

# BÁO CÁO LAB 4

Lớp: NT132.N11.ANTN

Giáo viên hướng dẫn: Đỗ Hoàng Hiển

Thông tin sinh viên:

Họ và tên: Nguyễn Bảo Phương

MSSV: 20520704

Họ và tên: Võ Anh Kiệt

MSSV: 20520606

## Bài làm

(Yêu cầu 1,2 đã báo cáo trên lớp)

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

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

**1.1.1.** Trong mô hình Workgroup:

- Các máy tính có quyền hạn ngang nhau, các máy tự bảo mật và quản lý các tài nguyên của riêng mình.
- Các máy tính trong mô hình này có quyền chia sẻ tài nguyên ngang nhau mà không cần sự chỉ định của server.
- Mỗi máy đều có một user account riêng, muốn truy cập vào máy nào phải có account của máy đó
- Tất cả máy tính đều phải ở cùng một subnet hoặc 1 local network

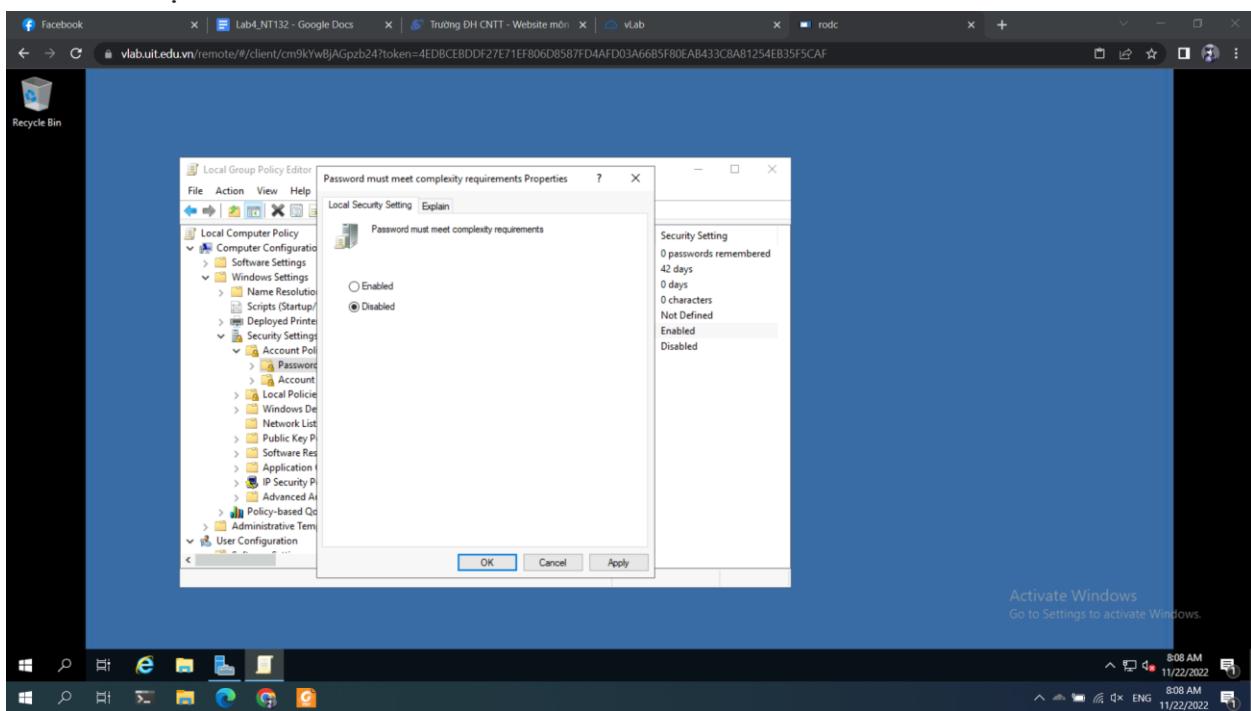
**1.1.2..**

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

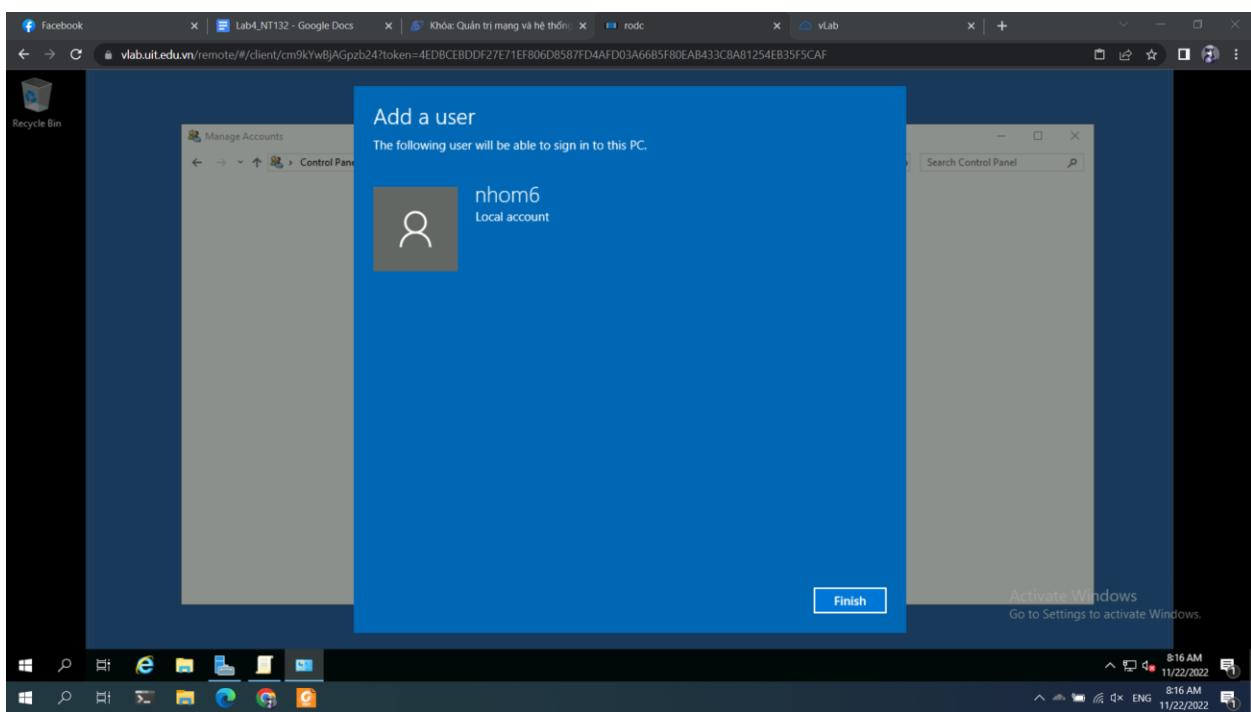
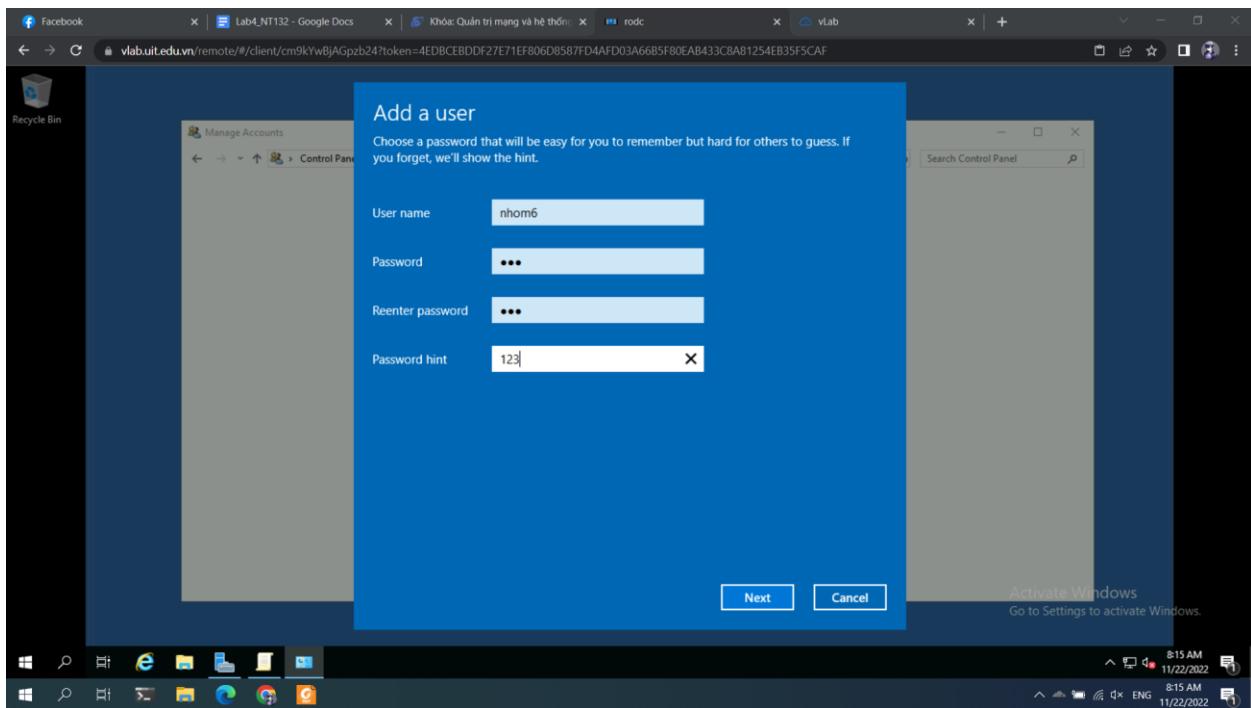
Nhược điểm là mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập; bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi mật

khẩu hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong Workgroup, nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó; việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng.

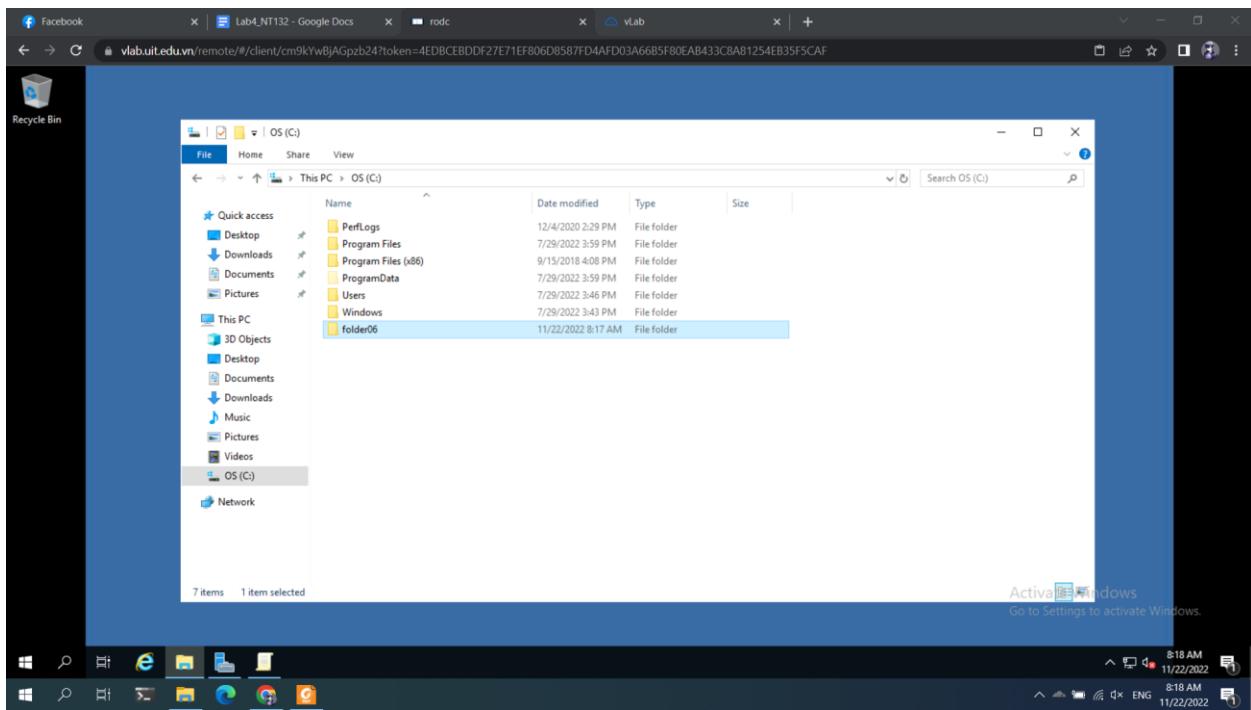
**Yêu cầu 1.2:** Xây dựng mô hình Workgroup để chia sẻ file như bên dưới.  
Cấu hình mật khẩu trên fileServer



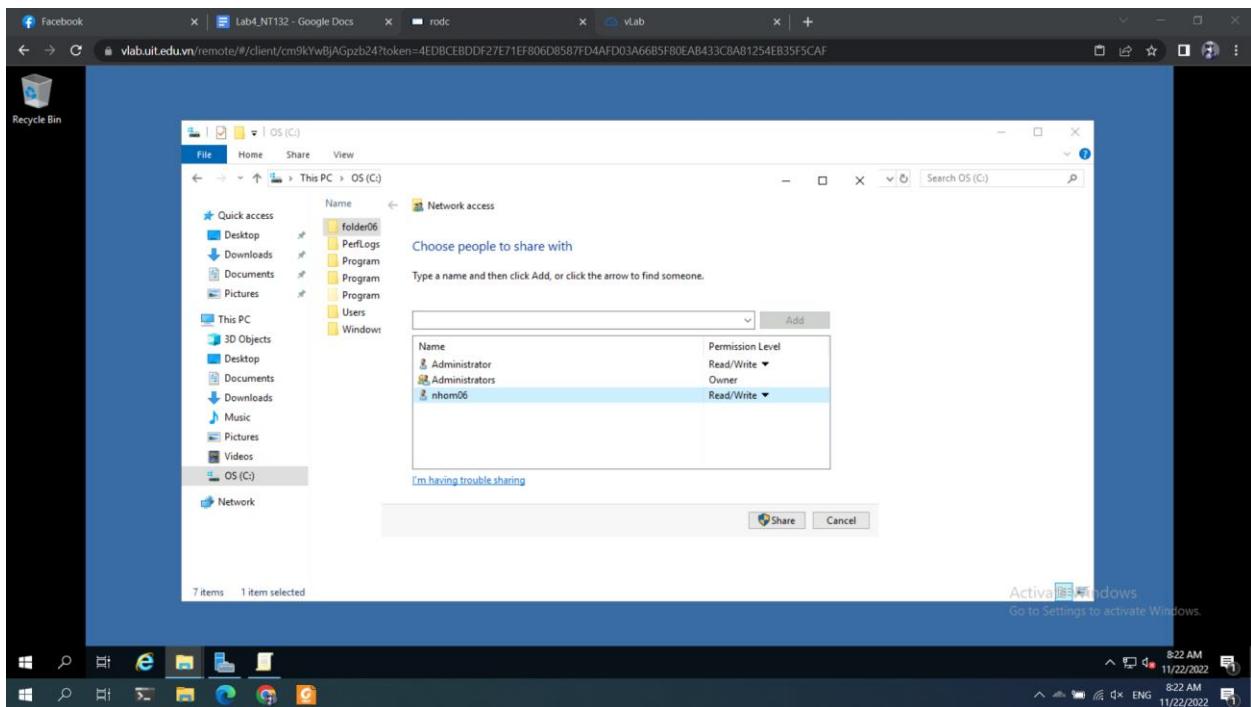
Tạo tài khoản nhom6 trên fileServer có mật khẩu là 123



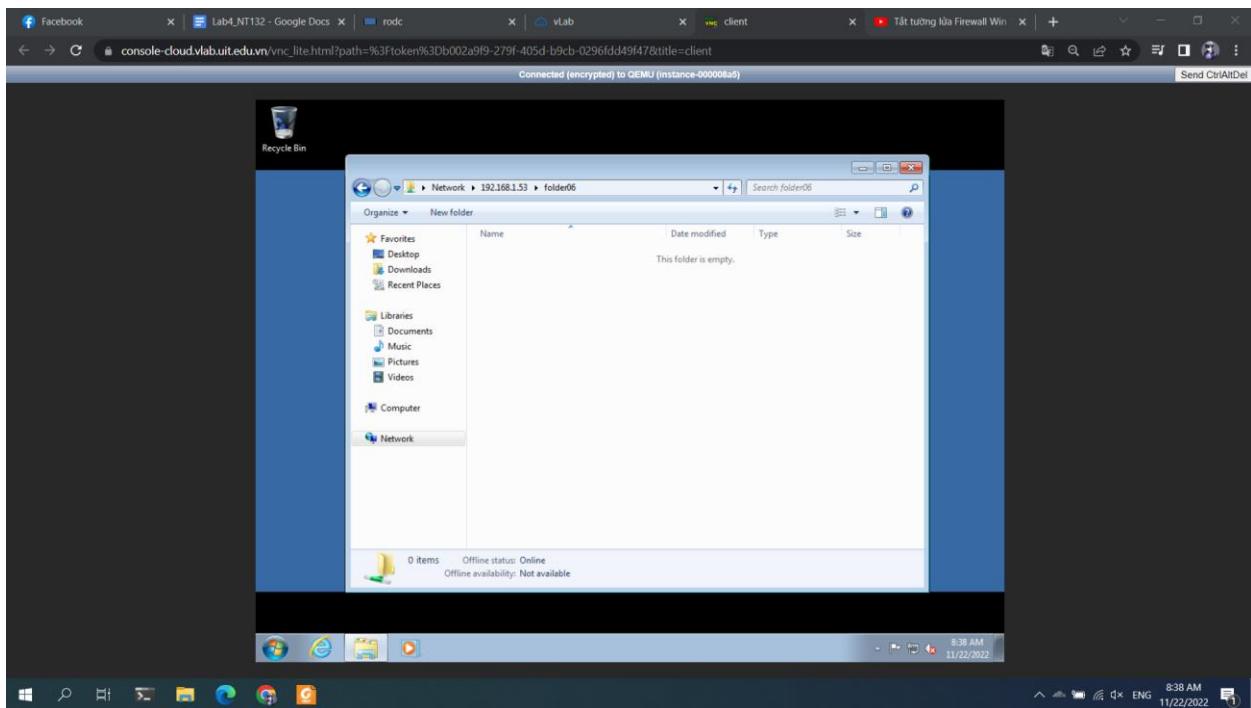
Tạo folder06 trên ổ C



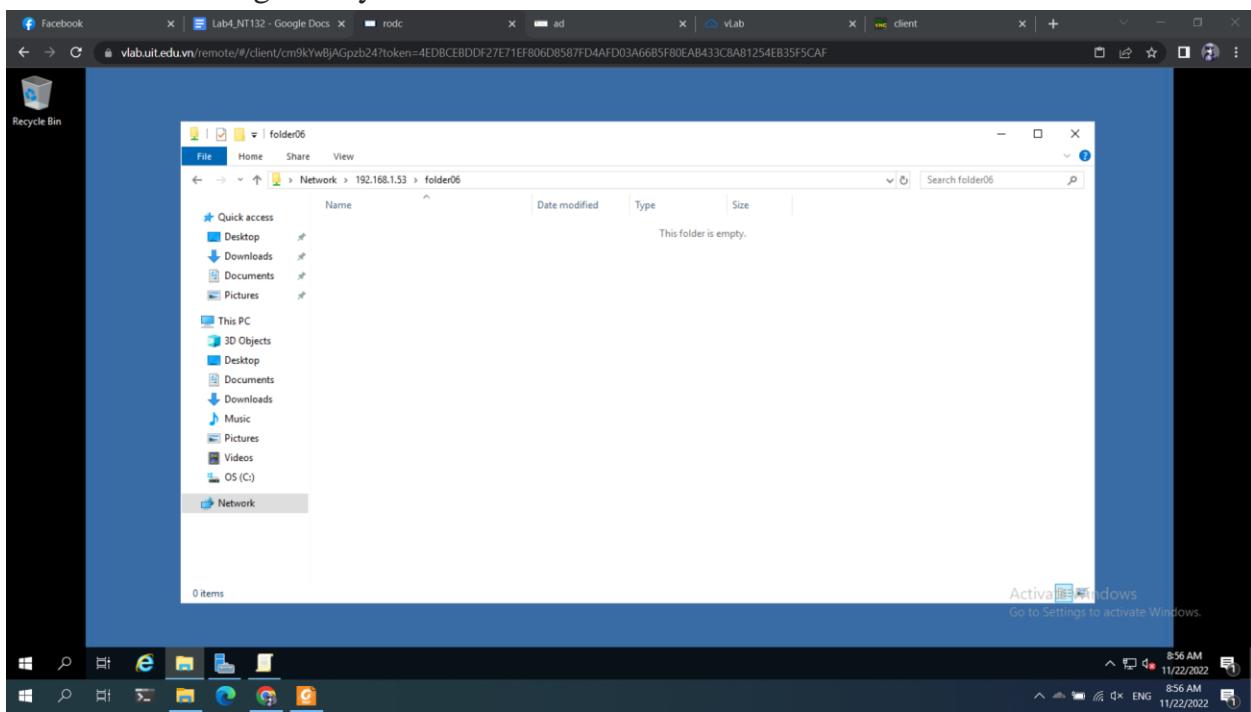
Chia sẻ folder06 cho user nhom06



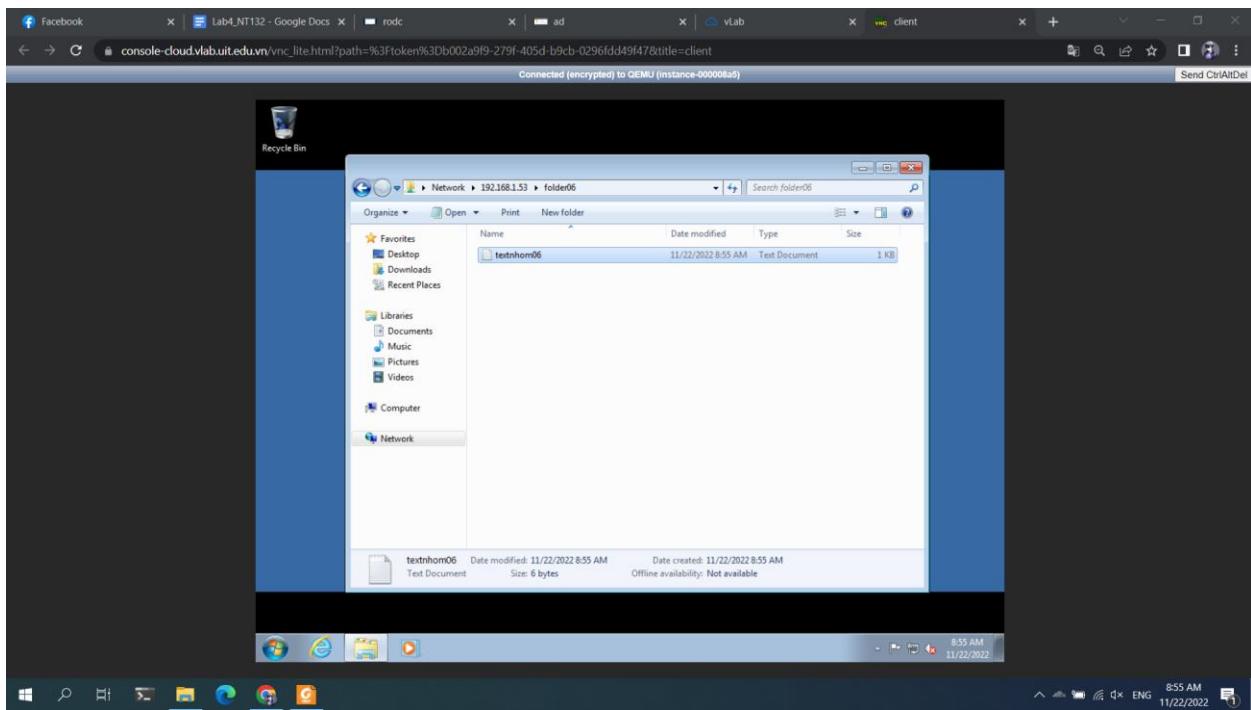
Kết nối thành công vào folder06 từ máy client



Kết nối thành công từ máy File Server



Tạo tập tin tùy ý ở máy client



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

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

### 2.1.1.

Active Directory hay AD là 1 dịch vụ thư mục đã được Microsoft phát triển dành cho những mạng dùng Windows domain. Theo đó dịch vụ này hiện tại đang bao gồm trong hầu hết những hệ điều hành Windows Server ở dạng tập hợp những dịch vụ và quy trình.

1 máy chủ nếu như chạy AD DS – Active Directory Domain Service sẽ gọi là domain controller. Theo đó nó sẽ ủy quyền và xác thực cho toàn bộ máy tính cũng như người dùng trong mạng loại Windows gán, thực thi những chính sách về bảo mật cho toàn bộ những cài đặt, máy tính hay cập nhật phần mềm.

Khi người dùng đăng nhập vào máy tính là domain của Windows thì AD sẽ kiểm tra mật khẩu đã đăng nhập và xác định người dùng là người dùng bình thường hay là quản trị viên của hệ thống.

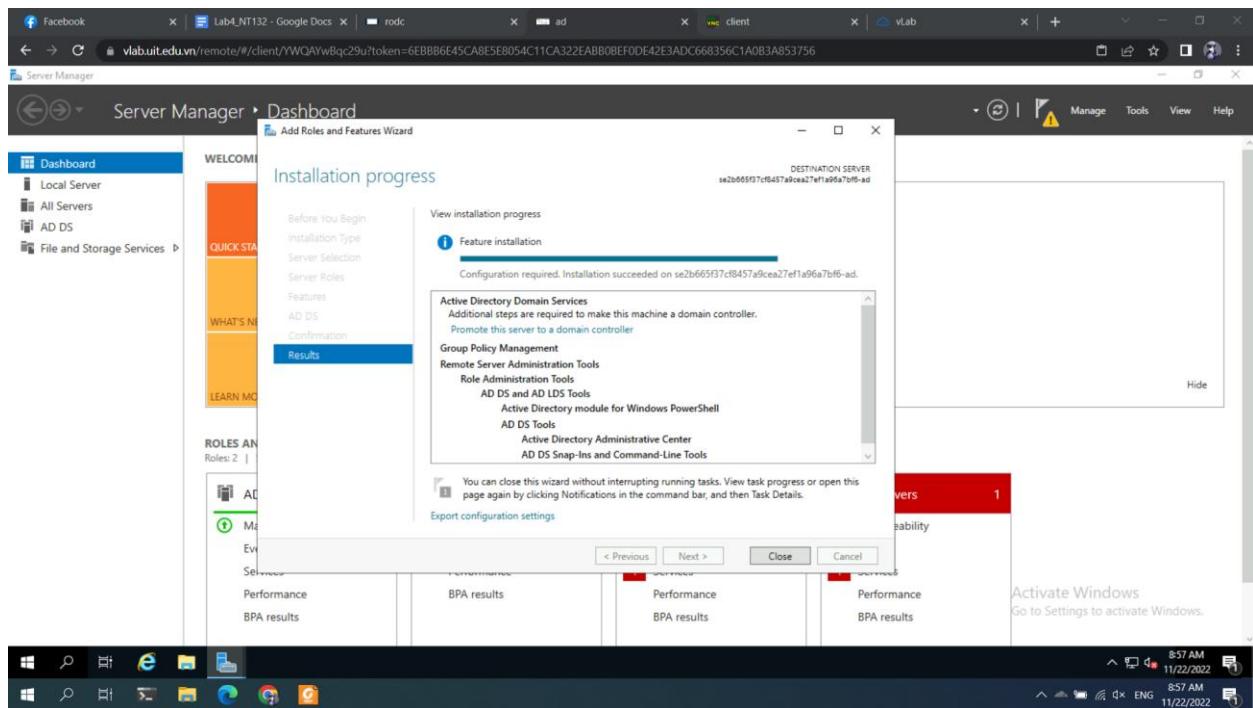
AD còn cho phép lưu trữ thông tin, quản lý cung cấp những cơ chế bị xác thực cũng như uỷ quyền, thiết lập 1 khung nhằm triển khai những dịch vụ khác có liên quan như: Rights Management Services, Lightweight Directory Services, Active Directory Federation Services và Certificate Services.

### 2.1.2 So sánh mô hình domain và workgroup

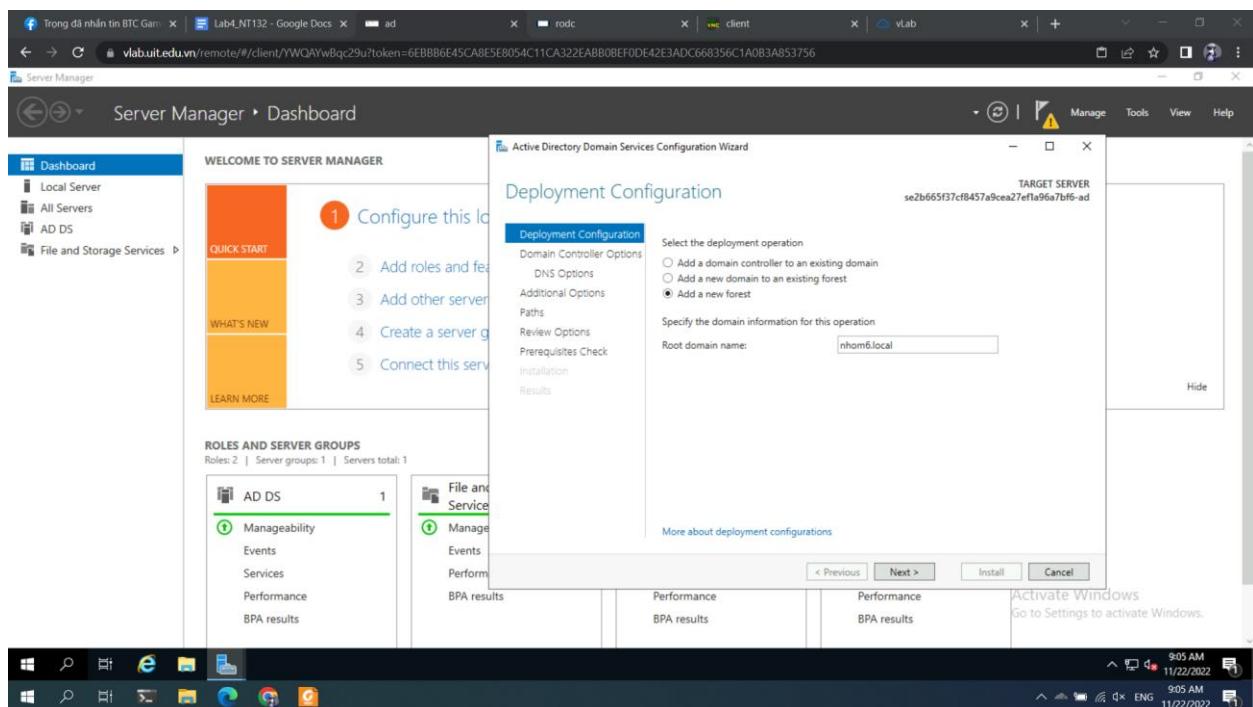
Mô hình Workgroup	Mô hình Domain
<ul style="list-style-type: none"><li>- Tất cả máy tính phải ở cùng một local network hoặc subnet</li><li>- Mỗi máy tính phải có một user account tạo riêng. Để đăng nhập vào một máy trong Workgroup thì phải có user account của máy đó.</li><li>- Tất cả các máy trong Workgroup đều ngang hàng với nhau</li><li>- Cài đặt dễ dàng</li><li>- Tính bảo mật thấp, không tập trung dữ liệu</li></ul>	<ul style="list-style-type: none"><li>- Các máy tính có thể ở local network khác nhau</li><li>- Nếu có 1 user domain thì có thể đăng nhập vào bất kỳ máy tính nào trên domain mà không cần có user account của máy đó</li><li>- Có 1 hay nhiều máy trong domain là máy chủ server. Người quản trị mạng sẽ dùng servers để kiểm soát các vấn đề về bảo mật và phân quyền (security and permissions) cho tất cả các máy trong domain.</li><li>- Cài đặt phức tạp</li><li>- Tính bảo mật cao bởi dữ liệu được tập trung tại máy server</li></ul>

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

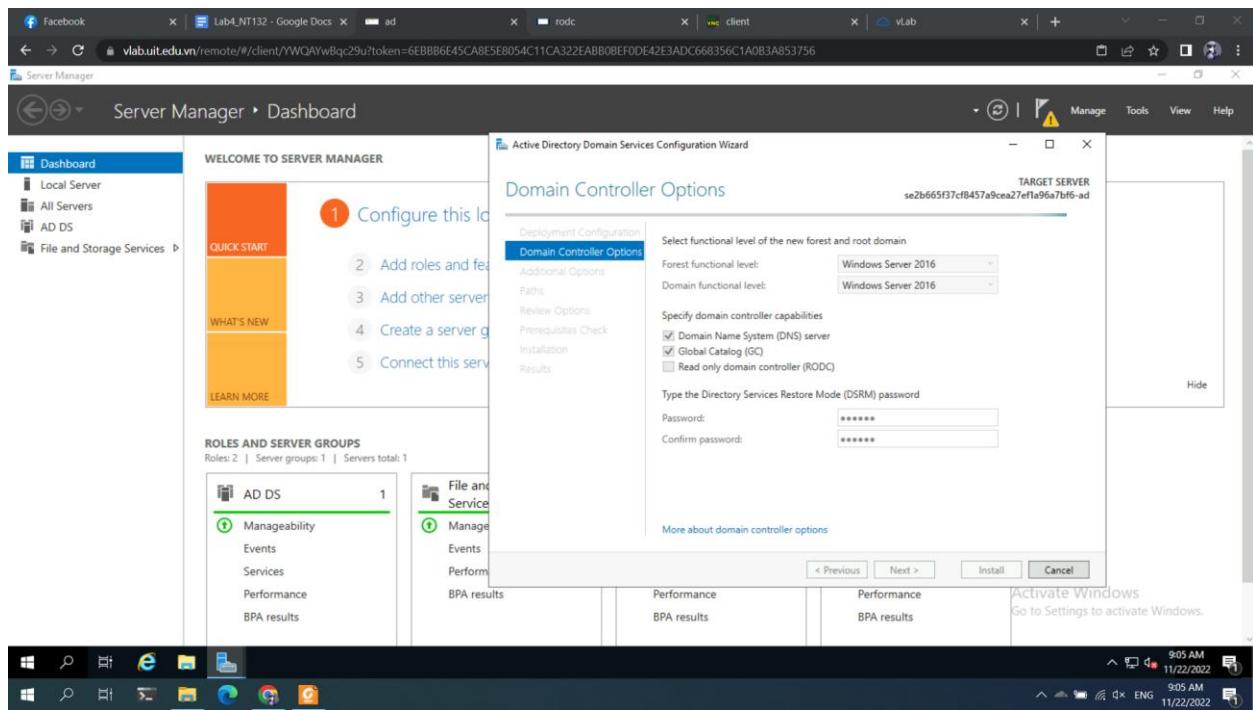
Cài đặt active trong Direct Domain



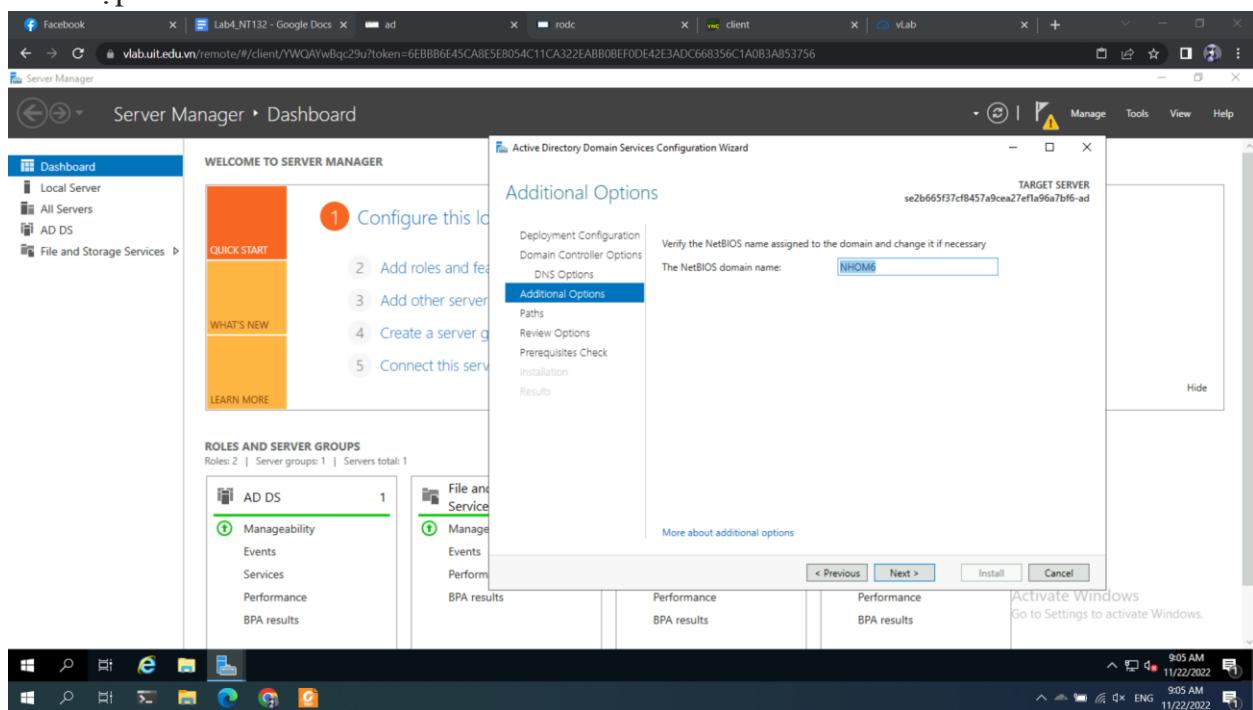
**Chọn Add a new forest và nhập domain nhom6.local**



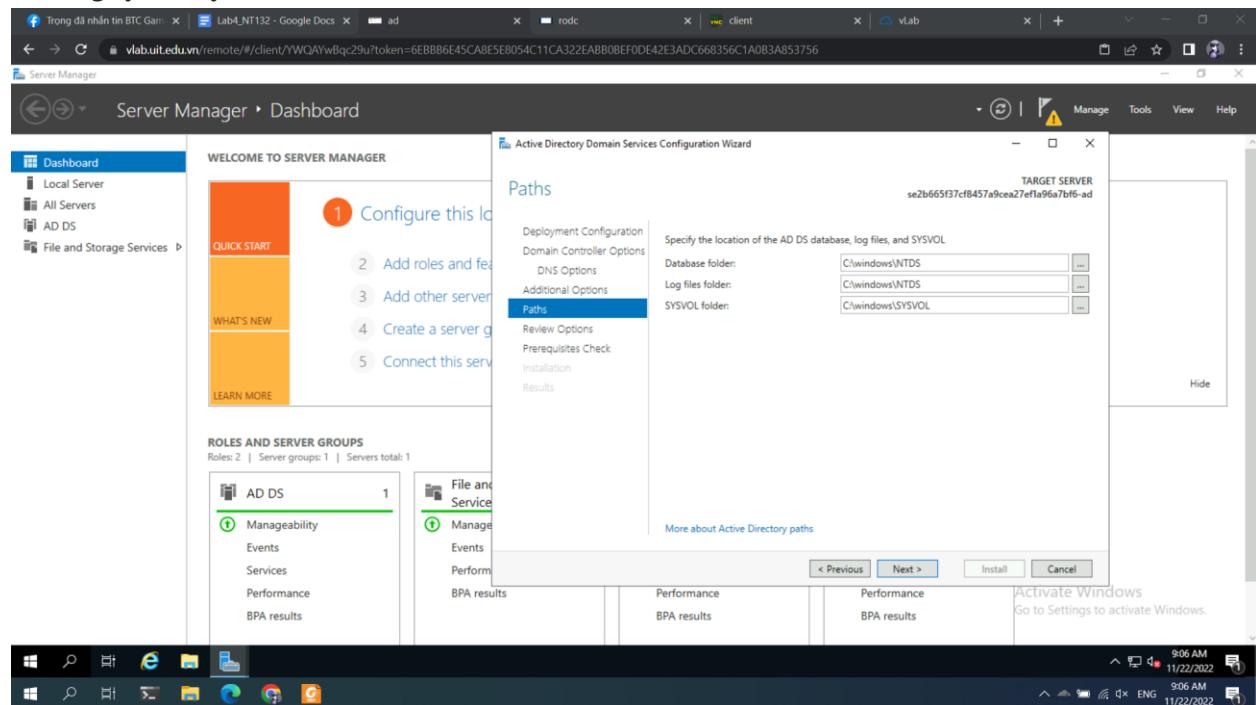
**Thiết lập DSRM password là : Qq@123**



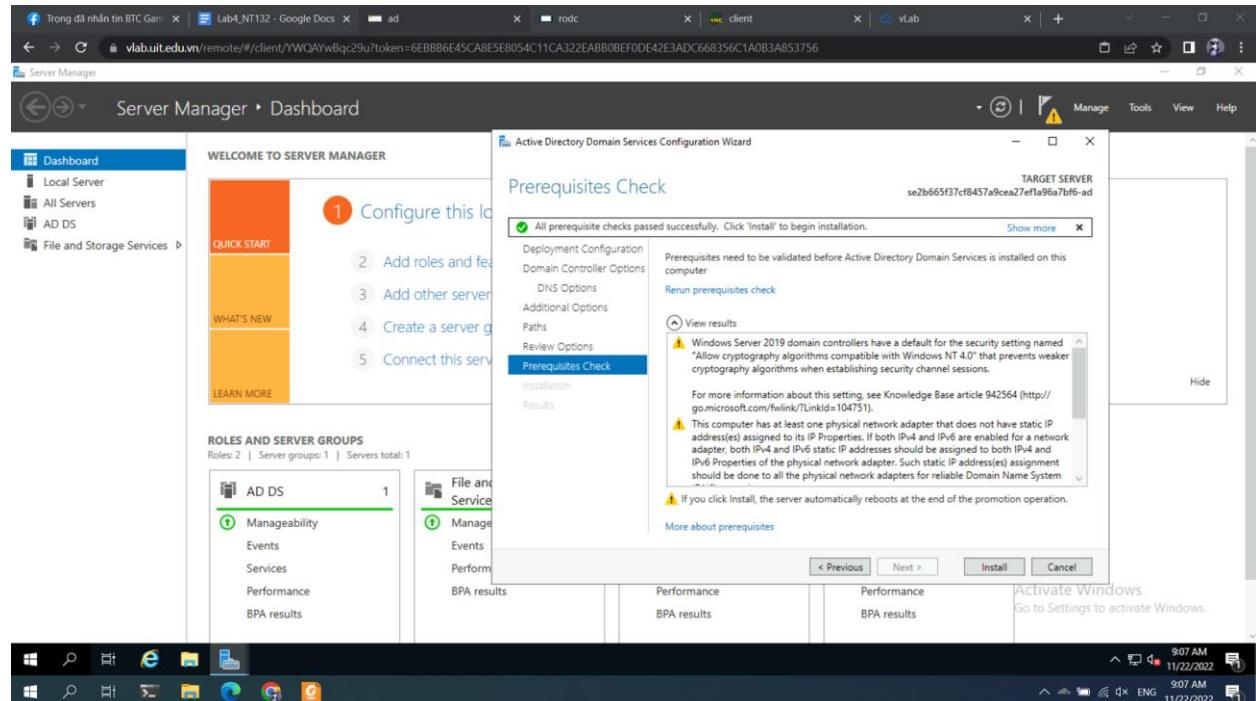
## Thiết lập NetBios domain name



## Giữ nguyên tùy chỉnh ở Paths

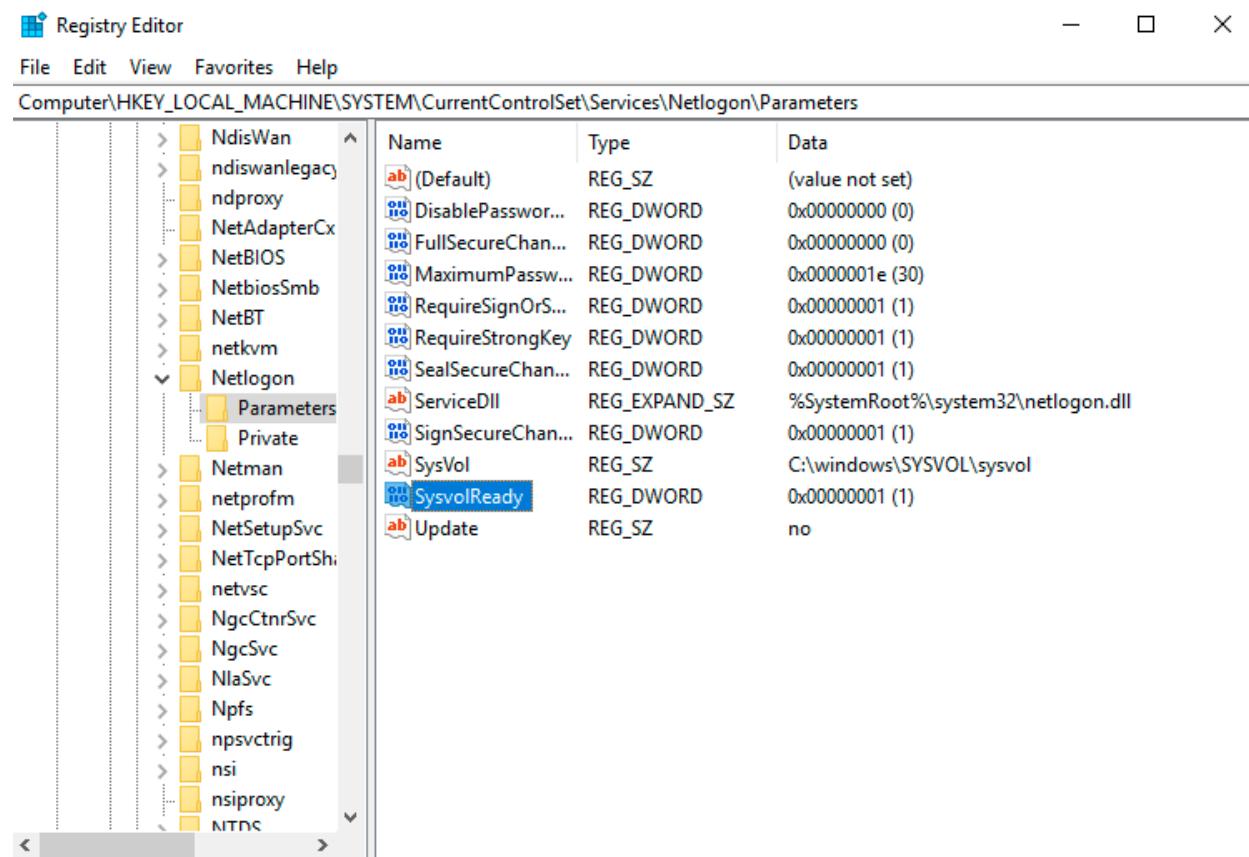


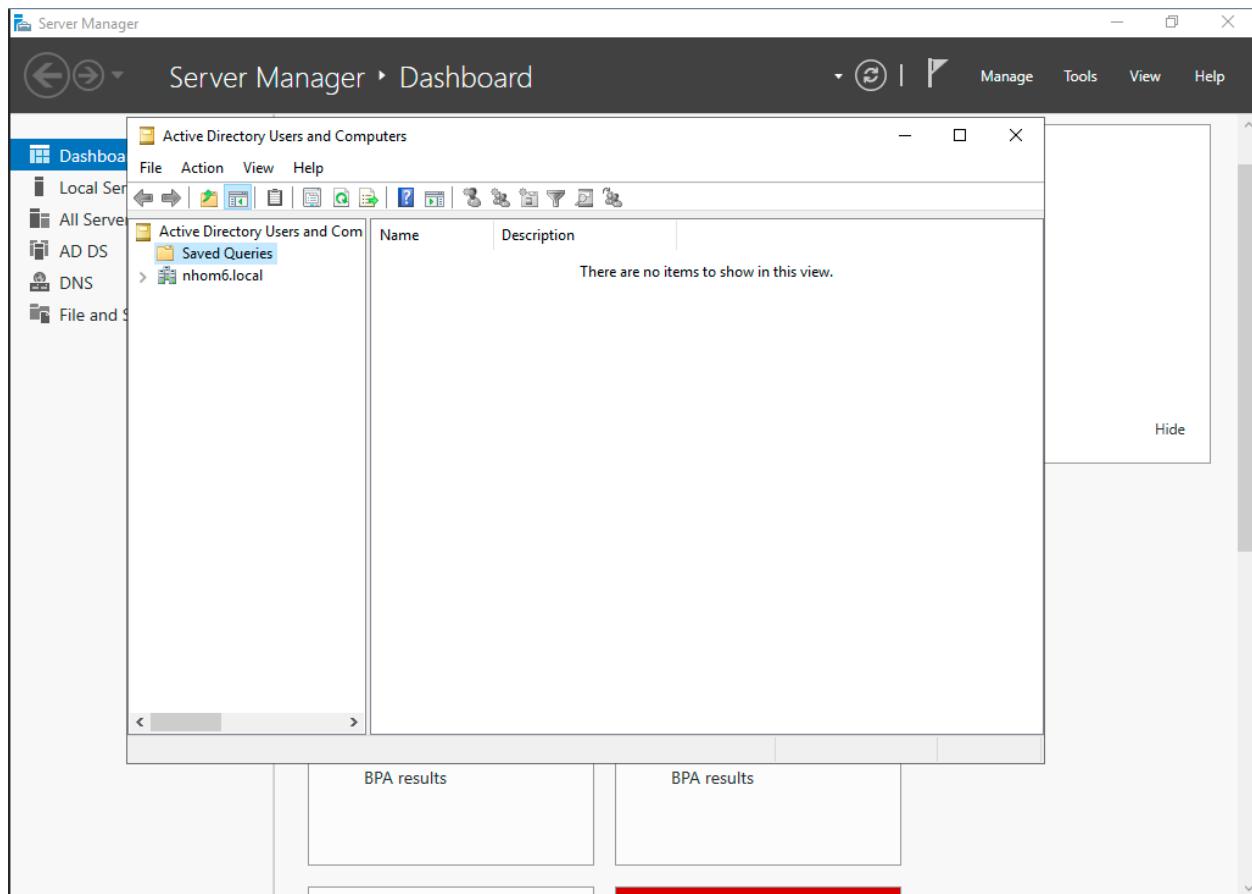
## Thực hiện bước Prerequisites Check hoàn thành.



Sau khi máy đã khởi động lại.

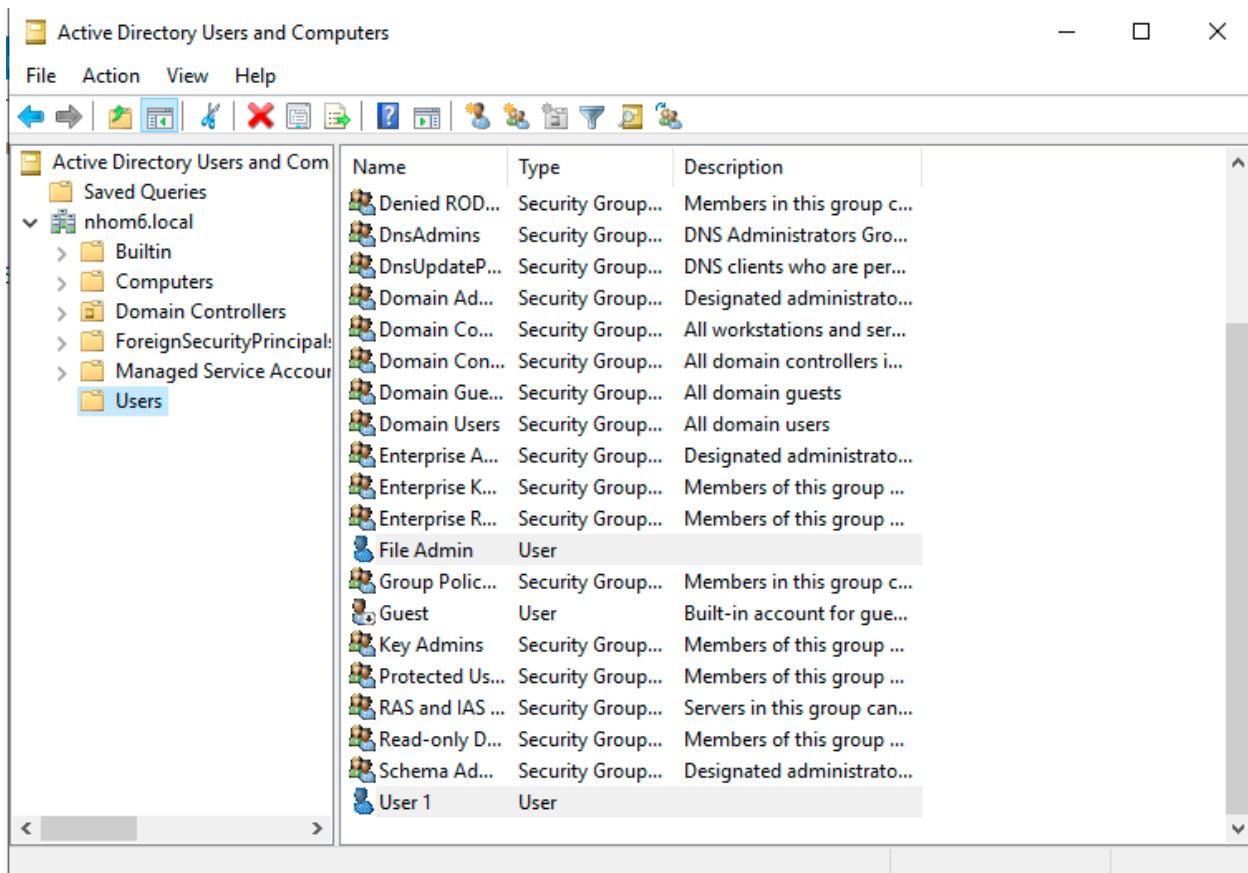
Ta vào chỉnh key **SysvolReady** ở  
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**





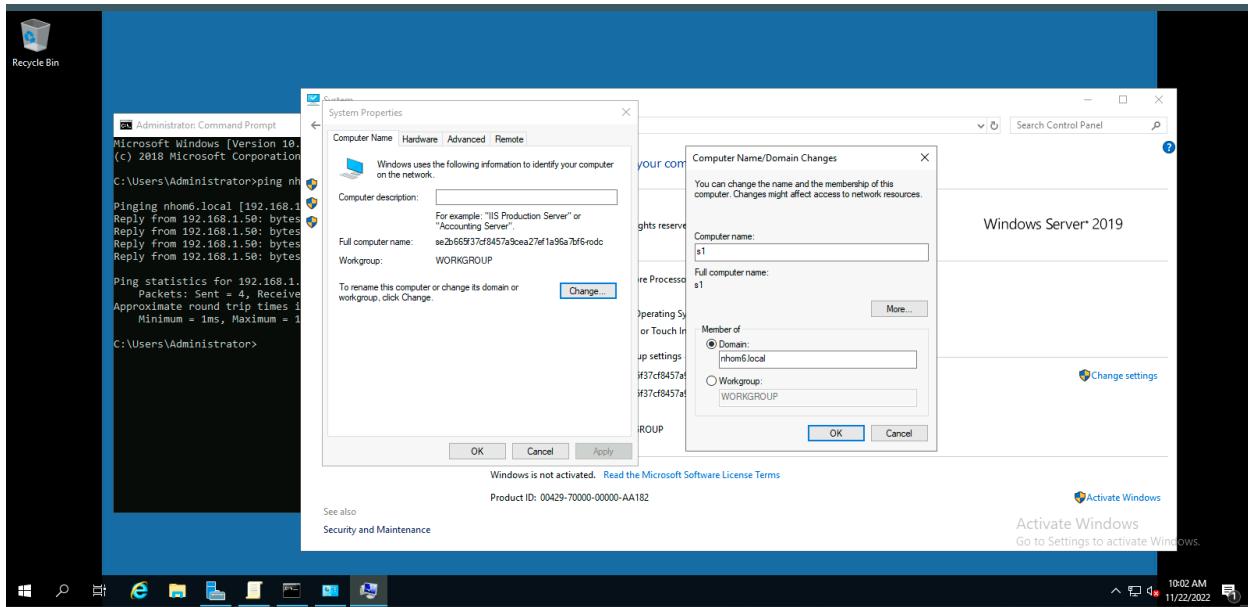
Tạo account **File admin** với password : Qq@12345678

Tạo account user1 với pass: Qq@12345678

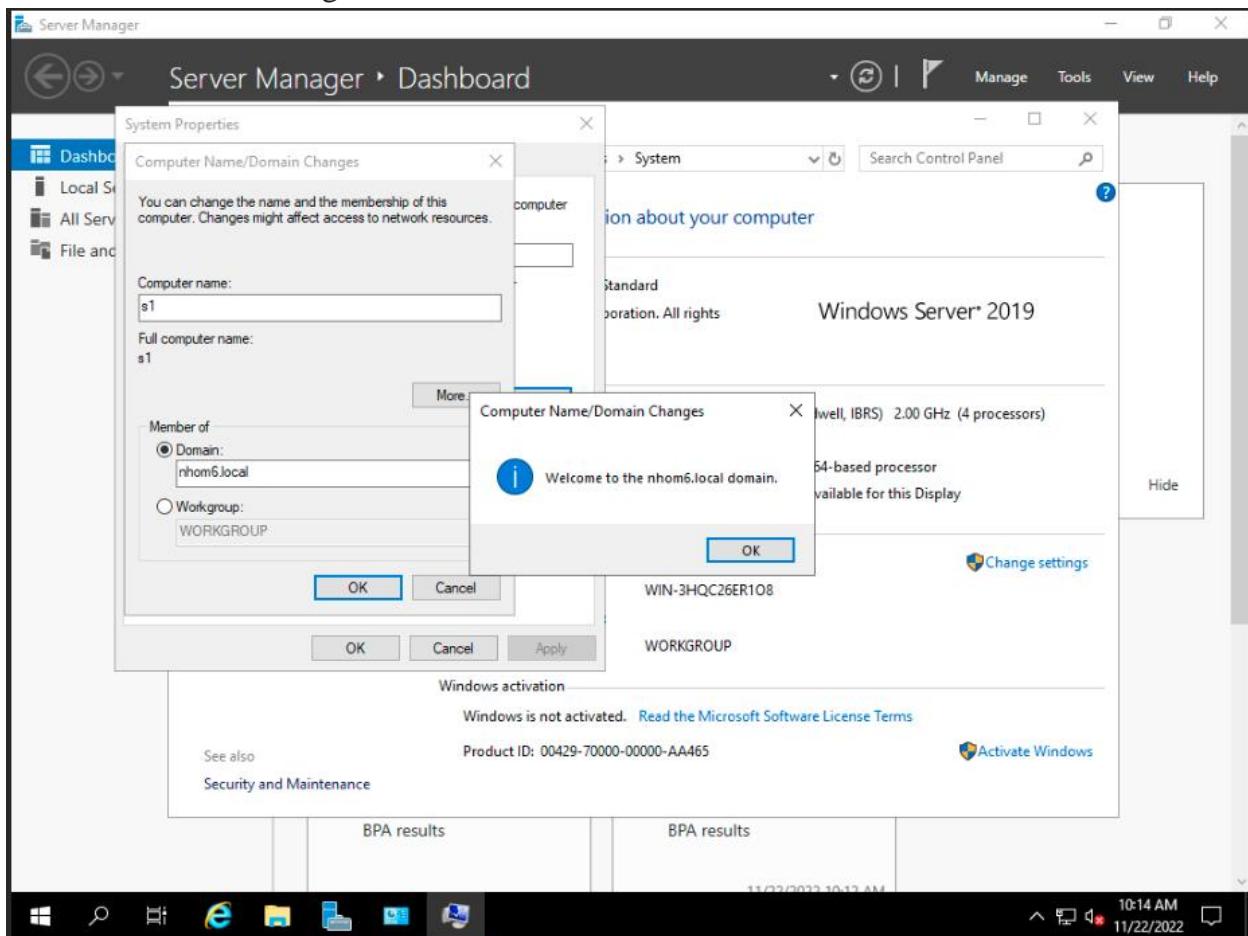


Kiểm tra kết nối tới domain (Sau khi chỉnh DNS)

```
Administrator: Command Prompt  
Microsoft Windows [Version 10.0.17763.1637]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
C:\Users\Administrator>ping nhom6.local  
  
Pinging nhom6.local [192.168.1.50] with 32 bytes of data:  
Reply from 192.168.1.50: bytes=32 time=1ms TTL=128  
  
Ping statistics for 192.168.1.50:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

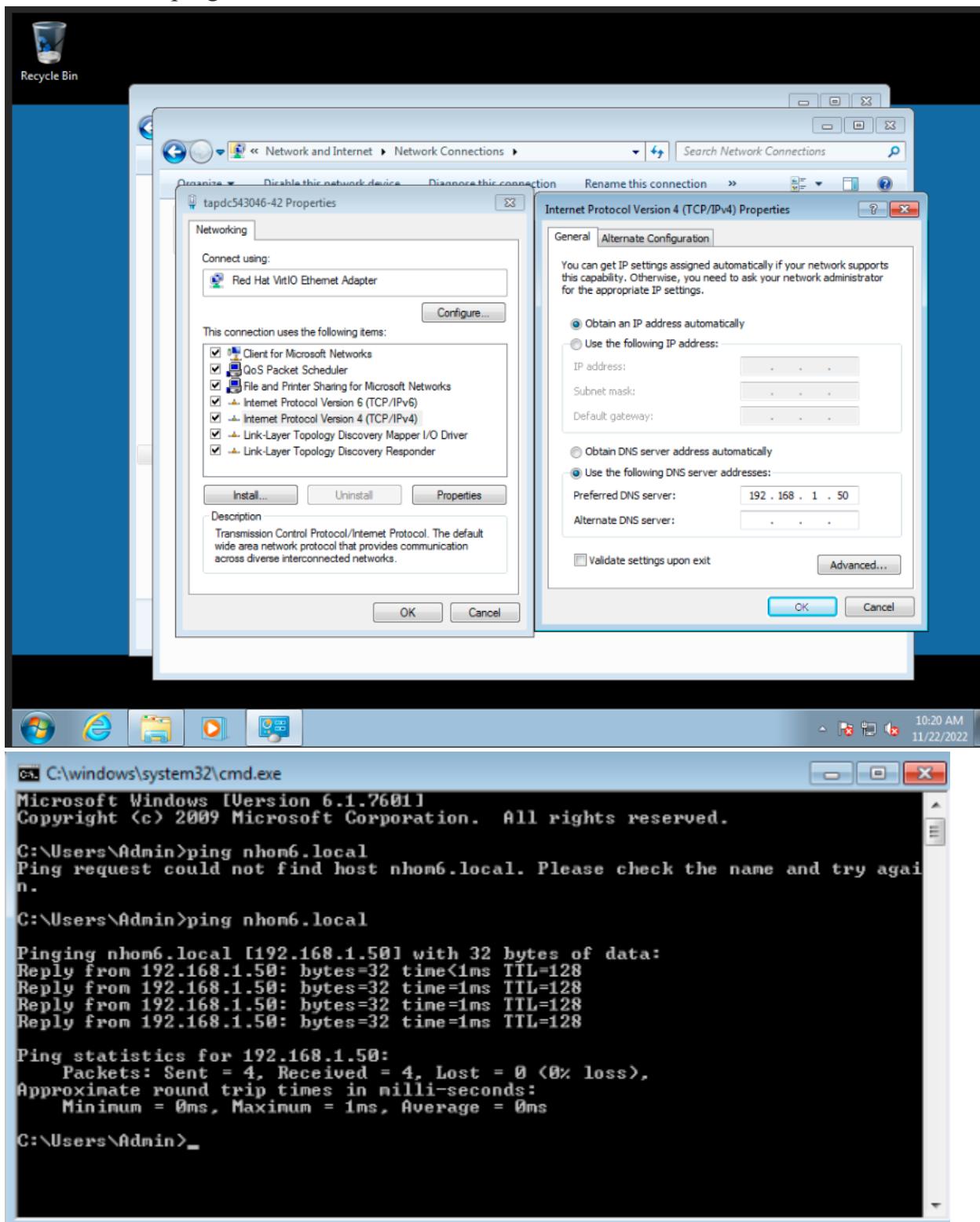


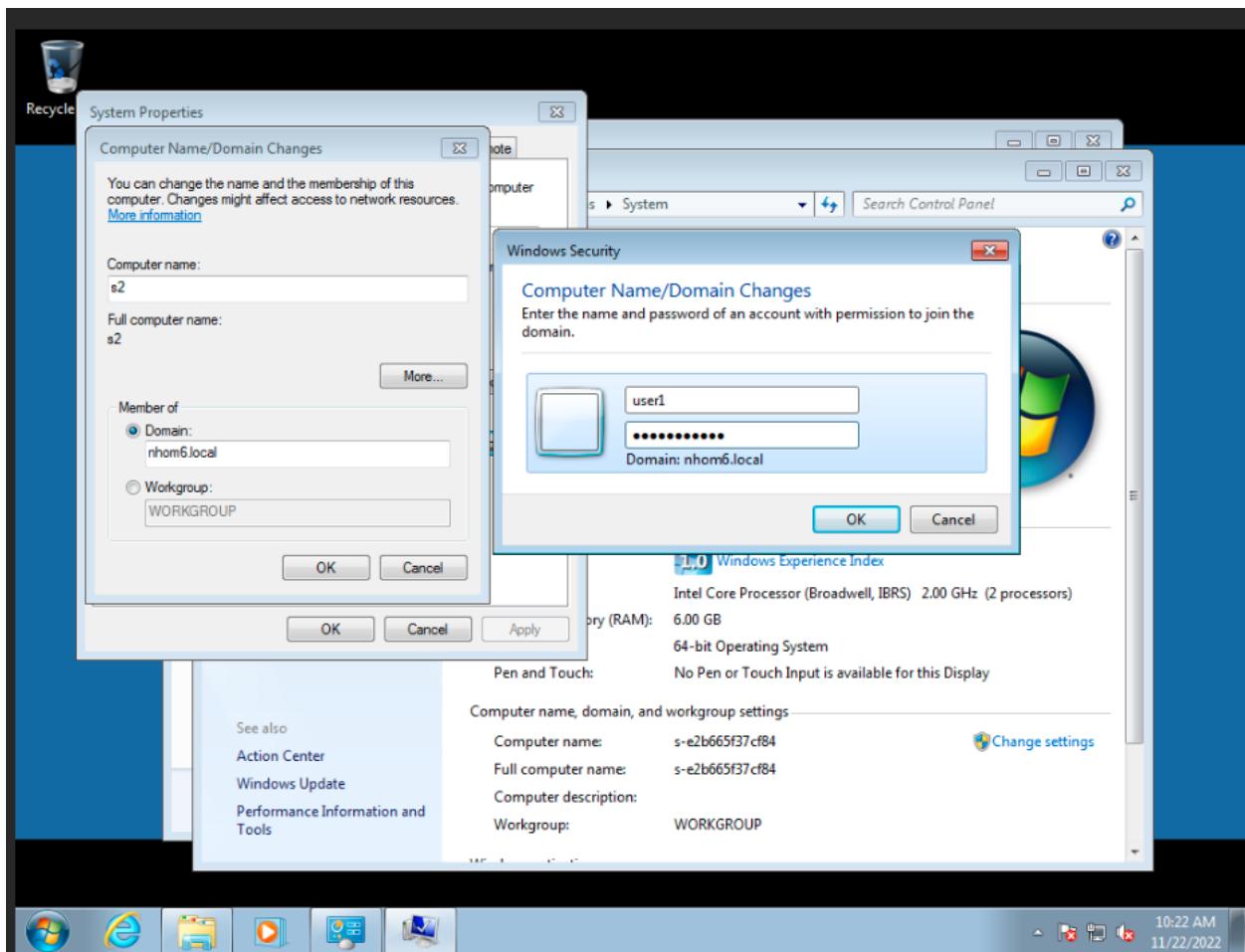
## File Server thành công thêm vào domain



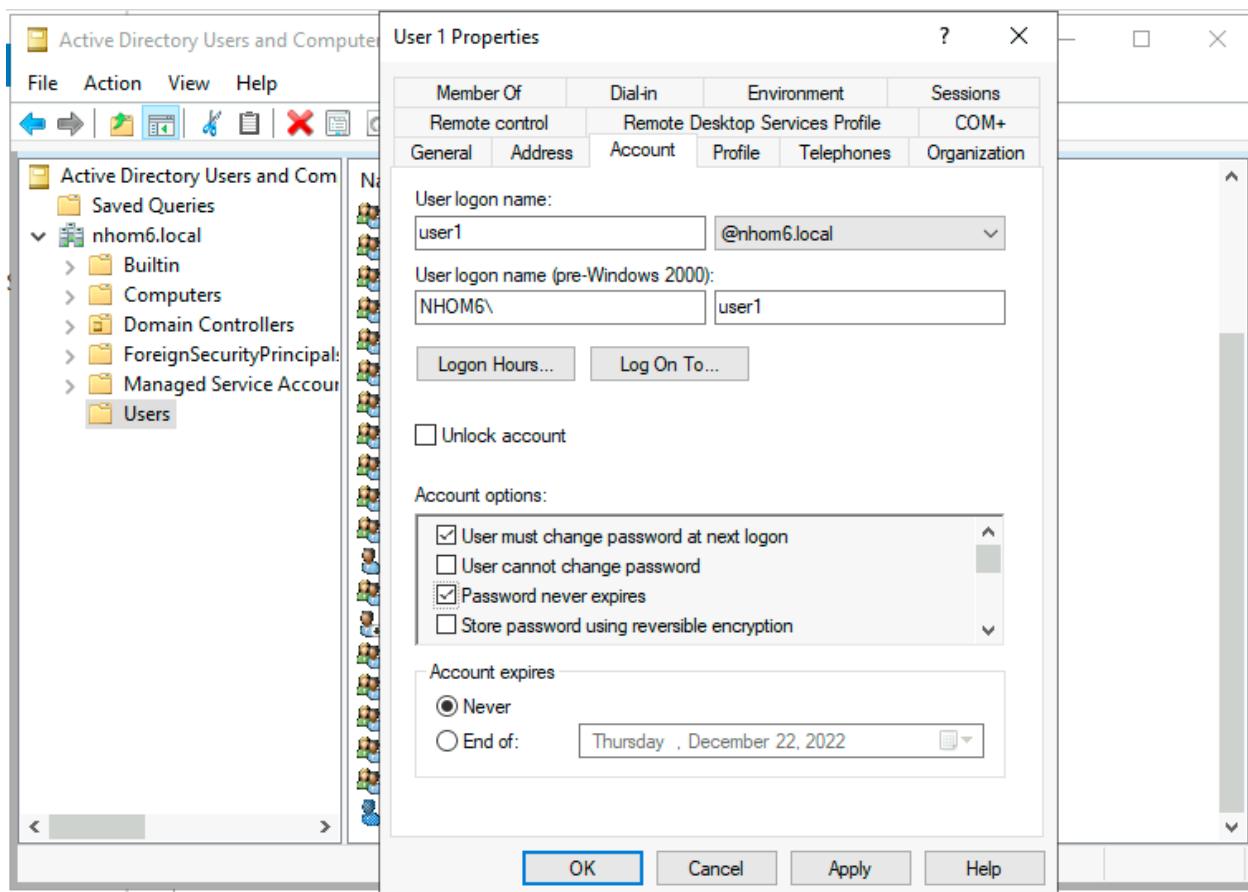
## Thêm máy client vào domain

Chỉnh DNS và ping để kiểm tra kết nối tới domain

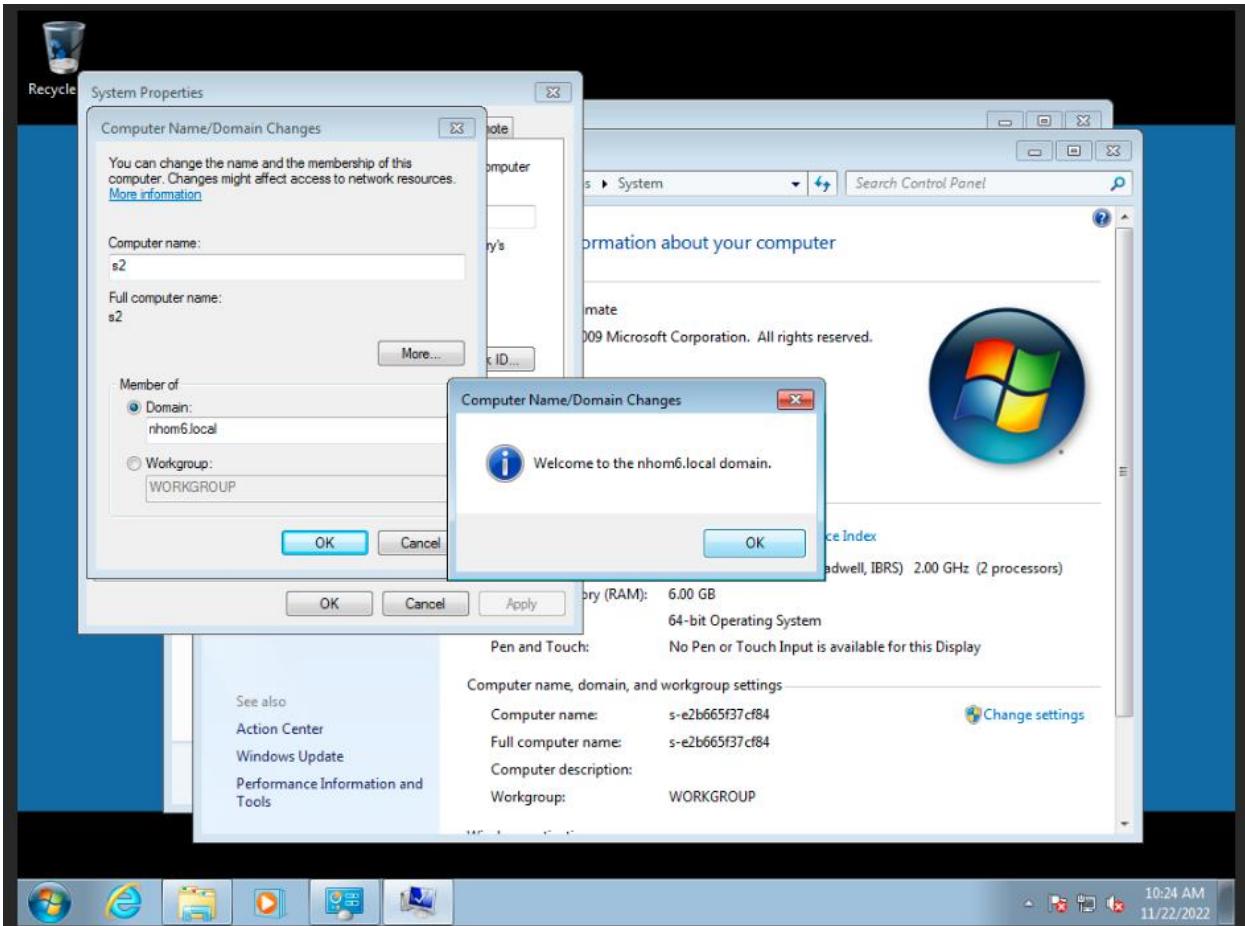




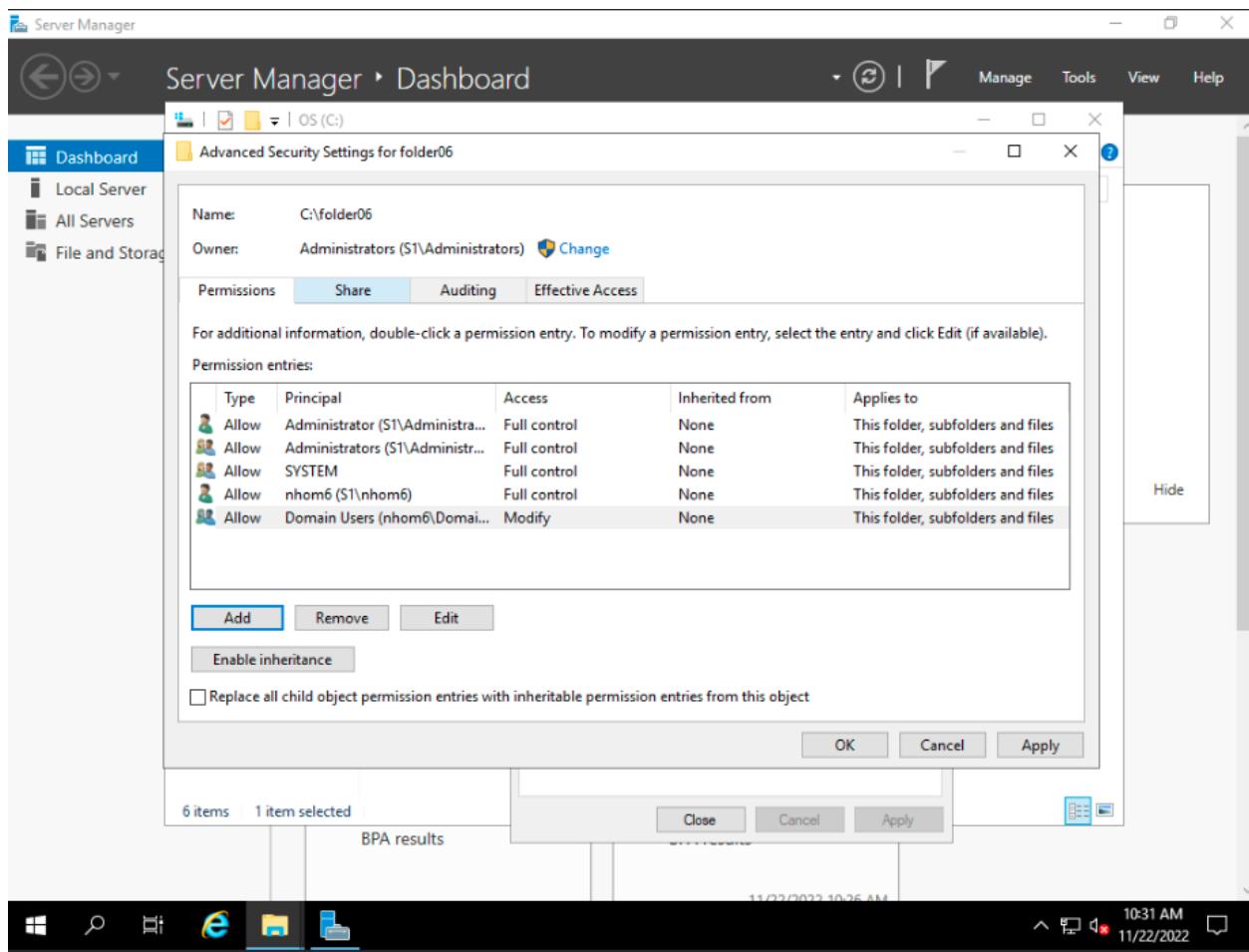
Nhớ chọn password never expired trong phần account user1 ở máy server



Thành công thêm máy client vào domain

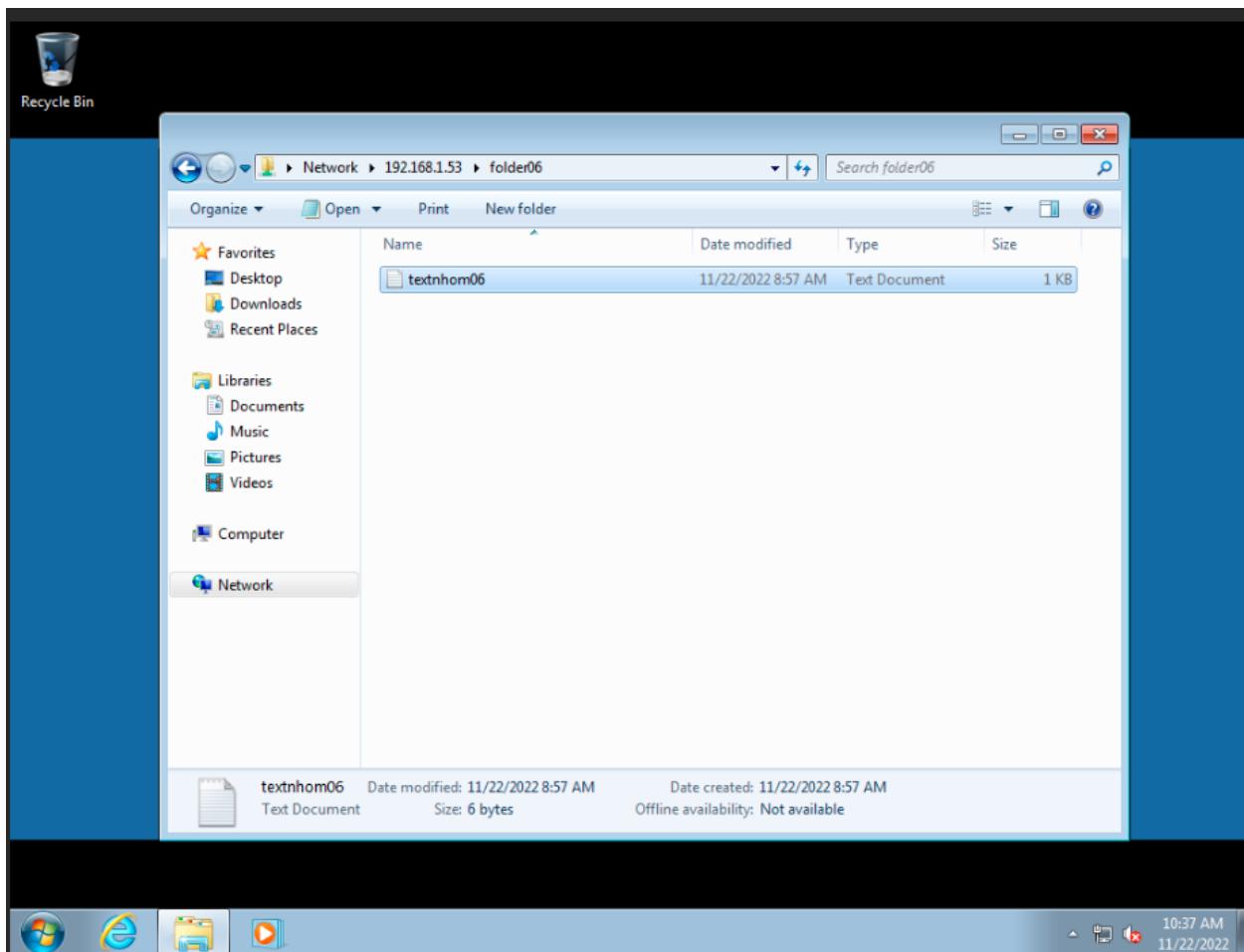


Phân quyền folder trên RODC

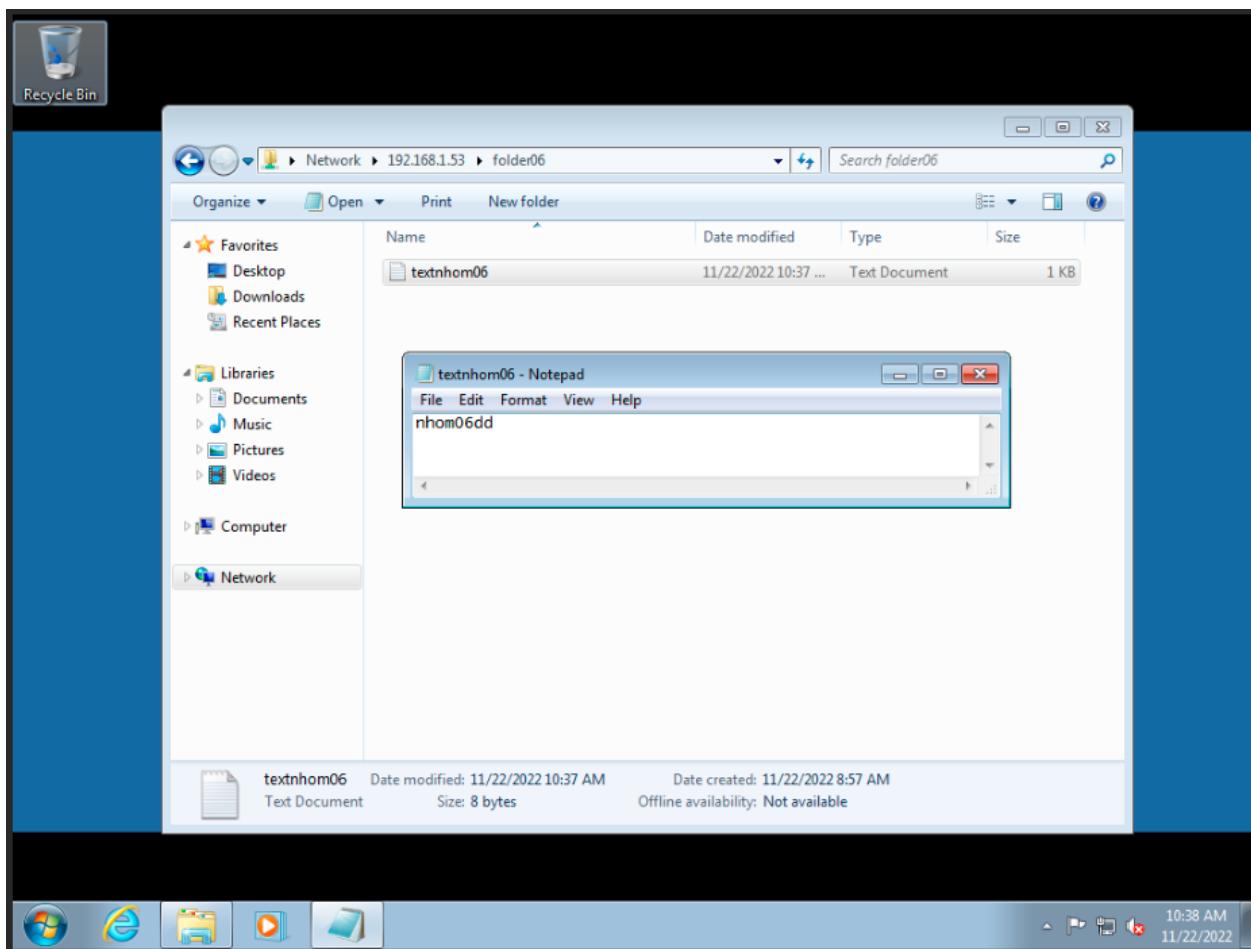


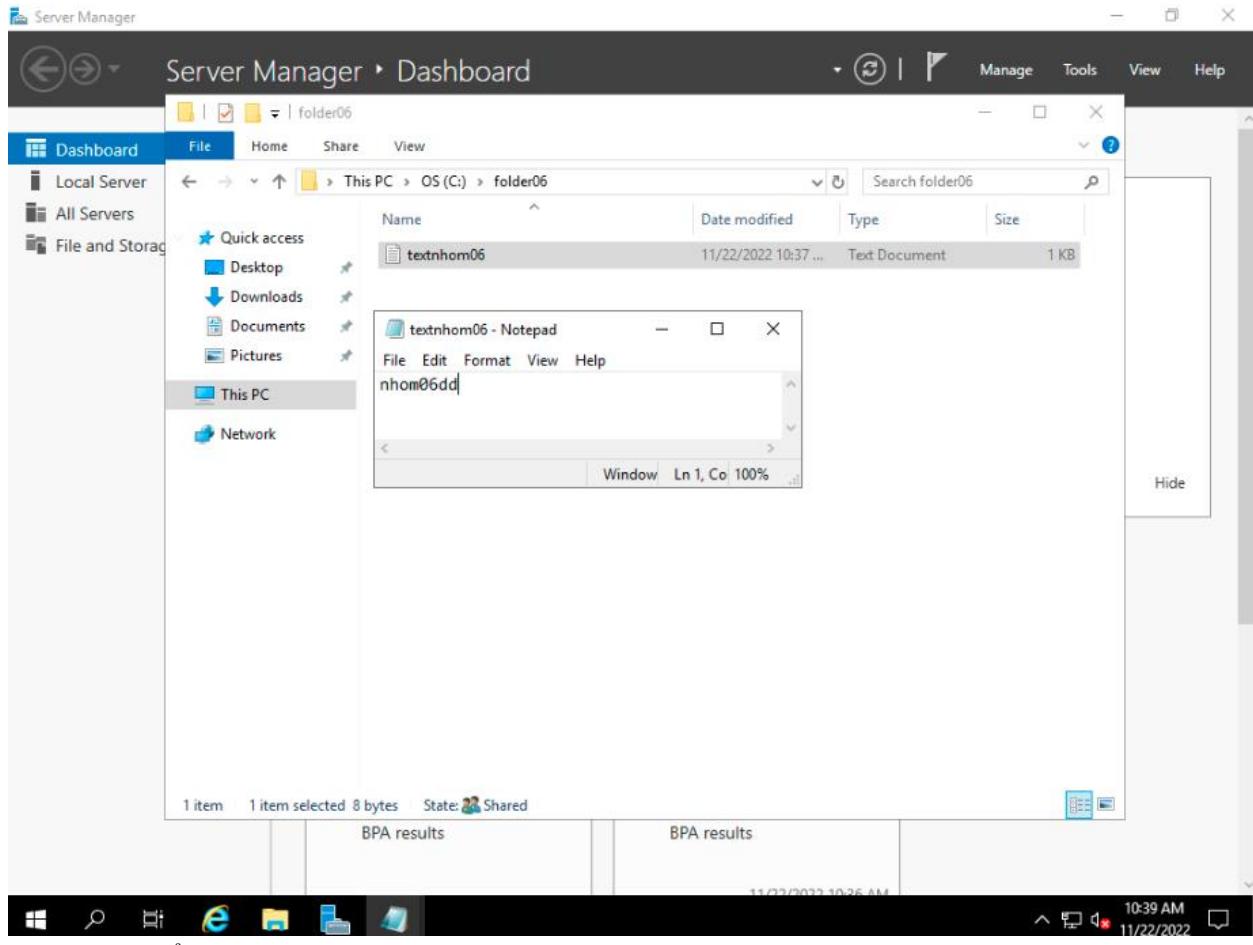
Đăng nhập với tài khoản NHOM6\user1, pass: Qq@12345678

Kết nối tới File Server



Kiểm tra các thao tác đọc ghi dữ liệu trong folder06





=> Ta có thể đọc file trong folder06 như bình thường, và khi chỉnh sửa file trong folder06, file tại folder06 ở **File Server** cũng bị thay đổi

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

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

### 3.1.1

Các domain được thêm vào Domain Controller là Additional Domain Controller.

### 3.1.2

ADC được dùng để cân bằng tải giữa các domain controller hiện có. Ngoài ra, nếu chẳng may Active Directory Domain Service (AD DS) bị lỗi thì Additional Domain controller có thể được dùng để xác thực. Từ đó đảm bảo tính liên tục của hoạt động kinh doanh.

### 3.1.3

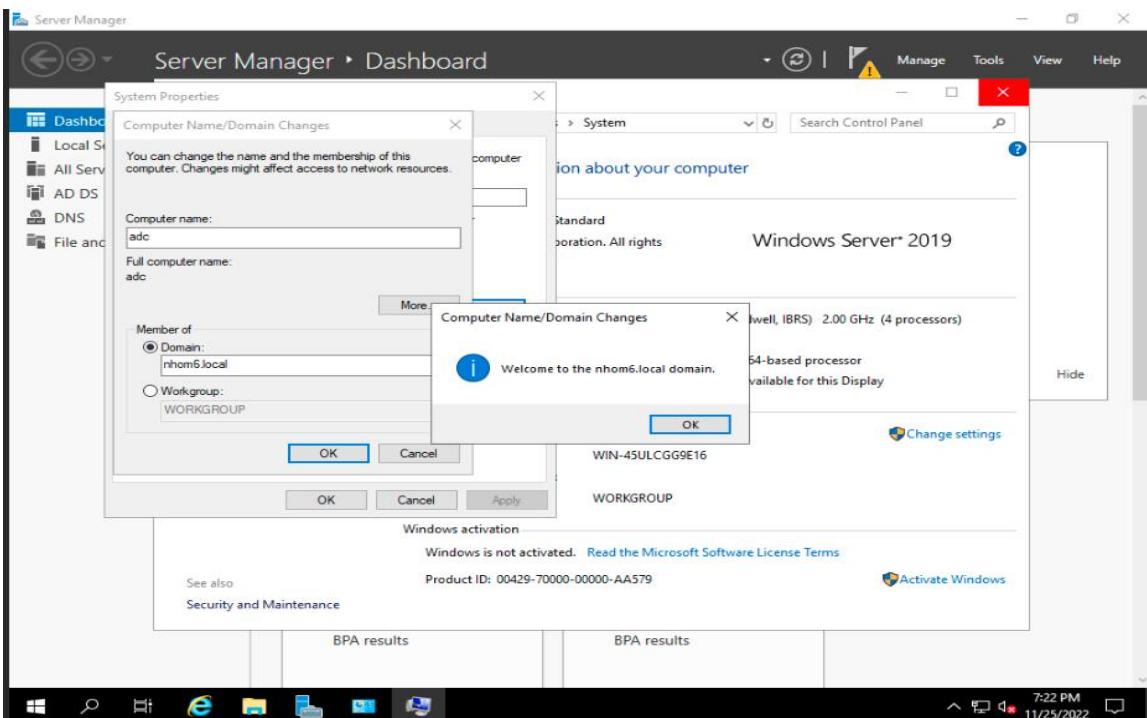
Khi nào cần sử dụng Additional Domain Controller:

- Trường hợp 1: Hệ thống có nhiều site: 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.
- Trường hợp 2: 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
- Trường hợp 3: Hệ thống có 1 site và 1 Domain Controller, hệ thống nhỏ → Dựng thêm ADC để 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

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 2016	192.168.1.52/24	192.168.1.52 192.168.1.50

Trước tiên ta sửa DNS, sửa computer name và thêm máy ADC vào domain **nhom6.local**



Ta ping thử tới nhom6.local để kiểm tra

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

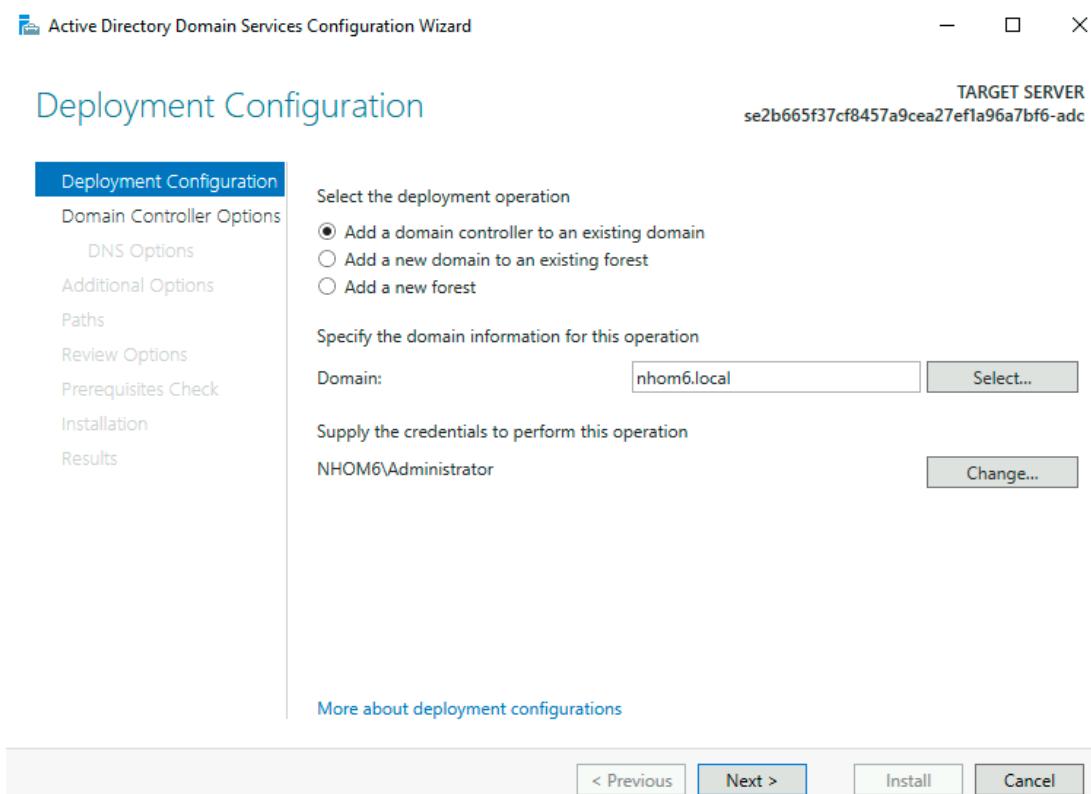
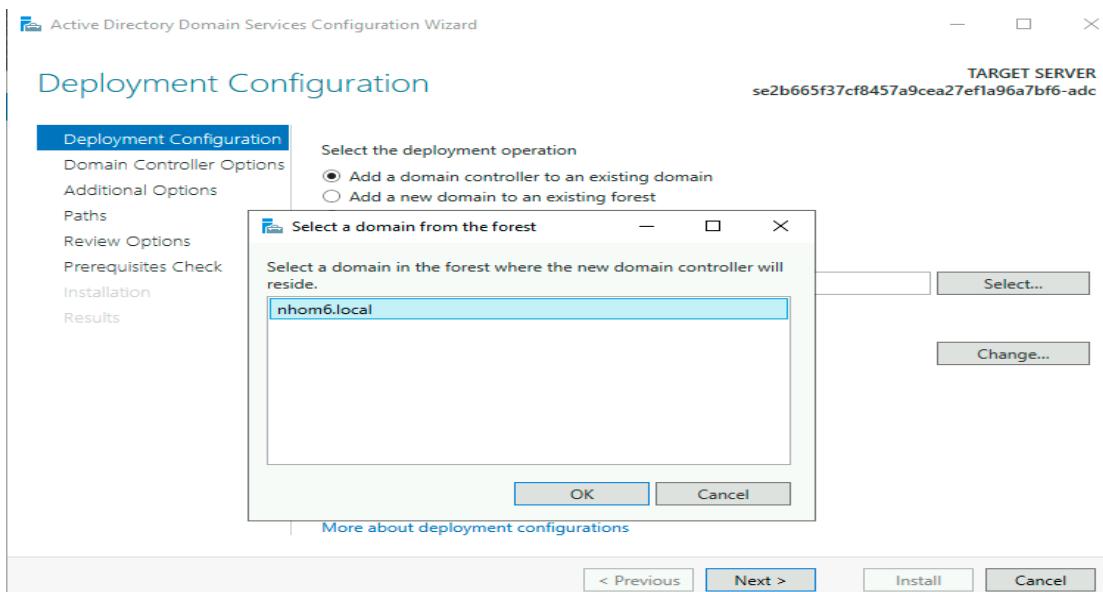
C:\Users\Administrator>ping nhom6.local

Pinging nhom6.local [192.168.1.50] with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time=2ms TTL=128
Reply from 192.168.1.50: bytes=32 time=1ms TTL=128
Reply from 192.168.1.50: bytes=32 time=1ms TTL=128
Reply from 192.168.1.50: bytes=32 time=1ms TTL=128

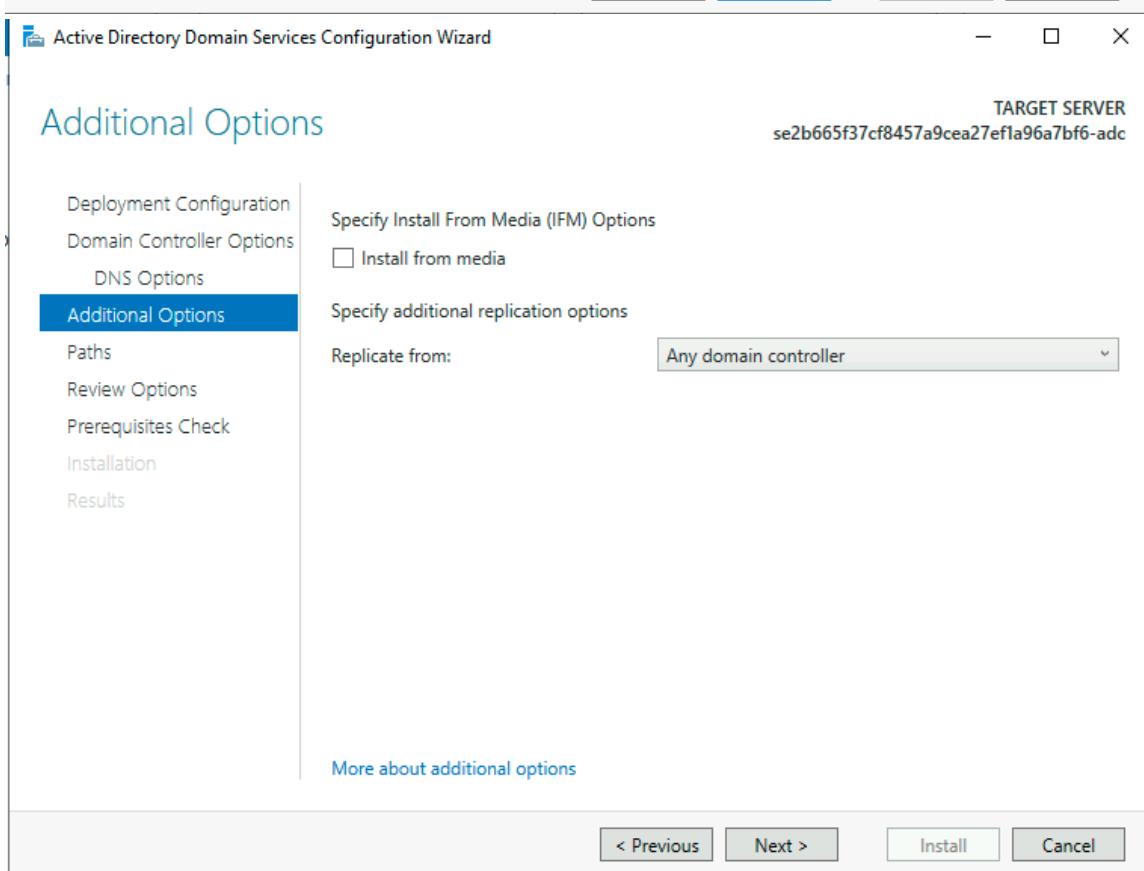
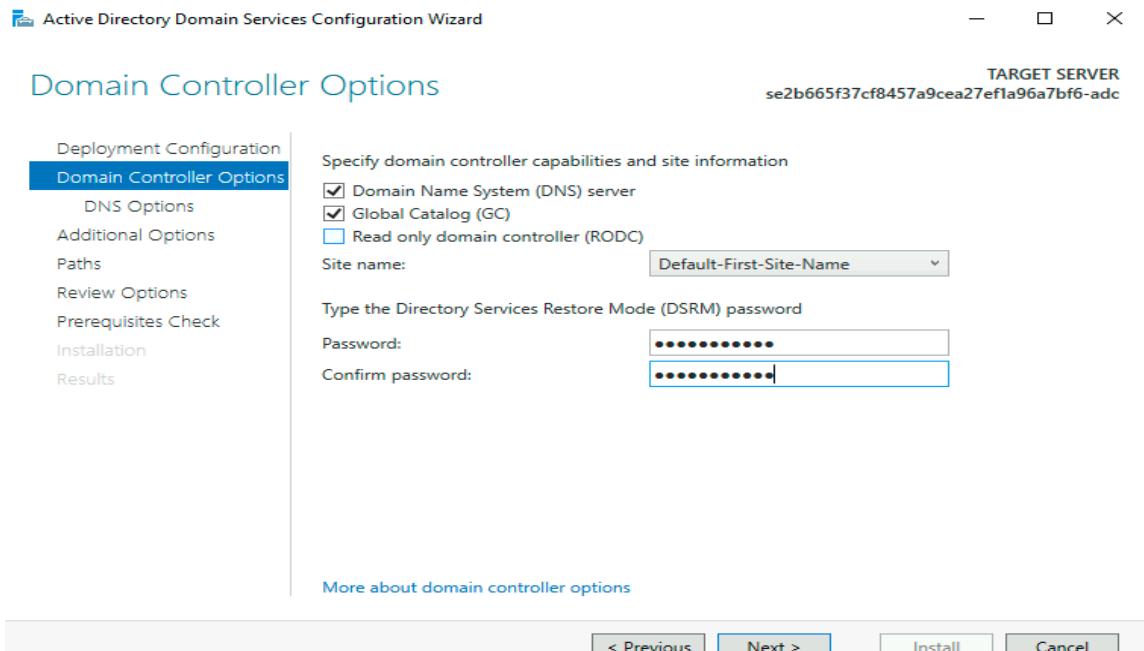
Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

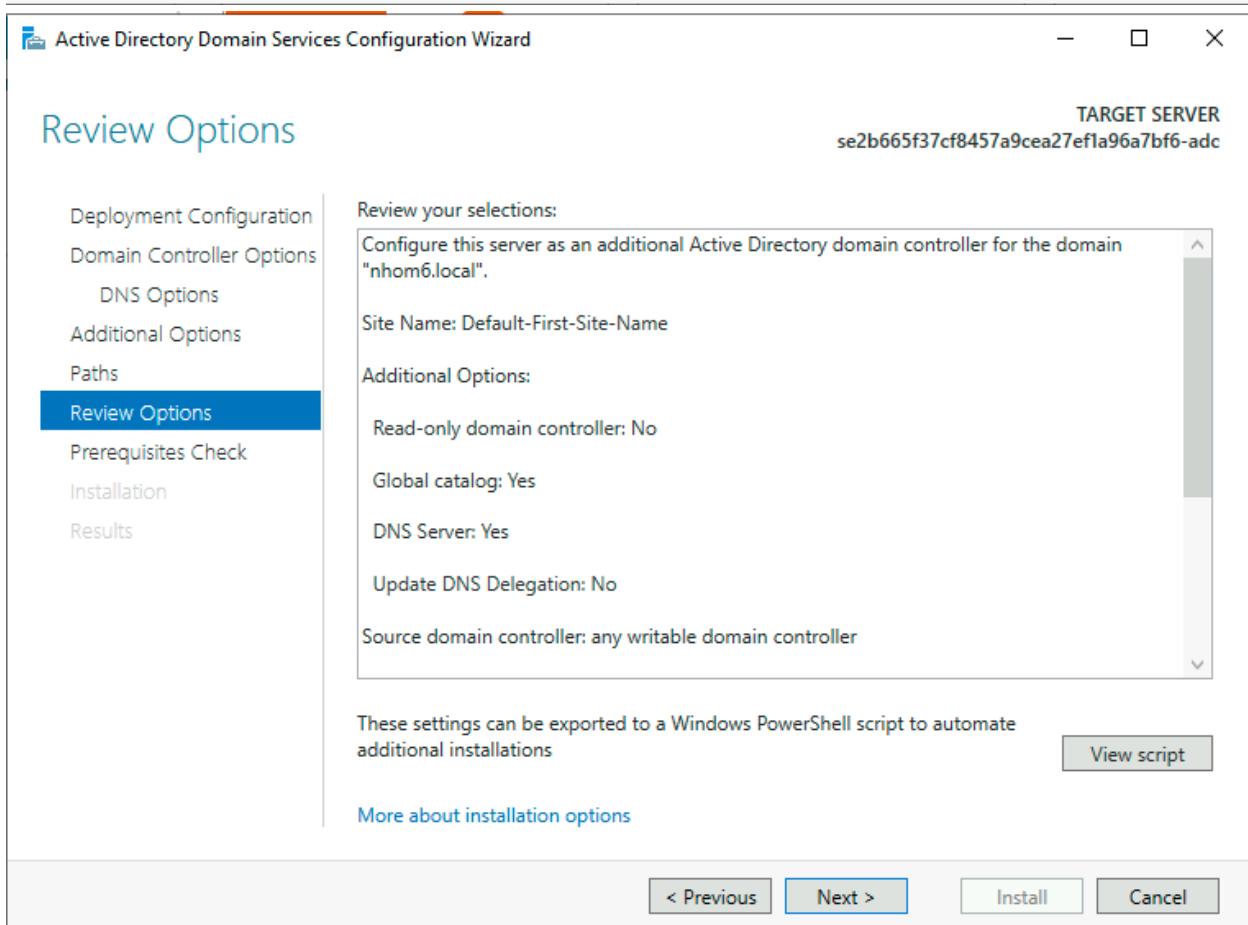
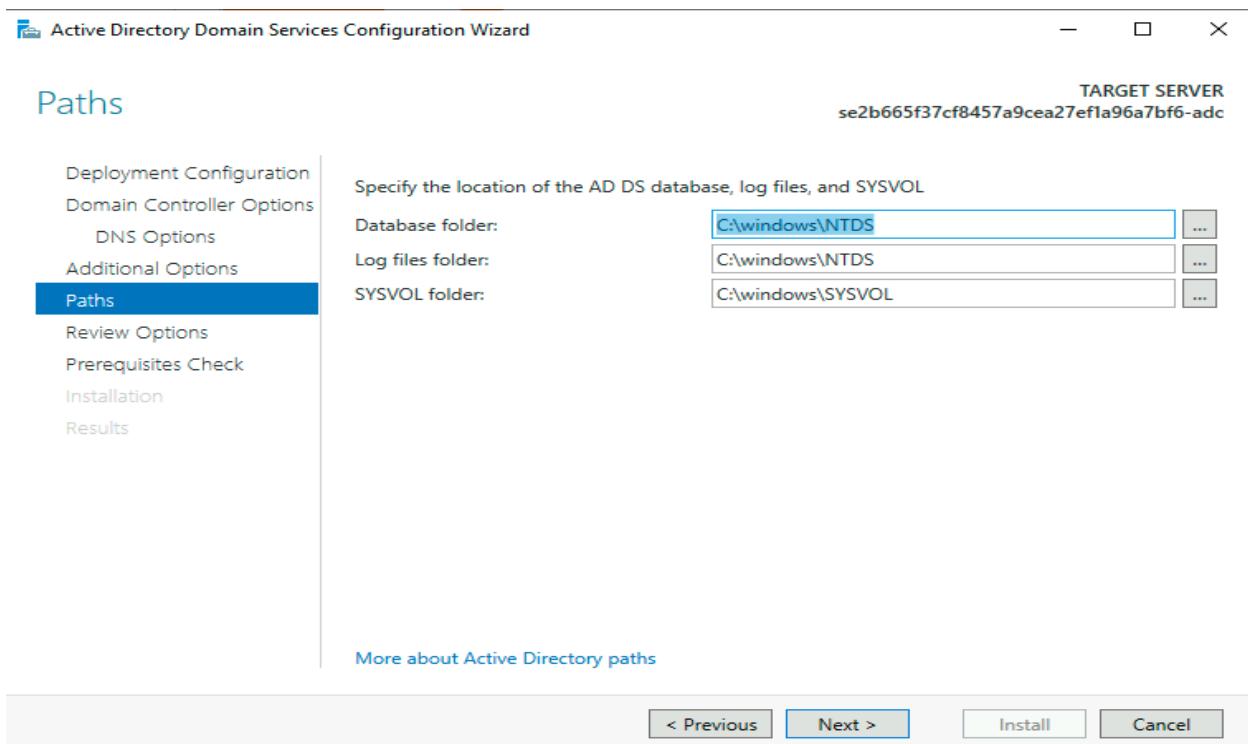
Bắt đầu các bước deploy máy thành ADC.

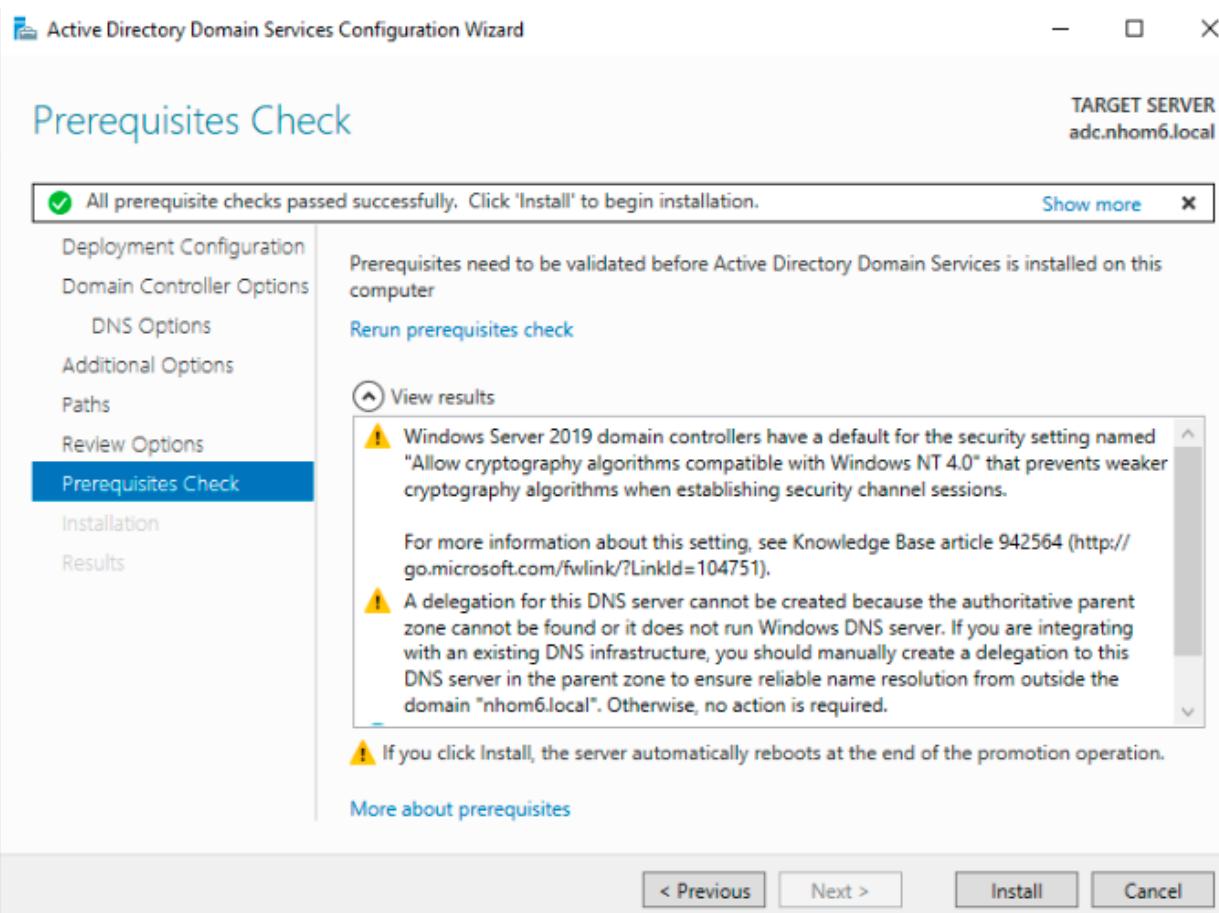
Ta chọn domain là nhom6.local, sau đó nhập username và password.



Thiết lập pass DSRM: Qq@12345678, sau đó nhấn **next** đến cuối cùng và nhấn **install**

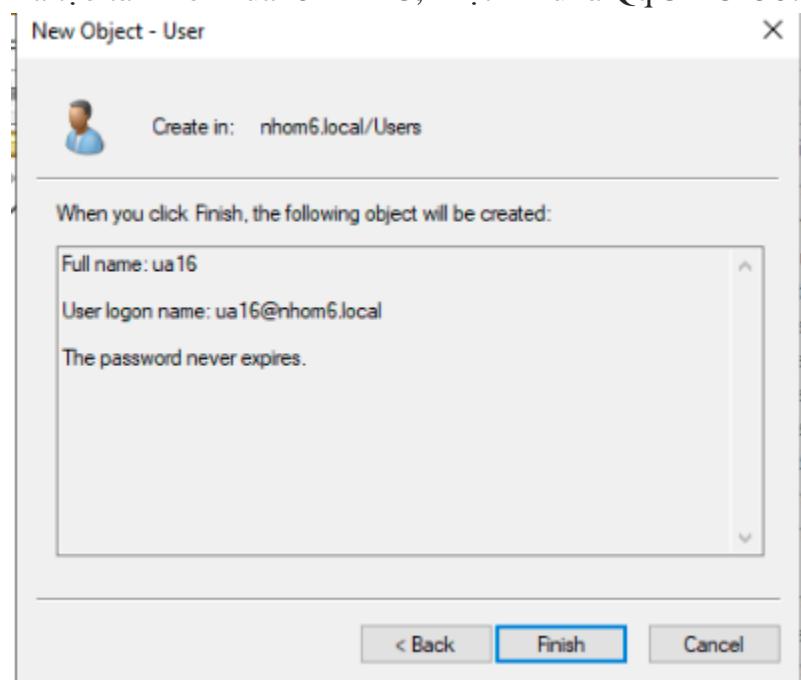




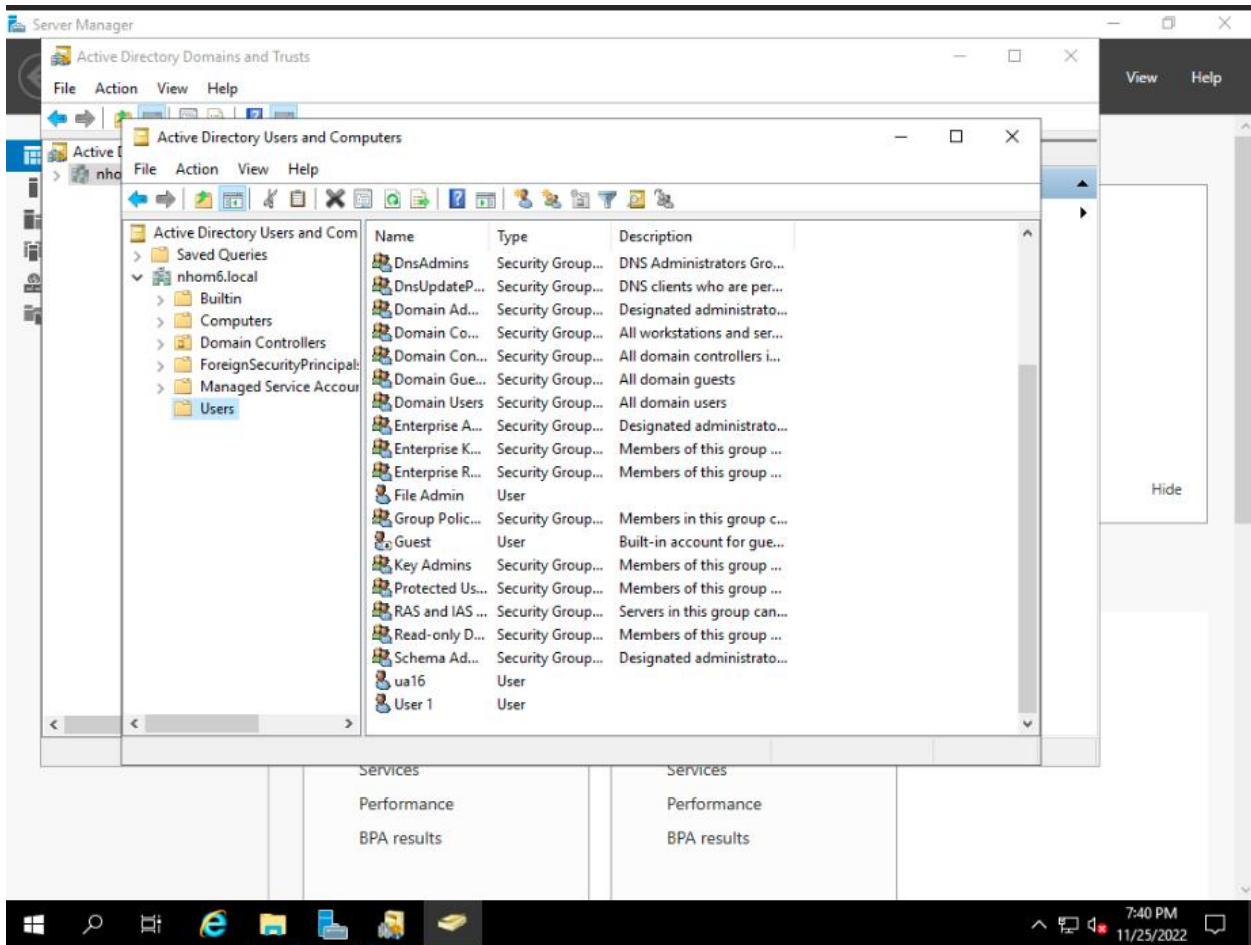


Sau đó máy sẽ tự khởi động lại

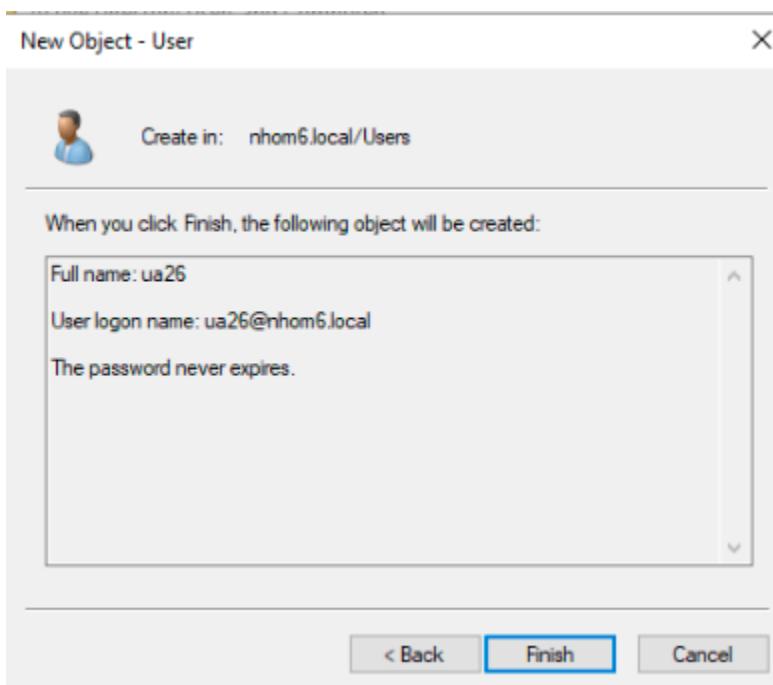
Ta tạo tài khoản ua16 ở PDC, mật khẩu là Qq@12345678



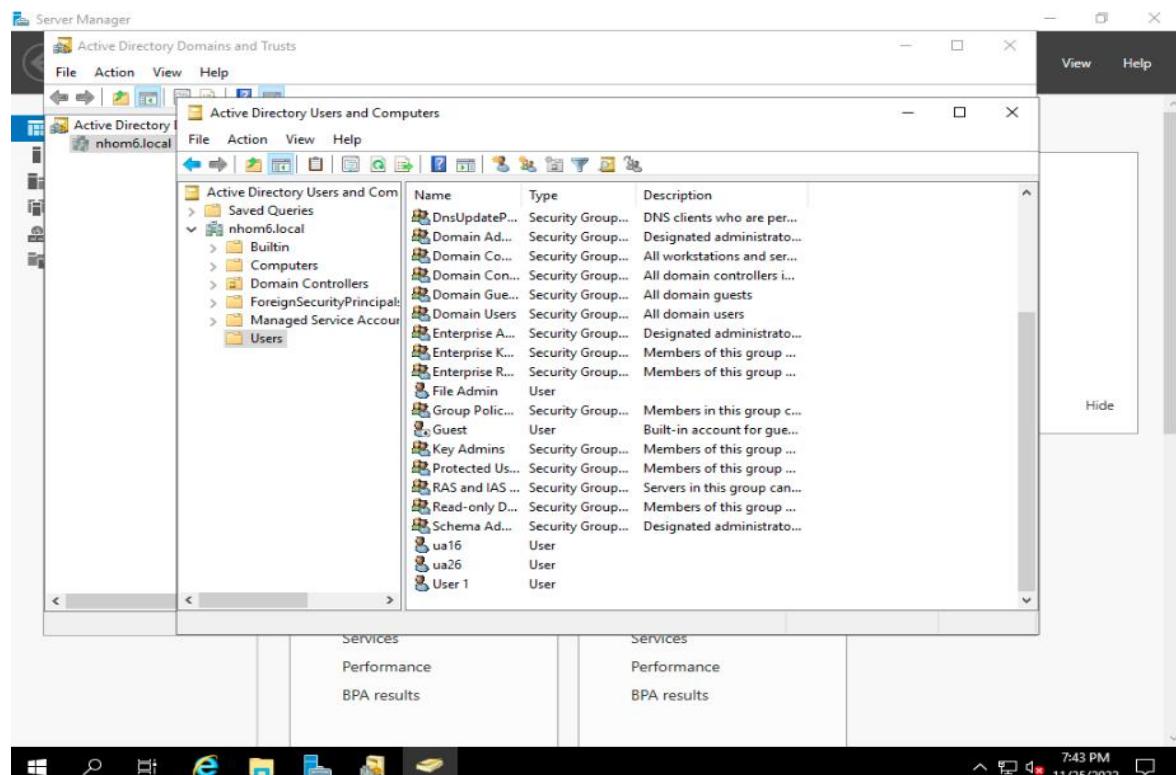
Kiểm tra lại trên máy ADC



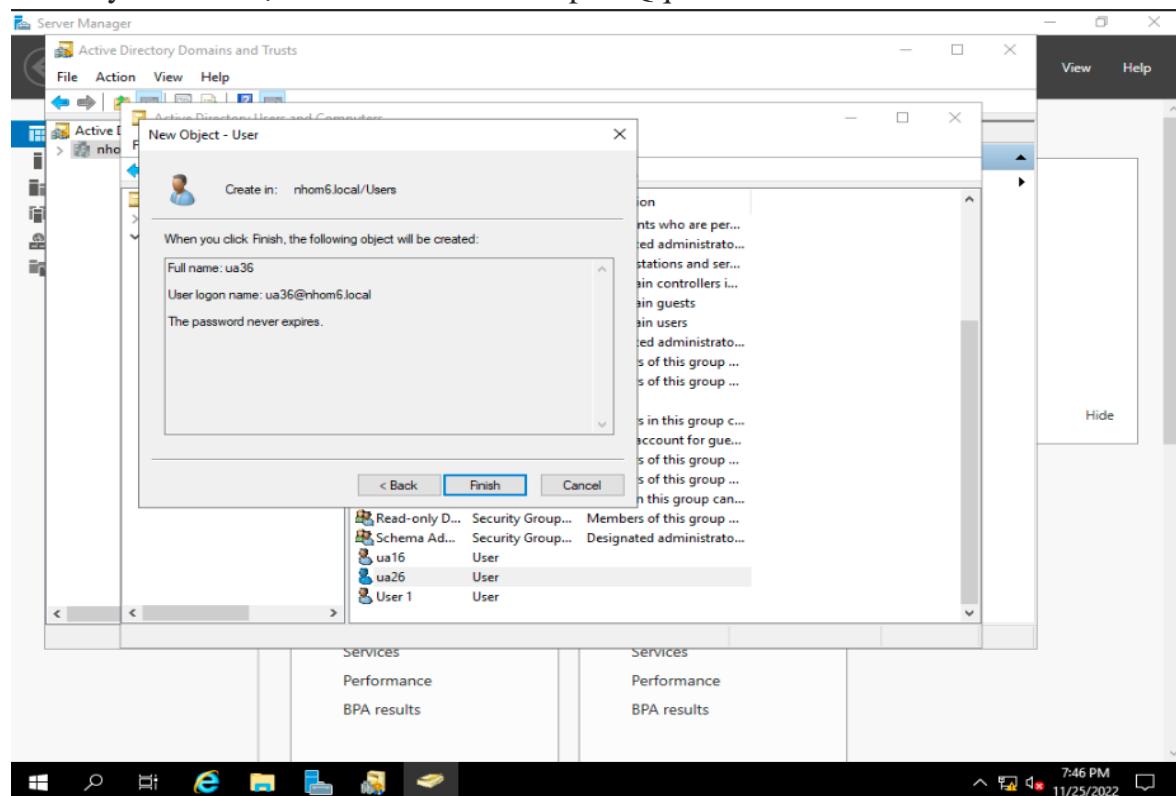
Tạo tài khoản ua26 trên máy ADC, mật khẩu là Qq@12345678



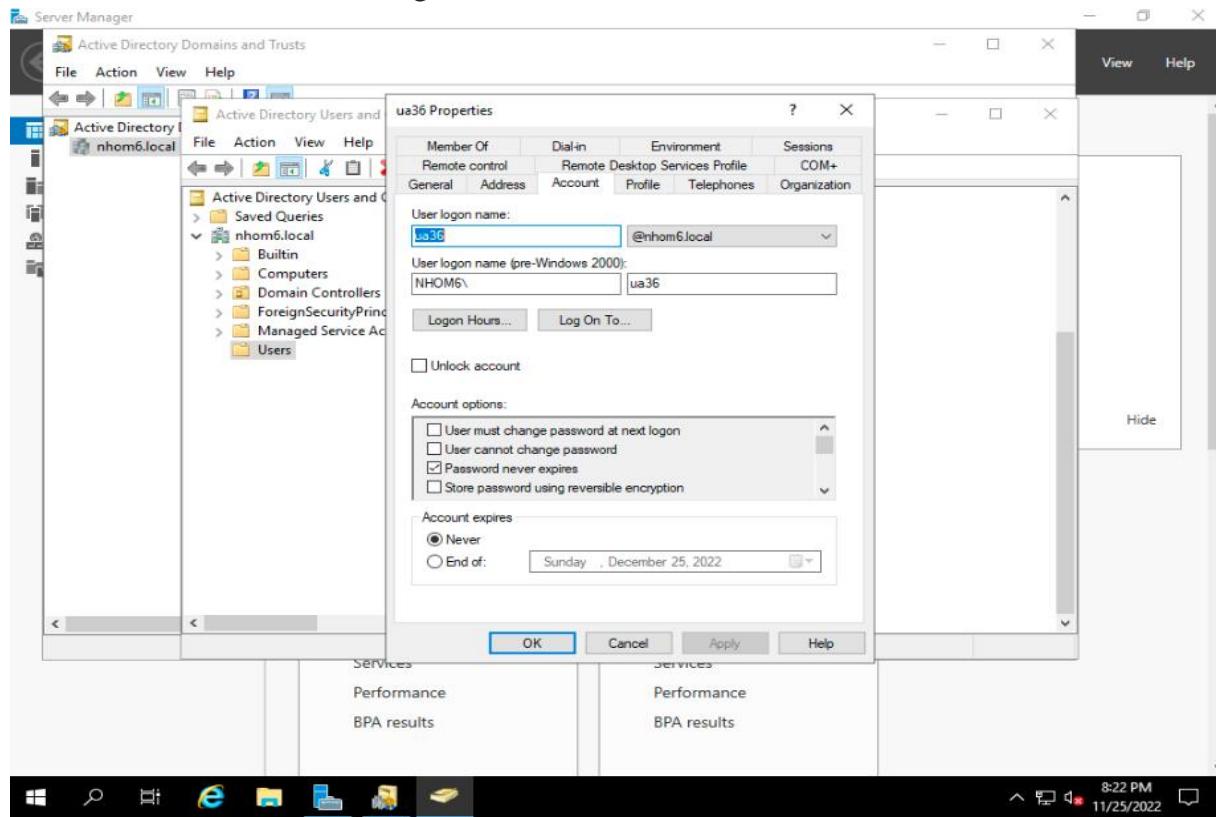
Và kiểm tra lại trên máy PDC



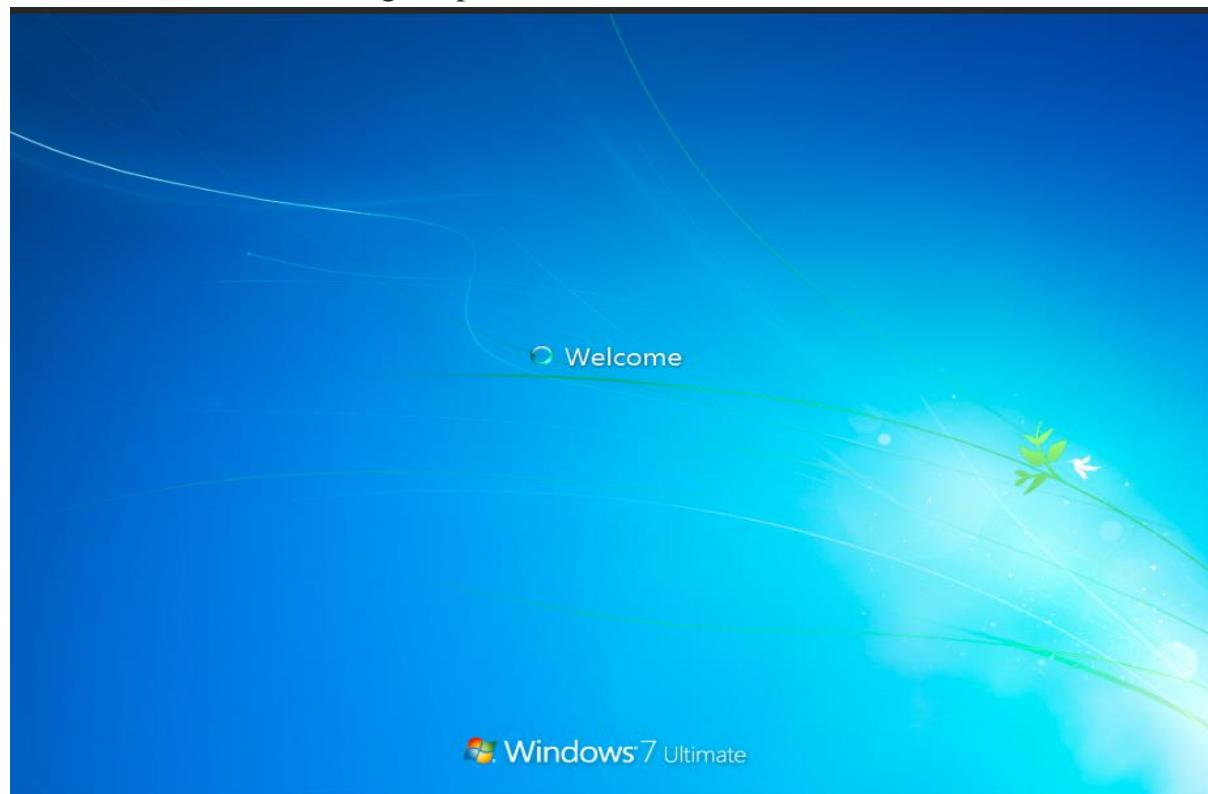
Tắt máy PDC và tạo tài khoản ua36 với passQq@12345678



Mở lại PDC và kiểm tra thông tin ua36



Tắt PDC, mở client và đăng nhập với tài khoản ua26



Ta thấy đăng nhập thành công

**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?

#### 4.1.1

Read-Only Domain Controller (ADC) là 1 dạng mới của Domain Controller có từ Windows Server 2008 . Với RODC doanh nghiệp có thể dễ dàng triển khai 1 domain controller tại những vị trí bảo mật không đảm bảo .

#### 4.1.2

RODC không thể tự thêm dữ liệu vào mà chỉ có thể đọc được dữ liệu từ một Primary Domain Controller (PDC) thông qua cơ chế Replication giữa các Domain Controller của Microsoft.

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.

#### 4.1.3

Cần 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.

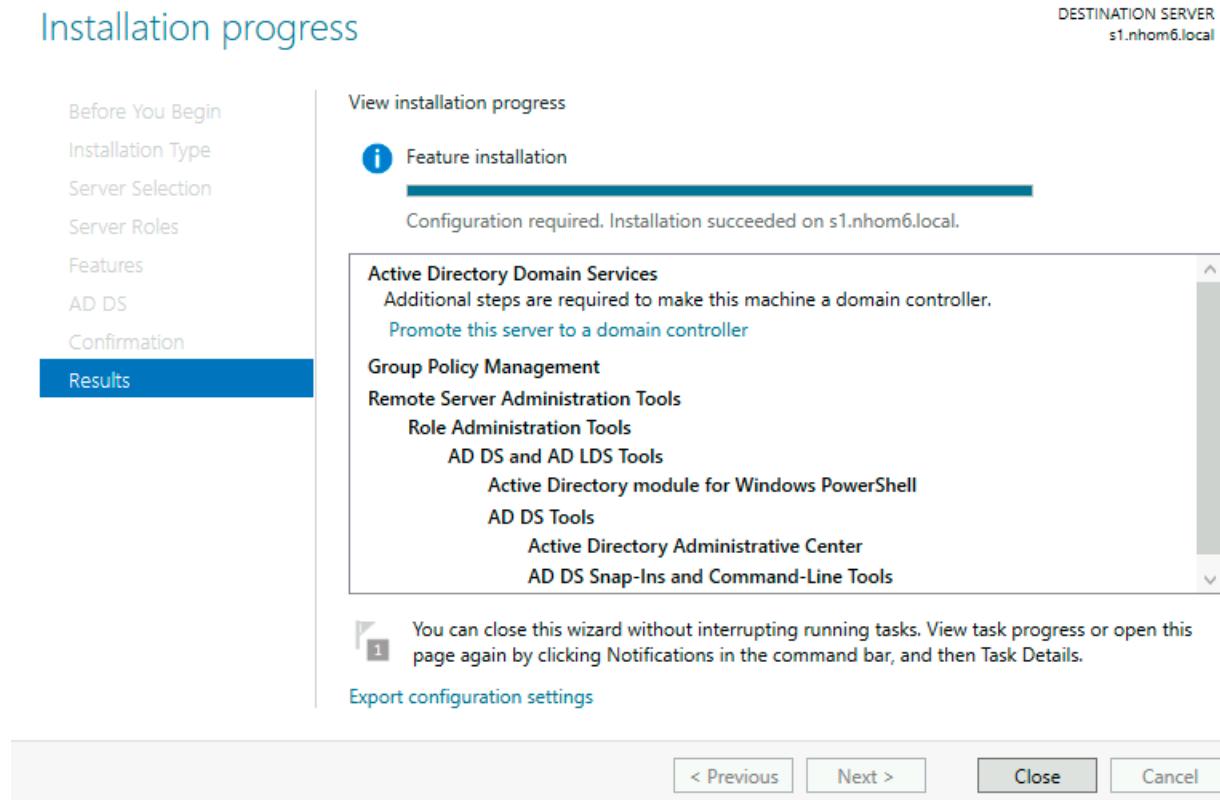
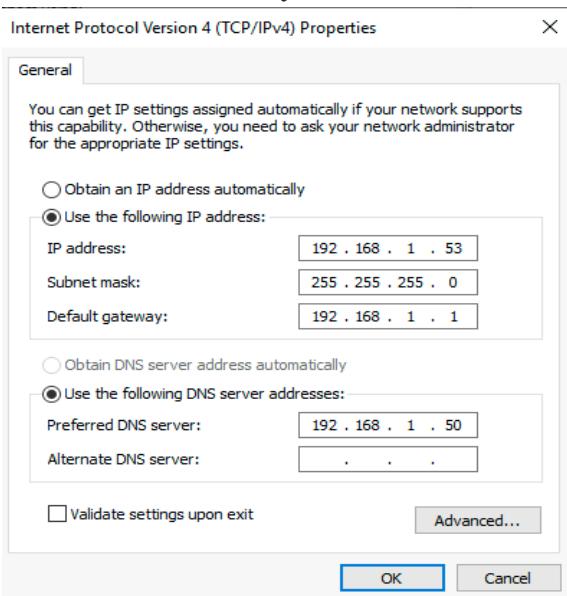
Vì RODC không thể thay đổi bất cứ thứ gì trong cơ sở dữ liệu Active Directory, và nếu chúng ta không để RODC lưu trữ thông tin về tài khoản được tạo bản sao đến thì cho dù đánh cắp được RODC thì cũng không thể sử dụng thông tin mà họ lấy được từ nó.

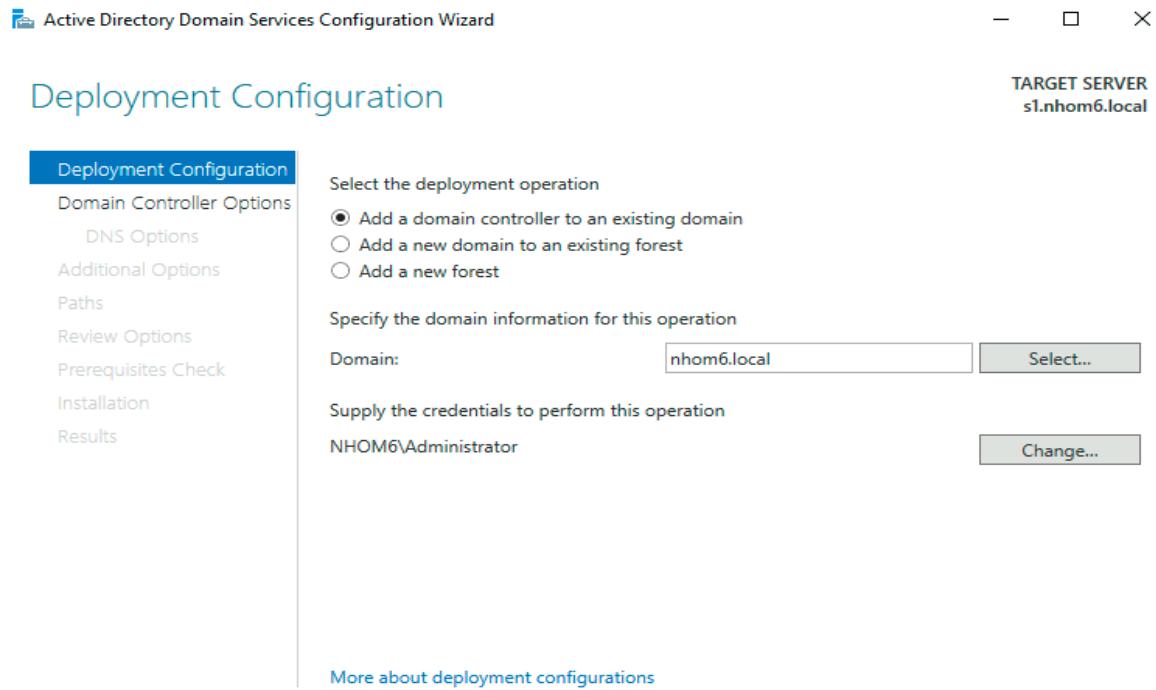
**Yêu cầu 4.2** Sinh viên triển khai mô hình Read-Only Domain Controller theo yêu cầu bên dưới.

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7	192.168.1.200/24	192.168.1.53 192.168.1.50
Primary DC	Windows Server 2019	192.168.1.50/24	192.168.1.50 192.168.1.53
Read-Only DC	Windows Server 2019	192.168.1.53/24	192.168.1.53 192.168.1.50

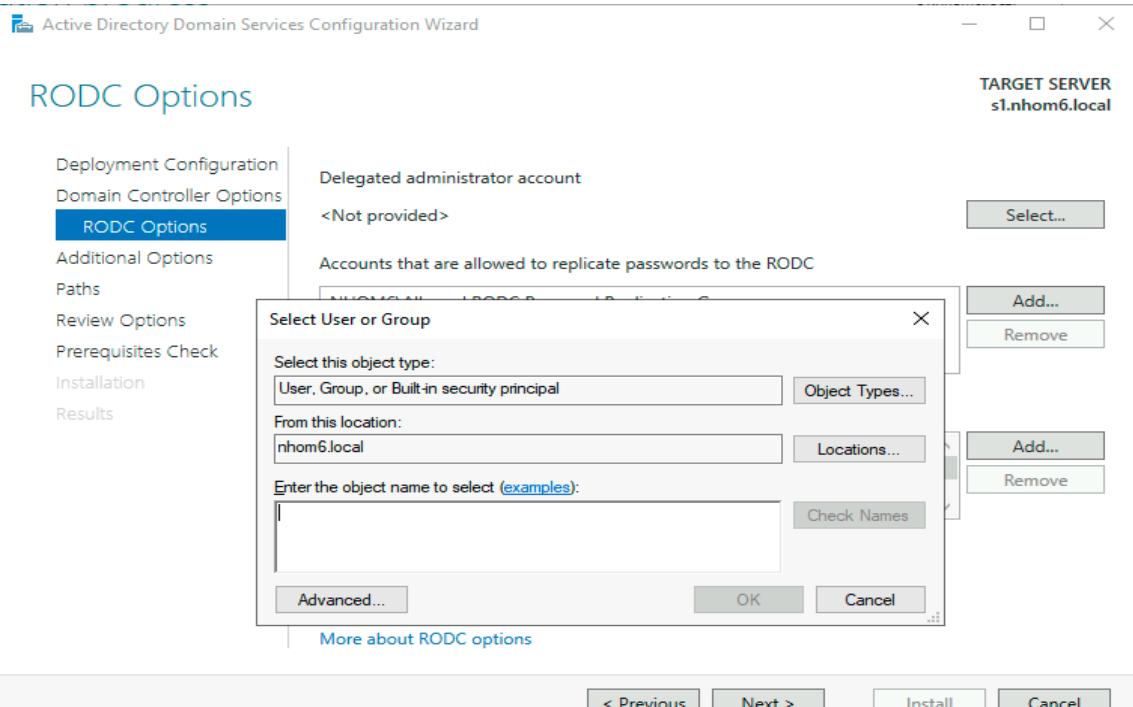
Client: passadmin: NHOM6\Administrator : AD@pass123

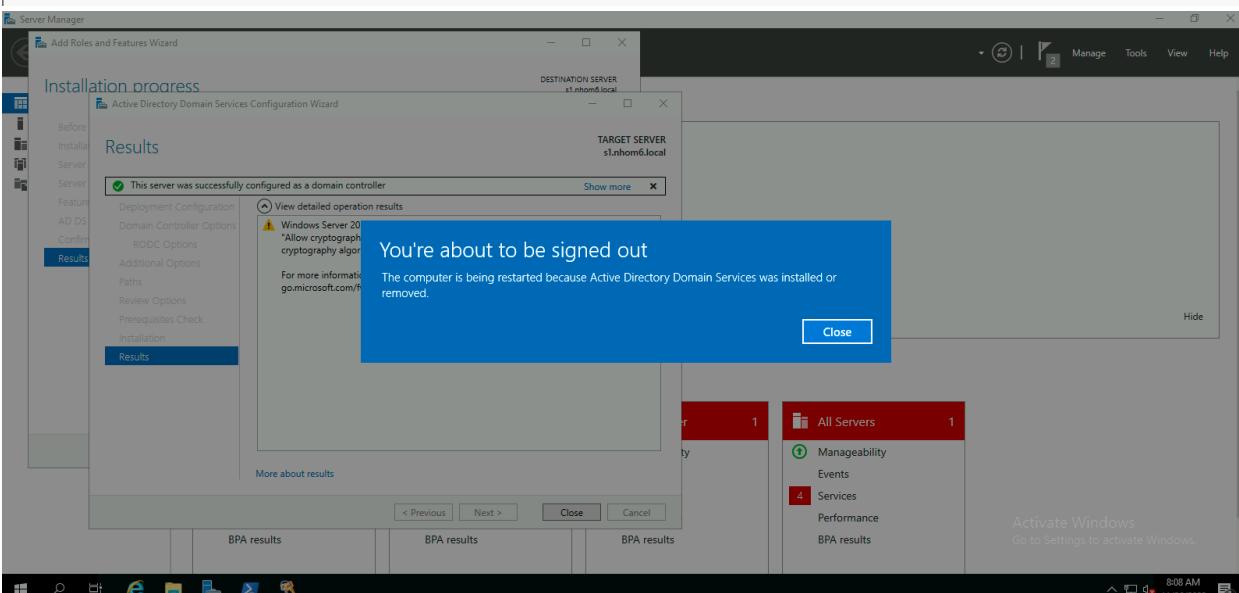
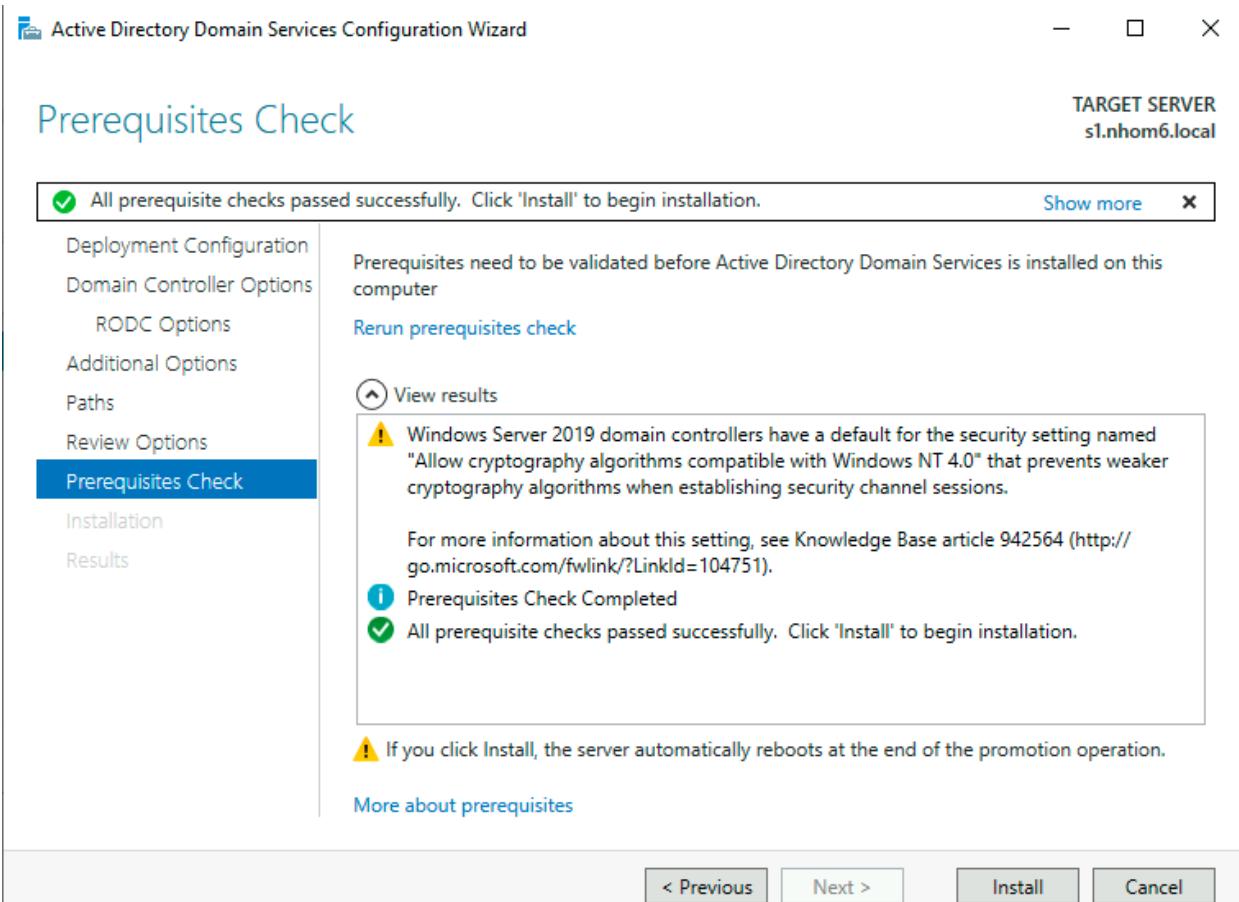
Ta sẽ làm việc ở máy RODC trước:



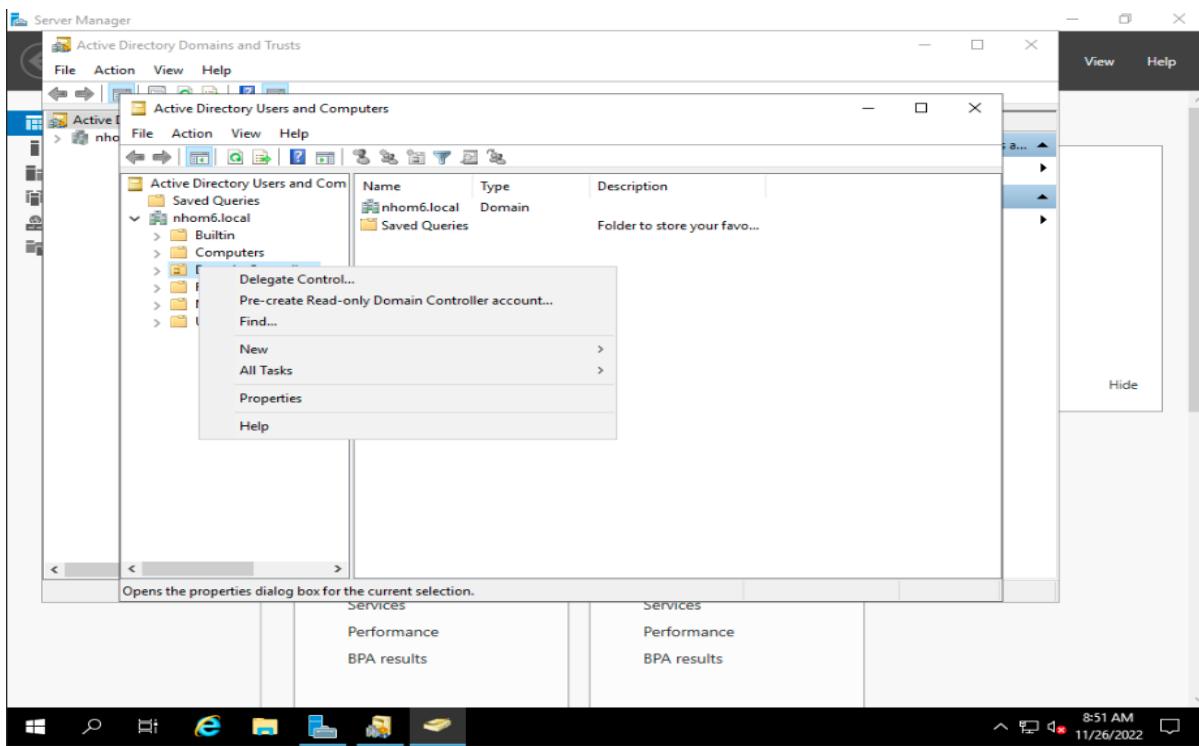


Đăng nhập với NHOM6\Administrator và pass ADC@pass123 để kết nối tới domain

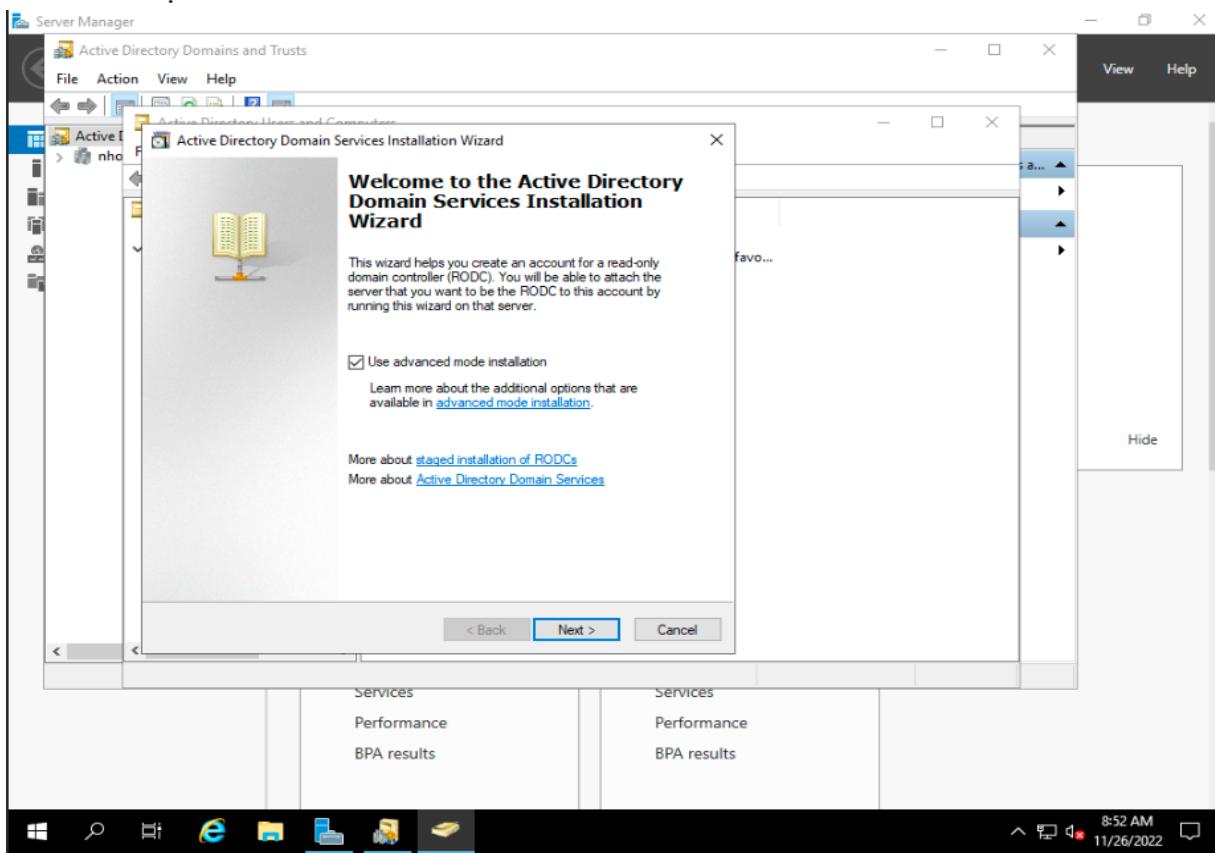




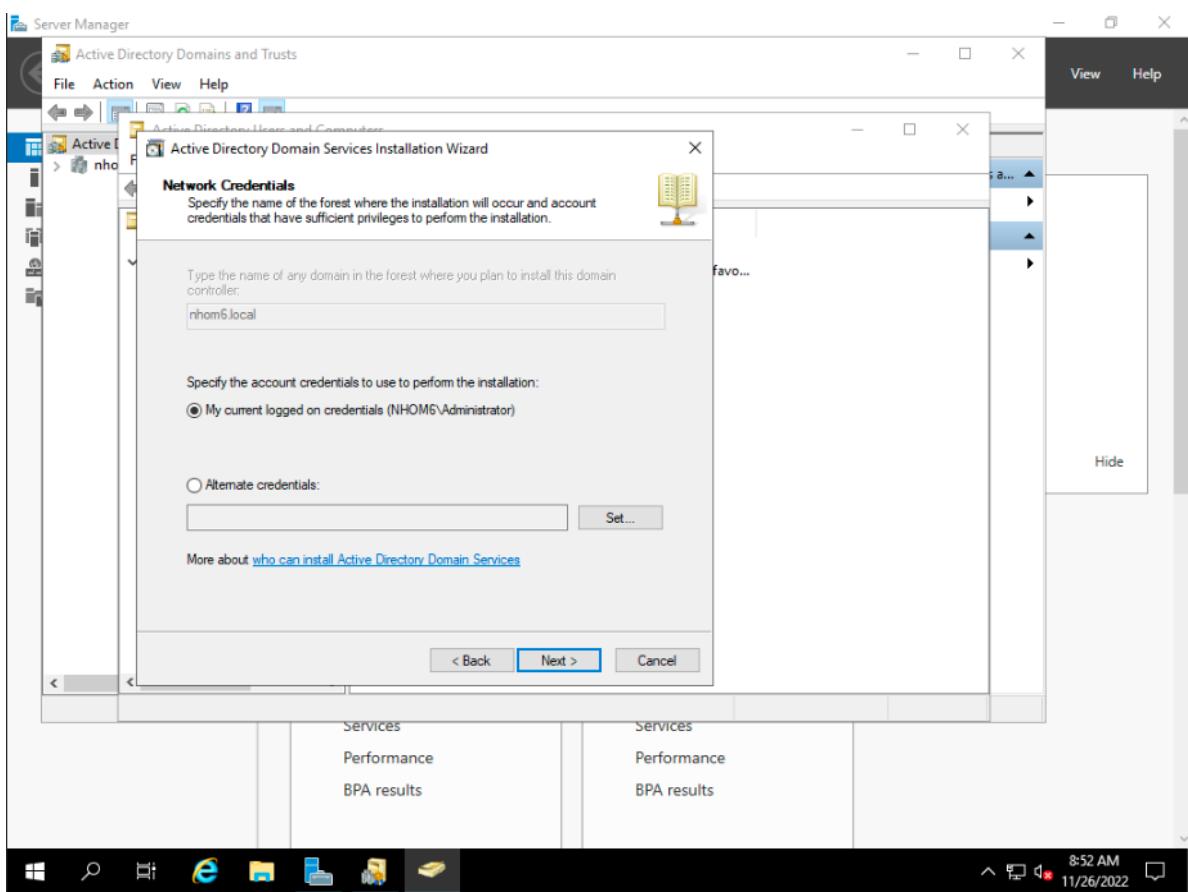
Sau đó ta login lại vào bằng acc NHOM6\Administrator



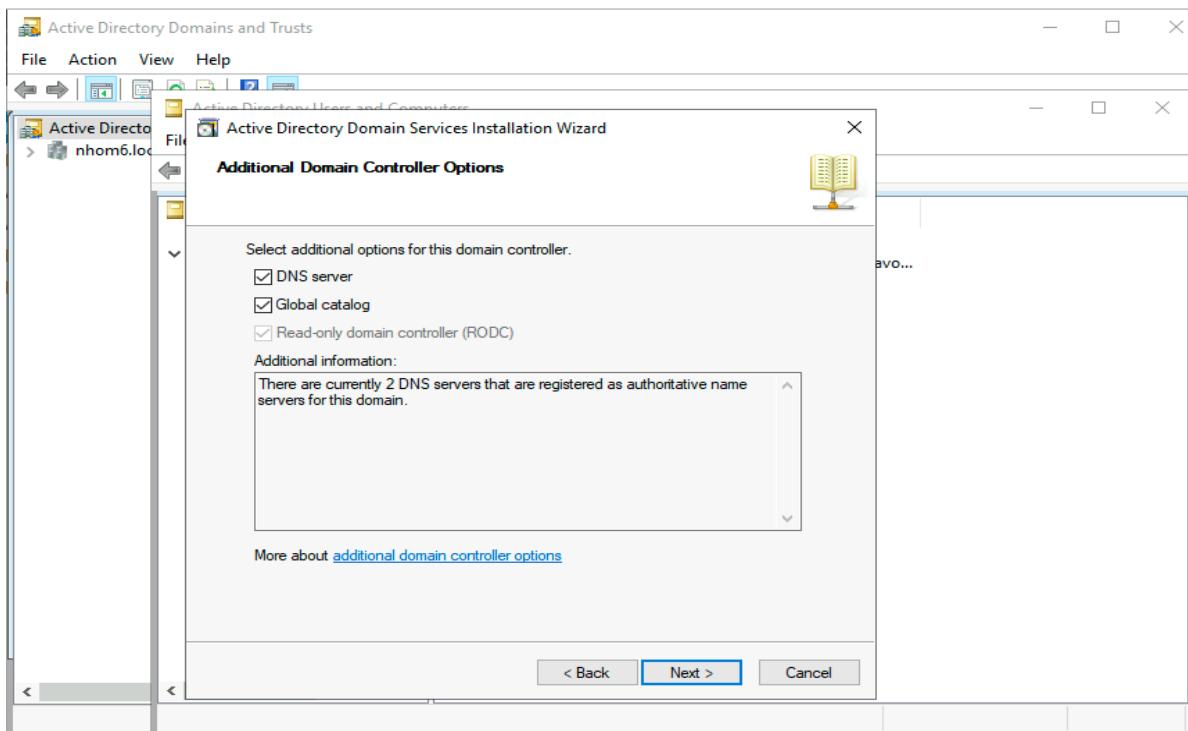
## Tiến hành tạo tài khoản cho RODC



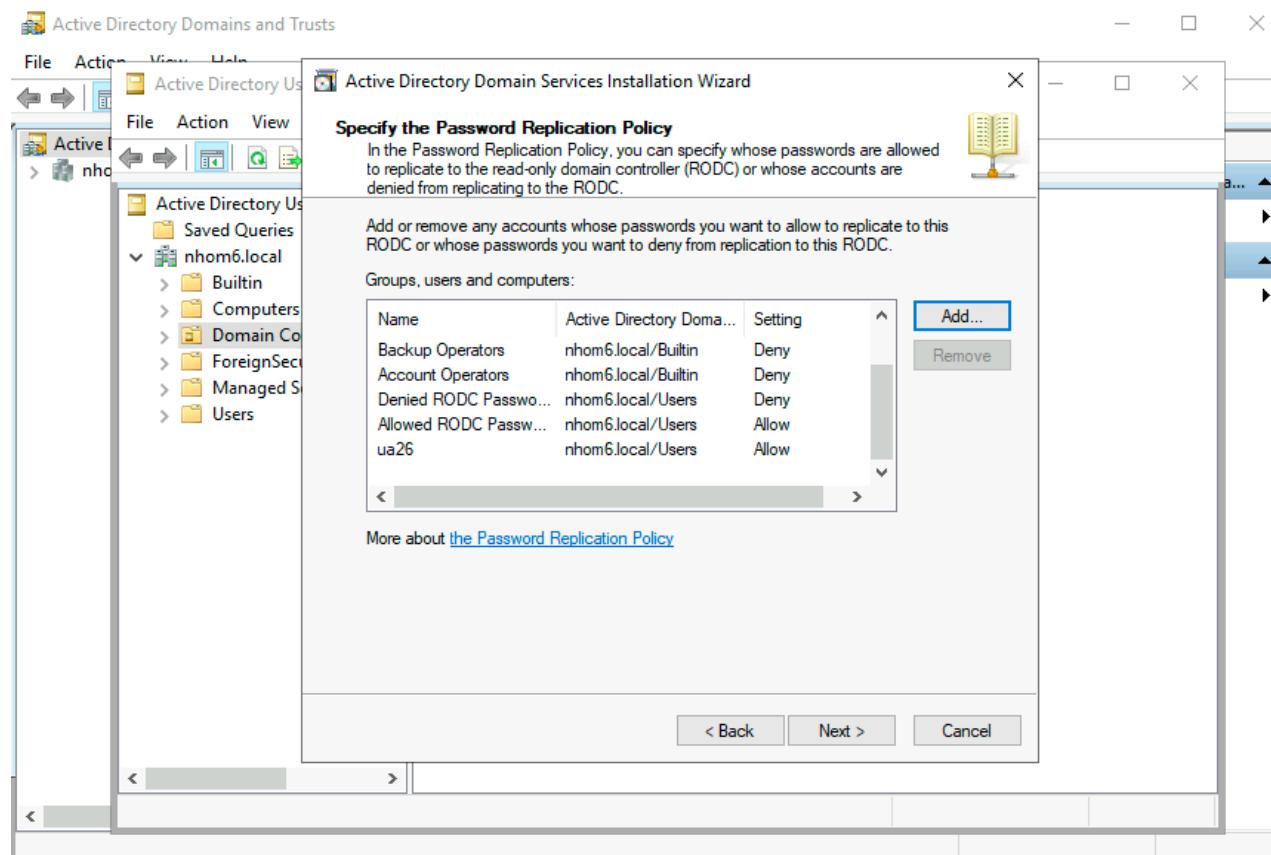
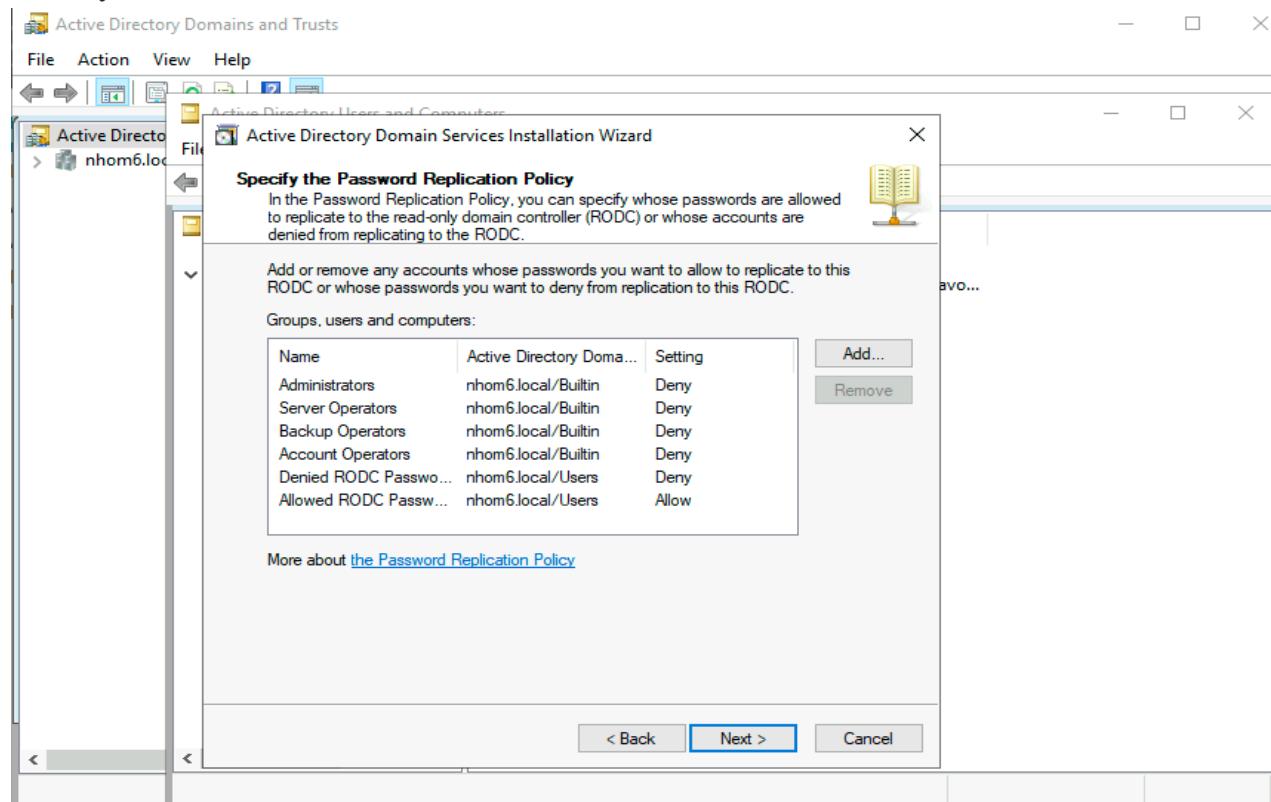
Nhấn next



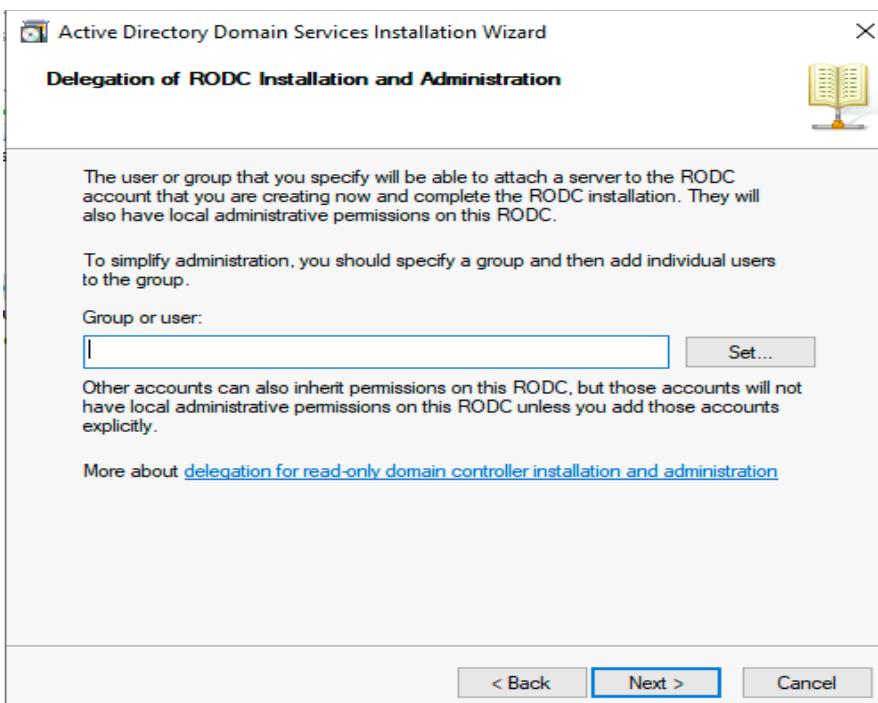
Nhấn next



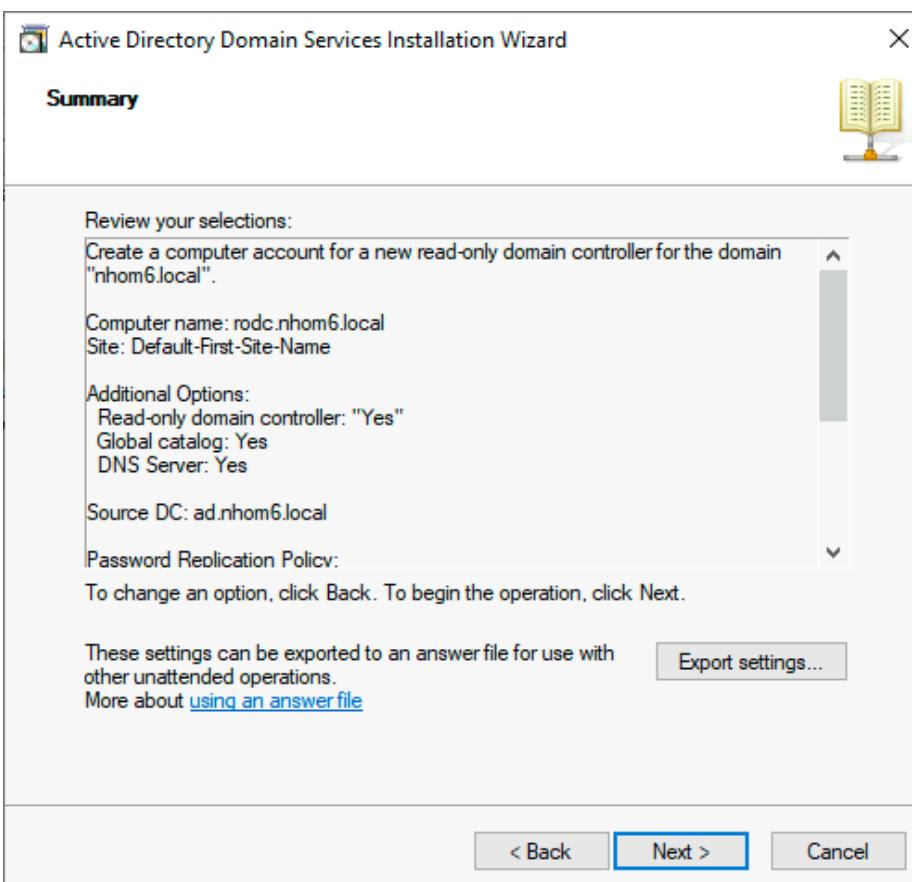
Tại đây ta nhấn add và thêm tài khoản ua26



Nhấn next



Nhấn next



Tiếp tục nhấn next và finish để hoàn tất

## Thêm máy s2

**S1 Properties**

This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
Account Operators	nhom6.local/Builtin	Deny
Administrators	nhom6.local/Builtin	Deny
Allowed RODC Passw...	nhom6.local/Users	Allow
Backup Operators	nhom6.local/Builtin	Deny
Denied RODC Passwo...	nhom6.local/Users	Deny
Server Operators	nhom6.local/Builtin	Deny

Advanced... Add... Remove OK Cancel Apply Help

**Select Users, Computers, Service Accounts, or Groups**

Select this object type:  Users, Computers, Service Accounts, Groups, or Built-in security principals  Object Types...

From this location: nhom6.local

Enter the object names to select (examples):

Advanced... OK Cancel

## Tạo user ur16 trên PDC

**Server Manager**

**Active Directory Domains and Trusts**

New Object - User

Create in: nhom6.local/Users

When you click Finish, the following object will be created:

- Full name: ur16
- User logon name: ur16@nhom6.local
- The password never expires.

Finish Back Cancel

Local Server 1 Manageability Events Services Performance BPA results 11/26/2022 11:52 PM

All Servers 1 Manageability Events Services Performance BPA results 11/26/2022 11:52 PM

Activate Windows Go to Settings to activate Windows.

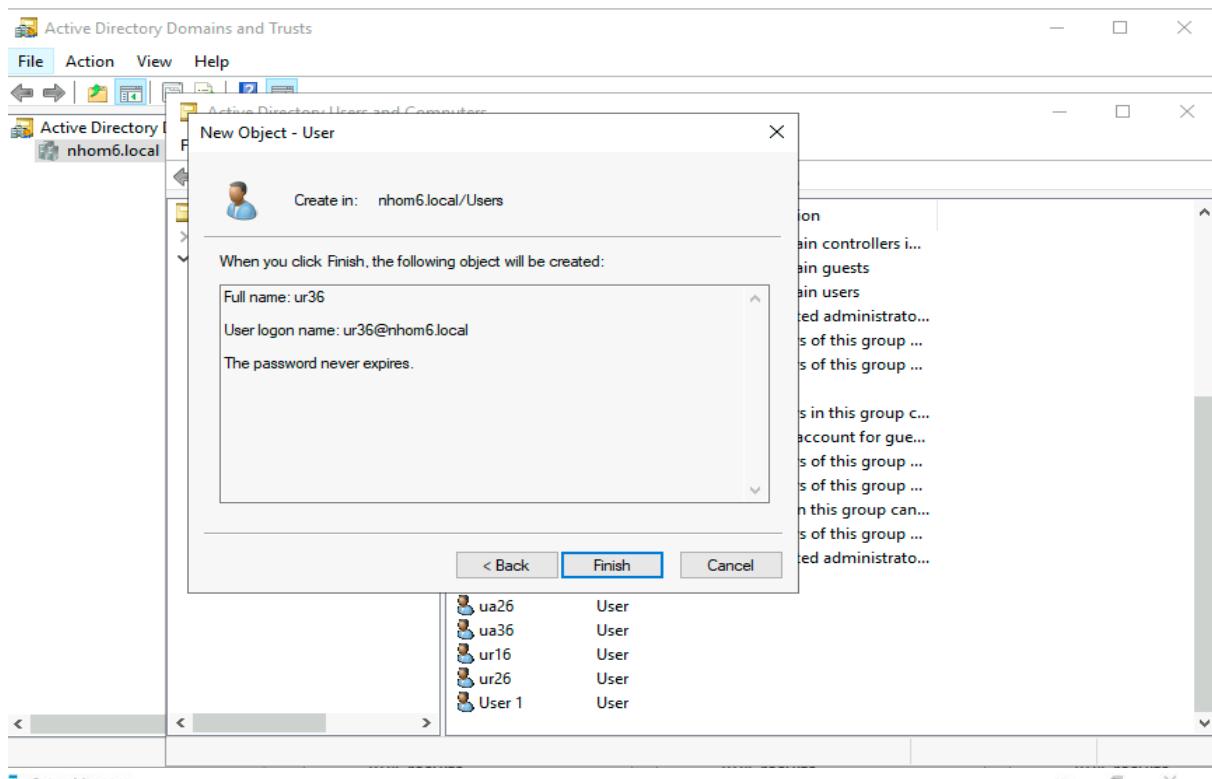
Kiểm tra trên RODC

Name	Type	Description
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 ...
File Admin	User	
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 can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
ua16	User	
ua26	User	
ua36	User	
ur16	User	
User 1	User	

Tạo tài khoản user ur26 trên RODC, và kiểm tra trên PDC

Name	Type	Description
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 ...
File Admin	User	
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 can...
Read-only D...	Security Group...	Members of this group ...
Schema Ad...	Security Group...	Designated administrato...
ua16	User	
ua26	User	
ua36	User	
ur26	User	
User 1	User	

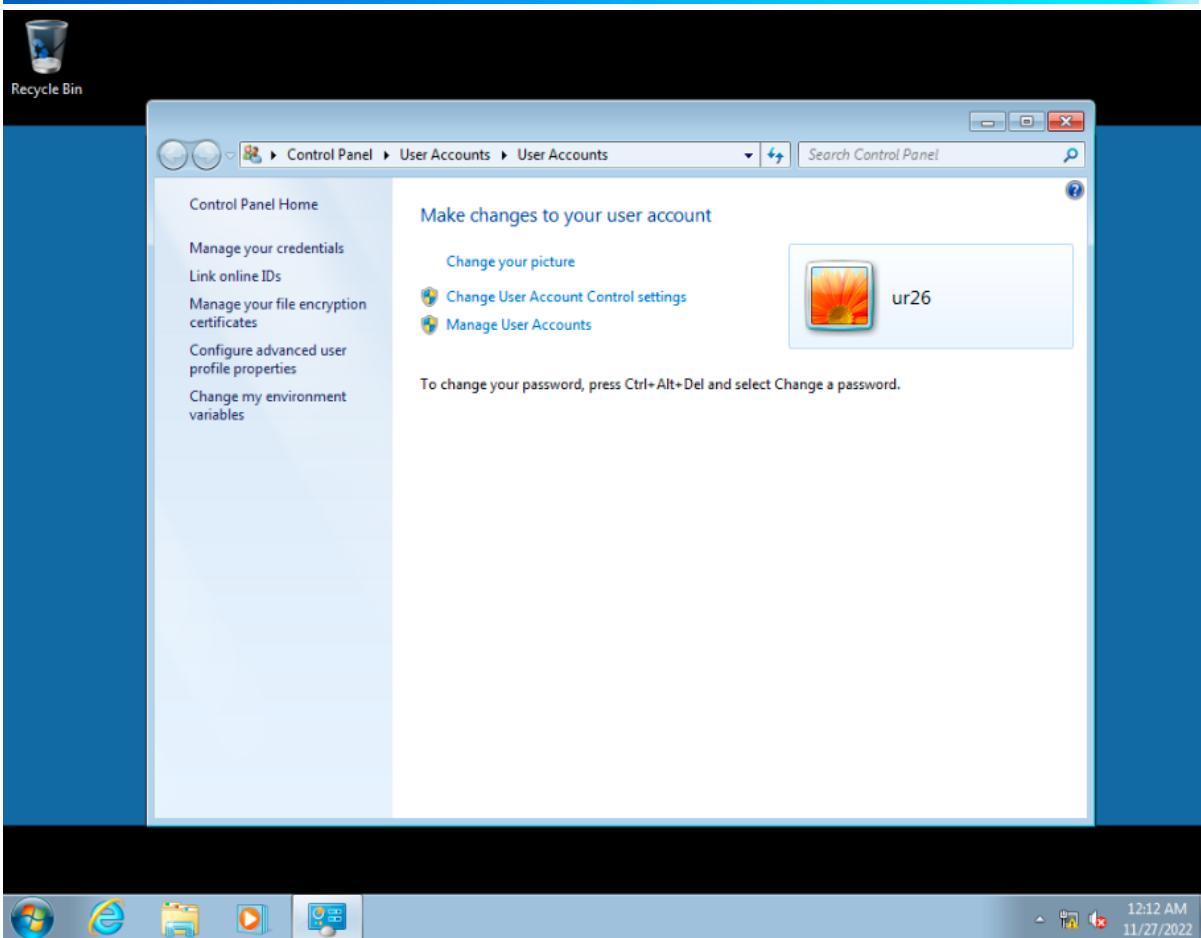
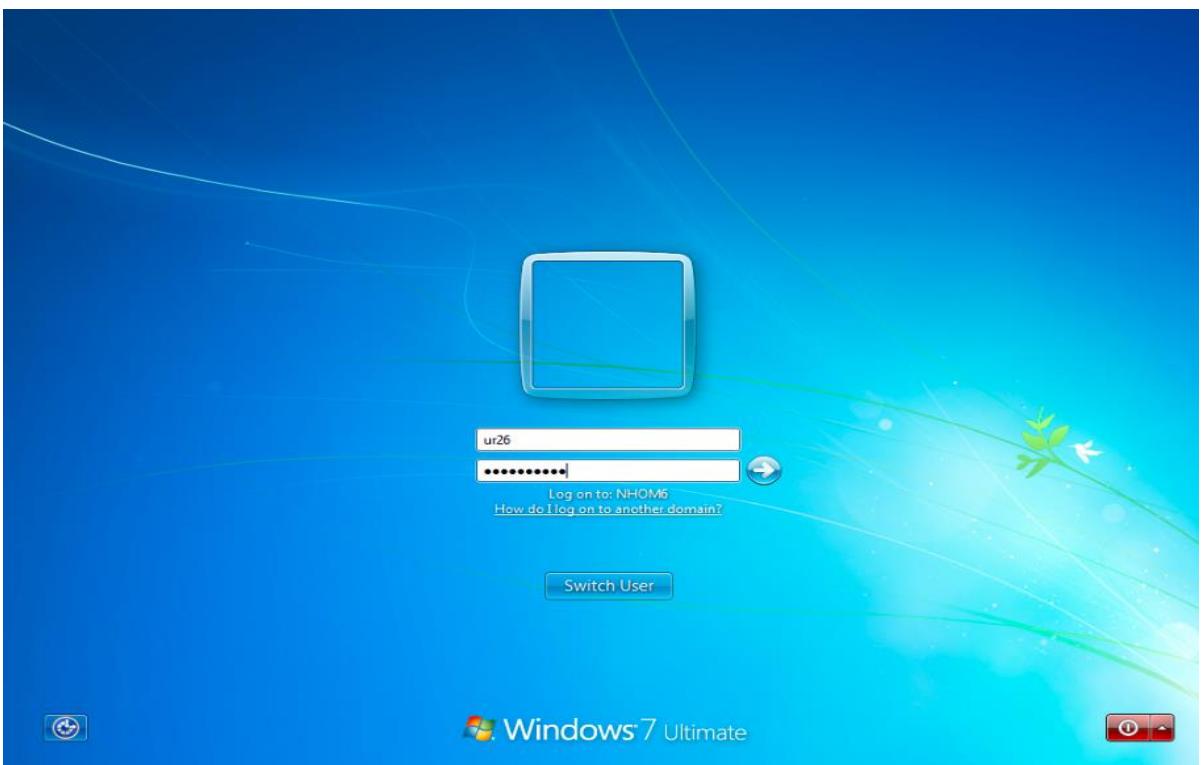
- Tắt máy Read-Only DC, thêm user ur36 trên Primary DC. Sau đó mở lại Read-Only DC và kiểm tra thông tin user này trên Read-Only DC.



The screenshot shows the 'Active Directory Domains and Trusts' management console. The left navigation pane is visible with items like 'Dashboard', 'Local', 'All Services', 'AD DS', 'DNS', and 'File and Storage'. The main pane displays the 'Active Directory Users and Computers' view for the 'nhom6.local' domain. The 'Users' container is selected under the 'nhom6.local' node. The right pane lists the users:

Name	Type	Description
Domain Guest	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise K... ...mputers	Security Group...	Members of this group ...
Enterprise R... ...oreignSecurityPrincipals	Security Group...	Members of this group ...
File Admin	User	
Group Policy...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...
RAS and IAS ...	Security Group...	Servers in this group can...
Read-only D... ...nabled Service Accounts	Security Group...	Members of this group ...
Schema Adm...	Security Group...	Designated administrato...
ua16	User	
ua26	User	
ua36	User	
ur16	User	
ur26	User	
ur36	User	
User 1	User	

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



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

