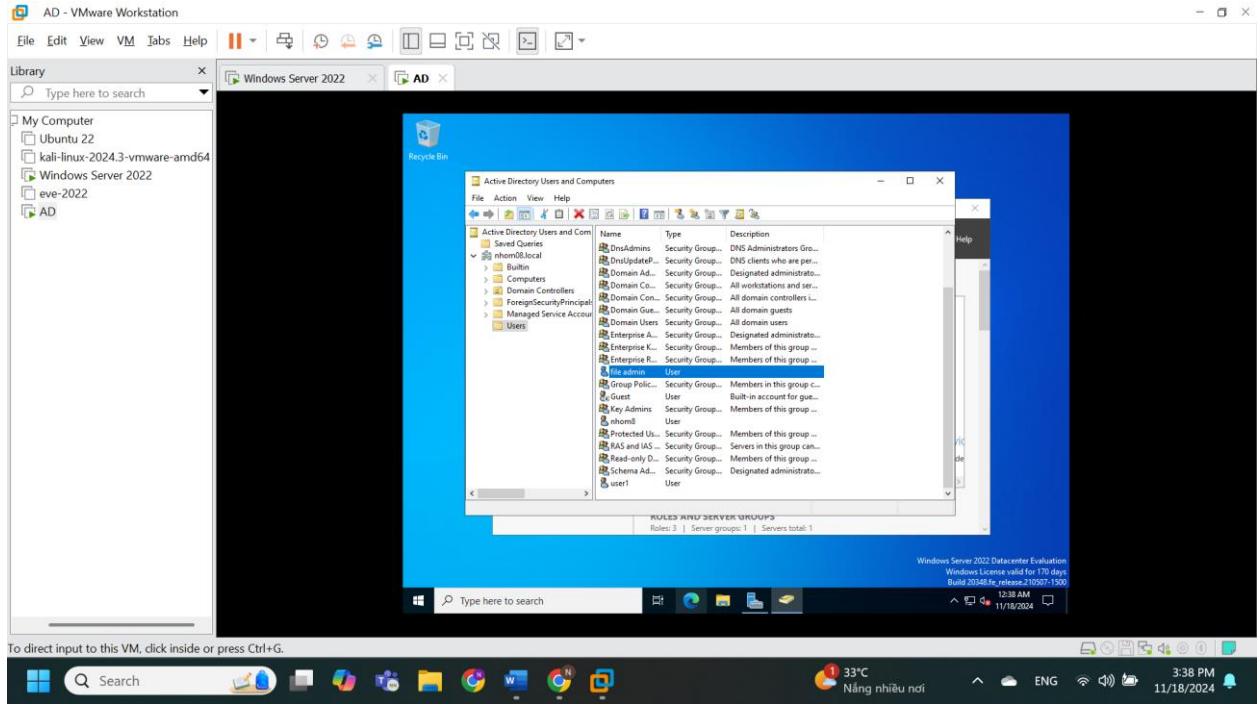
Bước 3: Tạo user trong Domain

- Đăng nhập vào máy chủ Active Directory (máy AD) với tài khoản NHOM08\Administrator (tài khoản trong domain).

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

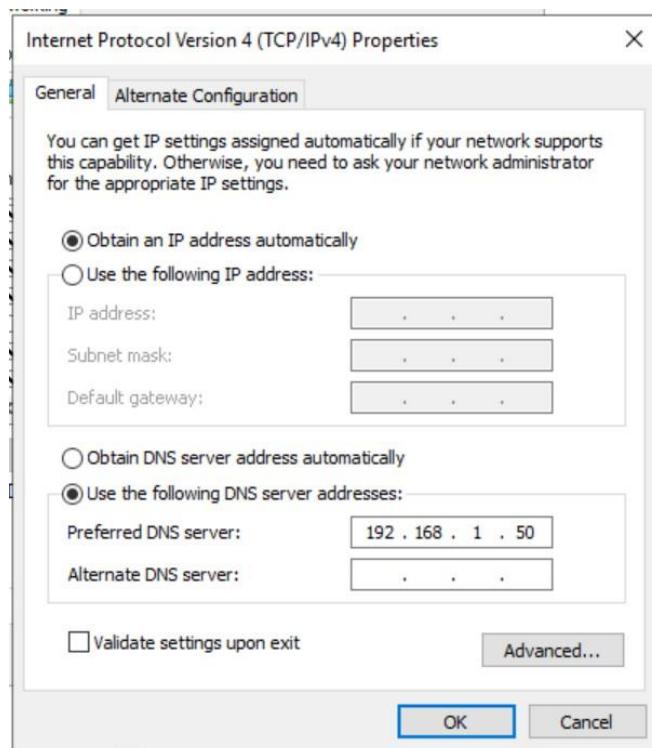
- Trong nhomX.local > Users, nhấp chuột phải trong khung hiển thị các user, chọn New > User và nhập thông tin user muốn tạo.



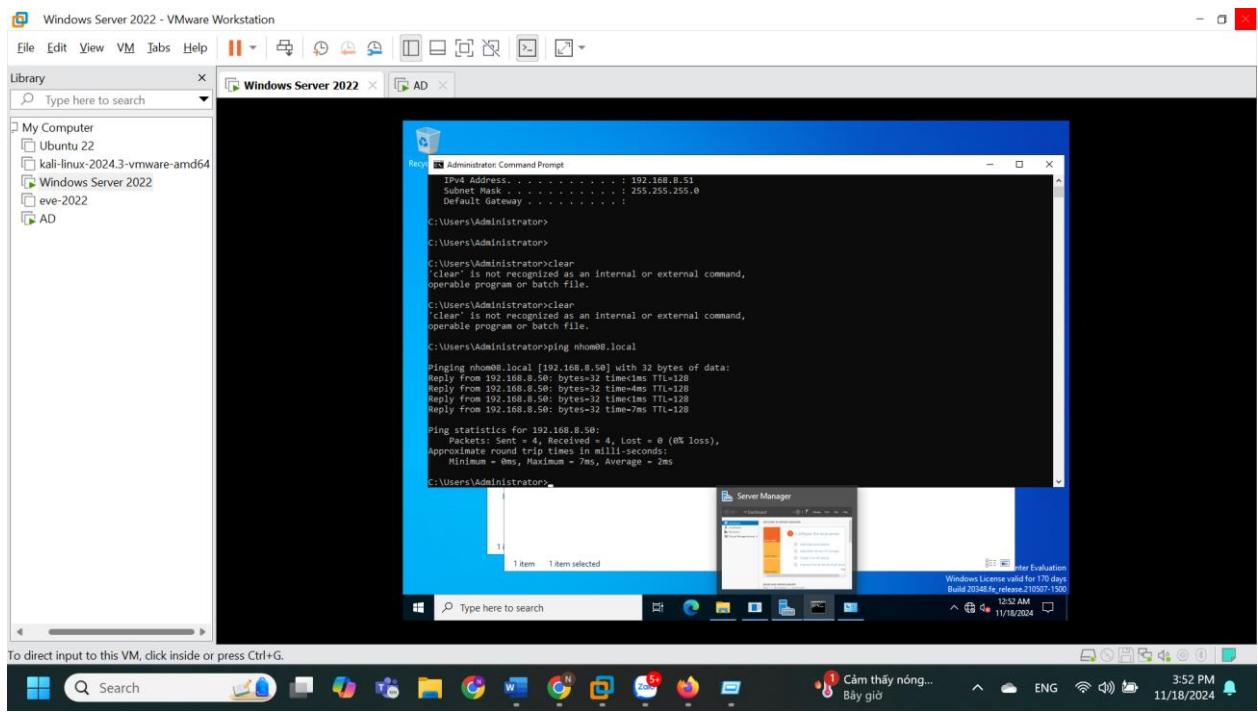


Bước 4: Thêm File Server vào domain đã tạo

- Kết quả phân giải tên miền



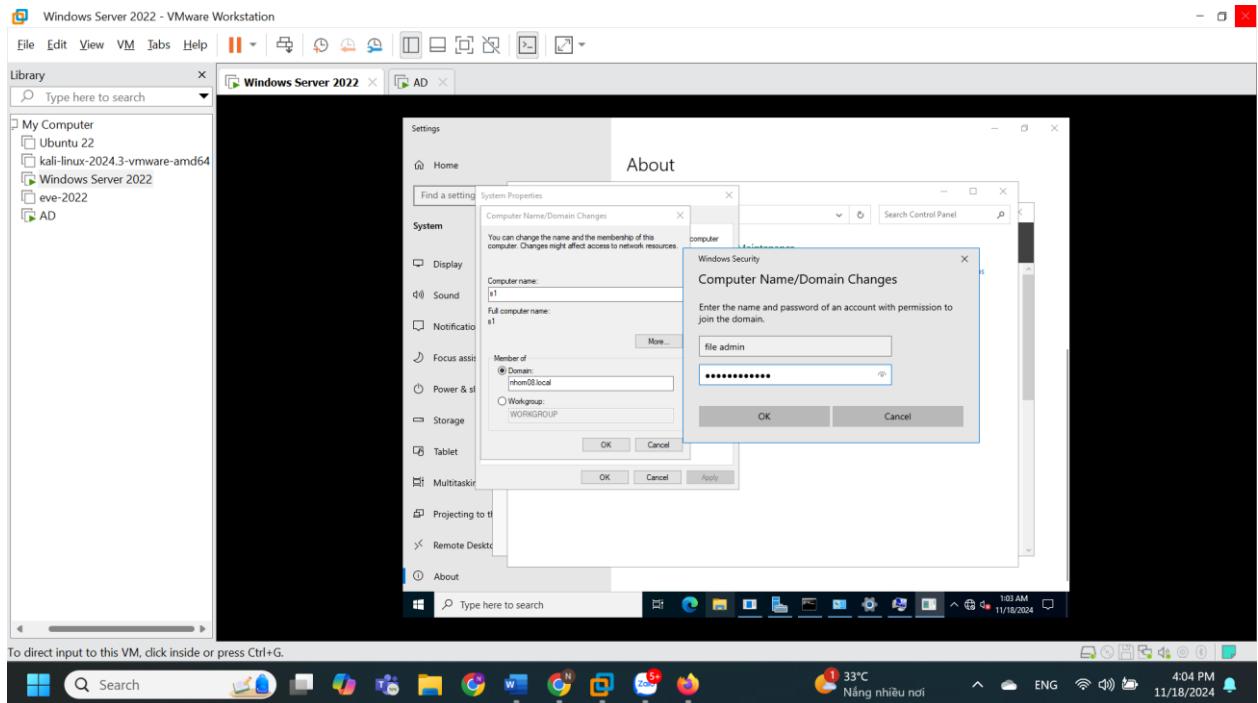
- Vào file server để ping tới nhom08.local



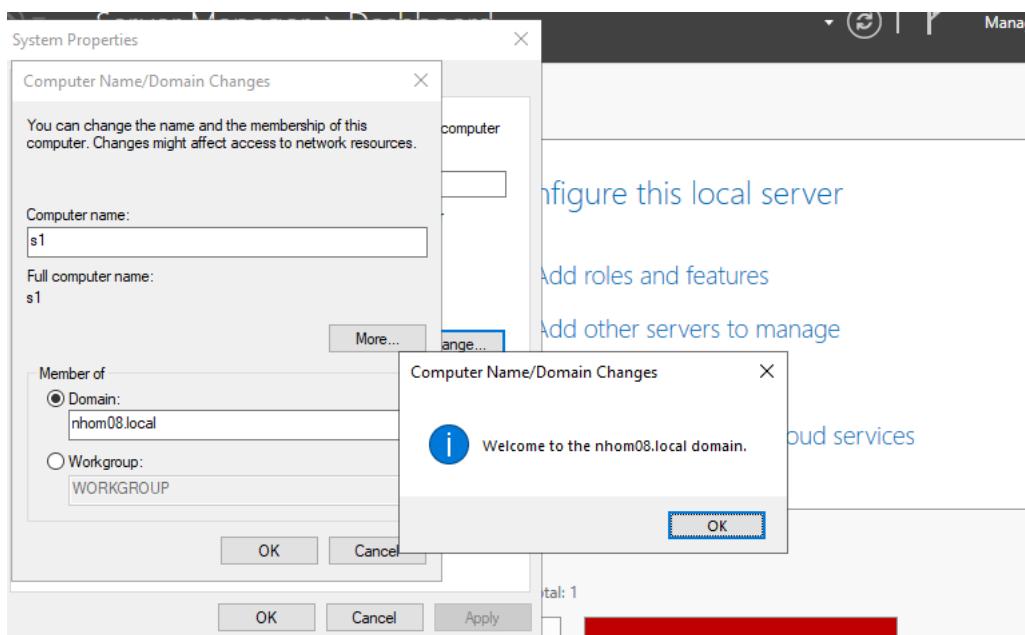
Vào mục System trong Control Panel, chọn Change settings.

- 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

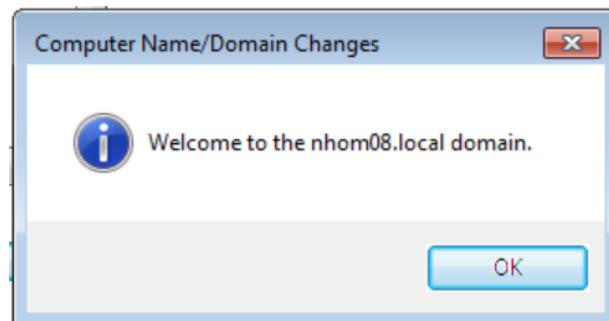
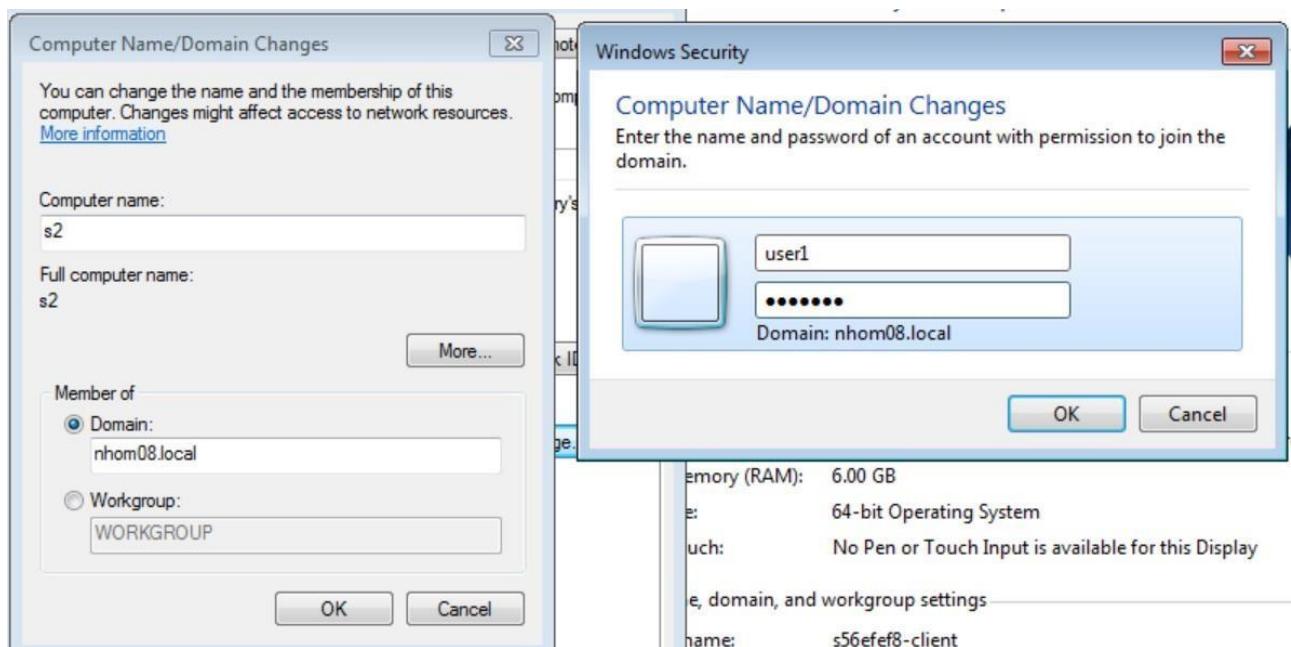
Tại file server



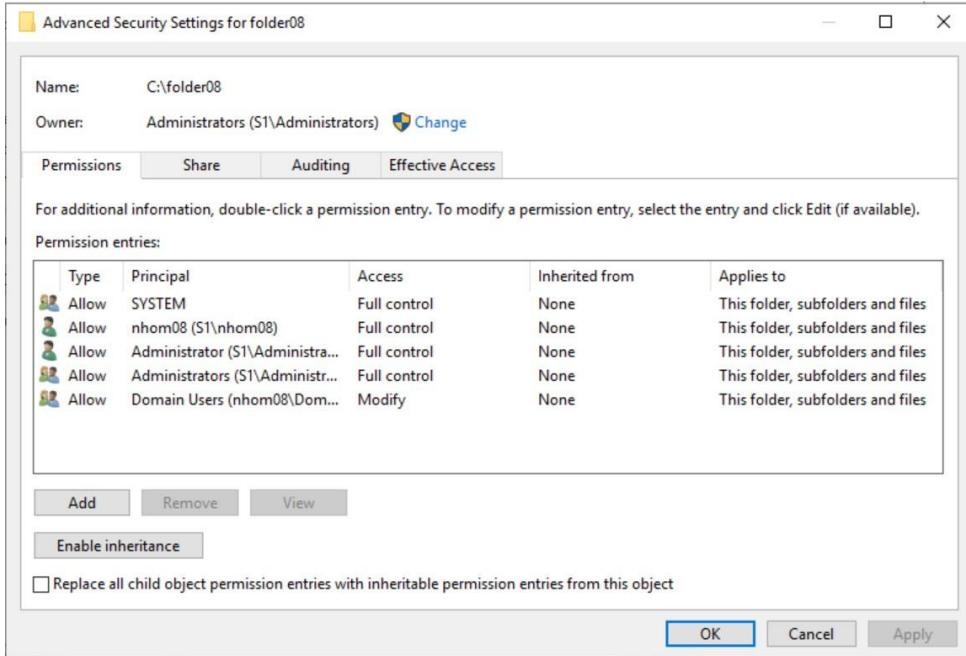
Thành công thêm vào domain



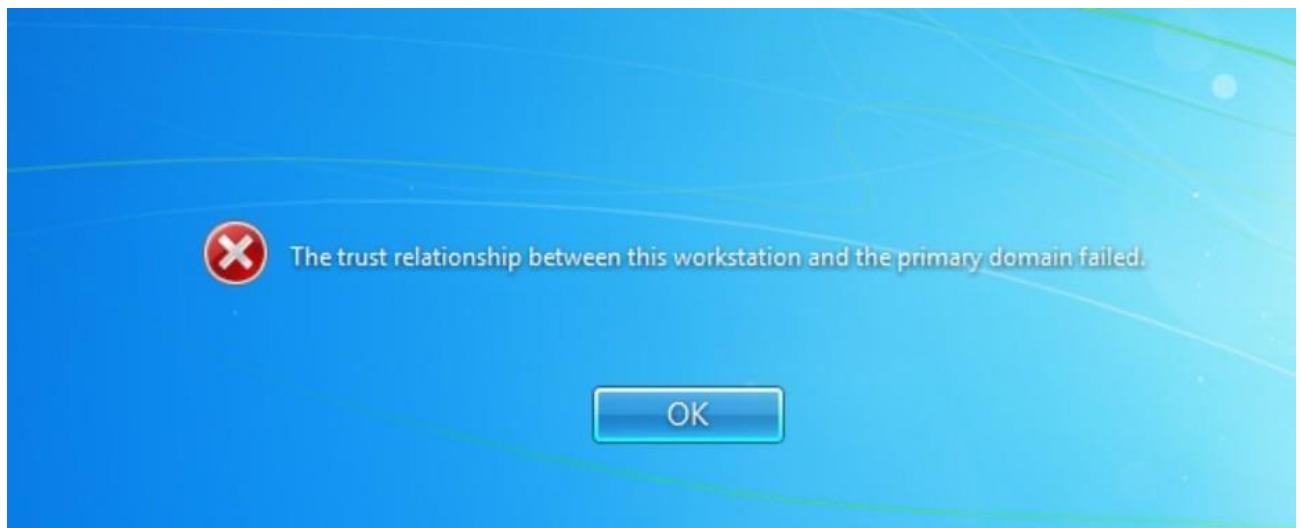
* Bước 5: Thêm máy client vào domain đã tạo.



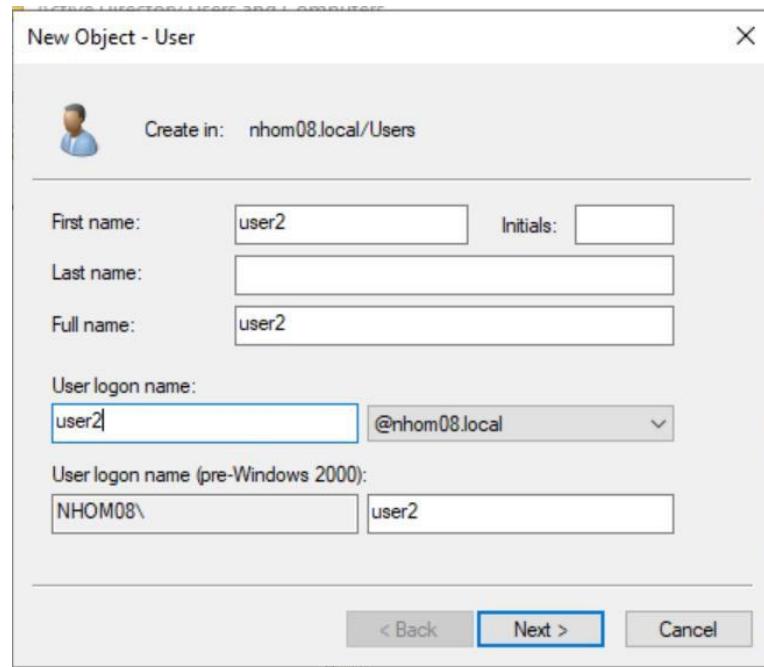
Bước 6: Phân quyền và chia sẻ file từ File Server



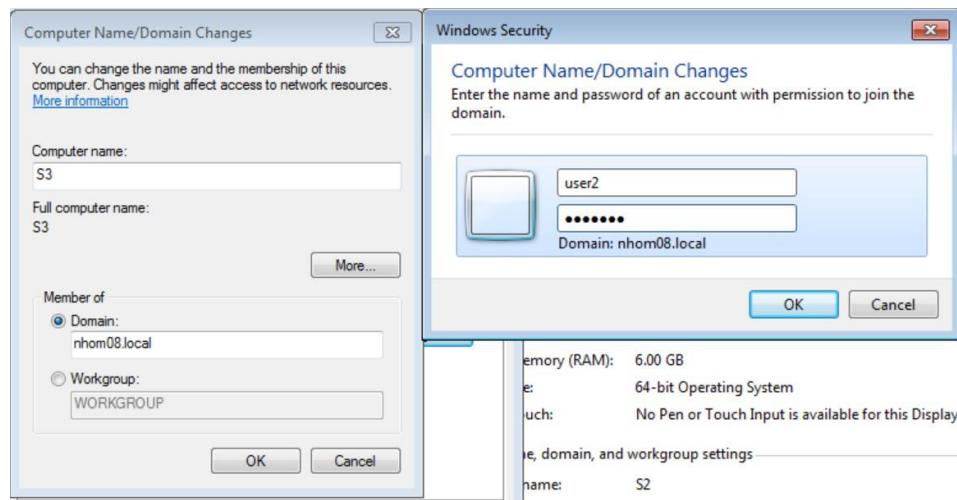
Bước 7: Tạo máy Client, đăng nhập với tài khoản NHOM08\user1



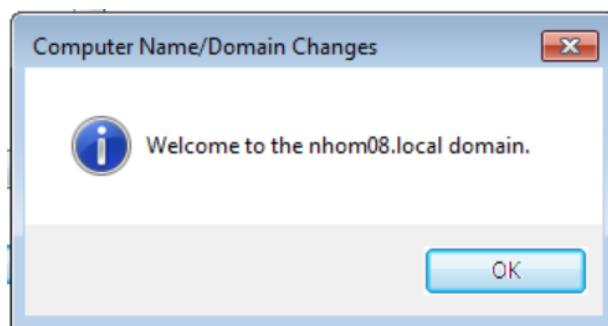
- Nhóm quyết định tạo user2 để thay thế cho user1, tạo như các bước tương tự với user1:



Tạo user user2



Tiến hành thêm Client vào domain nhom08.local



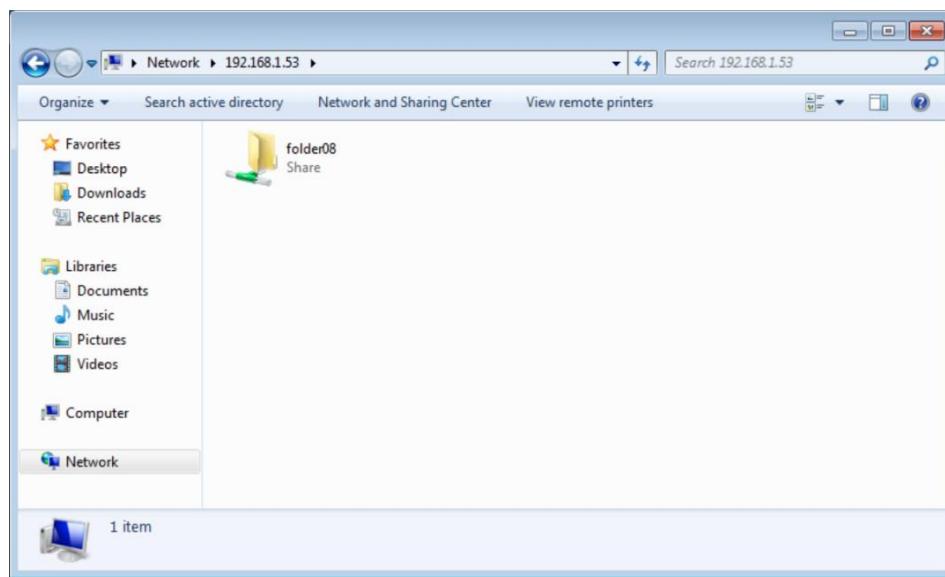
Thông báo xác thực thành công, Client sẽ được thêm vào domain.

- Sau đó Tạo máy Client, đăng nhập với tài khoản NHOM08\user2

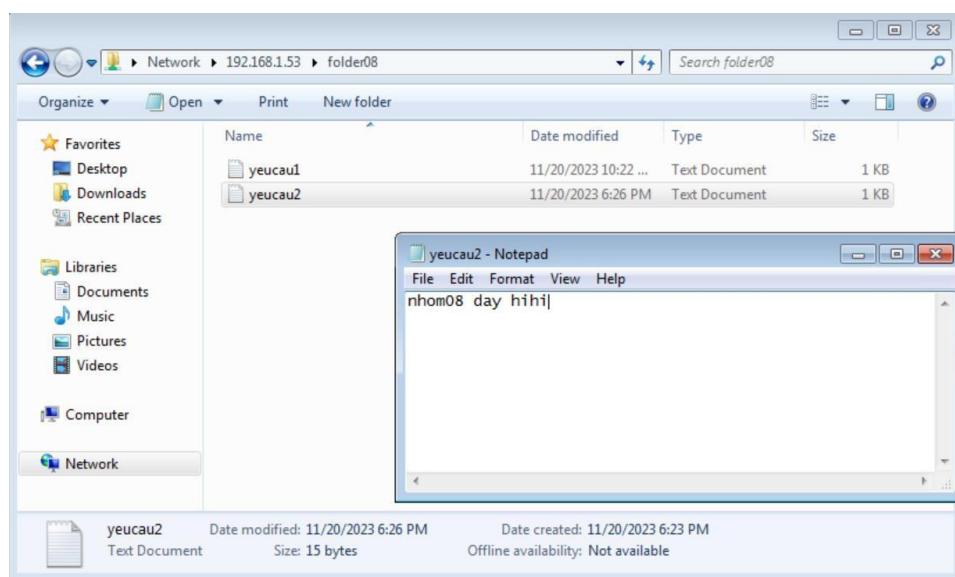


Đăng nhập vào tài khoản NHOM08\user2 tại máy Client

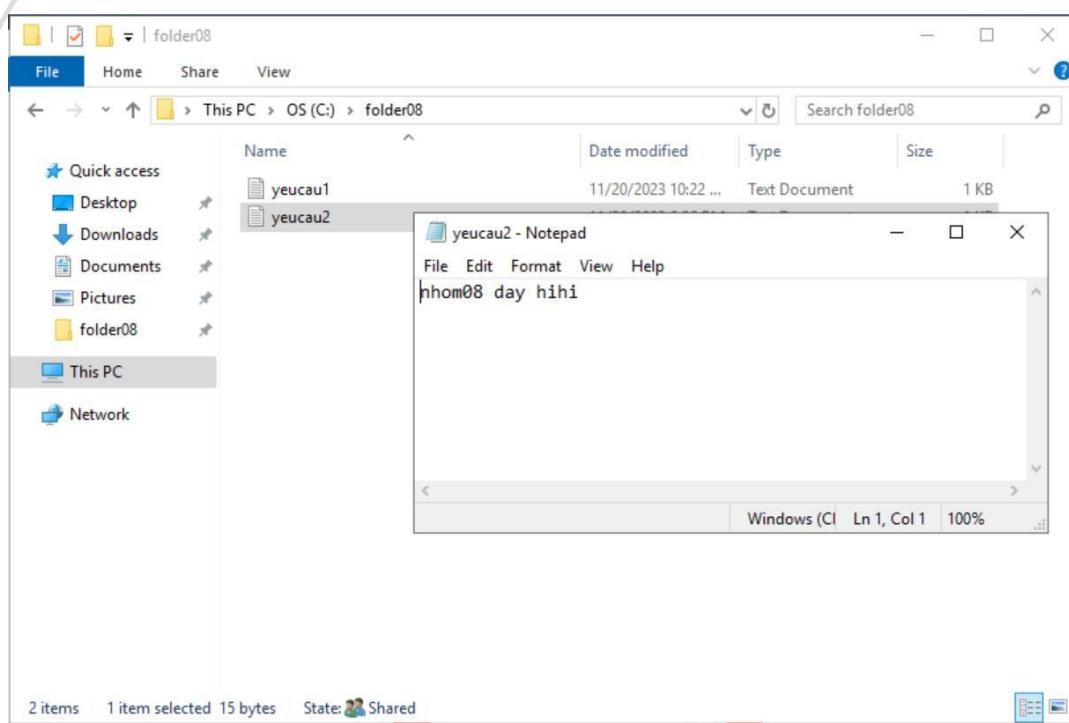
Bước 8: Vào Run và kết nối vào File Server. Kiểm tra các thao tác đọc, ghi dữ liệu tại thư mục folder08



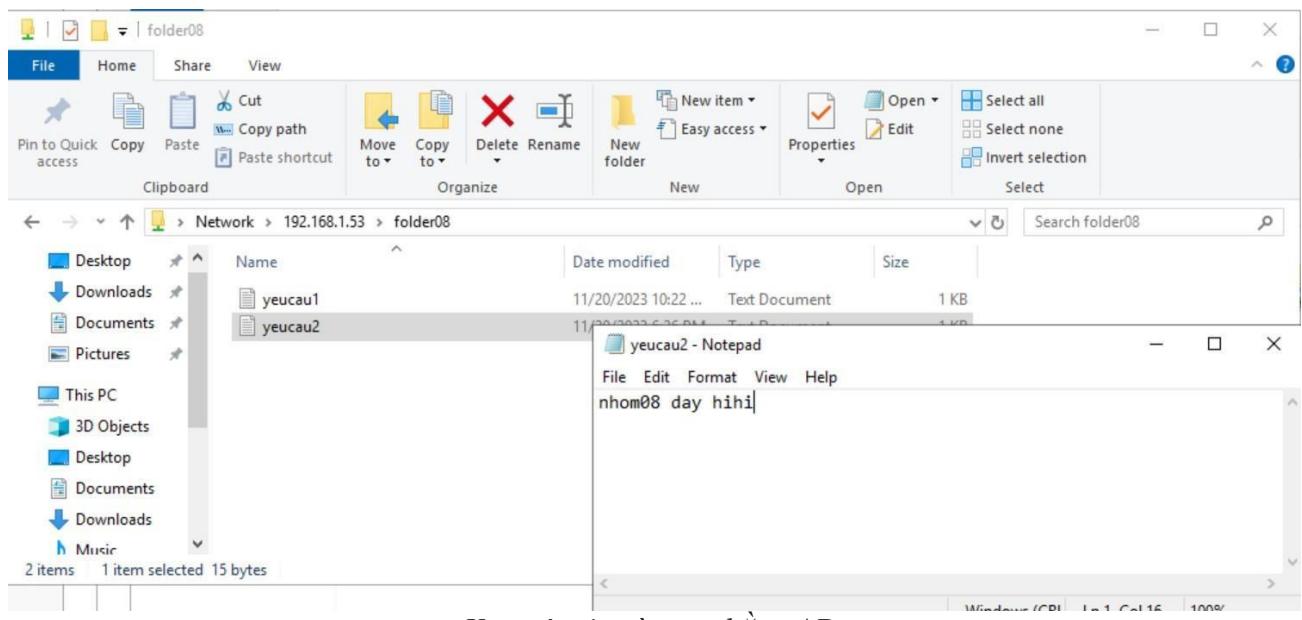
Kết nối vào File Server



Tạo tập tin trong máy Client



Xem tập tin vừa tạo bằng File Server



Xem tập tin vừa tạo bằng AD

Trình bày và giải thích khác biệt so với việc truy cập thư mục này ở mô hình Workgroup ở Phần 1?

- Khác biệt: User có thể xem và tạo tập tin, đồng thời có sự đồng bộ giữa các máy.
- Giải thích: So với mô hình **Workgroup** thì **Domain** sẽ có 1 máy làm server quản lý việc chia sẻ folder nhom08. **Server** quản lý các quyền của **User** trong **Domain** nên các user

được thêm vào domain với thông tin chứng thực được tạo từ trước thì có quyền xem và chỉnh sửa các file theo quyền đã được cấp từ trước.

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

1. Additional Domain Controller (ADC) là gì?

- Active Directory Domain Service (AD DS): Là trung tâm quản lý và chứng thực cho các đối tượng như: group, user, computer account... AD DS cung cấp tất cả các thông tin của một đối tượng cho các dịch vụ cần thiết, ví dụ cung cấp đầy đủ thông tin cho việc chứng thực khi user đăng nhập vào máy tính hay user truy cập tài nguyên...
- Primary Domain Controller (PDC): Trong một domain có thể có nhiều Domain Controller. Domain Controller đầu tiên gọi là Primary Domain Controller (PDC) hay Root domain
- Additional Domain Controller (ADC): Các Domain Controller thêm vào được gọi là Additional Domain Controller (ADC). Additional Domain Controller có thể coi như là giải pháp load balancing và failover của hệ thống Domain Controller, trong hệ thống mạng có thể có một hoặc nhiều Additional Domain. Dữ liệu chứng thực người dùng, DNS... của Domain được đồng bộ giữa Primary Domain Controller (PDC) và các Additional Domain Controller (ADC)

2. Mô hình ADC hoạt động như thế nào?

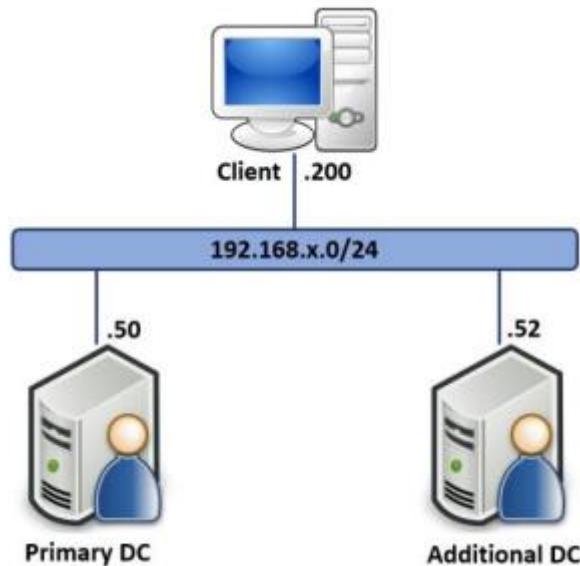
Additional Domain Controller (ADC) là một máy chủ trong mạng Active Directory (AD) mà được cấu hình để sao chép và đồng bộ hóa dữ liệu từ một Domain Controller (DC) chính. ADC hoạt động bằng cách sao chép cơ sở dữ liệu AD từ DC chính và cung cấp khả năng truy cập và xử lý yêu cầu từ người dùng và các dịch vụ khác. ADC giúp tăng cường tính sẵn sàng và khả năng chịu lỗi của hệ thống AD bằng cách phân phối khả năng xử lý và lưu trữ dữ liệu trên nhiều máy chủ trong mạng

3. Khi nào cần sử dụng ADC?

- Khi hệ thống cần nhiều sites: Nếu muốn các site được quản lý theo mô hình AD với cùng domain, ta cần dựng ADC ở các site để tăng tốc độ chứng thực cho các user ở từng site.
- Khi hệ thống có 1 site nhưng số lượng user lớn → Dựng thêm ADC để cân bằng tải giúp hệ thống nhanh hơn, tránh tình trạng quá tải và tắc nghẽn mạng
- Khi hệ thống có 1 site và 1 Domain Controller, hệ thống nhỏ → Dựng thêm ADC để đề phòng tình trạng khi DC gặp sự cố thì hệ thống công ty tê liệt dẫn đến tổn thất về kinh tế lẫn thời gian.

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

- Mô hình mạng như sau



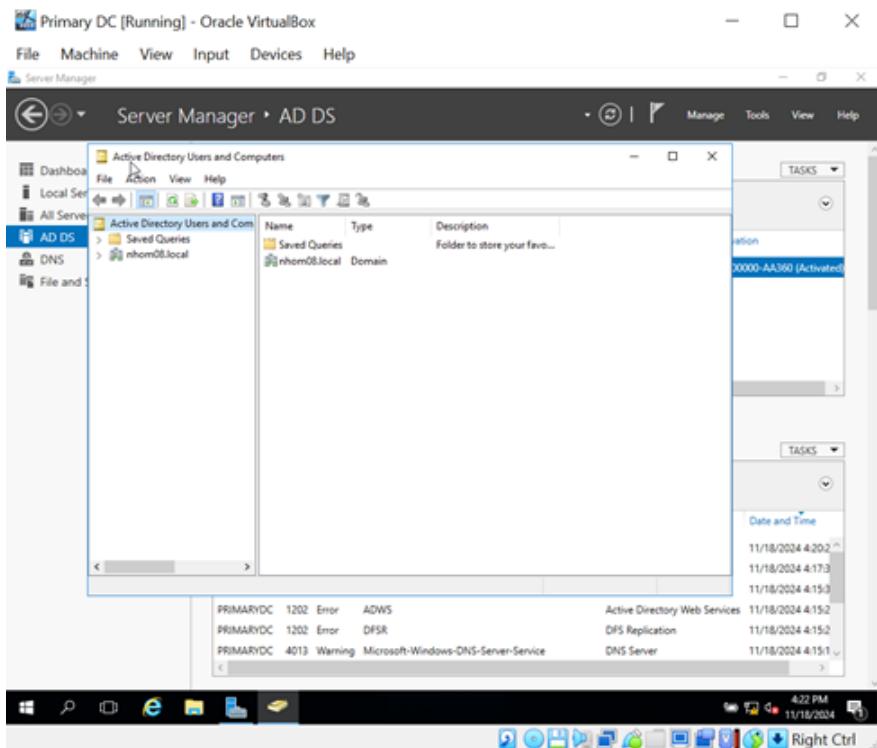
- IP của các máy.

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7	192.168.1.200/24	192.168.1.50 192.168.1.52
Primary DC	Windows Server 2019	192.168.1.50/24	192.168.1.50 192.168.1.52
Additional DC	Windows Server 2019	192.168.1.52/24	192.168.1.52 192.168.1.50

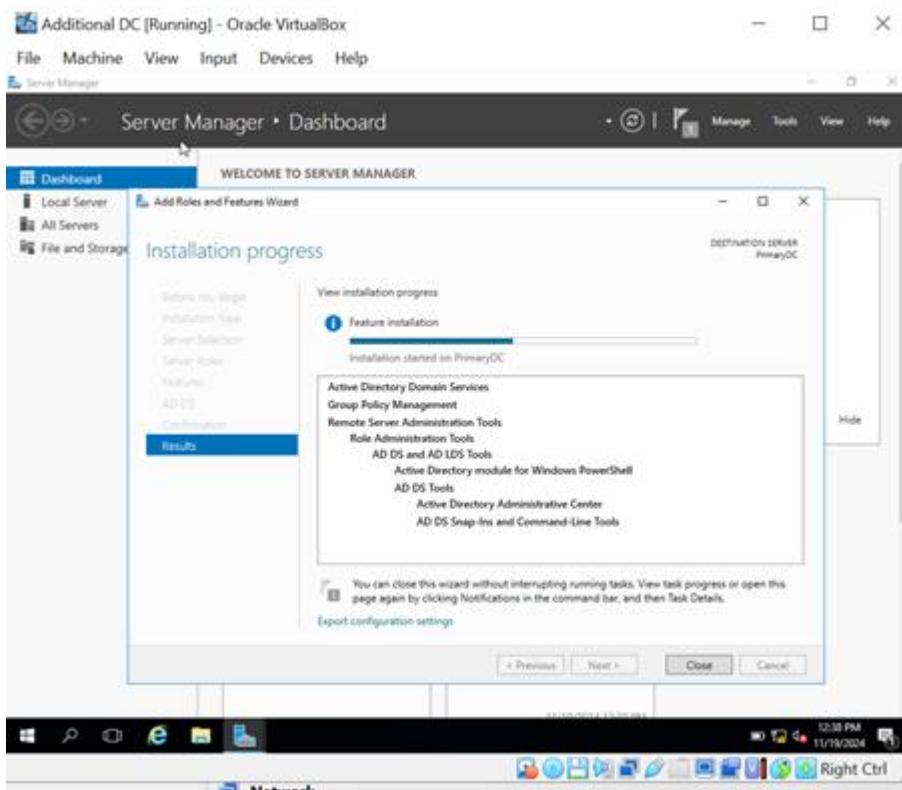
A. Triển khai mô hình Additional Domain Controller (ADC) với các thông tin trên

- Tạo Primary DC (192.168.1.50): thực hiện tạo domain nhom08.local

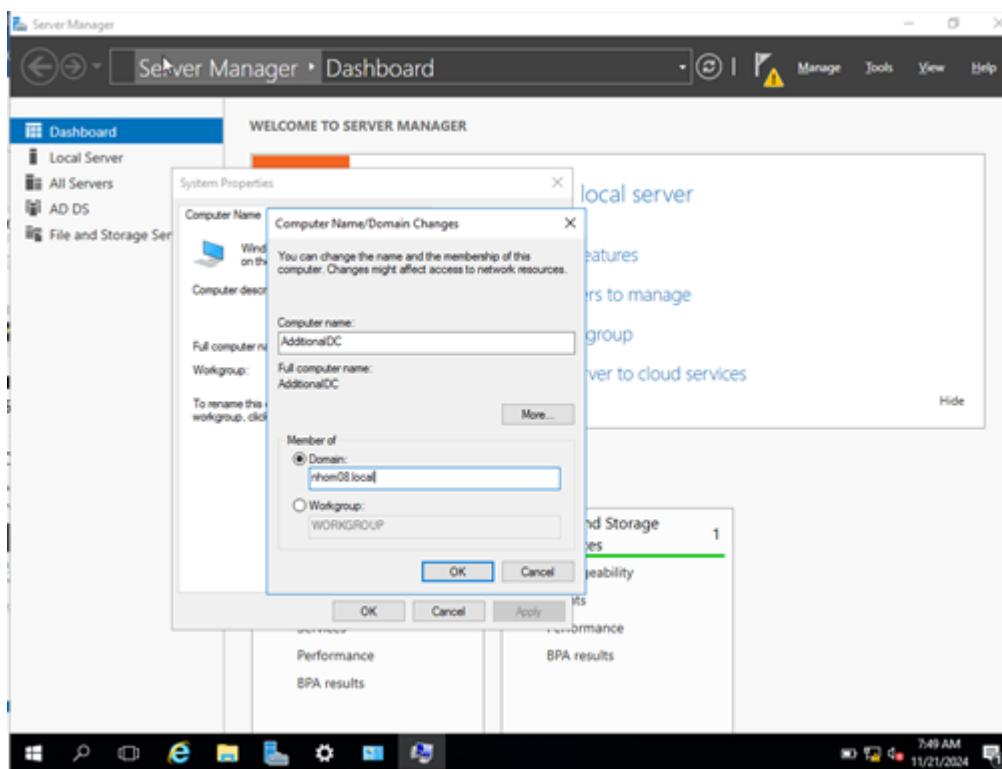
Lab 4: Setting up Active Directory in Windows Server



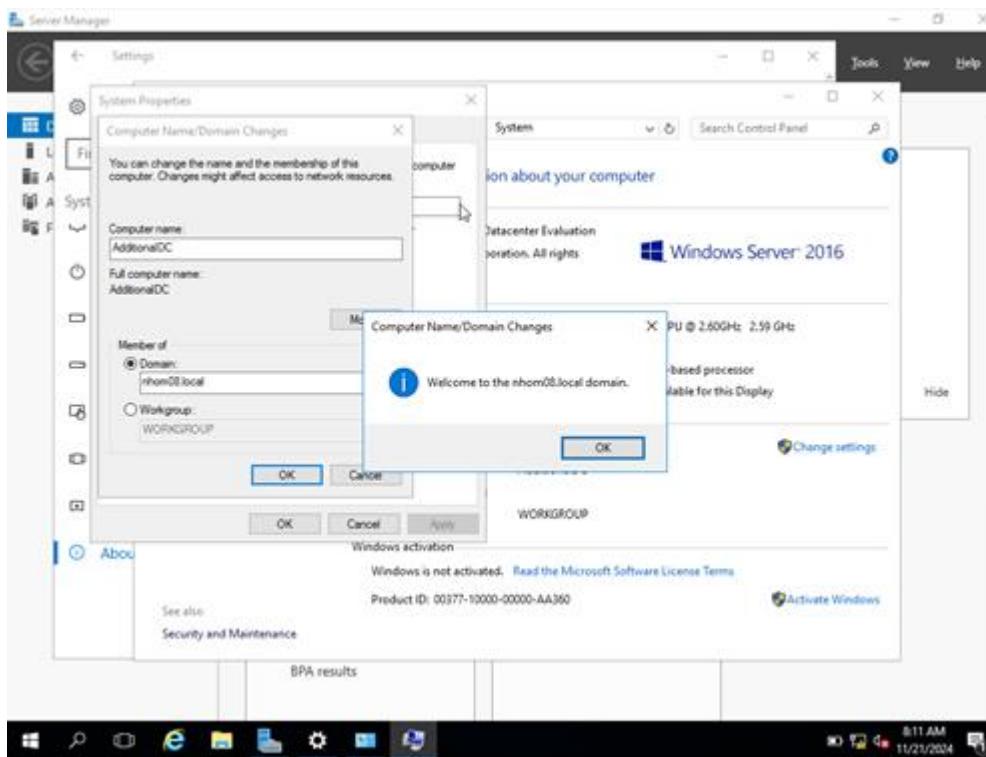
- Tạo Additional DC:
- + Triển khai AD cho máy Additional DC:



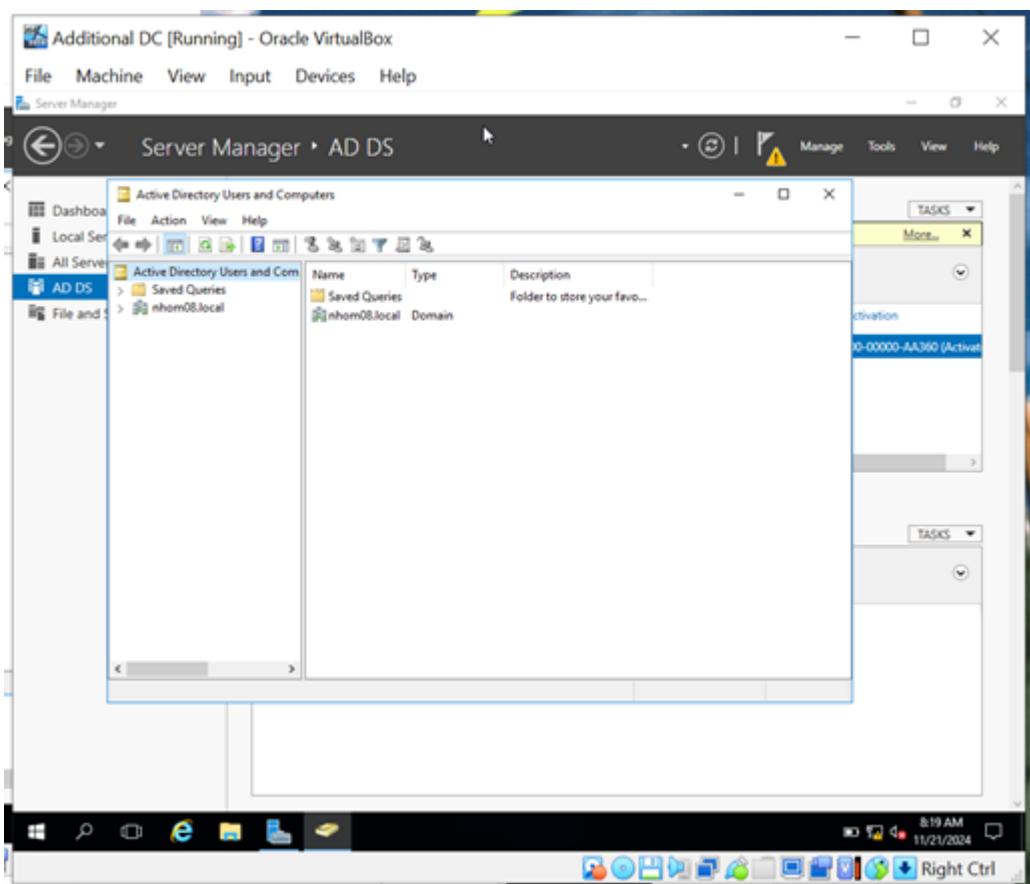
- + Thực hiện join vào Domain:



+ Nhập username và password cho tài khoản Administrator ==> Đã vào domain nhom08.local thành công

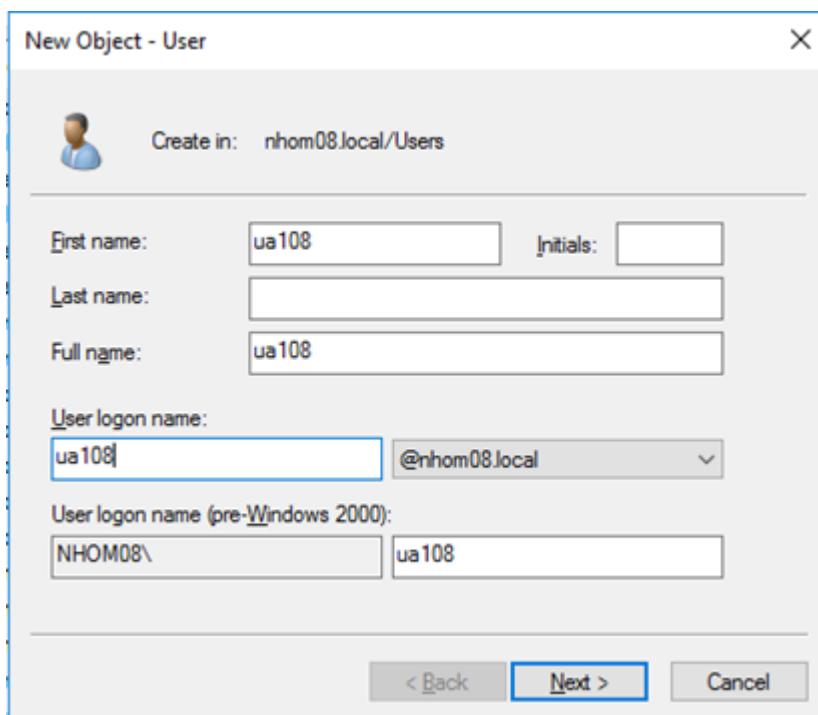


+ Nâng cấp Active Directory lên Additional Domain Controller: Vào Server Manager sẽ thấy biểu tượng cảnh báo, nhấp vào và chọn Promote this server to a domain controller để thực hiện tiếp phần thiết lập.



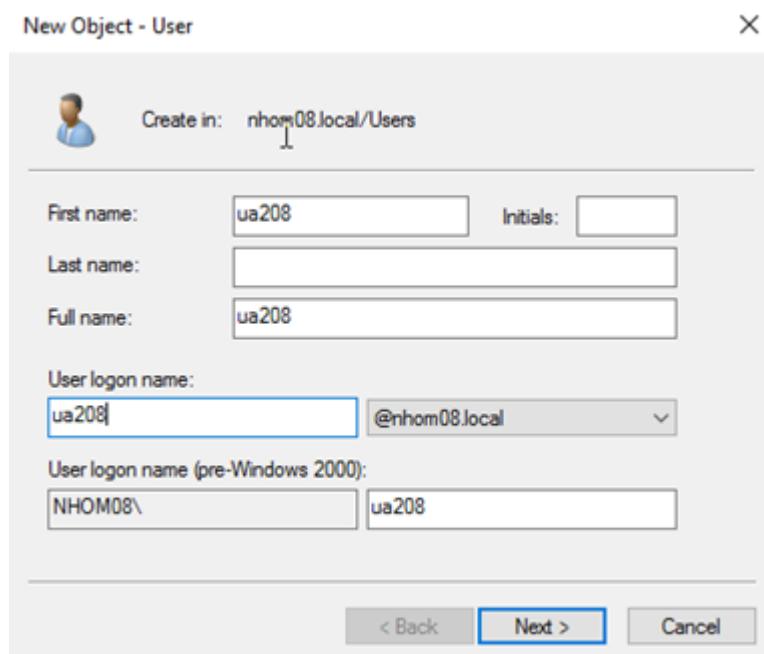
B. Thực hiện các yêu cầu theo đề bài:

- Tạo user ua108 trên Primary DC. Kiểm tra thông tin user này trên Additional DC.



- Kiểm tra lại thông tin user trong mục Active Directory Users and Computers của Additional DC

- b. Tạo user ua208 trên Additional DC. Kiểm tra thông tin user này trên Primary DC.



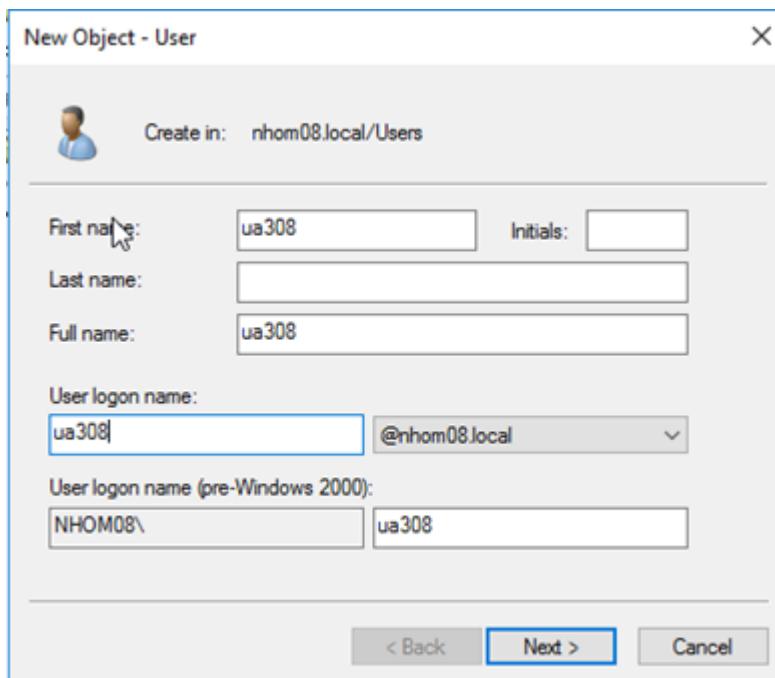
- Kiểm tra lại thông tin user trong Active Directory Users and Computers của Primary DC

Name	Type	Description
DnsAdmins	Security Group...	DNS Administrators Group
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	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 ...
RAS and IAS...	Security Group...	Servers in this group ca...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
ua108	User	
ua208	User	
vboxuser	User	

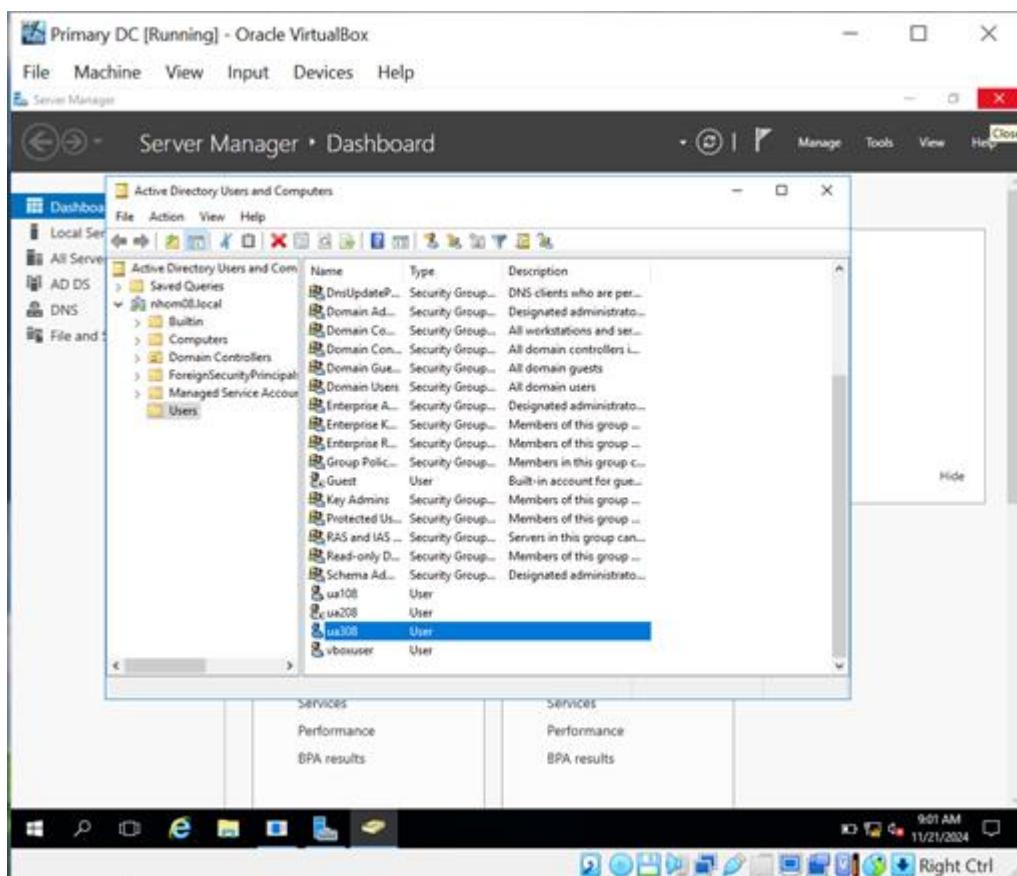
c. Tắt máy Primary DC, thêm user ua308 trên Additional DC. Sau đó mở lại Primary DC và kiểm tra thông tin user này trên Primary DC.

- Tắt Primary DC.

- Thực hiện thêm user ua308 trên Addtional DC:

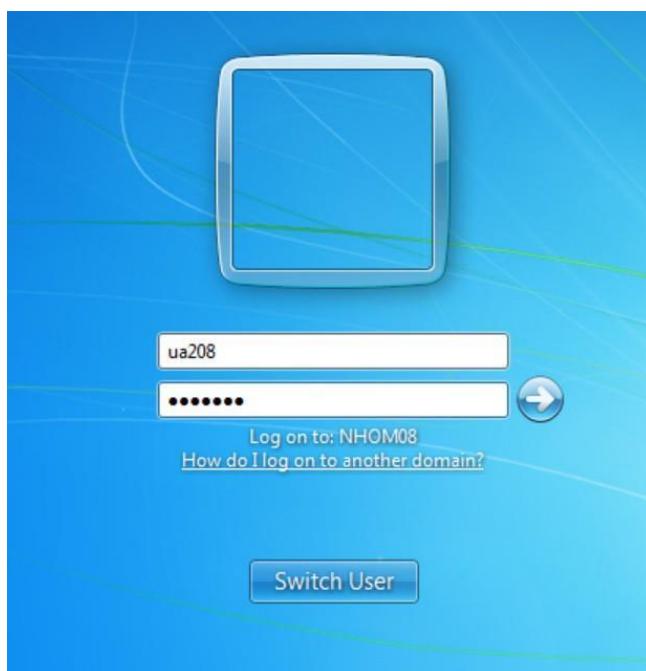


- Bật Primary DC lên và kiểm tra thông tin user:



d. Tắt máy Primary DC, login ua2X trên máy Client. Giải thích kết quả.

- Tắt Primary DC, thực hiện login user ua208:



- Thông tin user đăng nhập:



- **Giải thích kết quả:** Tắt máy PDC, nhưng vẫn login user ua208 trên máy Client thành công vì ADC có thể xem là 1 domain phụ, khi tắt Primary DC thì ADC đã thay thế Primary DC để trở thành Domain Controller. Vì vậy có thể ADC có sử dụng thông tin user của Primary DC để chứng thực và cho phép Client đăng nhập vào user ua208.

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

1. **Read-Only Domain Controller (ADC) 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 mà các quản trị viên không thể cập nhật trực tiếp cơ sở dữ liệu Active Directory. 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?

- RODC chỉ cho phép đọc dữ liệu từ Domain Controller chính (Primary Domain Controller – PDC) mà không cho phép thay đổi dữ liệu. Nhờ đó mà RODC lưu trữ một bản sao của cơ sở dữ liệu Active Directory (AD) trên đĩa cứng của nó, giúp cung cấp dữ liệu và dịch vụ xác thực trong môi trường phân tán tốt hơn
 - RODC mặc định không lưu trữ dữ liệu người dùng nên nếu không có kết nối với PDC thì RODC không hoạt động được. Do đó, muốn RODC vẫn hoạt động thì

chúng ta phải khai báo lưu trữ dữ liệu người dùng thông qua một policy riêng của RODC.

3. Khi nào cần sử dụng RODC?

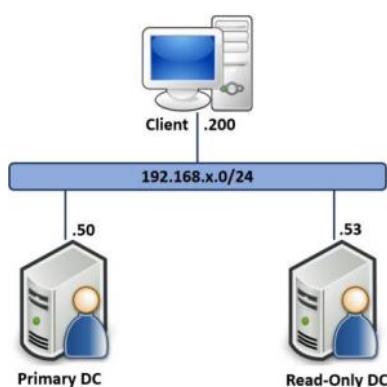
- Sử dụng RODC khi ta muốn triển khai một domain controller ở một vị trí xa máy chủ và không đảm bảo tính bảo mật. Vì RODC không thể thay đổi bất cứ thứ gì trong cơ sở dữ liệu Active Directory, và nếu chúng ta không để RODC lưu trữ thông tin về tài khoản được tạo bản sao đến thì cho dù đánh cắp được RODC thì cũng không thể sử dụng thông tin mà họ lấy được từ nó.

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

Additional Domain Controller (ADC)	Read Only Domain Controller (RODC)
Có thể đọc và ghi dữ liệu	Chỉ có thể đọc dữ liệu
Tính bảo mật thấp hơn RODC	Tính bảo mật cao hơn ADC
Là giải pháp giúp cân bằng tải	Làm giảm được phần trọng tải của máy chủ chính
Tăng tính sẵn sàng và tính chịu lỗi của hệ thống	Cung cấp an ninh tại các phòng ban chi nhánh
Khi cập nhật dữ liệu, ADC phải đồng bộ hóa dữ liệu trên toàn bộ máy chủ nên các ADC đều có khả năng như nhau	Khi cập nhật dữ liệu, RODC chỉ cần cập nhật trên máy chủ chính

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

Mô hình cần xây dựng:



Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7/8/10	192.168.x.200/24	192.168.x.53 192.168.x.50
Primary DC	Windows Server 2016	192.168.x.50/24	192.168.x.50 192.168.x.53
Read-Only DC	Windows Server 2016	192.168.x.53/24	192.168.x.53 192.168.x.50

Triển khai mô hình Read-Only Domain Controller (RODC) với thông tin như trên.

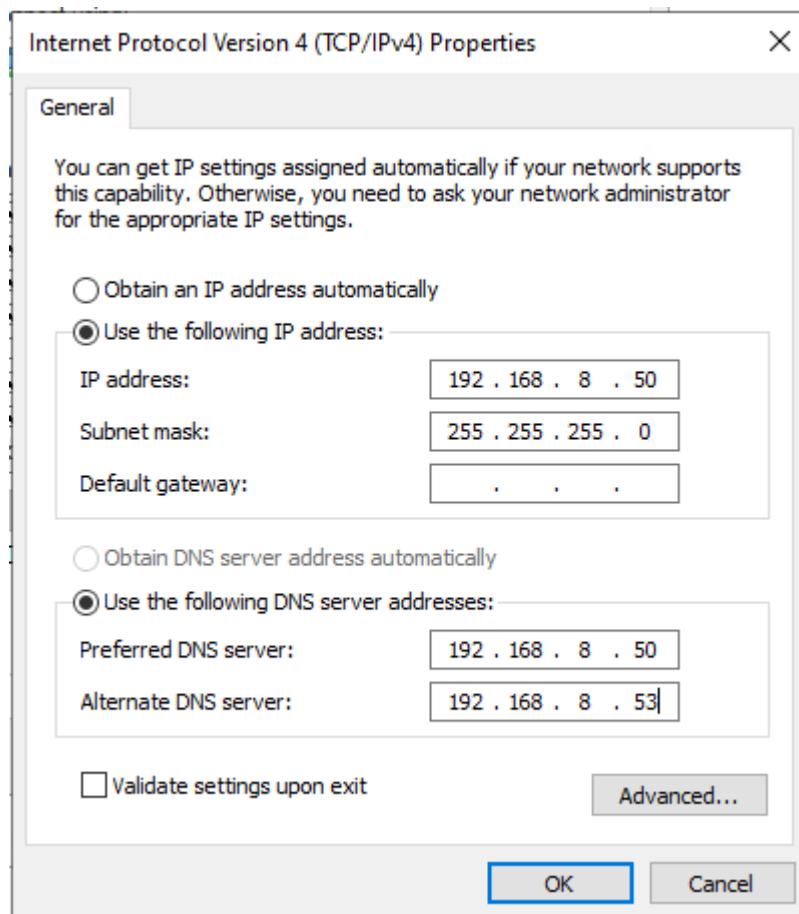
*Windows Server 2022: Primary DC

*Windows Server 2022 Clone: Read-Only DC

*Windows 10: Client

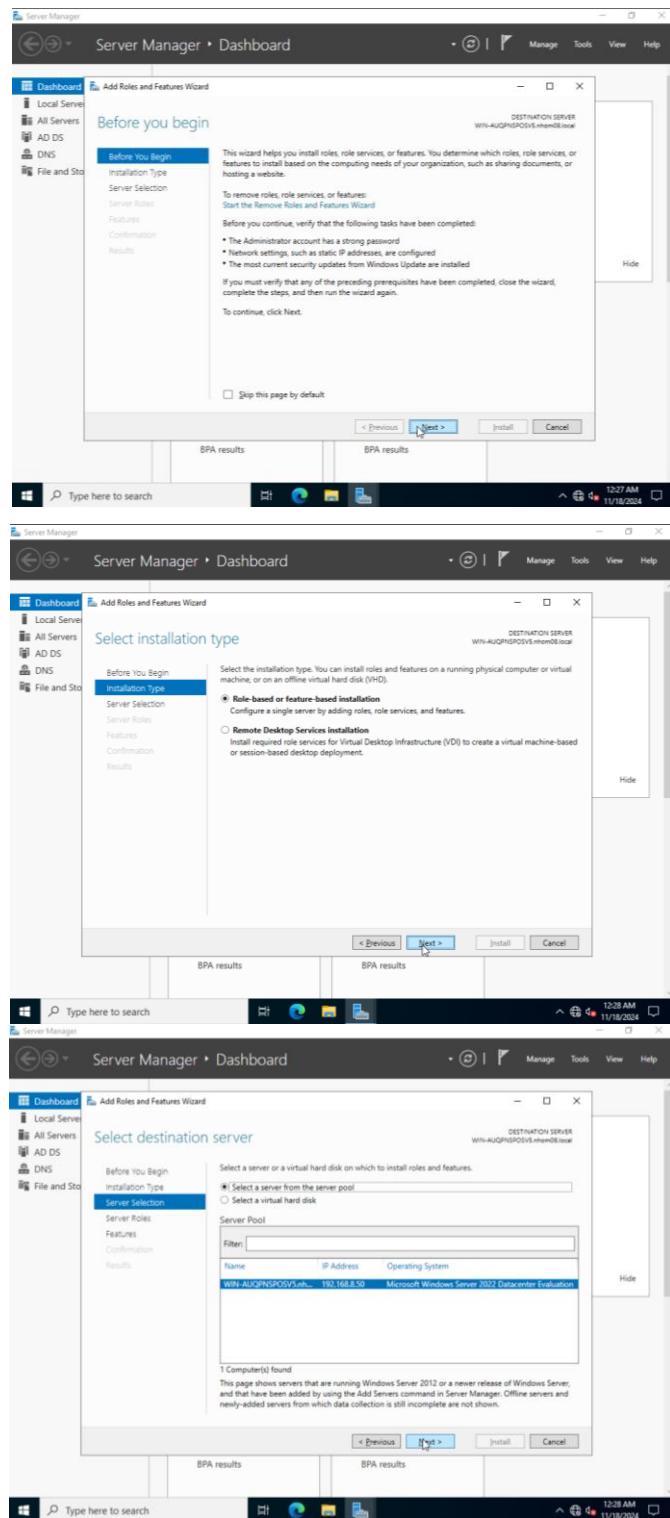
Primary DC

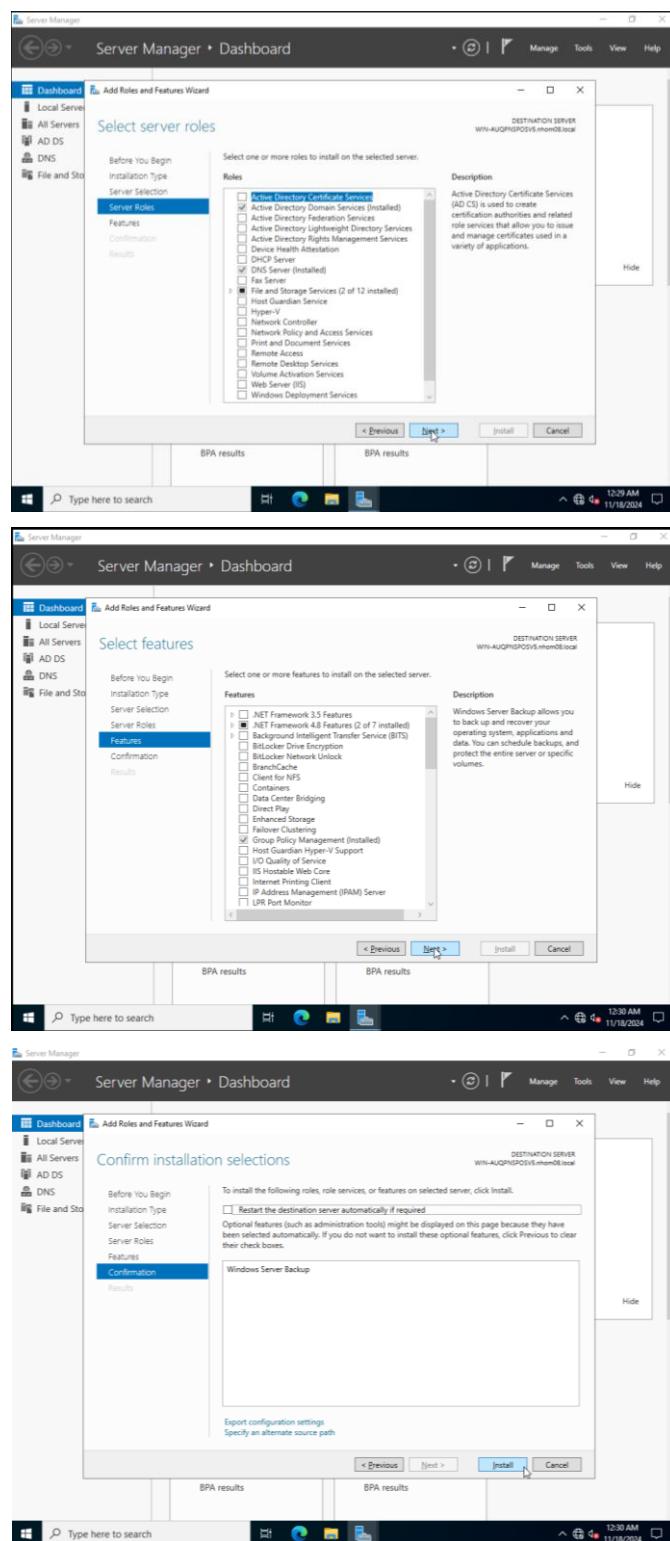
Cài đặt địa chỉ IP như đề bài yêu cầu



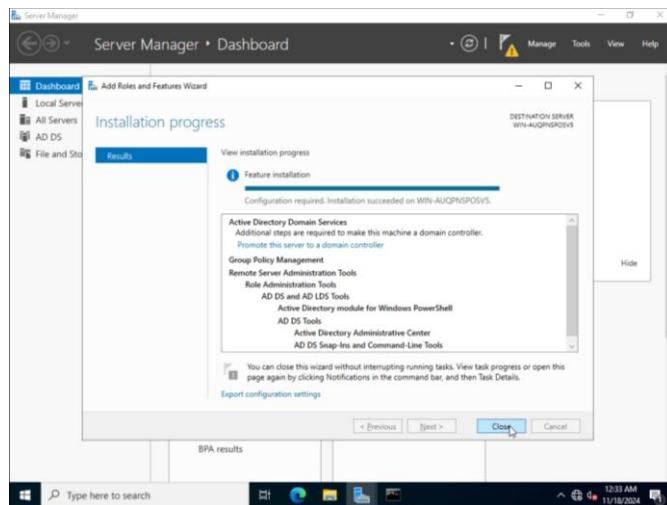
Thực hiện triển khai Active Directory trên Primary DC

Lab 4: Setting up Active Directory in Windows Server

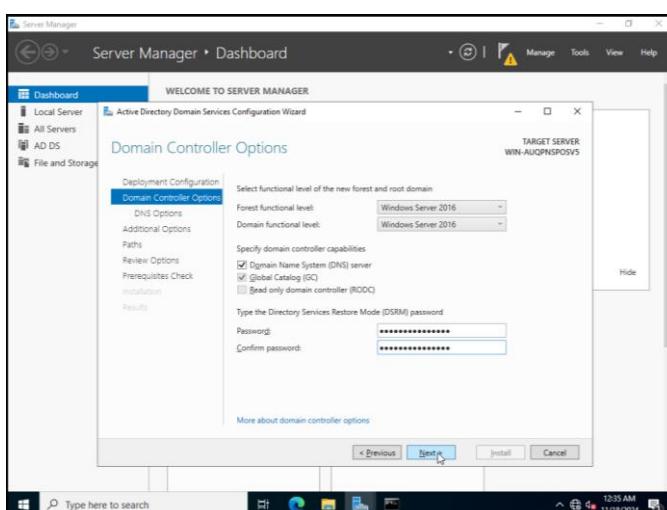
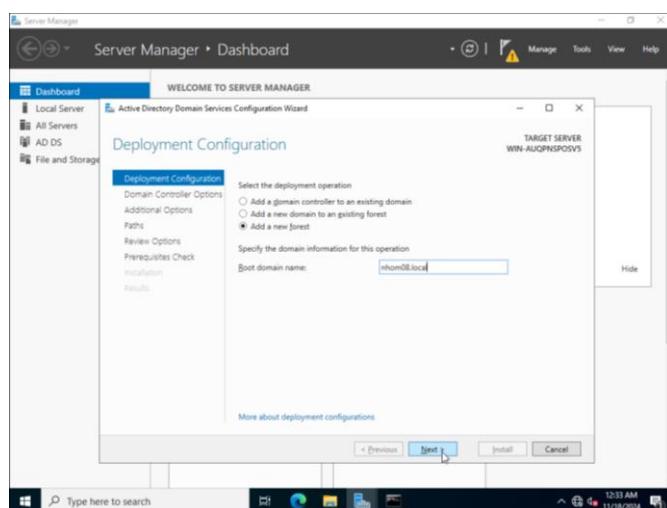


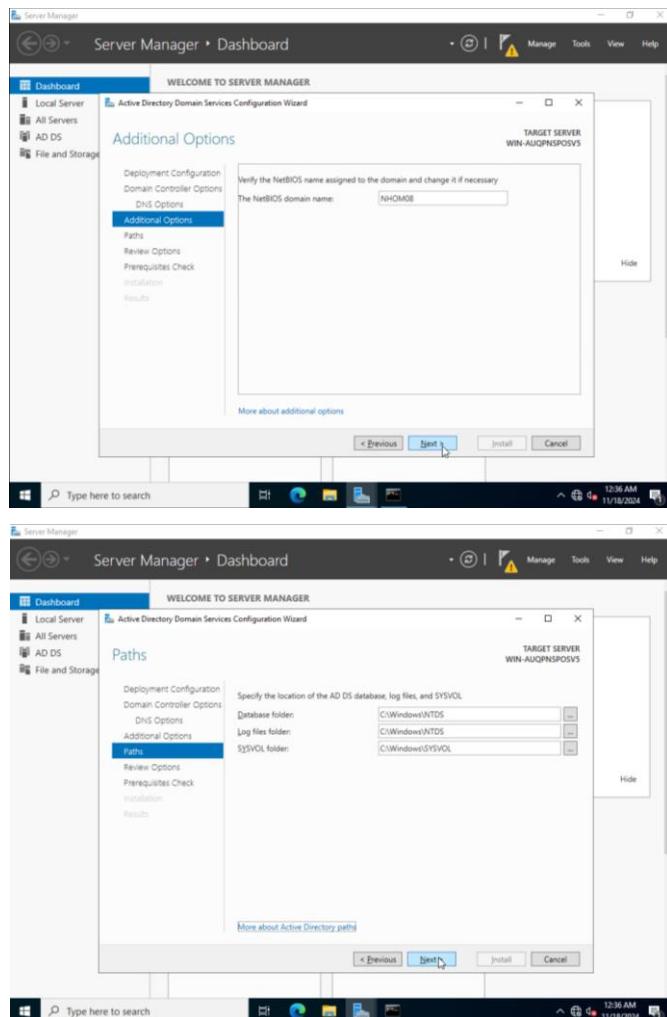


Lab 4: Setting up Active Directory in Windows Server



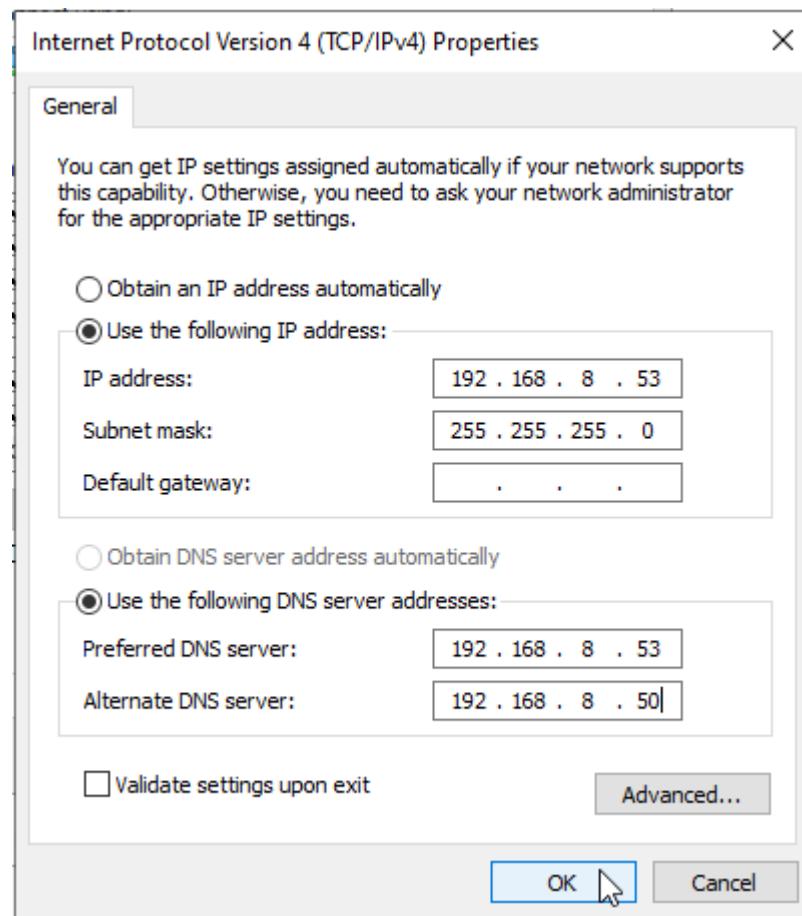
Nâng cấp Active Directory sang Additional Domain Controller trên Primary DC





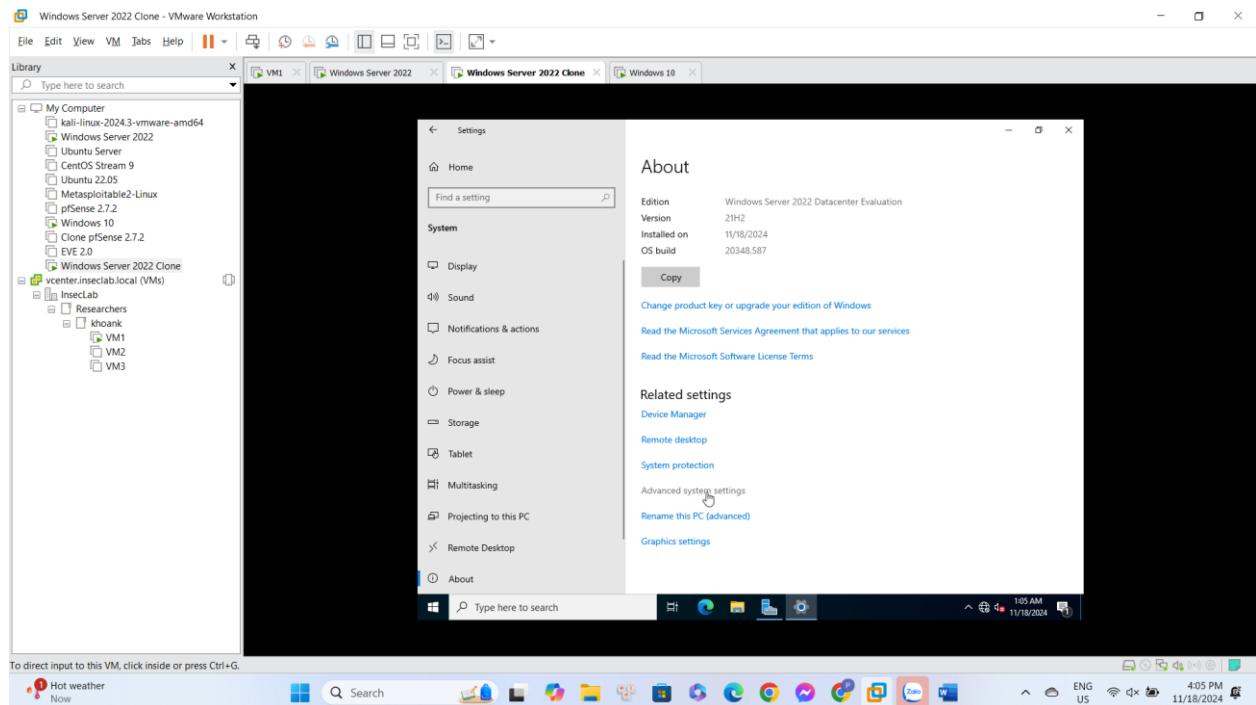
Read-Only DC

Cài đặt địa chỉ IP như đề bài yêu cầu



Thực hiện triển khai Active Directory tương tự như trên Primary DC

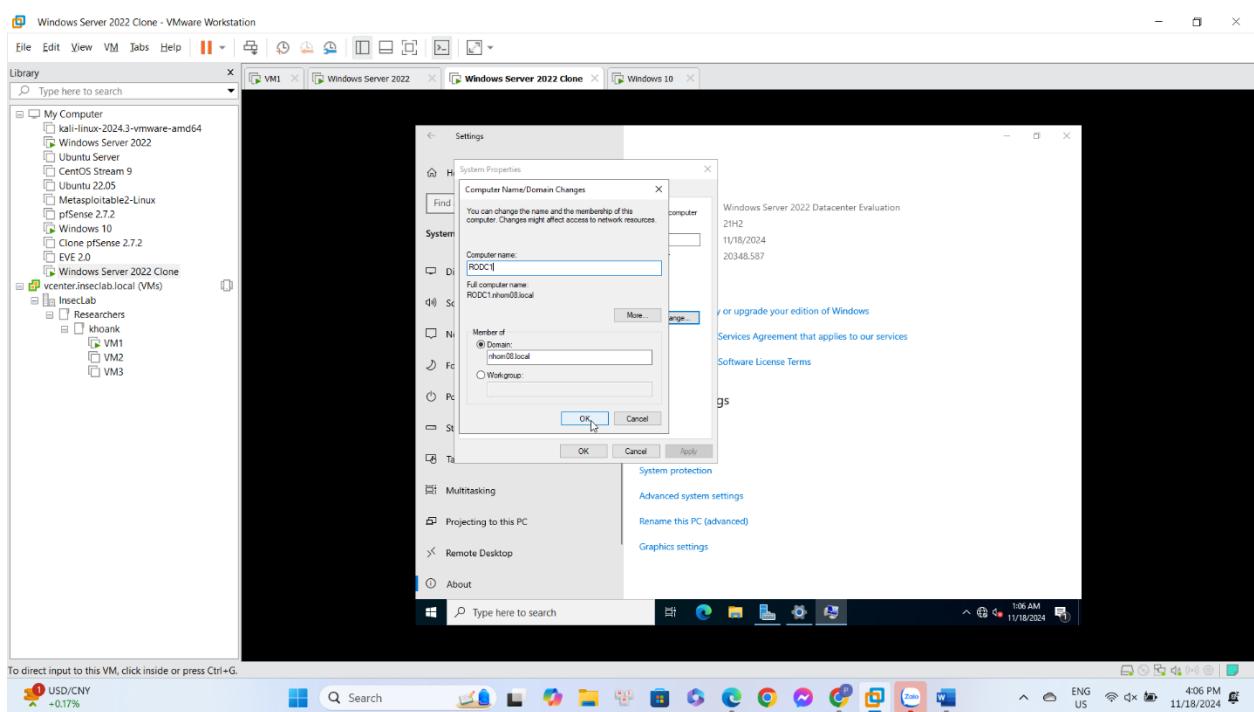
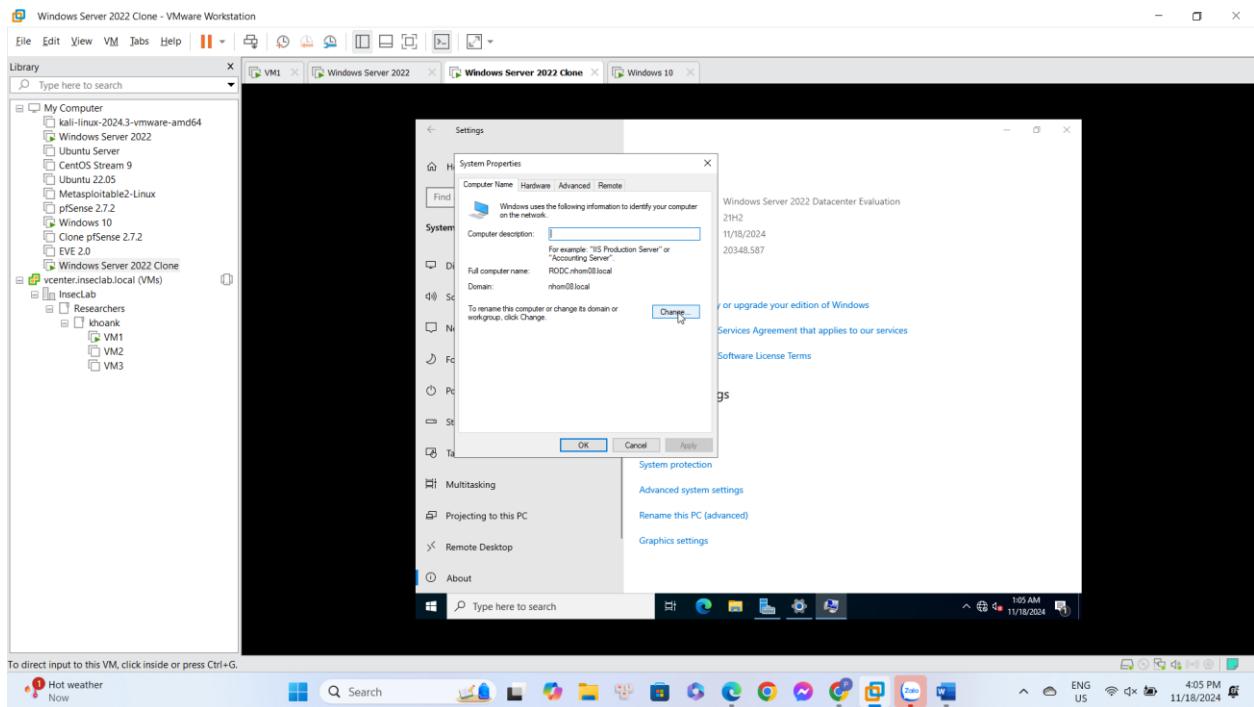
Tham gia domain (join domain) đã được tạo bởi Primary DC

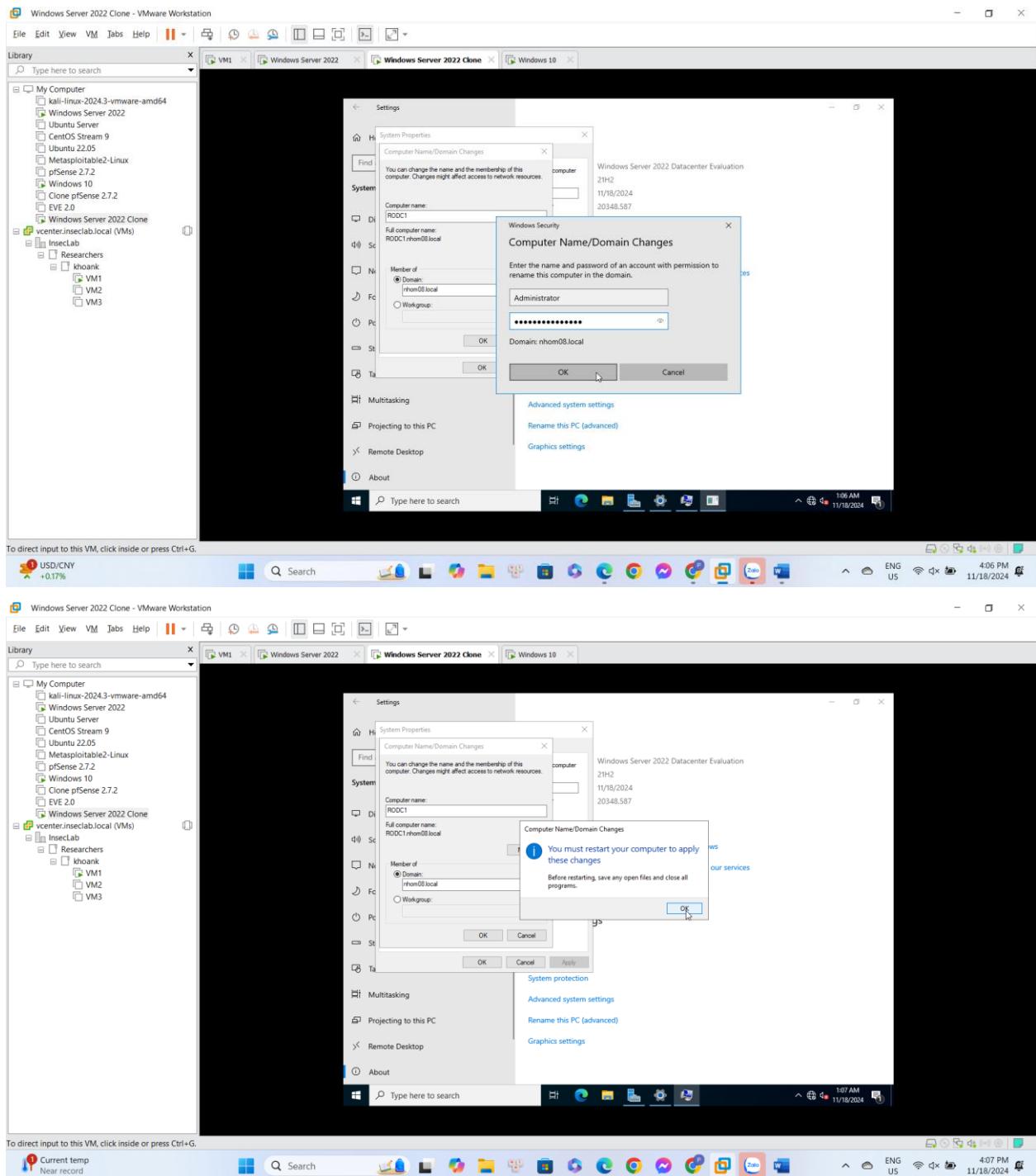


Lab 4: Setting up Active Directory in Windows Server

Nhóm 8

37



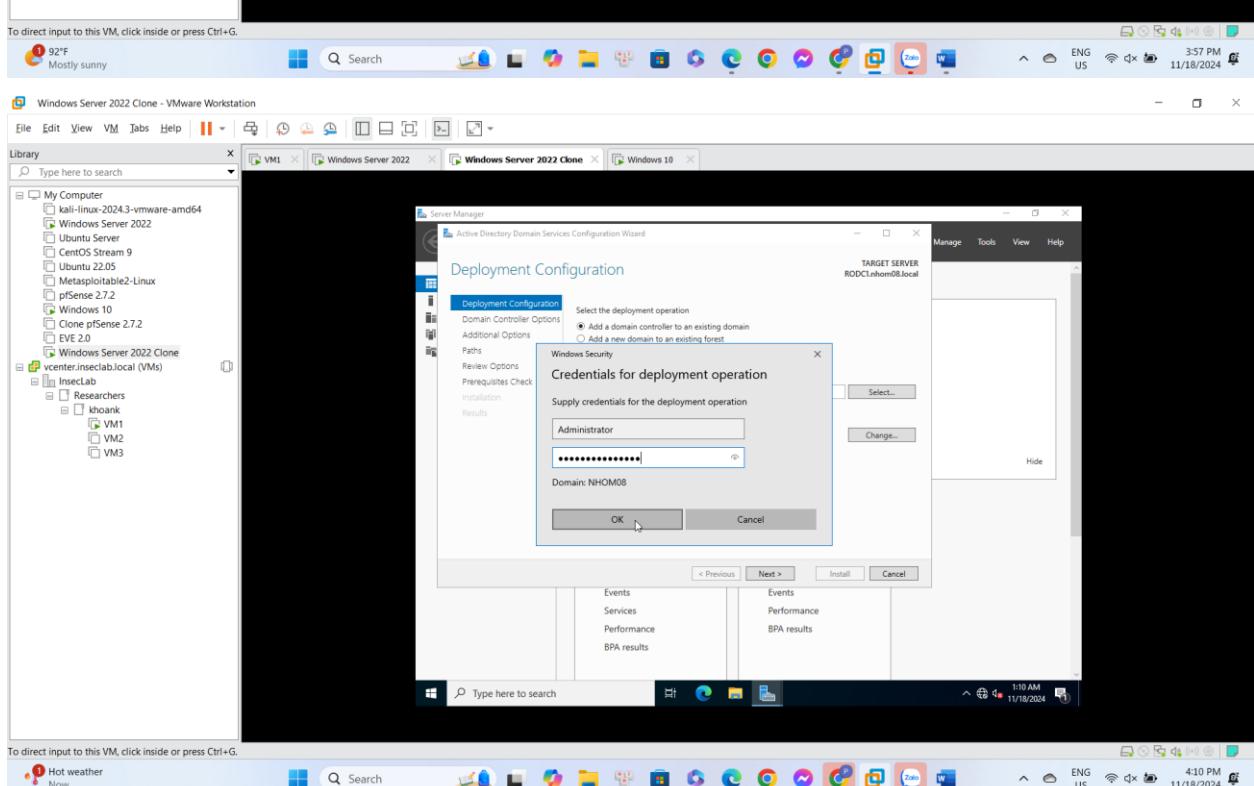
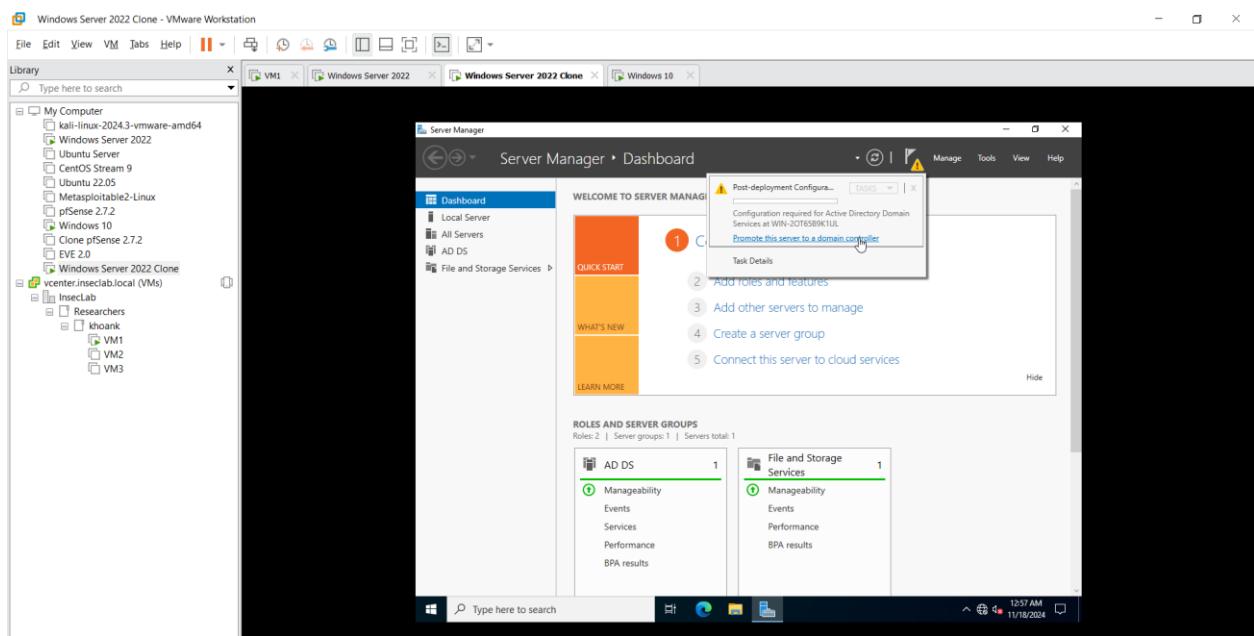


Nâng cấp máy thành Read-Only Domain Controller

Lab 4: Setting up Active Directory in Windows Server

Nhóm 8

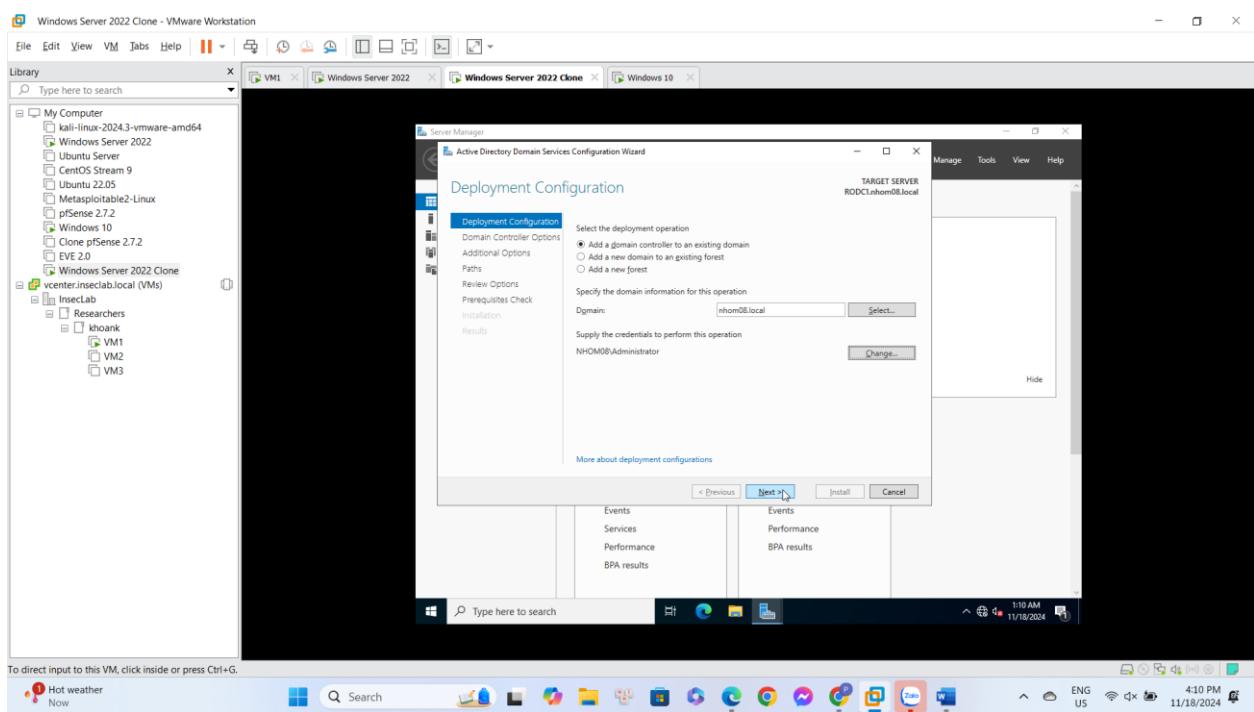
39



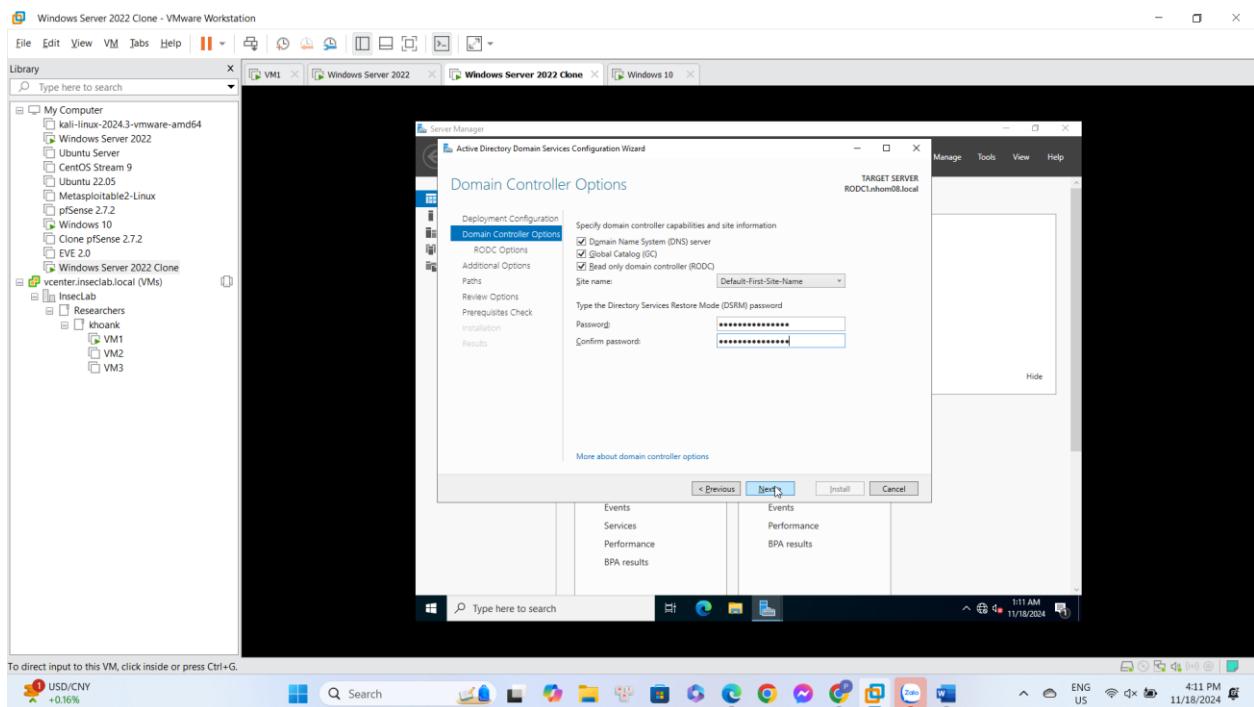
Lab 4: Setting up Active Directory in Windows Server

Nhóm 8

40

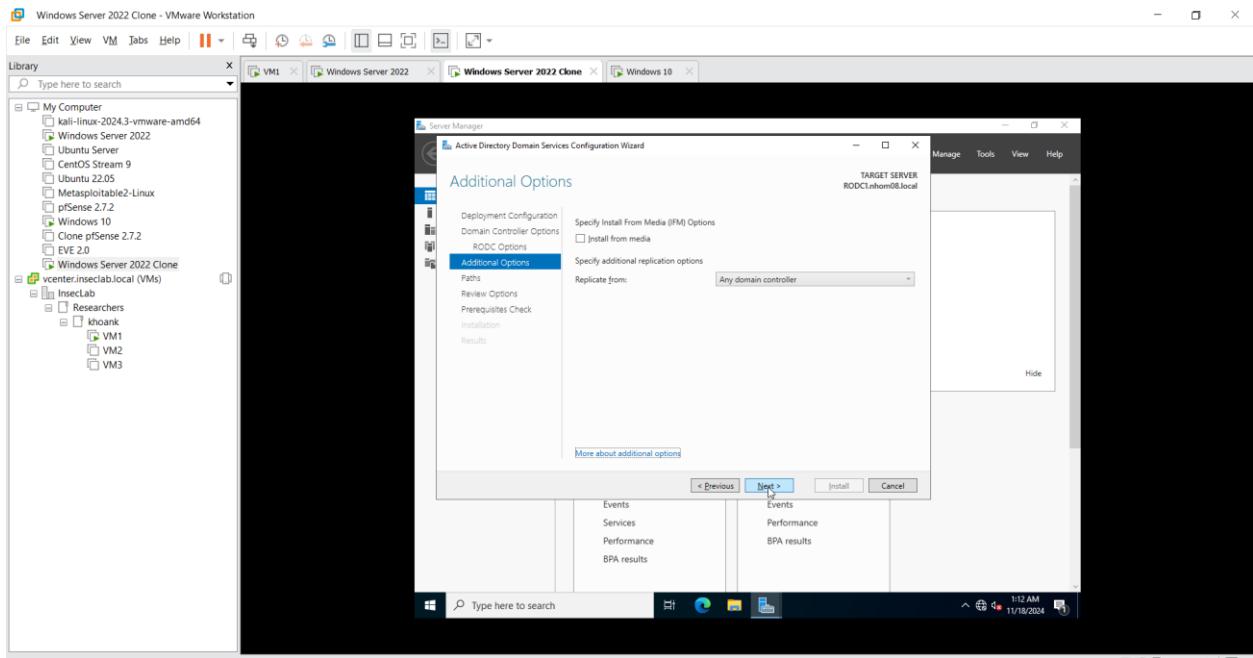
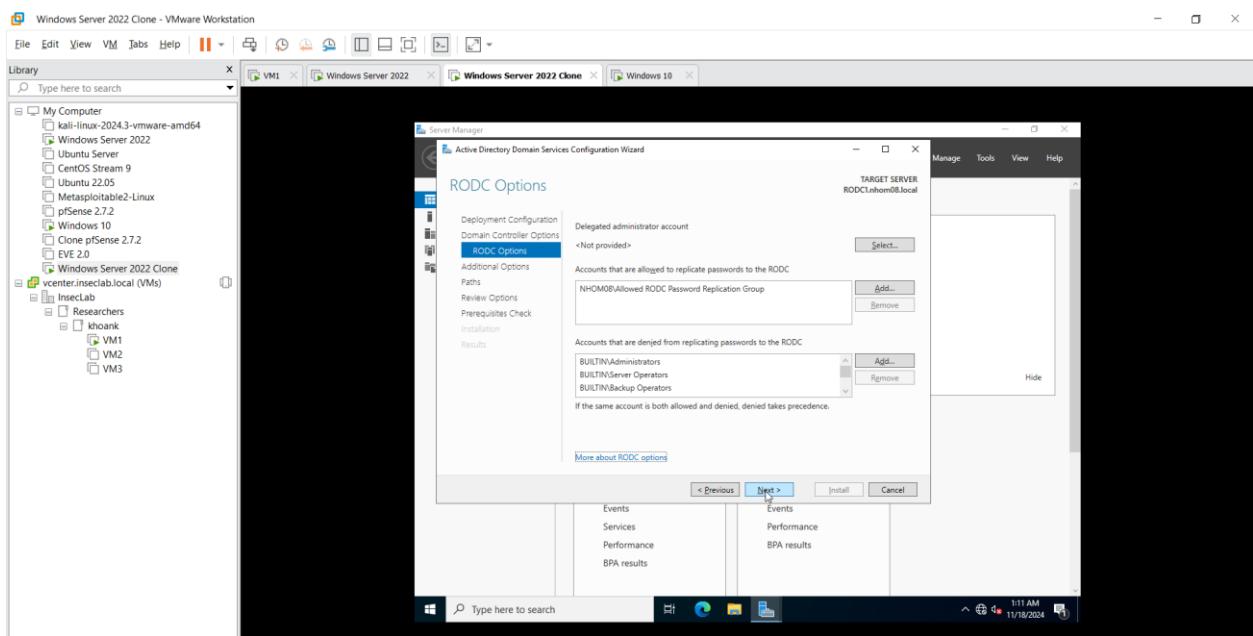


Chọn ô Read only domain controller (RODC)



Lab 4: Setting up Active Directory in Windows Server

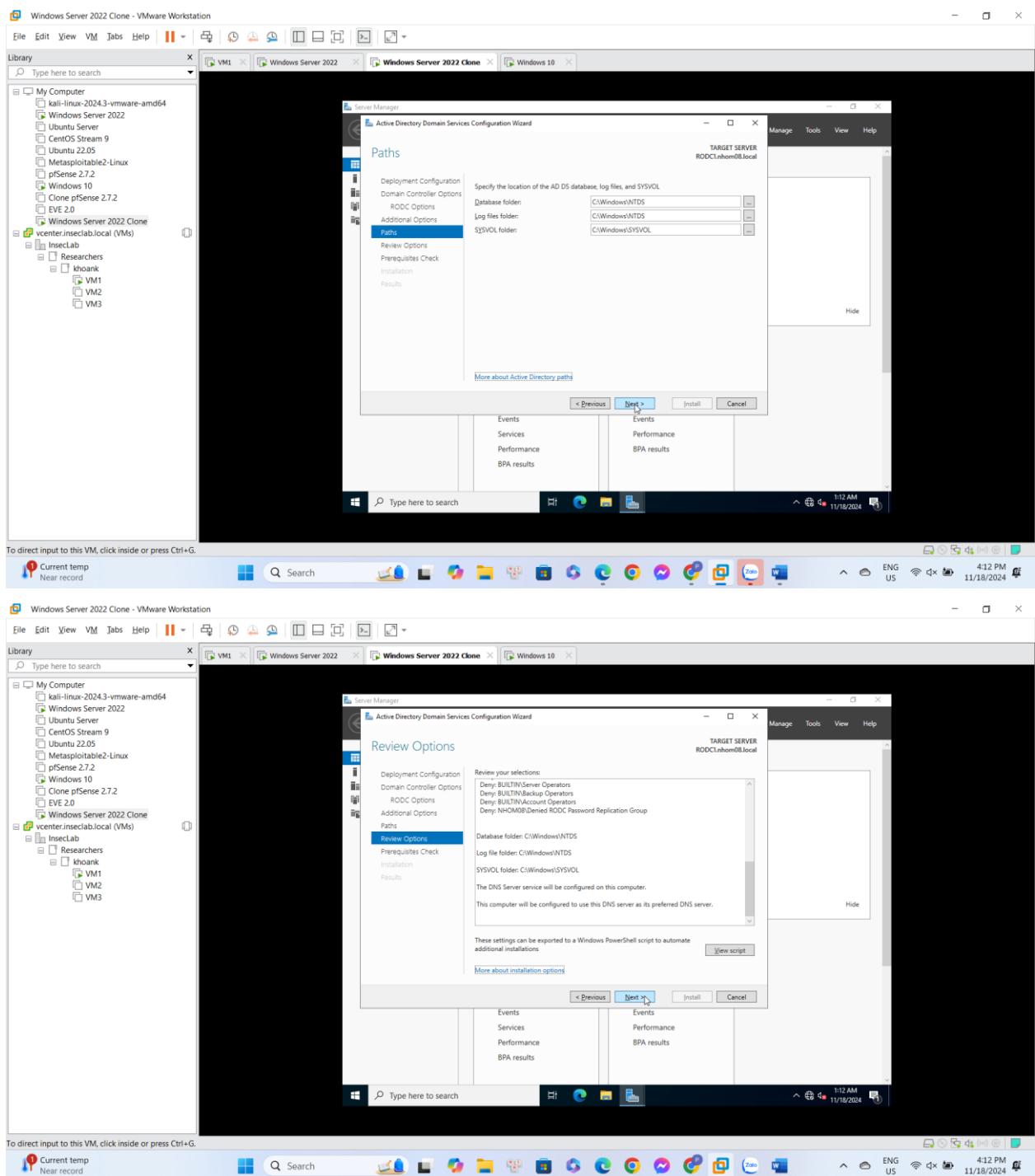
Nhóm 8 — 41



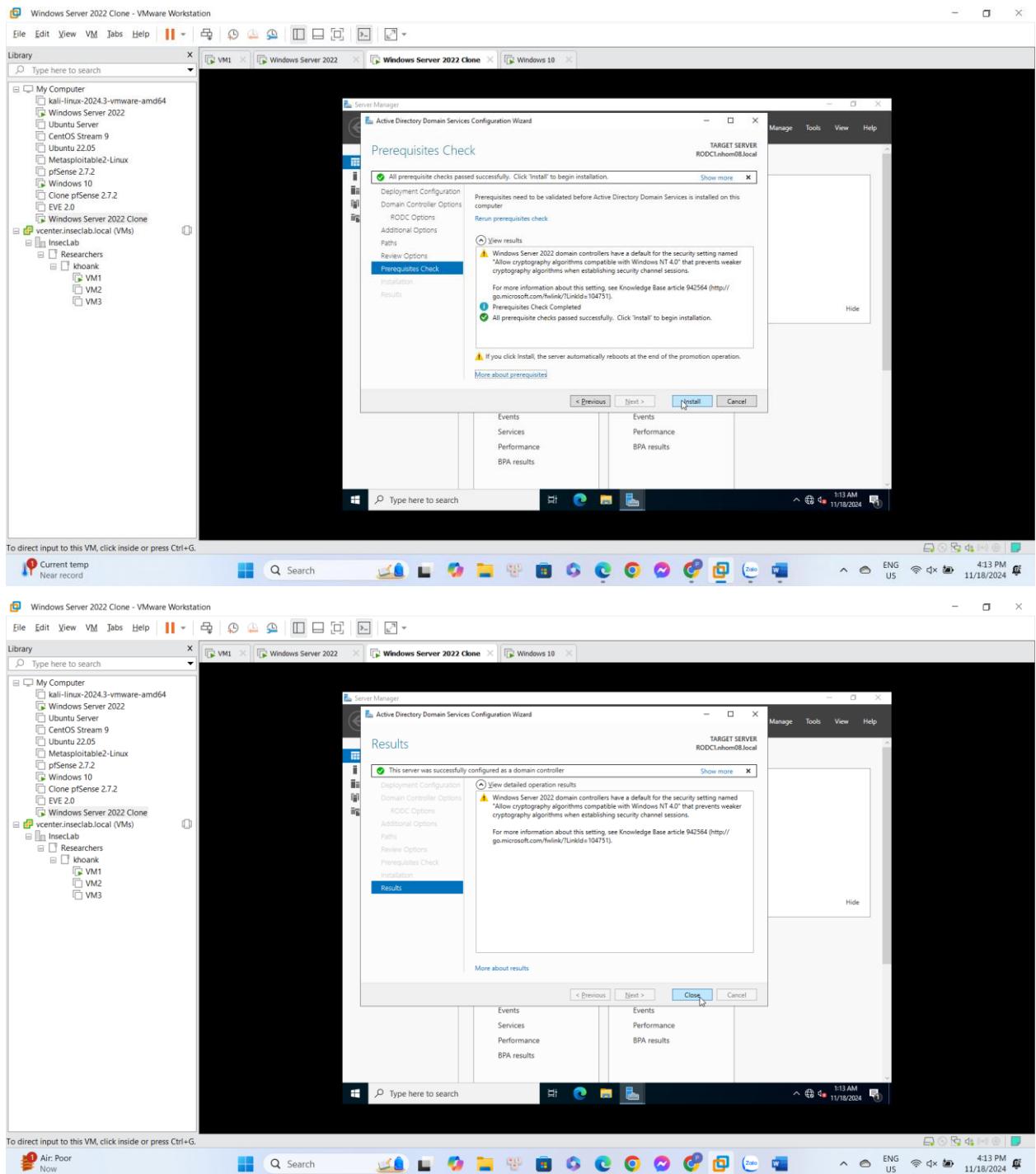
Lab 4: Setting up Active Directory in Windows Server

Nhóm 8

42

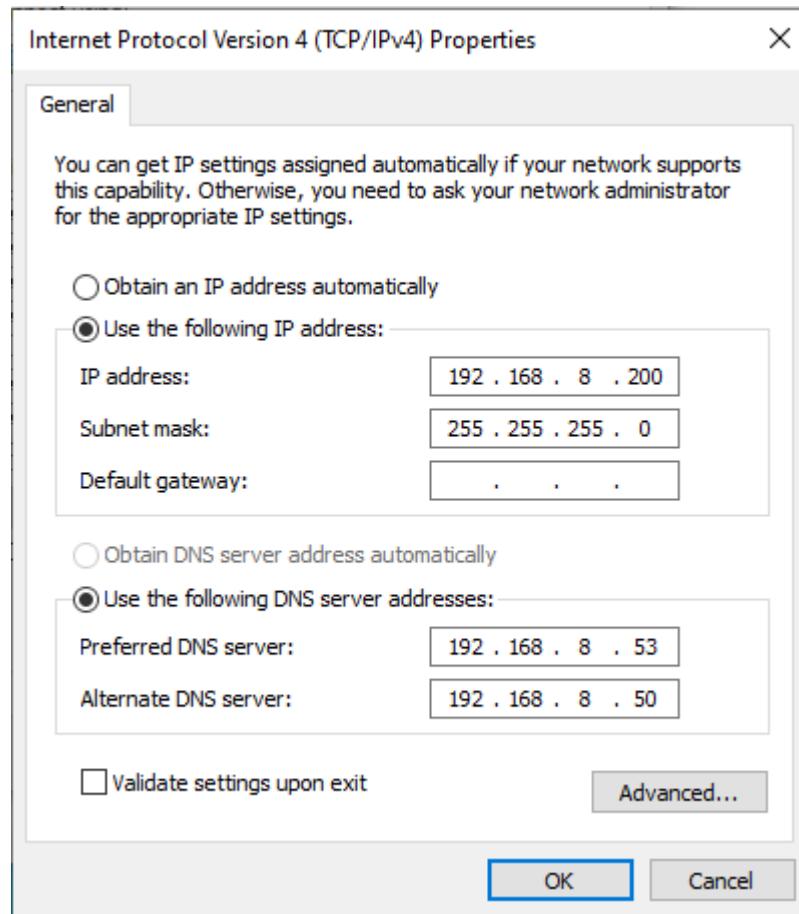


Lab 4: Setting up Active Directory in Windows Server

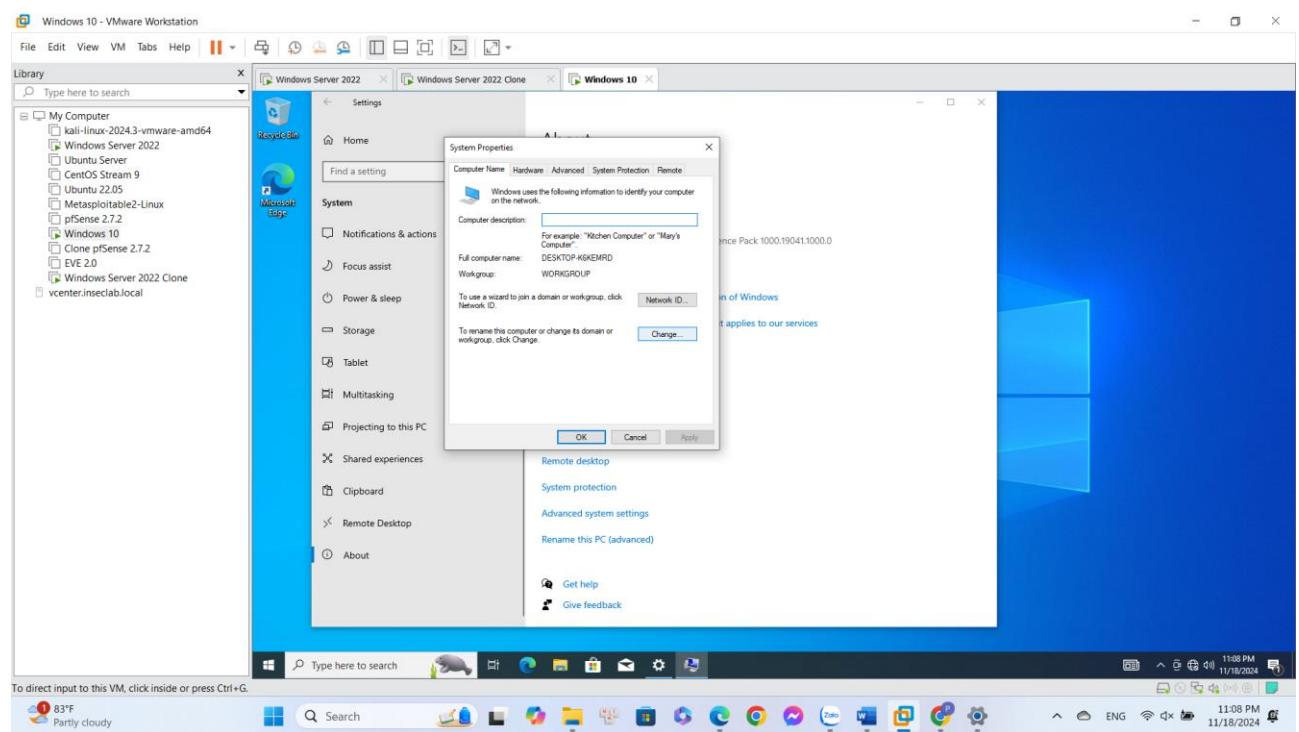


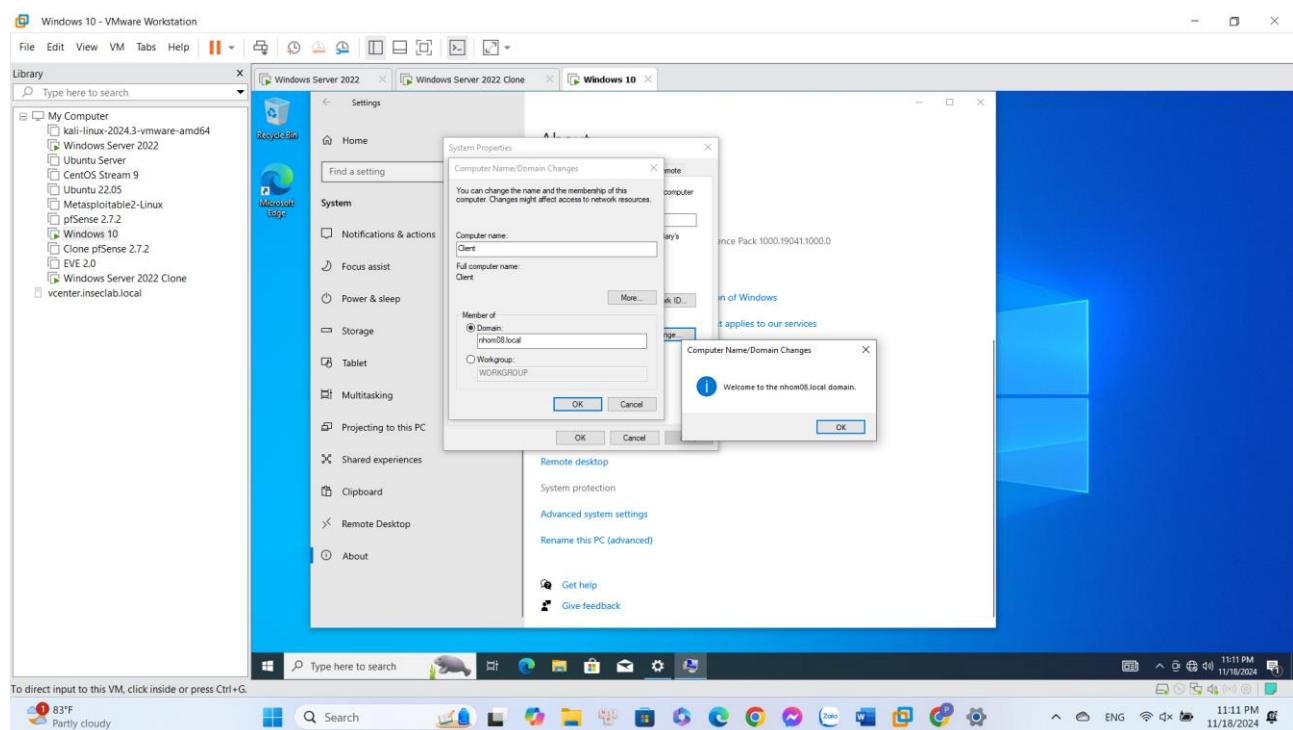
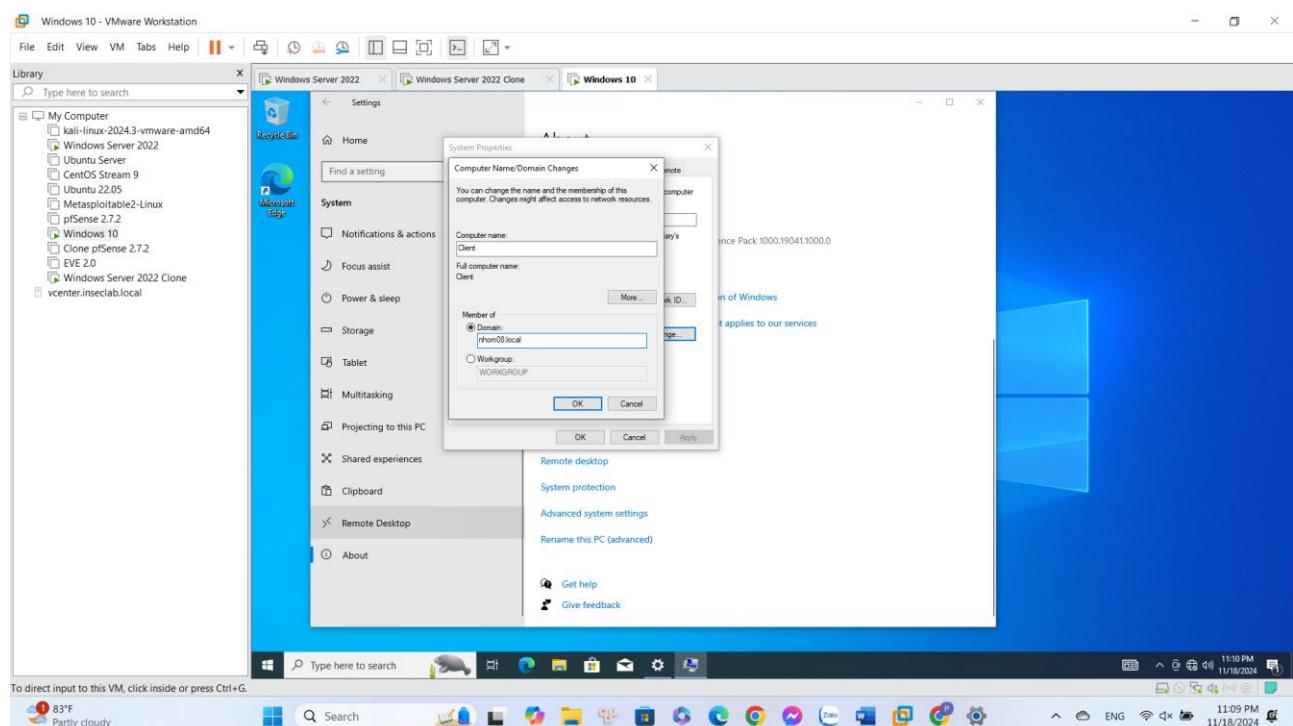
#Client

Cài đặt địa chỉ IP như đề bài yêu cầu

Lab 4: Setting up Active Directory in Windows Server

Tham gia domain (join domain) đã được tạo bởi Primary DC tương tự như trên RODC





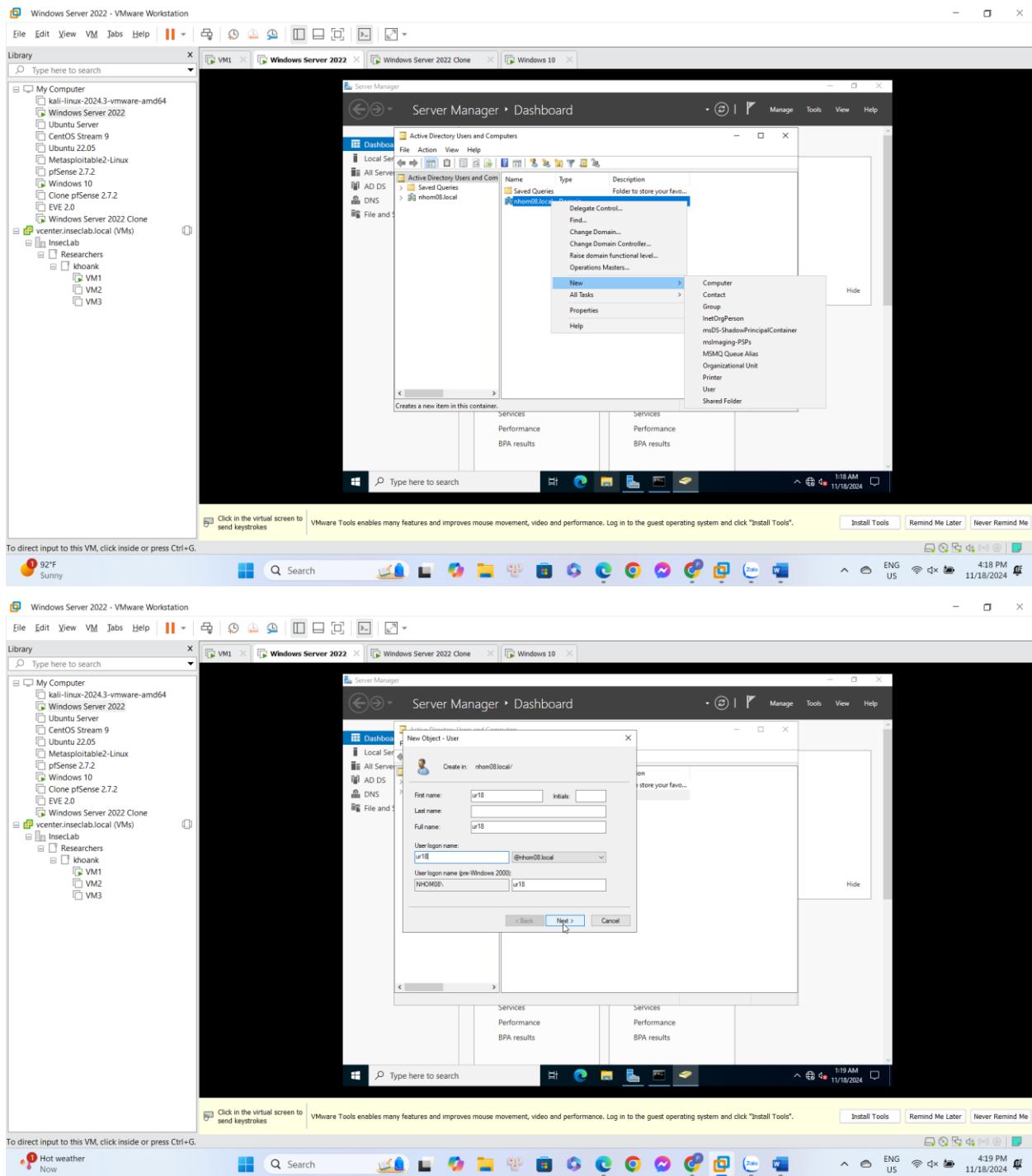
Thực hiện các công việc sau và kiểm tra kết quả (X là số thứ tự nhóm: 8)

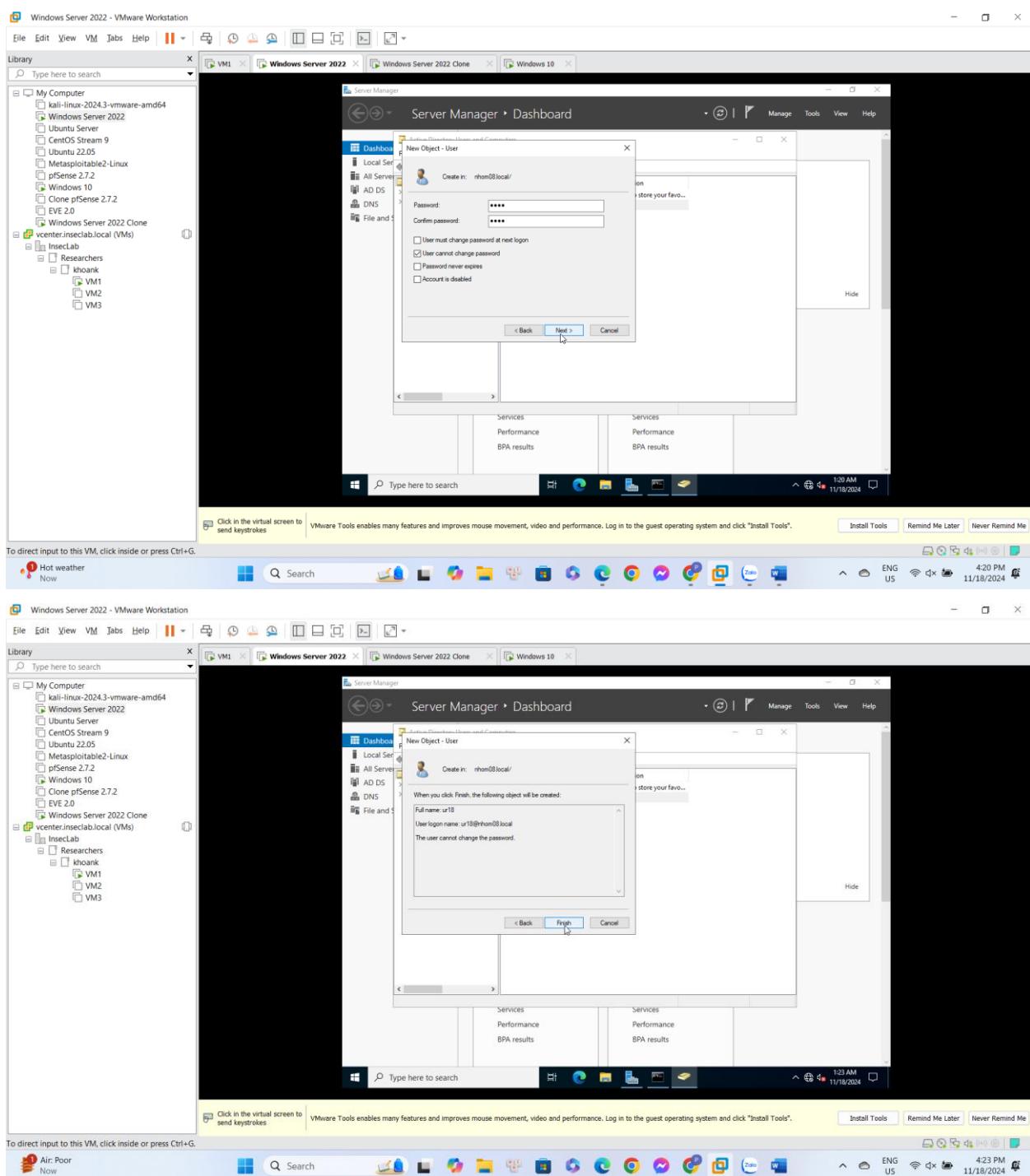
- Tạo user ur1X (ur18) trên Primary DC. Kiểm tra thông tin user này trên Read-Only DC.

Tạo user ur18 trên PDC

Lab 4: Setting up Active Directory in Windows Server

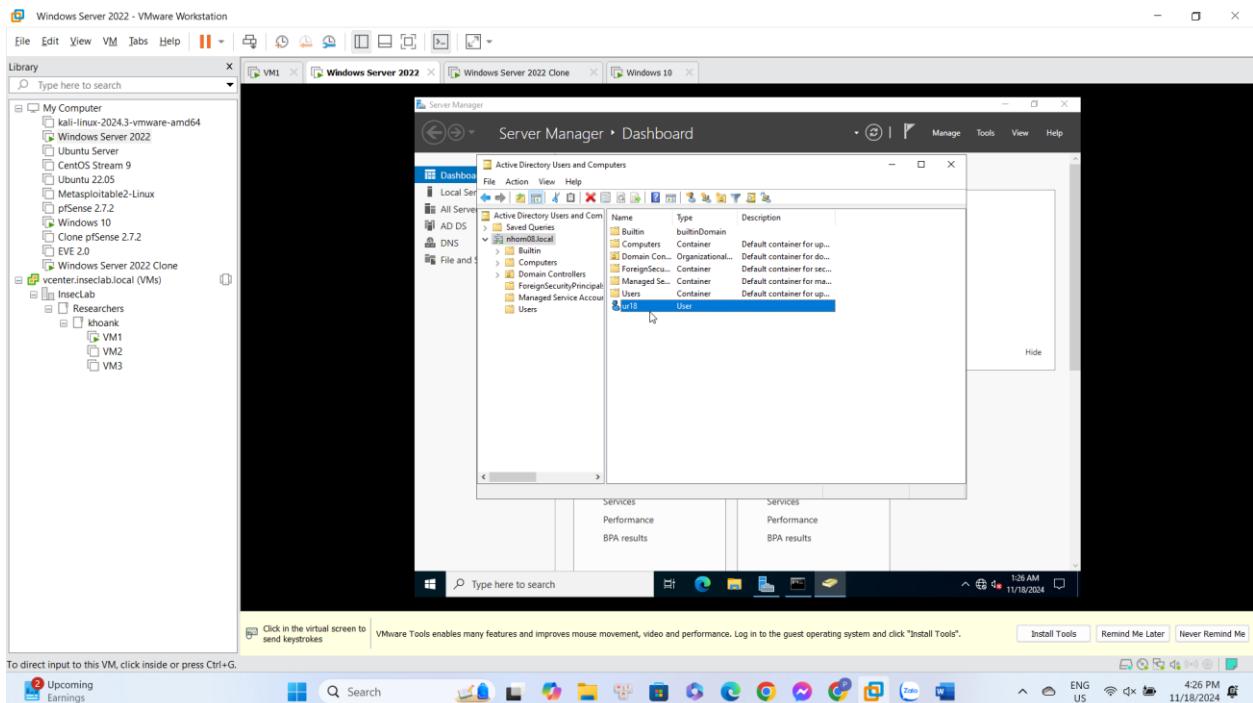
Nhóm 8 — 46



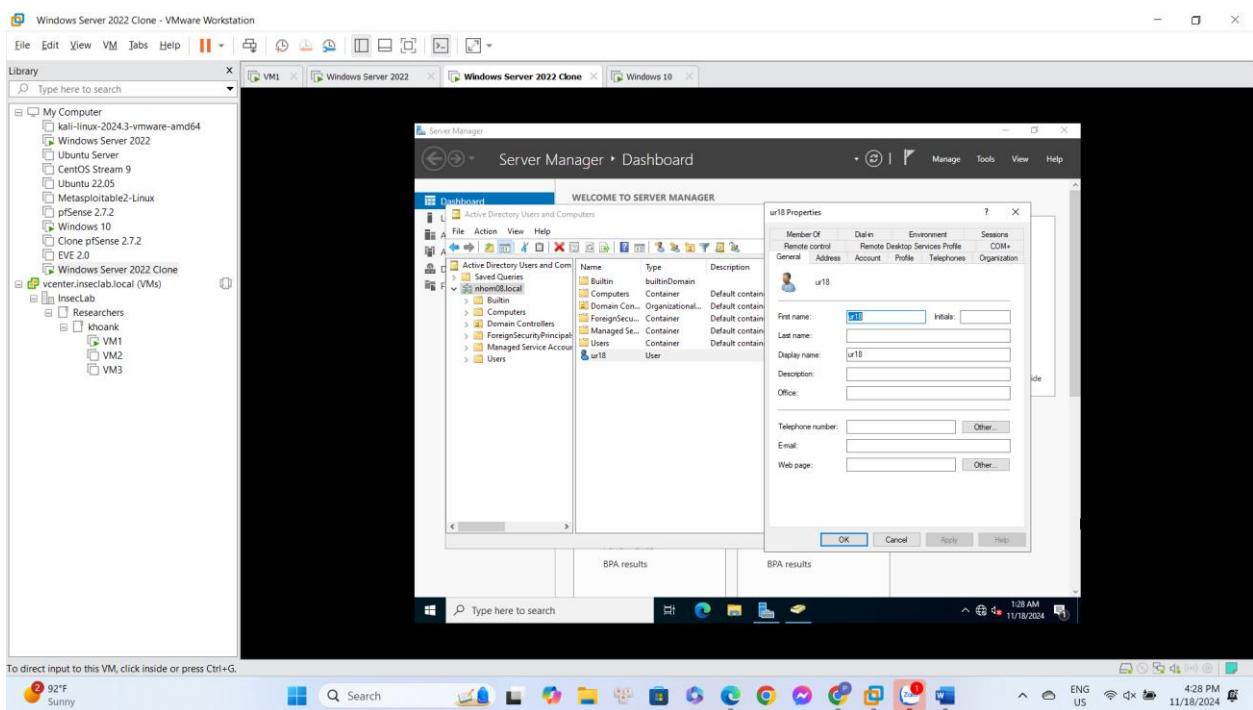


Kiểm tra lại user trên PDC

Lab 4: Setting up Active Directory in Windows Server

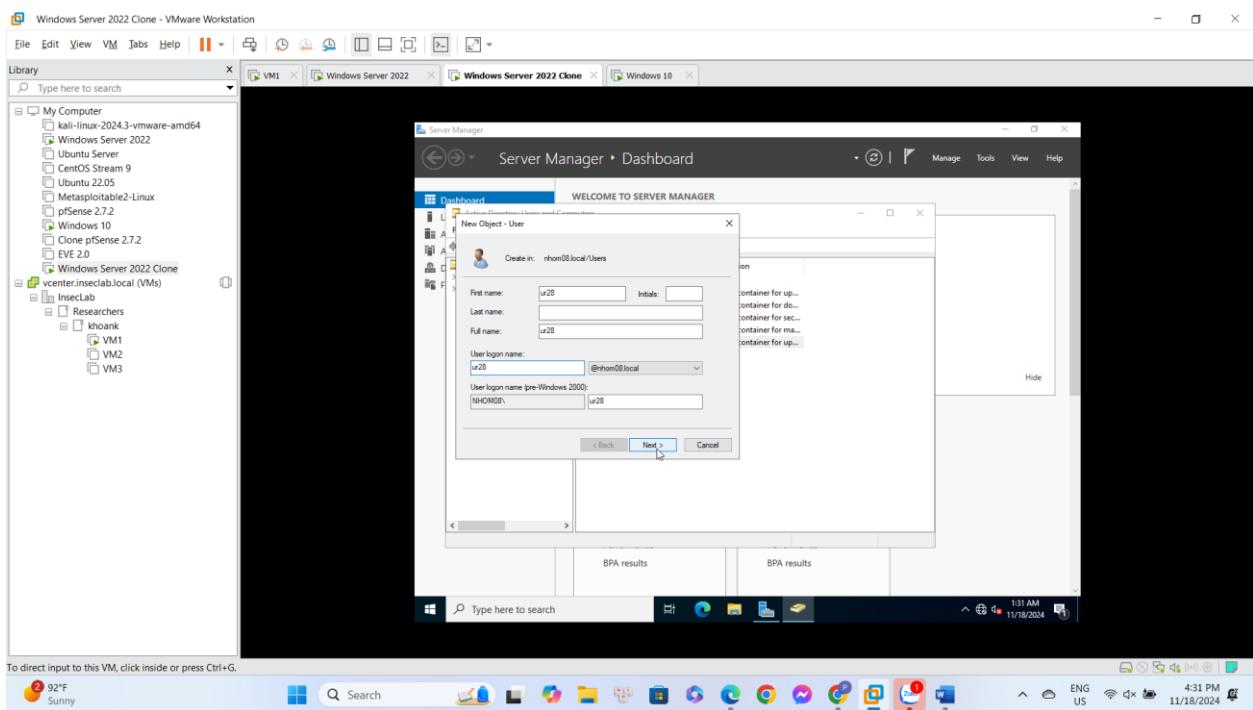


Kiểm tra user trên Read-Only DC

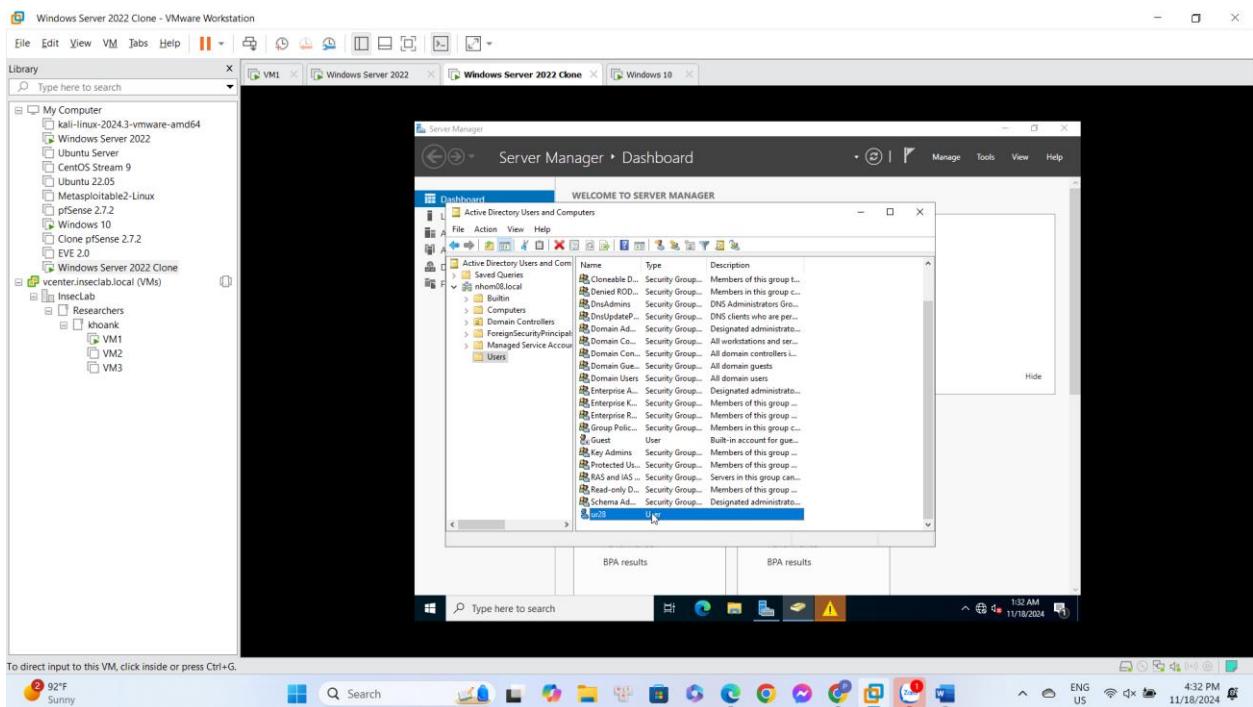


- Tạo user ur2X (ur28) trên Read-Only DC. Kiểm tra thông tin user này trên Primary DC.

Tạo user ur28 trên Read-Only DC

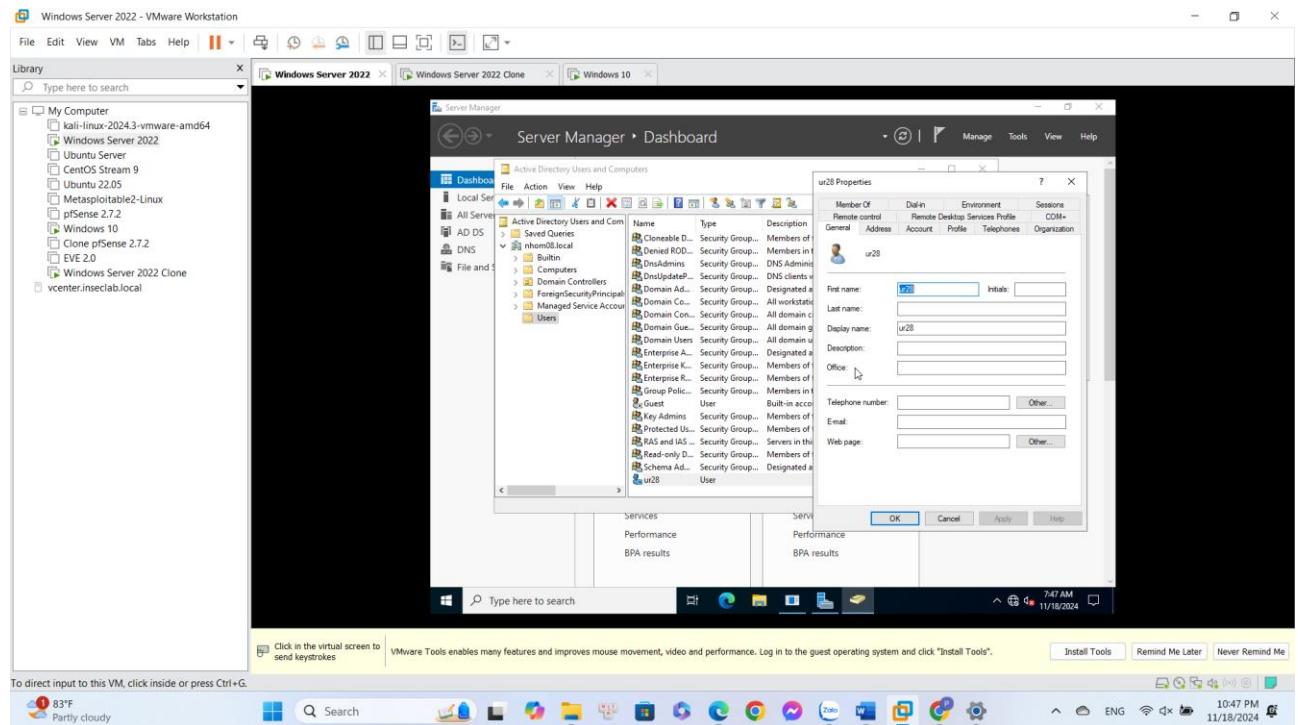


Kiểm tra lại user trên Read-Only DC



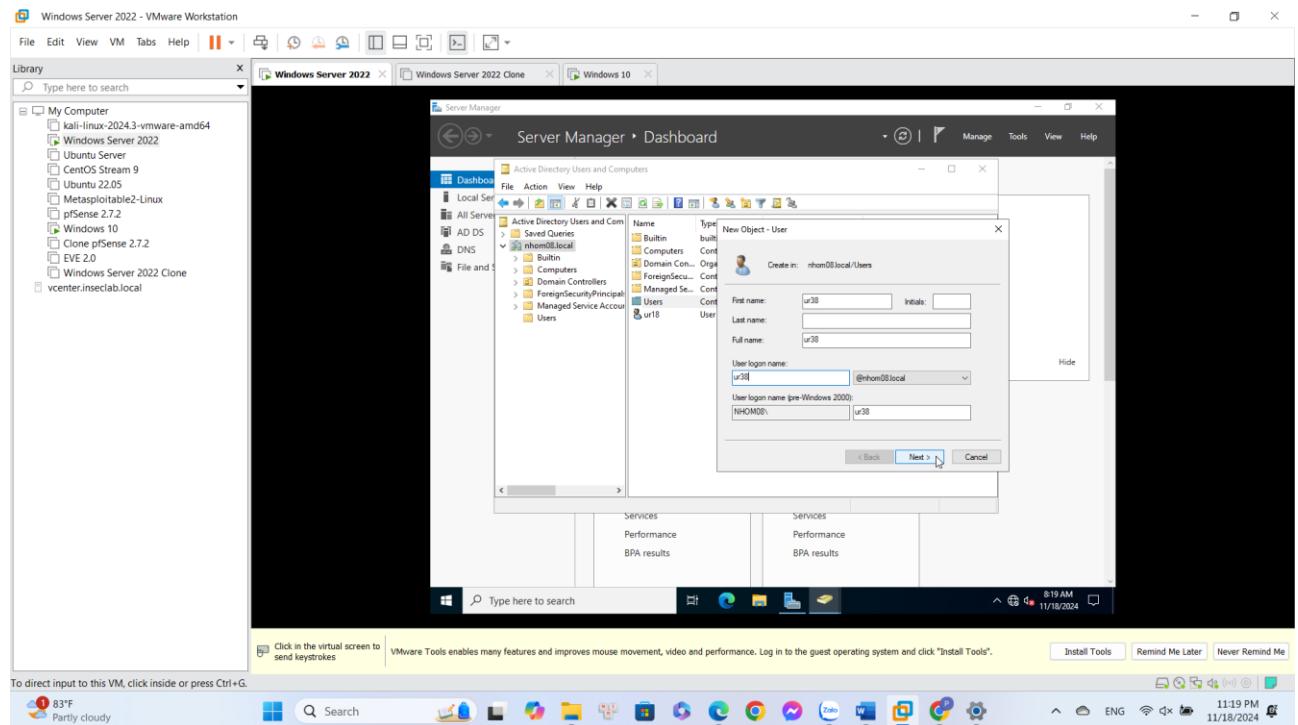
Kiểm tra user ur28 trên Primary DC

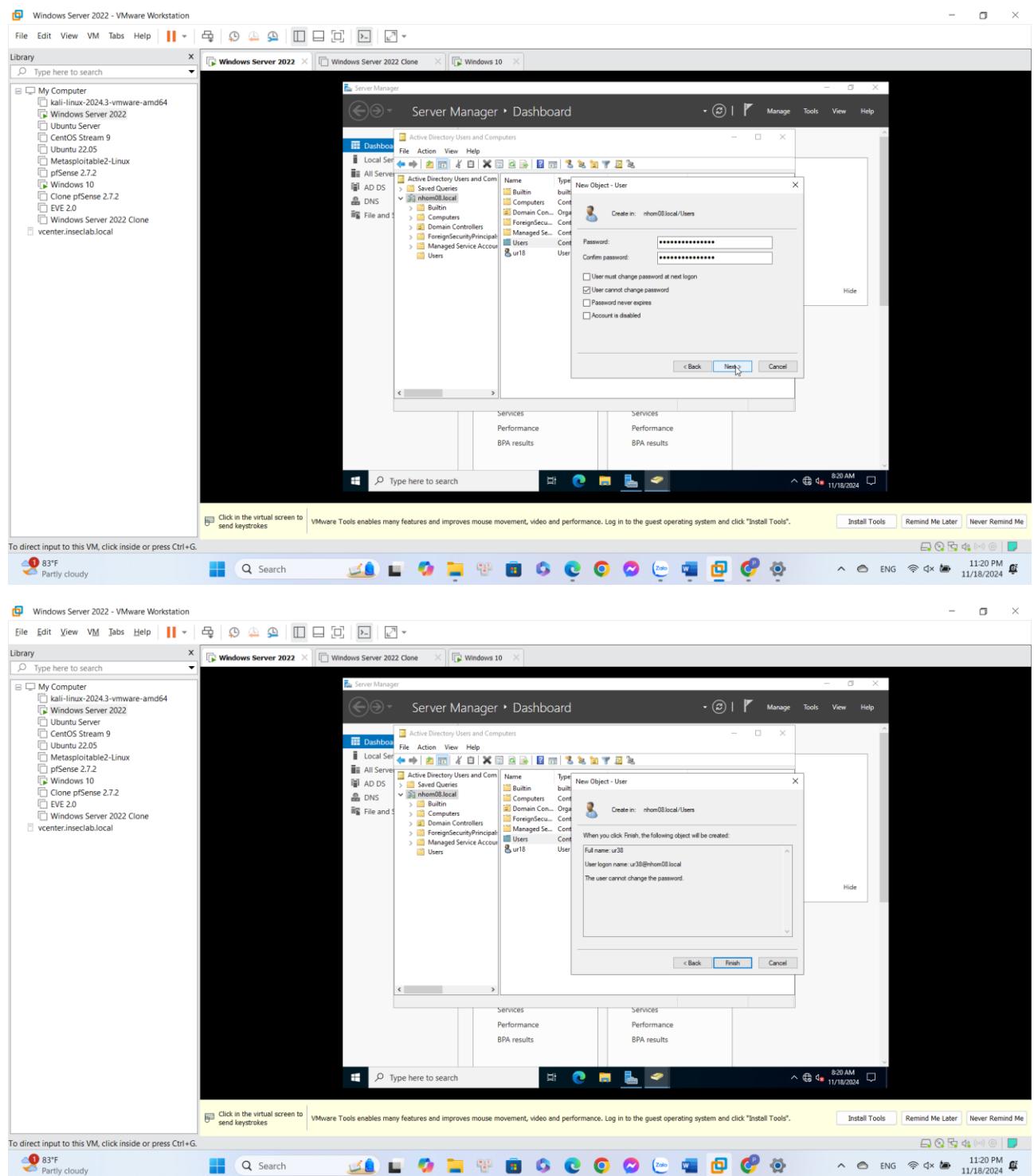
Lab 4: Setting up Active Directory in Windows Server



- Tắt máy Read-Only DC, thêm user ur3X (ur38) trên Primary DC. Sau đó mở lại Read-Only DC và kiểm tra thông tin user này trên Read-Only DC.

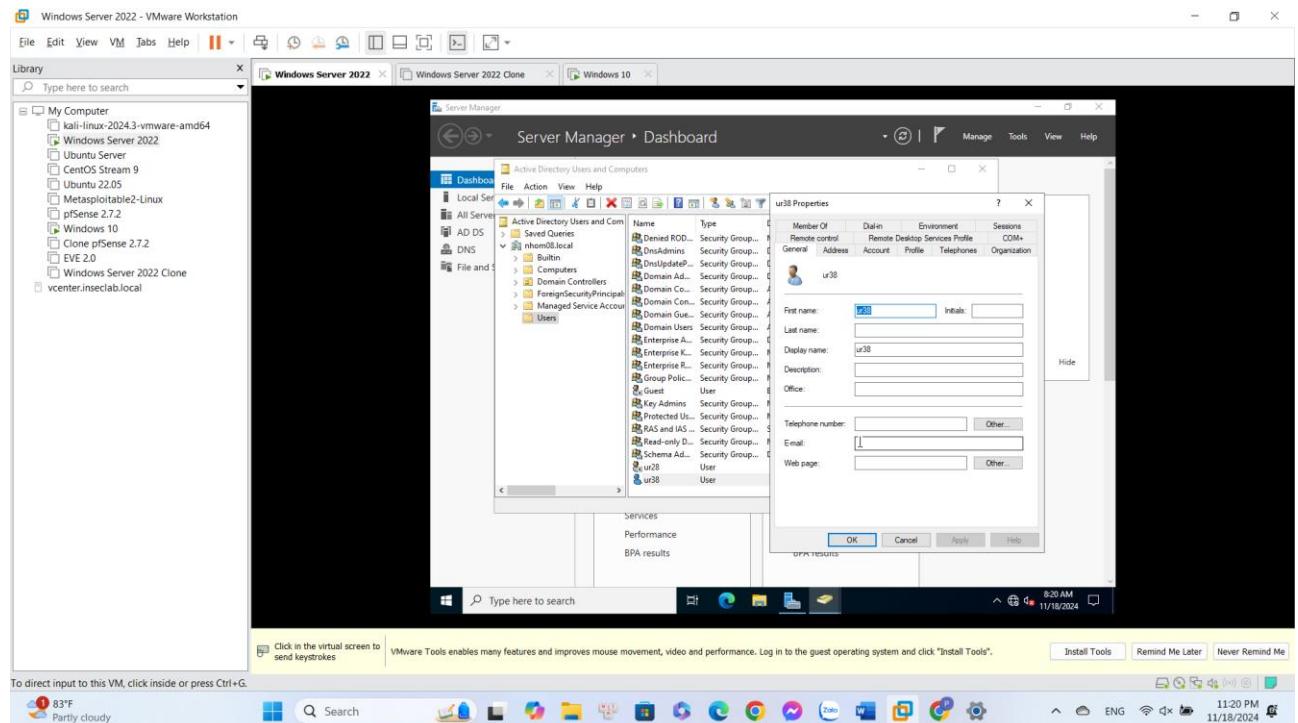
Thêm ur38 trên Primary DC khi đã tắt máy Read-Only DC



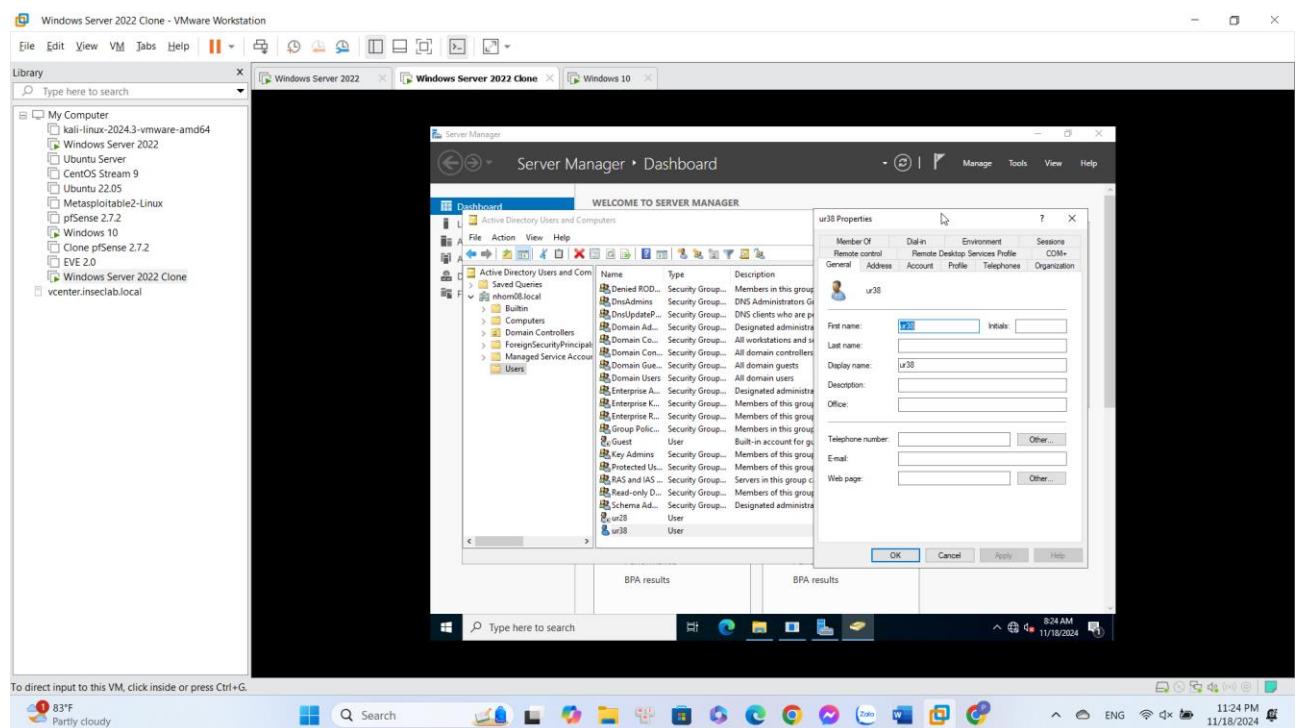


Kiểm tra lại trên Primary DC

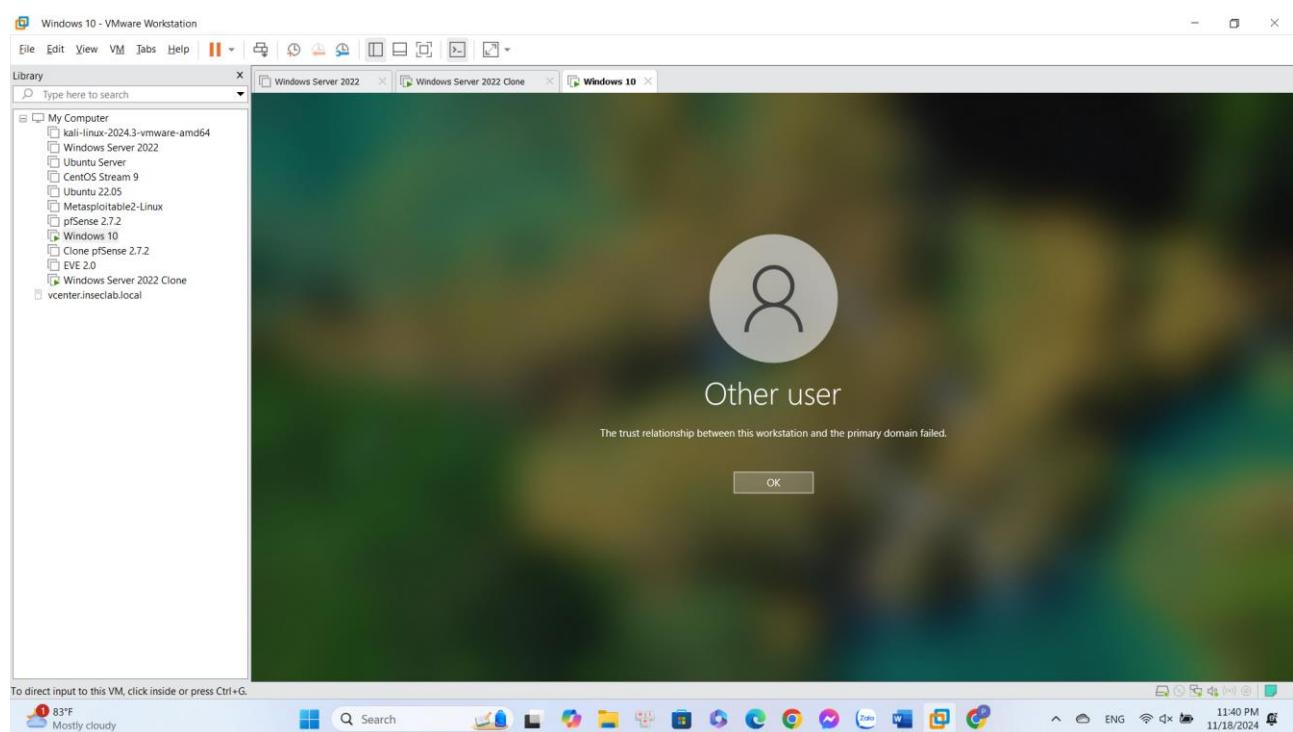
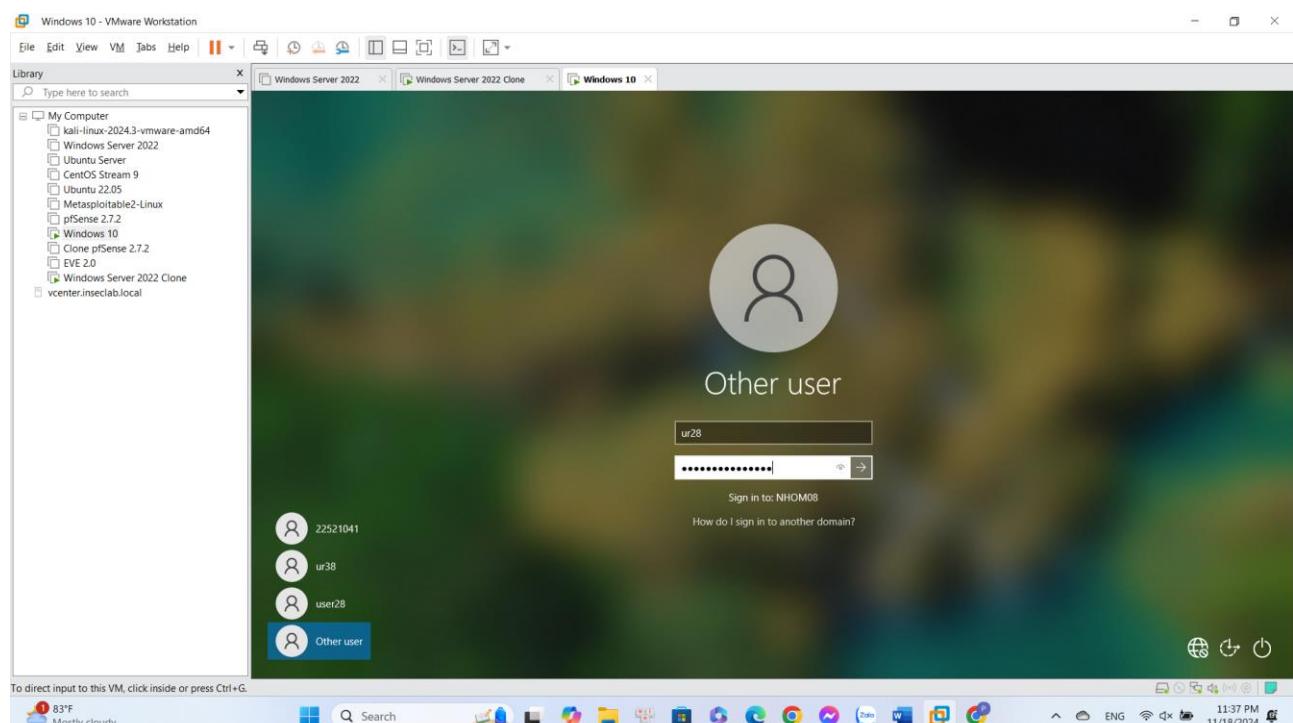
Lab 4: Setting up Active Directory in Windows Server



Mở lại RODC và kiểm tra thông tin ur38

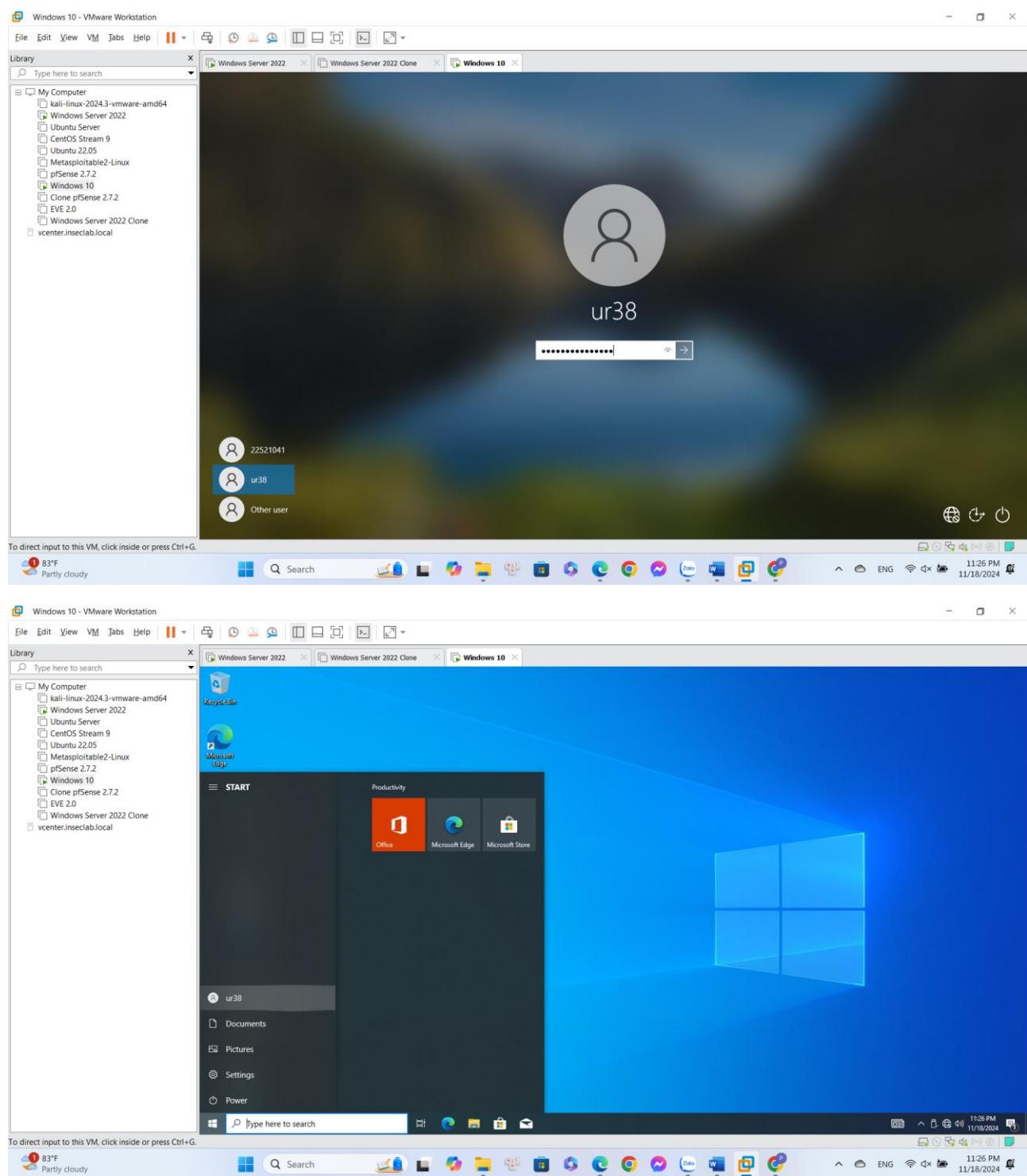


- Tắt máy Primary DC, login ur2X (ur28) trên máy Client. Giải thích kết quả.



Giải thích kết quả: Không login ur28 trên máy được vì máy RODC chỉ đóng vai trò là 1 Server, 1 bản sao đơn hướng của PDC nên khi tắt máy PDC thì không có Domain Controller nào hoạt động để xử lý việc chứng thực user và password của máy Client. không thể login ur28 trên máy Client.

- Tắt máy Read-Only DC, login ur3X (ur38) trên máy Client. Giải thích kết quả.



Giải thích kết quả: Login thành công trên máy. Vì quan trọng của Domain là máy PDC, RODC chỉ đóng vai trò là 1 bản sao của PDC do đó khi tắt máy RODC không làm ảnh hưởng đến việc login ur38 trên máy Client, PDC là Domain Controller vẫn hoạt động để xử lý việc chứng thực user và password của máy Client.