

Lab 4 - Triển khai Active Directory trên Windows Server

NT132.P11.ANTN

GVHD: Đỗ Hoàng Hiển

STT	Tên thành viên	MSSV
1	Vũ Ngọc Quốc Khánh	22520661
2	Nguyễn Đức Luân	22520825

1. Xây dựng mô hình Workgroup

Yêu cầu 1.1

Đề bài

Tìm hiểu và trả lời câu hỏi sau:

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

Trả lời

1. Workgroup trong Windows là một mô hình mạng ngang hàng (peer-to-peer) giúp các máy tính trong cùng một mạng nội bộ (LAN) có thể kết nối và chia sẻ tài nguyên như tệp tin, máy in, và thiết bị khác một cách dễ dàng mà không cần phải thiết lập một server trung tâm.

2.

- Ưu điểm**
 - Dễ cài đặt và sử dụng
 - Không cần máy chủ

- Nhược điểm**

Khó mở rộng

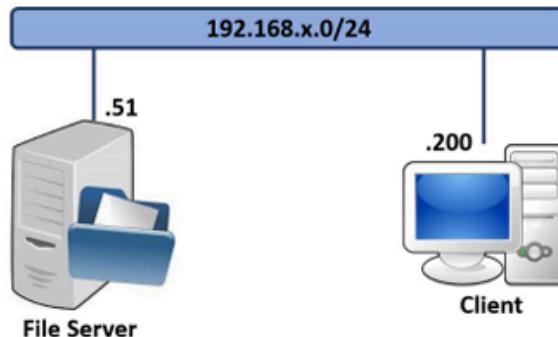
Có thể thiếu đồng nhất trong việc cấu hình các máy

Yêu cầu 1.2

Đề bài

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 2019	192.168.X.51/24
Client	Windows 7/8/10	192.168.X.200/24

Các bước thực hiện

Cấu hình IP cho máy File Server:

```
Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::10c6:8a66:29c6:2b5d%5
IPv4 Address. . . . . : 192.168.15.51
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.15.2
```

Cấu hình IP cho máy Client:

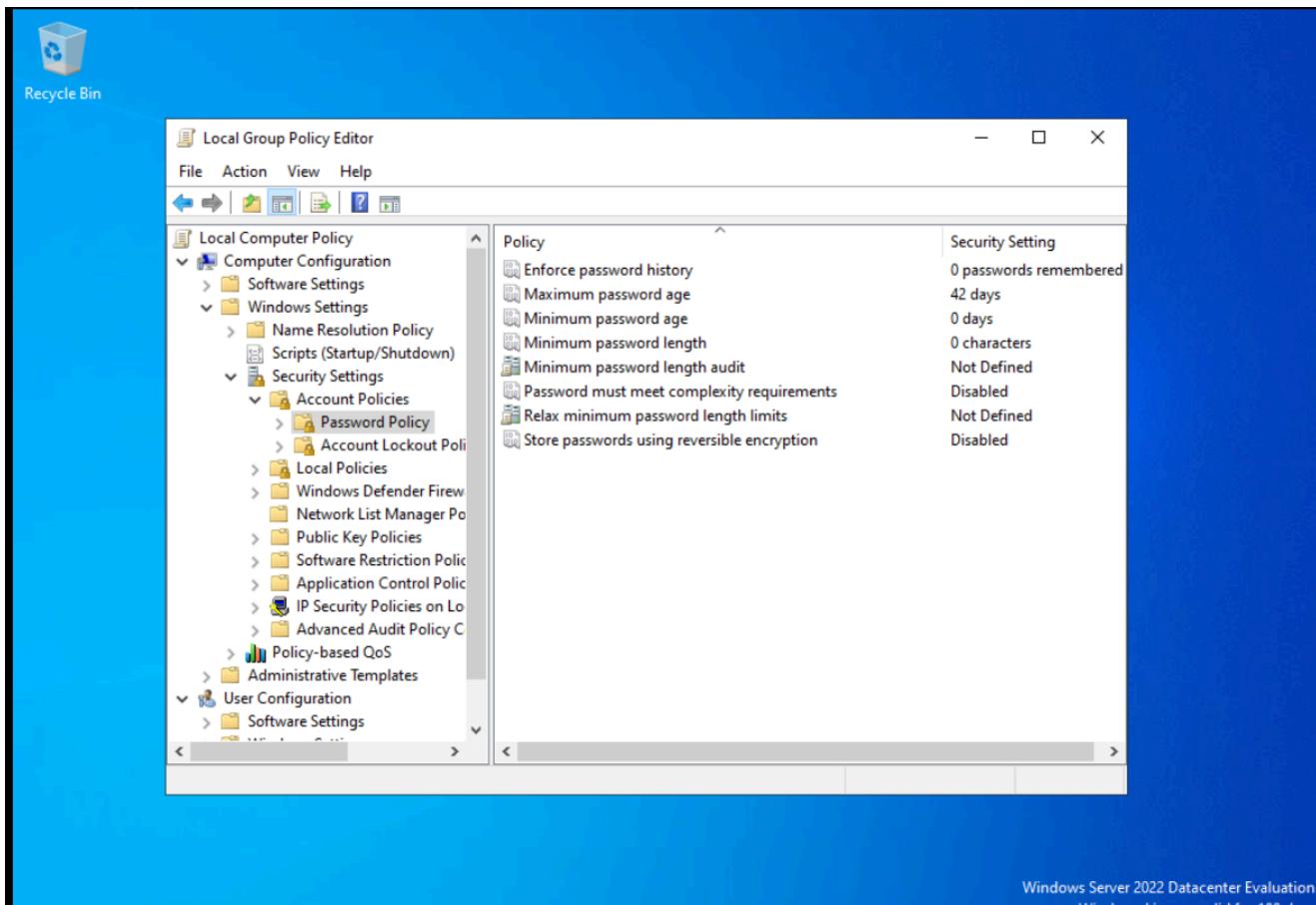
```
Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix  . : localdomain
Link-local IPv6 Address . . . . . : fe80::3ef5:d6bf:df08:2506%5
IPv4 Address. . . . . : 192.168.15.200
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.15.2
```

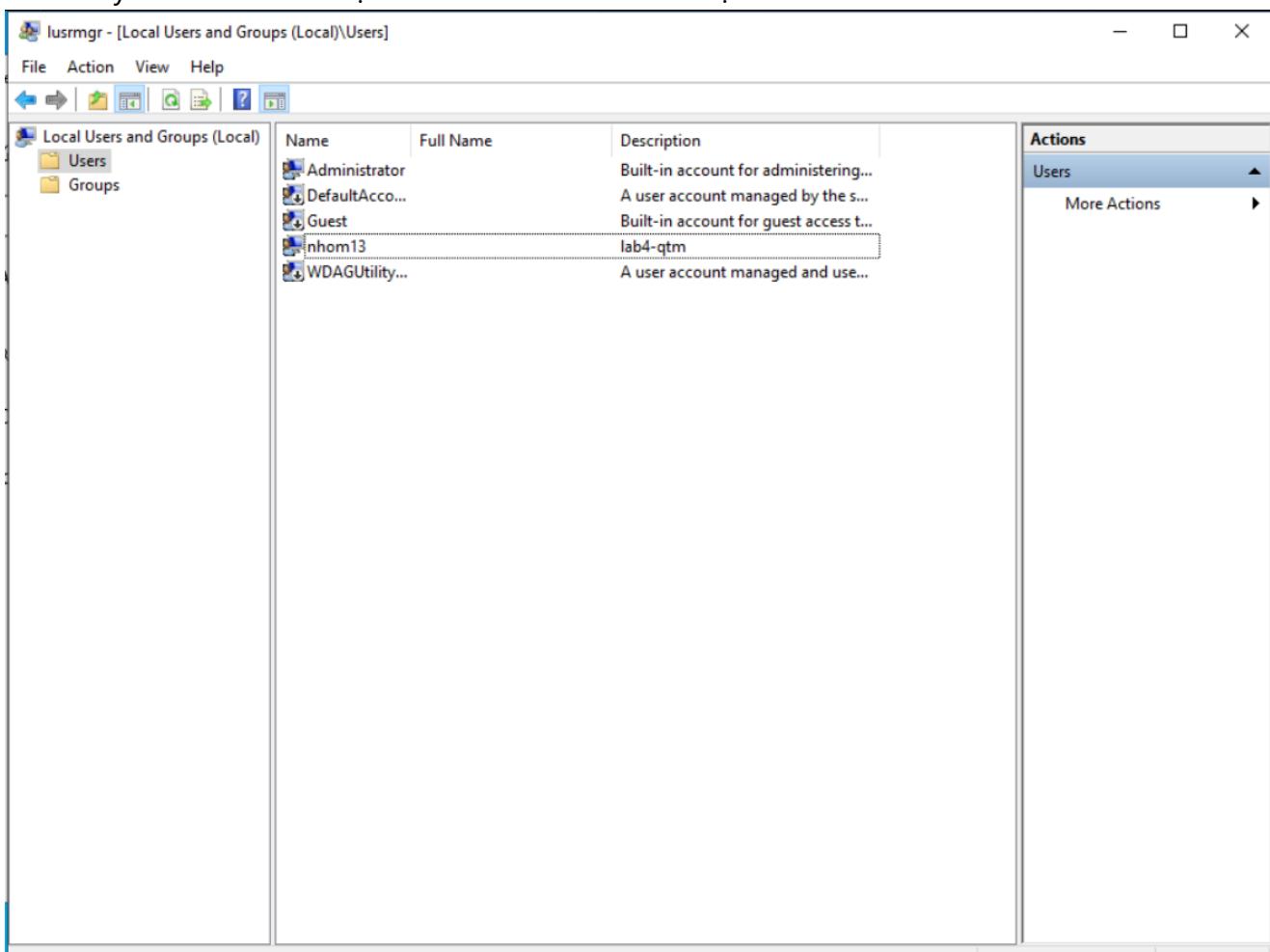
Bước 1:

Cấu hình chính sách mật khẩu trong File server:

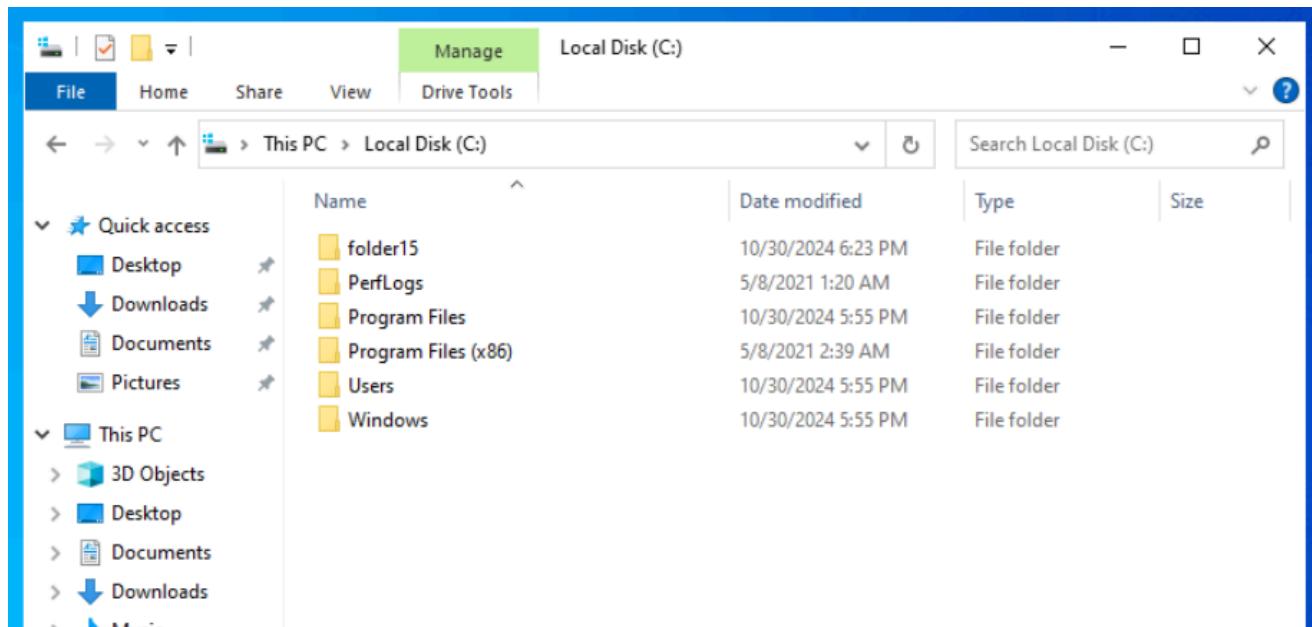


Bước 2:

Trên máy chủ File Server tạo tài khoản nhom13 có mật khẩu là 123:



Bước 3: trên ổ đĩa C:\ của File Server tạo thư mục folder15 để chia sẻ dữ liệu:



Bước 4: Thực hiện phân quyền chia sẻ trên thư mục **folder15** để user **nhom13** có quyền Read/Write.

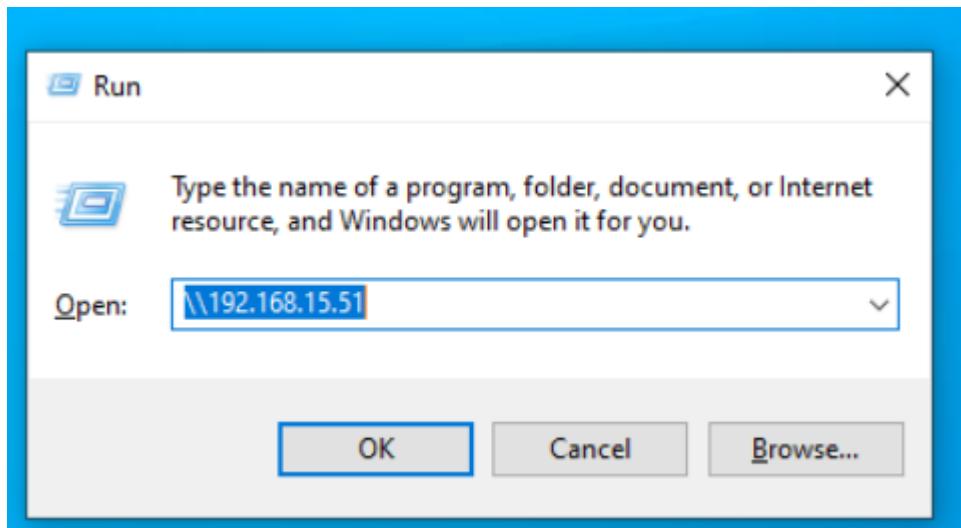
The dialog shows the "Choose people to share with" section. It includes a search bar, an "Add" button, and a table of users and their permission levels.

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
nhom13	Read/Write ▾

[I'm having trouble sharing](#)

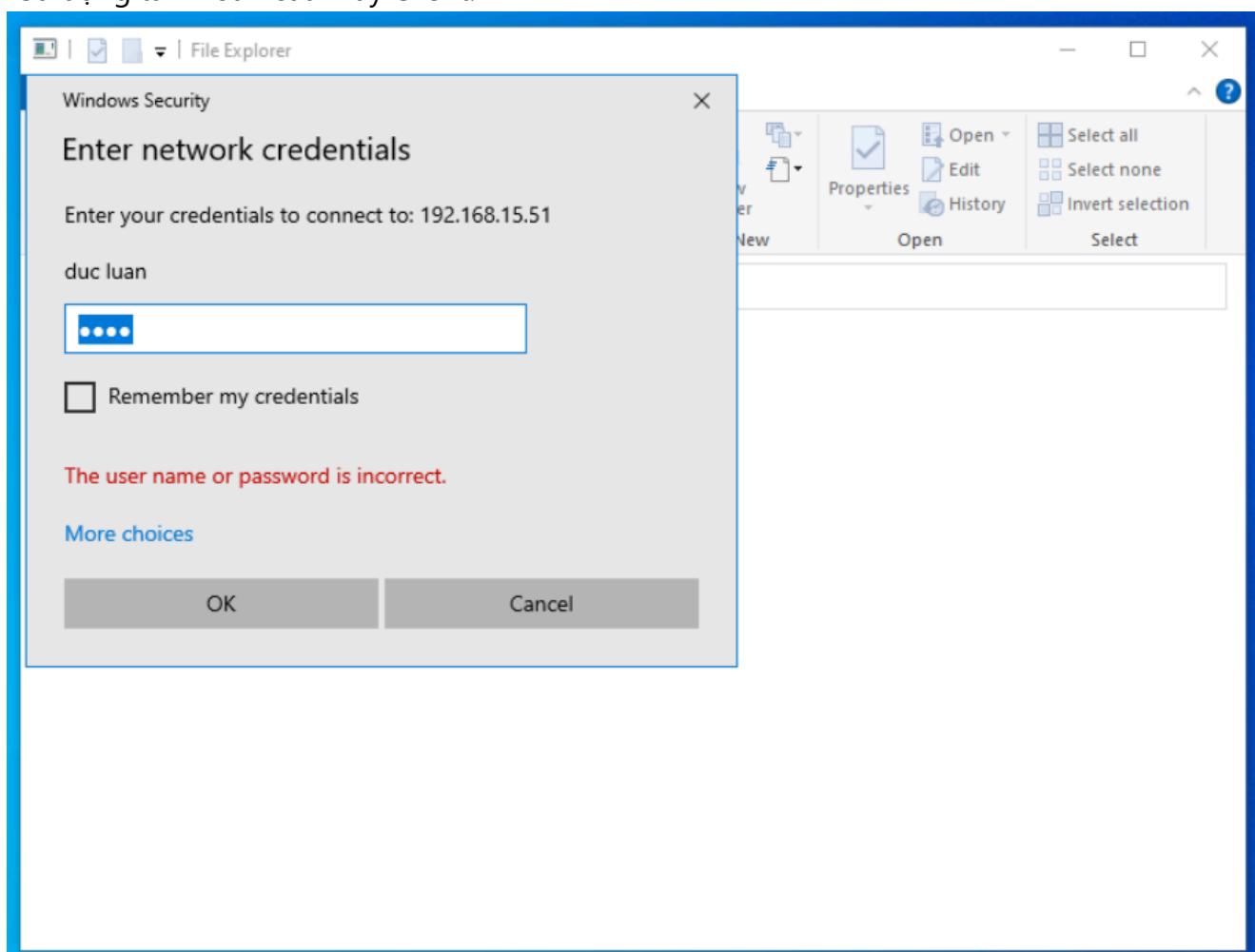
Share Cancel

Bước 5: Thực hiện kết nối tới File Server từ máy Client

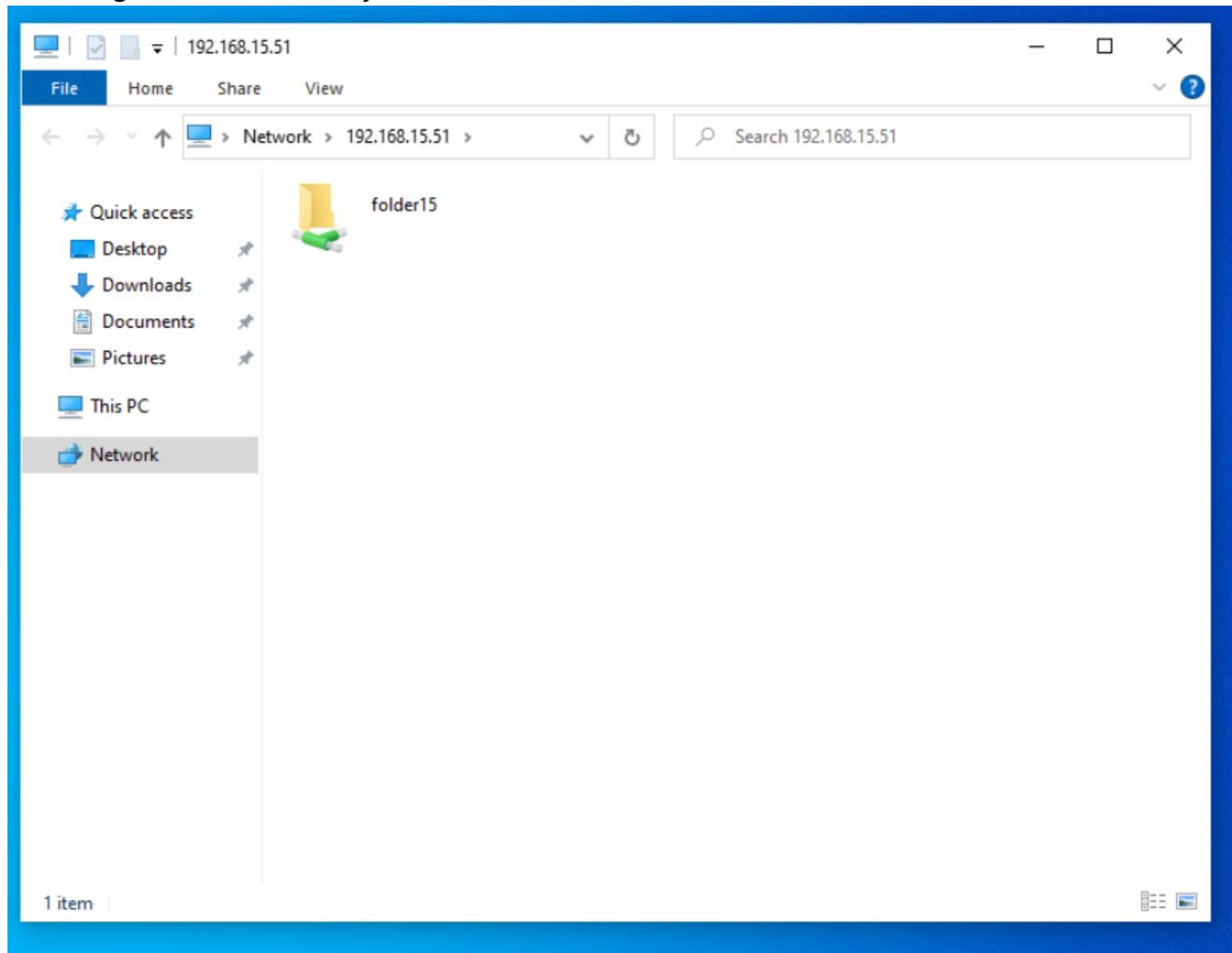


Bước 6: Nhập user xác thực để truy cập vào File Server trong 2 trường hợp:

-Sử dụng tài khoản của máy Client:

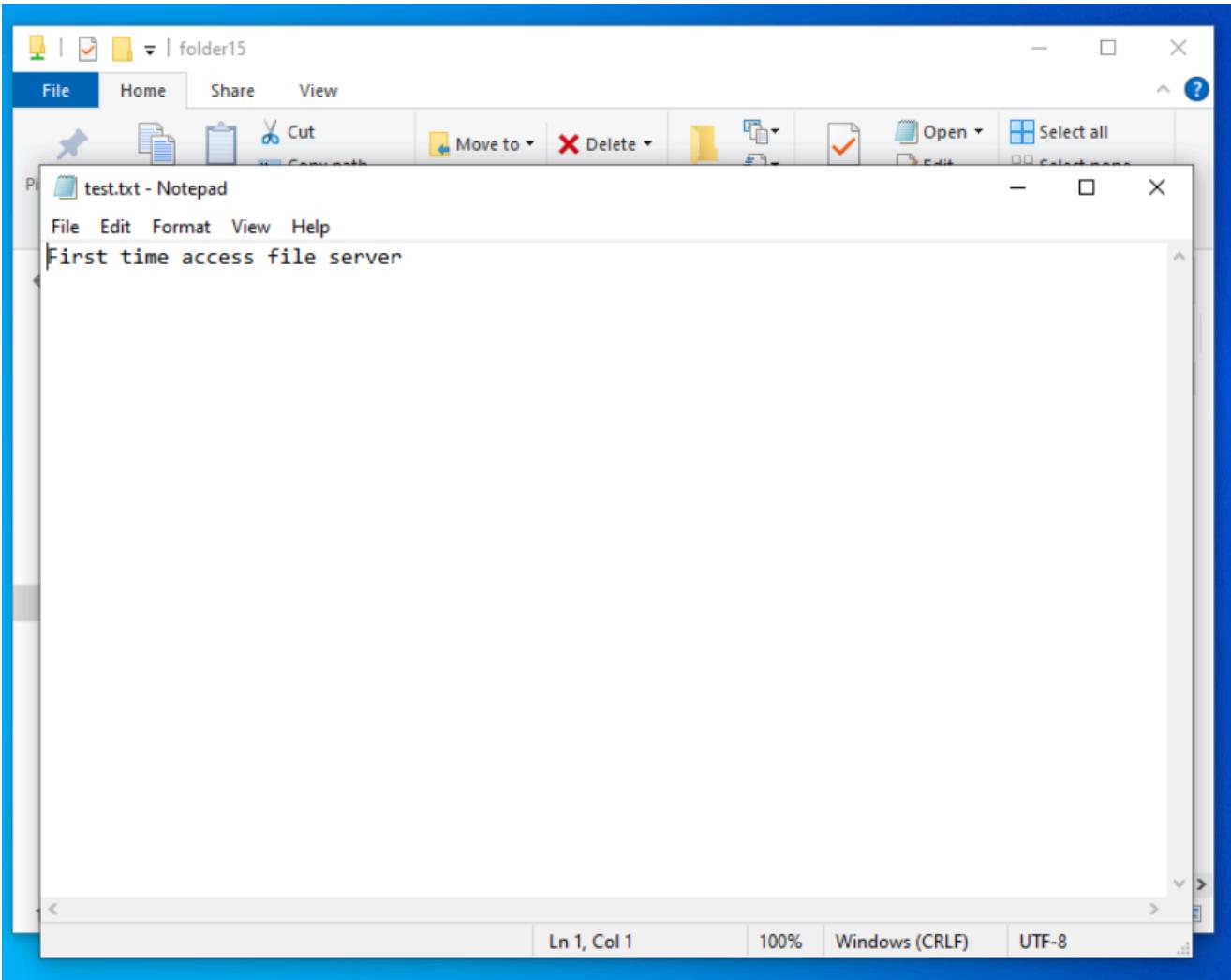
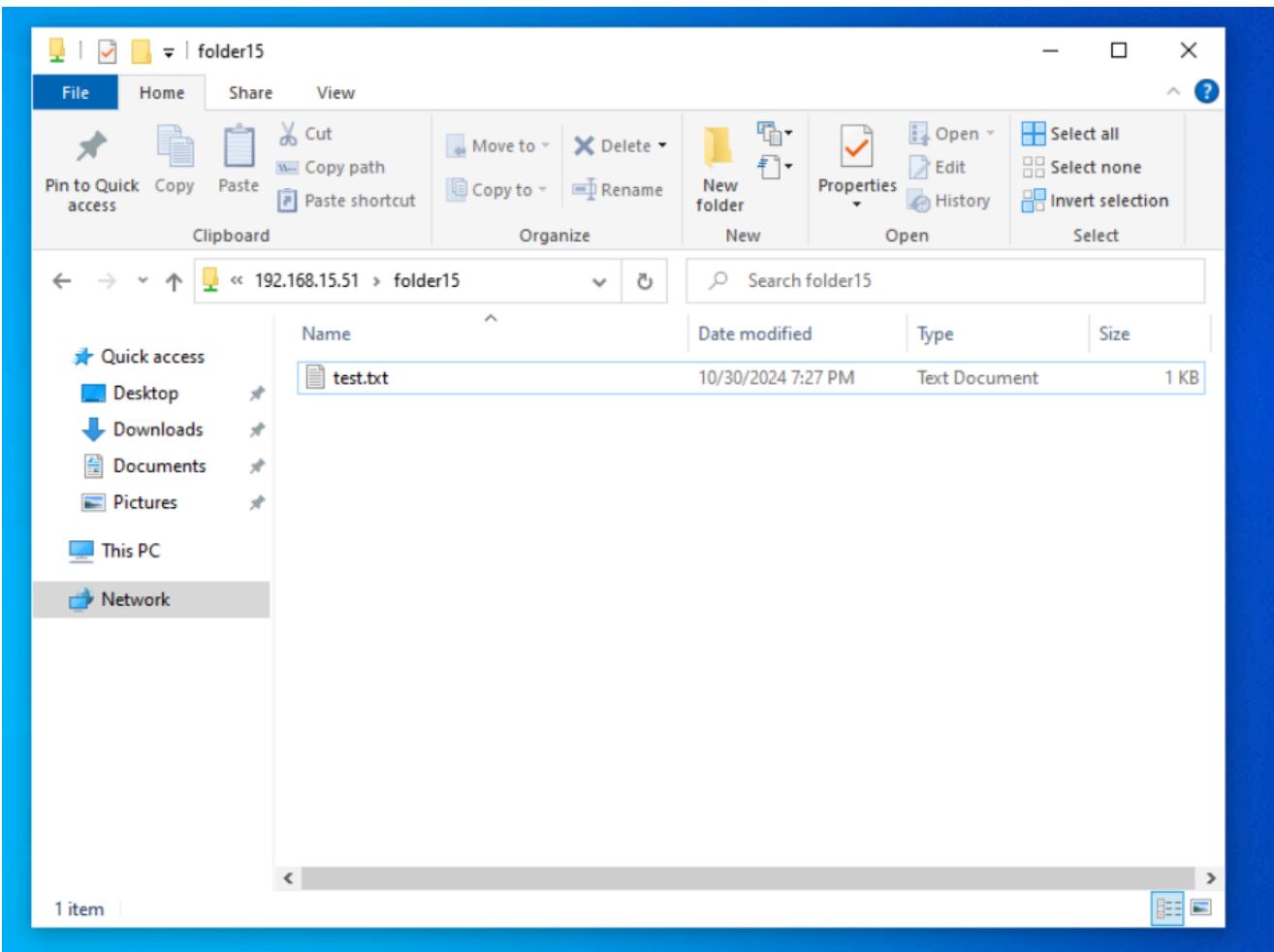


-Sử dụng tài khoản của máy File Server (user nhom13 đã tạo ở Bước 2):



Giải thích: vì ở File Server trên folder15 ta thực hiện việc share cho user nhom13 mà không share cho tài khoản của máy client nên khi đăng nhập vào File Server sử dụng tài khoản của máy client thì sẽ không vào được.

Bước 7: Sau khi truy cập thành công, trên máy Client tạo 1 tập tin tùy ý trong thư mục folder15. Báo cáo và giải thích kết quả thực hiện:



Giải thích kết quả thực hiện:

Vì user nhom13 trong folder15 đã được cấp quyền Read/Write nên trên folder15 ta có thể tạo được file test.txt và đọc được nội dung của file đó.

2. Triển khai Active Directory và xây dựng mô hình Domain

Yêu cầu 2.1

Đề bài

Tìm hiểu và trả lời câu hỏi sau:

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

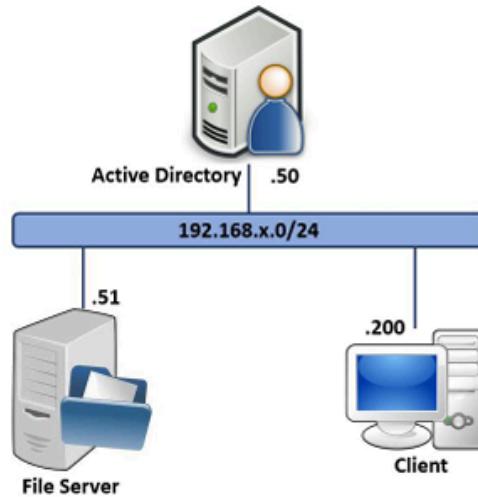
Trả lời

1. Active Directory (AD) là một dịch vụ quản lý danh tính và quyền truy cập do Microsoft phát triển, được sử dụng để quản lý người dùng, máy tính, tài nguyên và bảo mật trong một mạng doanh nghiệp. Nó là một thành phần chính của hệ điều hành Windows Server và giúp các tổ chức quản lý người dùng và tài nguyên mạng một cách tập trung và hiệu quả.
2.
 - Domain sẽ thích hợp cho các doanh nghiệp vì tính đồng bộ và quản lý của nó cũng như là có máy chủ tập trung. Việc mở rộng cũng sẽ dễ dàng tuy nhiên chi phí có thể cao hơn Workgroup
 - Workgroup lại yêu cầu chi phí thấp hơn nên sẽ thích hợp với các hệ thống nhỏ. Cách cấu hình và cài đặt dễ hơn

Yêu cầu 2.2

Đề bài

Xây dựng mô hình Domain như bên dưới.



Thông tin các máy:

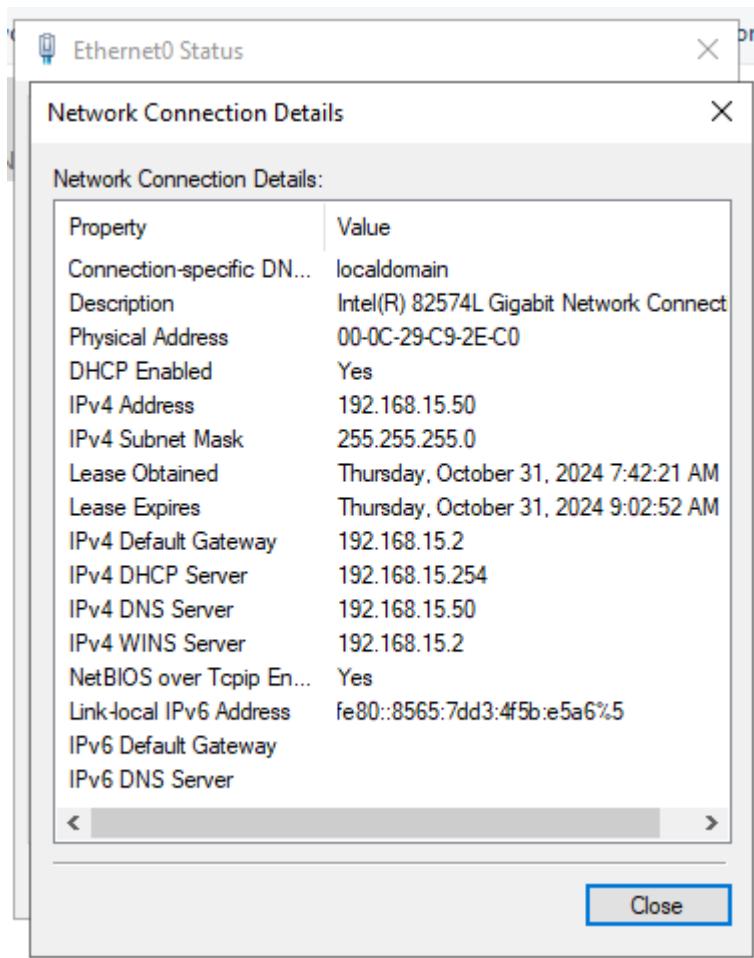
Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
File Server	Windows Server 2016	192.168.X.51/24	192.168.X.50
Active Directory	Windows Server 2016	192.168.X.50/24	192.168.X.50
Client	Windows 7/8/10	192.168.X.200/24	192.168.X.50

Các bước thực hiện

Cấu hình IP cho máy Active Directory:

```
Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::8565:7dd3:4f5b:e5a6%5
IPv4 Address . . . . . : 192.168.15.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.15.2
```

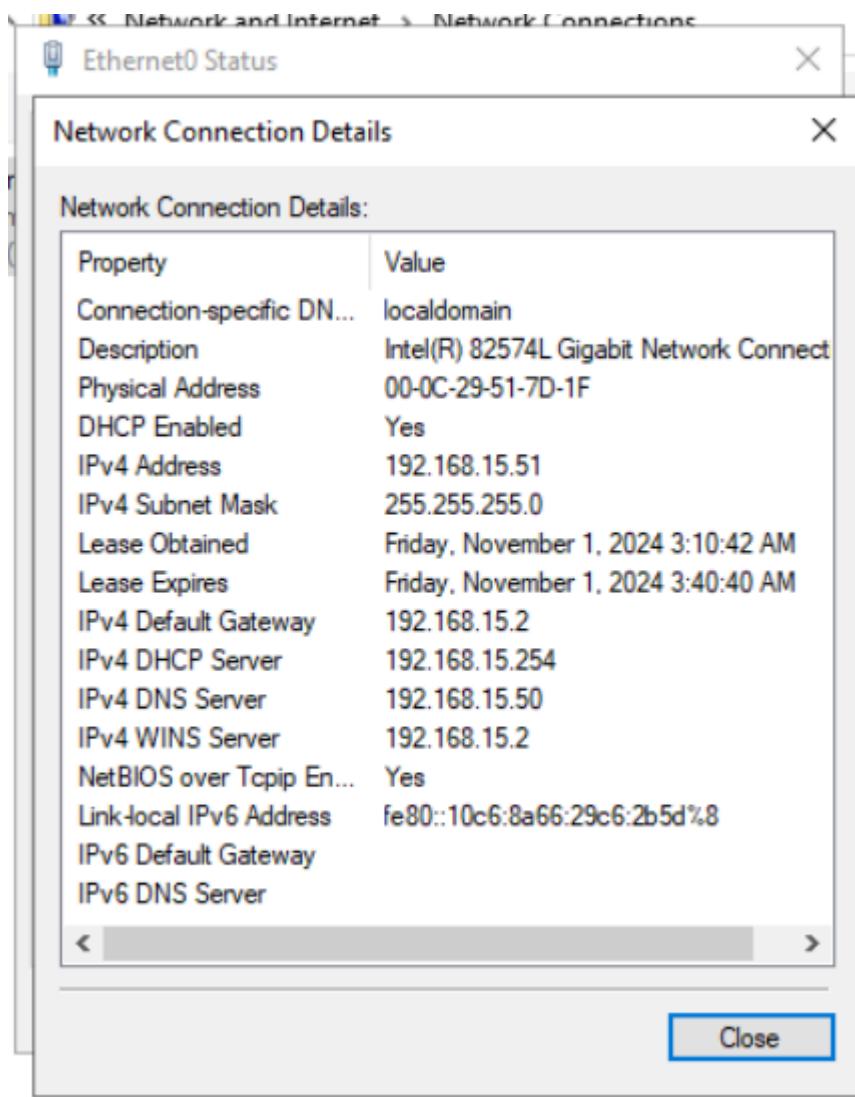


Cấu hình IP cho máy File Server:

Windows IP Configuration

Ethernet adapter Ethernet0:

```
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::10c6:8a66:29c6:2b5d%5
IPv4 Address . . . . . : 192.168.15.51
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.15.2
```

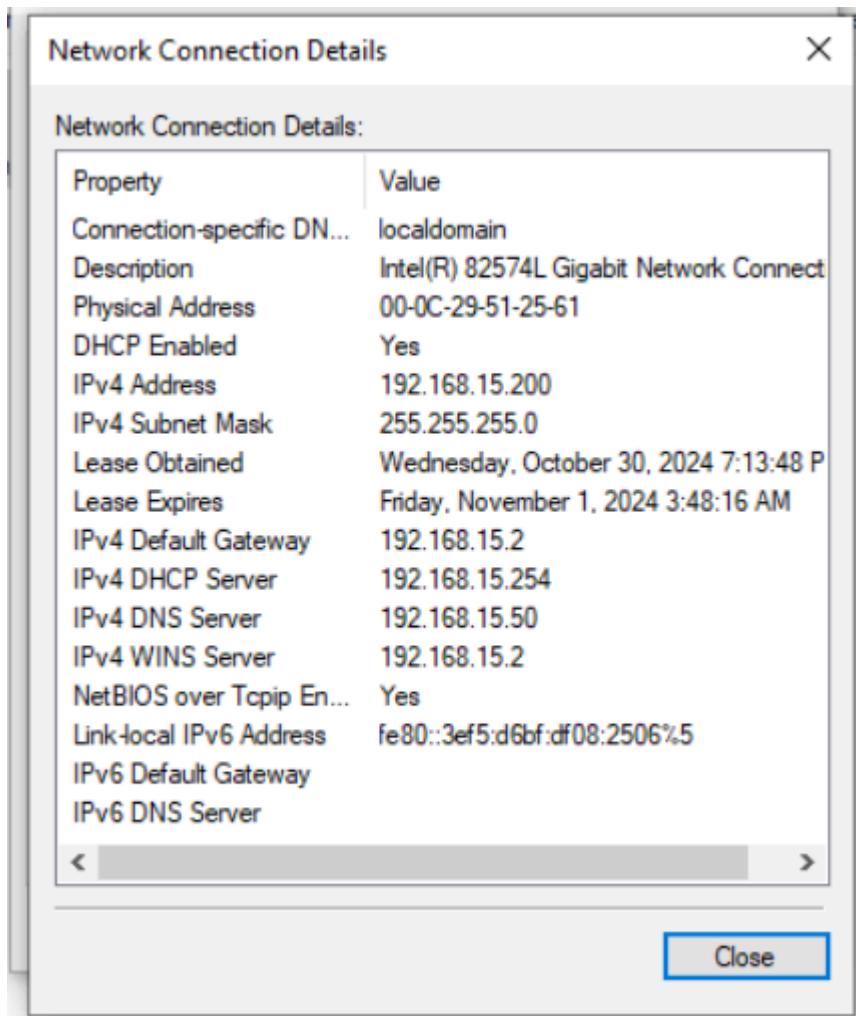


Cấu hình IP cho máy Client:

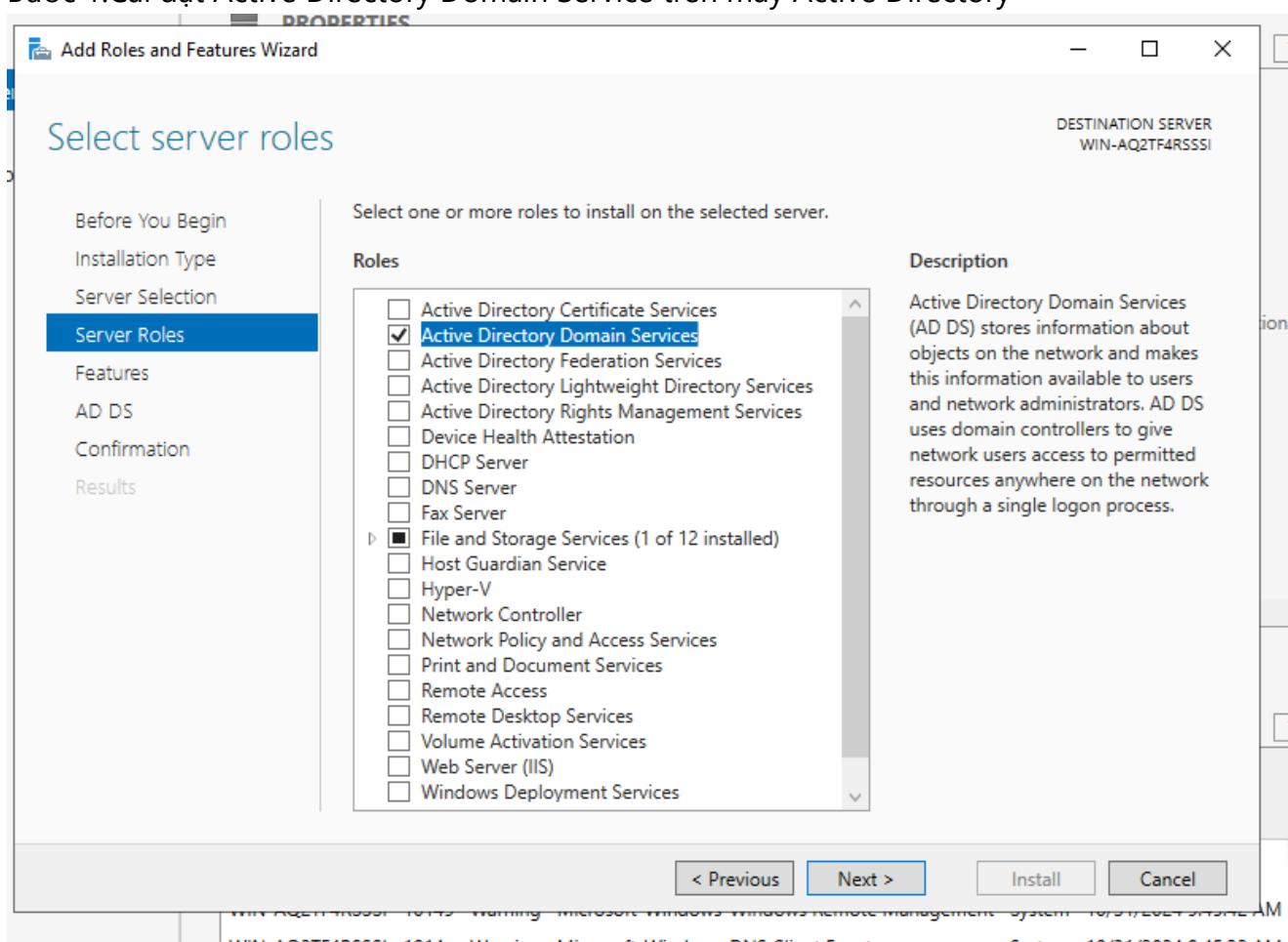
```
Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . : localdomain
  Link-local IPv6 Address . . . . . : fe80::3ef5:d6bf:df08:2506%5
  IPv4 Address . . . . . : 192.168.15.200
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.15.2
```



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



Select features

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results

Select one or more features to install on the selected server.

Features

- ▷ .NET Framework 3.5 Features
- ▷ .NET Framework 4.8 Features (2 of 7 installed)
- ▷ Background Intelligent Transfer Service (BITS)
- BitLocker Drive Encryption
- BitLocker Network Unlock
- BranchCache
- Client for NFS
- Containers
- Data Center Bridging
- Direct Play
- Enhanced Storage
- Failover Clustering
- Group Policy Management
- Host Guardian Hyper-V Support
- I/O Quality of Service
- IIS Hostable Web Core
- Internet Printing Client
- IP Address Management (IPAM) Server
- LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

< Previous

Next >

Install

Cancel

Before You Begin
Installation Type
Server Selection
Server Roles
Features:
AD DS
Confirmation
Results

View installation progress

i Feature installation

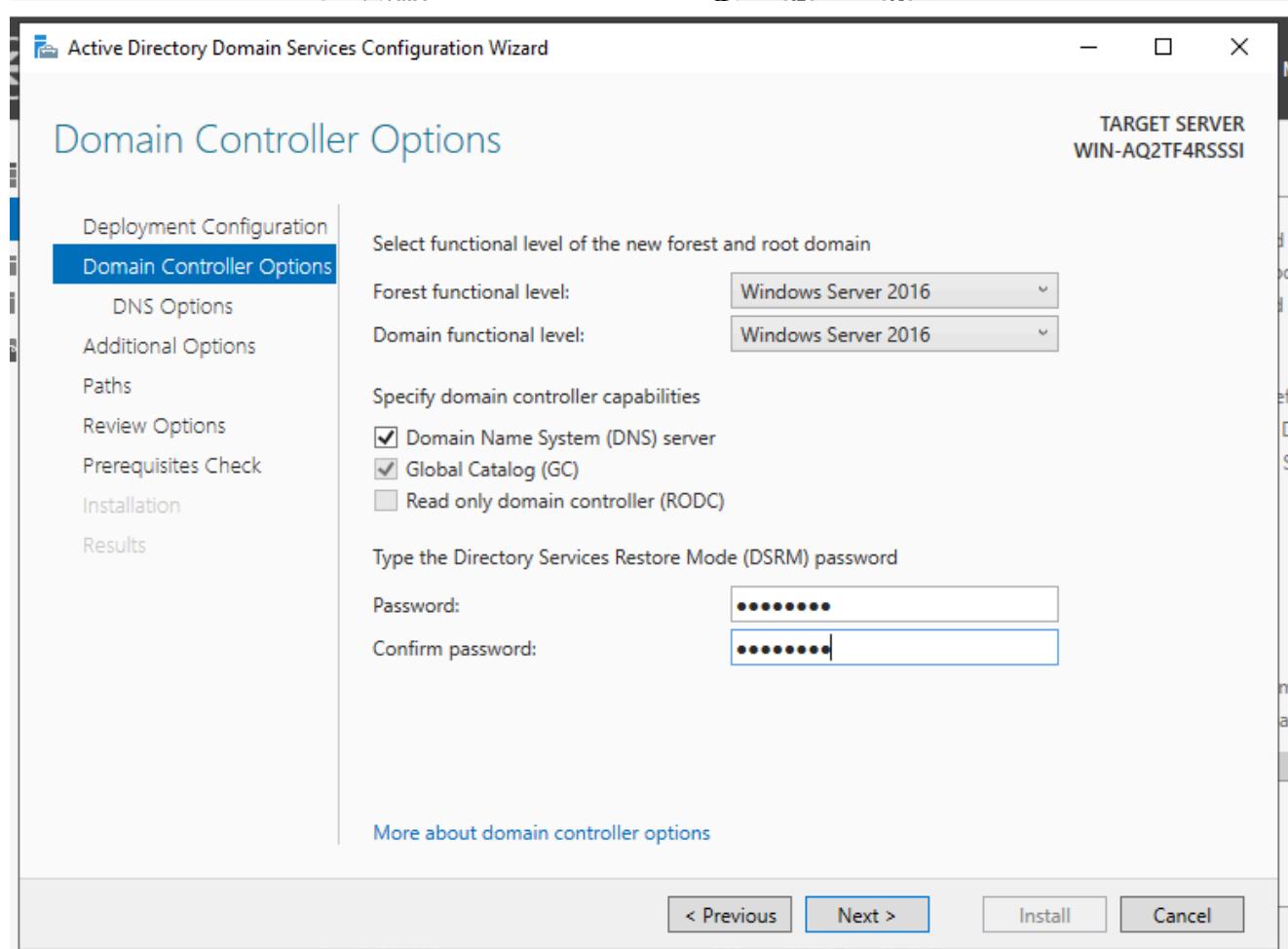
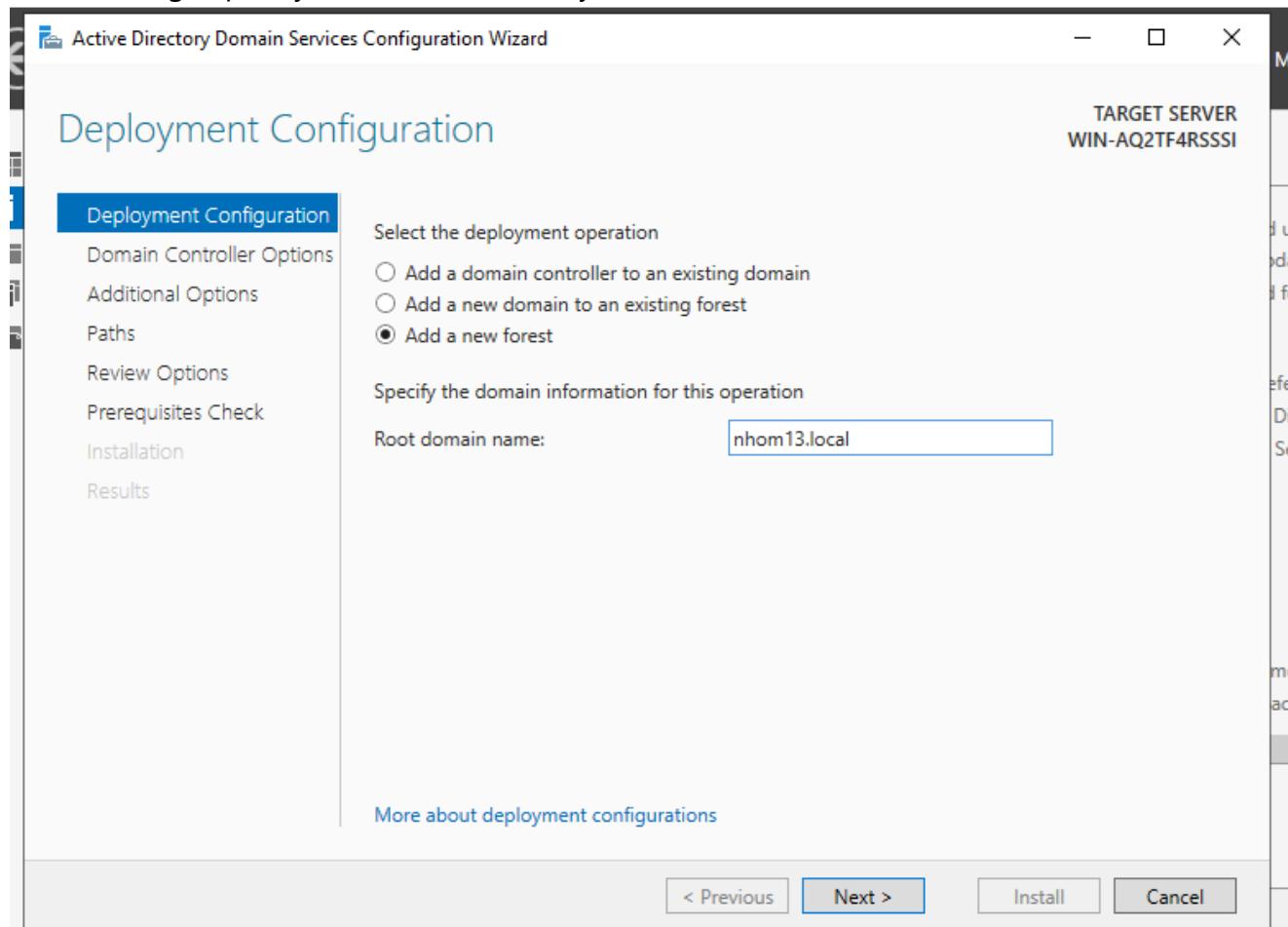


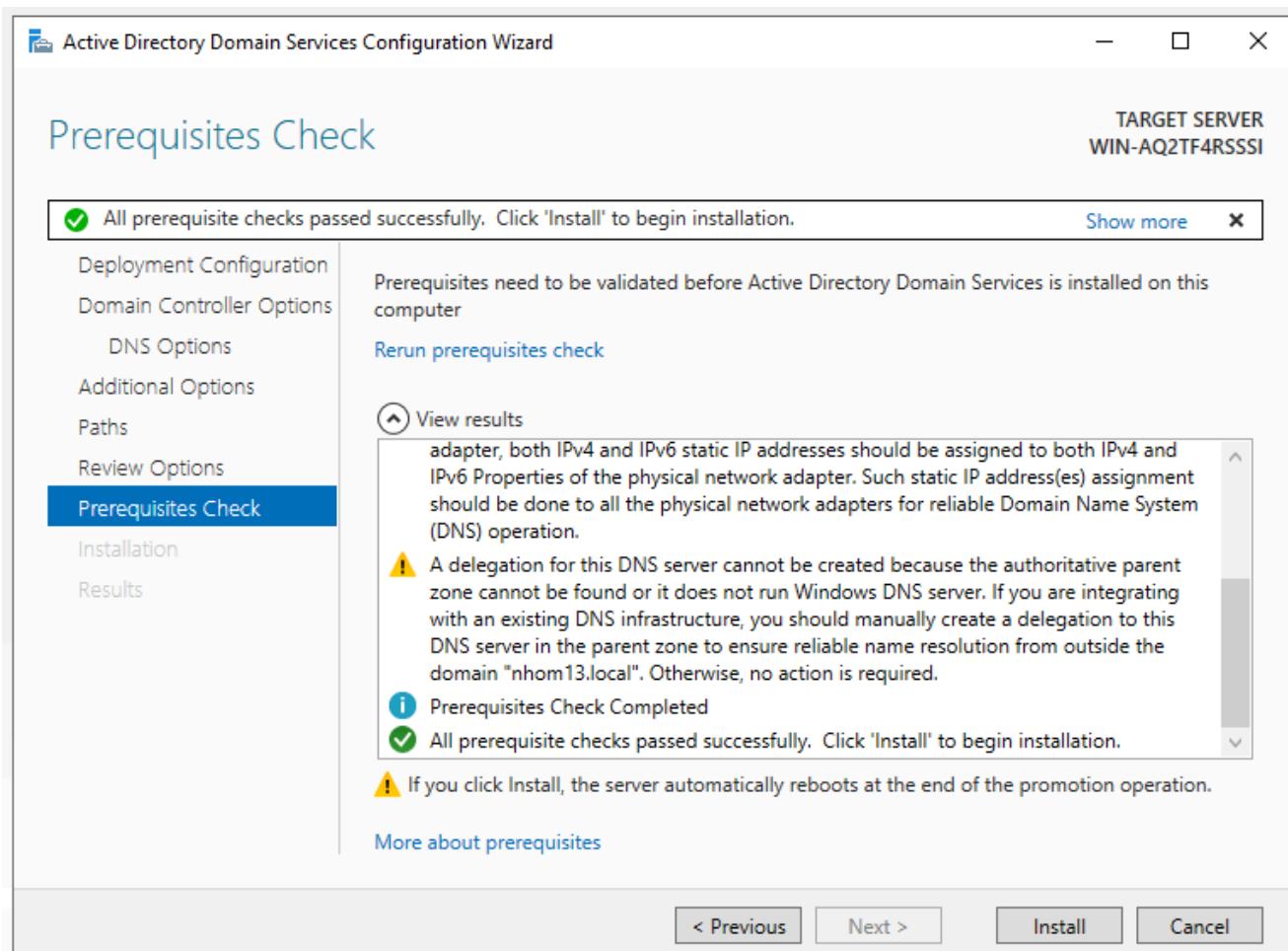
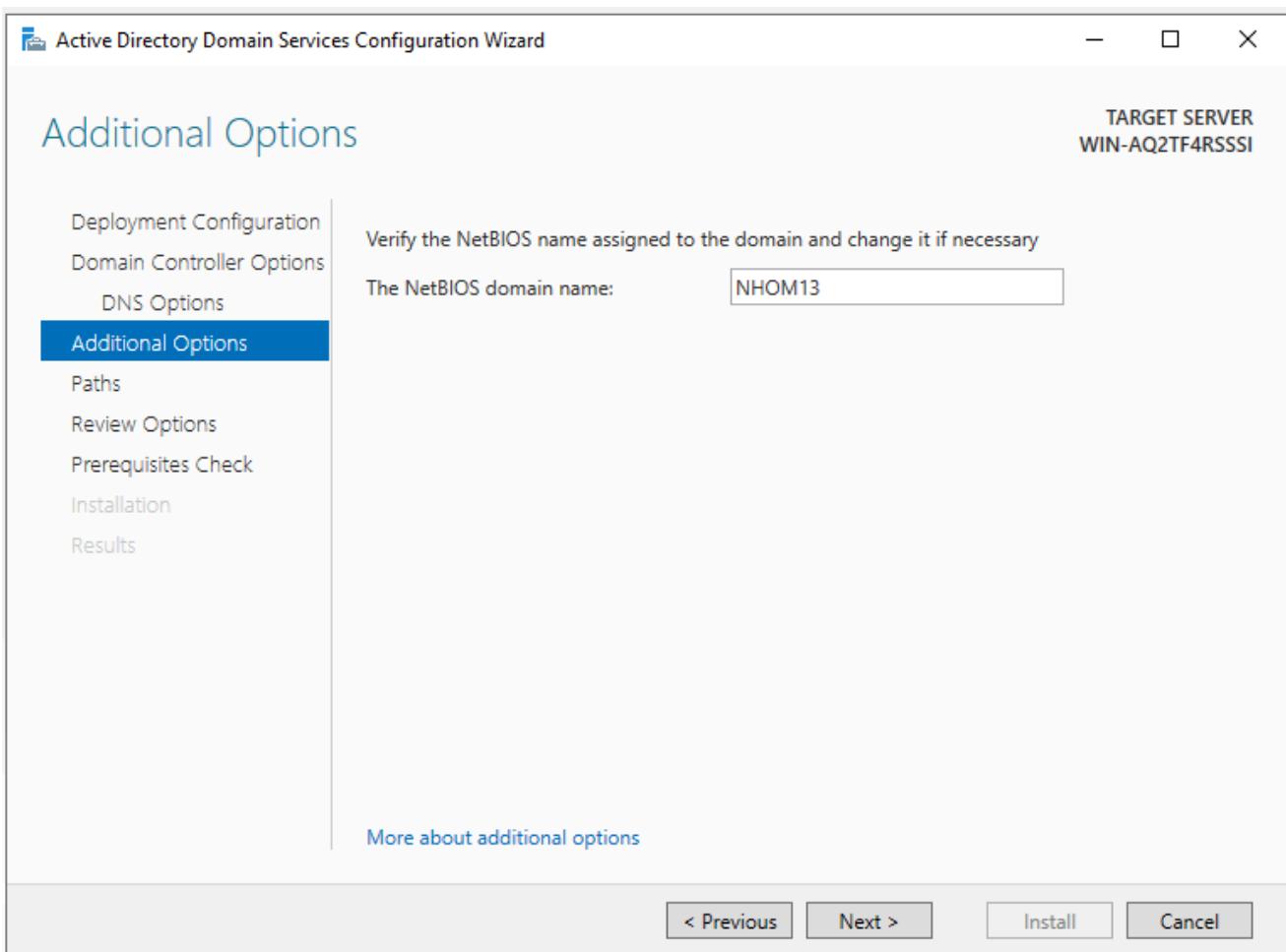
Installation started on ad

- Active Directory Domain Services
- Group Policy Management
- Remote Server Administration Tools
- Role Administration Tools
 - AD DS and AD LDS Tools
 - Active Directory module for Windows PowerShell
 - AD DS Tools
 - Active Directory Administrative Center
 - AD DS Snap-Ins and Command-Line Tools

 You can close this wizard without interrupting running tasks. View task progress or open this

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





Bước 3:Tạo user trong domain

Active Directory Users and Computers

New Object - User

Create in: nhom13.local/Users

First name: File Admin Initials:

Last name:

Full name: File Admin

User logon name:
fileadmin @nhom13.local

User logon name (pre-Windows 2000):
NHOM13\fileadmin

< Back Next > Cancel

Active Directory Users and Computers

New Object - User

Create in: nhom13.local/Users

First name: user1 Initials:

Last name:

Full name: user1

User logon name:
user1 @nhom13.local

User logon name (pre-Windows 2000):
NHOM13\user1

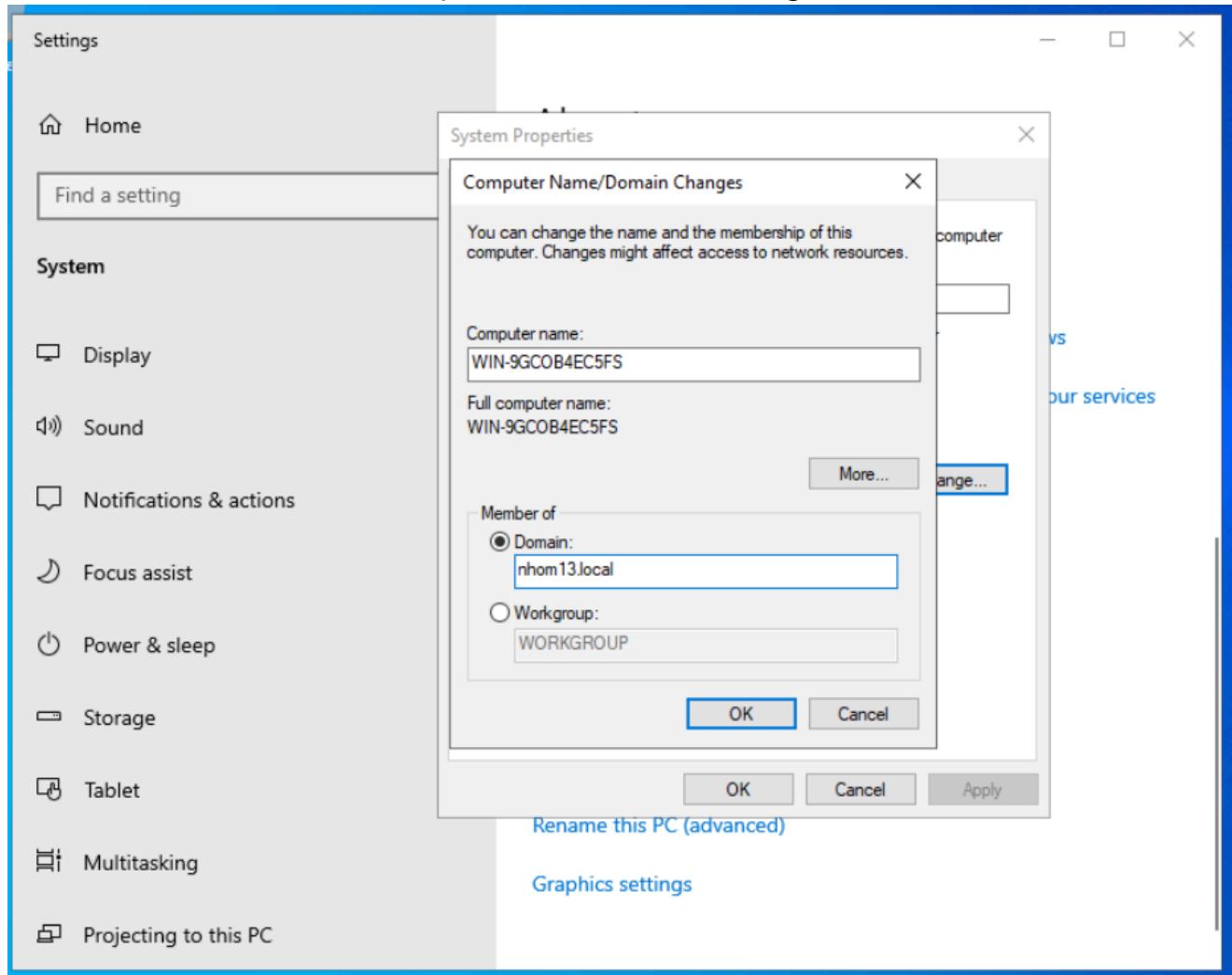
< Back Next > Cancel

Bước 4: Thêm File Server vào domain đã tạo.

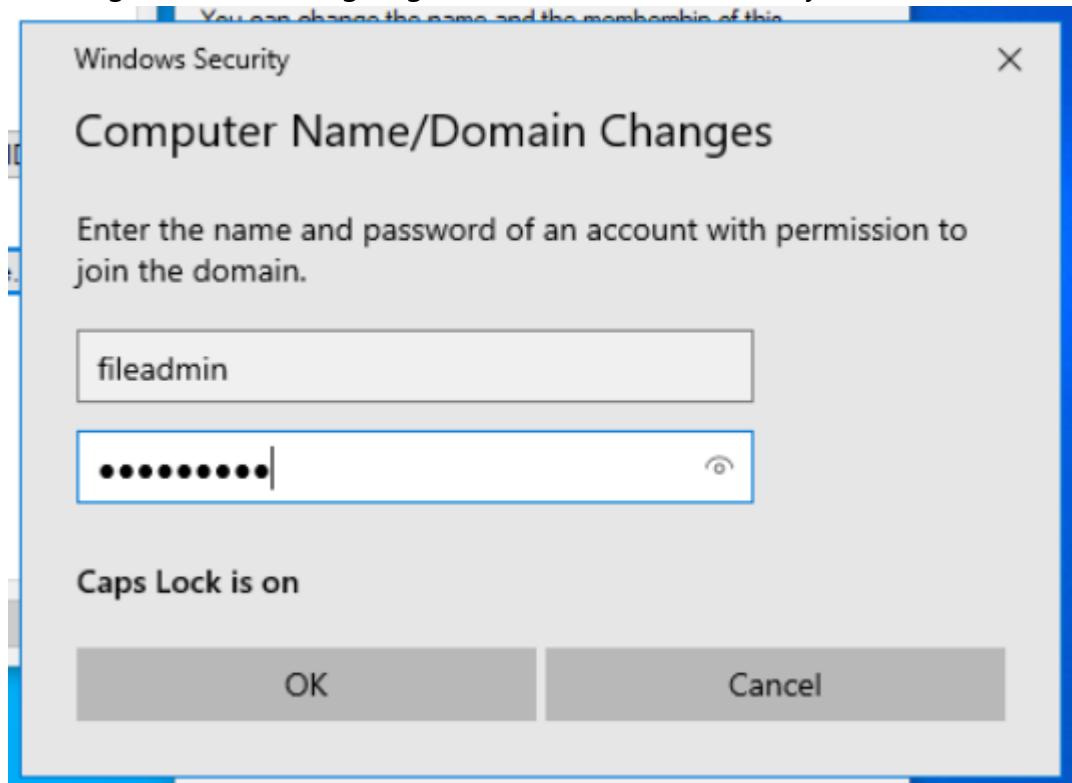
Trên máy File Server, kiểm tra kết nối đến domain:

```
Pinging 192.168.15.50 with 32 bytes of data:  
Reply from 192.168.15.50: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.15.50:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

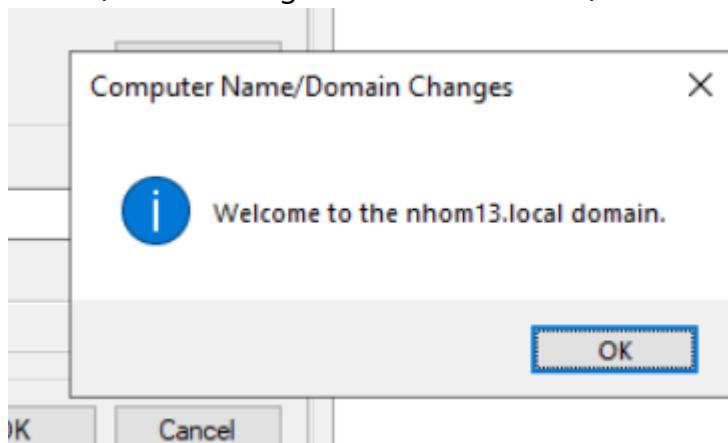
Trong cửa sổ System Properties, tab Computer Name, chọn Change. Sau đó tại trường Member of, chọn Domain và nhập tên domain muốn tham gia:



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.

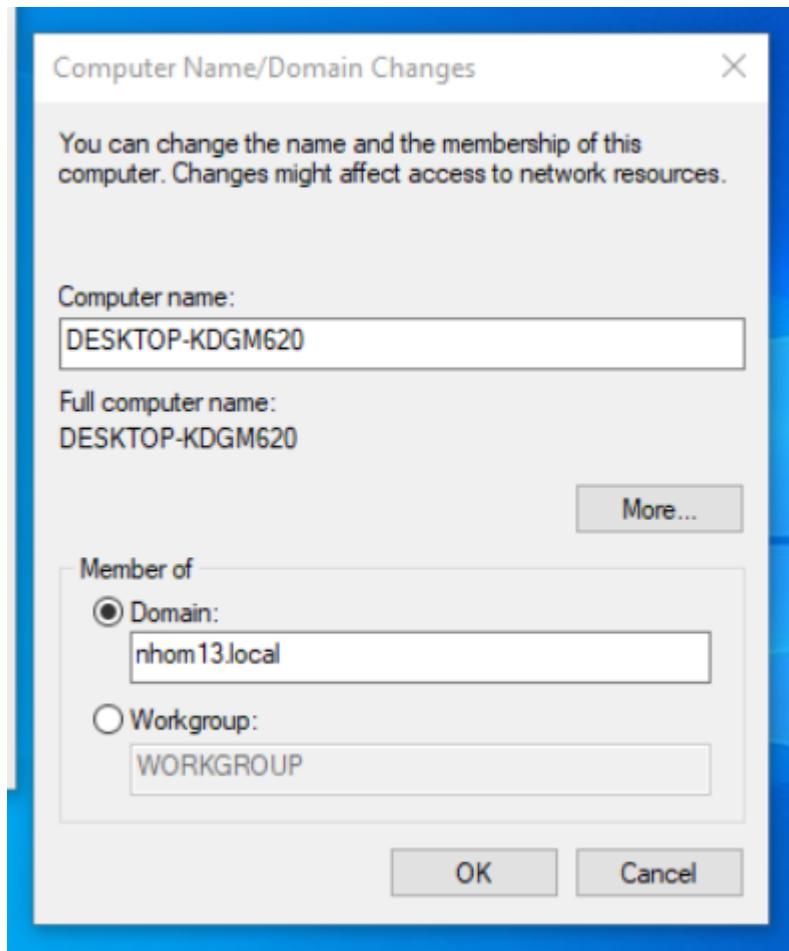
Bước 5: Thêm máy client vào domain đã tạo.

Thực hiện quá trình tương tự Bước 4 để thêm máy client vào domain.

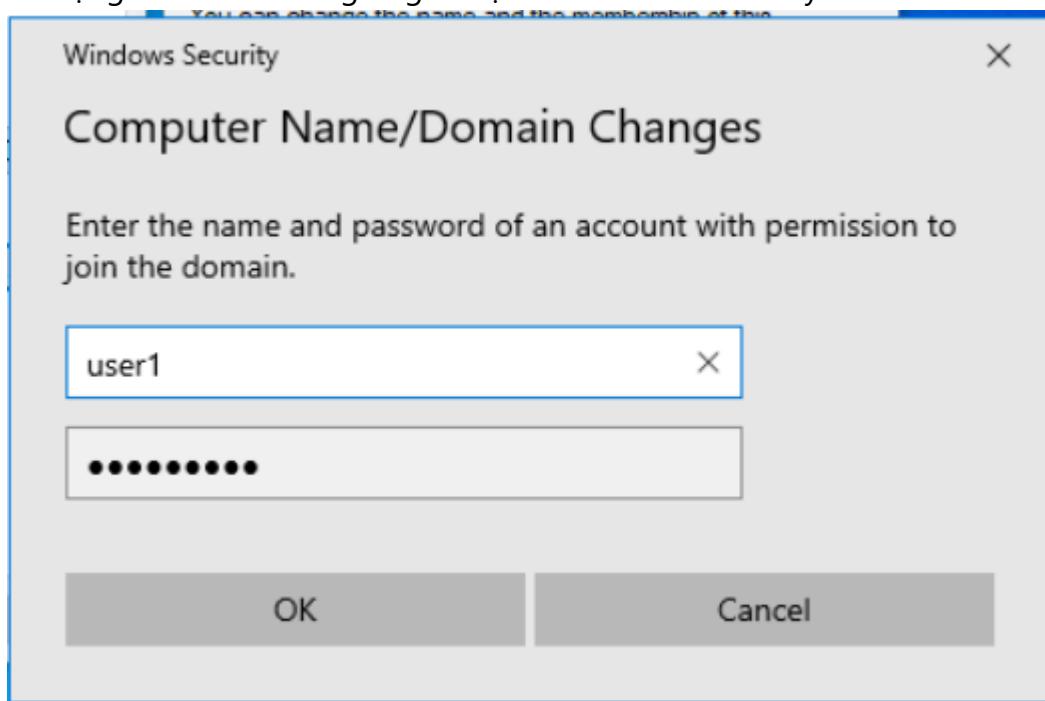
Trên máy Client, kiểm tra kết nối đến domain:

```
Pinging 192.168.15.50 with 32 bytes of data:  
Reply from 192.168.15.50: bytes=32 time=1ms TTL=128  
Reply from 192.168.15.50: bytes=32 time=1ms TTL=128  
Reply from 192.168.15.50: bytes=32 time<1ms TTL=128  
Reply from 192.168.15.50: bytes=32 time<1ms TTL=128  
  
Ping statistics for 192.168.15.50:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

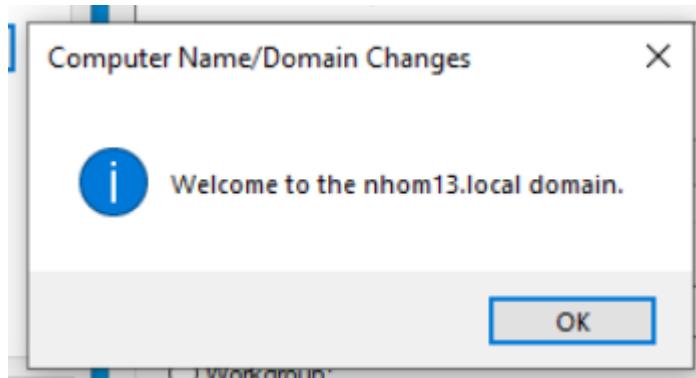
Trong cửa sổ System Properties, tab Computer Name, chọn Change. Sau đó tại trường Member of, chọn Domain và nhập tên domain muốn tham gia



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



Xác thực thành công thì Client sẽ được thêm vào domain.



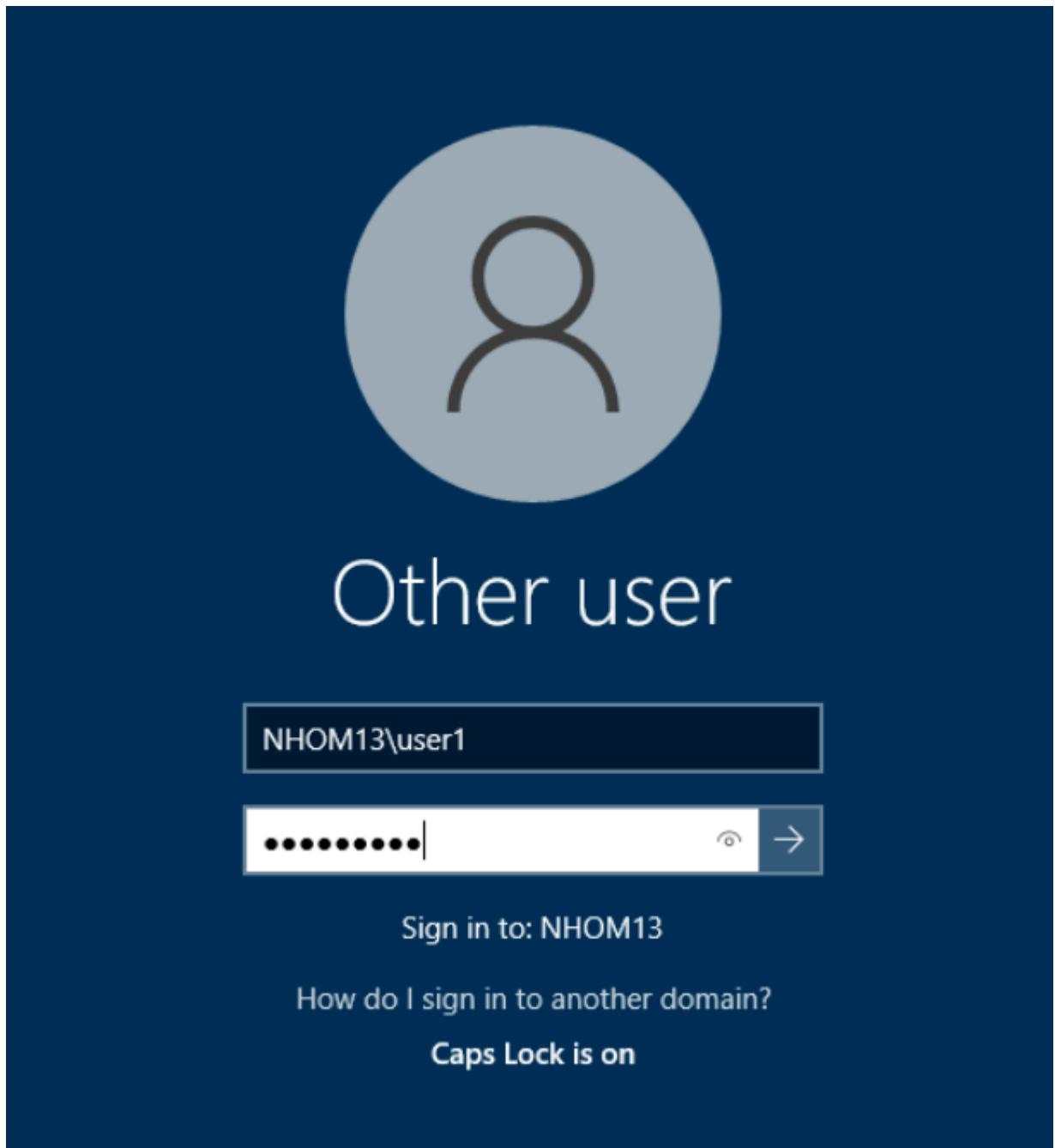
Sau khi quá trình này hoàn tất, tiến hành khởi động lại File Server

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

Đăng nhập lại vào File Server và thực hiện phân quyền lại folderX của File Server:

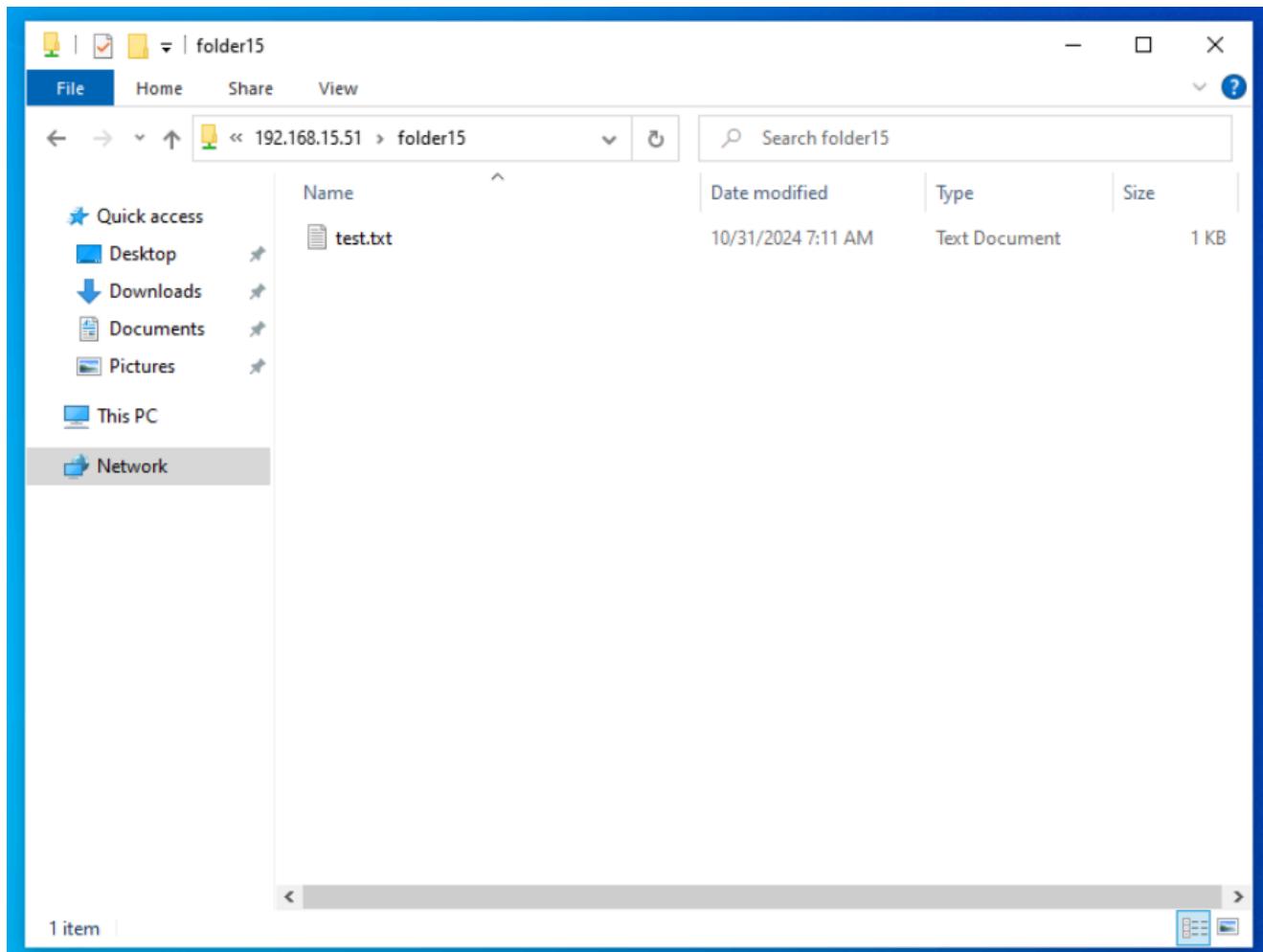
Type	Principal	Access	Inherited from	Applies to
Allow	Administrator (WIN-9GCOB4EC5FS\Administrators)	Full control	None	This folder, subfolders
Allow	Administrators (WIN-9GCOB4EC5FS\Adm...)	Full control	None	This folder, subfolders
Allow	nhom13 (WIN-9GCOB4EC5FS\nhom13)	Full control	None	This folder, subfolders
Allow	SYSTEM	Full control	None	This folder, subfolders
Allow	Domain Users (NHOM13\Domain Users)	Modify	None	This folder, subfolders

Bước 7: Tại máy Client, đăng nhập với tài khoản NHOM13\user1 (tài khoản trong domain):

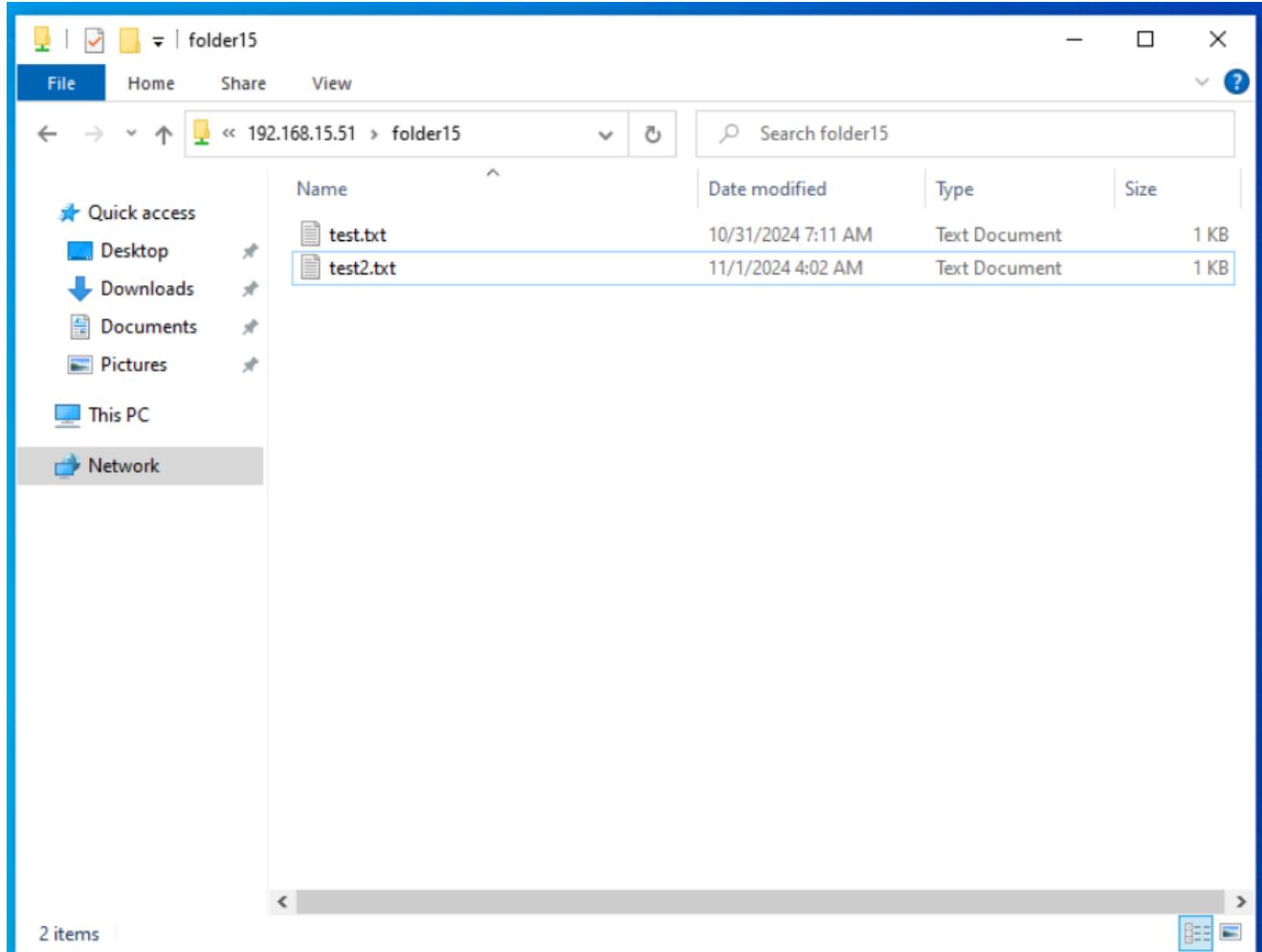


Bước 8: Sau khi đăng nhập, trên Client vào Run và kết nối vào File Server. Kiểm tra các thao tác đọc, ghi dữ liệu tại thư mục này folderX (giống với bài 1).

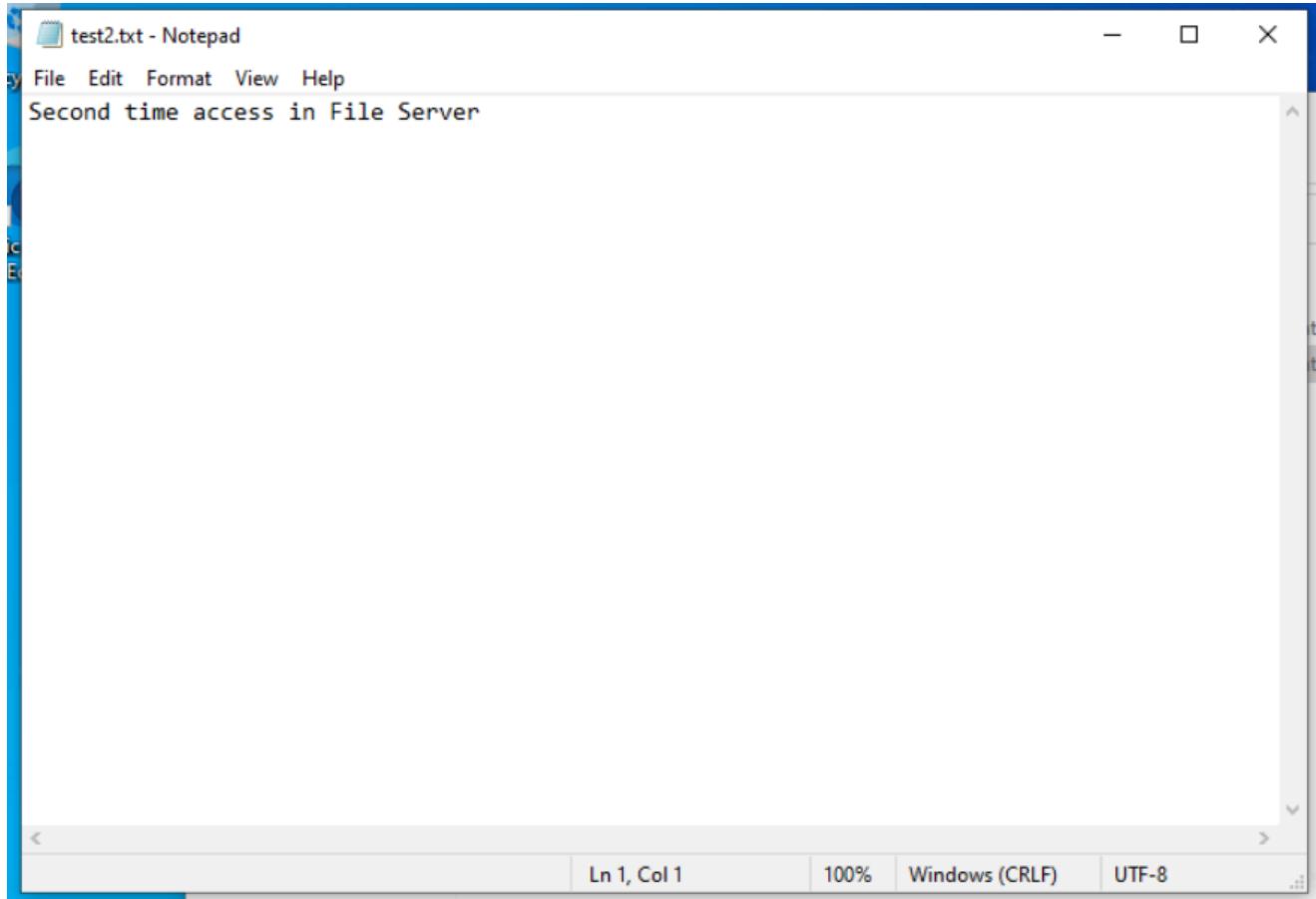
Sau khi chạy lệnh Run và kết nối với File Server, ta không cần phải thực hiện đăng nhập:



Tạo một file text và lưu trong File Server:



Xem nội dung file vừa tạo:



Sự khác biệt trong việc truy cập thư mục ở mô hình Domain so với mô hình Workgroup:

- +Ở mô hình Domain ta chỉ cần thực hiện đăng nhập một lần ở bước đăng nhập đăng nhập với tài khoản NHOM13\user1
- +Ở mô hình Workgroup ta thực hiện đăng nhập sau khi thực hiện lệnh Run và mỗi lần thoát ra phải đăng nhập lại (đăng nhập riêng lẻ).

Giải thích:

Trong mô hình Domain, quyền truy cập thư mục được quản lý tập trung qua máy chủ domain controller. Người dùng chỉ cần đăng nhập một lần và có thể truy cập tài nguyên trong toàn hệ thống với các chính sách bảo mật đồng nhất, giúp quản lý và bảo mật tốt hơn.

Trong khi đó, ở mô hình Workgroup, mỗi máy tính tự quản lý tài khoản và quyền truy cập riêng. Người dùng phải đăng nhập vào từng máy khi cần, và không có chính sách bảo mật tập trung, khiến việc quản lý phức tạp và bảo mật kém hơn.

3. Xây dựng mô hình Additional Domain Controller cho dịch vụ Active Directory

Yêu cầu 3.1

Đề bài

Sinh viên hãy tìm hiểu và trả lời câu hỏi:

Additional Domain Controller (ADC) là gì?

ADC là một máy chủ bổ sung trong hệ thống Active Directory, đóng vai trò như một Domain Controller thứ hai hoặc phụ trong cùng một miền (domain). Nó giữ bản sao đầy đủ và đồng bộ của cơ sở dữ liệu Active Directory, có thể thực hiện các chức năng tương tự như Domain Controller chính (Primary Domain Controller – PDC). ADC giúp tăng cường tính sẵn sàng và khả năng dự phòng cho hệ thống, đảm bảo hệ thống vẫn hoạt động ngay cả khi một Domain Controller gặp sự cố.

Mô hình ADC hoạt động như thế nào?

ADC hoạt động dựa trên việc sao chép (replication) dữ liệu từ Domain Controller chính hoặc các ADC khác trong cùng domain. Tất cả các Domain Controller, bao gồm cả ADC, đồng bộ dữ liệu Active Directory của chúng theo lịch trình sao chép, đảm bảo mọi thay đổi (như thêm hoặc xóa người dùng, cập nhật thông tin bảo mật) đều được truyền đến tất cả các Domain Controller. Điều này tạo ra tính nhất quán trên toàn bộ hệ thống. Khi nhận yêu cầu xác thực hoặc tra cứu từ người dùng, ADC có thể xử lý trực tiếp yêu cầu mà không cần gửi về Domain Controller chính, giúp giảm tải và cải thiện hiệu suất.

Khi nào cần sử dụng ADC?

Tăng cường tính sẵn sàng và dự phòng: Nếu Domain Controller chính gặp sự cố, ADC sẽ tiếp quản vai trò xác thực và quản lý tài nguyên, đảm bảo hệ thống không bị gián đoạn.

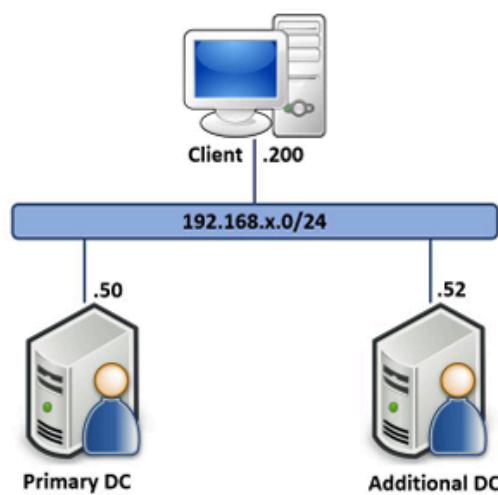
Giảm tải và cải thiện hiệu suất: Khi có nhiều người dùng trong cùng một mạng hoặc nhiều chi nhánh, việc sử dụng ADC tại các vị trí khác nhau sẽ giúp giảm tải cho Domain Controller chính và tăng tốc độ phản hồi.

Đảm bảo tính liên tục cho hệ thống: Các tổ chức có yêu cầu cao về thời gian hoạt động liên tục (uptime) thường triển khai ADC để tránh tình trạng gián đoạn do phụ thuộc vào một Domain Controller duy nhất.

Yêu cầu 3.2

Đề bài

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



Lab 4: Triển khai Active Directory trên Windows Server

Thông tin các máy:

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7/8/10	192.168.X.200/24	192.168.X.50 192.168.X.52
Primary DC	Windows Server 2016	192.168.X.50/24	192.168.X.50 192.168.X.52
Additional DC	Windows Server 2016	192.168.X.52/24	192.168.X.52 192.168.X.50

Các bước thực hiện

Bước 1

Thay đổi ip trên Primary DC

```
C:\> ipconfig /all  
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Description . . . . . : Intel(R) 82574L Gigabit Network Connection  
Physical Address. . . . . : 00-0C-29-EC-33-6C  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::557:4d0:5d3d:a545%6(PREFERRED)  
IPv4 Address. . . . . : 192.168.15.50(PREFERRED)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Thursday, October 31, 2024 8:01:19 AM  
Lease Expires . . . . . : Thursday, October 31, 2024 8:52:30 AM  
Default Gateway . . . . . : 192.168.15.2  
DHCP Server . . . . . : 192.168.15.254  
DHCPv6 IAID . . . . . : 100666409  
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-B4-04-00-0C-29-EC-33-6C  
DNS Servers . . . . . : 192.168.15.50  
192.168.15.52  
Primary WINS Server . . . . . : 192.168.15.2  
NetBIOS over Tcpip. . . . . : Enabled  
  
C:\Users\Administrator>
```

Thay đổi ip trên ADC

```
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Description . . . . . : Intel(R) 82574L Gigabit Network Connection  
Physical Address. . . . . : 00-0C-29-30-DE-69  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::70e7:c13b:b3c6:2166%6(PREFERRED)  
IPv4 Address. . . . . : 192.168.15.52(PREFERRED)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Thursday, October 31, 2024 8:08:49 AM  
Lease Expires . . . . . : Thursday, October 31, 2024 8:53:57 AM  
Default Gateway . . . . . : 192.168.15.2  
DHCP Server . . . . . : 192.168.15.254  
DHCPv6 IAID . . . . . : 100666409  
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-B4-F9-3C-00-0C-29-30-DE-69  
DNS Servers . . . . . : 192.168.15.50  
192.168.15.52  
Primary WINS Server . . . . . : 192.168.15.2  
NetBIOS over Tcpip. . . . . : Enabled  
  
C:\Users\Administrator>
```

Thay đổi ip trên client

```
Ethernet adapter Ethernet0:  
  
Connection-specific DNS Suffix . : localdomain  
Description . . . . . : Intel(R) 82574L Gigabit Network Connection  
Physical Address. . . . . : 00-0C-29-9C-DD-53  
DHCP Enabled. . . . . : Yes  
Autoconfiguration Enabled . . . . . : Yes  
Link-local IPv6 Address . . . . . : fe80::9b97:4f4b:9d17:1735%6(PREFERRED)  
IPv4 Address. . . . . : 192.168.15.200(PREFERRED)  
Subnet Mask . . . . . : 255.255.255.0  
Lease Obtained. . . . . : Thursday, October 31, 2024 8:00:22 AM  
Lease Expires . . . . . : Thursday, October 31, 2024 8:55:53 AM  
Default Gateway . . . . . : 192.168.15.2  
DHCP Server . . . . . : 192.168.15.254  
DHCPv6 IAID . . . . . : 100666409  
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-85-ED-60-00-0C-29-9C-DD-53  
DNS Servers . . . . . : 192.168.15.50  
192.168.15.52  
Primary WINS Server . . . . . : 192.168.15.2  
NetBIOS over Tcpip. . . . . : Enabled  
  
C:\Users\victim>
```

Cài đặt domain trên Primary DC

progress

DESTINATION SERVER
WIN-M1OGG1F4MDS

[View installation progress](#)

Feature installation

Configuration required. Installation succeeded on WIN-M1OGG1F4MDS.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools

 You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

Cài đặt AD trên AD

Server Manager

Active Directory Domain Services Configuration Wizard

TARGET SERVER
WIN-M1OGG1F4MDS

Review Options

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Review your selections:

- The NetBIOS name of the domain: NHOM13
- Forest Functional Level: Windows Server 2016
- Domain Functional Level: Windows Server 2016

Additional Options:

- Global catalog: Yes
- DNS Server: Yes
- Create DNS Delegation: No
- Database folder: C:\Windows\NTDS

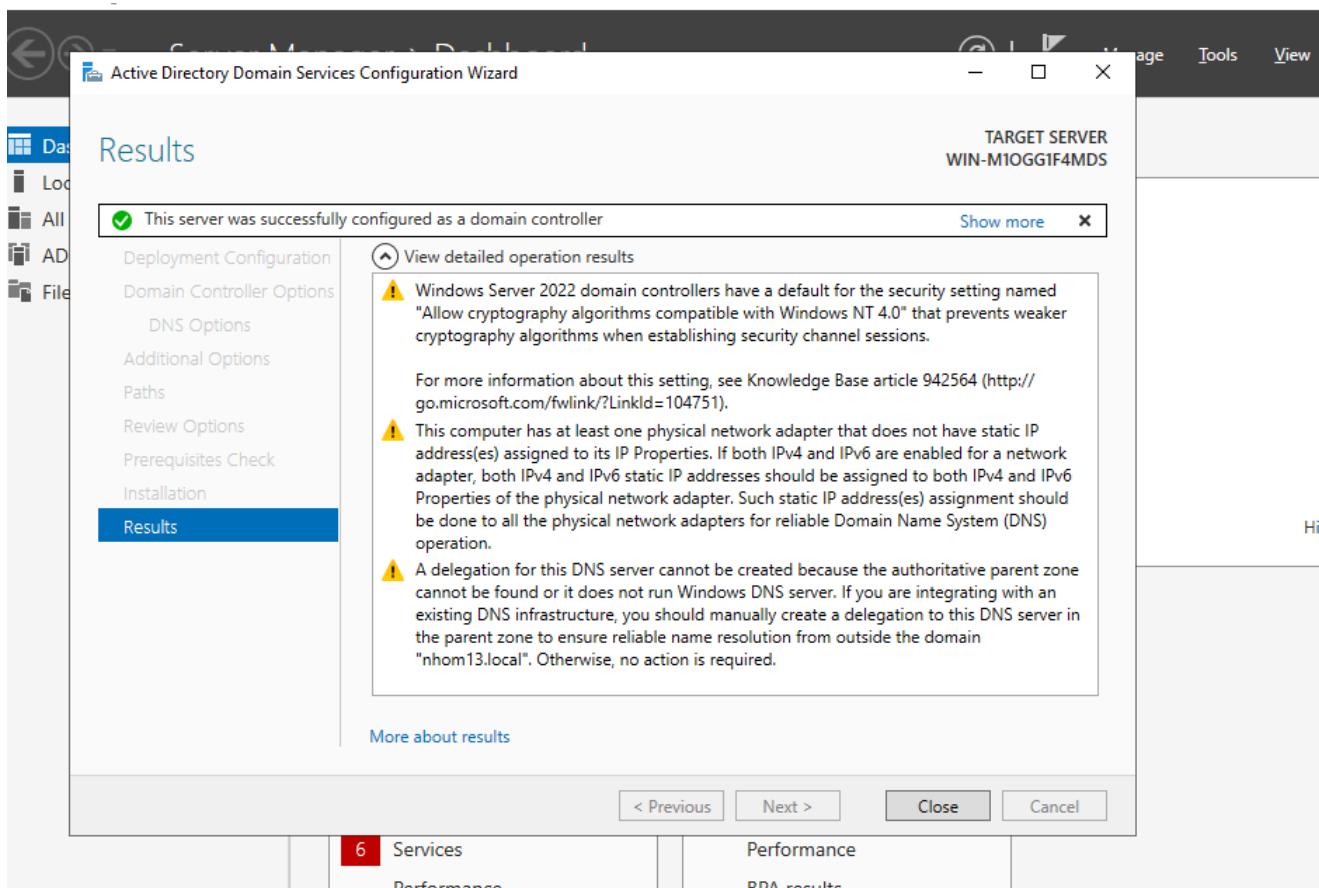
These settings can be exported to a Windows PowerShell script to automate additional installations

[View script](#)

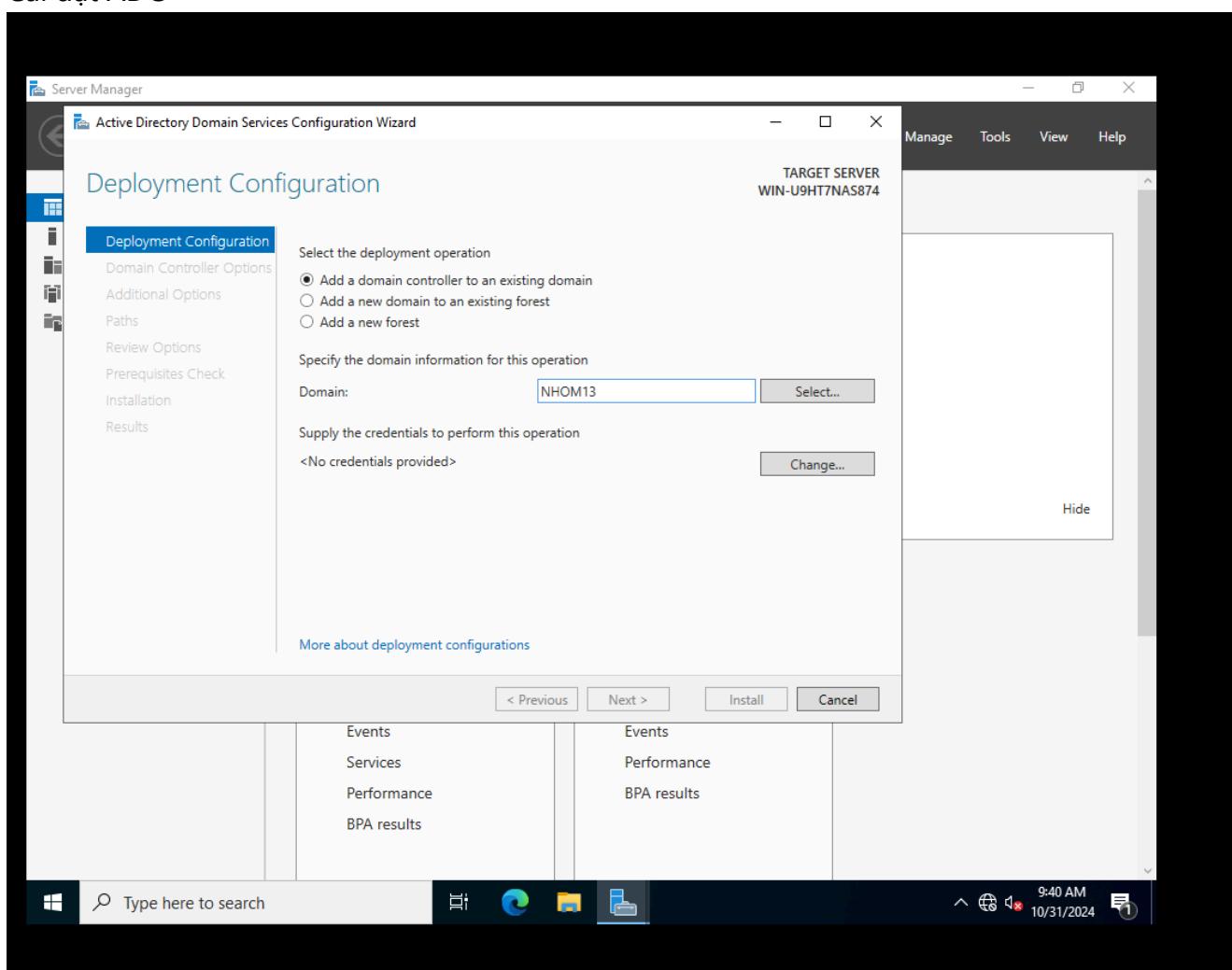
More about installation options

< Previous | Next > | Install | Cancel

Services | Performance

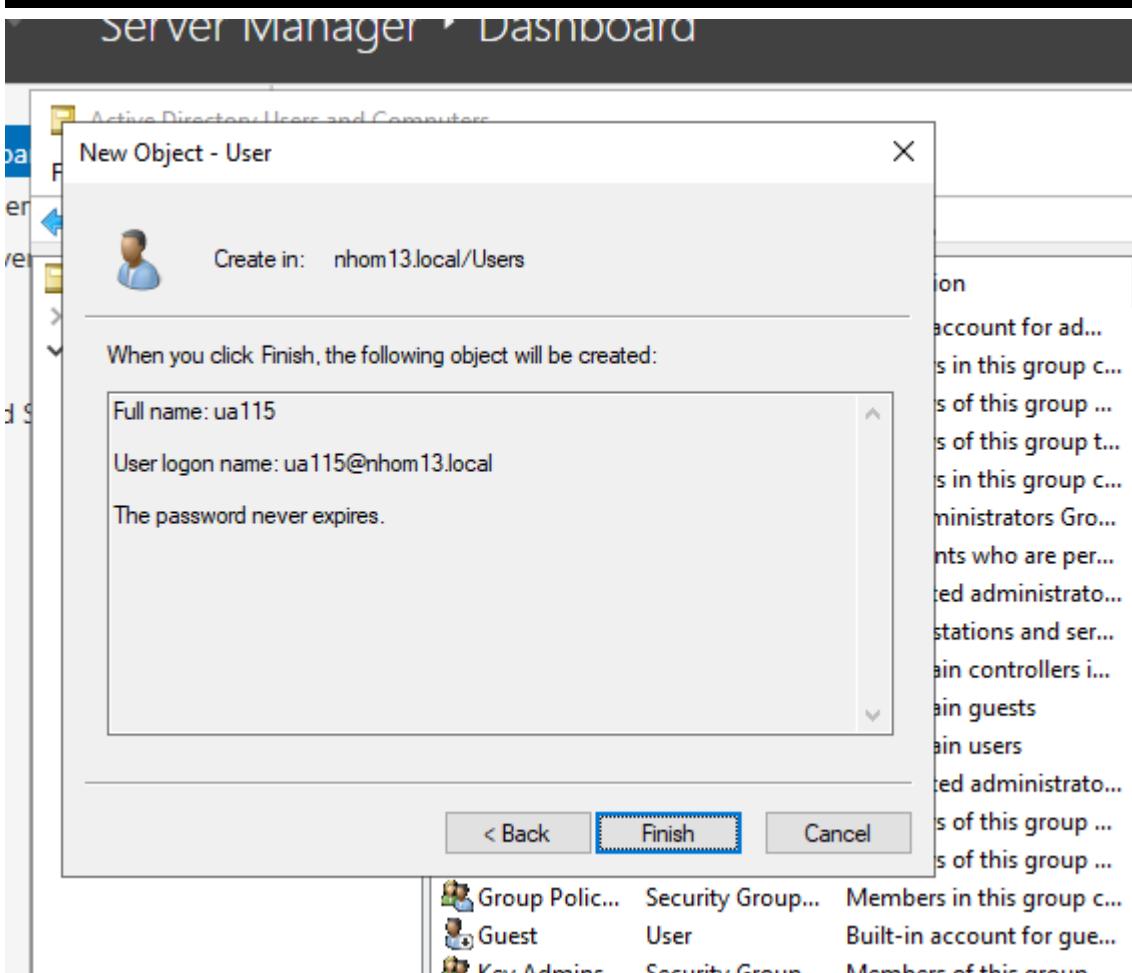
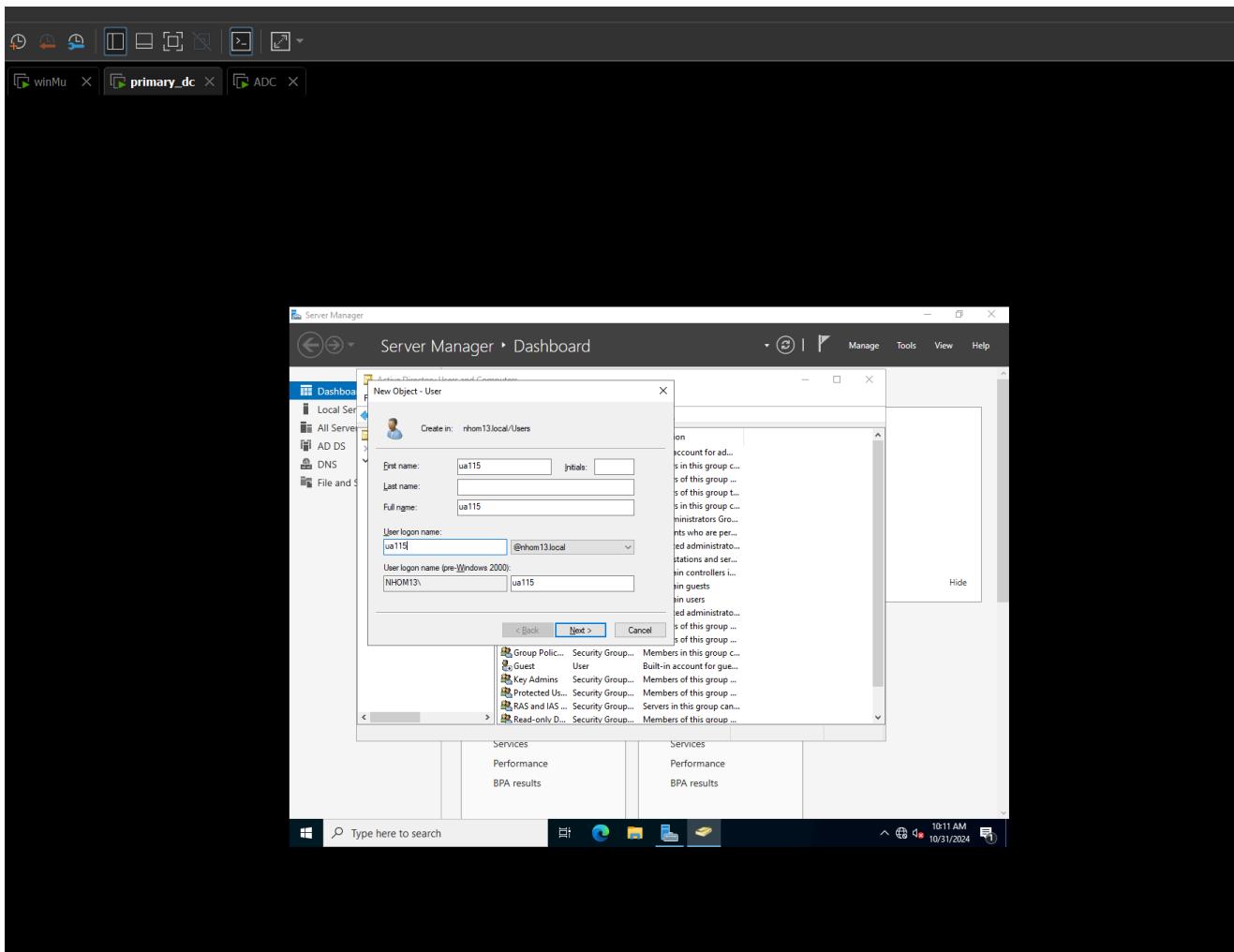


Cài đặt ADC

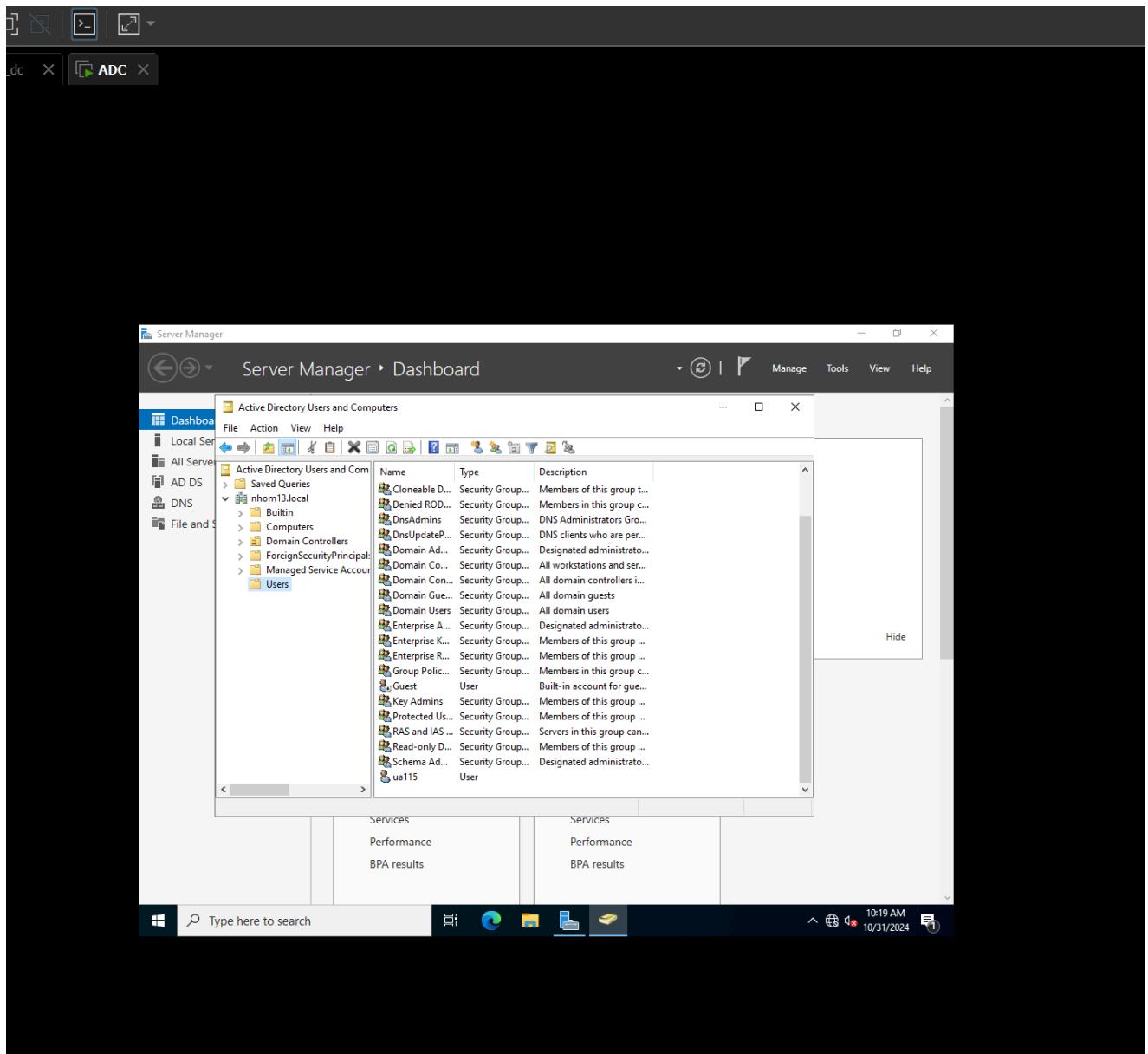


Bước 2

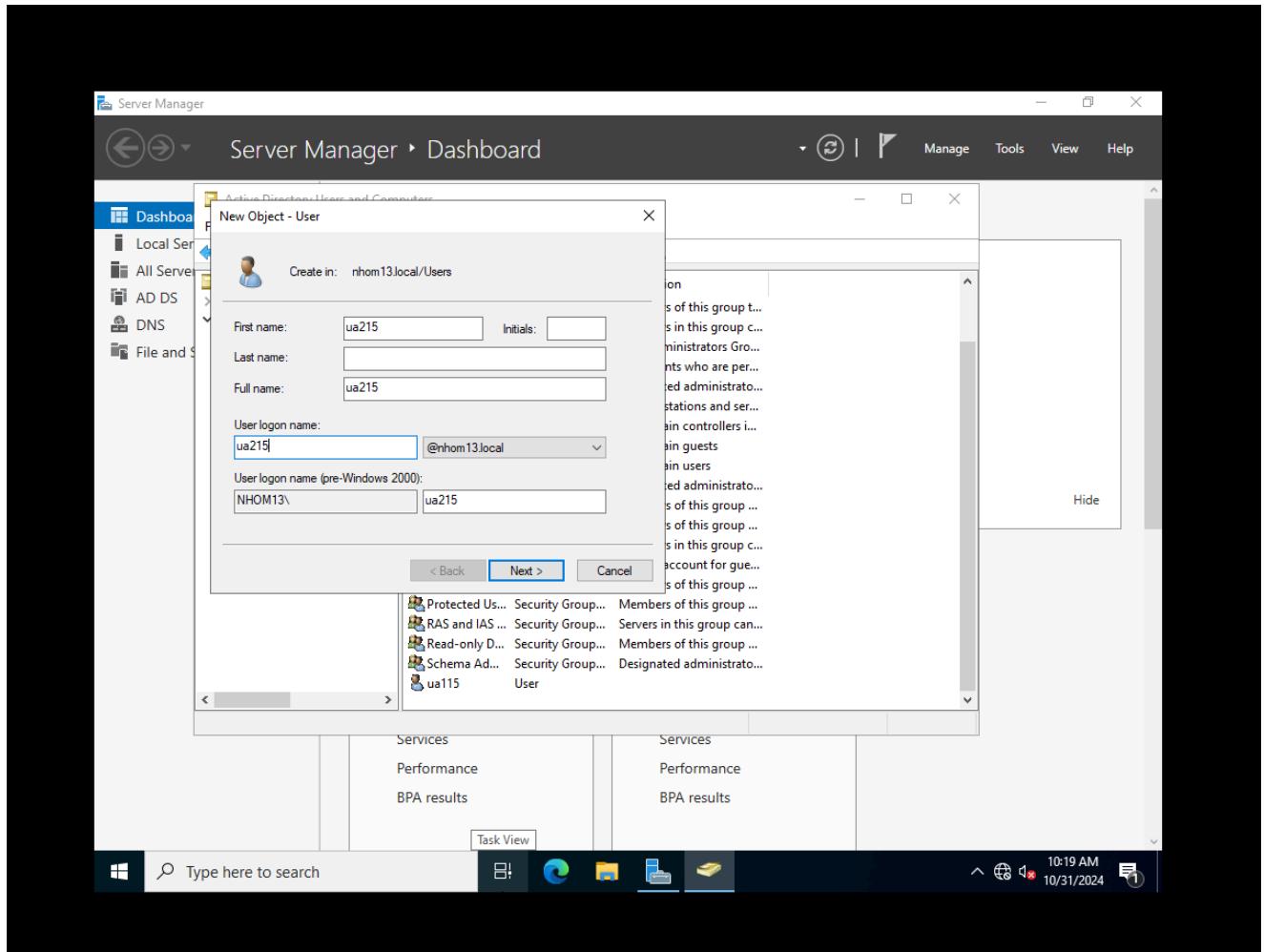
Tạo ua1X



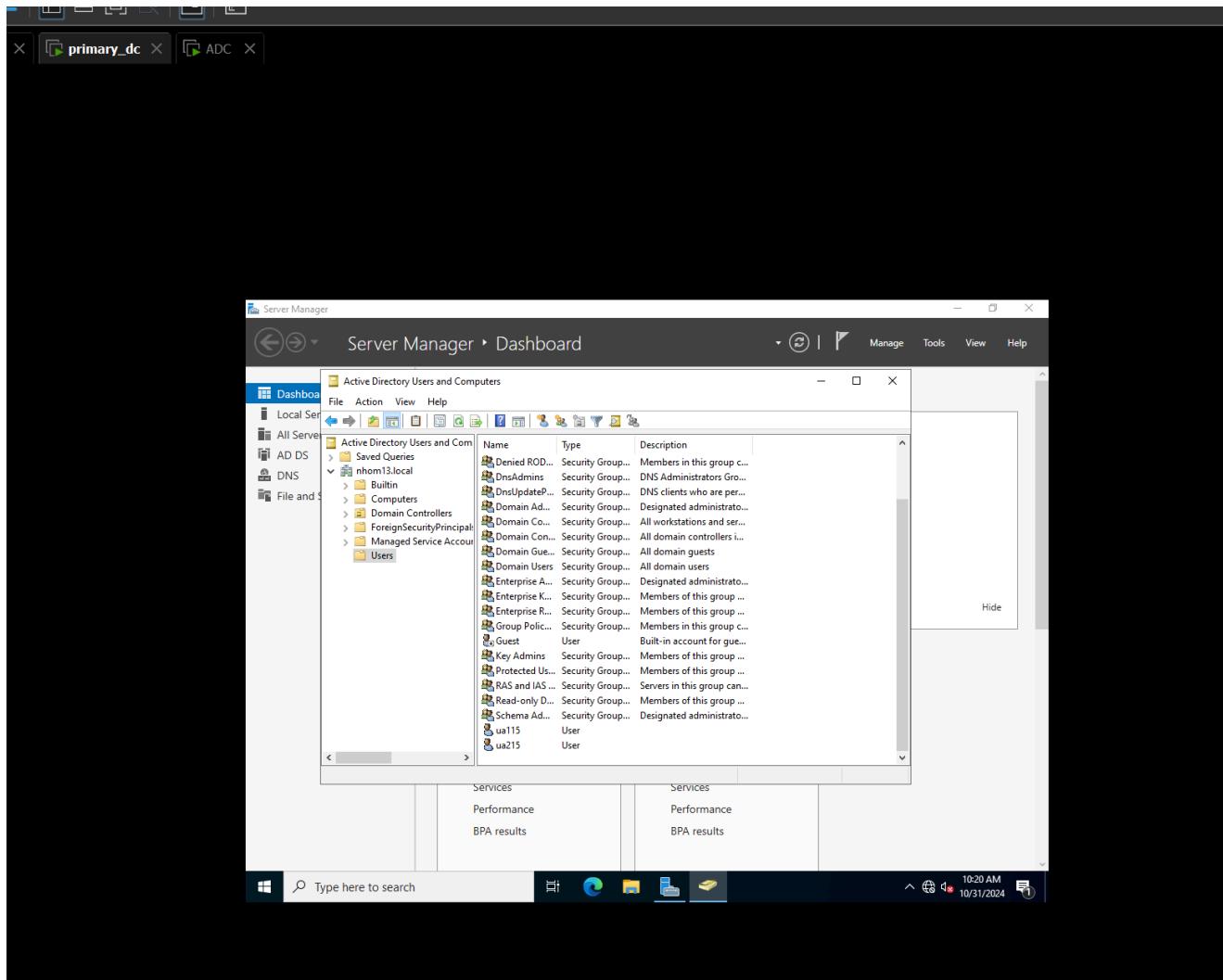
Kiểm tra trên ADC



Tạo ua2X



Kiểm tra trên primary DC

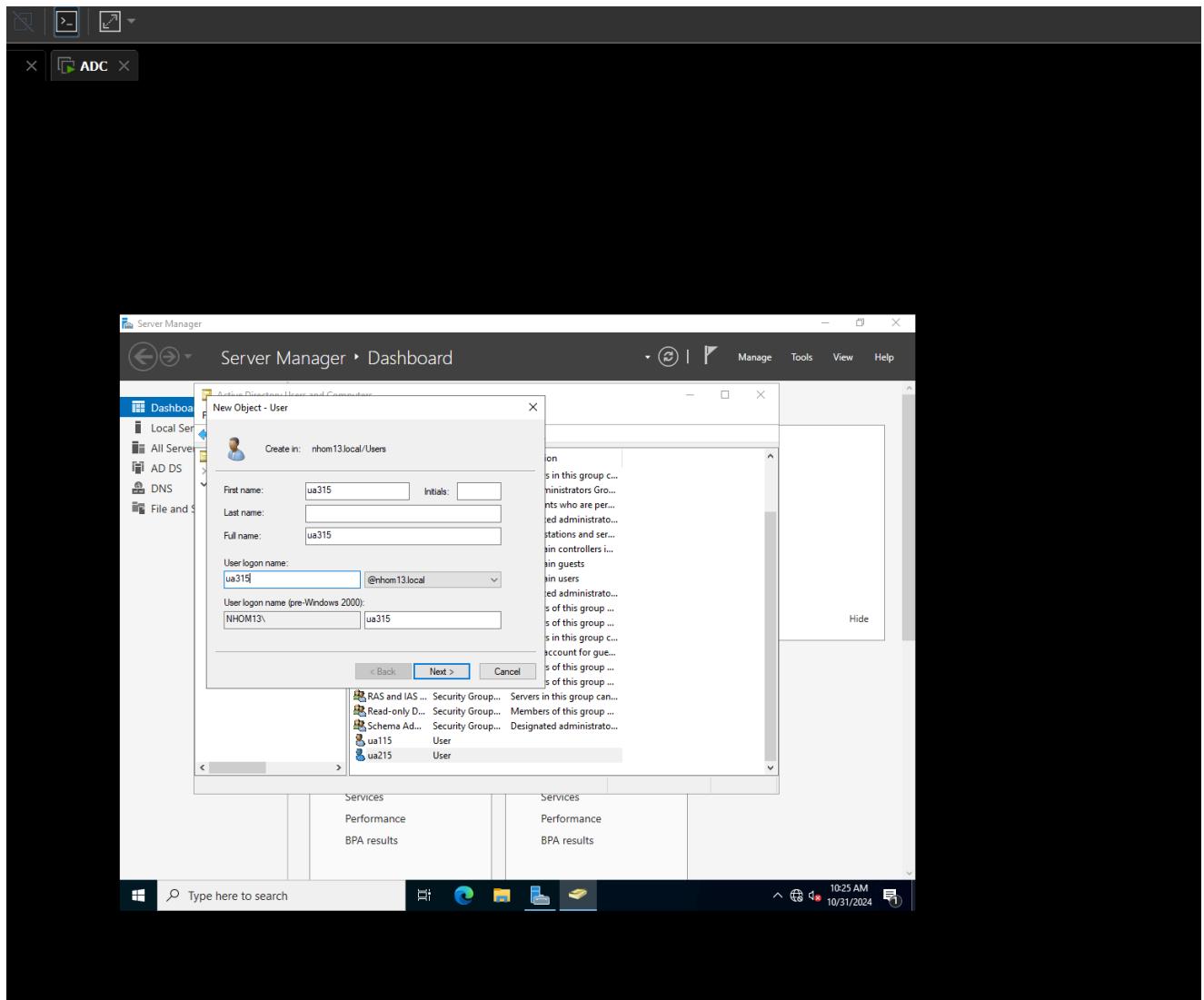


Tắt primary DC

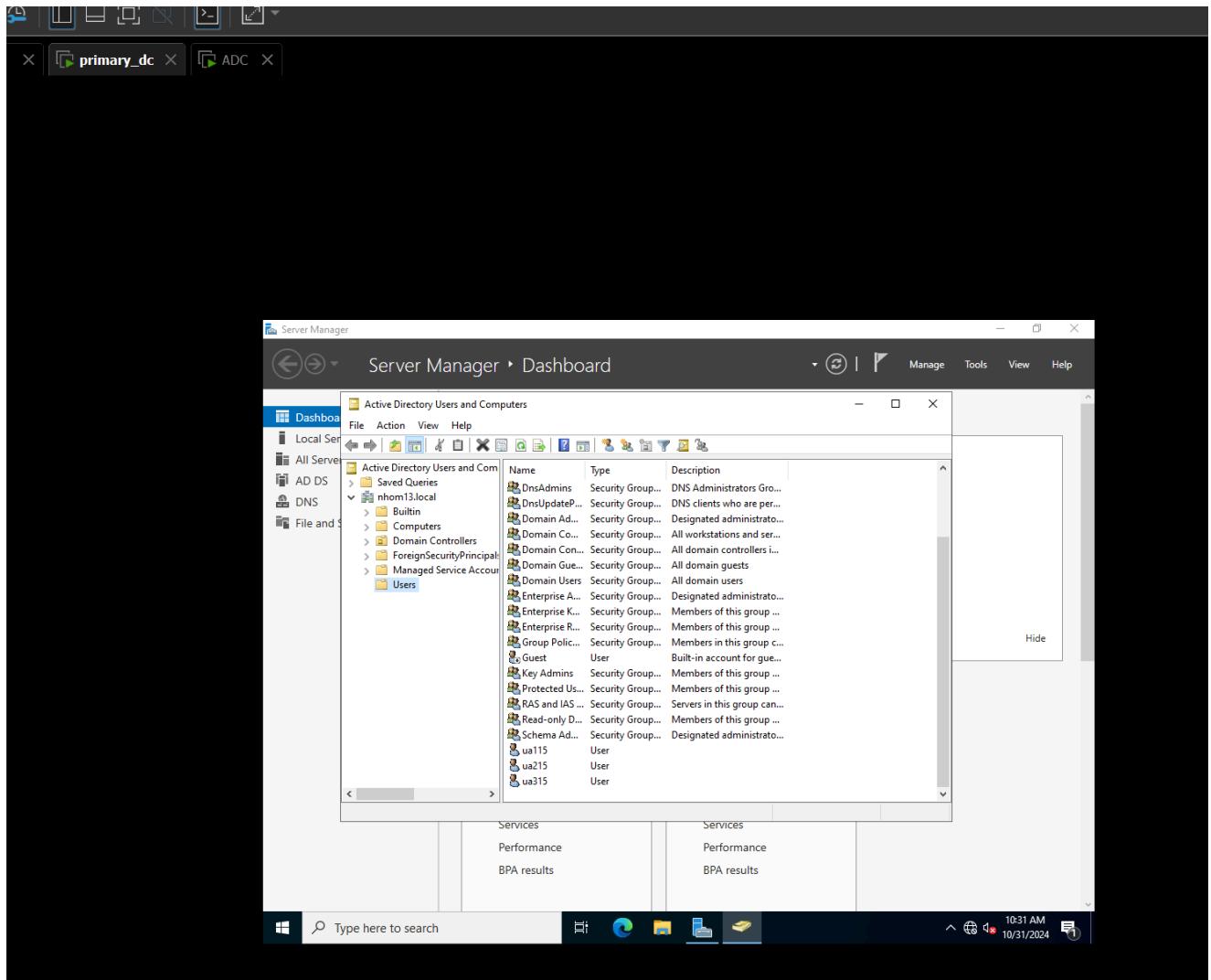
A screenshot of the Hyper-V Manager interface. The title bar says "primary_dc". The left sidebar shows "My Computer" with icons for "kuli", "winMu", "primary_dc" (which is selected), "ADC", and "RODC". The main pane displays details for the "primary_dc" VM. It has two buttons: "Power on this virtual machine" and "Edit virtual machine settings". Below that, there's a section titled "Devices" with the following specifications:

Memory	4 GB
Processors	4
Hard Disk (NVMe)	40 GB
CD/DVD (SATA)	Using file C:\User...
Floppy	Using file autoinst...
Network Adapter	NAT

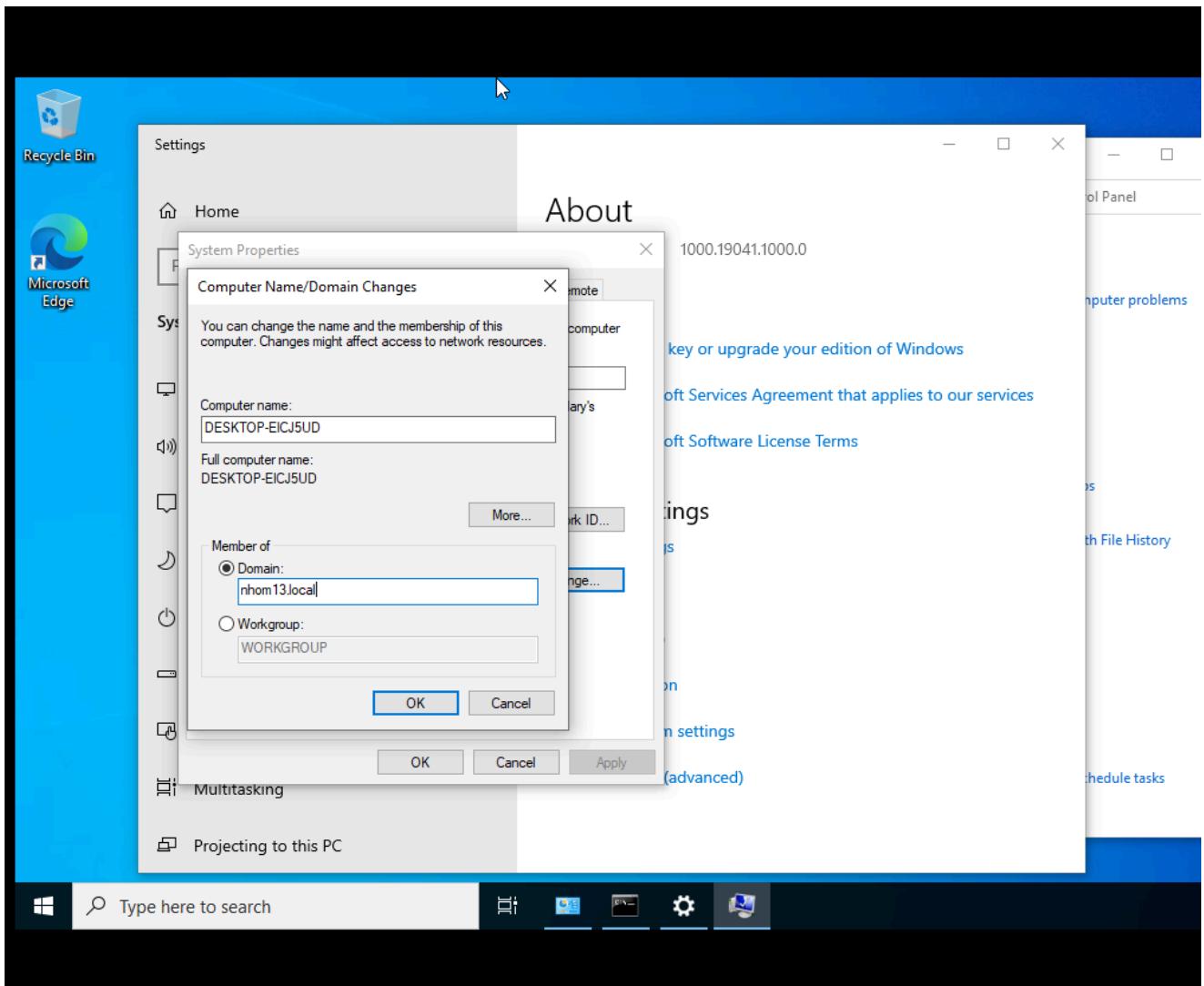
Tạo ua3X trên ADC



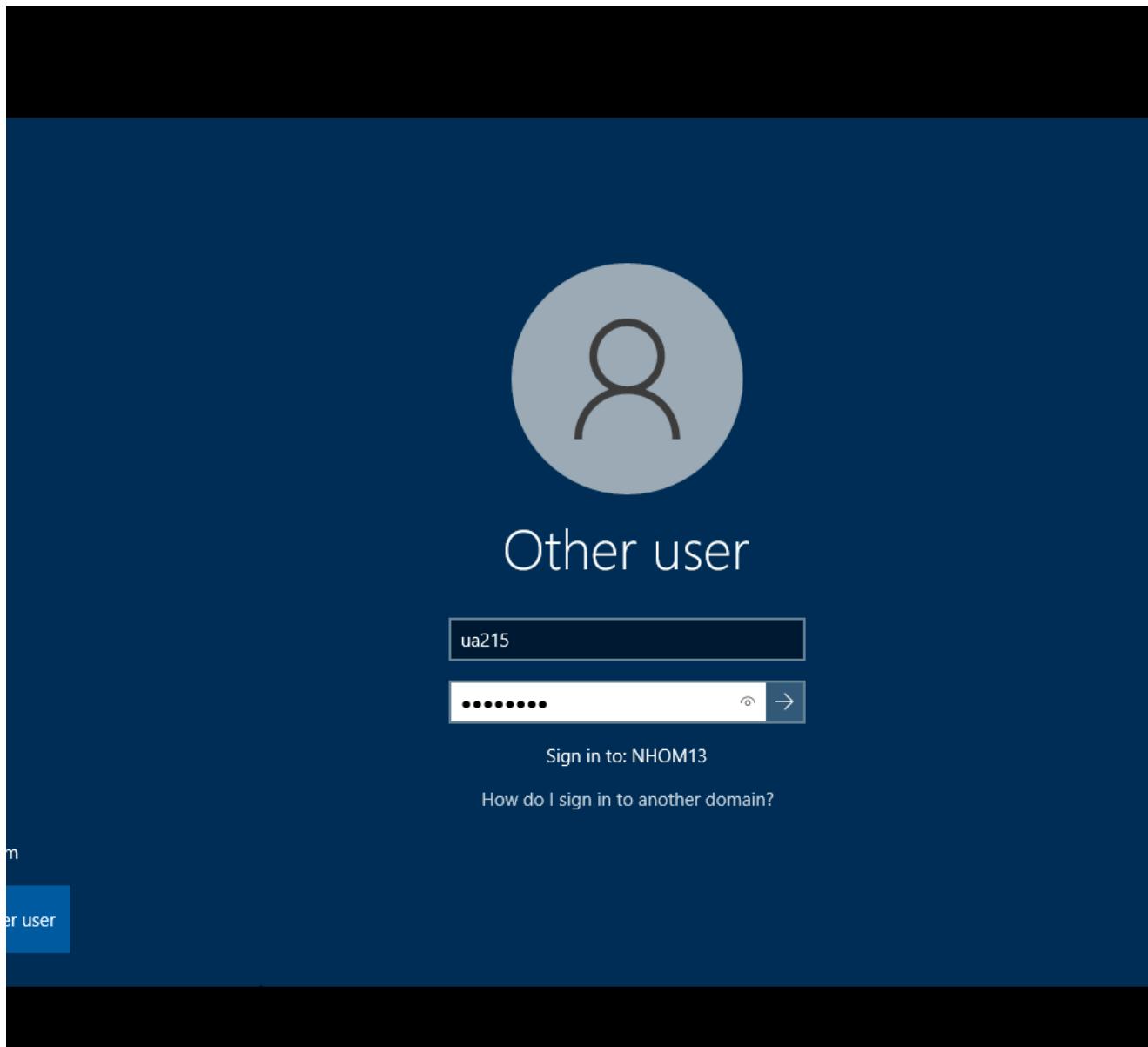
Kiểm tra trên primary DC



Thêm client vào domain



Đăng nhập client khi tắt primary DC



4. Xây dựng mô hình Read-only Domain Controller

Yêu cầu 4.1

Đề bài

Sinh viên hãy tìm hiểu và trả lời câu hỏi:

Read-Only Domain Controller (RODC) là gì?

RODC là một loại Domain Controller (DC) trong hệ thống Active Directory của Microsoft, lưu trữ bản sao của cơ sở dữ liệu Active Directory dưới dạng chỉ đọc. RODC được thiết kế để triển khai ở các văn phòng chi nhánh hoặc các môi trường không an toàn, nơi không cần tính năng ghi hoặc không muốn lưu trữ thông tin nhạy cảm.

Mô hình RODC hoạt động như thế nào?

RODC chỉ lưu trữ bản sao cơ sở dữ liệu của Active Directory dưới dạng chỉ đọc. Khi nhận yêu cầu từ người dùng, RODC có thể cung cấp thông tin về tài khoản, nhóm và các đối tượng khác từ cơ sở dữ liệu mà không cho phép cập nhật trực tiếp. Nếu có yêu cầu thay đổi hoặc

chỉnh sửa, RODC sẽ chuyển tiếp yêu cầu này đến một Domain Controller có quyền ghi (writable DC) để xử lý. RODC cũng hỗ trợ việc lưu trữ thông tin xác thực của một số tài khoản cụ thể (credential caching), nhưng mặc định không lưu trữ thông tin mật khẩu của tất cả tài khoản trong mạng để giảm nguy cơ lọt dữ liệu.

Khi nào cần sử dụng RODC?

Khi triển khai tại các văn phòng từ xa, nơi không có đội ngũ IT chuyên trách.

Để giảm thiểu rủi ro về bảo mật nếu một Domain Controller bị xâm nhập hoặc mất cắp tại các địa điểm không an toàn.

Khi muốn giảm thiểu tải mạng do yêu cầu từ văn phòng chi nhánh về trung tâm dữ liệu.

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

Khả năng cập nhật: ADC có khả năng đọc và ghi dữ liệu, cho phép thực hiện các cập nhật trực tiếp vào Active Directory, trong khi RODC chỉ có khả năng đọc dữ liệu và chuyển tiếp các yêu cầu ghi đến một DC khác.

Bảo mật: RODC bảo mật hơn khi triển khai ở các địa điểm không an toàn vì không lưu trữ toàn bộ thông tin mật khẩu và các cập nhật có thể bị hạn chế.

Quản lý: RODC yêu cầu ít quyền hơn ADC và thường dễ quản lý tại các chi nhánh hoặc địa điểm từ xa vì không cần phải quản lý toàn bộ cơ sở dữ liệu hoặc hỗ trợ các tính năng ghi.

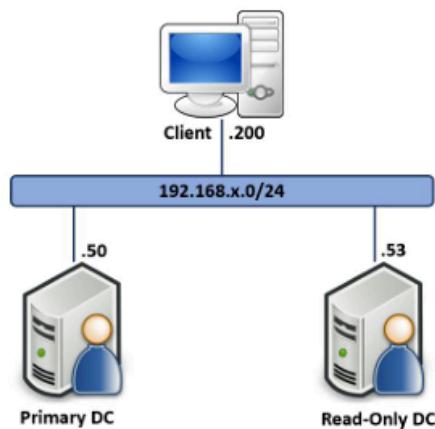
Khả năng phục hồi: ADC là một DC đầy đủ nên có khả năng phục hồi tốt hơn, trong khi RODC chỉ là một bản sao và cần có kết nối với DC chính để xử lý các yêu cầu ghi.

Yêu cầu 4.2

Đề bài

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

Mô hình cần xây dựng:



Thông tin các máy

Lab 4: Triển khai Active Directory trên Windows Server

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

Các bước thực hiện

Thay đổi ip trên Primary DC

```
localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-EC-33-6C
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::557:4d0:5d3d:a545%6(PREFERRED)
IPv4 Address. . . . . : 192.168.15.50(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, November 6, 2024 1:30:46 PM
Lease Expires . . . . . : Wednesday, November 6, 2024 3:03:48 PM
Default Gateway . . . . . : 192.168.15.2
DHCP Server . . . . . : 192.168.15.254
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-B4-EB-04-00-0C-29-EC-33-6C
DNS Servers . . . . . : ::1
                           192.168.15.50
                           192.168.15.53
Primary WINS Server . . . . . : 192.168.15.2
NetBIOS over Tcpip. . . . . : Enabled
```

Thay đổi ip trên client

```
localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-9C-DD-53
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::9b97:4f4b:9d17:1735%14(PREFERRED)
IPv4 Address. . . . . : 192.168.15.200(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, November 6, 2024 1:29:56 PM
Lease Expires . . . . . : Wednesday, November 6, 2024 3:06:35 PM
Default Gateway . . . . . : 192.168.15.2
DHCP Server . . . . . : 192.168.15.254
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-85-ED-60-00-0C-29-9C-DD-53
DNS Servers . . . . . : 192.168.15.50
                           192.168.15.53
Primary WINS Server . . . . . : 192.168.15.2
NetBIOS over Tcpip. . . . . : Enabled
```

Thay đổi ip trên RODC

```
localdomain

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . : localdomain
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-0C-29-4D-E2-57
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6927:592b:137f:5d98%5(PREFERRED)
IPv4 Address. . . . . : 192.168.15.53(PREFERRED)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Tuesday, November 5, 2024 10:45:44 PM
Lease Expires . . . . . : Wednesday, November 6, 2024 12:03:16 AM
Default Gateway . . . . . : 192.168.15.2
DHCP Server . . . . . : 192.168.15.254
DHCPv6 IAID . . . . . : 100666409
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-BD-9B-6A-00-0C-29-4D-E2-57
DNS Servers . . . . . : 192.168.15.50
                           192.168.15.53
Primary WINS Server . . . . . : 192.168.15.2
NetBIOS over Tcpip. . . . . : Enabled
```

Cài đặt role trên Primary DC

progress

DESTINATION SERVER
WIN-M1OGG1F4MDS

[View installation progress](#)

Feature installation

Configuration required. Installation succeeded on WIN-M1OGG1F4MDS.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

[Active Directory module for Windows PowerShell](#)

AD DS Tools

[Active Directory Administrative Center](#)

[AD DS Snap-Ins and Command-Line Tools](#)



You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

Cài đặt role trên RODC

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Domain Services

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

[Active Directory module for Windows PowerShell](#)

AD DS Tools

[Active Directory Administrative Center](#)

[AD DS Snap-Ins and Command-Line Tools](#)

[Export configuration settings](#)

[Specify an alternate source path](#)

Chỉnh thành RODC

Controller Options

TARGET SERVER
WIN-OKGUU9TOEUD

Configuration Controller Options

Specify domain controller capabilities and site information

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Site name:

Default-First-Site-Name



Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

Optional Options

TARGET SERVER
WIN-OKGUU9TOEUD

Content Configuration

Controller Options

Options

Additional Options

Options

Sites Check

DN

Specify Install From Media (IFM) Options

- Install from media

Specify additional replication options

Replicate from:

primarydc.nhom13.local



Additional Options

TARGET SERVER
RODC.nhom13.local

- Deployment Configuration
- Domain Controller Options
- RODC Options
- Additional Options**
- Paths
- Review Options
- Prerequisites Check
- Installation
- Results

Specify Install From Media (IFM) Options

Install from media

Specify additional replication options

Replicate from:

primarydc.nhom13.local



Tạo ur1X trên PrimaryDC (X là số thứ tự nhóm)

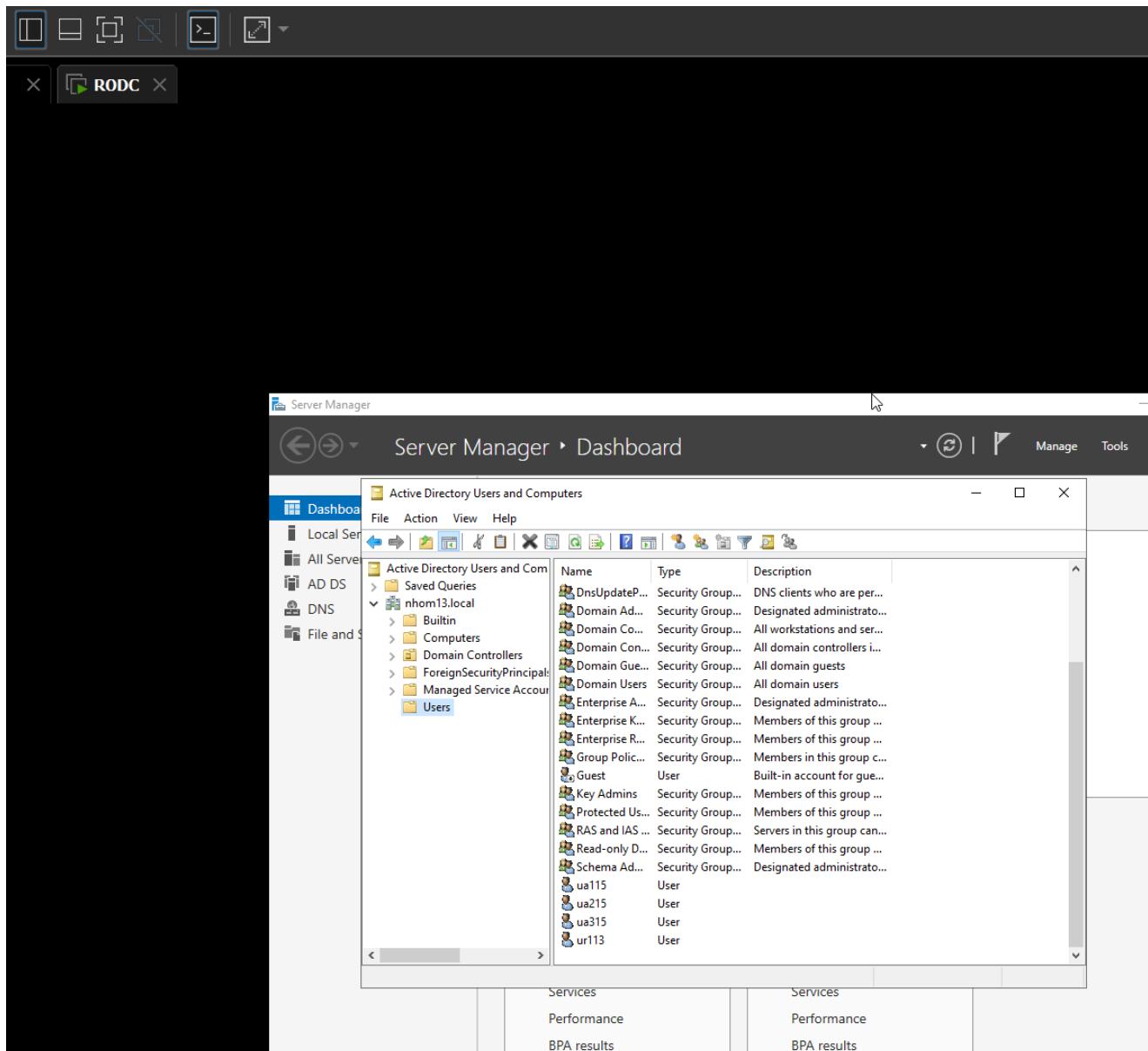
The screenshot shows the Windows Server Manager interface. On the left, the navigation pane includes 'Dashboard', 'Local Server', 'All Servers', 'AD DS', 'DNS', and 'File and S...'. The main area displays the 'New Object - User' dialog box under 'Active Directory Users and Computers'. The dialog box has the following fields:

- Create in: nhom13.local/Users
- Password: (redacted)
- Confirm password: (redacted)
- Checkboxes:
 - User must change password at next logon
 - User cannot change password
 - Password never expires
 - Account is disabled

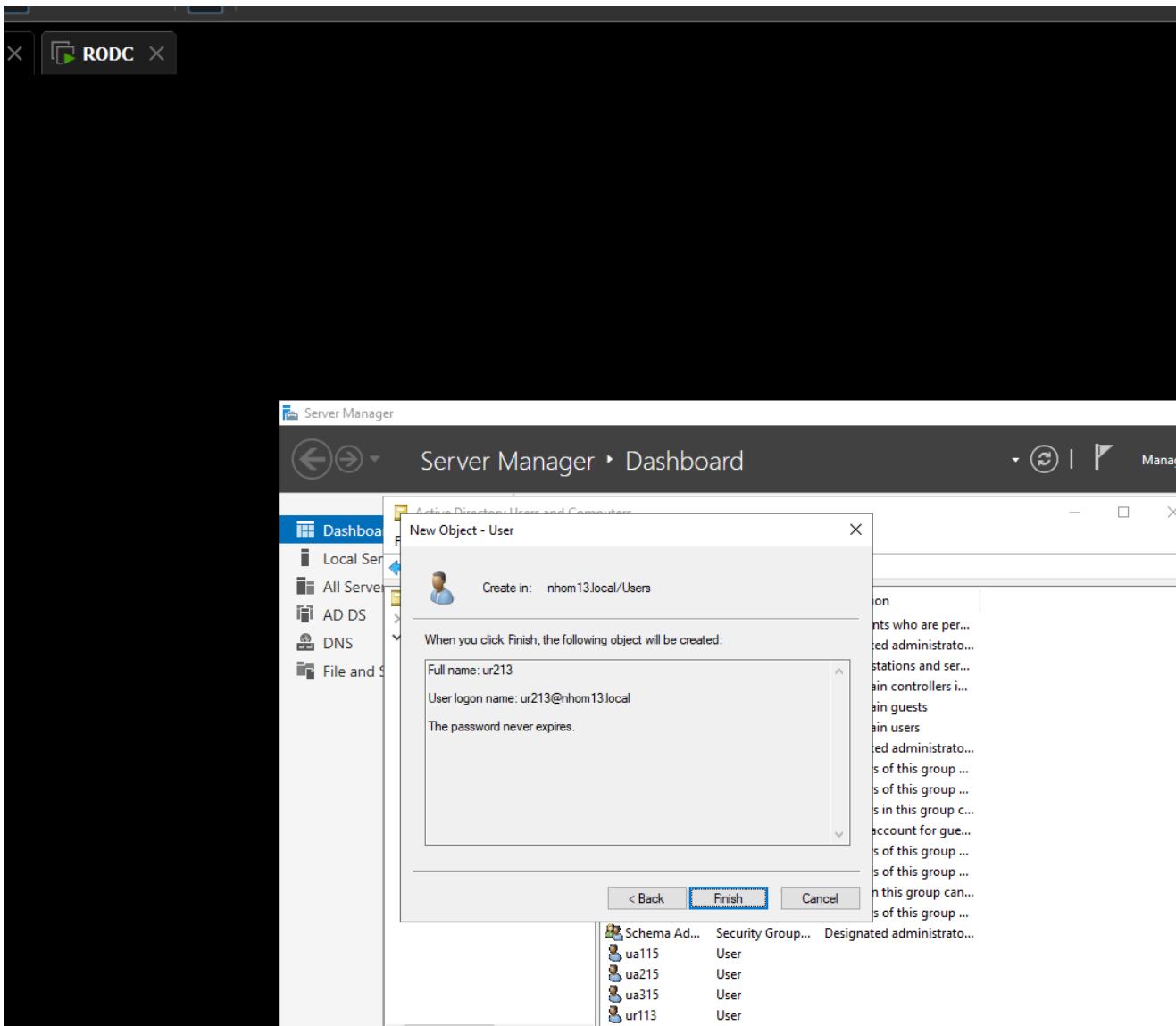
At the bottom of the dialog are buttons: '< Back', 'Next >', and 'Cancel'. Below the dialog, there is a list of objects in the Active Directory:

- Read-only D...
- Security Group...
- Members of this group ...
- Schema Ad...
- Security Group...
- Designated administrato...
- ua115
- User
- ua215
- User

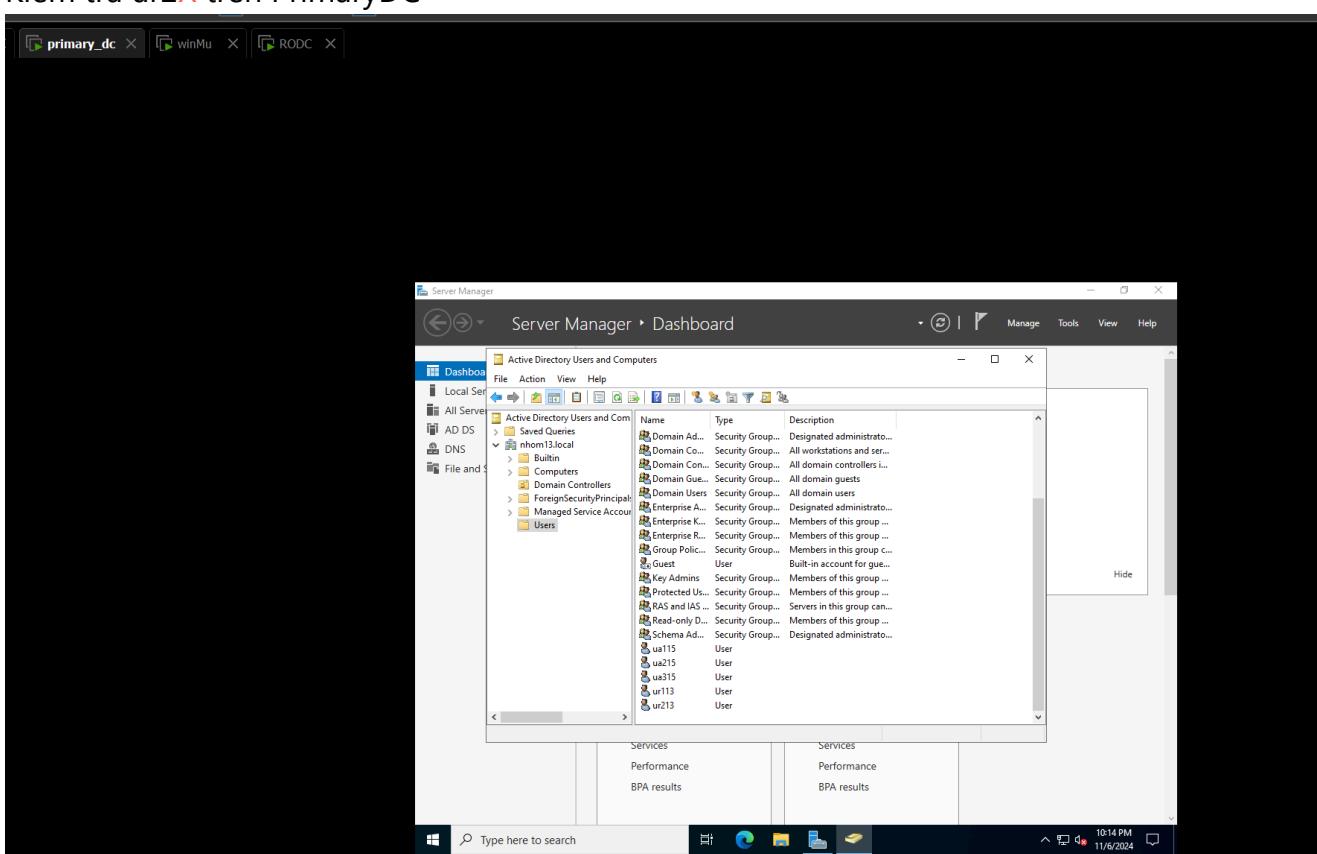
Kiểm tra ur1X trên RODC



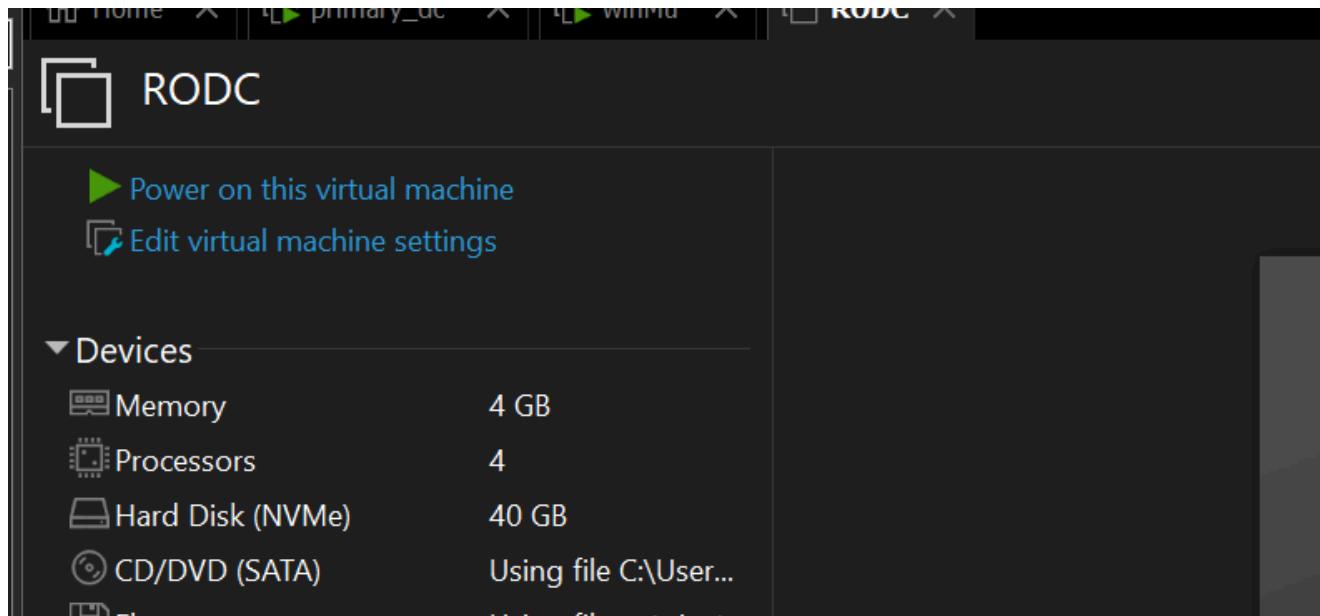
Tạo ur2X trên RODC



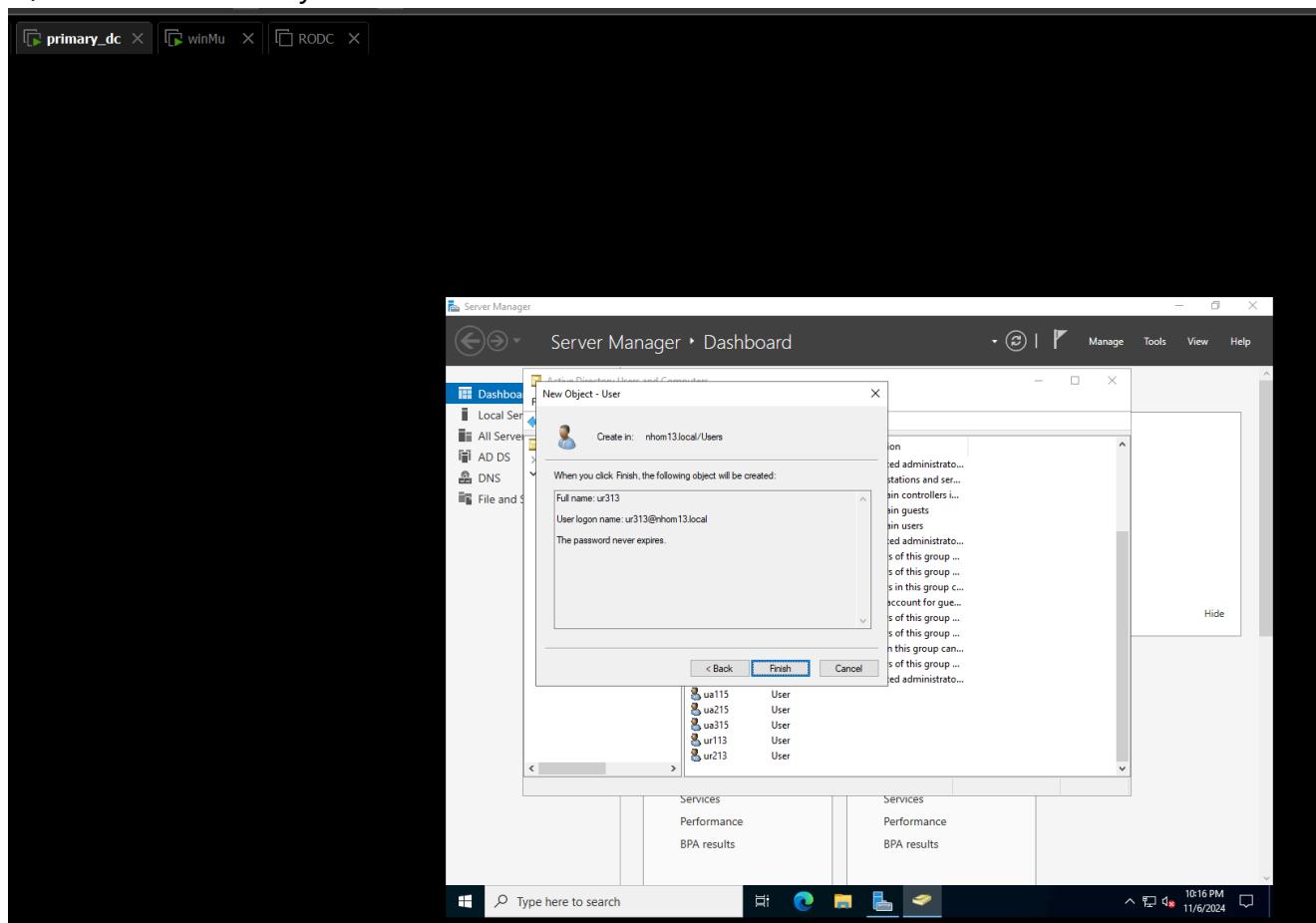
Kiểm tra ur2X trên PrimaryDC



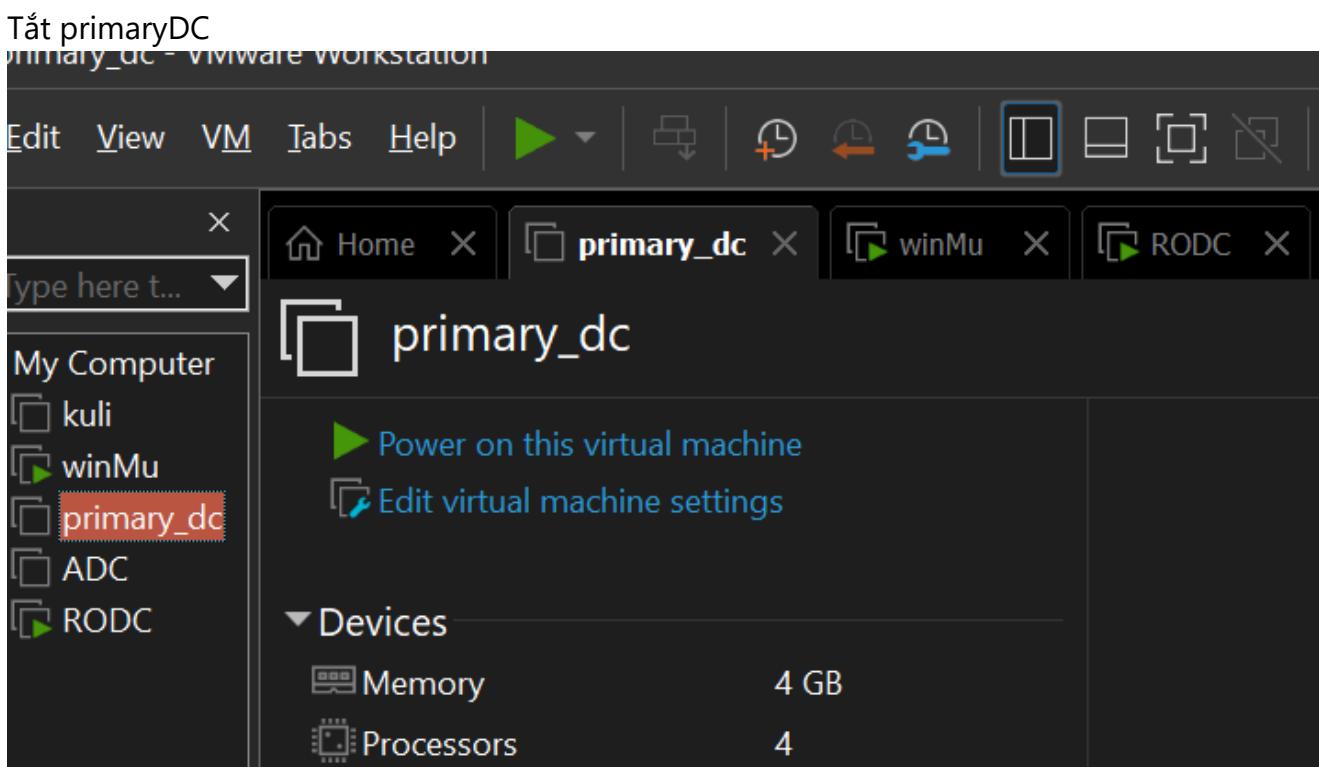
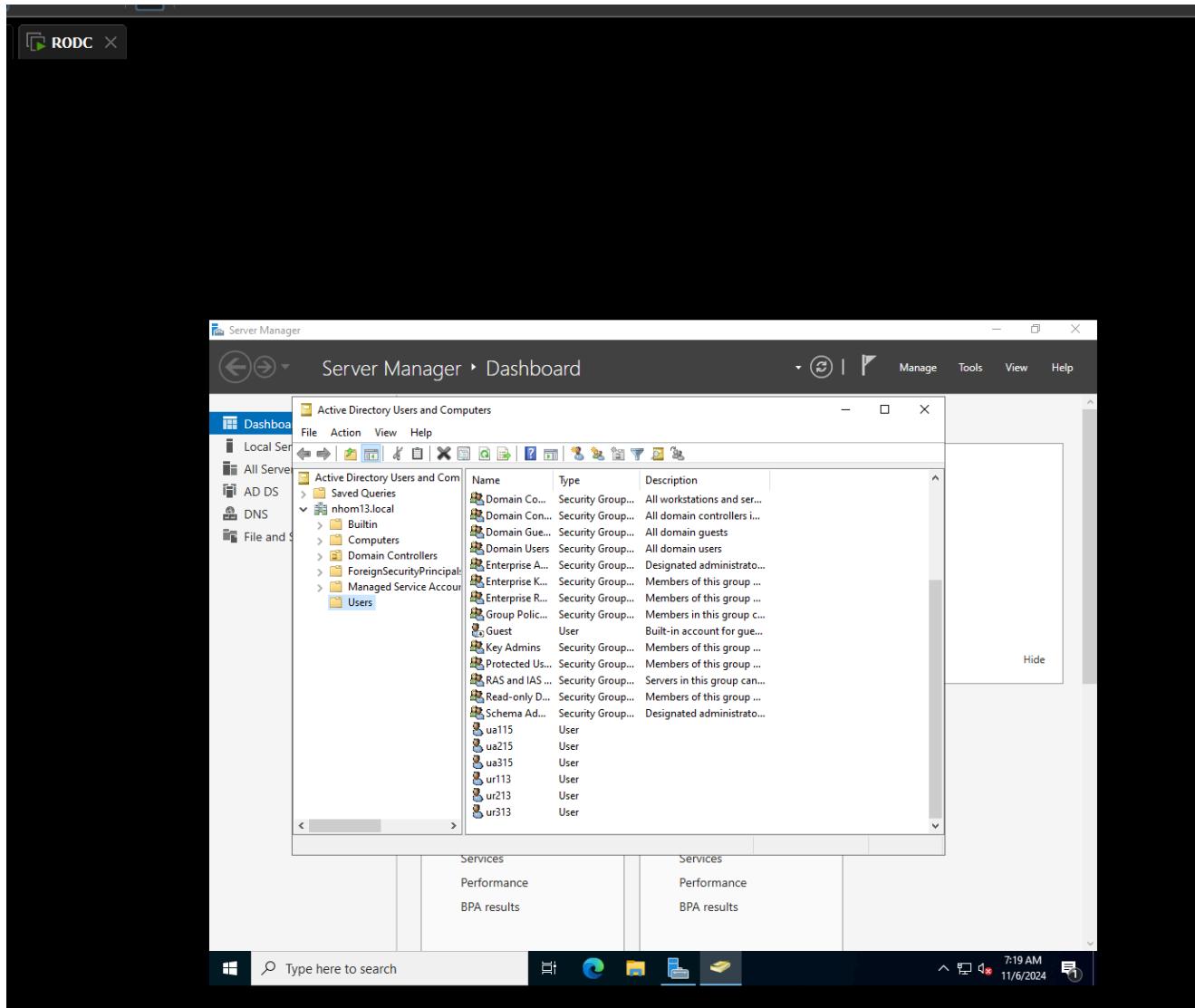
Tắt RODC



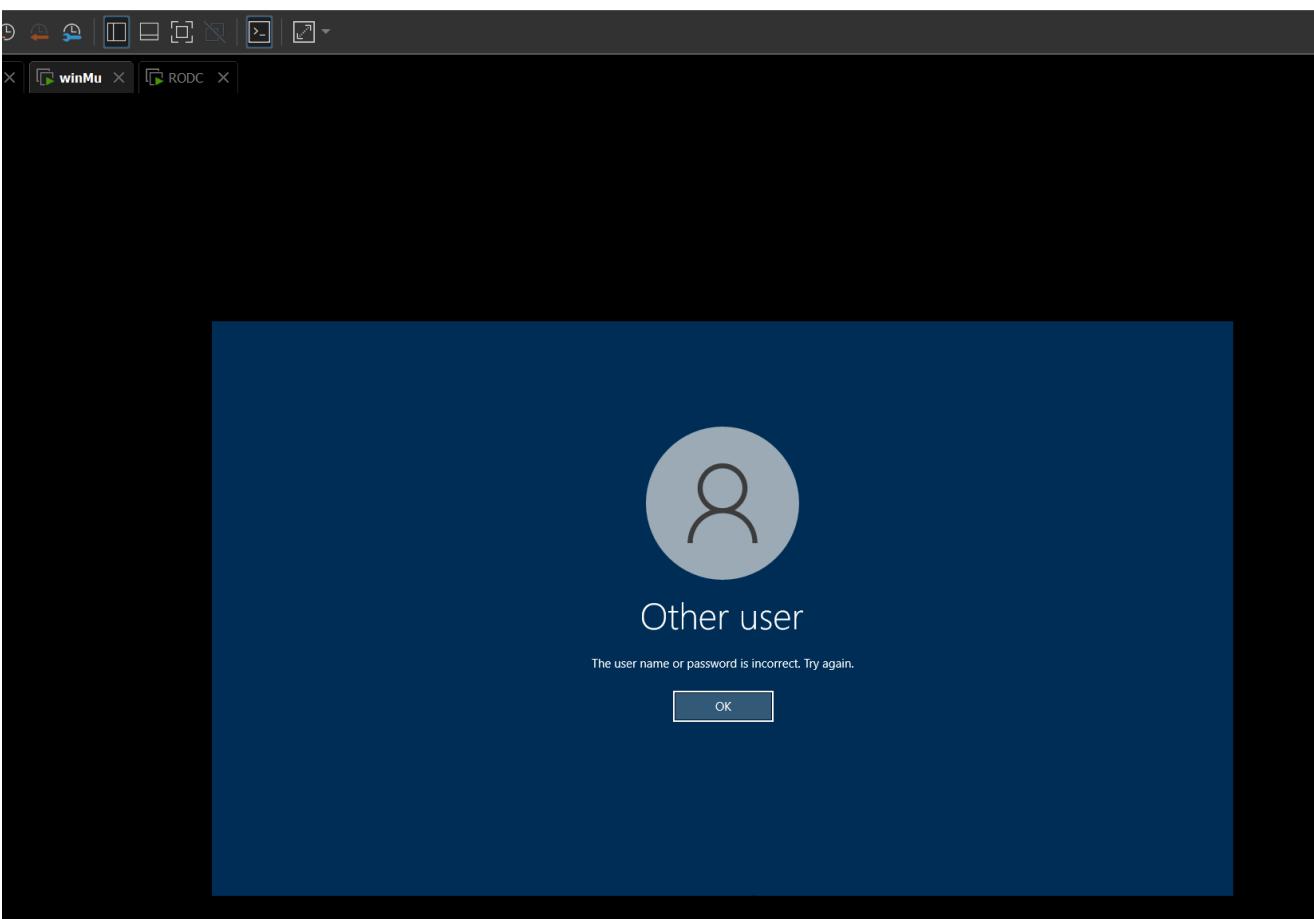
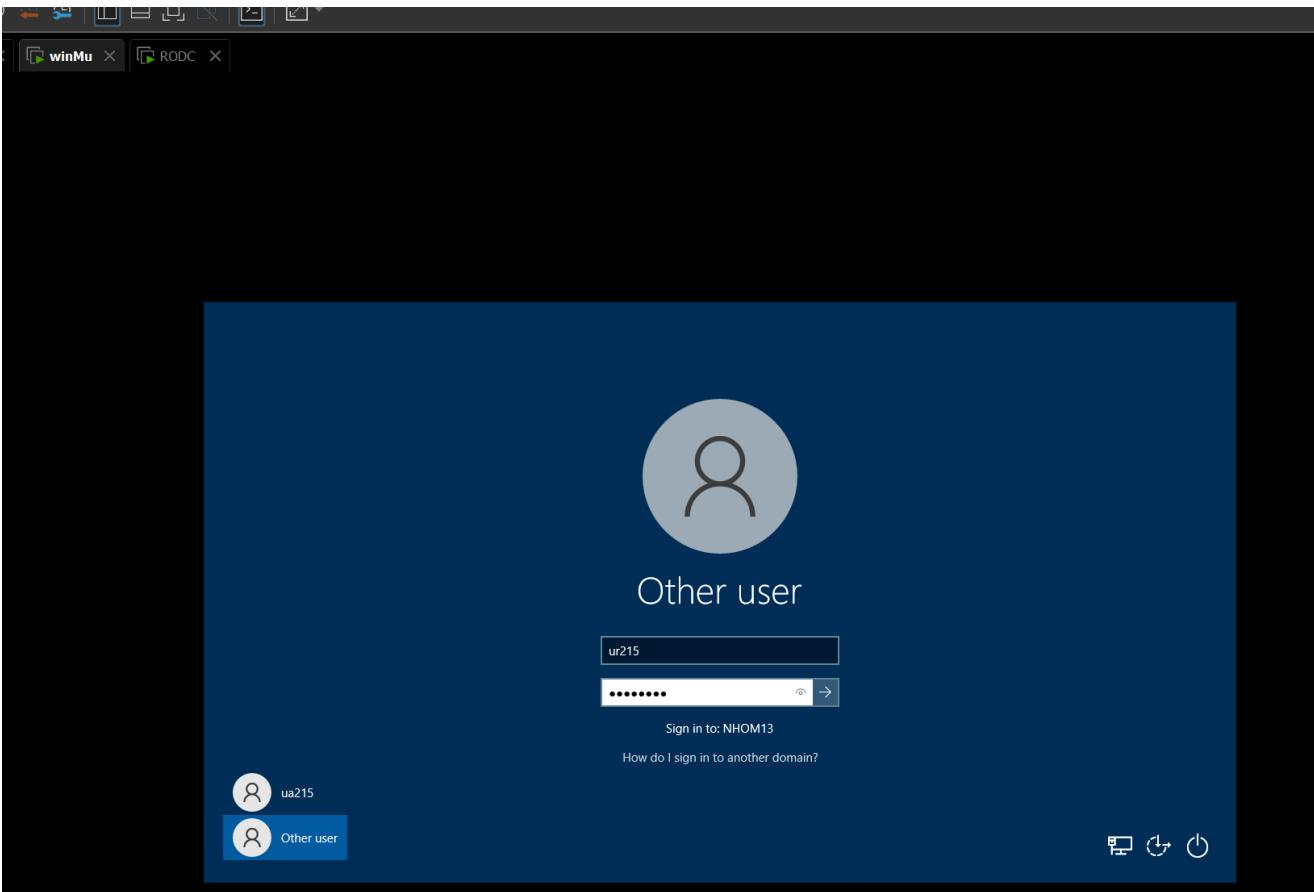
Tạo ur3X trên PrimaryDC



Kiểm tra ur3X trên RODC

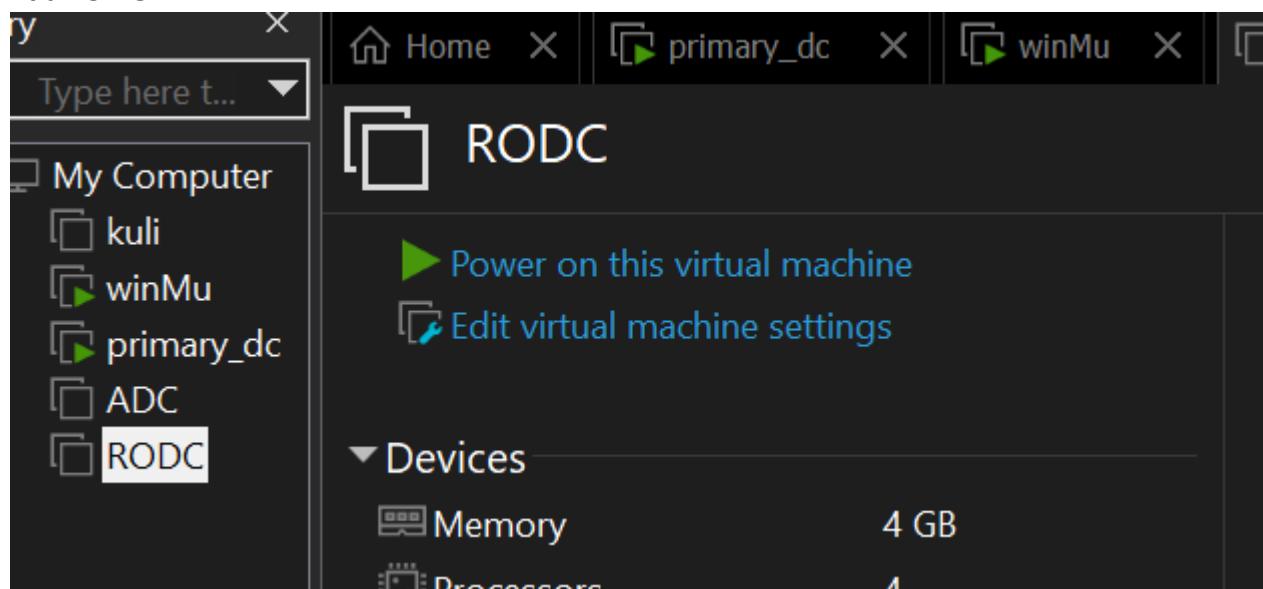


Đăng nhập ur2X trên client

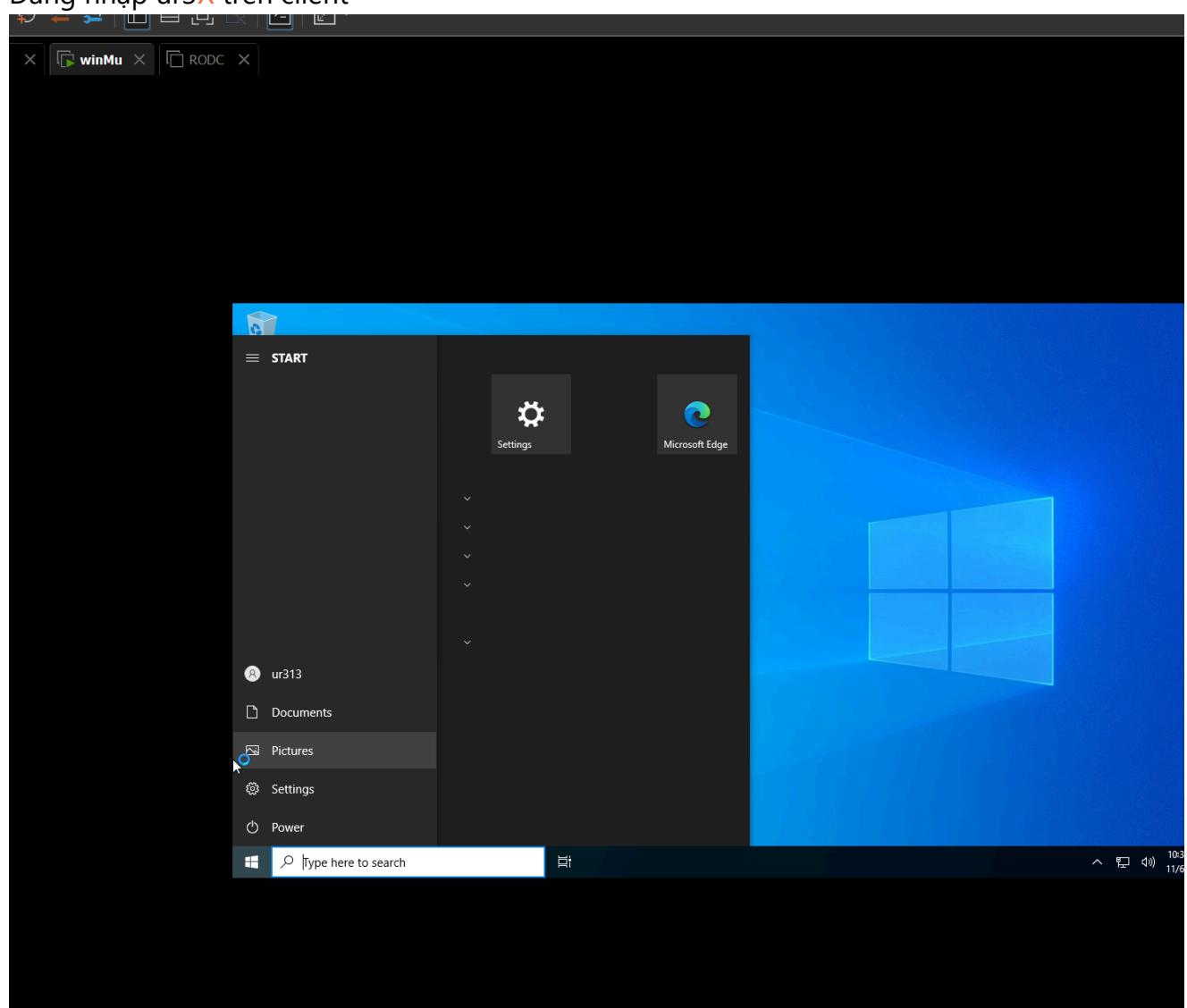


Giải thích: Vì ur2X được tạo trên RODC mà RODC chỉ có quyền đọc nên những thay đổi trên Active Directory thông qua RODC sẽ không có tác dụng

Tắt RODC



Đăng nhập ur3X trên client



Giải thích: Vì ur3X được tạo trên PrimaryDC và RODC sẽ đọc và kiểm tra trên Active Directory.