TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN – ĐHQG-HCM
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

Bài thực hành số 03: TRIỂN KHAI ACTIVE DIRECTORY TRÊN WINDOWS SERVER

Môn học: Quản trị mạng và hệ thống

Lớp: NT132.P11.ANTT.2

THÀNH VIÊN THỰC HIỆN (Nhóm 12):

STT	Họ và tên	MSSV
1	Thái Ngọc Diễm Trinh	22521541
2	Phan Nguyễn Nhật Trâm	22521501
3	Phạm Thị Cẩm Tiên	22521473
4	Nguyễn Khánh Linh	22520769

Điểm tự đánh giá
10

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	2 tuần
Phân chia công việc	
Ý kiến *(nếu có)* + Khó khăn + Đề xuất, kiến nghị	

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

MỤC LỤC

A. BÁO CÁO CHI TIẾT

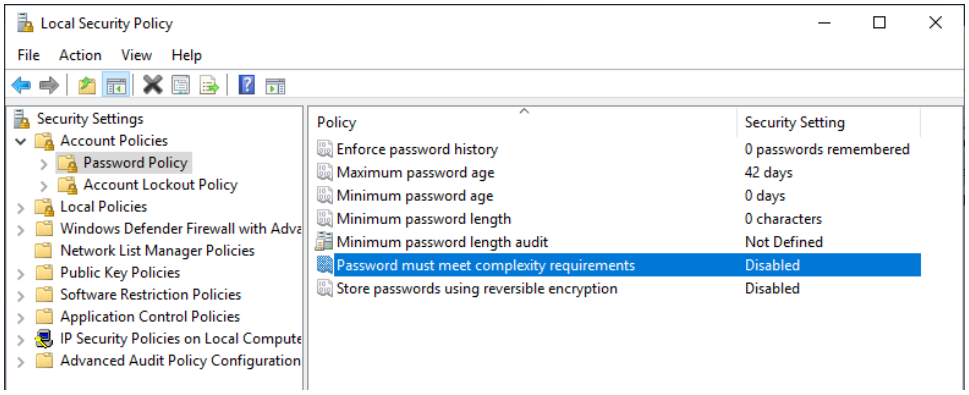
1. Xây dựng mô hình Workgroup

- Mô hình:

	IP Address	Operating System
File Server	192.168.26.14/24	Windows Server 2019
Client	192.168.26.16	Windows 10

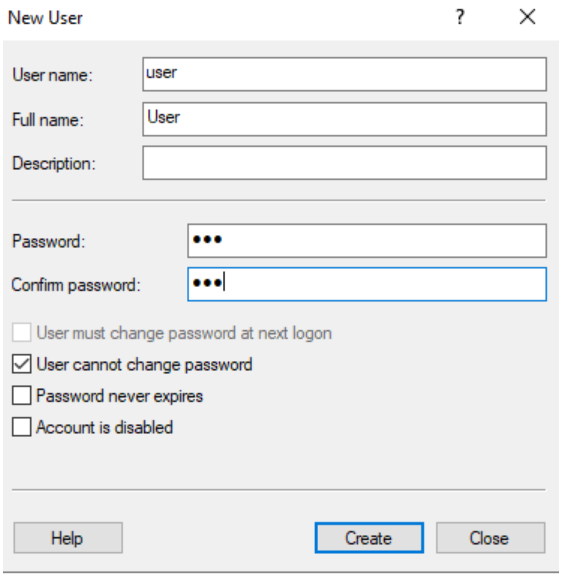
1.1. Tạo tài khoản người dùng user có mật khẩu là 123, và thiết lập không cho phép người dùng thay đổi thông tin của mình, chỉ có Administrator mới có quyền thay đổi.

- Đầu tiên, tắt chính sách password phức tạp để có thể đặt password theo mong muốn:



Hình 1. Vô hiệu hóa tính năng password must need complexity requirements

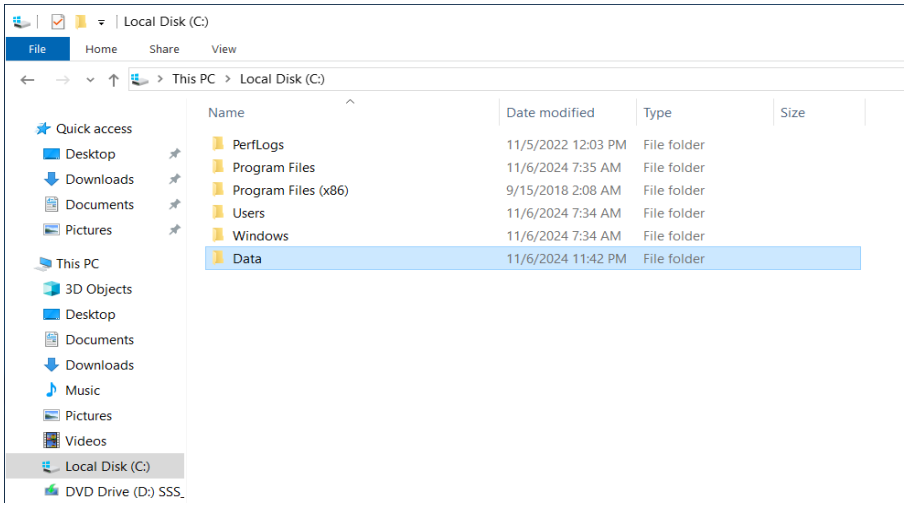
- Tạo user với các thiết lập gồm username là user và password là 123 và thiết lập không cho phép người dùng thay đổi thông tin:



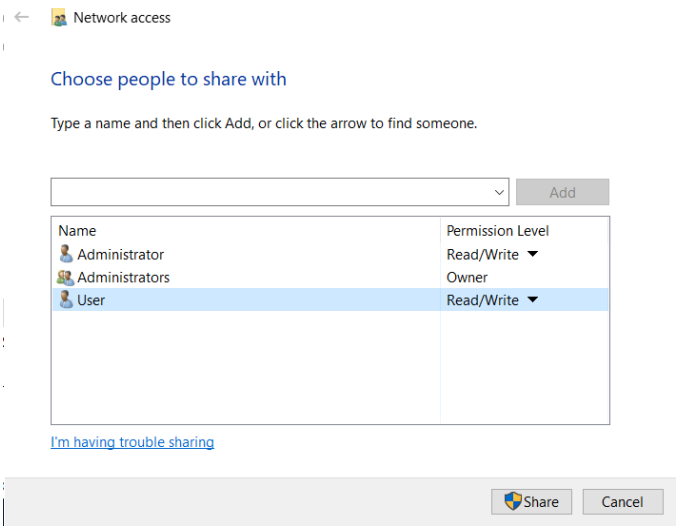
Hình 2. Tạo user

1.2. Tạo thư mục Data, cấu hình chia sẻ để có thể truy cập đến dữ liệu của thư mục này từ máy khác.

- Tạo thư mục và thiết lập chia sẻ:



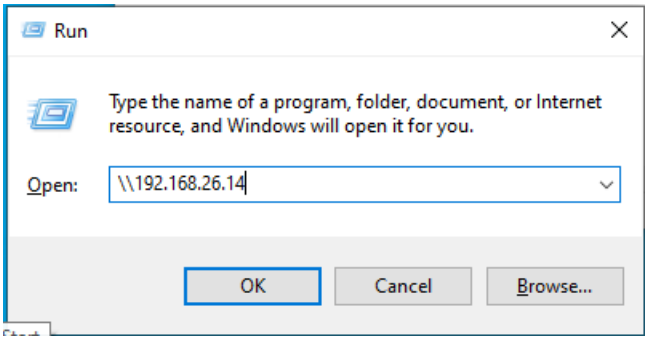
Hình 3. Tạo thư mục Data



Hình 4. Cấu hình chia sẻ cho thư mục

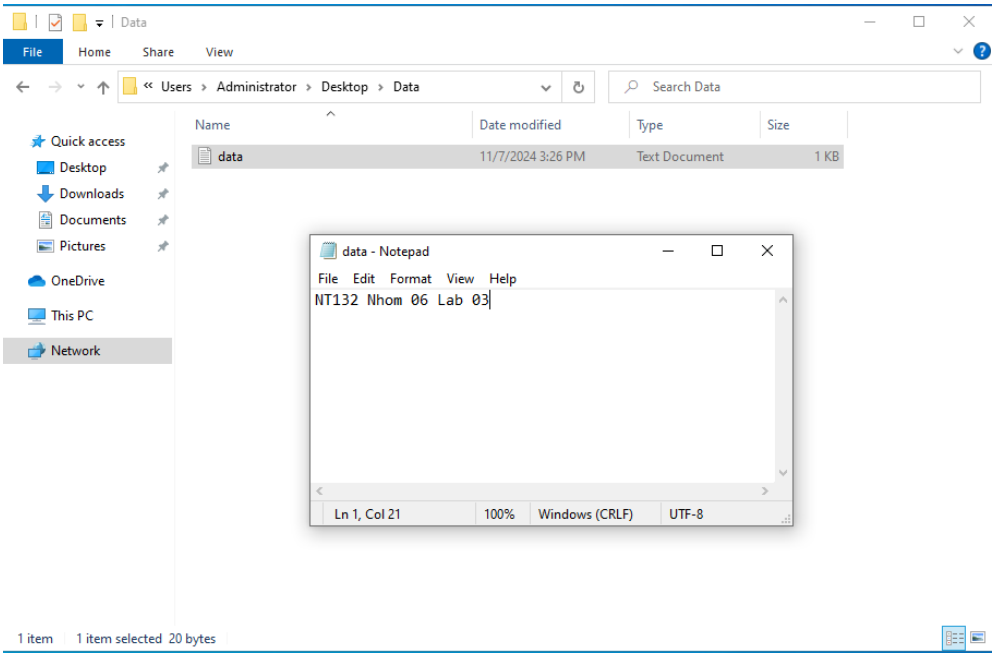
1.3. Từ máy Client, truy cập đến File Server, tạo mới File và thư mục bất kỳ trong thư mục được chia sẻ.

- Ở máy client, mở Run và chạy như dưới để kết nối với File Server

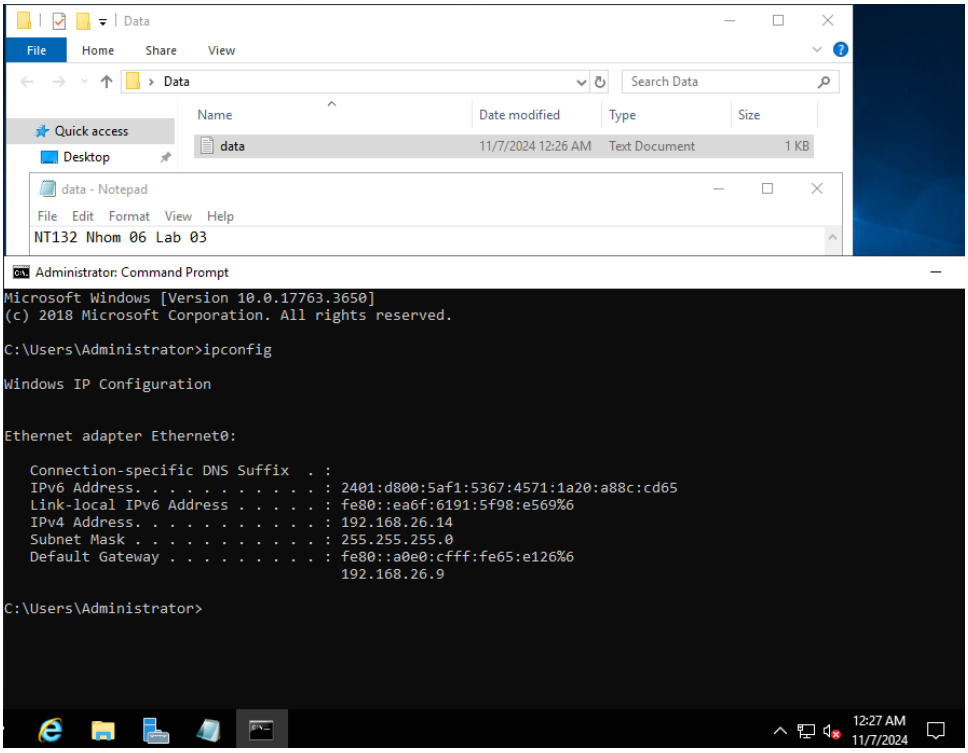


Hình 5. Client kết nối vào File Server

- Khi này có thể xem, thêm, xóa, sửa các file trong thư mục được chia sẻ



Hình 6. Client tạo file trong thư mục chia sẻ



Hình 7. File server xem file được client tạo

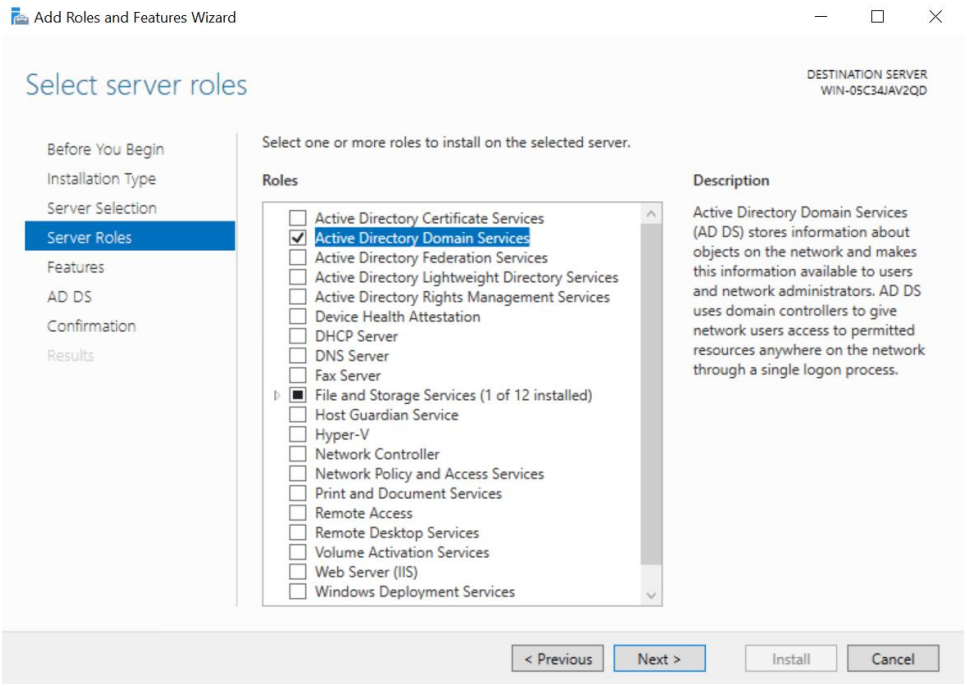
2. Triển khai Active Directory và xây dựng mô hình Domain

- Mô hình:

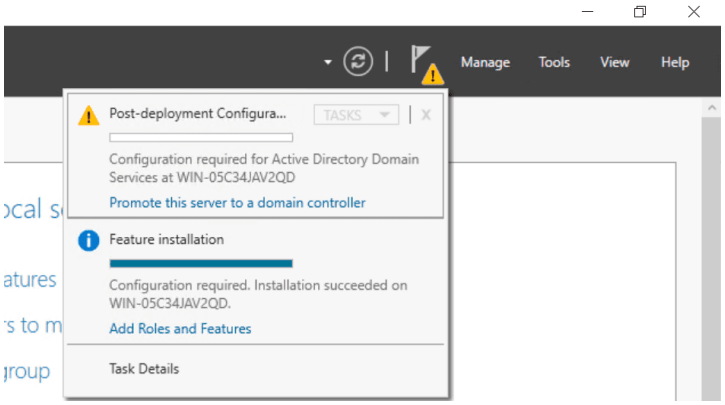
	IP Address	DNS	Operating System
Active Directory	192.168.26.169/24	192.168.26.169	Windows Server 2019
File Server	192.168.26.14/24	192.168.26.169	Windows Server 2019
Client	192.168.26.99/24	192.168.26.169	Windows

2.1. Trên máy Active Directory, thực hiện các yêu cầu sau:

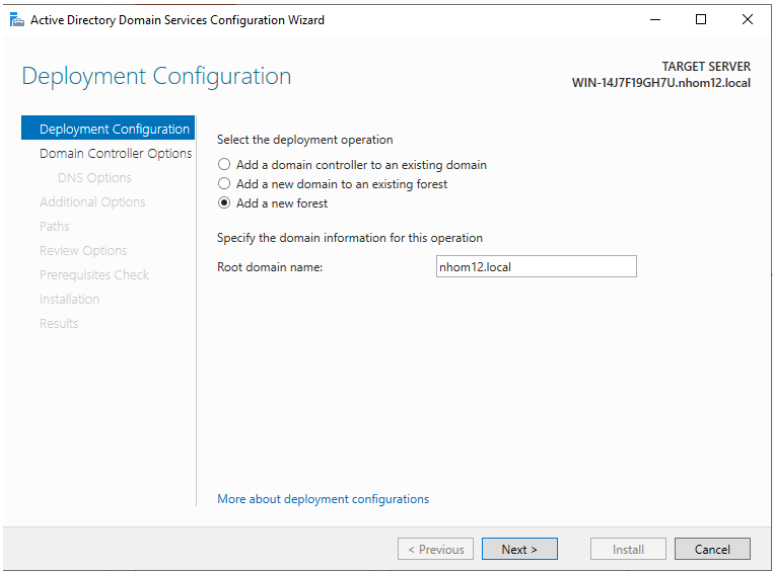
- **Đặt địa chỉ IP và các thông tin tương tự như trong bảng trên.**
- **Thiết lập Primary DNS Suffix thành nhomX.local (với X là số thứ tự của nhóm).**
- **Cài đặt dịch vụ Active Directory Domain Service.**
- **Nâng cấp máy chủ Active Directory thành Domain Controller**.
  - Mở hộp Run, chạy lệnh ***sysdm.cpl***, chọn ***Change***, thiết lập ***Primary DNS Suffix*** thành ***nhom12.local***
  - Cài đặt dịch vụ Active Directory Domain Service.
    - Ở Dashboard, chọn ***Add roles and features***
    - Chọn Next ở các phần, ở Server Roles tick chọn ***Active Directory Domain Services*** và tiếp tục chọn Next ở các trang sau. Cuối cùng chọn Install



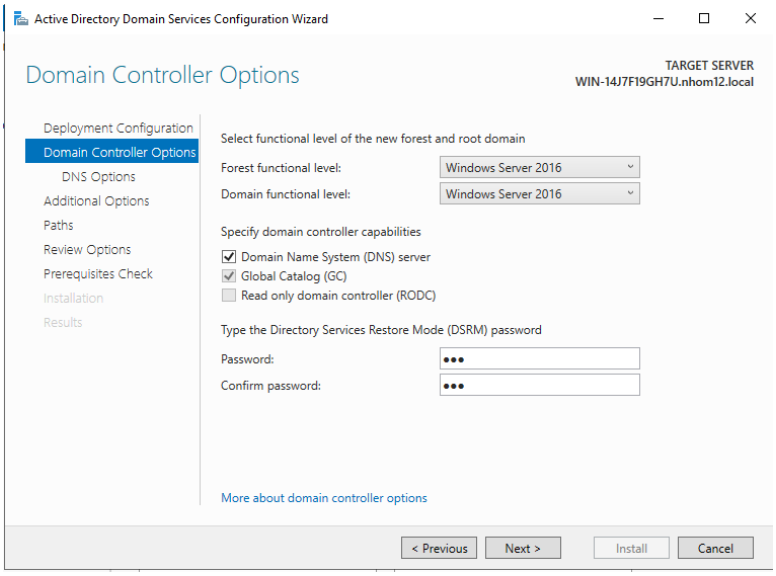
- Nâng cấp máy chủ Active Directory thành Domain Controller.
  - Ở hình lá cờ, chọn ***Promote this server to a domain controller***



  - Ở Deployment Configuration, chọn ***Add a new forest***, điền tên domain là ***nhom12.local***



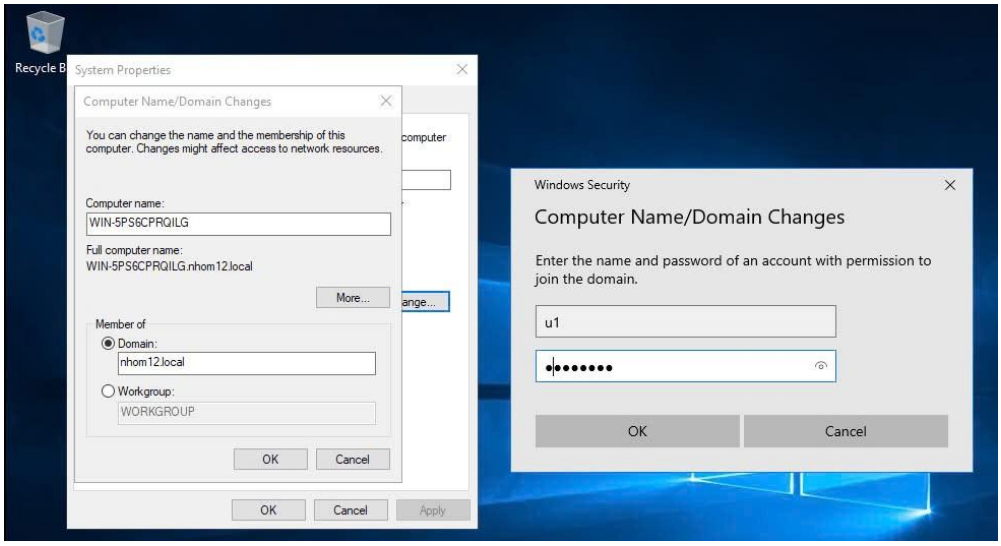
  - Ở Domain Controller Option, đặt 1 password



  - Các phần khác chọn Next và cuối cùng là Install.

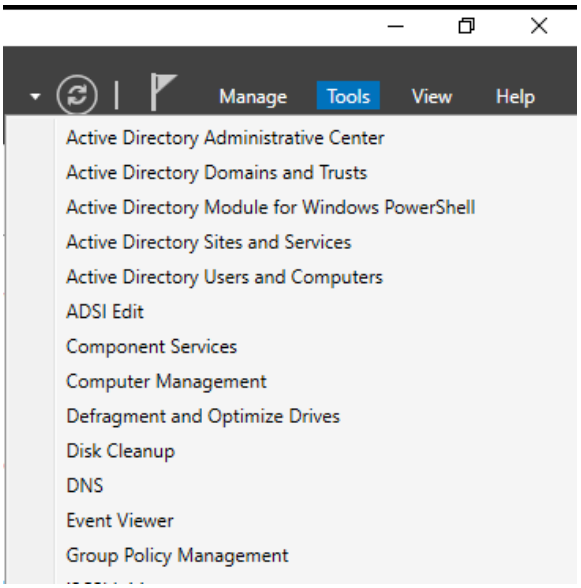
2.2. Thiết lập để máy chủ File (File Server) và Client tham gia vào Domain

- Mở hộp Run, chạy lệnh ***sysdm.cpl***, chọn Change, thiết lập Domain là ***nhom12.local***

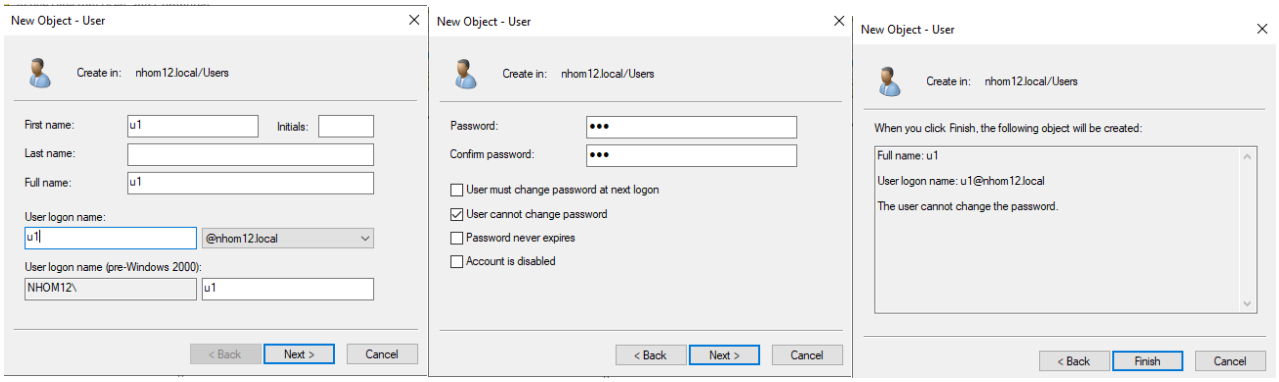


2.3. Sử dụng công cụ "Active Directory User and Computer" để tạo tài khoản u1/123 trên Active Directory

- Ở Tools, chọn ***Active Directory User and Computer***

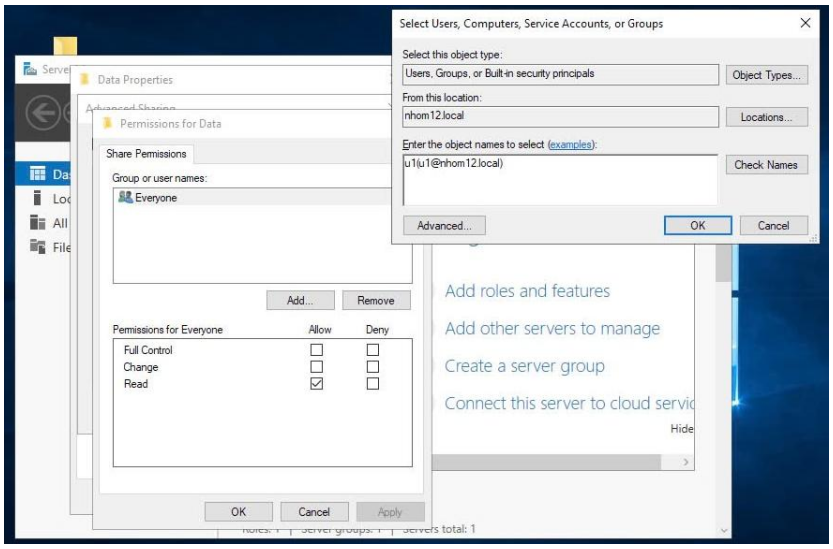


- Chọn User, New ⇨ User, thiết lập một số thông tin cho user cần tạo

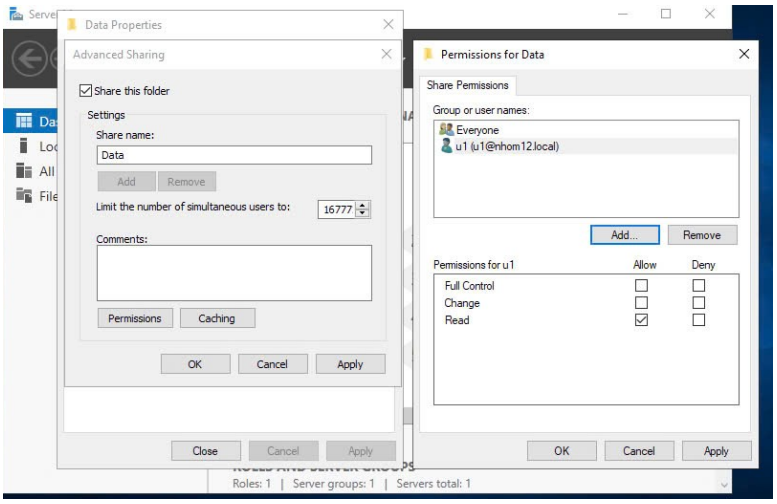


2.4. Trên File Server, phân quyền thư mục Data cho User u1/123 (tài khoản này lưu trữ trên Active Directory) quyền đọc và ghi.

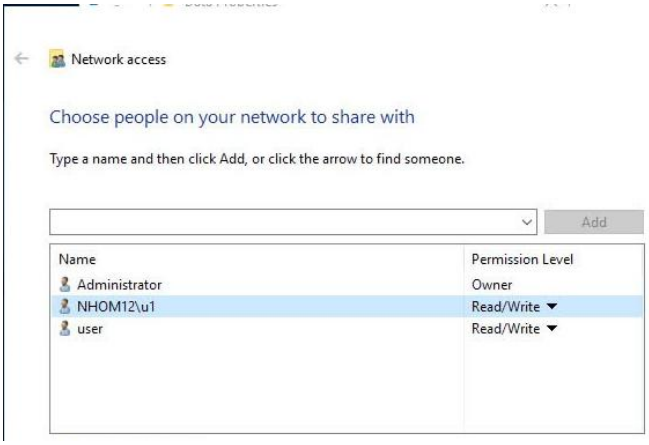
- Trong Properties của thư mục chia sẻ, chọn ***Advanced Sharing***, chọn Permission, chọn Add, sau đó thêm tên user cần chia sẻ vào



- Kết quả sau khi thêm

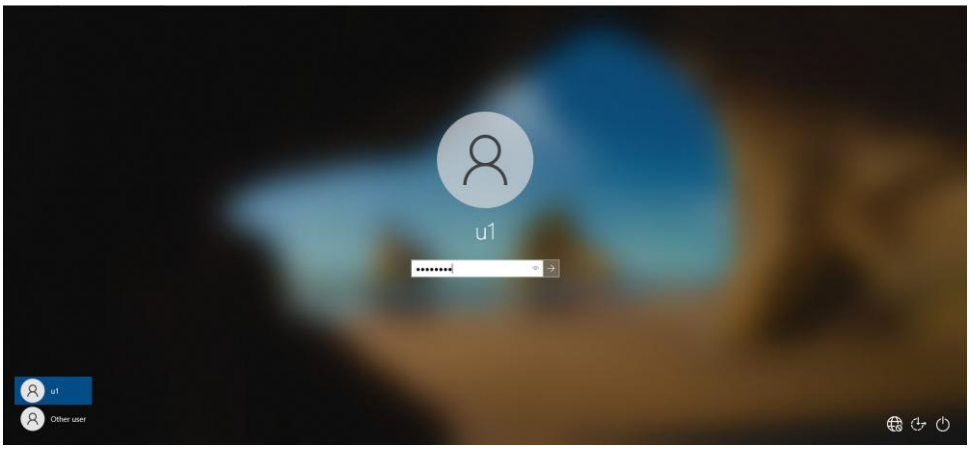


- Lúc này có thể chỉnh sửa quyền của user trong lúc chia sẻ thư mục



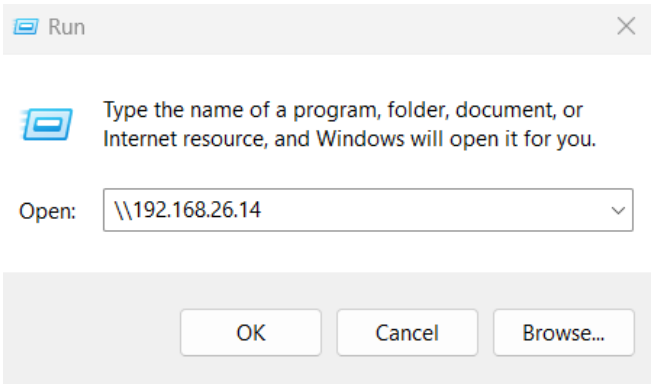
2.5. Từ máy Client, đăng nhập với tài khoản uit\u1 (tài khoản này được lưu trữ trên máy chủ Active Directory). Sau đó truy cập vào File Server để lấy dữ liệu và kiểm tra các thao tác đọc, ghi dữ liệu.

- Đăng nhập vào tài khoản u1:



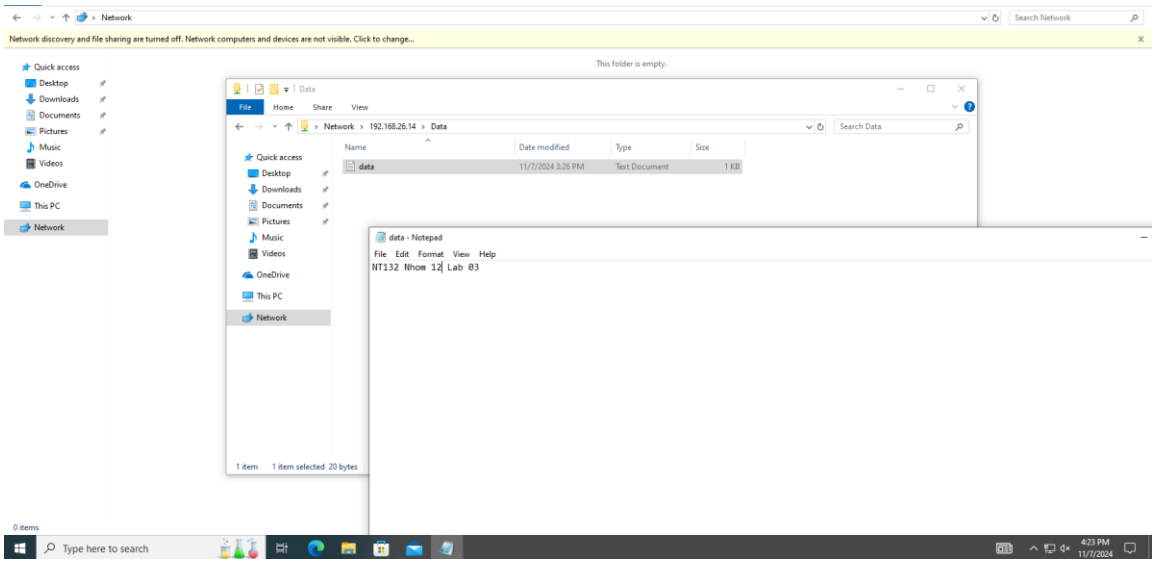
Hình 8. Client đăng nhập vào tài khoản u1

- Sau khi đăng nhập vào thành công, mở Run và nhập địa chỉ IP của File Server:



Hình 9. Client truy cập đến thư mục chia sẻ trên File Server

- Khi này, client có thể thêm, xóa, sửa tùy ý trong thư mục chia sẻ:



Hình 10. Client có thể chỉnh sửa nội dung bên trong thư mục chia sẻ

2.6. Tìm hiểu và so sánh sự khác nhau giữa mô hình Workgroup và mô hình Domain.

Workgroup	Domain
Tất cả các máy đều ngang hàng với nhau, không có máy nào có quyền kiểm soát máy khác.	Có một máy Active Directory có quyền hạn cao hơn, quản lý tất cả các máy khác trong mạng.
Mỗi máy duy trì một cơ sở dữ liệu riêng của nó.	Các dữ liệu của các máy đều được lưu trữ trong cơ sở dữ liệu trung tâm.
Mỗi máy có một quy tắc xác thực riêng với các tài khoản người dùng.	Có các máy chủ xác thực tập trung quy định quy tắc xác thực.
Mỗi máy tính đều có thiết lập tài khoản người dùng. Nếu người dùng có tài khoản trên máy tính đó thì chỉ có người dùng đó mới có thể truy cập vào máy tính đó.	Nếu người dùng có tài khoản trong miền thì người dùng có thể đăng nhập vào bất kỳ máy tính nào khác có trong miền.
Cài đặt trên máy cần thay đổi thủ công cho từng máy tính.	Việc thực hiện thay đổi trong một máy sẽ được tự động thực hiện thay đổi tương tự cho tất cả các máy khác có trong mạng.
Tất cả các máy tính phải cùng một mạng cục bộ.	Các máy tính có thể nằm trong một mạng cục bộ khác.

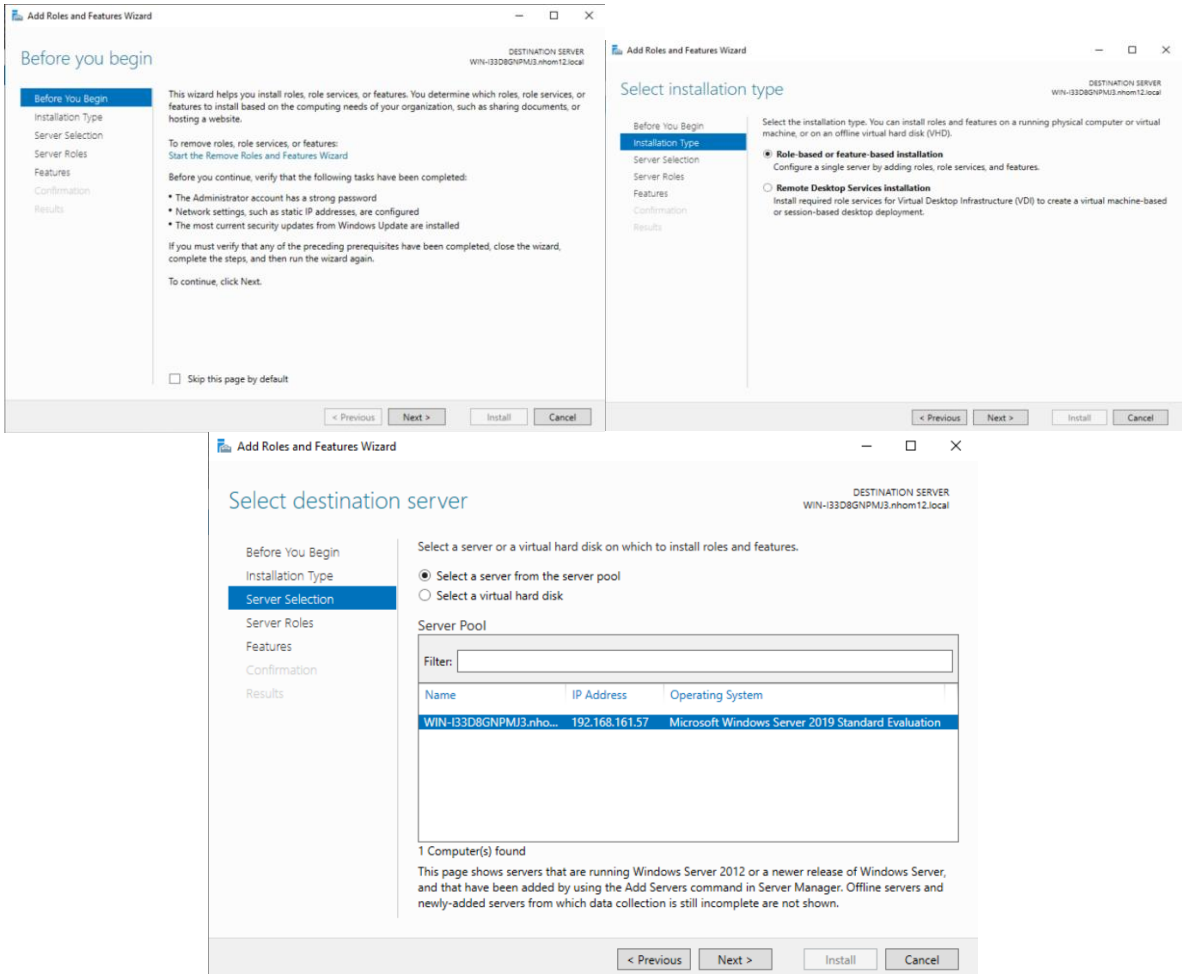
3. Xây dựng mô hình ADC cho dịch vụ Active Directory

- Mô hình:

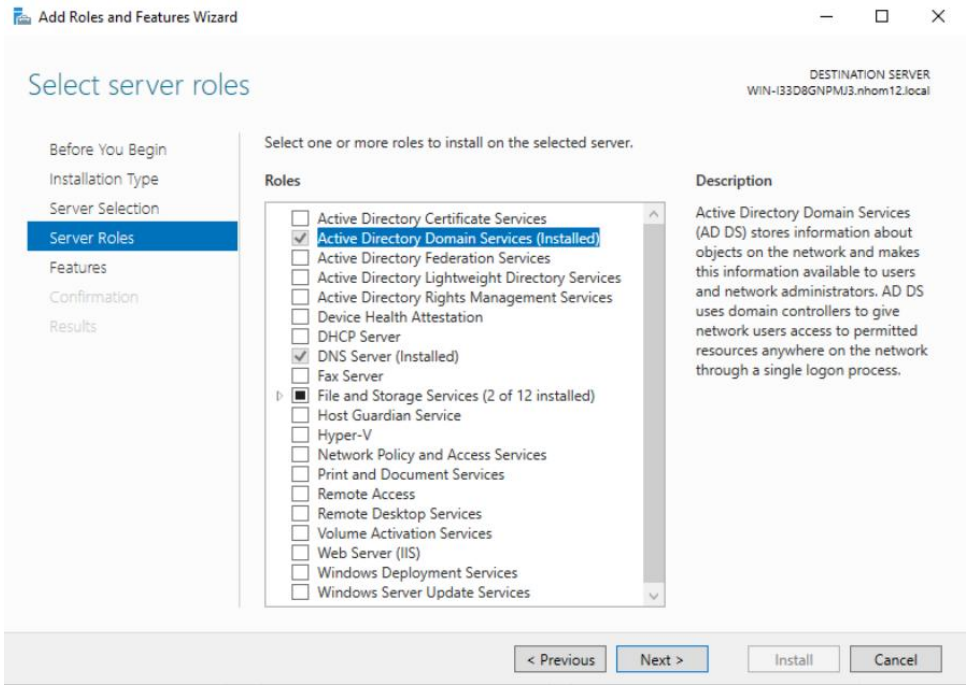
	IP Address	DNS	Operating System
Primary Active Directory	192.168.161.196/24	192.168.161.196	Windows Server 2019
Additional Active Directory	192.168.161.57/24	192.168.161.196	Windows Server 2019
Client	192.168.161.212/24	192.168.161.196	Windows

3.1. Nâng cấp máy Primary Active Directory lên thành Primary Controller (thực hiện tương tự như trong yêu cầu 2.1)

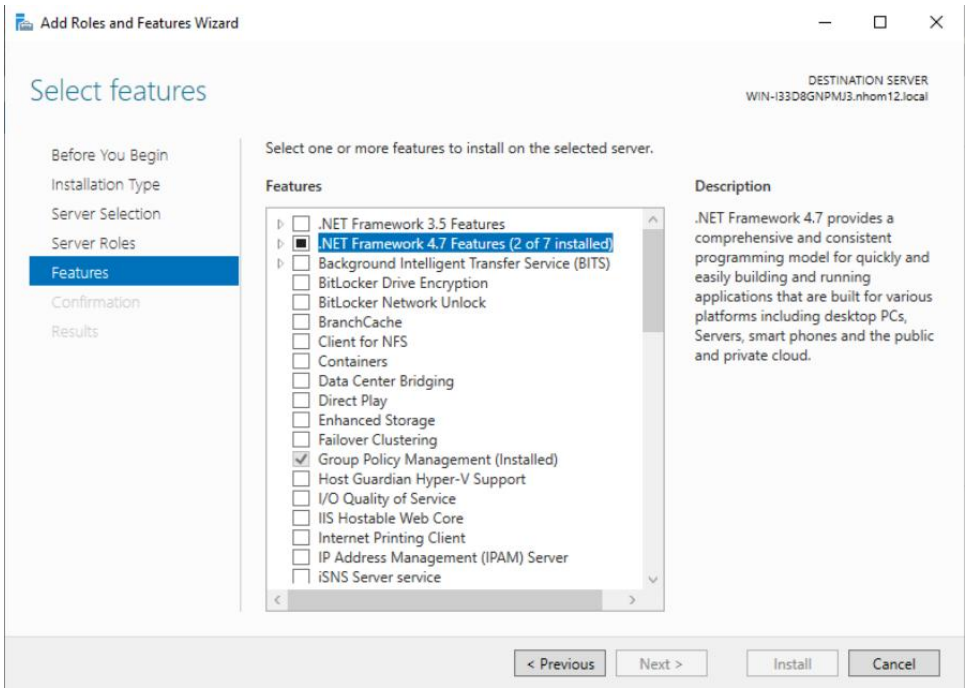
- Chọn ***Add roles and features***



- Chọn ***Active Directory Domain Services*** ở Server Roles

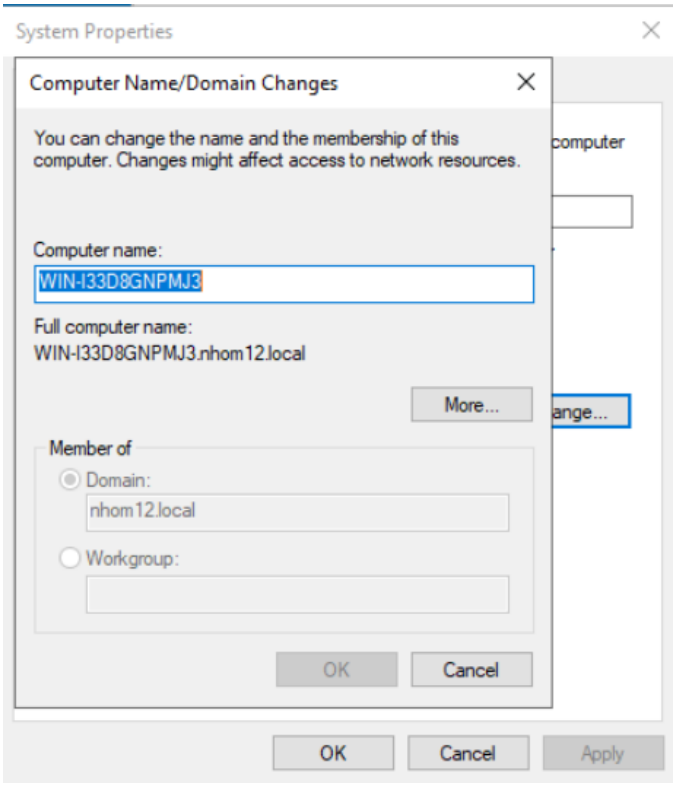


- Giữ nguyên các thiết lập mặc định và chọn Next, Install

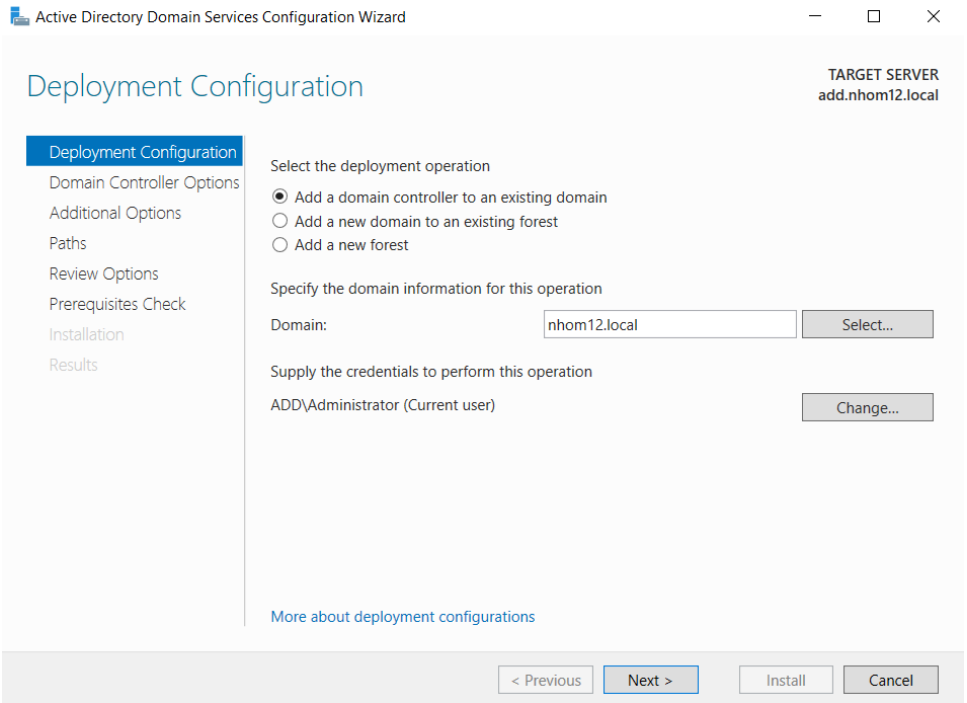


3.2. Tham gia máy chủ 2 (Additional Active Directory) vào Domain và nâng cấp máy chủ này thành Additional Domain Controller.

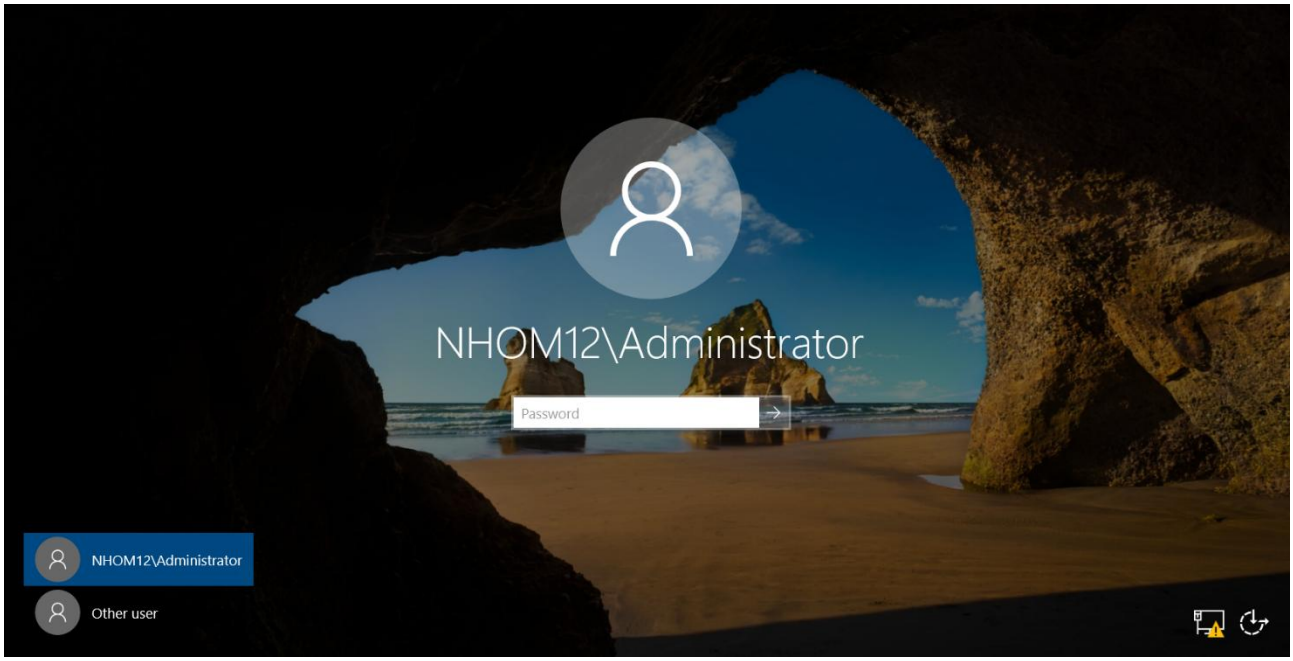
- Tham gia máy chủ 2 vào domain **nhom12.local**



- Nâng cấp máy chủ Active Directory thành Domain Controller.
  - Ở hình lá cờ, chọn ***Promote this server to a domain controller***
  - Ở Deployment Configuration, chọn ***Add a domain controller to an existing domain***, nhập tên domain là ***nhom12.local***, chọn Change để đăng nhập vào tài khoản Administrator của domain

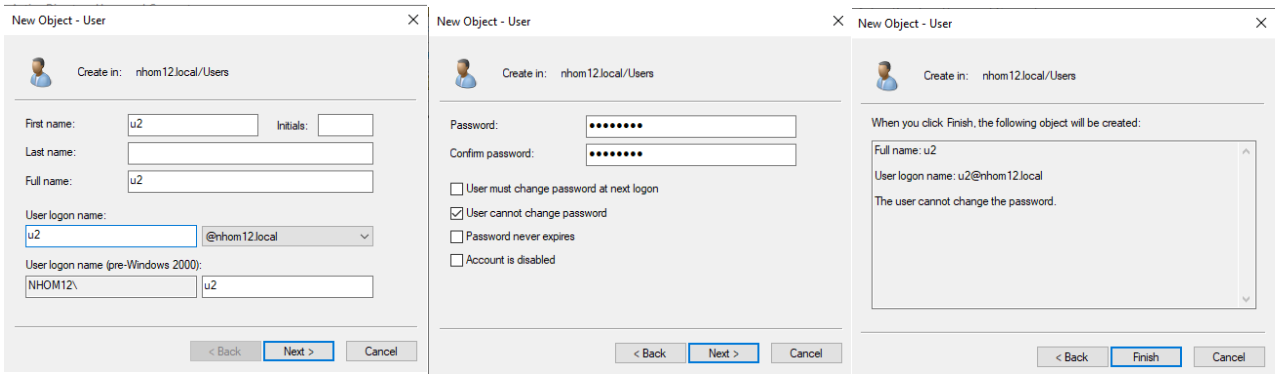


- Giữ nguyên các thiết lập mặc định và chọn Next

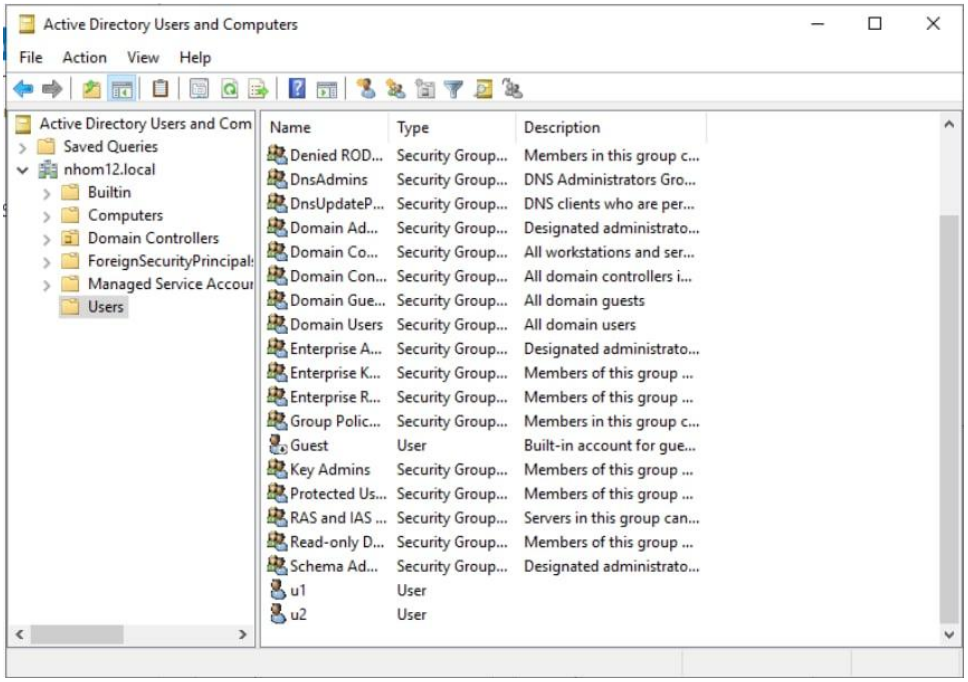


3.3. Trên Primary Domain Controller, tạo tài khoản u2/123. Sau đó, quan sát trên Additional Domain Controller xem tài khoản u2 có được đồng bộ sang không?

- Trên Primary Domain Controller, tạo tài khoản u2



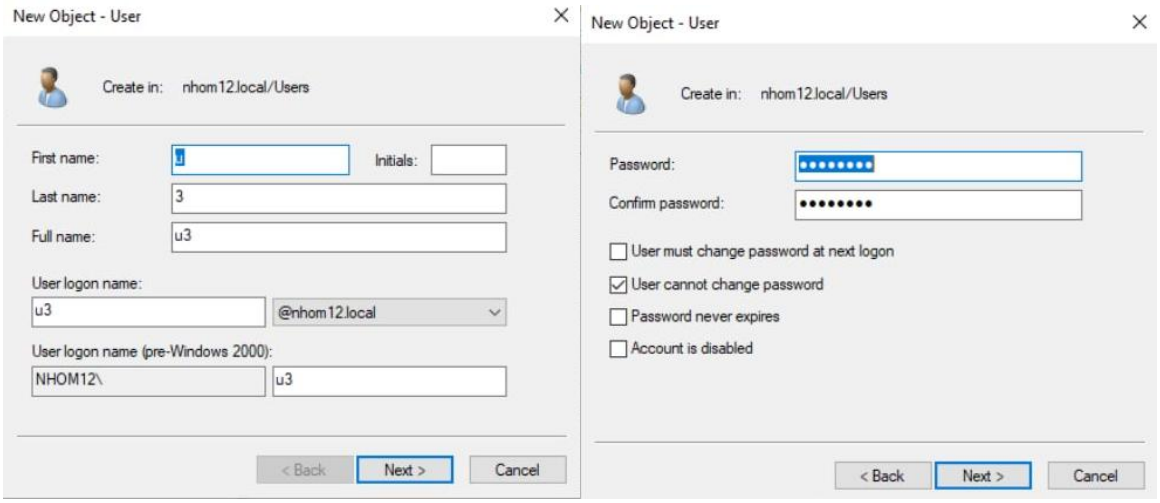
- Quan sát trên máy Additional Domain Controller, có thấy tài khoản u2 được đồng bộ:



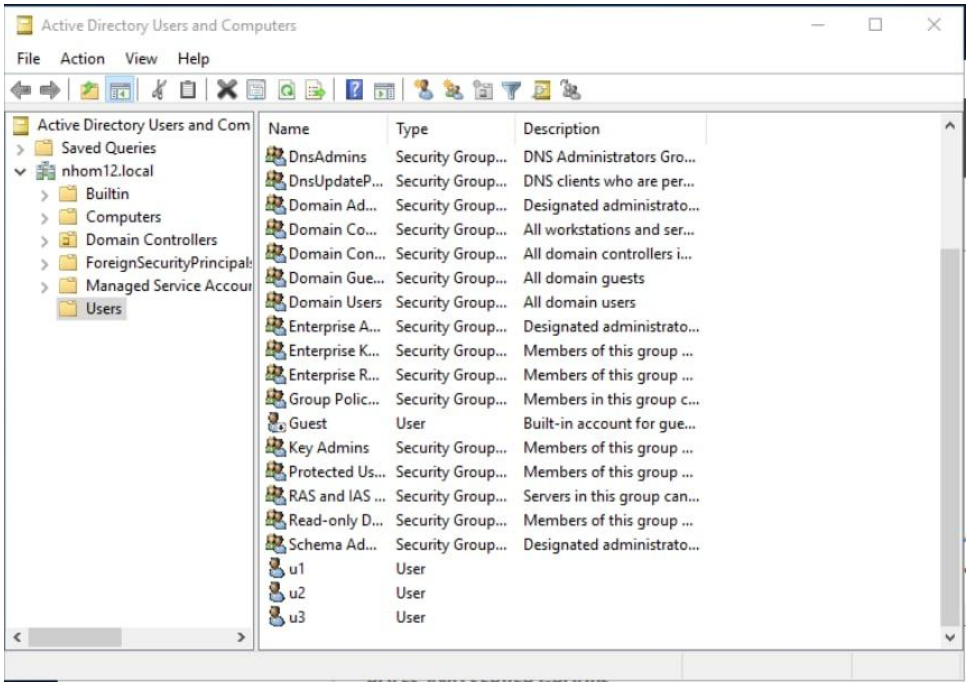
Hình 11. User u2 được đồng bộ trên máy Additional Domain Controller

3.4. Trên Additional Domain Controller, tạo tài khoản u3/123. Sau đó, quan sát trên Primary Domain Controller xem tài khoản u3 có được đồng bộ sang không?

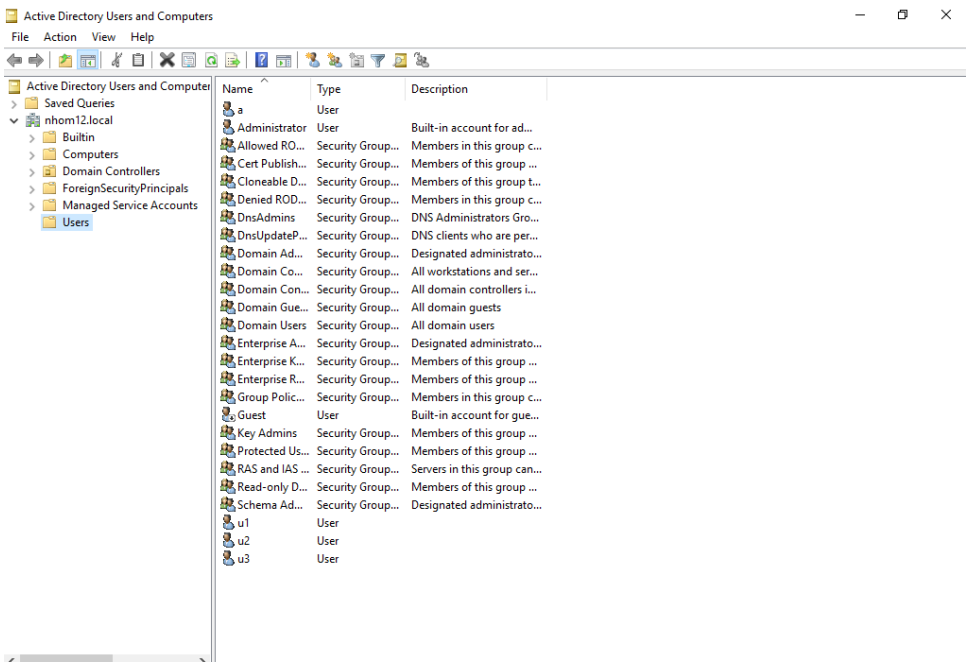
- Trên Additional Active Controller, tạo tài khoản u3:



- Tạo thành công user trên Additional Domain Controller

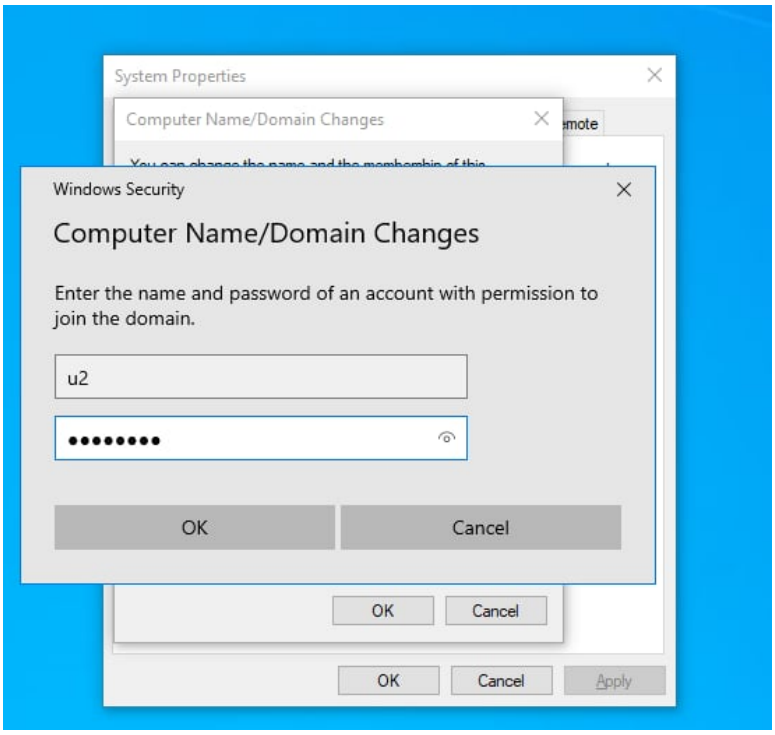


- Kiểm tra trên Primary Domain Controller thấy tài khoản u3 đã được đồng bộ:

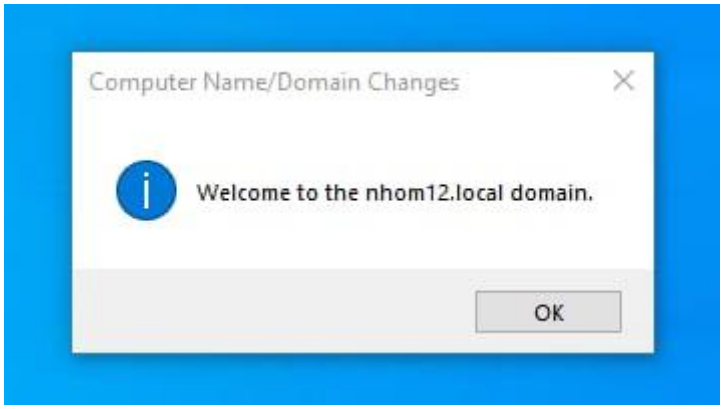


3.5. Trên máy Client, đăng nhập bằng tài khoản u2. Có thể đăng nhập được không?

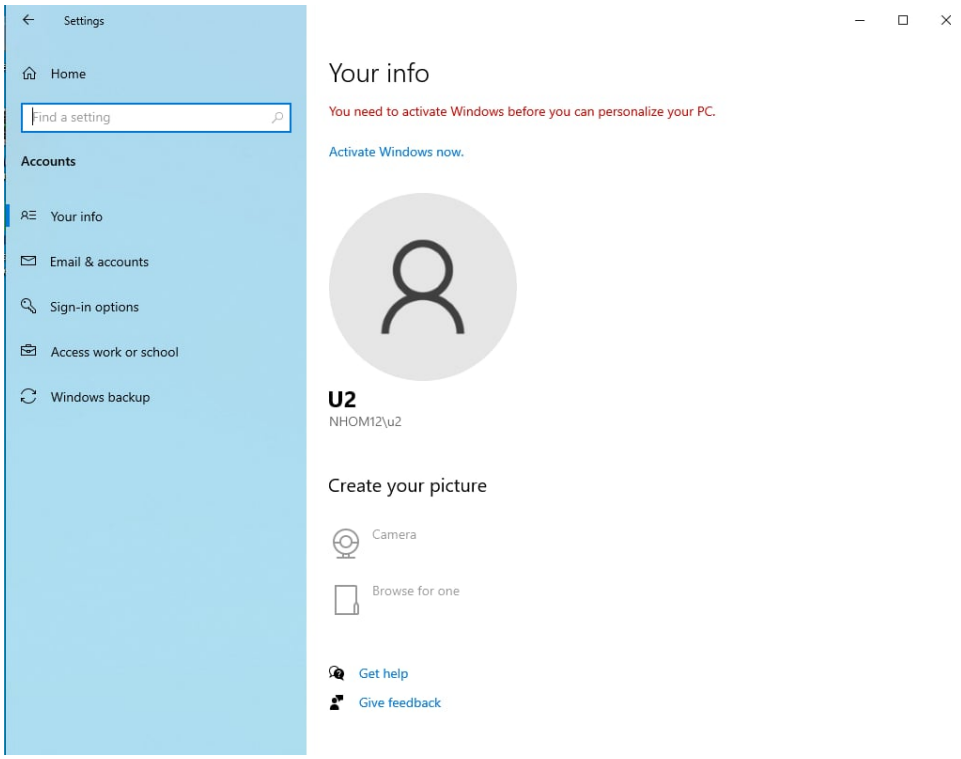
- Trên máy client, đăng nhập bằng tài khoản u2:



Hình 12. Thêm u2 và chung domain



Hình 13. Thêm u2 và chung domain thành công



Hình 14. Đăng nhập vào u2 thành công

3.6. Tắt máy Primary Domain Controller, sau đó login bằng tài khoản u2 trên máy Client. Có thể đăng nhập được không? Rút ra nhận xét.

- Sau khi tắt máy Primary Domain Controller, vẫn có thể đăng nhập vào tài khoản u2 trên máy Client bình thường.
- Nhận xét: Trong mô hình ADC này, máy Additional Domain Controller có chức năng tương tự với Primary Domain Controller, giúp cân bằng tải và khả năng chịu lỗi. Khi máy Primary Domain Controller bị lỗi thì máy Additional Domain Controller có thể thay thế PDC để xác thực và đảm bảo tính khả dụng cho hệ thống.

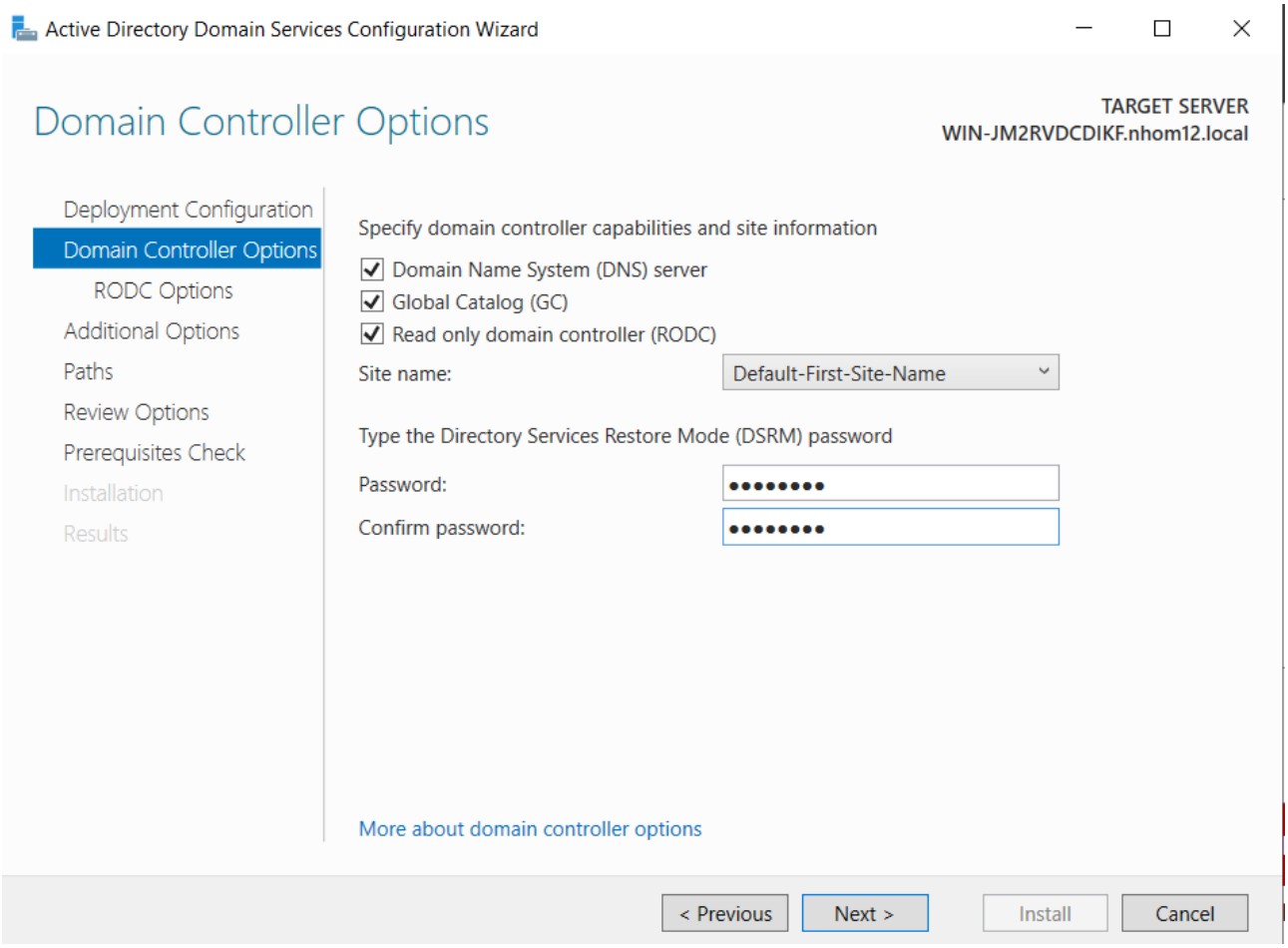
B. MỞ RỘNG

Tìm hiểu và xây dựng mô hình RODC cho dịch vụ Active Directory như sau. Sau khi thực hành phần mở rộng, hãy so sánh sự khác nhau giữa mô hình ADC và mô hình RODC.

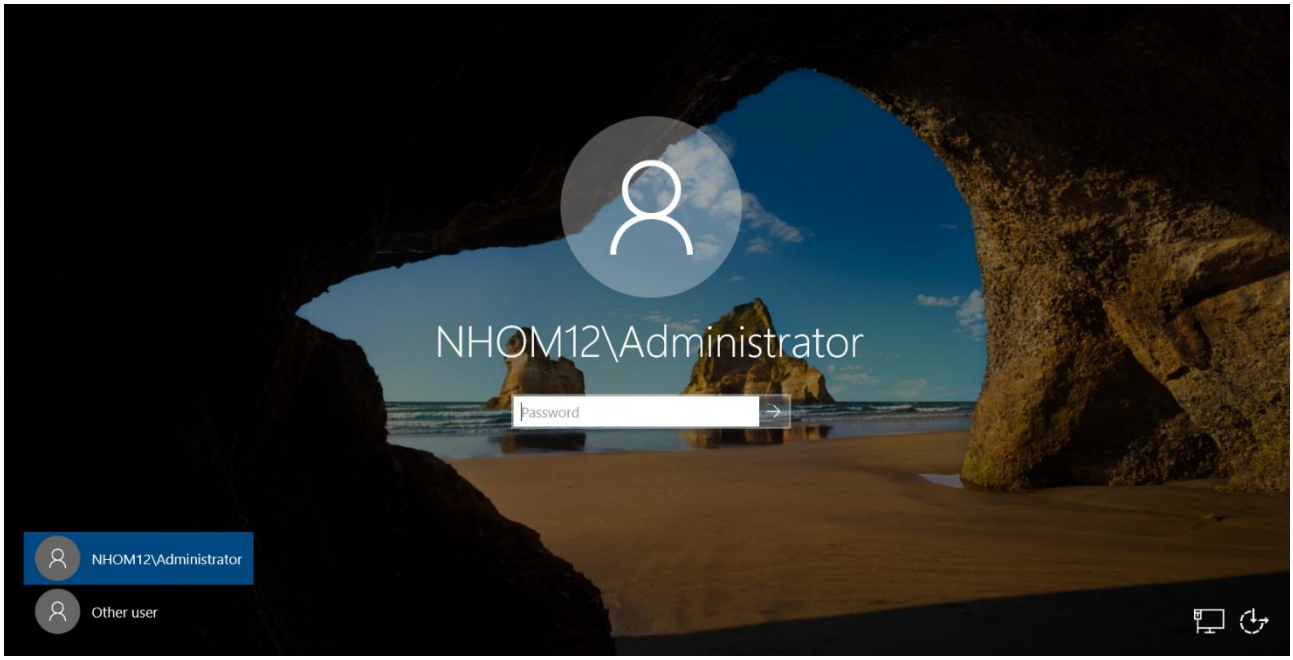
- Mô hình:

	IP Address	DNS	Operating System
Primary Active Directory	192.168.161.196/24	192.168.161.196	Windows Server 2019
Additional Active Directory	192.168.161.212/24	192.168.161.196	Windows Server 2019
Client	192.168.161.57/24	192.168.161.196	Windows

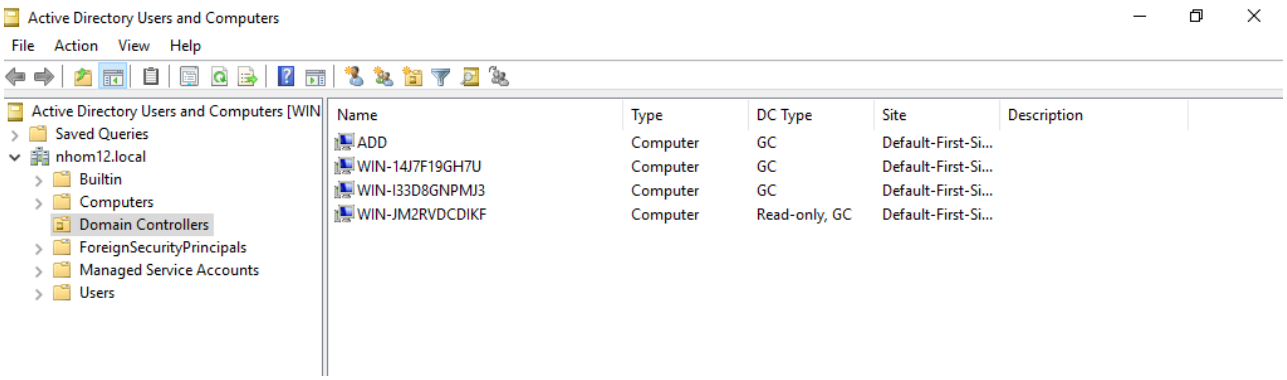
- Bên phía Windows Server 2, tại bước cấu hình Active Directory Services chọn ***Read only domain controller***:

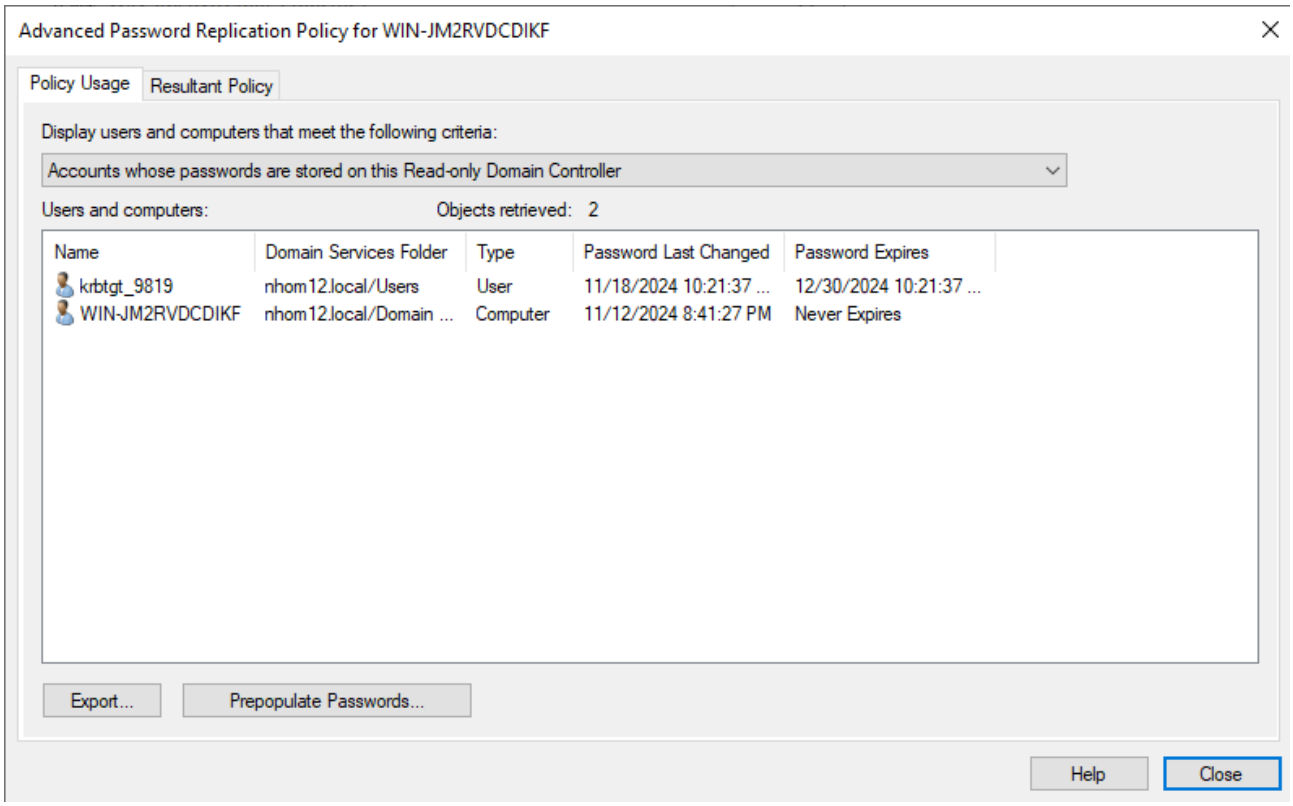


- Sau khi cấu hình thành công, một yêu cầu khởi động lại được gửi và windows server đã trở thành RODC thành công

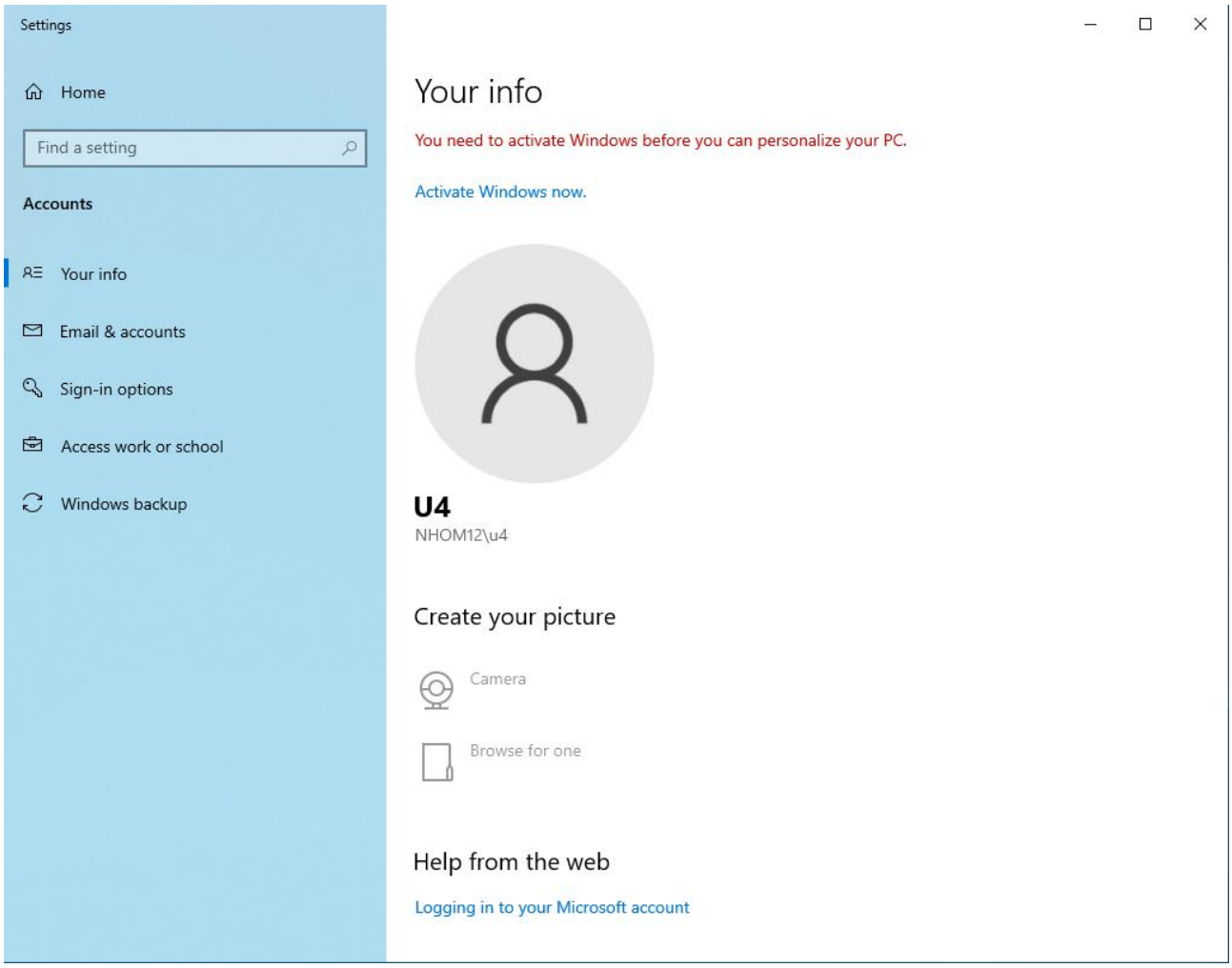


- Server RODC quan sát được trên máy Primary Domain Controller:





- Thêm user u4 vào group read-only và đăng nhập thành công:



- So sánh sự khác nhau giữa mô hình ADC và mô hình RODC:

ADC	RODC
Máy chủ Additional Active Directory có quyền hạn đầy đủ, có thể thực hiện tất cả các chức năng bao gồm thay đổi dữ liệu và cấu hình.	Máy chủ Read-Only Active Directory chỉ có thể đọc và không thể chỉnh sửa.
Có nguy cơ xảy ra rủi ro khi phía Additional Active Directory bị tấn công và kiểm soát.	Có tính bảo mật cao hơn vì máy chủ Read-Only Active Directory chỉ có thể nhận dữ liệu từ Primary Active Directory mà không lo bị chỉnh sửa.
Dữ liệu bị thay đổi trên 1 máy Additional Active Directory sẽ dẫn đến tất cả các ADC khác trong cùng miền bị thay đổi.	Read-Only Active Directory không thể thay đổi dữ liệu và sẽ không sao chép các thay đổi đến các máy chủ khác.

C. TÀI LIỆU THAM KHẢO

1.Kardashevsky, C., & Kardashevsky, C. (2024, June 24). *How to install and configure Read-Only Domain Controller (RODC)?* TheITBros.com. https://theitbros.com/read-only-domain-controller-rodc/

2.Narayanan, B. (2023, July 14). *What is a Read Only Domain Controller (RODC). Windows Active Directory.* https://www.windows-active-directory.com/read-only-domain-controller.html