

# BÁO CÁO THỰC HÀNH

Môn học: Quản trị mạng và hệ thống

Tên chủ đề: Triển khai Active Directory trên Windows Server

GVHD: Đỗ Hoàng Hiển

Nhóm: 02

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.011.ANTT.1

STT	Họ và tên	MSSV	Email
1	Nguyễn Triệu Thiên Bảo	21520155	21520155@gm.uit.edu.vn
2	Trần Lê Minh Ngọc	21521195	21521195@gm.uit.edu.vn
3	Huỳnh Minh Khuê	21522240	21522240@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Nội dung	Tình trạng
1	Yêu cầu 1	100%
2	Yêu cầu 2	100%
3	Yêu cầu 3	100%
4	Yêu cầu 4	100%

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

<sup>1</sup> Ghi nội dung công việc, các kịch bản trong bài Thực hành

# BÁO CÁO CHI TIẾT

## 1. Xây dựng mô hình Workgroup

**Yêu cầu 1.1** 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. Mô hình Workgroup hoạt động như thế nào?

- Định nghĩa: Mô hình Workgroup (hay còn gọi là mô hình Peer-to-Peer) là một kiểu mô hình mạng trong đó các thiết bị và máy tính trong mạng kết nối với nhau trực tiếp, không thông qua một máy chủ trung tâm.
- Quy mô sử dụng: Mô hình Workgroup thường được sử dụng trong các môi trường văn phòng nhỏ hoặc gia đình (bởi vì những nơi này số lượng thiết bị kết nối trong mạng không quá lớn và việc chia sẻ tài nguyên giữa các thiết bị rất cần thiết).
- Cách thức hoạt động: Trong mô hình này, các thiết bị trong mạng sẽ đóng vai trò như nhau, không có máy chủ trung tâm để điều khiển và phân phối tài nguyên. Mỗi thiết bị sẽ chứa các tài liệu và dữ liệu của riêng mình, và có thể chia sẻ cho các thiết bị khác trong mạng. Việc quản lý và bảo mật dữ liệu trong mô hình Workgroup thường được thực hiện trên từng thiết bị riêng lẻ.

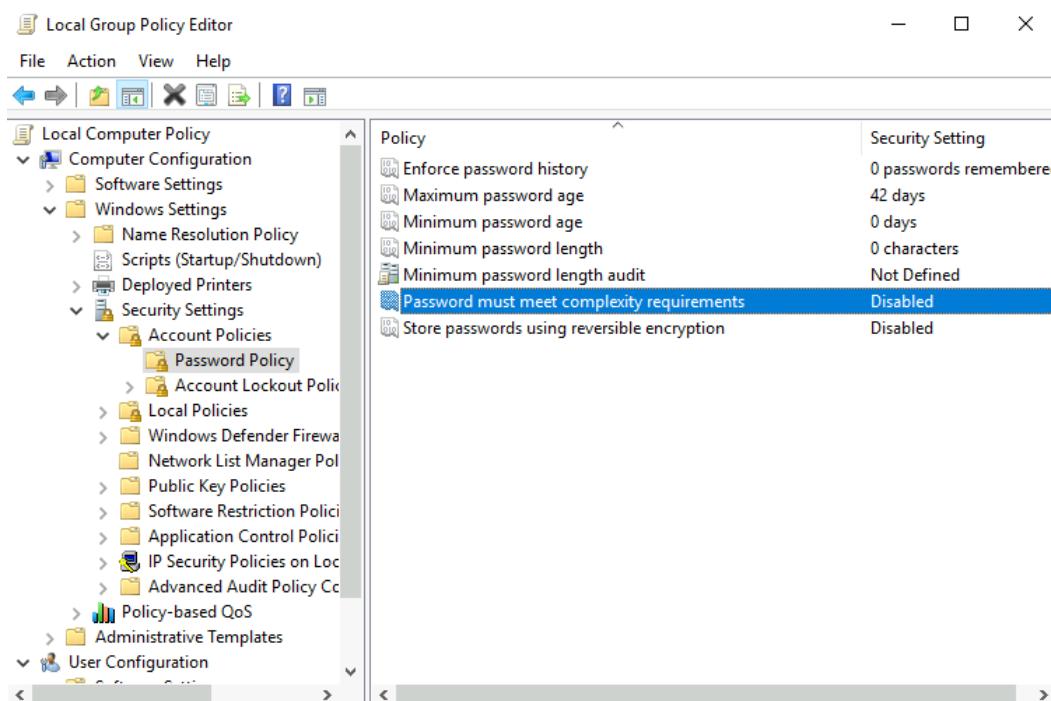
### 2. Trình bày ưu và nhược điểm của mô hình Workgroup.

- Ưu điểm:
  - Không yêu cầu máy tính chạy trên hệ điều hành Windows Server để tập trung hóa thông tin bảo mật.
  - 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.
  - Thuận tiện đối với nhóm có số máy tính ít và gần nhau ( $\leq 20$  máy).
- Nhược điểm:
  - Mỗi người dùng phải có một tài khoản người dùng trên mỗi máy tính mà họ muốn đăng nhập.
  - Bất kỳ sự thay đổi tài khoản người dùng, như là thay đổi mật khẩu hoặc thêm tài khoản người dùng mới, phải được làm trên tất cả các máy tính trong Workgroup, nếu bạn quên bổ sung tài khoản người dùng mới tới một máy tính trong nhóm thì người dùng mới sẽ không thể đăng nhập vào máy tính đó và không thể truy xuất tới tài nguyên của máy tính đó.
  - Việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người dùng có tài khoản trên máy tính đó được sử dụng.
  - Khả năng quản lý hạn chế và không đủ an toàn trong việc chia sẻ tài nguyên trong mạng, đặc biệt là khi số lượng thiết bị kết nối trong mạng tăng lên.

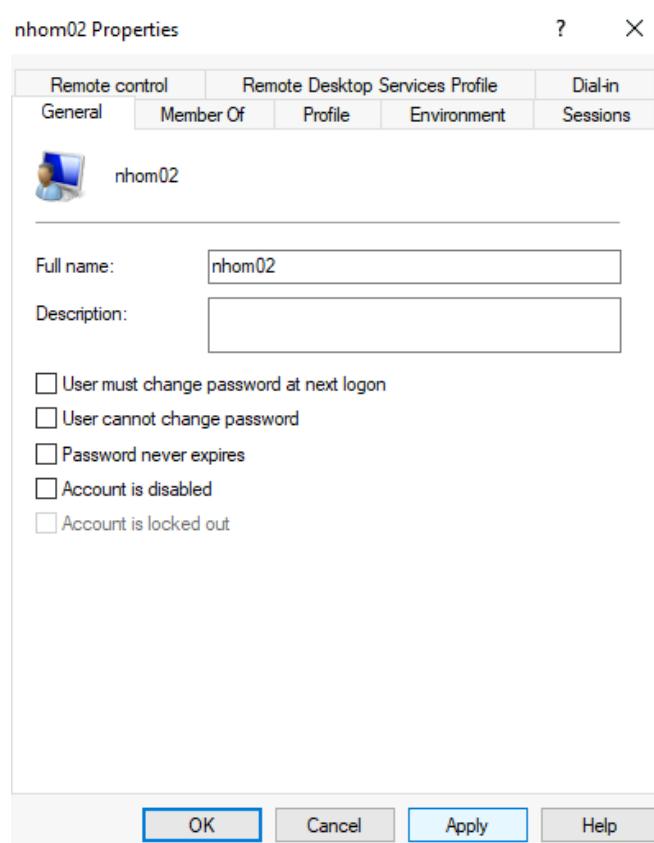
**Yêu cầu 1.2** Xây dựng mô hình Workgroup để chia sẻ file như bên dưới.

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

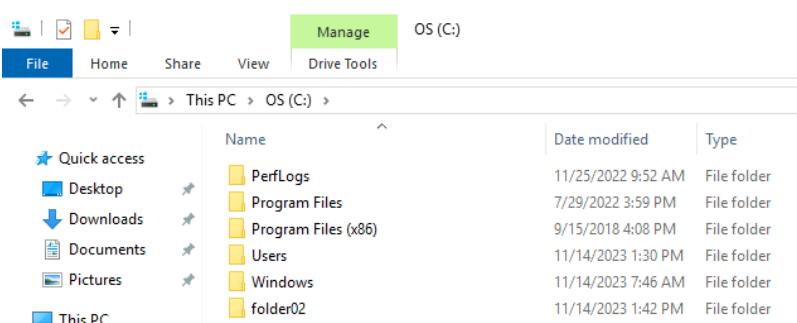
Chỉnh sửa chính sách tại **Windows Settings > Security Settings > Account Policies > Password Policy**. Tại mục **Password must meet complexity requirements**, thay đổi thành **Disabled**.



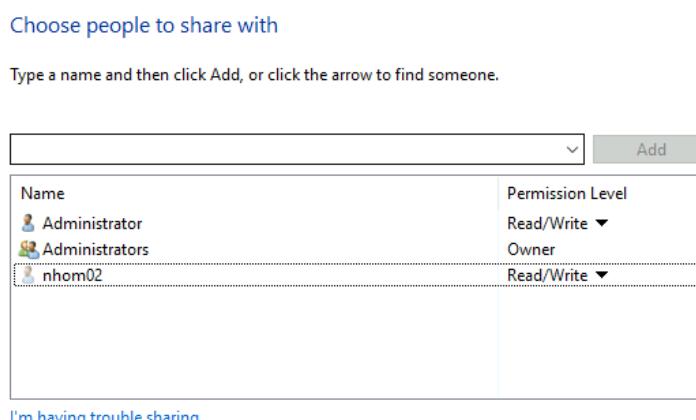
- Bước 2:** Trên máy chủ File Server, tạo tài khoản nhom02 có mật khẩu là 123.



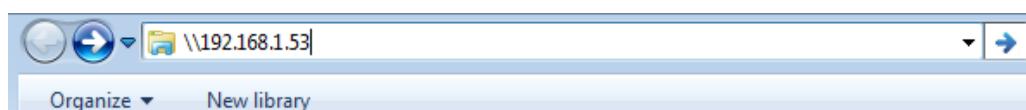
- Bước 3:** Trên ổ đĩa C:\ của File Server, tạo 1 thư mục **folder02** để chia sẻ dữ liệu.



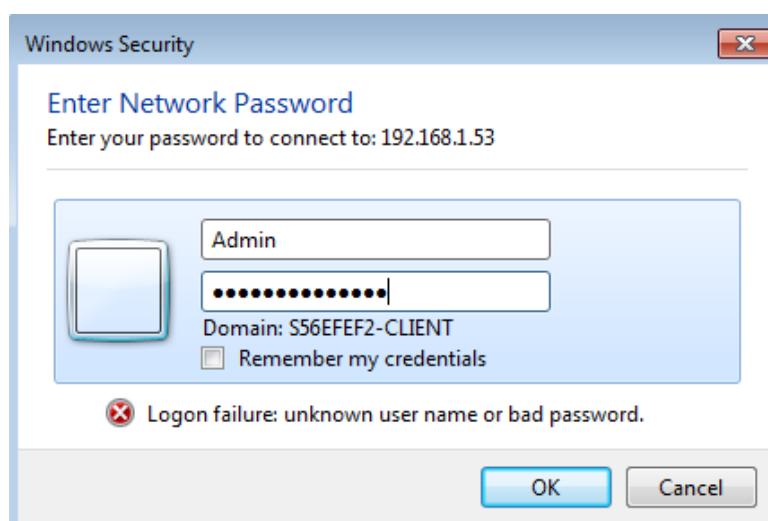
- Bước 4:** Nhấp chuột phải vào tên thư mục **folder02**, chọn **Give access to > Specific people...** Thực hiện phân quyền chia sẻ trên thư mục này để user **nhom02** có quyền Read/Write.



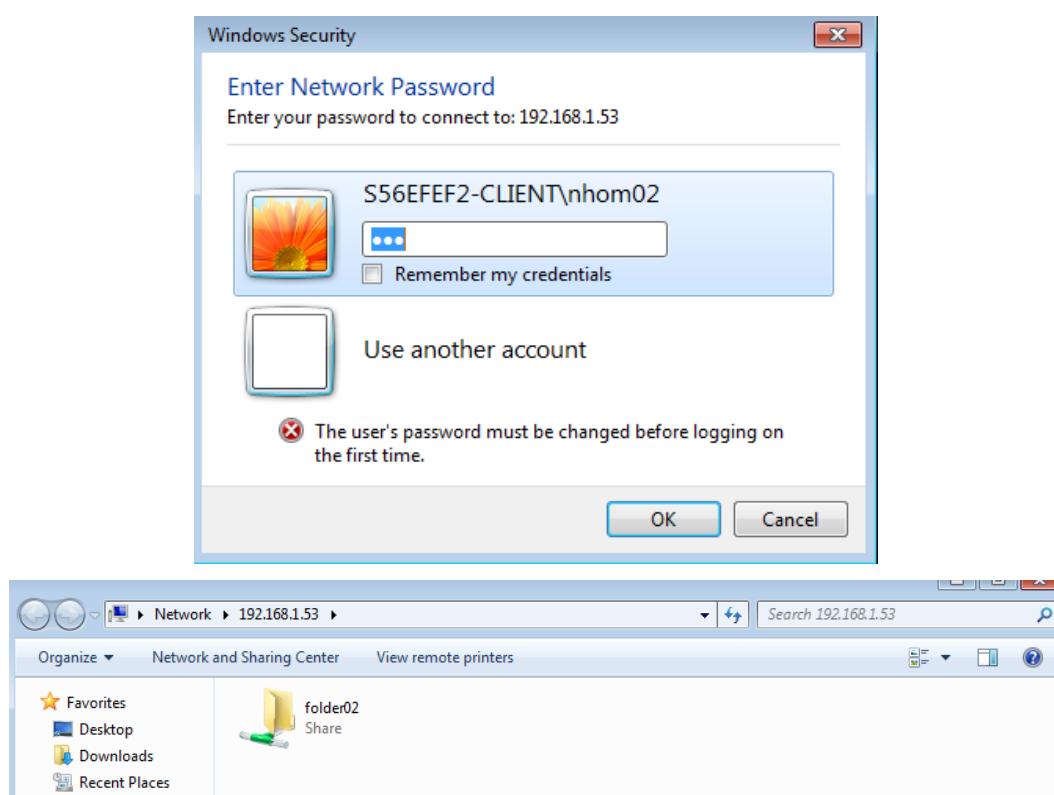
- Bước 5:** Từ máy Client, kết nối vào máy chủ File Server. Vào Windows Explorer, gõ địa chỉ IP của máy File Server với cú pháp như sau: \192.168.1.53.



- Bước 6:** Nhập user xác thực để truy cập vào File Server trong 2 trường hợp:
  - Sử dụng tài khoản của máy Client.



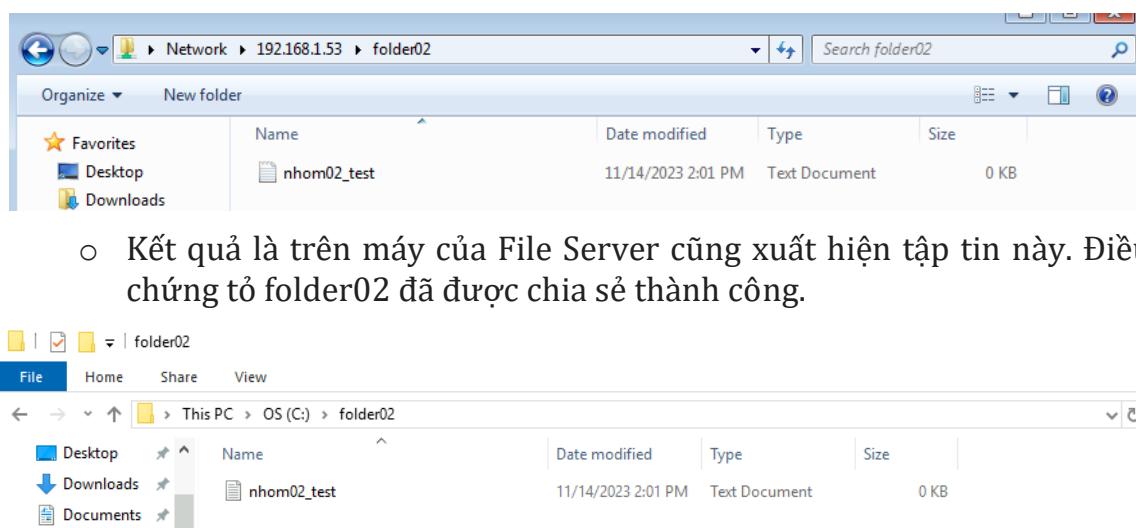
- Sử dụng tài khoản của máy File Server (user nhom02 đã tạo ở Bước 2).



⇒ Kết nối thành công

#### Kiểm tra và giải thích kết quả của 2 trường hợp trên.

- Sử dụng tài khoản của máy Client: không thể kết nối bởi vì tài khoản của Client chưa được cấu hình cho phép đọc hay ghi hay chia sẻ trên tệp tin folder02 .
- Sử dụng tài khoản của máy File Server: kết nối thành công bởi vì như bước 4 user nhom02 đã được phân quyền để chia sẻ trên thư mục folder02.
- Bước 7:** Sau khi truy cập thành công, trên máy Client tạo 1 tập tin tuỳ ý trong thư mục folder02. **Báo cáo và giải thích kết quả thực hiện.**
  - Trên máy Client ta tạo một thư mục nhom02\_text.txt để chia sẻ.



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

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

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

*Trả lời:*

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

Active Directory là một dịch vụ quản lý tài nguyên mạng được phát triển bởi Microsoft, chủ yếu được sử dụng trong môi trường hệ thống Windows Server. Active Directory giúp quản lý các tài nguyên như máy tính, người dùng, nhóm và các thiết bị mạng khác, đồng thời cung cấp các tính năng xác thực và phân quyền cho người dùng. Nó cũng cho phép quản lý các chính sách bảo mật, quản lý phân phối ứng dụng, cấu hình máy tính từ xa và các tính năng khác. Active Directory rất hữu ích trong việc quản lý hệ thống mạng lớn và phức tạp.

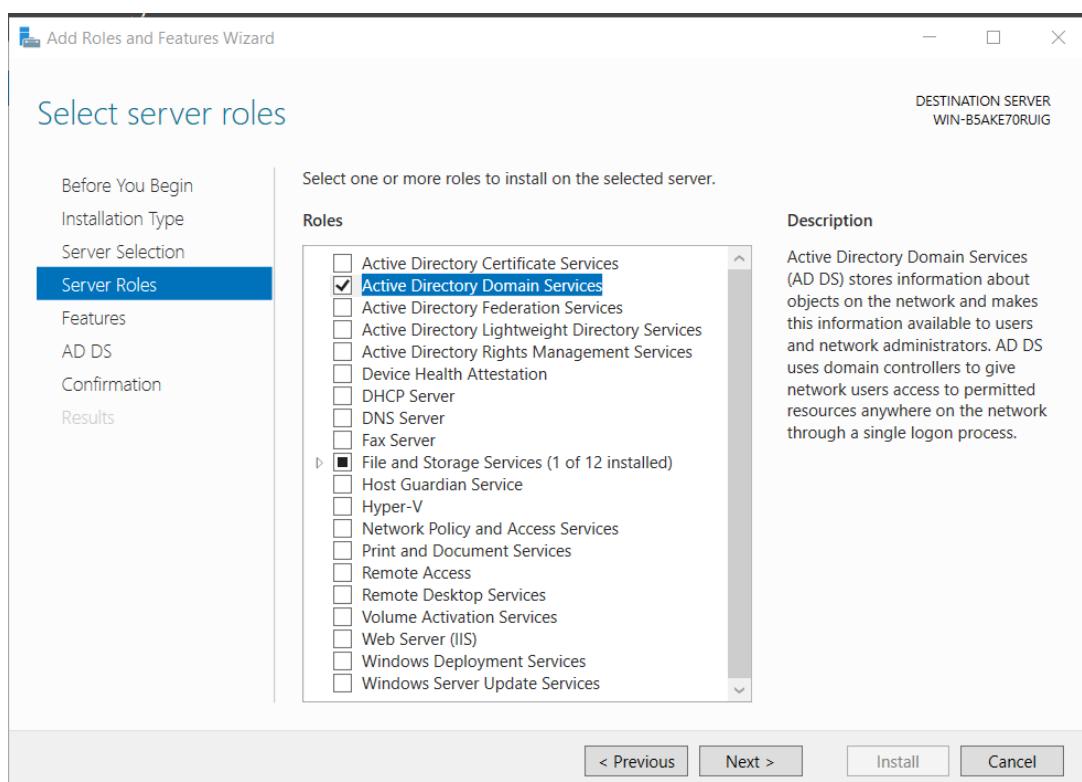
### 2. So sánh mô hình Domain và Workgroup?

Mô hình Workgroup	Mô hình Domain
<ul style="list-style-type: none"> <li>- Là một mô hình phân cấp đơn giản, trong đó các máy tính gắn kết với nhau và chia sẻ tài nguyên mà không có sự quản lý tập trung.</li> <li>- Mỗi máy tính trong mạng có quyền quản lý tài nguyên của nó và quyết định chia sẻ hay không chia sẻ cho các máy tính khác trong mạng.</li> <li>- Cấu trúc mạng Workgroup thường được sử dụng cho các mạng nhỏ, với số lượng máy tính ít.</li> <li>- Không có một máy chủ chính nào quản lý toàn bộ mạng.</li> </ul>	<ul style="list-style-type: none"> <li>- Là một mô hình phân cấp phức tạp hơn, trong đó một máy chủ trung tâm (domain controller) quản lý tất cả các tài nguyên và các thiết bị khác trong mạng.</li> <li>- Các thành viên trong mạng được đăng ký vào domain và được phép truy cập vào các tài nguyên mạng theo quy định của domain.</li> <li>- Quản trị viên có thể tạo ra các chính sách thống nhất cho toàn bộ mạng, đảm bảo tính an toàn và hiệu quả trong việc quản lý tài nguyên.</li> <li>- Mô hình Domain thường được sử dụng cho các tổ chức và doanh nghiệp lớn, nơi số lượng máy tính lớn và việc quản lý phải thực hiện tập trung.</li> </ul>

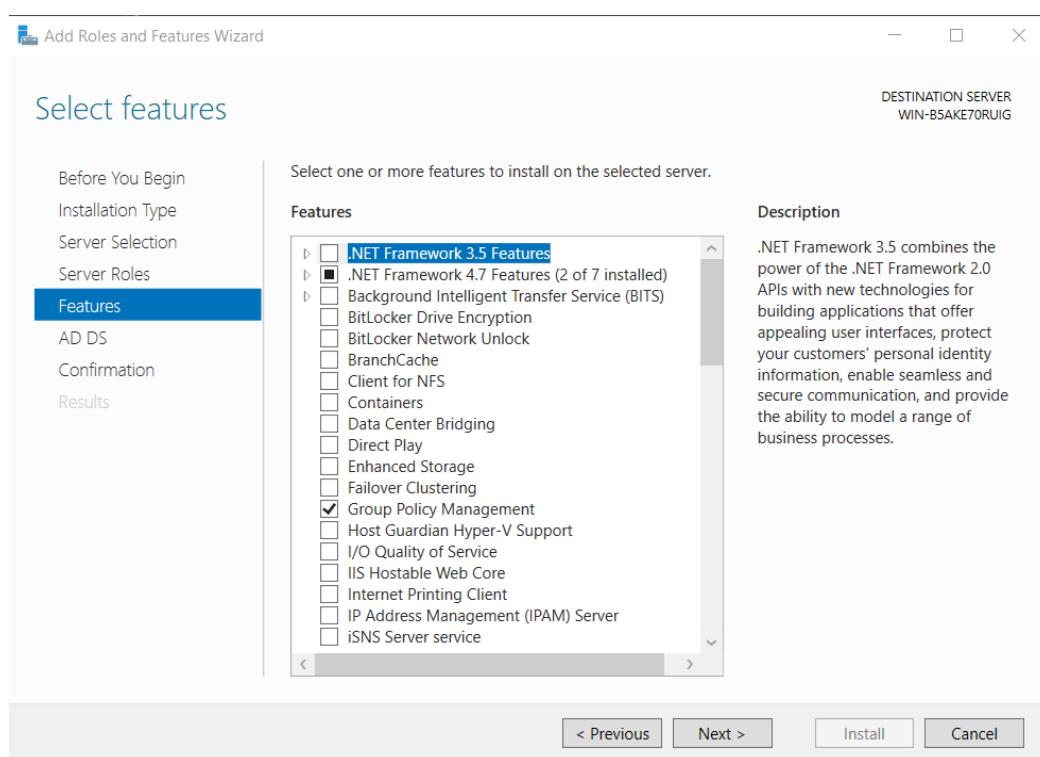
**Yêu cầu 2.2.** Xây dựng mô hình Domain như bên dưới.

### Sử dụng máy RODC làm File Server

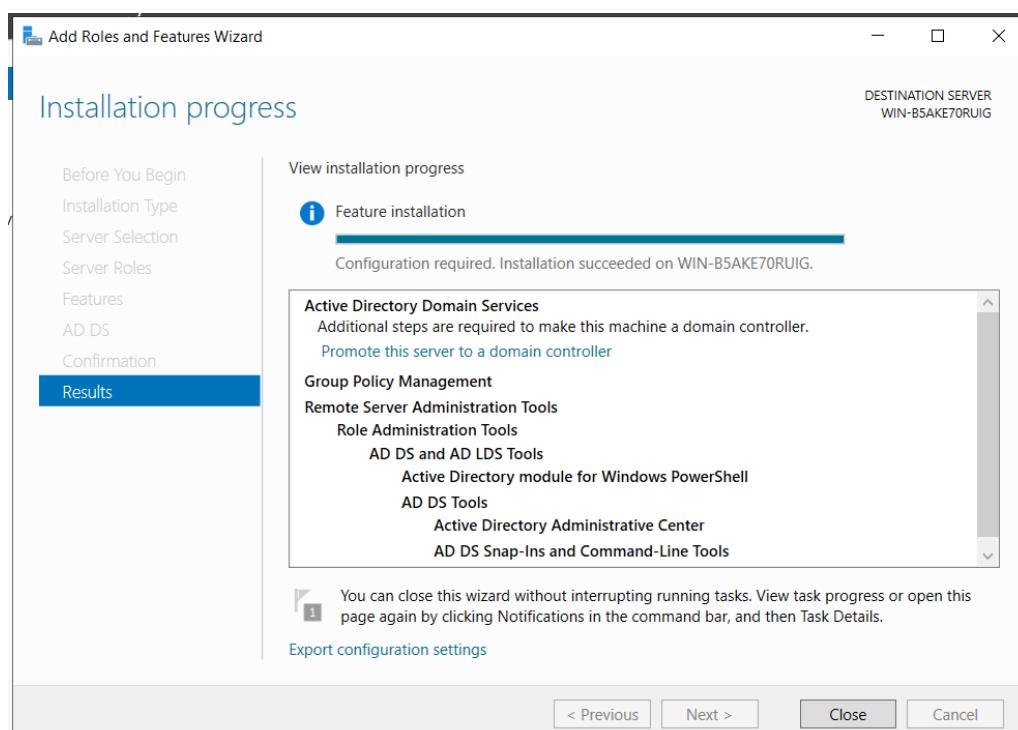
- **Bước 1:** Cài đặt Active Directory Domain Service trên máy Active Directory
  - Vào **Server Manager > Manage > Add Roles and Features**
  - Chọn **Next** tại các bước **Before You Begin, Installation Type, Server Selection**
  - Tại bước **Server Roles**, chọn **Active Directory Domain Services**.



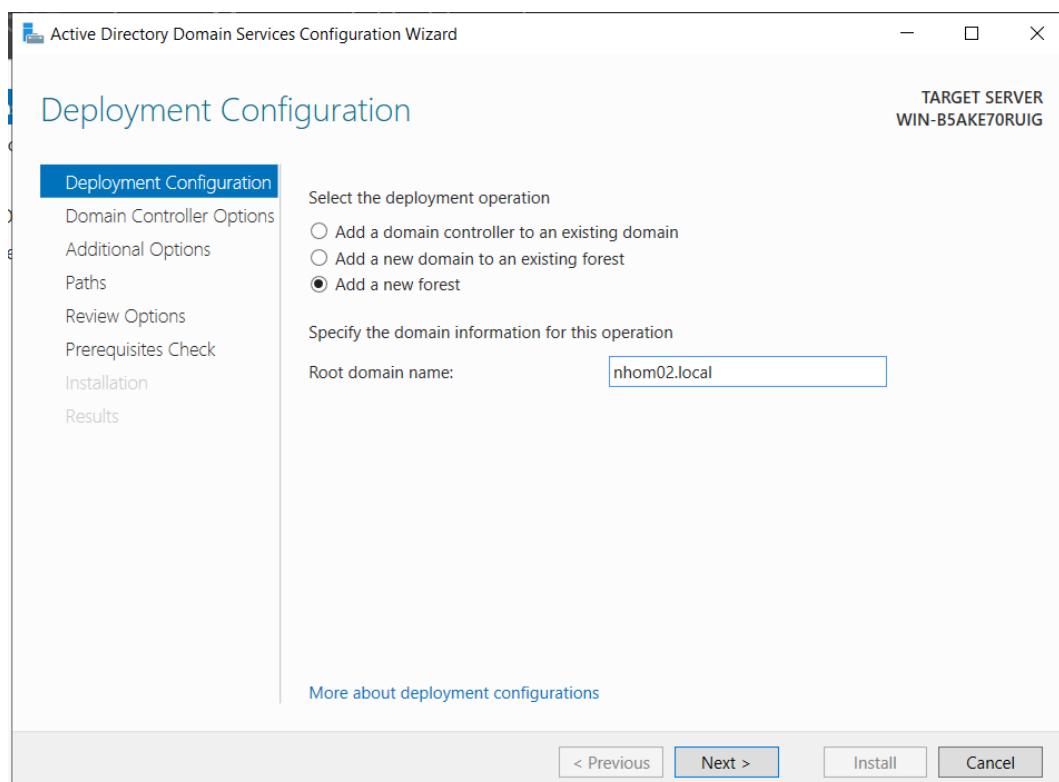
- Ở bước **Features**, chọn **Group Policy Management**.



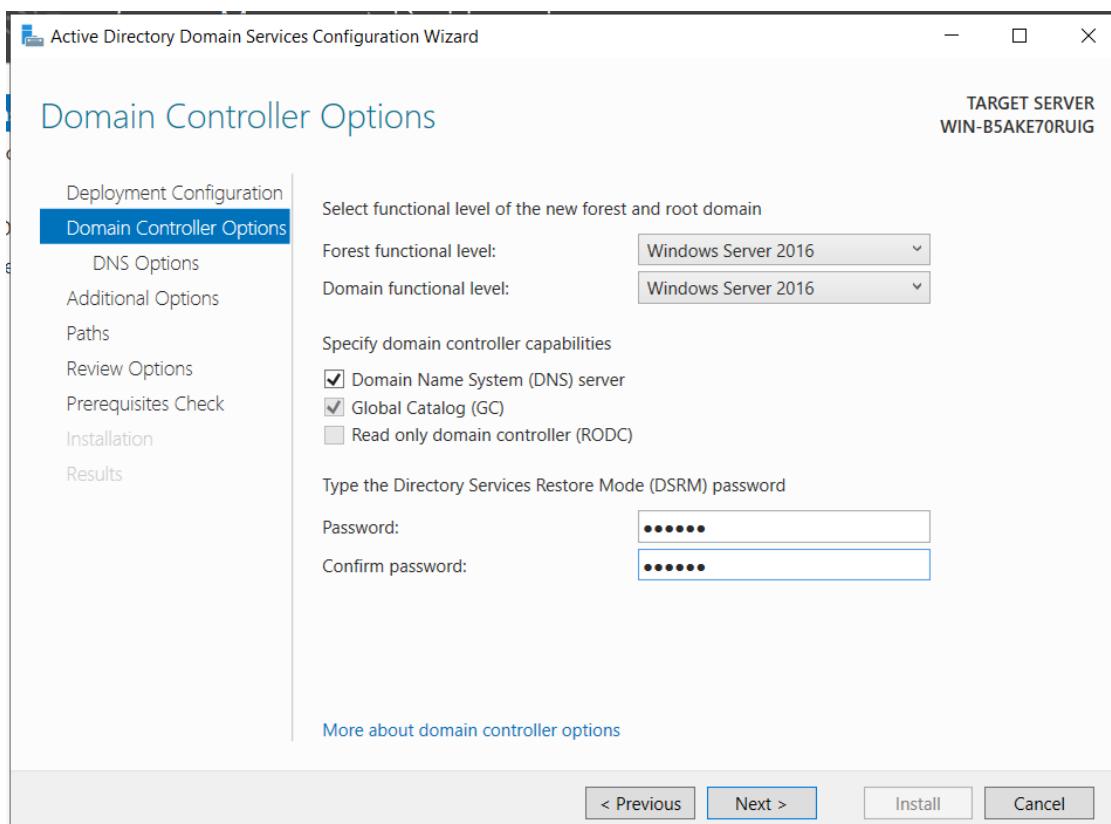
- Ở bước **AD DS**, chọn **Next**.
- Ở bước **Confirmation**, xác nhận lại thông tin và chọn **Install**.
- Chờ quá trình cài đặt hoàn thành và chọn **Close** để kết thúc.



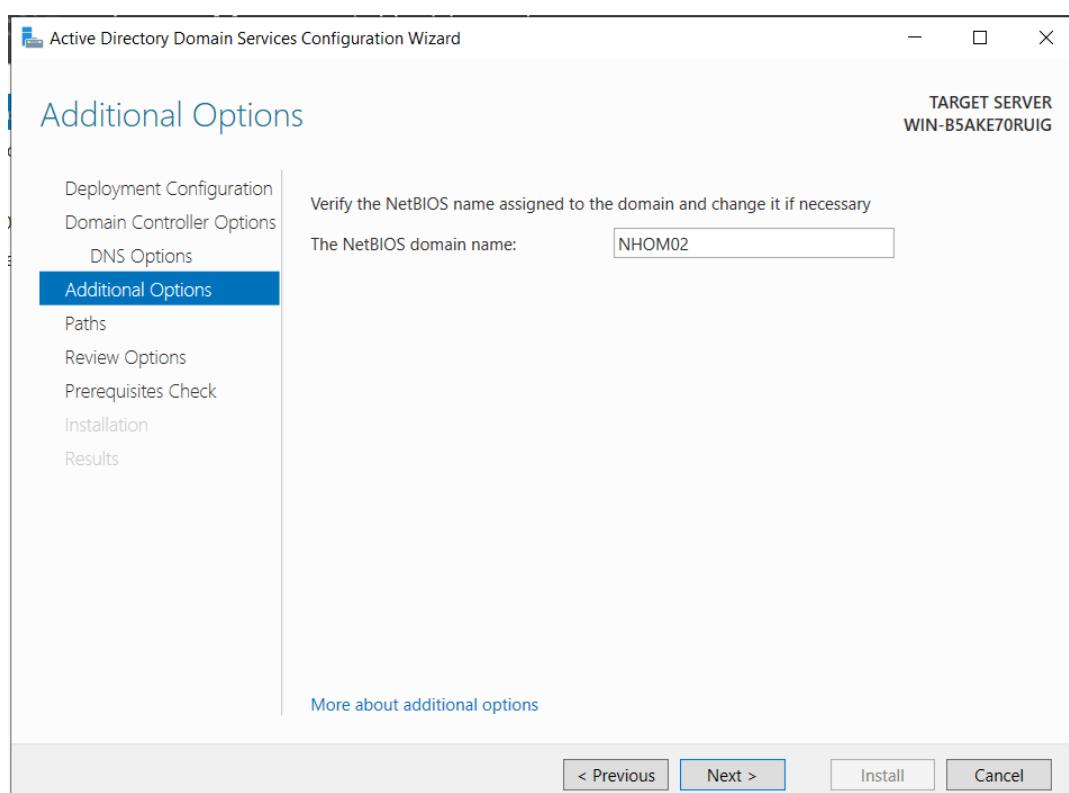
- **Bước 2:** Nâng cấp máy chủ Active Directory lên Domain Controller
  - Vào **Server Manager** sẽ thấy biểu tượng cảnh báo, nhấp vào và chọn **Promote this server to a domain controller**.
  - Chọn **Add new forest** và gõ domain **nhom02.local** vào mục **Root domain**.



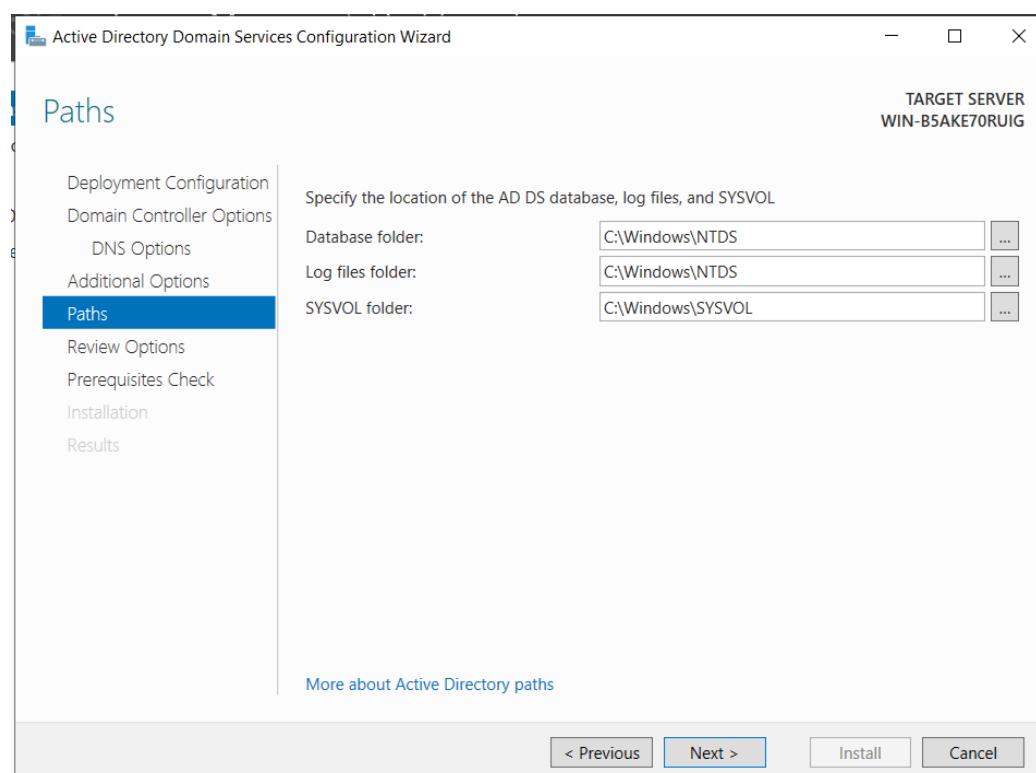
- Tiếp theo, thiết lập DSRM password: Nhóm02.local và các thiết lập như bên dưới.



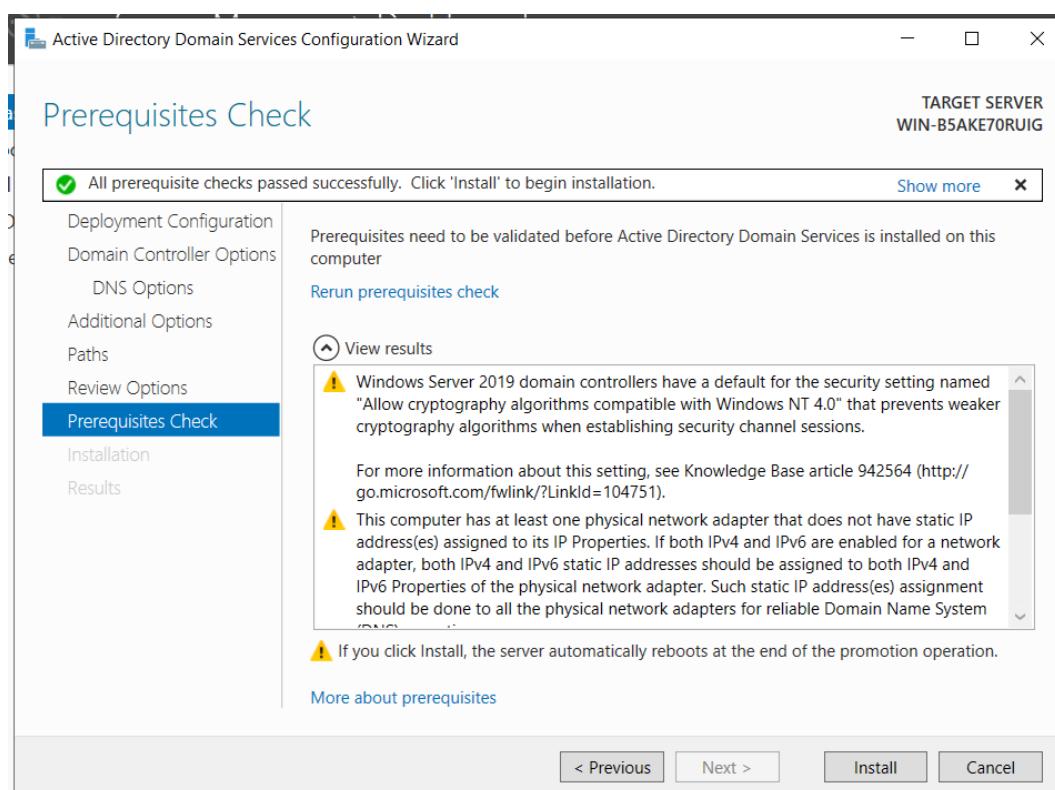
- Thiết lập NetBIOS domain name

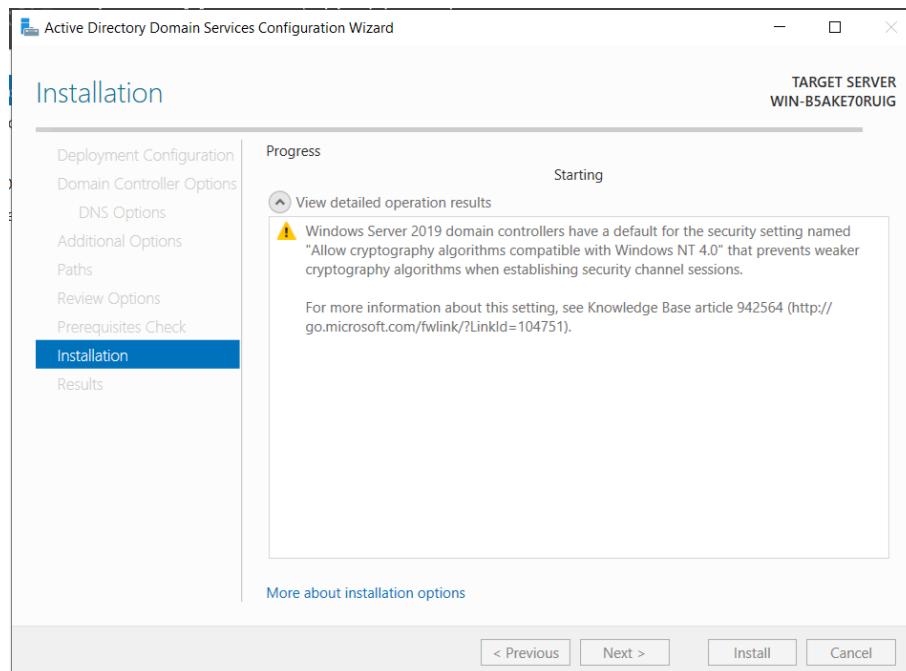


- Giữ nguyên các tùy chỉnh mặc định ở mục Paths



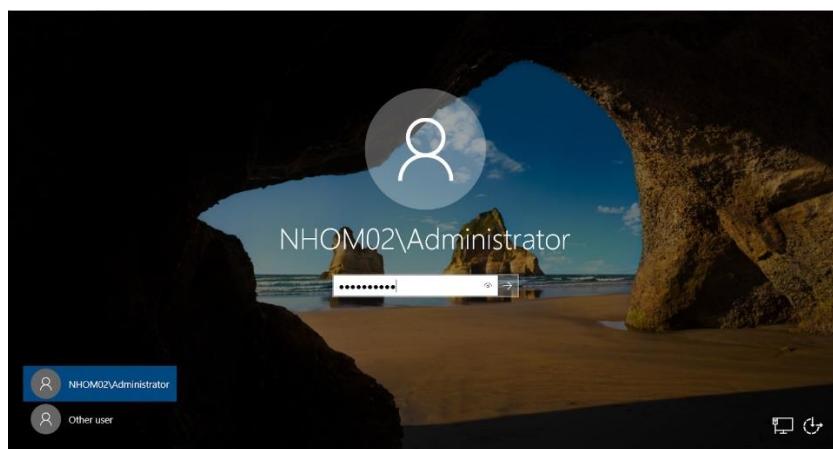
- Thực hiện bước Prerequisites Check hoàn thành, sau đó chọn Install và chờ quá trình nâng cấp hoàn tất.



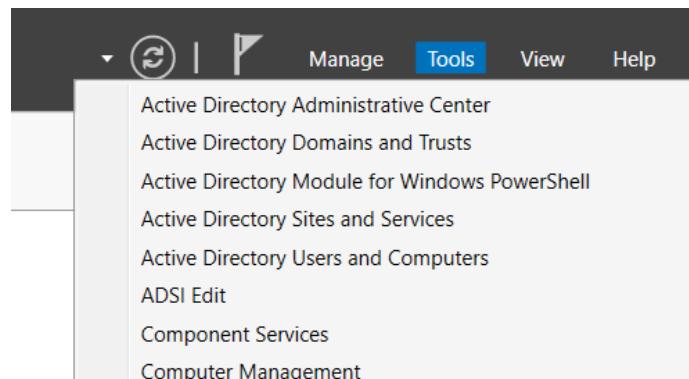


- **Bước 3: Tạo user trong domain**

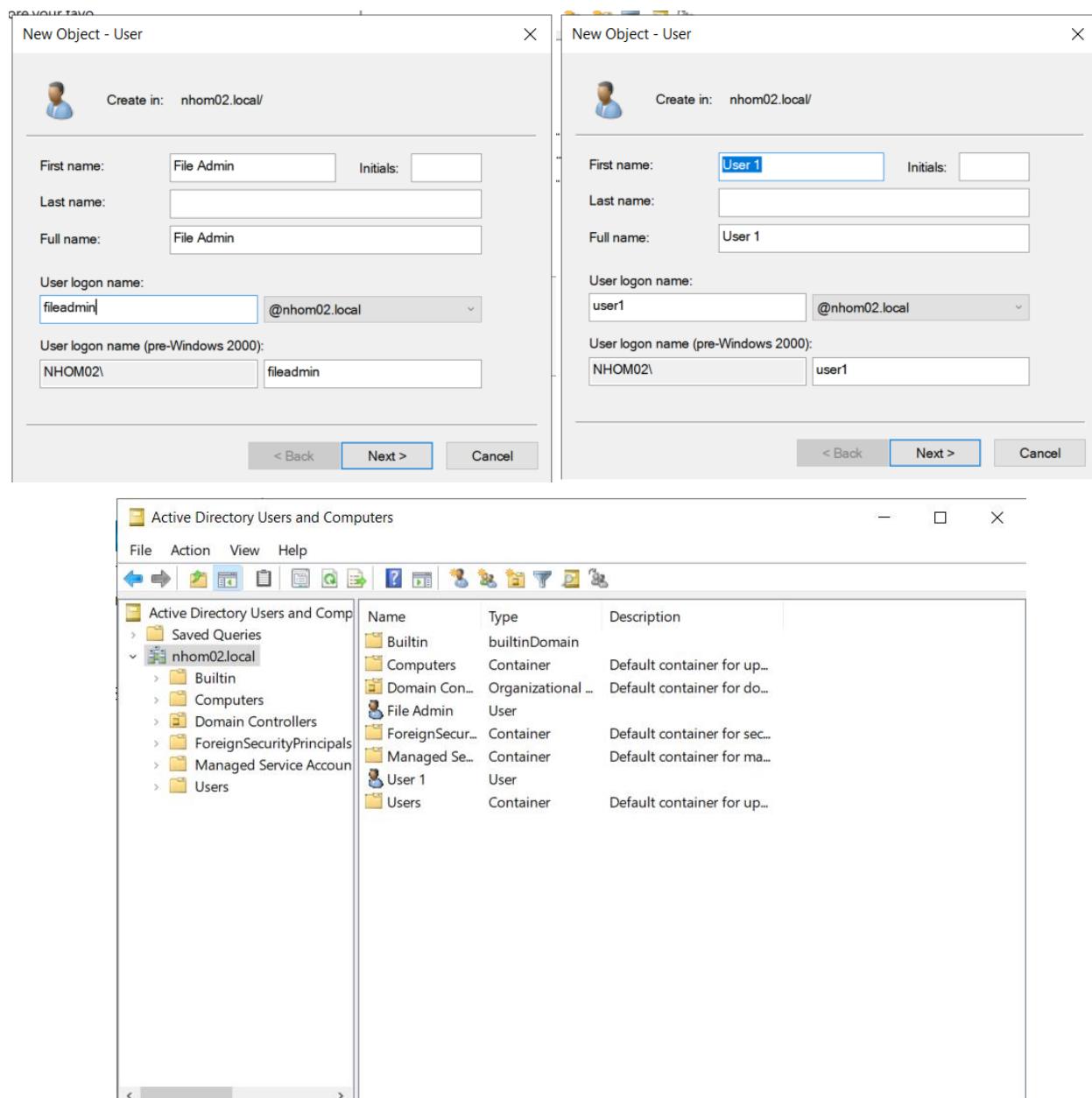
- Bước này tạo 2 user **fileadmin** và **user1** trong domain để sử dụng khi thêm File Server và Client vào domain ở các bước sau.
- Đăng nhập vào máy chủ Active Directory (máy AD) với tài khoản **NHOM02\Administrator** (tài khoản trong domain).



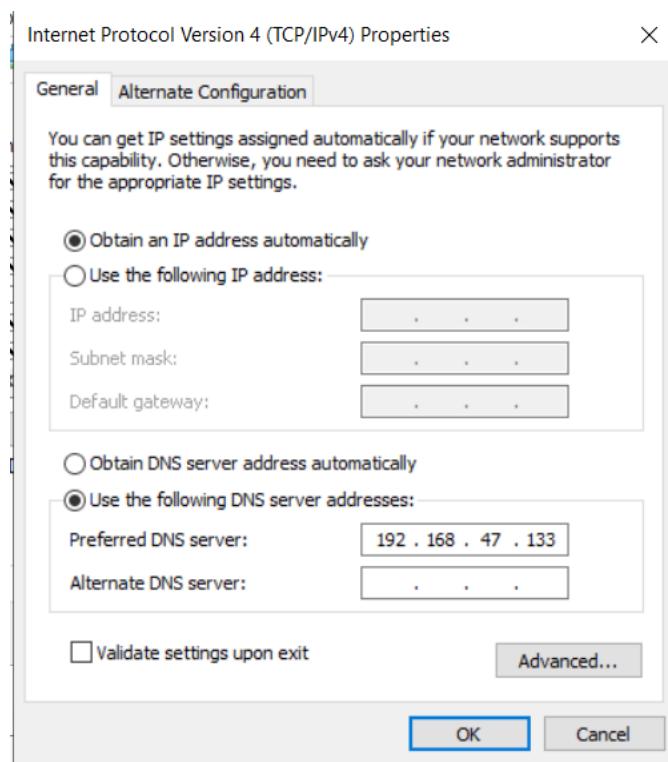
- Vào Server Manager > Tools > Active Directory Users and Computers.



- Trong **nhom02.local > Users**, nhấp chuột phải trong khung hiển thị các user, chọn **New > User** và nhập thông tin user muốn tạo. Thực hiện tạo 2 user **fileadmin** và **user1**, password của 2 user là Nhom02.local



- Bước 4:** Thêm File Server vào domain đã tạo. Tạo cấu hình DNS trên File Server



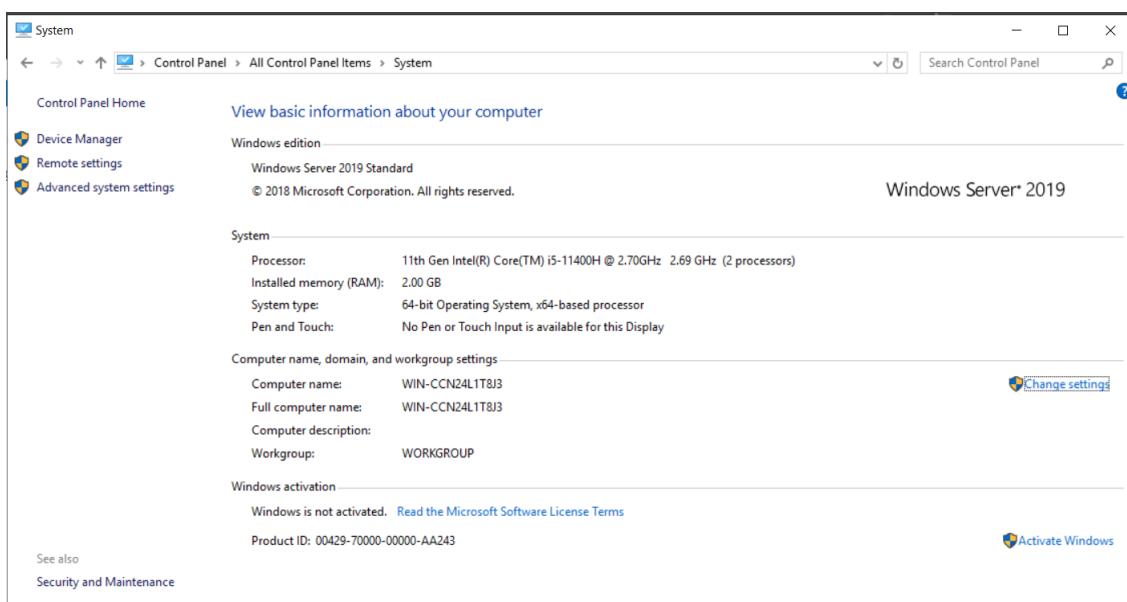
- Trên máy File Server, kiểm tra kết nối đến domain.

```
C:\Users\Administrator>ping nhom02.local

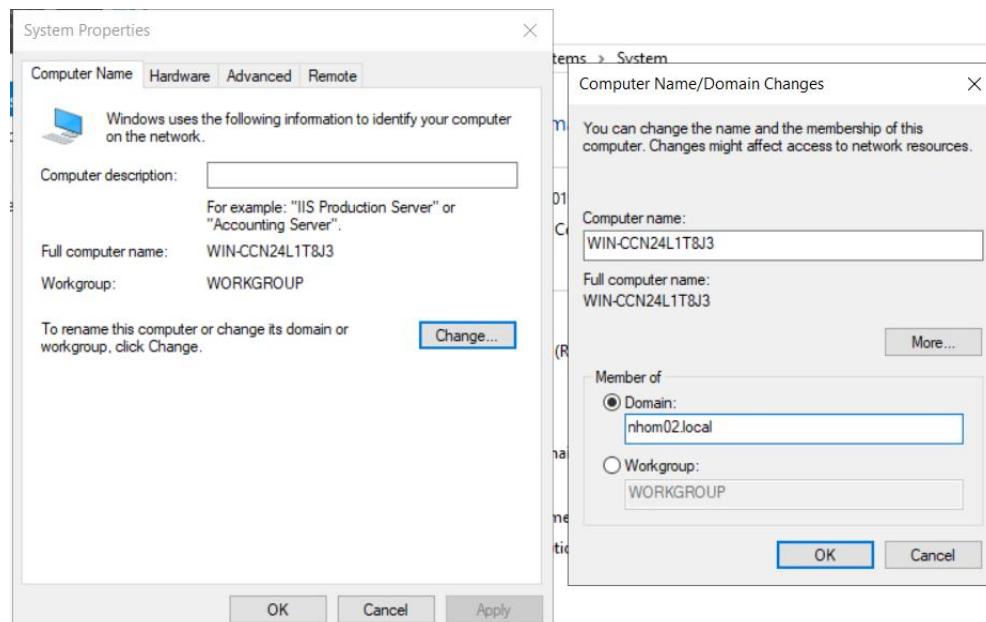
Pinging nhom02.local [192.168.47.133] with 32 bytes of data:
Reply from 192.168.47.133: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.47.133:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

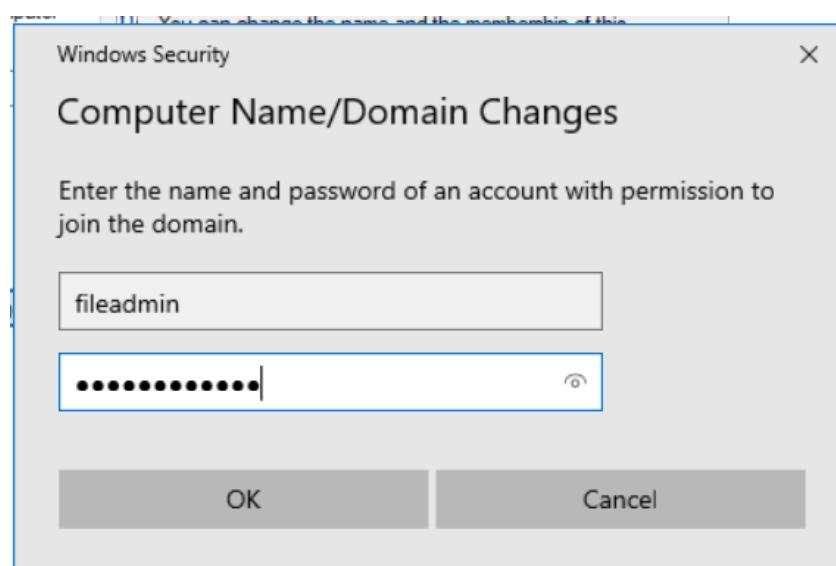
- Vào mục System trong Control Panel, chọn Change settings.



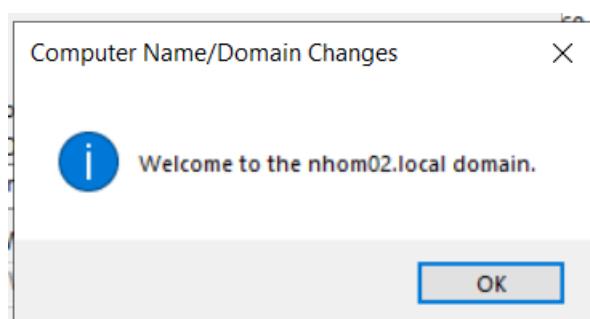
- Trong cửa sổ **System Properties**, tab **Computer Name**, chọn **Change**. Sau đó tại trường **Member of**, chọn **Domain** và nhập tên domain muốn tham gia.



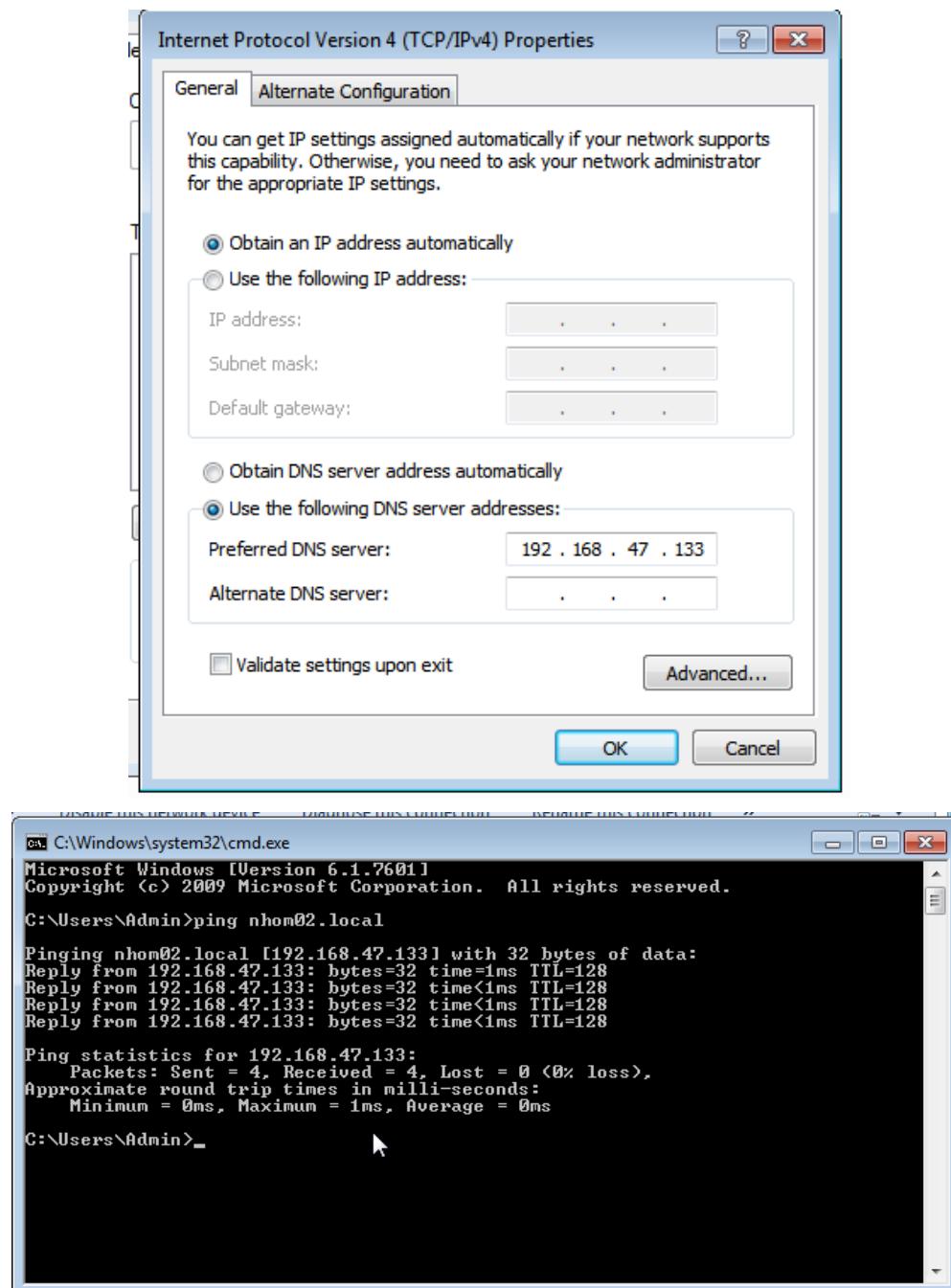
- Sử dụng tài khoản tương ứng đã tạo trên Active Directory ở bước 3 để xác thực

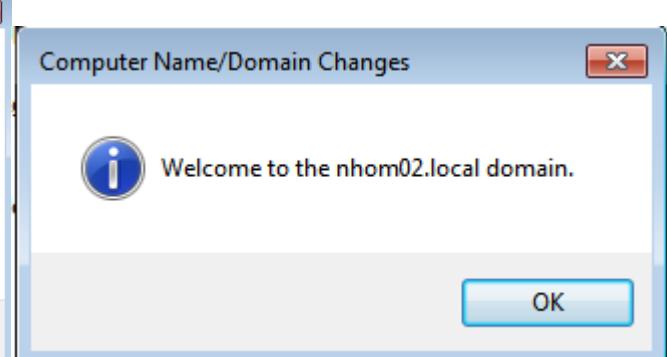
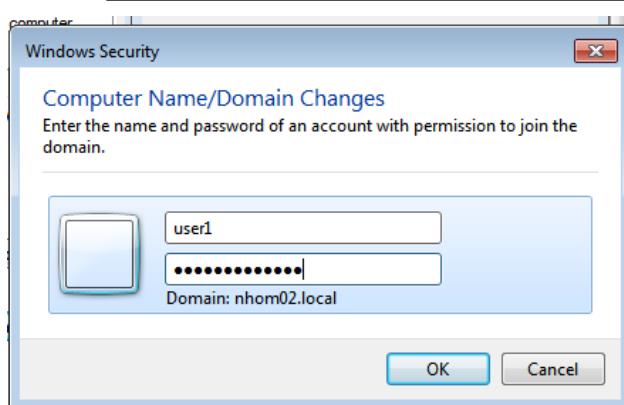
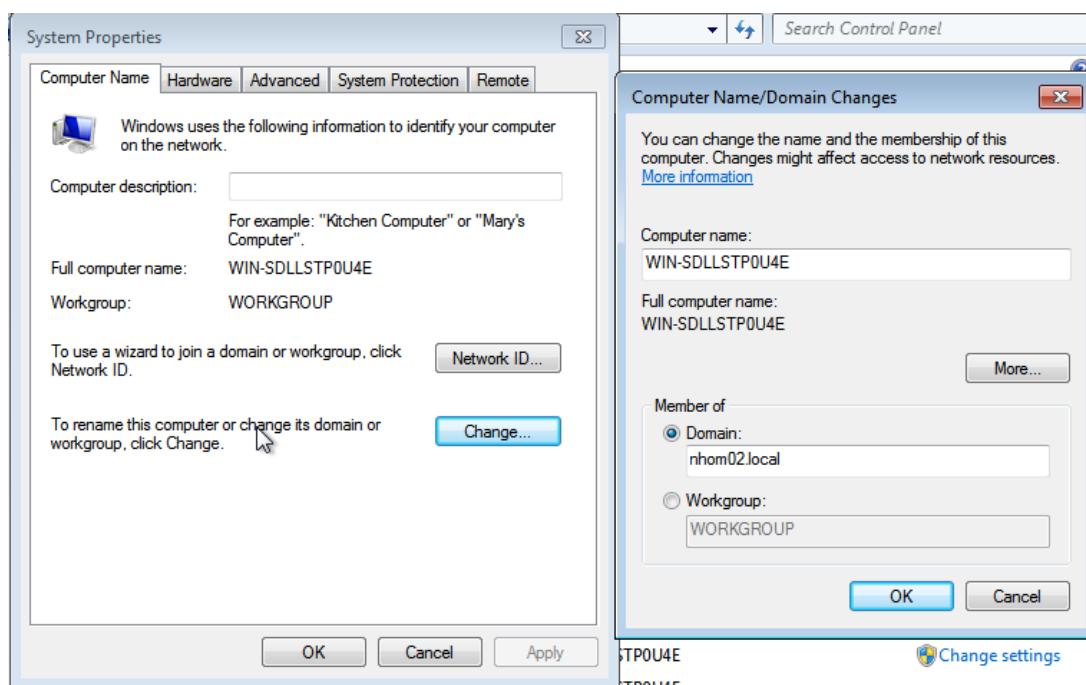
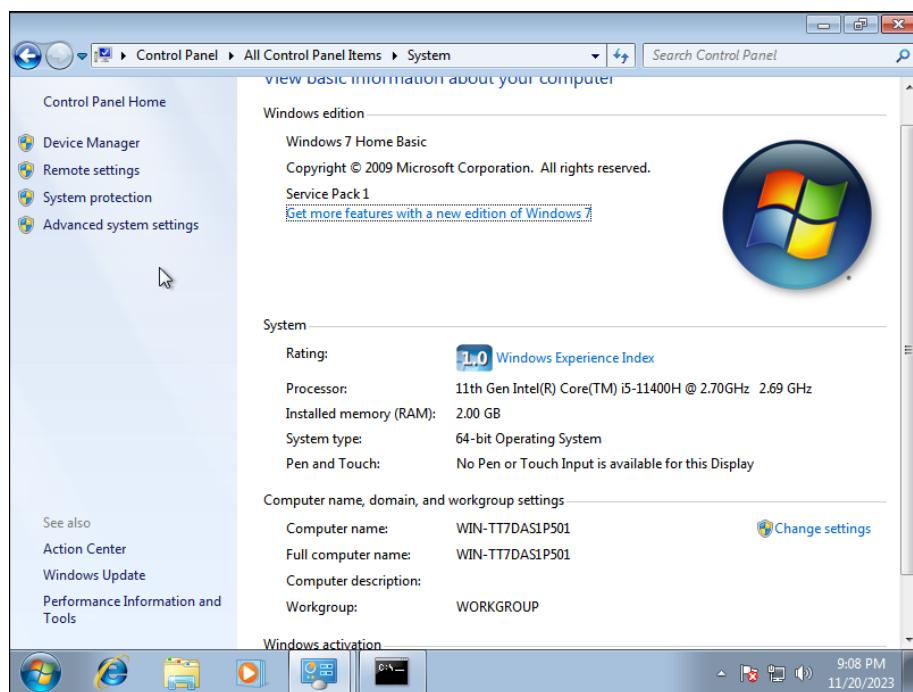


- Xác thực thành công thì File Server sẽ được thêm vào domain.

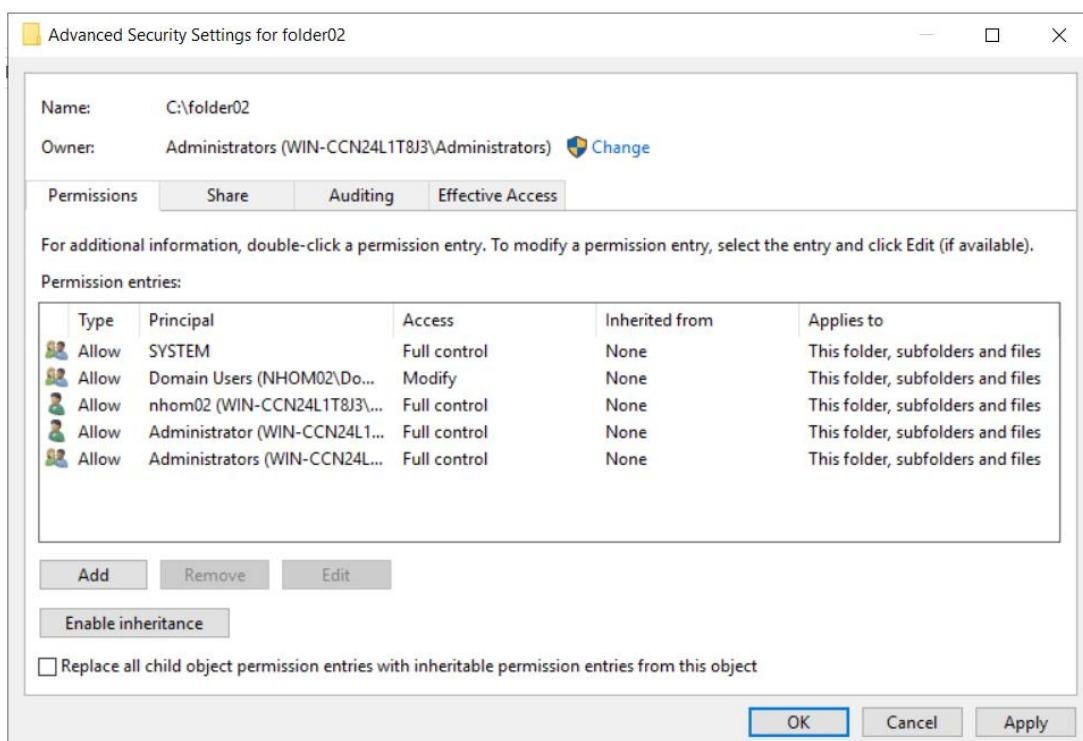


- Sau khi quá trình này hoàn tất, tiến hành khởi động lại File Server.
- **Bước 5:** Thêm máy client vào domain đã tạo. Thực hiện quá trình tương tự Bước 4 để thêm máy client vào domain.

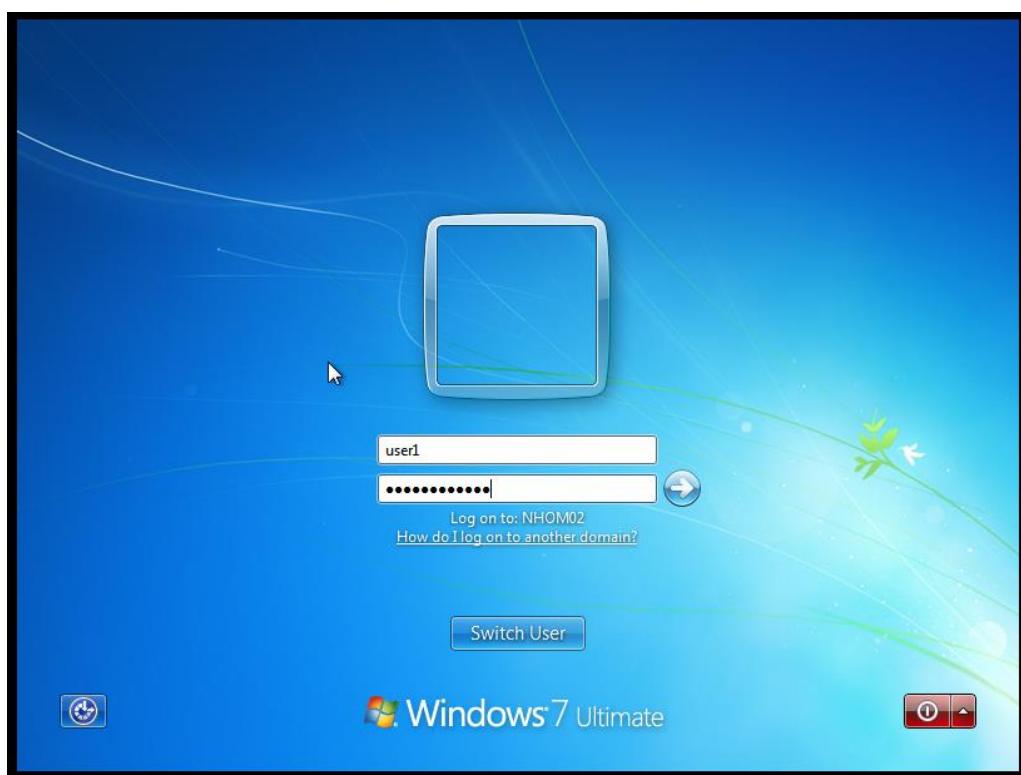




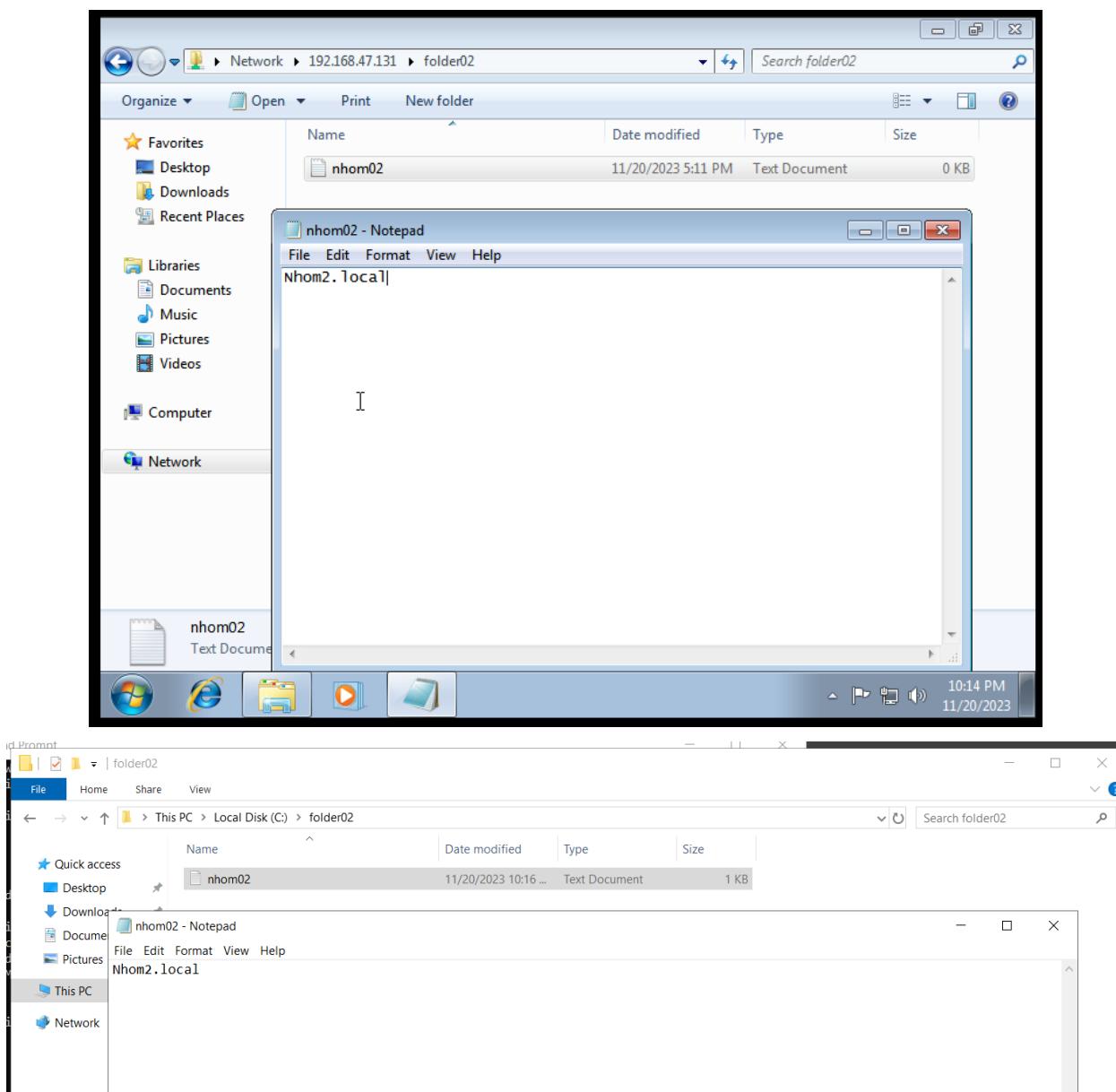
- Bước 6:** Phân quyền và chia sẻ file từ File Server
  - Đăng nhập lại vào File Server và thực hiện phân quyền lại folder02 của File Server.



- Bước 7:** Tại máy Client, đăng nhập với tài khoản NHOM02\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 **folder02** (giống với bài 1)



⇒ Ta có thể đọc file trong folder02 như bình thường, và khi chỉnh sửa file trong folder02, file tại folder02 ở File Server cũng bị thay đổi.

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

- **Mô hình Workgroup:**

- Người dùng và tài nguyên địa phương: Mỗi máy tính trong Workgroup duy trì danh sách người dùng và tài nguyên của riêng mình. Người dùng cần tạo tài khoản trên mỗi máy tính mà họ muốn truy cập.
- Xác thực Địa phương: Xác thực người dùng được thực hiện tại máy tính nơi người dùng đăng nhập. Mỗi máy tính xác thực người dùng mà nó chia sẻ.

- **Mô hình Active Directory:**

- Quản lý Tập trung: Active Directory duy trì một cơ sở dữ liệu chung với thông tin về người dùng, máy tính, và các đối tượng khác trong toàn bộ domain.
- Xác thực Trung tâm: Active Directory thực hiện xác thực tập trung, giúp người dùng đăng nhập vào bất kỳ máy tính nào trong domain sử dụng cùng một tài khoản và mật khẩu.

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

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

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

Trả lời:

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

- Active Directory là một dịch vụ quản lý tập trung của Microsoft, được sử dụng để quản lý tài nguyên mạng trong môi trường Windows.
- Một Additional Domain Controller (ADC) là một máy chủ được cấu hình để làm bổ sung cho một Primary Domain Controller (PDC) hoặc một Main Domain Controller (MDC). Trong mô hình Active Directory, có thể có nhiều máy chủ chạy dịch vụ Domain Controller để cung cấp redundancy và tăng khả năng chịu lỗi cho hệ thống. Khi có nhiều hơn một Domain Controller trong mạng, thông tin người dùng, nhóm, và các đối tượng khác trong Active Directory được sao chép giữa các máy chủ để đảm bảo tính nhất quán và khả năng truy cập từ nhiều vị trí.
- Khi một máy chủ Domain Controller (chẳng hạn như PDC) gặp sự cố, các ADC có thể tiếp tục cung cấp dịch vụ và duy trì tính nhất quán của Active Directory trong khi sự cố đang được giải quyết. Điều này giúp tăng cường khả năng chịu lỗi và khả năng sẵn sàng của hệ thống Active Directory.

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

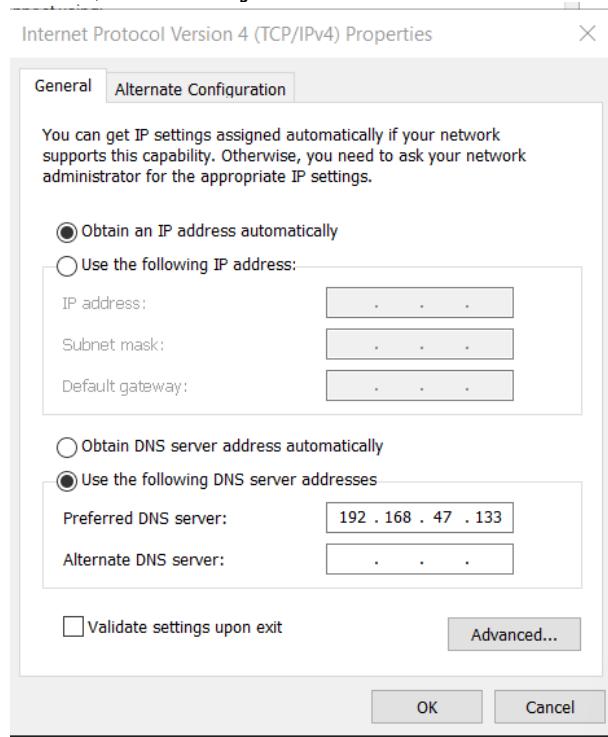
- Thu thập thông tin: ADC thu thập thông tin về các tài khoản người dùng từ hệ thống quản lý người dùng và thực hiện việc đồng bộ hóa dữ liệu với Active Directory. Thông tin bao gồm tên, email, tên đăng nhập, mật khẩu và các thông tin khác liên quan đến tài khoản người dùng.
- Kiểm tra dữ liệu: Sau khi thu thập thông tin, ADC kiểm tra tính hợp lệ của dữ liệu để đảm bảo chính xác và đầy đủ.
- Đồng bộ dữ liệu: Nếu dữ liệu được xác thực chính xác, ADC tiến hành cập nhật dữ liệu vào Active Directory. Quá trình đồng bộ này có thể được cấu hình theo nhiều cách khác nhau, ví dụ như tạo mới tài khoản người dùng, xóa tài khoản, thay đổi thông tin tài khoản, và nhiều hơn nữa.
- Giám sát và báo cáo: Mô hình ADC cho phép quản trị viên giám sát các hoạt động đồng bộ hóa và báo cáo về tình trạng hiện tại của hệ thống.

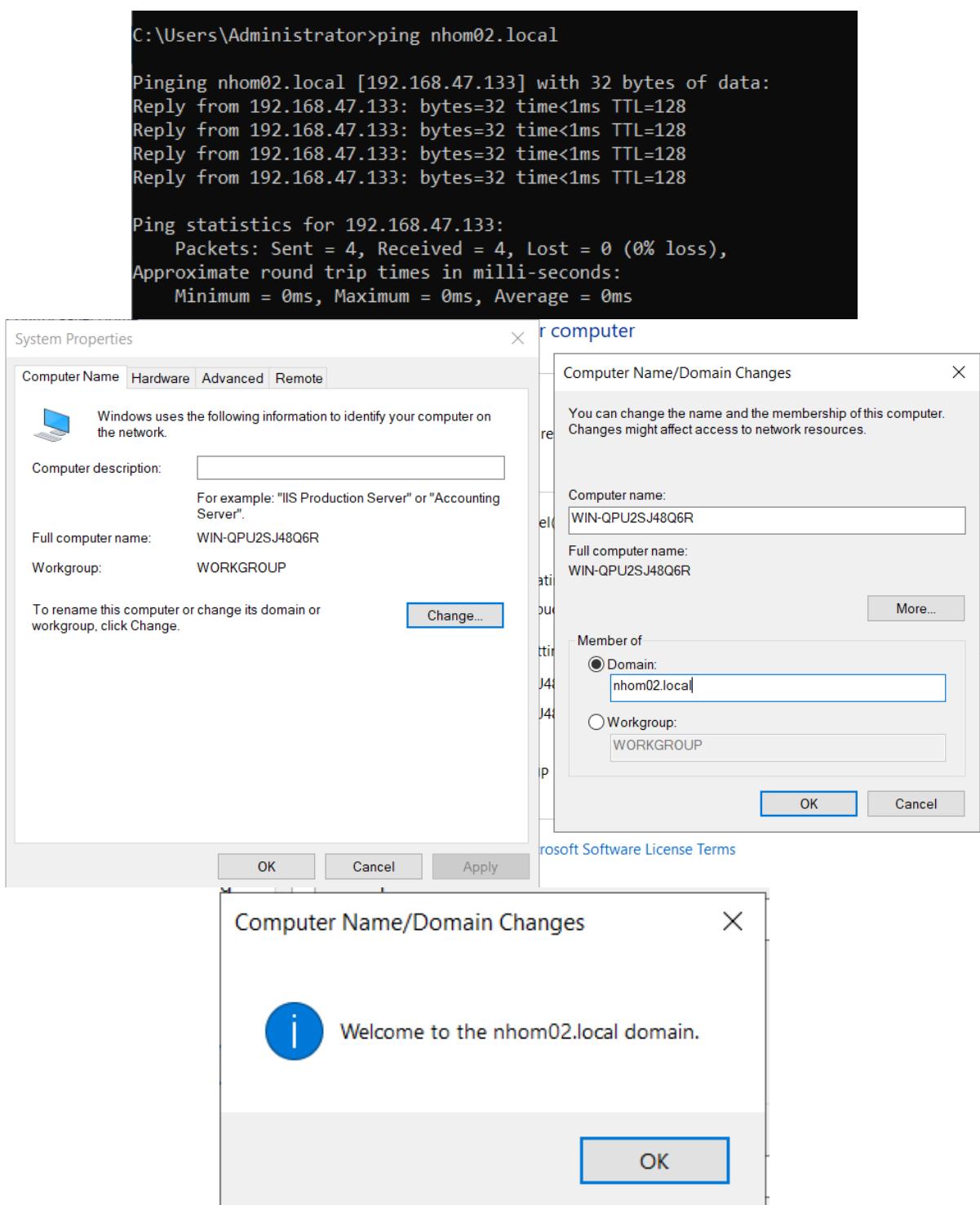
#### 3. Khi nào cần sử dụng ADC?

- Khi có nhiều Domain Controllers trong mạng, nếu một trong số chúng gặp sự cố, các ADC khác vẫn có thể tiếp tục cung cấp dịch vụ và duy trì tính nhất quán của Active Directory. Điều này giúp giảm thiểu ảnh hưởng của sự cố đối với khả năng sẵn sàng của hệ thống.
- Khi mạng có một lượng lớn người dùng hoặc thiết bị, việc có nhiều ADC có thể giảm áp lực cho một Domain Controller duy nhất và cải thiện hiệu suất hệ thống.
- Các ADC giúp phân tán tải công việc xử lý xác thực và giữ cho thông tin trong Active Directory được sao chép trên nhiều máy chủ. Điều này giúp đảm bảo tính nhất quán của dữ liệu và giảm nguy cơ mất dữ liệu nếu một máy chủ gặp sự cố.
- Trong môi trường có các chi nhánh địa lý khác nhau, việc triển khai ADC tại các địa điểm đó có thể cải thiện hiệu suất và giảm độ trễ cho người dùng tại những vị trí đó. Các ADC có thể giúp tăng cường bảo mật bằng cách phân tán quyền truy cập và quản lý chúng ở cấp độ địa chỉ IP hoặc vị trí vật lý khác nhau.

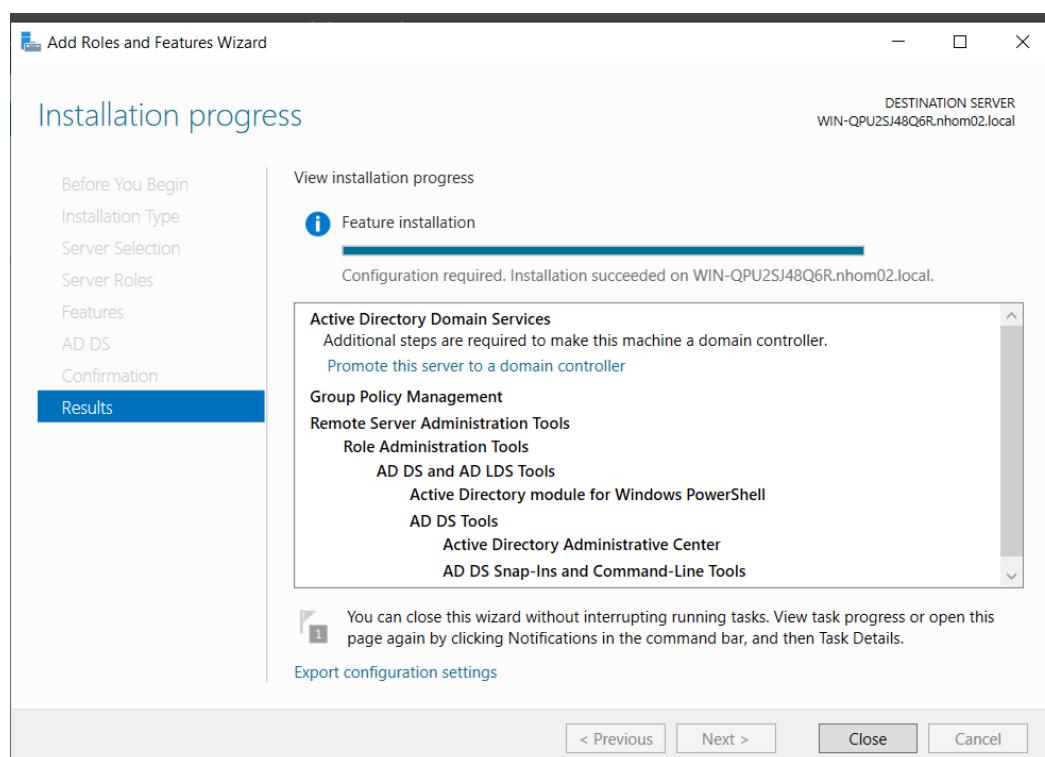
**Yêu cầu 3.2.** Sinh viên triển khai mô hình Additional Domain Controller theo yêu cầu bên dưới.

- **Bước 1:** Triển khai mô hình Additional Domain Controller (ADC) với thông tin trên.
- **Bước 2:** Thực hiện các công việc sau và kiểm tra kết quả (X là số thứ tự nhóm)
  - Tạo user ua1X trên Primary DC. Kiểm tra thông tin user này trên Additional DC.
  - Tạo user ua2X trên Additional DC. Kiểm tra thông tin user này trên Primary DC.
  - Tắt máy Primary DC, thêm user ua3X trên Additional DC. Sau đó mở lại Primary DC và kiểm tra thông tin user này trên Primary DC.
  - Tắt máy Primary DC, login ua2X trên máy Client. Giải thích kết quả.
- Trước tiên ta sửa DNS, thêm máy ADC vào domain nhom02.local

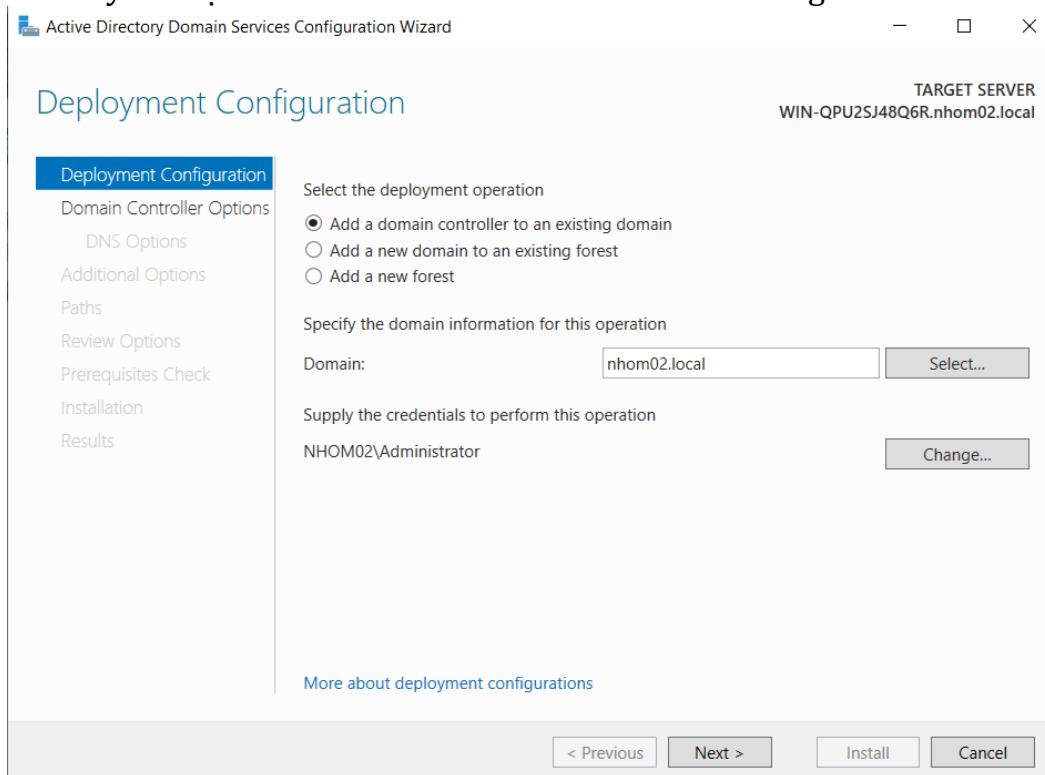




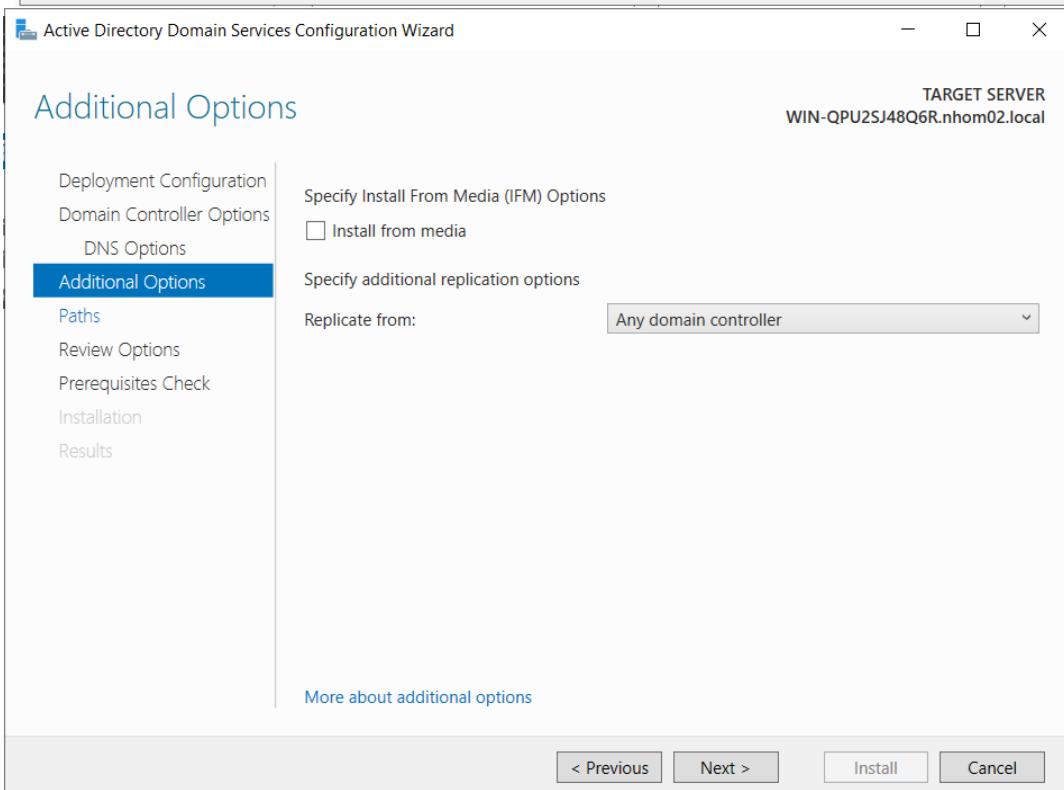
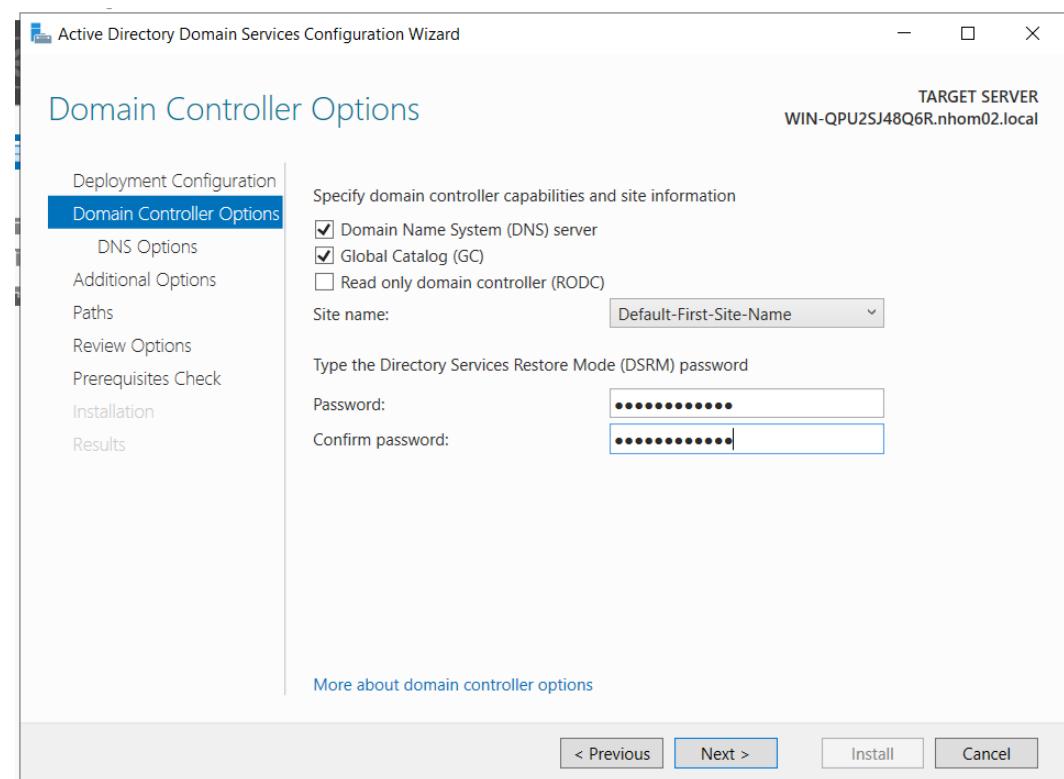
- Tiếp theo ta sẽ cấu hình máy thành ADC
  - Bắt đầu cài đặt như yêu cầu 2 nhưng ở phần nâng cấp thành AD sẽ có khác biệt

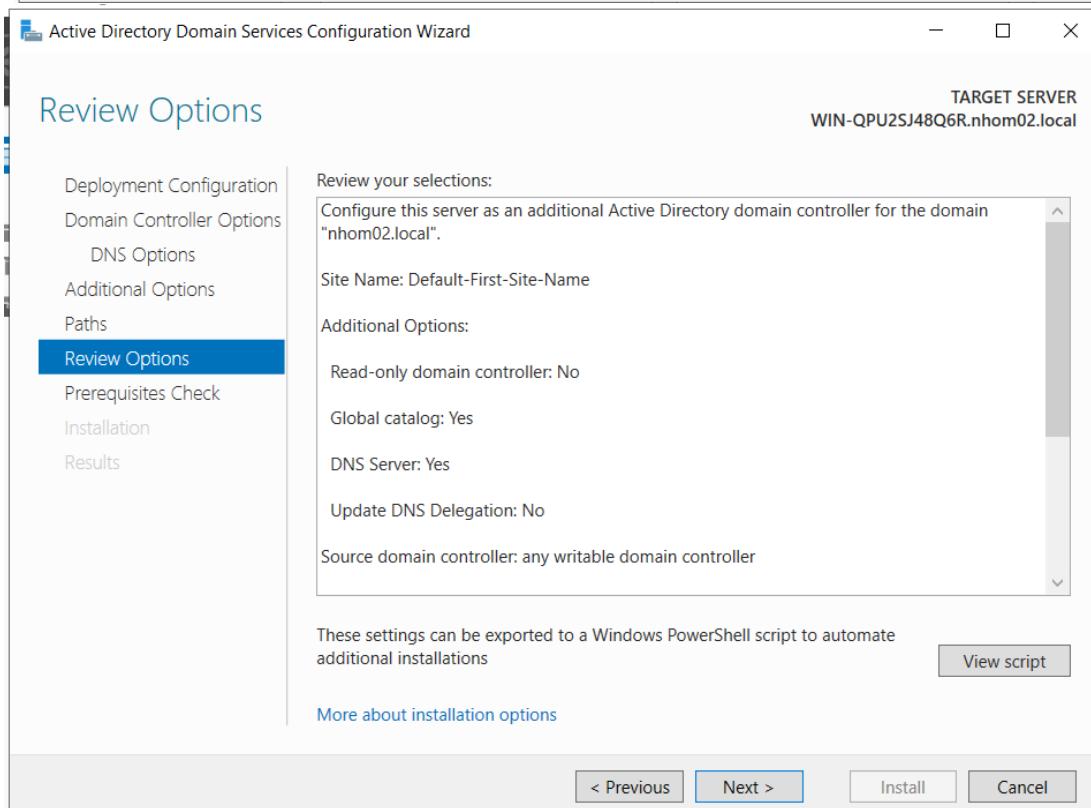
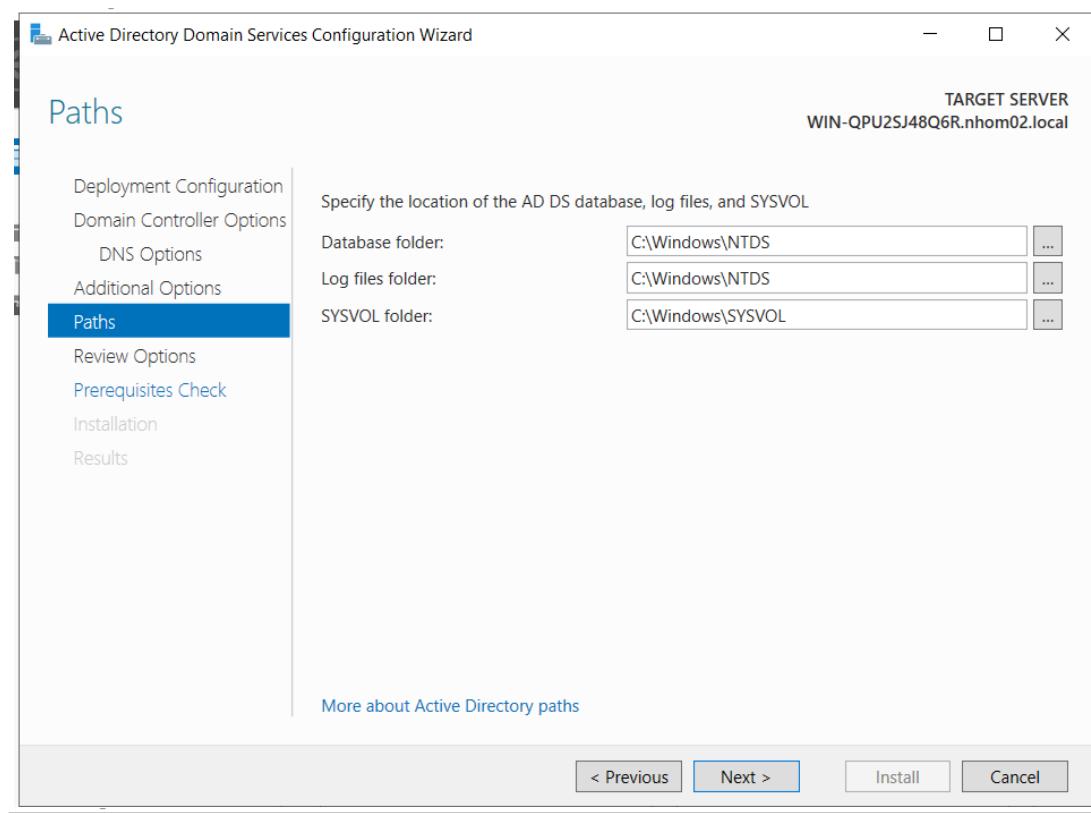


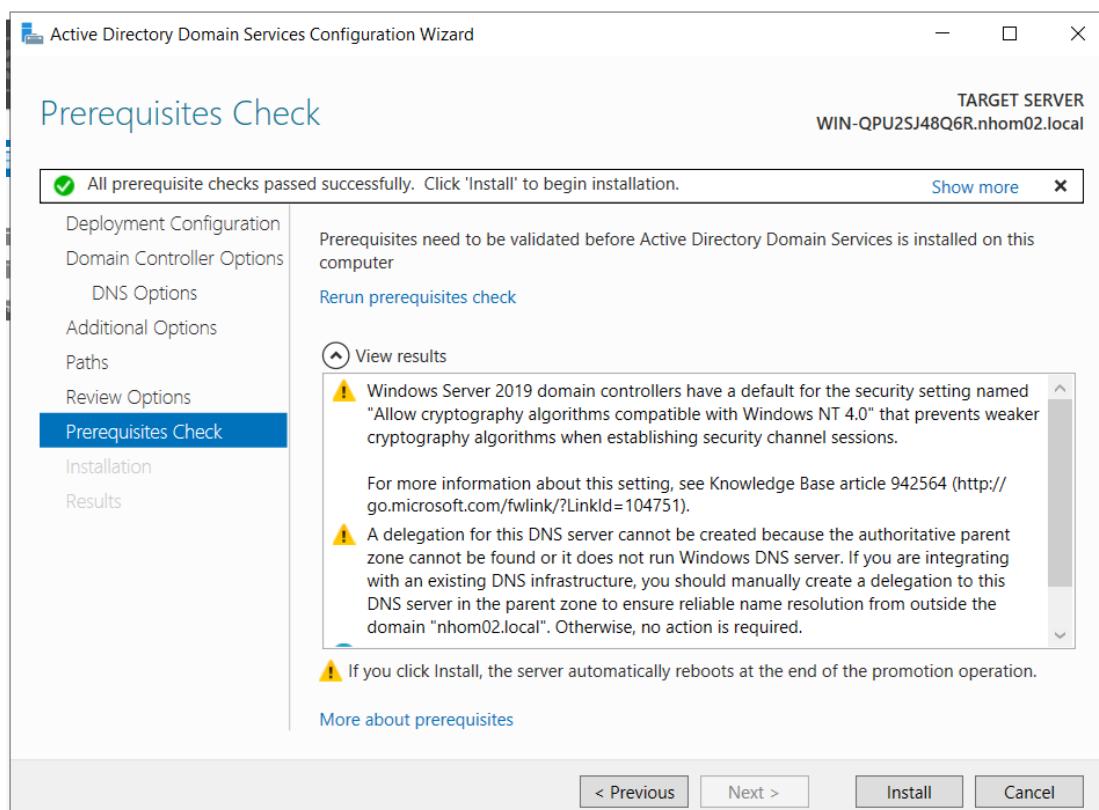
- Ở đây ta chọn “Add a domain controller to an existing domain”



- Thiết lập DSRM password là Nhom02.local







- Tạo user ua12 trên Primary DC

Create in: nhom02.local/

First name: ua12      Initials:

Last name:

Full name: ua12

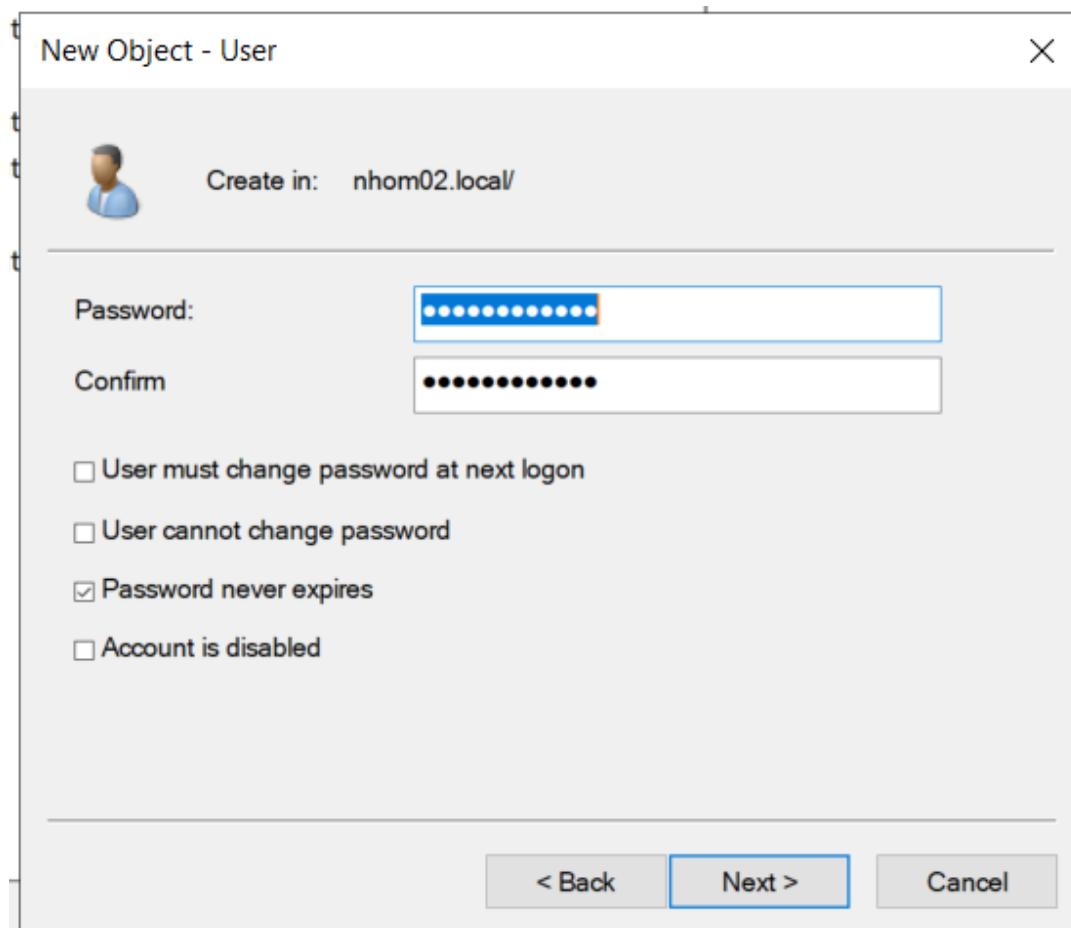
User logon name:

ua16 @nhom02.local

User logon name (pre-Windows 2000):

NHOM02\ua16

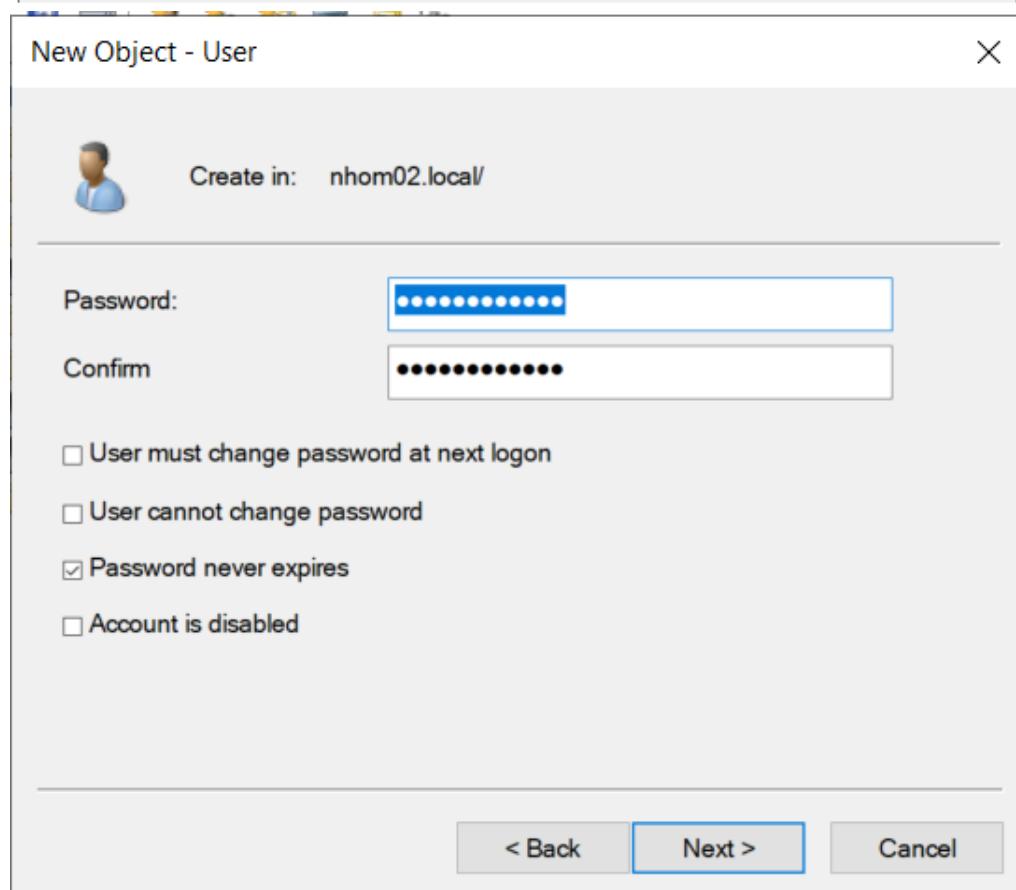
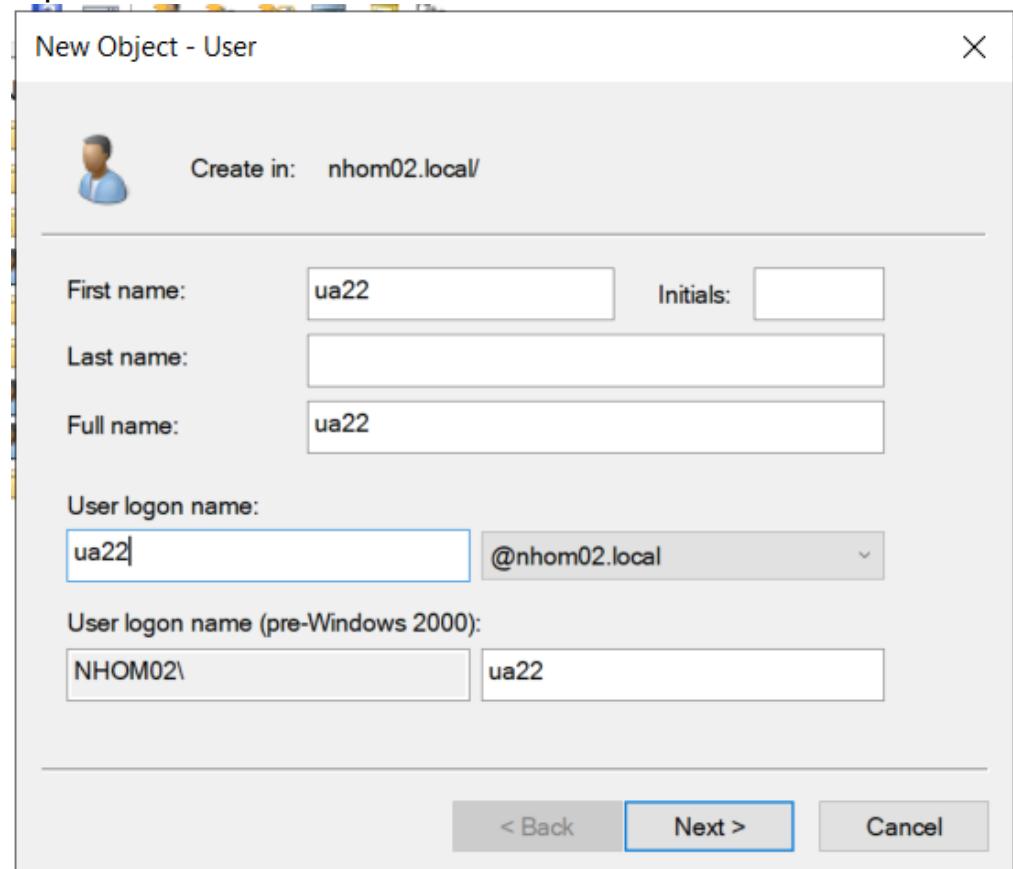
< Back      Next >      Cancel



- Kiểm tra thông tin user này trên Additional DC. Ta thấy **ua12** đã có trong bảng users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational ...	Default container for do...
File Admin	User	
ForeignSecur...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
<b>ua12</b>	User	
User 1	User	
Users	Container	Default container for up...

- Tạo user ua22 trên Additional DC.



- Kiểm tra thông tin user này trên Primary DC. Ta thấy **ua22** đã có trong bảng Users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Controllers	Organizational ...	Default container for do...
File Admin	User	
ForeignSecurityPrincipals	Container	Default container for sec...
Managed Service Accou...	Container	Default container for ma...
ua12	User	
ua22	User	
User 1	User	
Users	Container	Default container for up...

- Tắt máy Primary DC, thêm user **ua32** trên Additional DC.

New Object - User

Create in: nhom02.local/

First name: ua33 Initials:

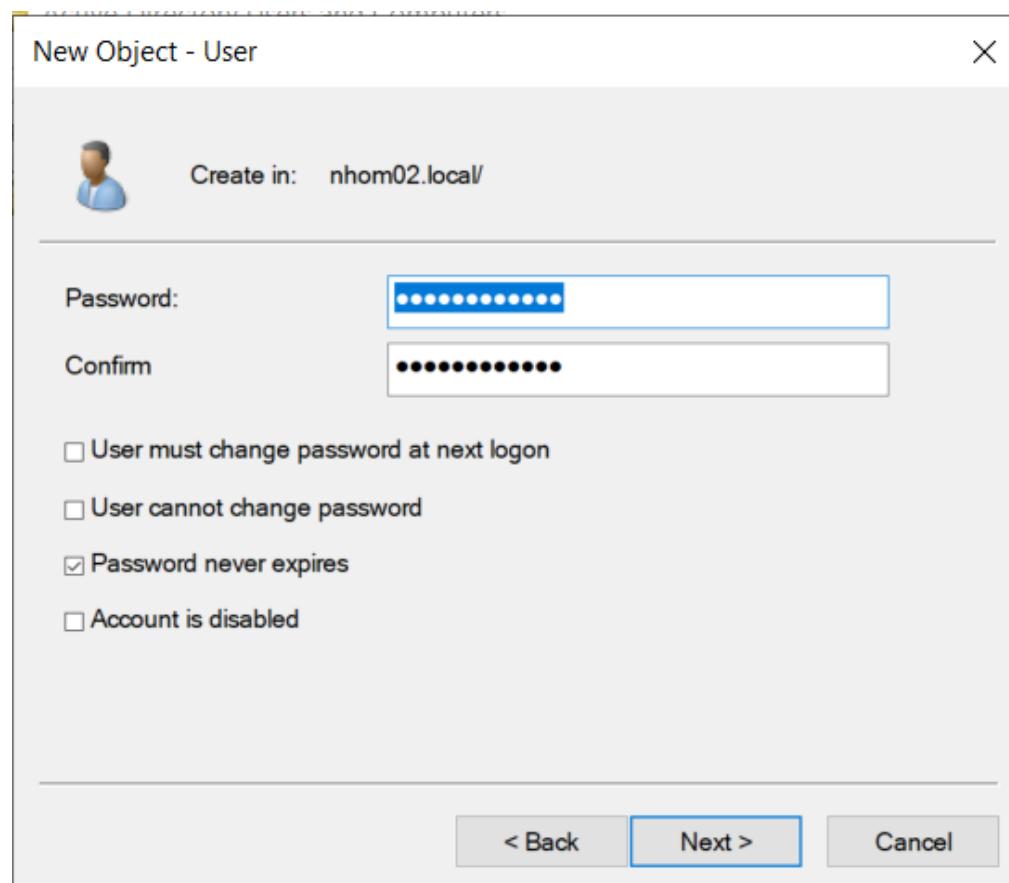
Last name:

Full name: ua33

User logon name:  
ua33 @nhom02.local

User logon name (pre-Windows 2000):  
NHOM02\ ua33

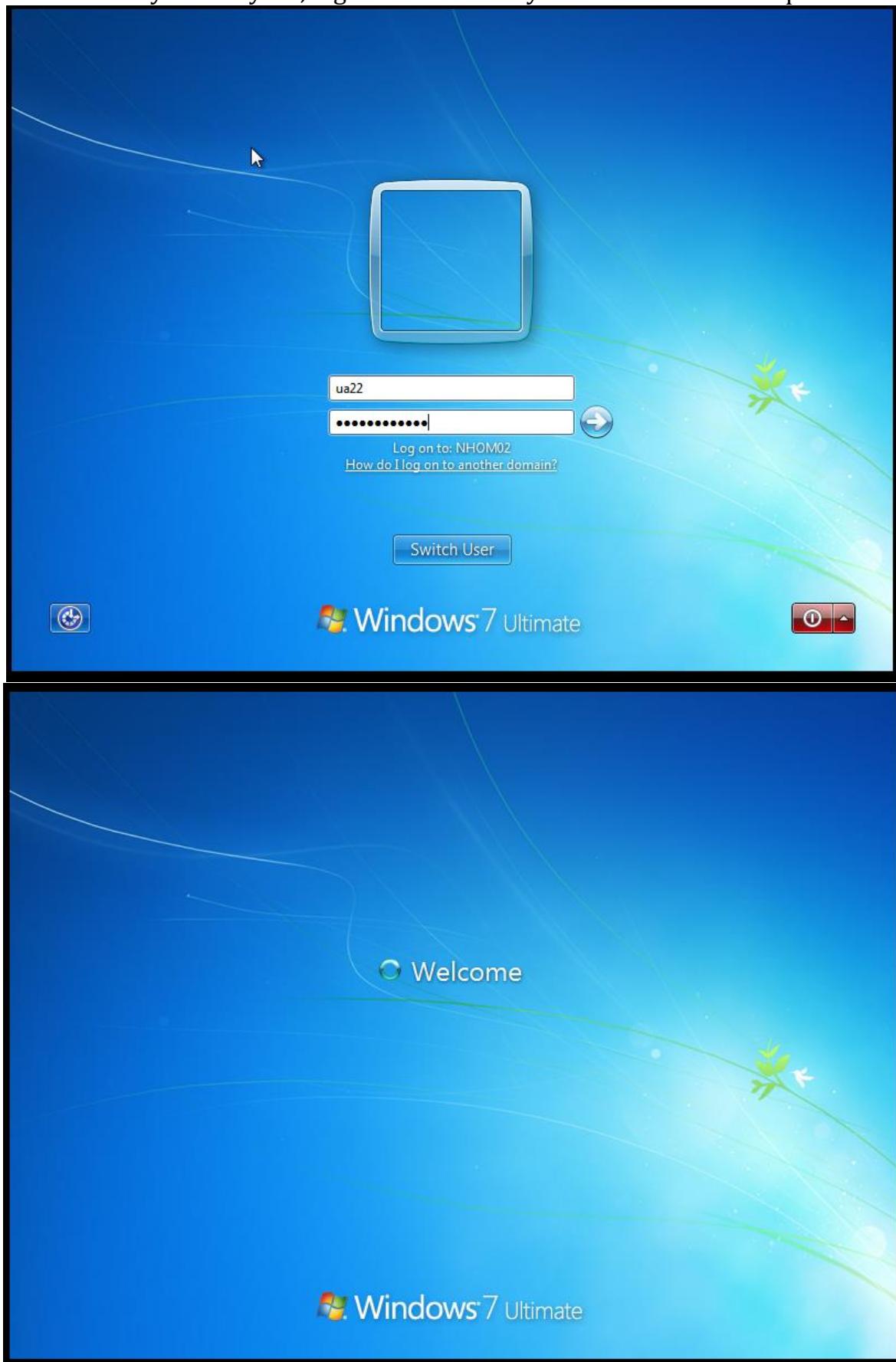
< Back Next > Cancel



- Sau đó mở lại Primary DC và kiểm tra thông tin user này trên Primary DC. Ta thấy **ua33** đã có trong bảng Users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for up...
Domain Con...	Organizational ...	Default container for do...
ForeignSecur...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
File Admin	User	
ua12	User	
ua22	User	
ua33	User	
User 1	User	

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



⇒ Ta thấy đăng nhập thành công. ADC đã chịu trách nhiệm đăng nhập trong lúc PDC không hoạt động

#### 4. Xây dựng mô hình Read-only Domain Controller

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

1. Read-Only Domain Controller (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?

*Trả lời:*

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

- RODC là một loại Domain Controller trong môi trường Active Directory, nhưng khác với các Domain Controller thông thường (bao gồm cả PDC, MDC, và các ADC), RODC chủ yếu chỉ cho phép đọc dữ liệu từ Active Directory. Nó không thể ghi (write) thông tin vào cơ sở dữ liệu Active Directory.
  - RODC là một phần trong chiến lược bảo mật của Microsoft và thường được triển khai trong các môi trường phức tạp với nhiều chi nhánh và vị trí địa lý.
2. Mô hình RODC hoạt động như thế nào?

Mô hình RODC (Read-Only Domain Controller) hoạt động như một phần của hệ thống Active Directory, nhưng với một số đặc điểm chủ yếu liên quan đến quyền truy cập và bảo mật.

Chi tiết cách mô hình RODC hoạt động:

- Sinh dữ liệu từ Domain Controller chính (PDC hoặc MDC): Ban đầu, dữ liệu từ Domain Controller chính (Primary Domain Controller hoặc Main Domain Controller) được sao chép đến RODC. Dữ liệu này bao gồm thông tin về người dùng, nhóm, chính sách, và các đối tượng khác trong Active Directory.
- Chỉ đọc, không ghi (Read-Only): Sau khi dữ liệu được sao chép, RODC chỉ cho phép đọc dữ liệu từ Active Directory, không thể thực hiện các thao tác ghi. Điều này bảo vệ dữ liệu khỏi sự thay đổi không mong muốn và giảm nguy cơ bảo mật.
- Quản lý quyền truy cập local: RODC lưu trữ một bản sao của dữ liệu Active Directory địa phương, giảm độ trễ cho người dùng và ứng dụng tại chi nhánh cụ thể. Nó quản lý quyền truy cập địa phương, giảm áp lực trên đường truyền mạng giữa chi nhánh và trung tâm dữ liệu.
- Cache thông tin local: RODC lưu trữ một cache thông tin địa phương, giúp cung cấp dữ liệu nhanh chóng khi có yêu cầu đọc từ các máy trạm và người dùng tại chi nhánh.
- Quản lý xác thực: RODC có khả năng xác thực người dùng tại local mà không cần gửi yêu cầu xác thực đến Domain Controller chính. Điều này giảm độ trễ và tăng hiệu suất cho người dùng tại chi nhánh.
- Đảm bảo tính nhất quán: Dữ liệu địa phương được cập nhật thông qua quá trình trao đổi và đồng bộ hóa từ Domain Controller chính khi cần thiết, đảm bảo tính nhất quán của Active Directory.

Mô hình RODC thường được triển khai trong các môi trường có nhiều chi nhánh và vị trí địa lý để cải thiện hiệu suất, tính nhất quán và bảo mật trong hệ thống Active Directory.

### 3. Khi nào cần sử dụng RODC?

Những trường hợp cần sử dụng RODC:

- Khi có nhiều chi nhánh hoặc vị trí địa phương và muốn giảm độ trễ cho người dùng tại các địa điểm đó. RODC giúp cung cấp dữ liệu địa phương mà không cần phải truy cập DC chính từ xa.
- Trong các môi trường không an toàn, nơi mà an ninh có thể bị đe dọa, RODC giảm nguy cơ lộ thông tin do nó chỉ cho phép đọc dữ liệu và không thể thực hiện các thao tác ghi.
- Khi cần cải thiện tính nhất quán của dữ liệu Active Directory và giảm áp lực trên đường truyền mạng bằng cách lưu trữ bản sao của dữ liệu địa phương, giúp giảm độ trễ cho người dùng và ứng dụng.
- RODC có thể giúp cải thiện hiệu suất cho người dùng tại các chi nhánh bằng cách giảm thời gian phản hồi và tăng khả năng đáp ứng.
- Trong các vị trí không an toàn, nơi mà an ninh có thể bị đe dọa, triển khai RODC giúp giảm nguy cơ bị chiếm đóng và bảo vệ thông tin quan trọng của Active Directory.
- Trong môi trường có nhiều chi nhánh nhỏ hoặc có băng thông mạng hạn chế, việc triển khai RODC có thể giúp tối ưu hóa giao thông mạng và cải thiện hiệu suất.
- RODC có khả năng xác thực người dùng tại địa phương mà không cần truy cập DC chính, giảm độ trễ và tăng khả năng chịu lỗi.

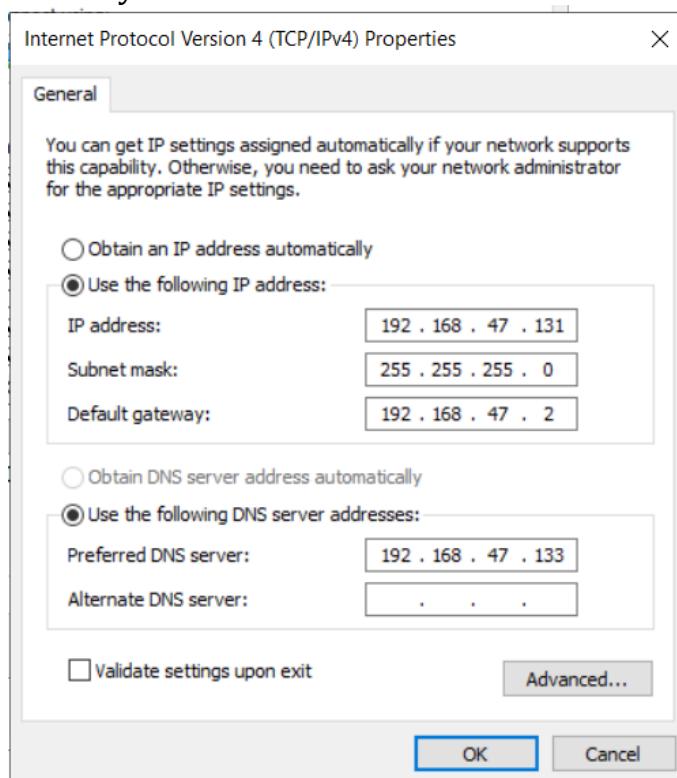
### 4. So sánh sự khác nhau giữa mô hình ADC và mô hình RODC?

- Sự khác nhau chính giữa hai mô hình này là RODC cung cấp tính năng bảo mật cao hơn so với ADC. Việc sử dụng RODC giúp giảm thiểu rủi ro bị tấn công từ bên ngoài, vì khi các máy chủ ADC bị tấn công và thông tin trên máy chủ này bị xâm nhập, hacker sẽ không thể tạo ra các thay đổi trên hệ thống do RODC chỉ có chức năng đọc thông tin từ các máy chủ ADC.
- Ngoài ra, sử dụng RODC cũng giúp tăng hiệu suất và tính khả dụng của hệ thống Active Directory, bởi vì khi một máy chủ ADC bị tắt hoặc không thể truy cập được, RODC vẫn có thể phục vụ người dùng.
- Tuy nhiên, việc triển khai mô hình RODC cũng có nhược điểm là không thể đáp ứng yêu cầu cho các ứng dụng cần quản lý và cập nhật thông tin trên Active Directory. Do đó, việc lựa chọn sử dụng mô hình ADC hay RODC phải dựa trên các yêu cầu cụ thể của hệ thống và môi trường kinh doanh.

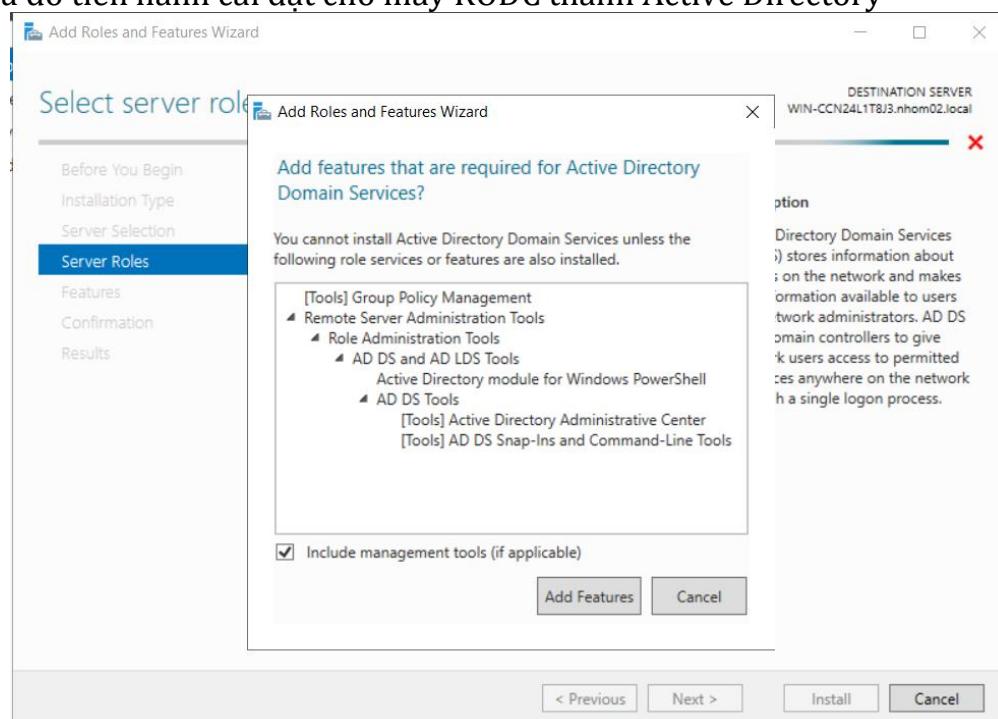
**Yêu cầu 4.2** Sinh viên triển khai mô hình Read-Only Domain Controller theo yêu cầu bên dưới

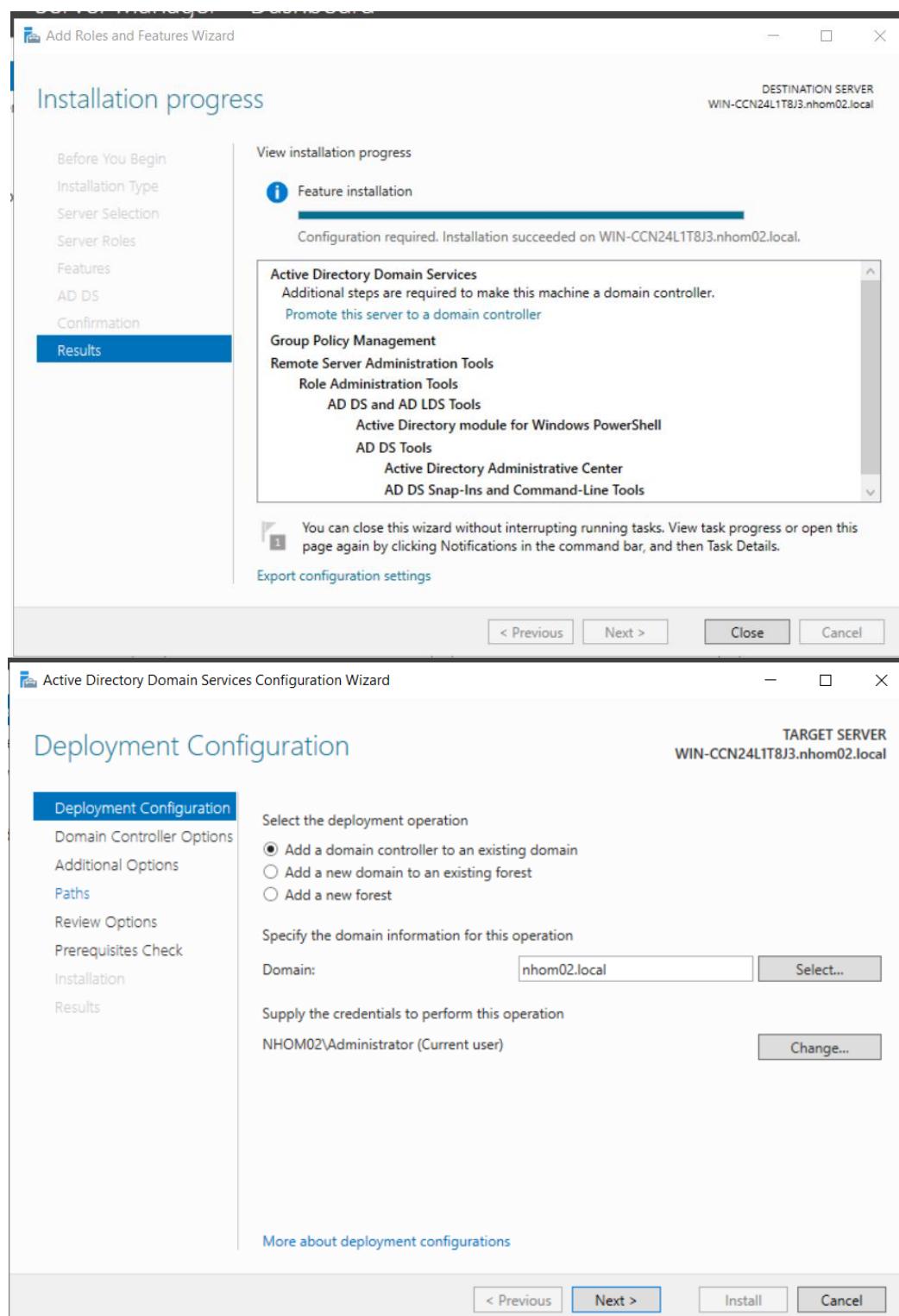
- **Bước 1:** Triển khai mô hình Read-Only Domain Controller (RODC) với thông tin như trên.
- **Bước 2:** Thực hiện các công việc sau và kiểm tra kết quả (X là số thứ tự nhóm)
  - Tạo user ur1X trên Primary DC. Kiểm tra thông tin user này trên Read-Only DC.

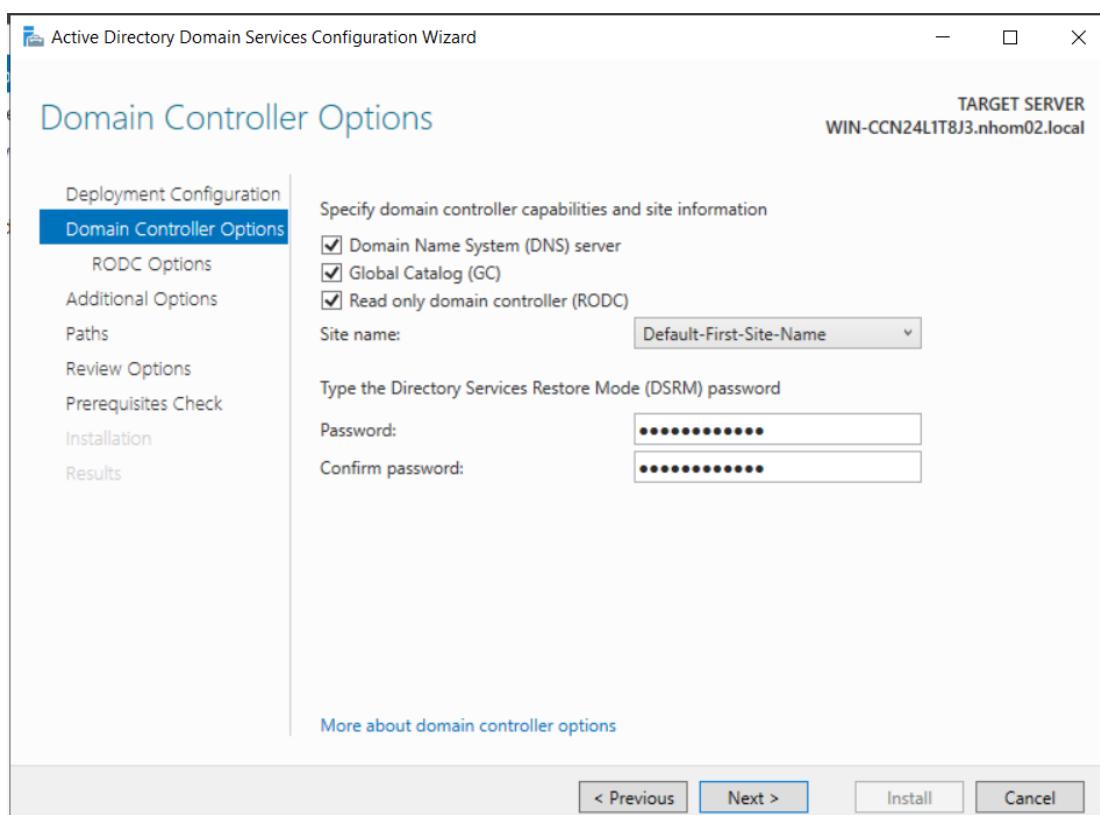
- Tạo user ur2X trên Read-Only DC. Kiểm tra thông tin user này trên Primary DC.
- Tắt máy Read-Only DC, thêm user ur3X trên Primary DC. Sau đó mở lại Read-Only DC và kiểm tra thông tin user này trên Read-Only DC.
- Tắt máy Primary DC, login ur2X trên máy Client. Giải thích kết quả.
- Tắt máy Read-Only DC, login ur3X trên máy Client. Giải thích kết quả.
- Cấu hình DNS cho máy RODC



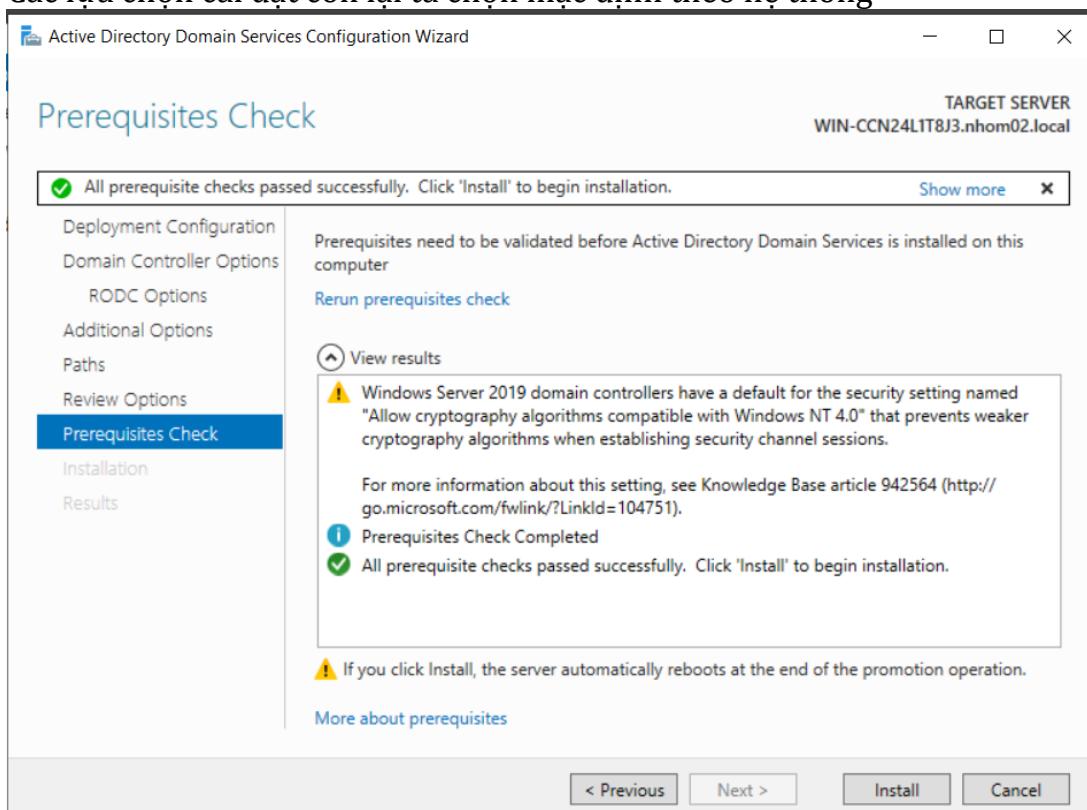
- Sau đó tiến hành cài đặt cho máy RODC thành Active Directory



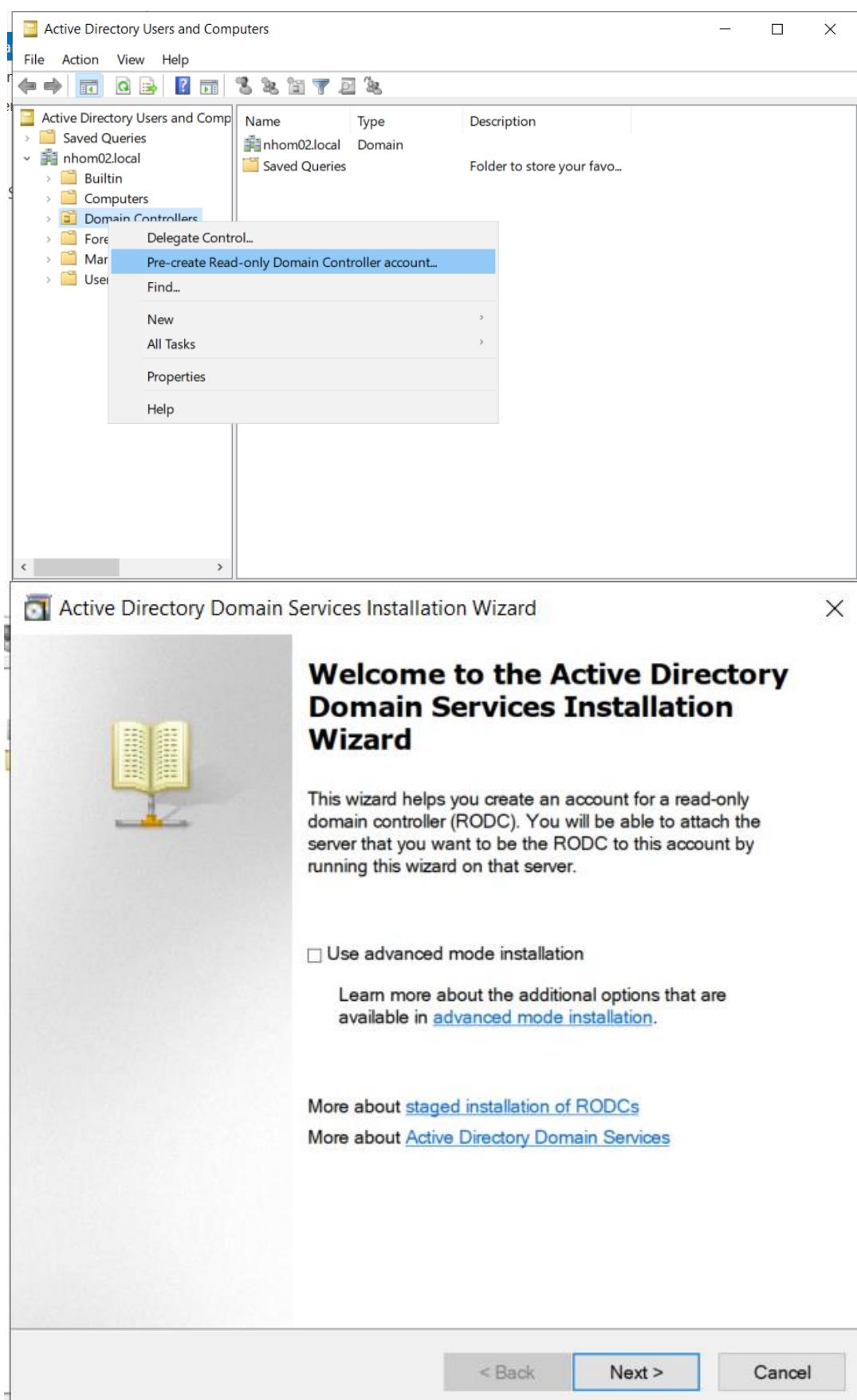


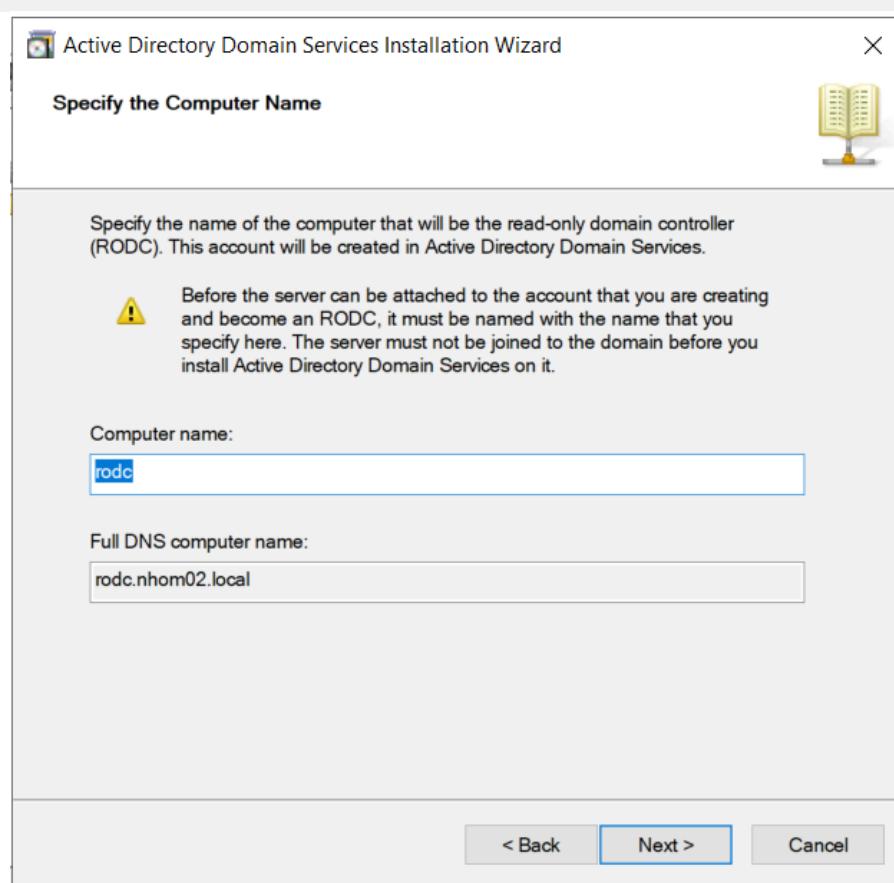
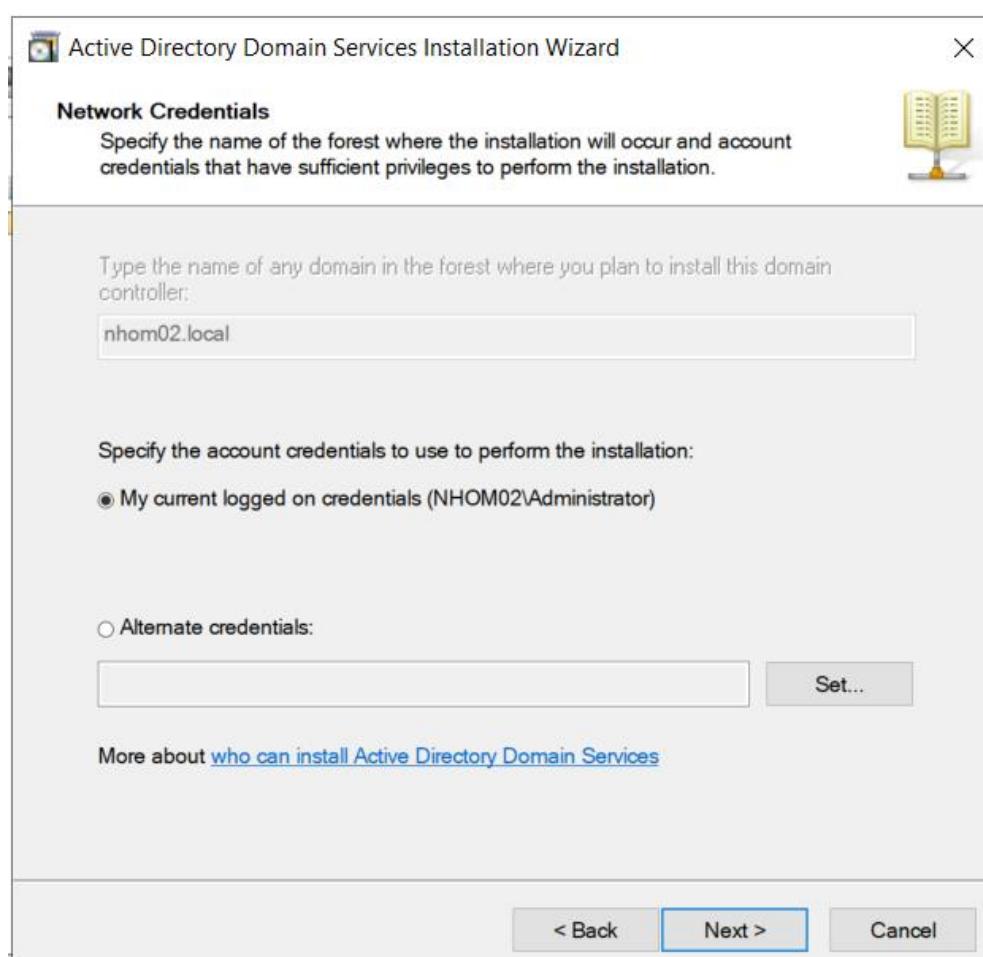


- Các lựa chọn cài đặt còn lại ta chọn mặc định theo hệ thống



- Sau khi cài đặt thành công, máy sẽ tự động restart
- Cuối cùng ta tạo account quản lý RODC này





**Active Directory Domain Services Installation Wizard**

**Select a Site**  
Select a site for the new domain controller.

Sites:

Site	Description
Default-First-Site-Name	

< Back      Next >      Cancel

**Active Directory Domain Services Installation Wizard**

**Additional Domain Controller Options**

Select additional options for this domain controller.

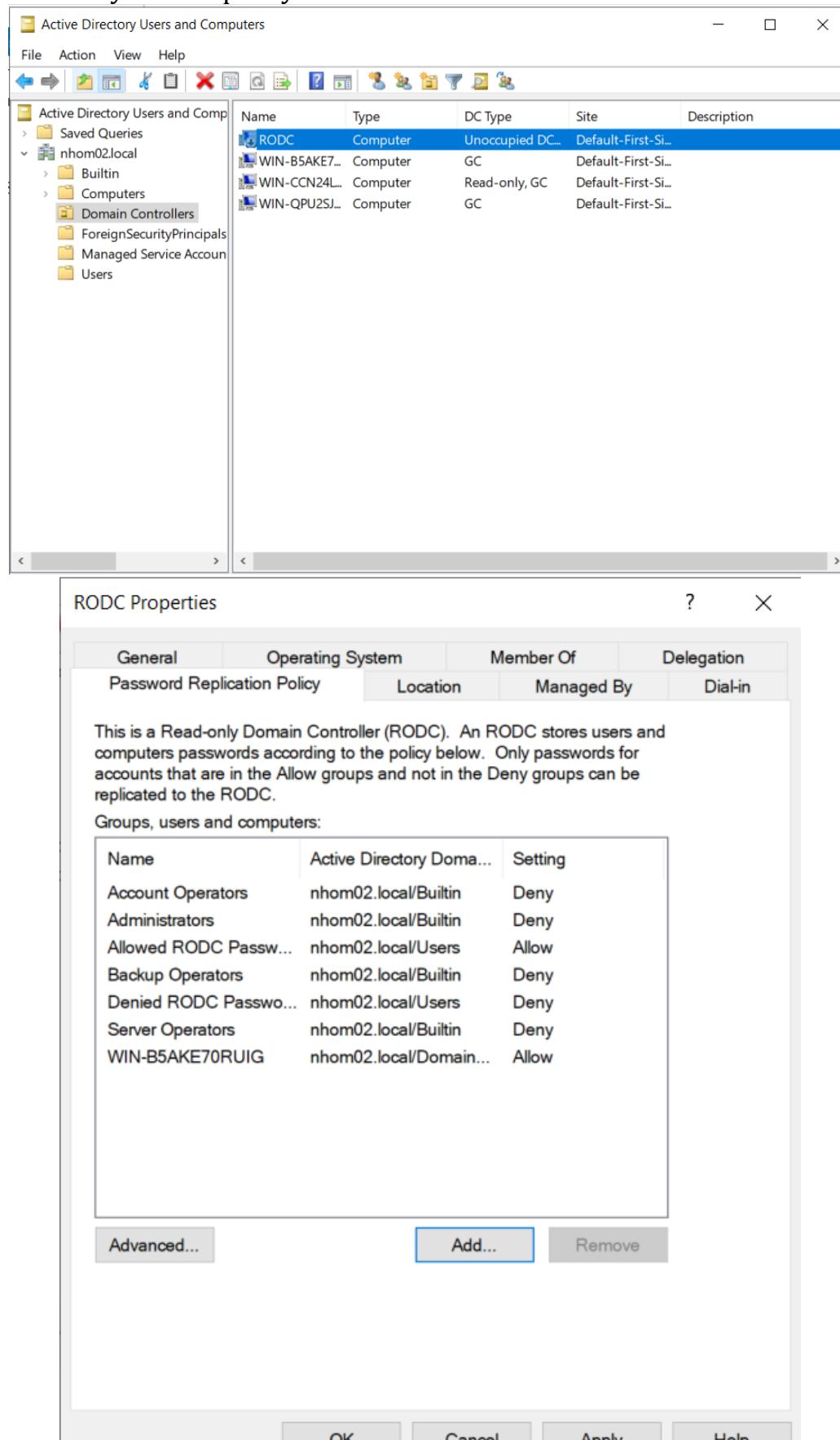
DNS server  
 Global catalog  
 Read-only domain controller (RODC)

Additional information:  
There are currently 2 DNS servers that are registered as authoritative name servers for this domain.

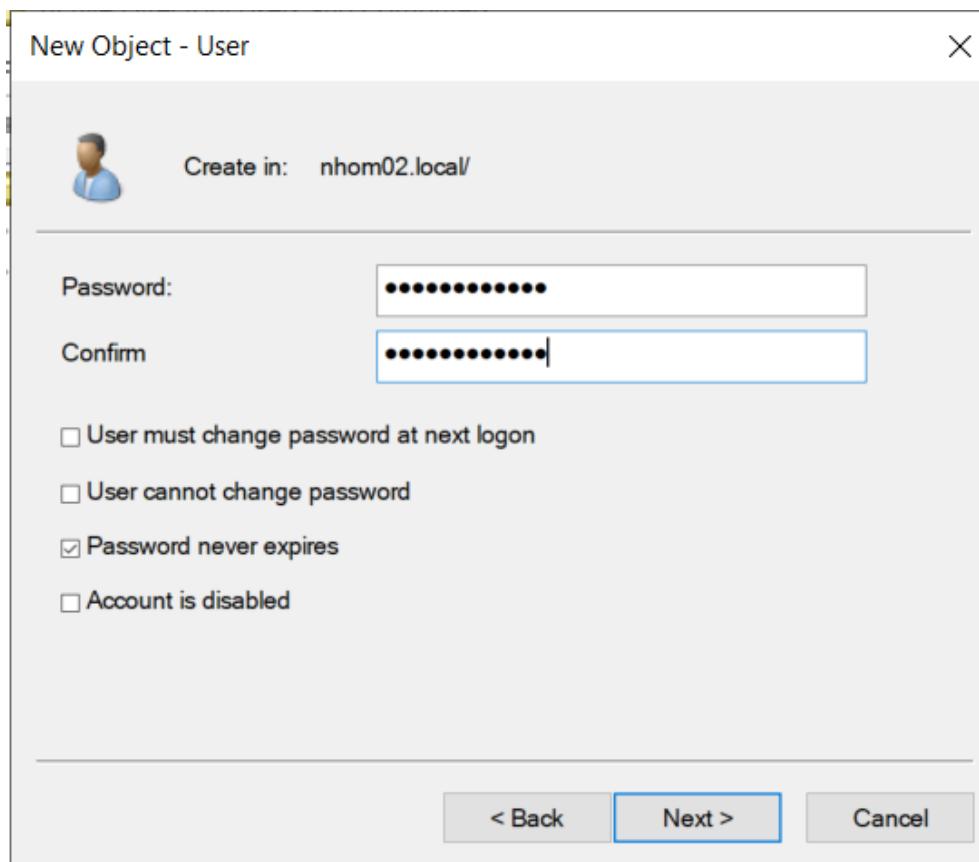
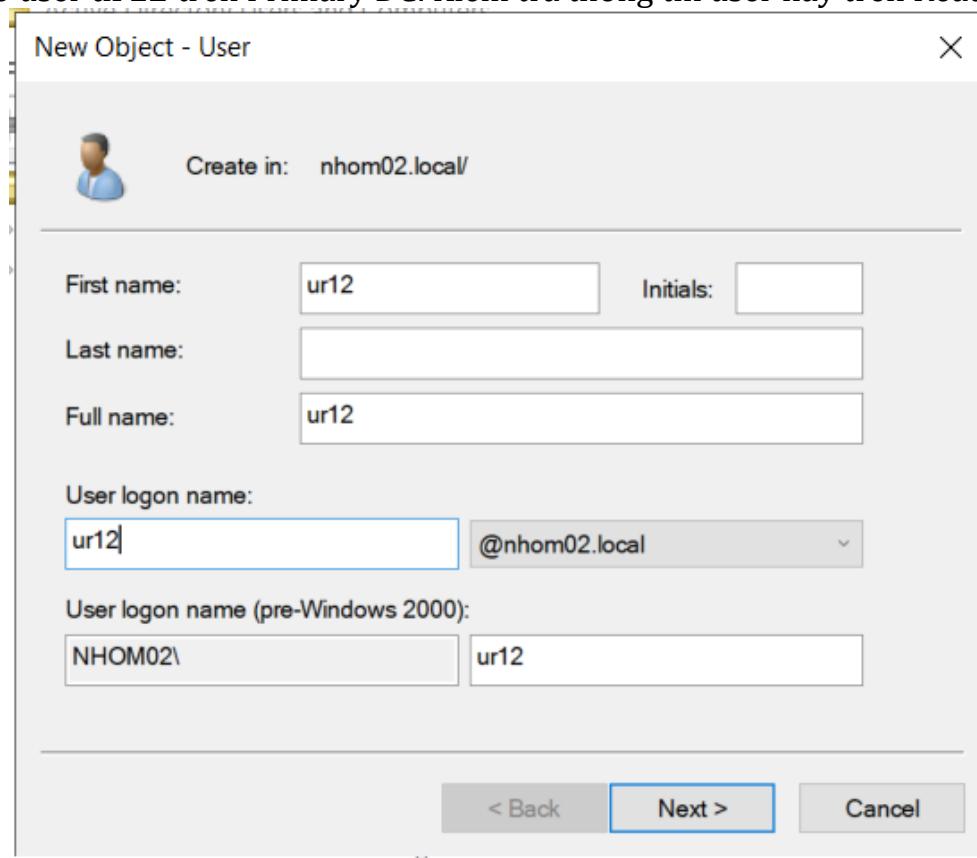
More about [additional domain controller options](#)

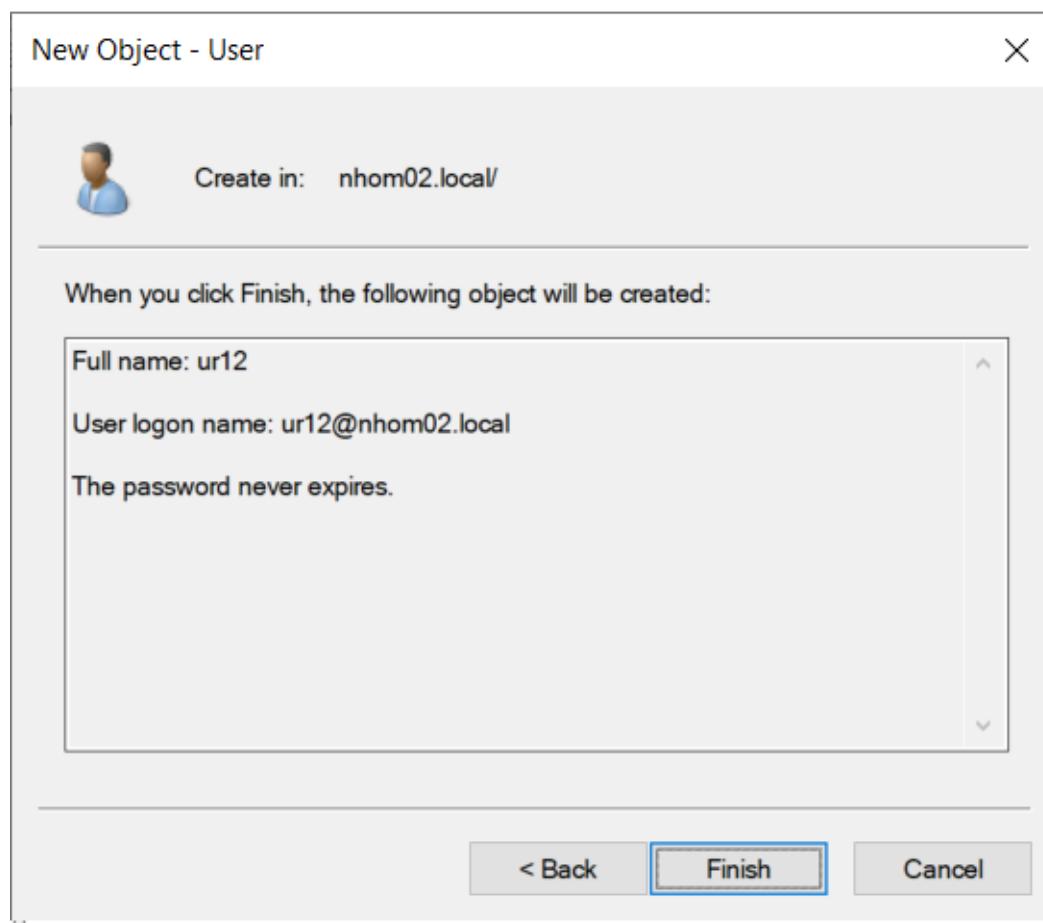
< Back      Next >      Cancel

- Ta add máy AD vào policy của RODC



- Tạo user **ur12** trên Primary DC. Kiểm tra thông tin user này trên Read-Only DC.

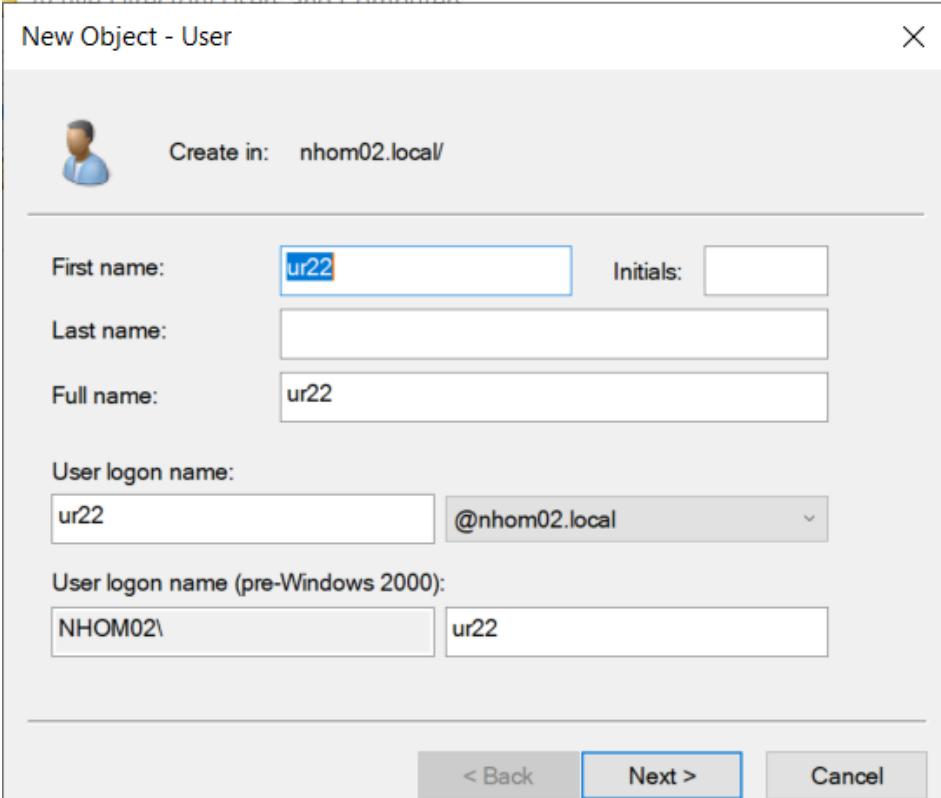
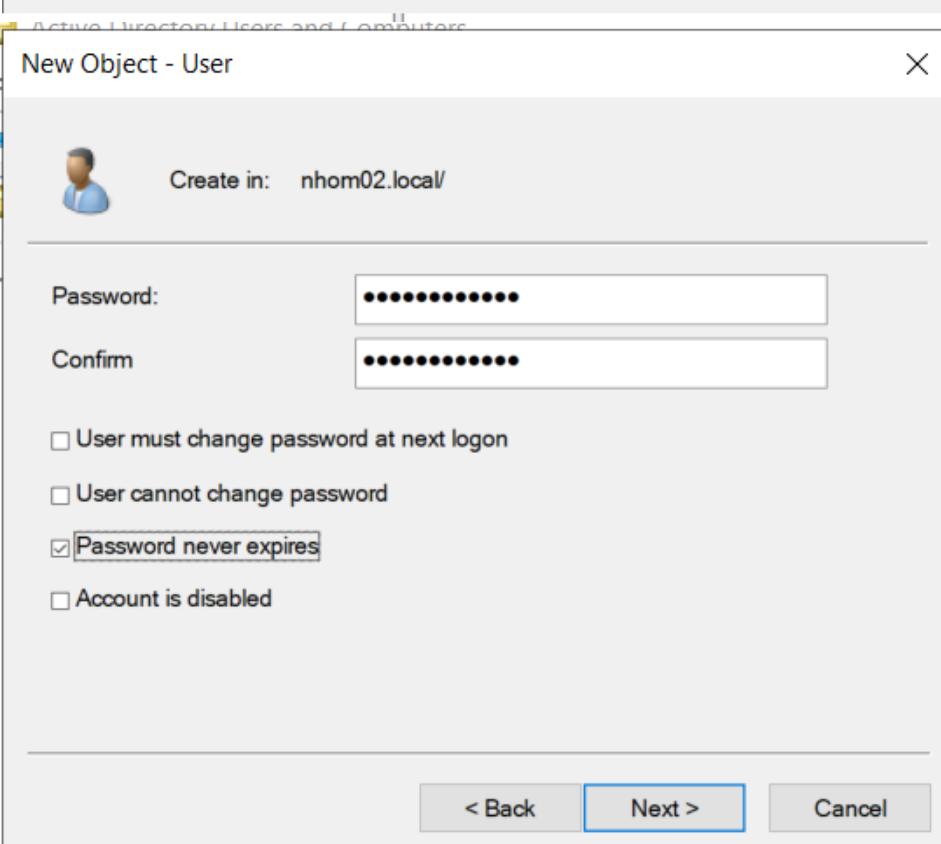


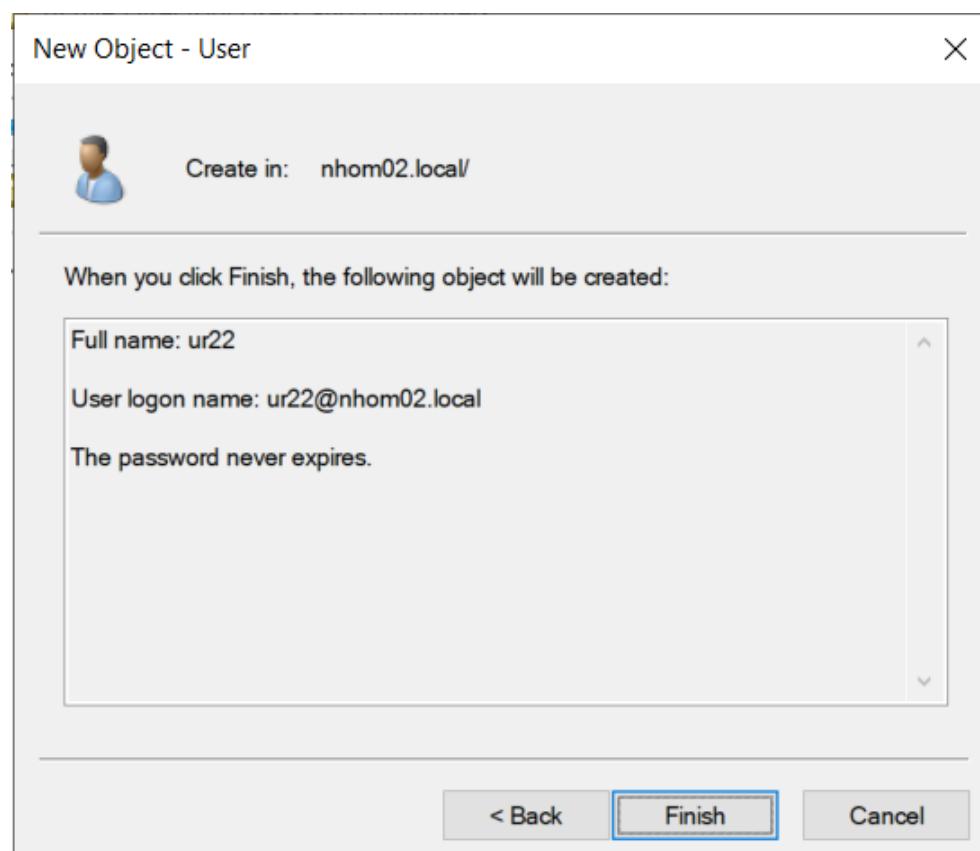


- Kiểm tra trên máy RODC. Ta thấy **ur12** đã có trong bảng **Users**

Name	Type
Builtin	builtinDomain
Computers	Container
Domain Controllers	Organizational
ForeignSecurityPrincip...	Container
Managed Service Acco...	Container
Users	Container
File Admin	User
ua12	User
ua22	User
ua33	User
<b>ur12</b>	<b>User</b>
User 1	User

- Tạo user ur22 trên Read-Only DC. Kiểm tra thông tin user này trên Primary DC.



- Kiểm tra trên PDC. Ta thấy **ur22** đã có trên bảng Users

ur22 Properties			
Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	
<b>General</b>	Address	Account	Profile
			Telephones
			Organization
ur22			
First name: <input type="text" value="ur22"/> Initials: <input type="text"/>			
Last name: <input type="text"/>			
Display name: <input type="text" value="ur22"/>			
Description: <input type="text"/>			
Office: <input type="text"/>			
Telephone number: <input type="text"/> Other...			
E-mail: <input type="text"/>			
Web page: <input type="text"/> Other...			

- Tắt máy Read-Only DC, thêm user **ur32** trên Primary DC. Sau đó mở lại Read-Only DC và kiểm tra thông tin user này trên Read-Only DC.

New Object - User

Create in: nhom02.local/

First name: ur33 Initials:

Last name:

Full name: ur33

User logon name:  
ur33 @nhom02.local

User logon name (pre-Windows 2000):  
NHOM02\ur33

< Back Next > Cancel

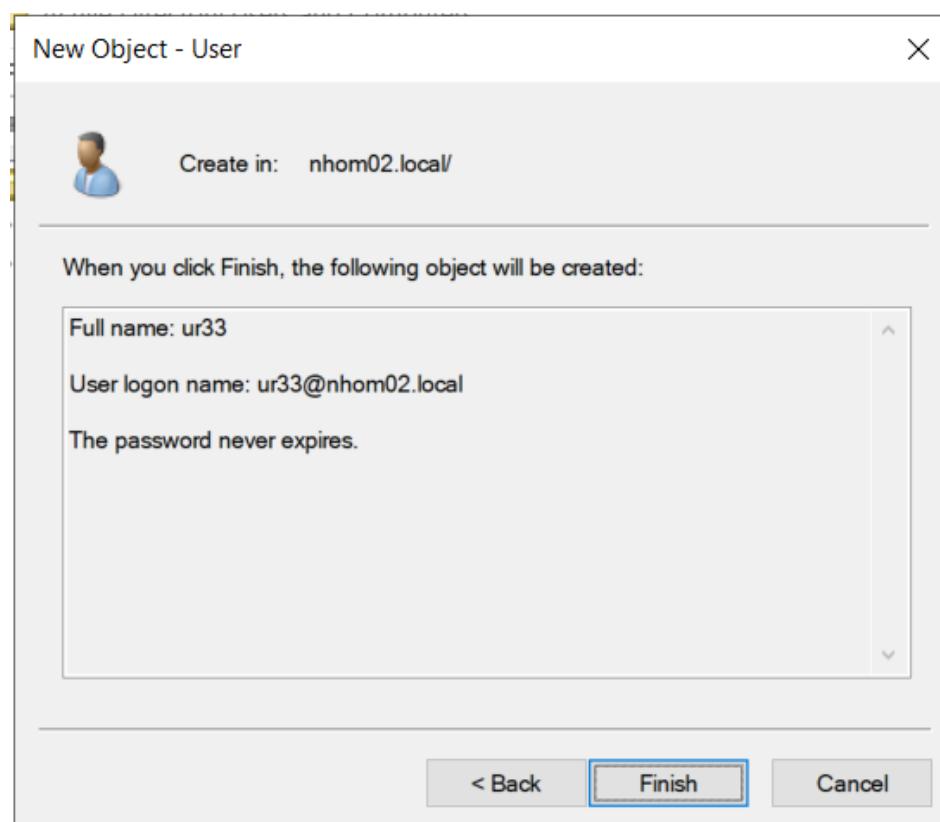
New Object - User

Create in: nhom02.local/

Password:  Confirm

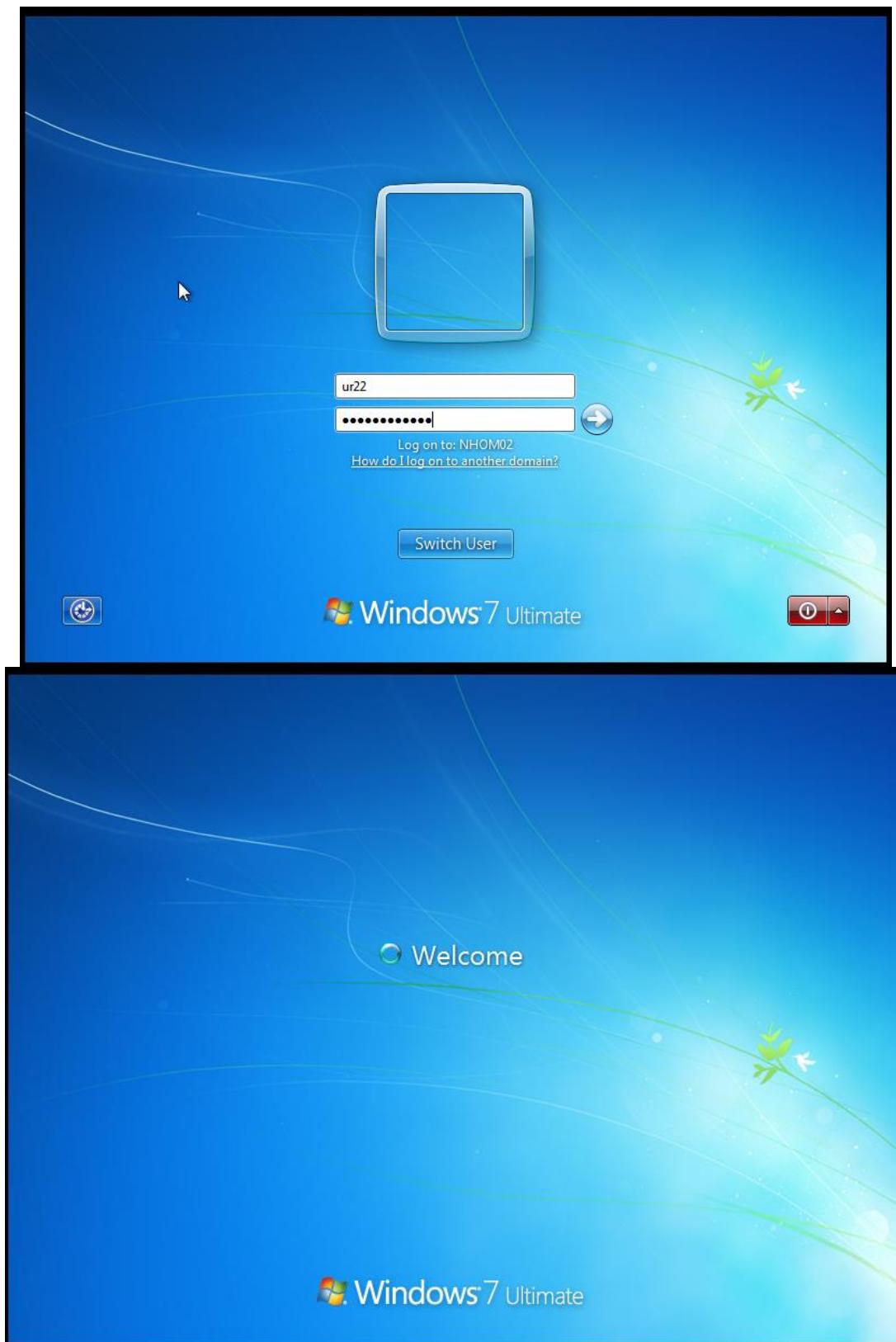
User must change password at next logon  
 User cannot change password  
 Password never expires  
 Account is disabled

< Back Next > Cancel

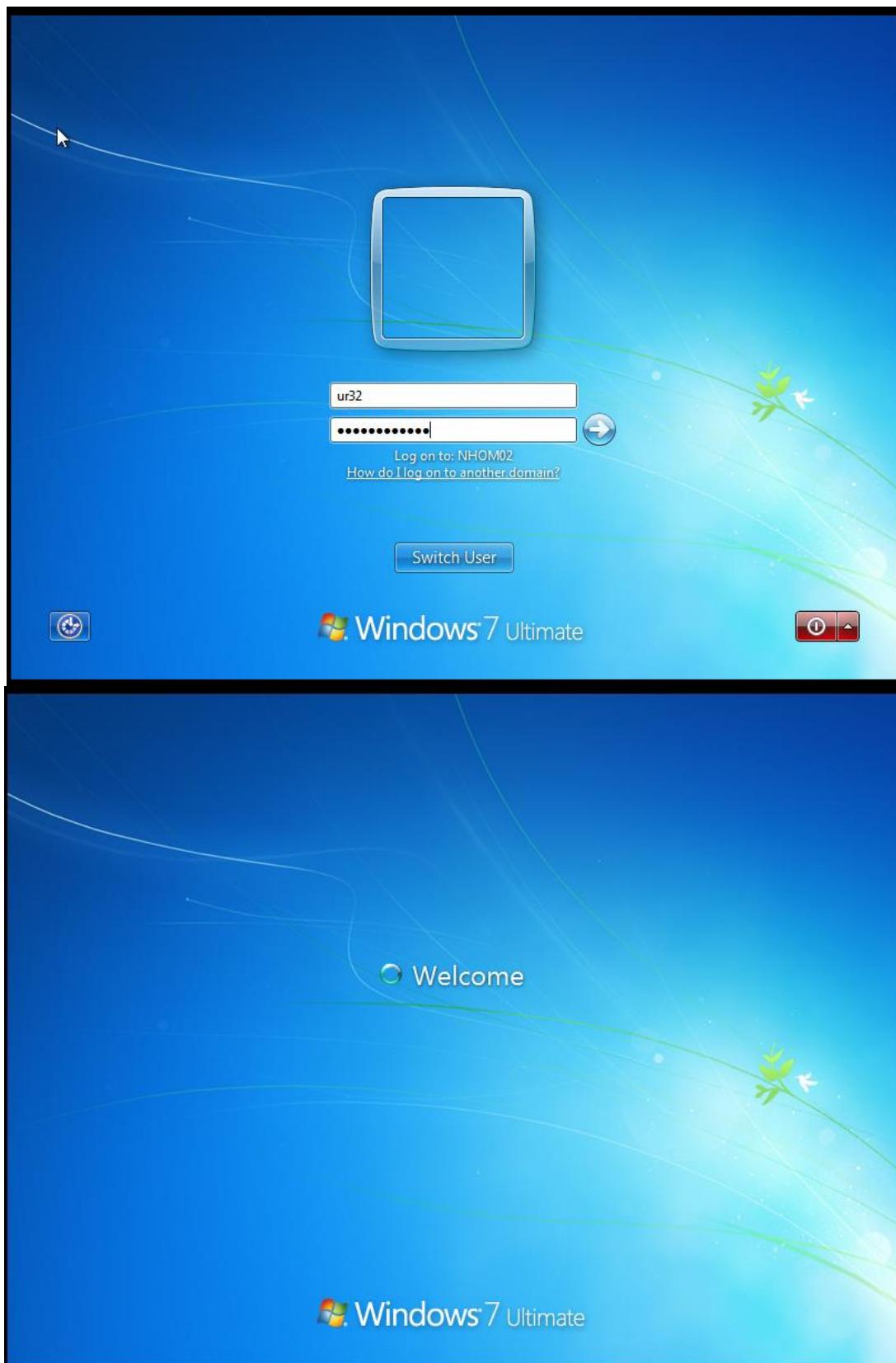


- Mở lại Read-Only DC và ta thấy ur32 đã có trên bảng Users

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	
Domain Controllers	Organizational ...	
ForeignSecurityPrincip...	Container	
Managed Service Acco...	Container	
Users	Container	
File Admin	User	
ua12	User	
ua22	User	
ua33	User	
ur12	User	
ur22	User	
<b>ur33</b>	User	
User 1	User	



- ⇒ Đăng nhập thành công.
- ⇒ Giải thích: Vì ta đã thêm PDC (máy AD) vào passwod policy của RODC nên RODC có lưu lại các account trên PDC (ur22, ur32). Khi user log in vào domain có thể thông qua RODC, cho dù RODC không thể kết nối tới PDC



- ⇒ Đăng nhập thành công.
- ⇒ Giải thích: ur33 dù được tạo trên RODC nhưng account trên RODC được cập nhật lên PDC (máy AD) nếu máy có hoạt động. Đồng nghĩa, account này được lưu trên PDC nên khi RODC không hoạt động, user log in vào domain sẽ thông qua PDC.