

# BÁO CÁO THỰC HÀNH

Môn học: Quản trị mạng và hệ thống

Kỳ báo cáo: Buổi 04(Session 04)

Tên chủ đề: Triển khai Active Directory trên Windows Server

GVHD: Đỗ Hoàng Hiển

Ngày báo cáo: 8/11/2023

Nhóm: 11

## 1. THÔNG TIN CHUNG:

(Liệt kê tất cả các thành viên trong nhóm)

Lớp: NT132.011.ANTN

STT	Họ và tên	MSSV	Email
1	Nguyễn Vũ Anh Duy	21520211	21520211@gm.uit.edu.vn
2	Lưu Gia Huy	21520916	21520916@gm.uit.edu.vn

## 2. NỘI DUNG THỰC HIỆN:<sup>1</sup>

STT	Công việc	Kết quả tự đánh giá
1	Yêu cầu 1.1	100%
2	Yêu cầu 1.2	100%
3	Yêu cầu 2.1	100%
4	Yêu cầu 2.2	100%
5	Yêu cầu 3.1	100%
6	Yêu cầu 3.2	100%
7	Yêu cầu 4.1	100%
8	Yêu cầu 4.2	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

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

1. Mô hình Workgroup hoạt động như thế nào?

- Các máy tính có quyền hạn ngang nhau, 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.

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

Ưu điểm	Nhược điểm
<ul style="list-style-type: none"> <li>- Workgroup không yêu cầu máy tính chạy trên hệ điều hành Windows Server để tập trung hóa thông tin bảo mật.</li> <li>- Workgroup thiết kế và hiện thực đơn giản và không yêu cầu lập kế hoạch có phạm vi rộng và quản trị như domain.</li> <li>- Workgroup thuận tiện đối với nhóm có số máy tính ít (<math>\leq 10</math> máy) và gần nhau.</li> </ul>	<ul style="list-style-type: none"> <li>- Người dùng phải có một account trên mỗi máy tính mà họ muốn đăng nhập.</li> <li>- Bất kỳ sự thay đổi tài khoản người dùng, như: thay đổi mật khẩu, thêm tài khoản người dùng mới, ... Phải được làm trên tất cả các máy tính trong Workgroup. Nếu 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.</li> <li>- Việc chia sẻ thiết bị và file được xử lý bởi các máy tính riêng, và chỉ cho người có tài khoản trên máy tính đó được sử dụng.</li> </ul>

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

- Kiểm tra và giải thích kết quả của 2 trường hợp truy cập vào File Server:

+ Sử dụng tài khoản của máy Client.

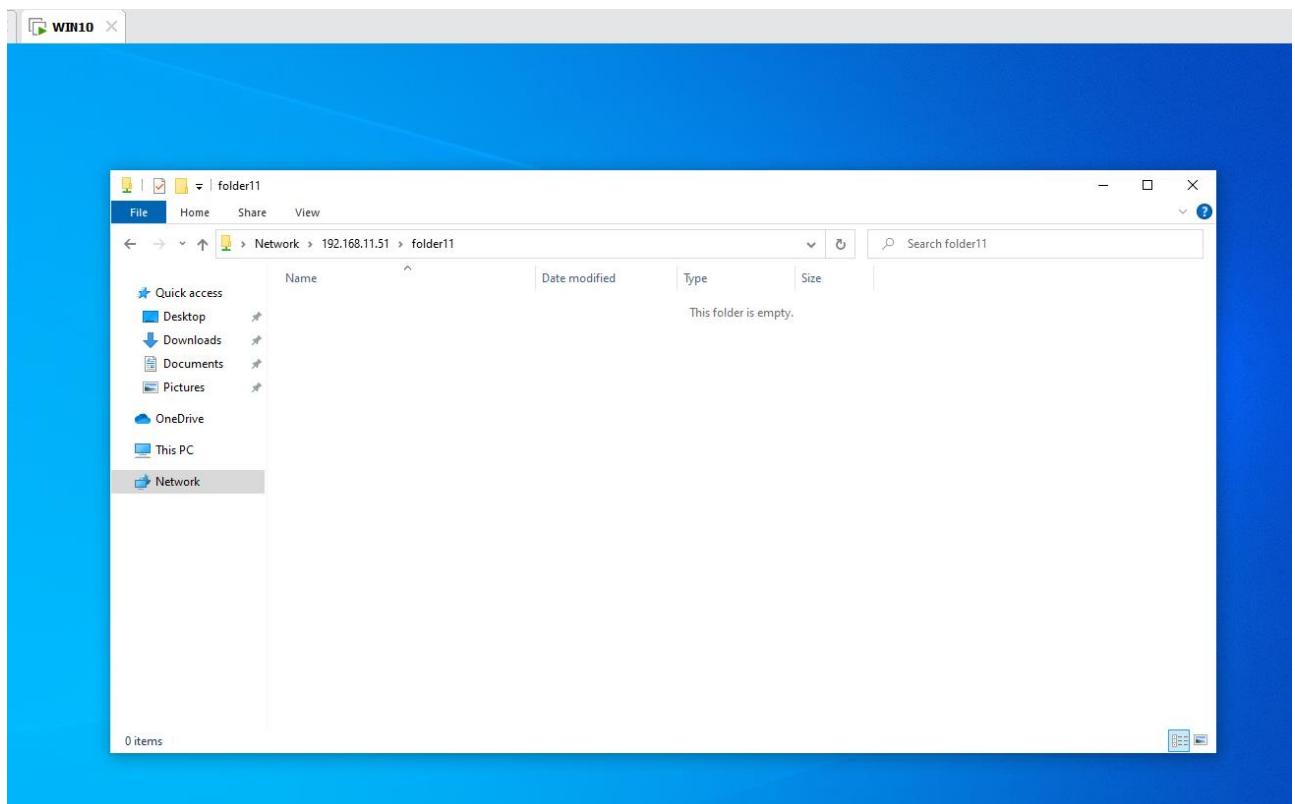
→ Kết quả: không truy cập được File Server.

→ Do bên File Server không có user account đó.



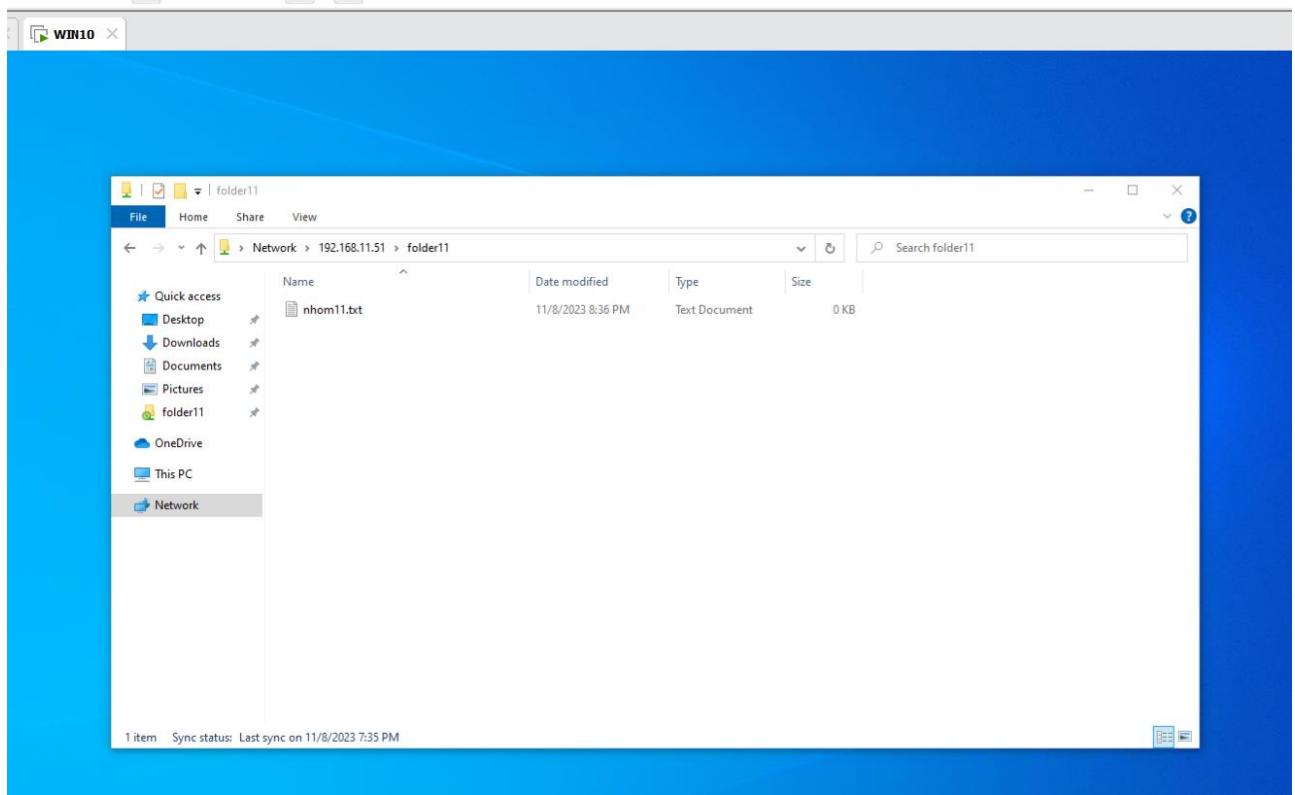
Báo lỗi sai password.

- + Sử dụng tài khoản của máy File Server (user nhom11 đã tạo ở Bước 2).
- Kết quả: đã truy cập được “folder11” ở File Server.
- Do cùng local network và bên File Server có account “nhom11” nên sẽ truy cập được “folder11” do File Server chia sẻ.

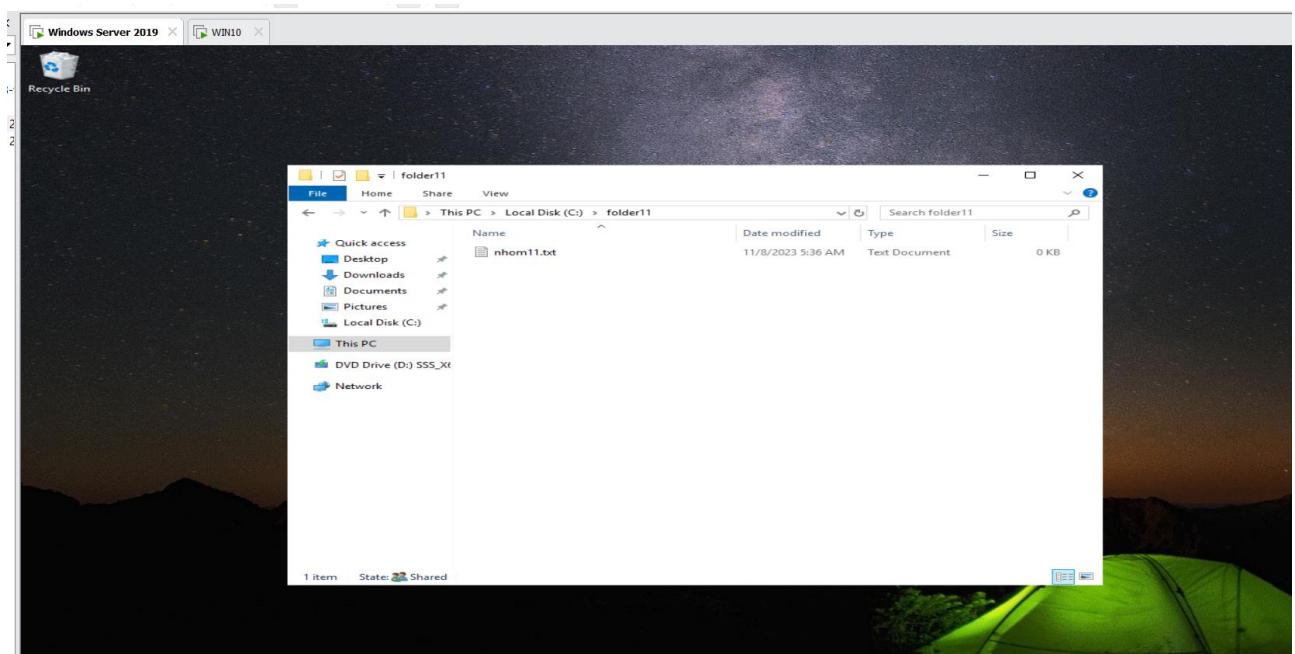


Kết quả.

→ Ta tạo file “nhom11.txt” bên phía client.



Kết quả tạo file bên client.



Bên File Server đã có file “nhom11.txt” do bên client dùng account “nhom11” truy cập và tạo file mới.

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

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

- 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. Một 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, 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.

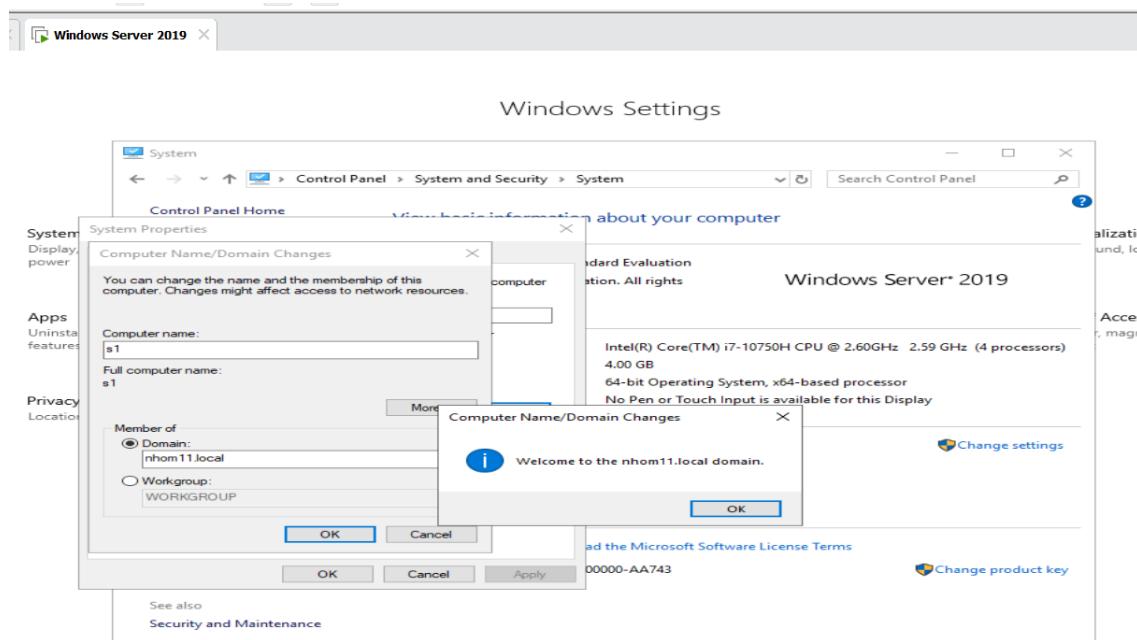
- AD còn cho phép lưu trữ thông tin, quản lý, cung cấp những cơ chế xác thực cũng như ủy quyền, thiết lập 1 khung nhằm triển khai những dịch vụ khác: Rights Management Services, Lightweight Directory Services, Active Directory Federation Services và Certificate Services.

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

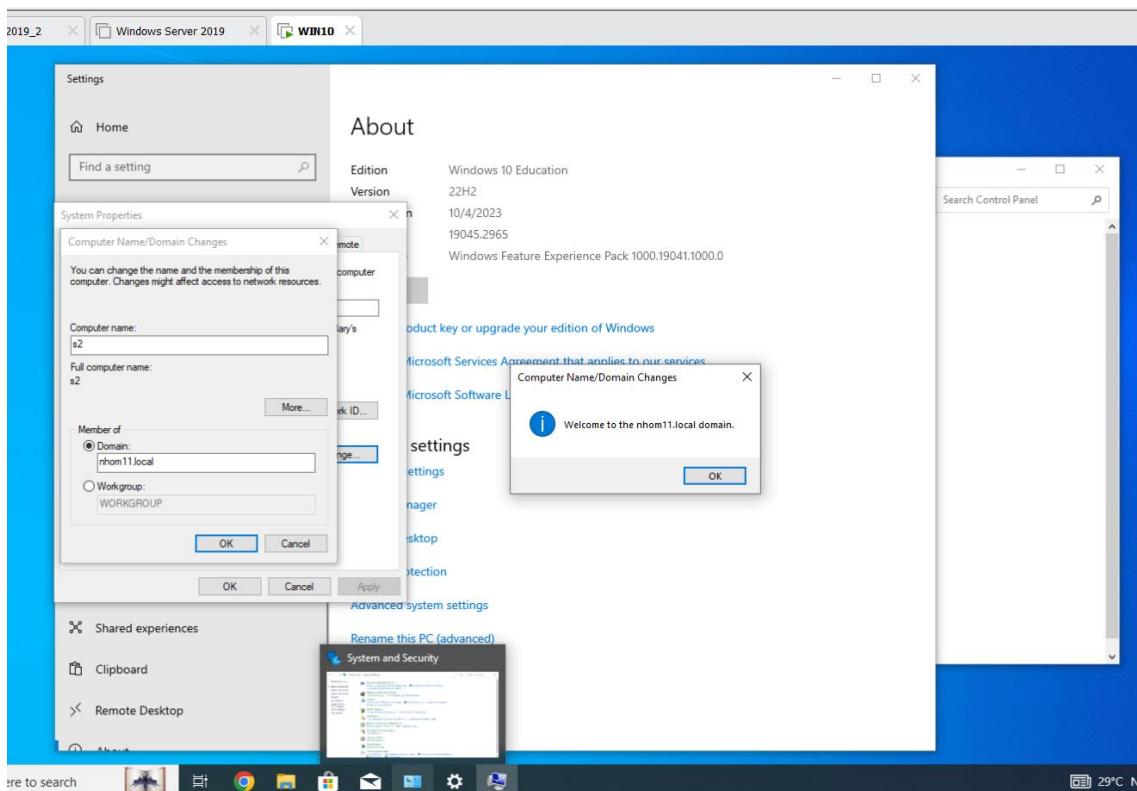
	Mô hình Workgroup	Mô hình domain
Network	- Tất cả máy tính phải ở cùng một local network hoặc subnet.	- Có thể ở local network khác nhau.
Account	- Mỗi máy tính phải có một user account tạo riêng.	- Nếu có 1 user domain thì có thể đăng nhập vào bất kỳ máy tính nào trên domain.
Privilege	- Tất cả máy trong Workgroup đều ngang hàng với nhau.	- 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 cho tất cả các máy trong domain.
Setting	- Cài đặt dễ dàng.	- Cài đặt phức tạp.
Security	- Tính bảo mật thấp, không tập trung dữ liệu.	- Tính bảo mật cao bởi dữ liệu được tập trung tại máy server.

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

- Sau khi nâng cấp máy chủ Active Directory lên Domain Controller và tạo user trong domain. Ta thực hiện thêm File Server và Client vào domain đã tạo.

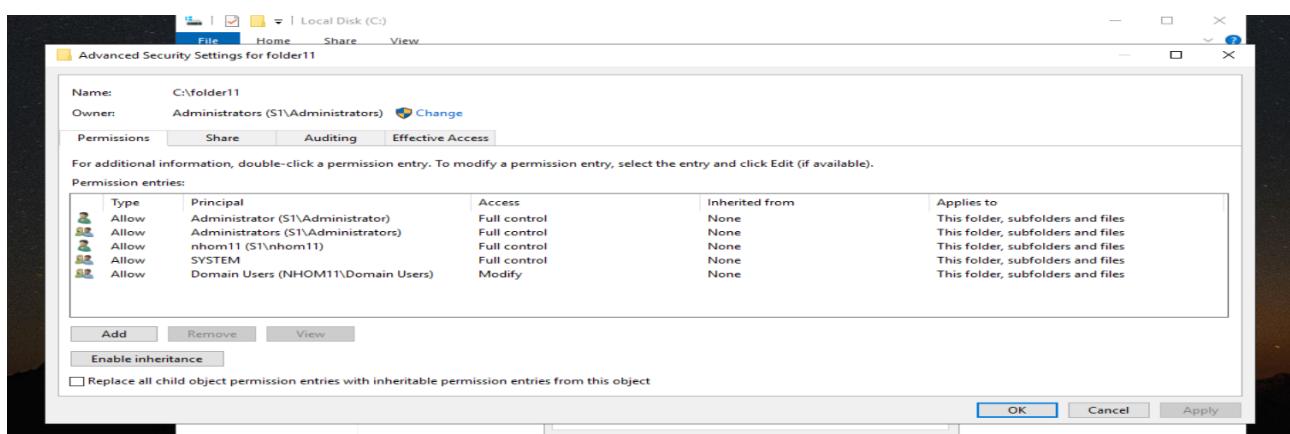


Kết quả xác thực thành công, File Server báo đã được thêm vào domain.



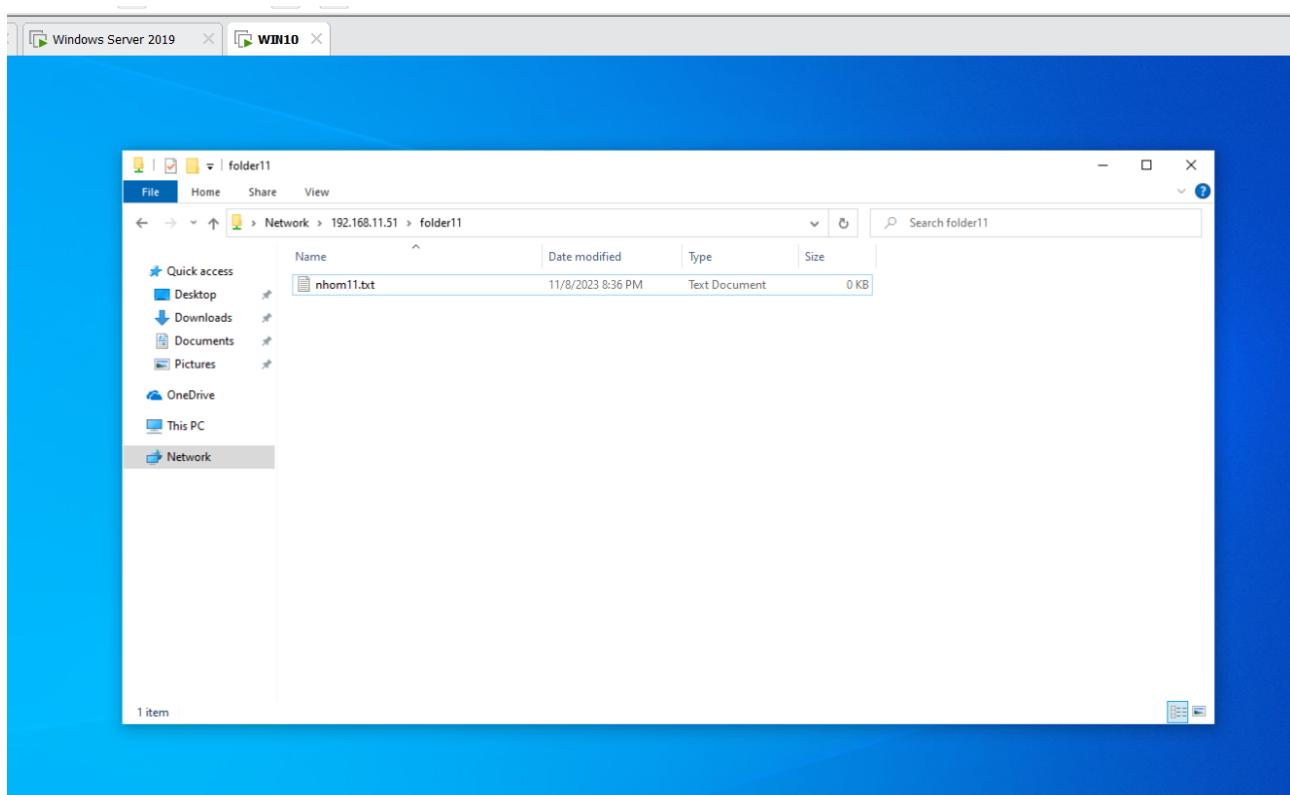
Kết quả xác thực thành công, Client báo đã được thêm vào domain.

- Tiếp theo, ta tiến hành phân quyền cho “folder11” trong File Server.



Kết quả phân quyền cho “folder11”.

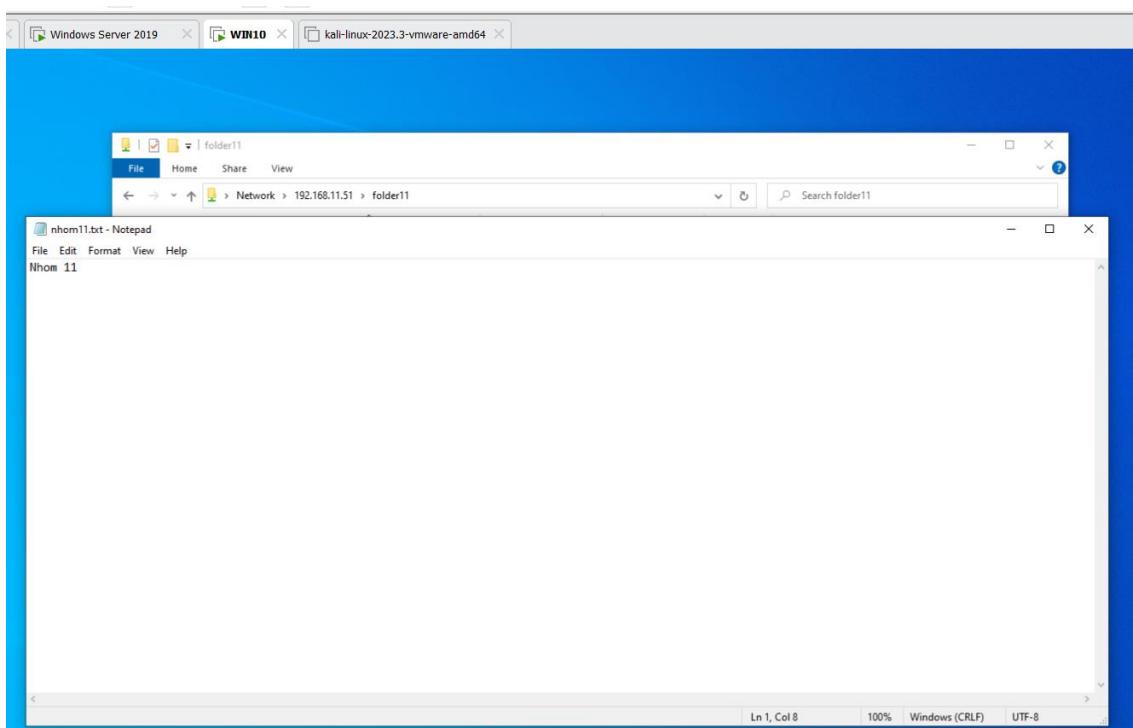
- Các bước thiết lập đã xong, bây giờ ta bắt đầu sử dụng mô hình Domain. Ta đăng nhập từ máy client bằng account “NHOM11\user1”, sau đó kết nối tới File Server bằng cách RUN <\\192.168.11.51>. Cuối cùng, thử click vào “folder11”.



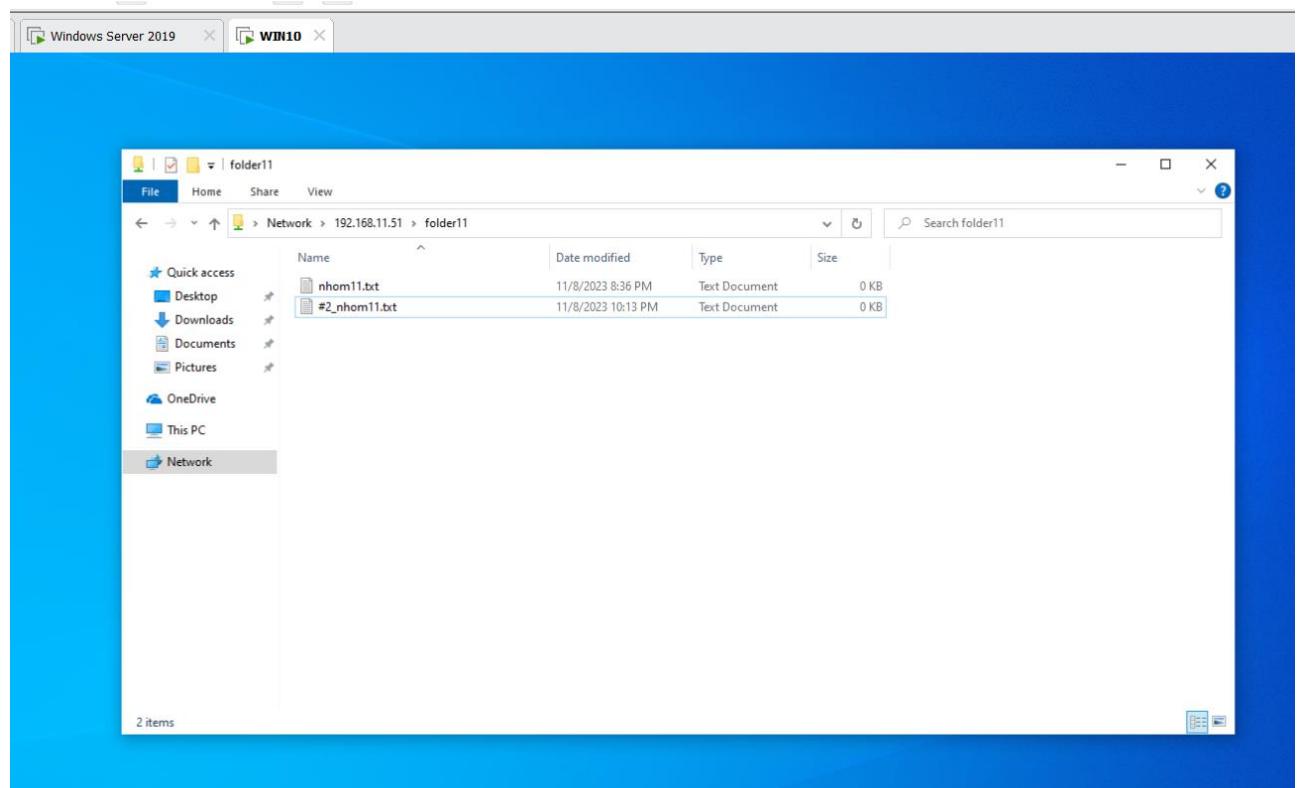
Kết quả truy cập thành công vào “folder11”.



- Test chức năng đọc, ghi dữ liệu và tạo file mới trong “folder11”.

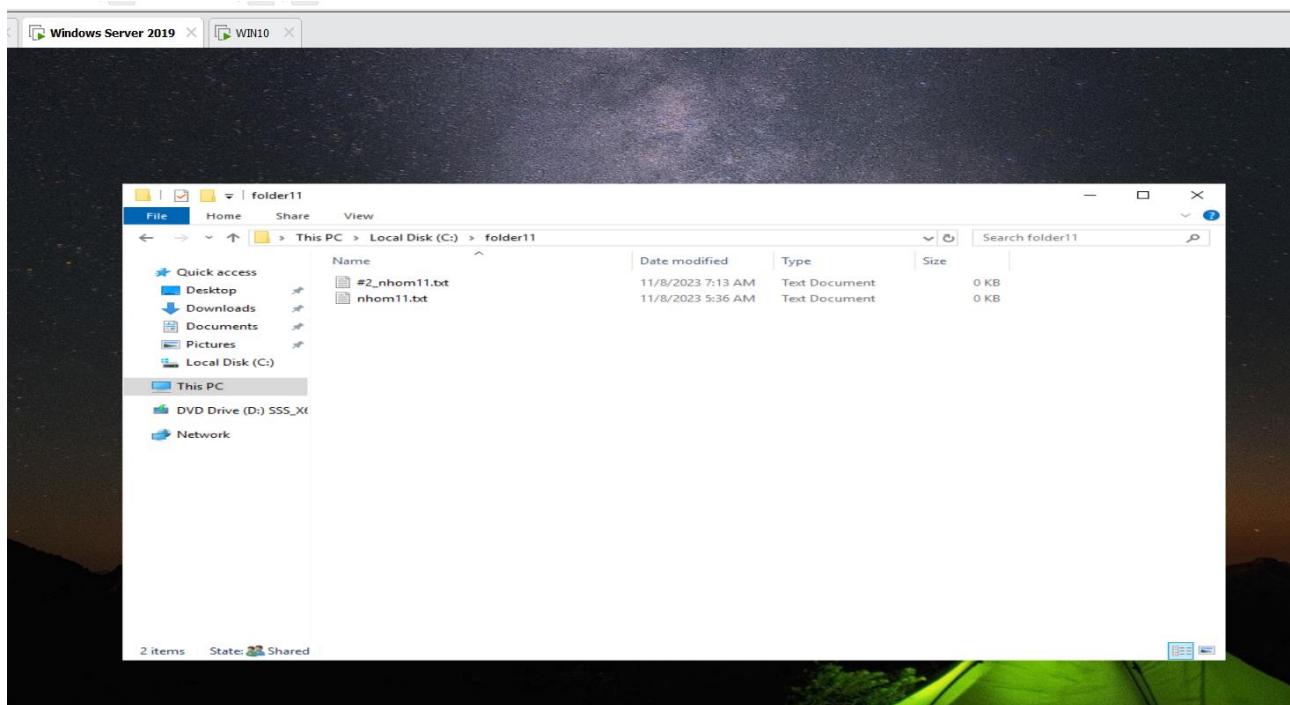


Kết quả ghi và đọc lại dữ liệu.



Kết quả tạo file mới “#2\_nhom11.txt” bên client “NHOM11\user1”.

- Kiểm tra lại bên File Server.



File “#2\_nhom11.txt” đã có bên File Server.

→ **Kết luận:** Về mặt cài đặt, mô hình Domain phức tạp hơn Workgroup. Nhưng đổi lại, các máy có thể ở local network khác nhau, và nếu có 1 user domain thì có thể đăng nhập vào bất kỳ máy tính nào trên domain thay vì account dính theo máy như Workgroup.

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

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

→ ADC là các domain được thêm vào Domain Controller.

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

→ 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. Khi nào cần sử dụng ADC?

Khi nào cần sử dụng Additional Domain Controller:

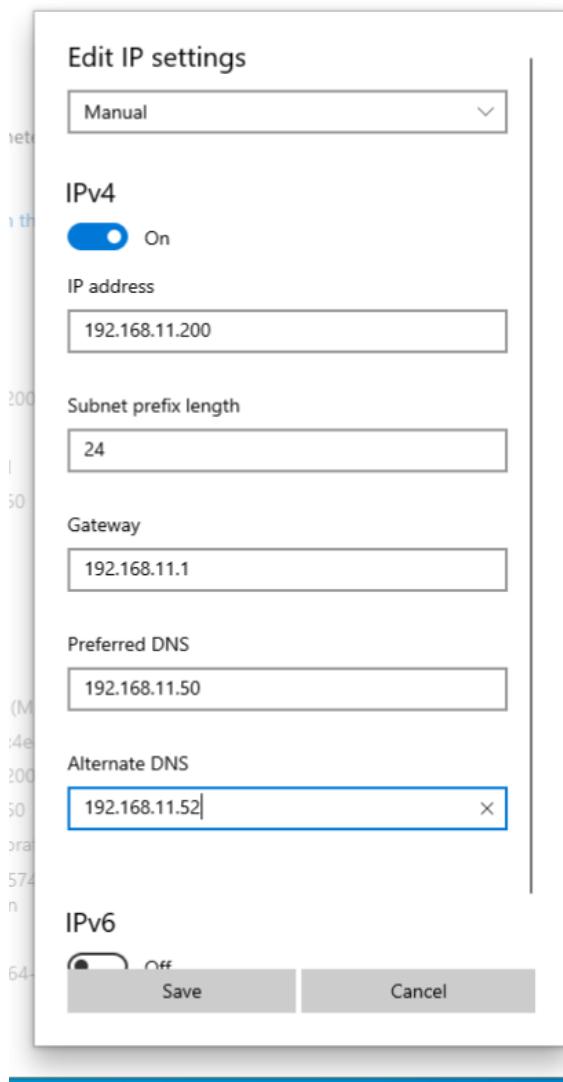
→ Trường hợp 1: Hệ thống có nhiều site: Nếu muốn các site được quản lý theo mô hình AD với cùng domain, ta cần dựng ADC ở các site → Để tăng tốc độ chứng thực cho các user ở từng site.

→ Trường hợp 2: Hệ thống có 1 site nhưng số lượng user lớn: Dụng thêm ADC để cân bằng tải → Giúp hệ thống nhanh hơn, tránh tình trạng quá tải và tắc nghẽn mạng.

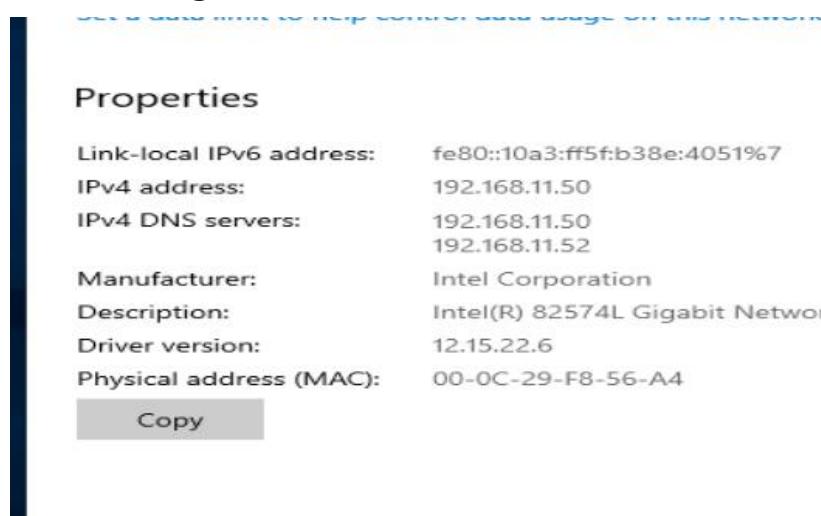
→ Trường hợp 3: Hệ thống có 1 site và 1 Domain Controller, hệ thống nhỏ: Dựng thêm ADC → Để phòng tình trạng khi Domain Controller gặp sự cố thì hệ thống công ty tê liệt dẫn đến tổn thất về kinh tế lần thời gian.

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

- Tận dụng máy User1 và Active Directory ở bài 2 để làm client và PDC. Chỉ thêm 1 Window Server để làm ADC.
- Thêm thông số DNS Server trên client.

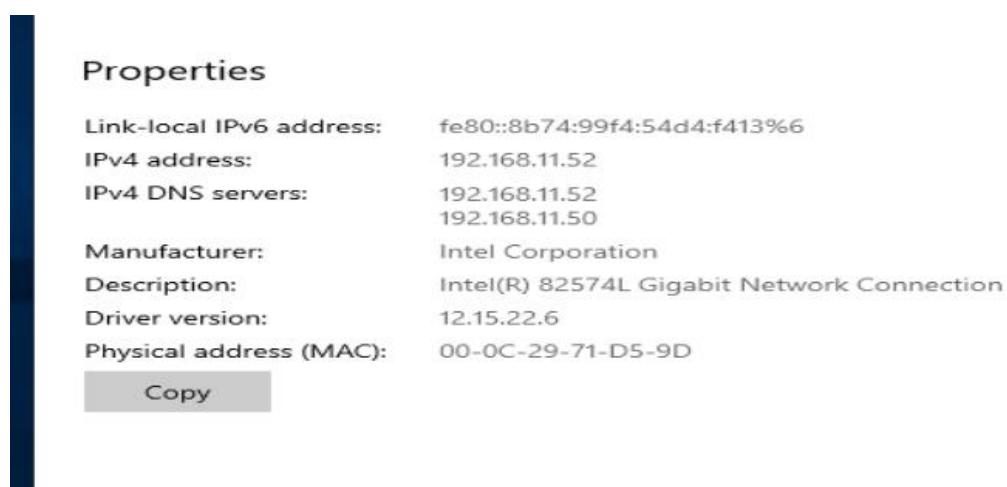


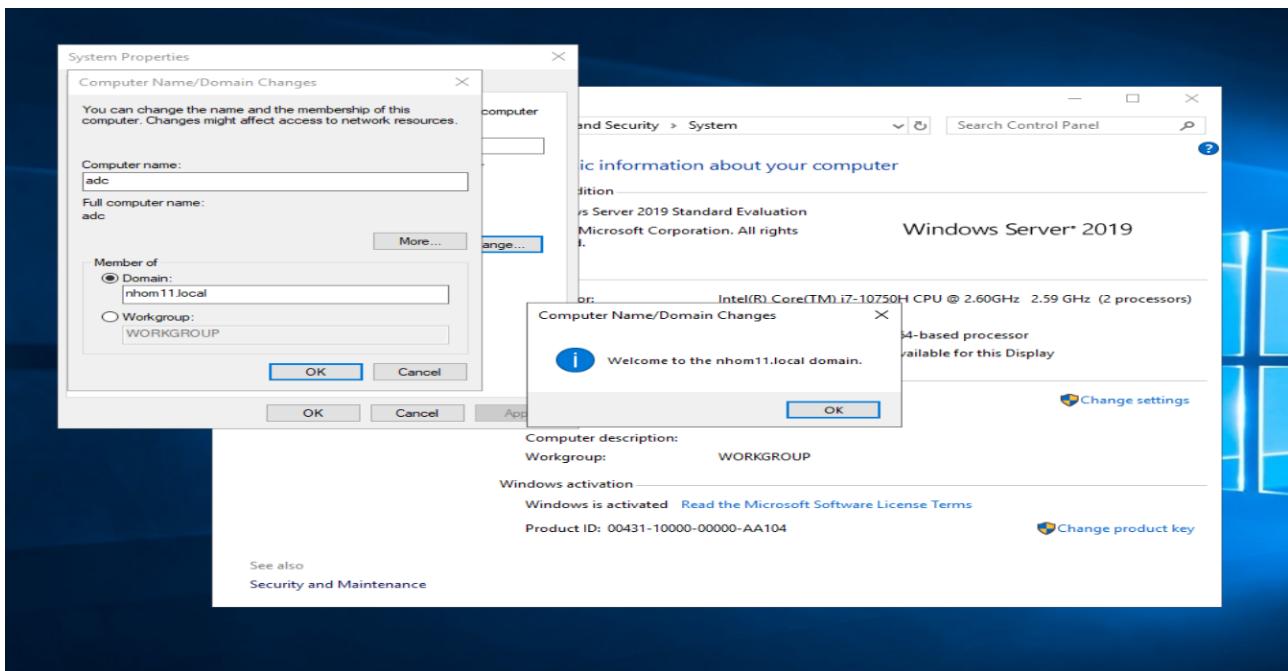
- Thêm thông số DNS Server trên PDC.



- Cài đặt ADC trên 1 Window Server mới.

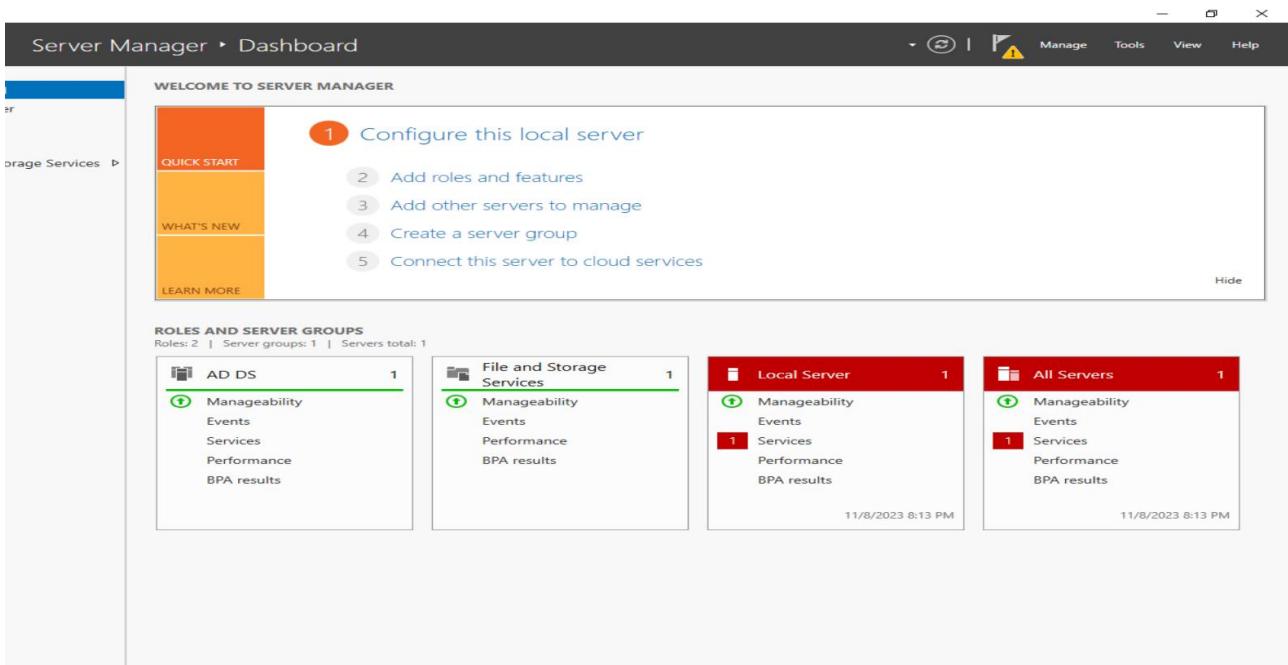
B1: Ta thiết lập trước IP tĩnh, DNS Server, Computer Name.





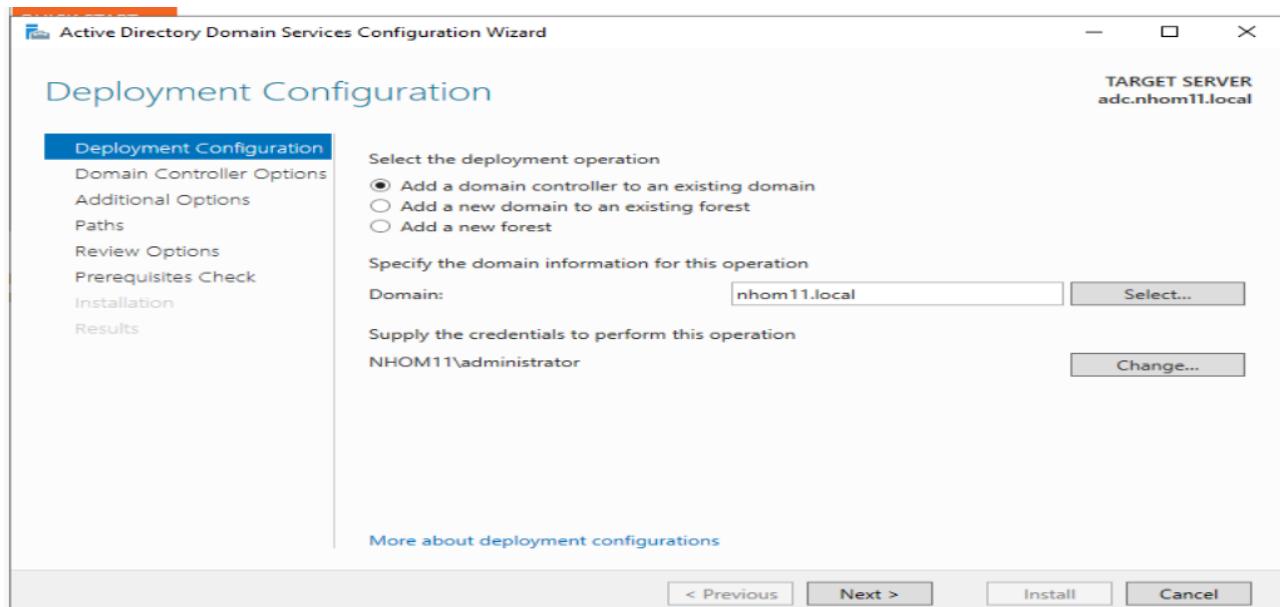
Kết quả thêm máy Windows Server mới vào domain.

## B2: Cài đặt AD DS tương tự như PDC ở yêu cầu 2.

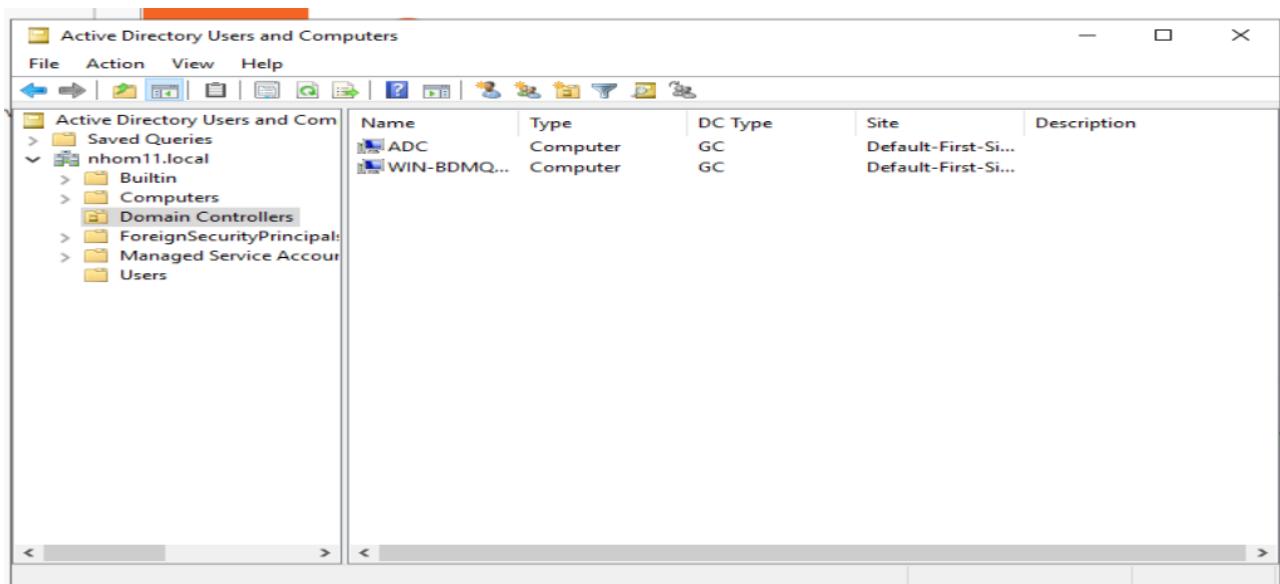


Kết quả cài đặt AD DS.

B3: Nâng cấp lên ADC cũng tương tự như các bước ở yêu cầu 2, nhưng ở bước “Deployment Configuration”, ta phải chọn “Add a domain controller to an existing domain”, chọn domain “nhom11.local” và supply the credentials là account administrator bên PDC.



- Ở những bước còn lại, tương tự như hướng dẫn ở yêu cầu 2.

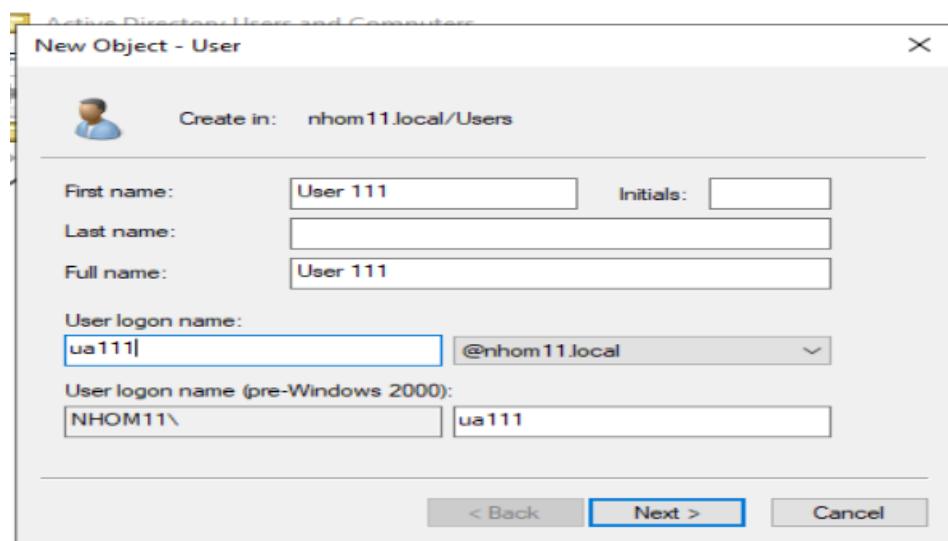


ADC đã có trong Domain Controllers.

➔ Ta đã triển khai xong mô hình ADC. Để kiểm tra tính đúng đắn, ta thực hiện các tasks sau:

- Tạo user ua111 trên Primary DC. Kiểm tra thông tin user này trên Additional DC.

+ Tạo ua111 trên PDC.



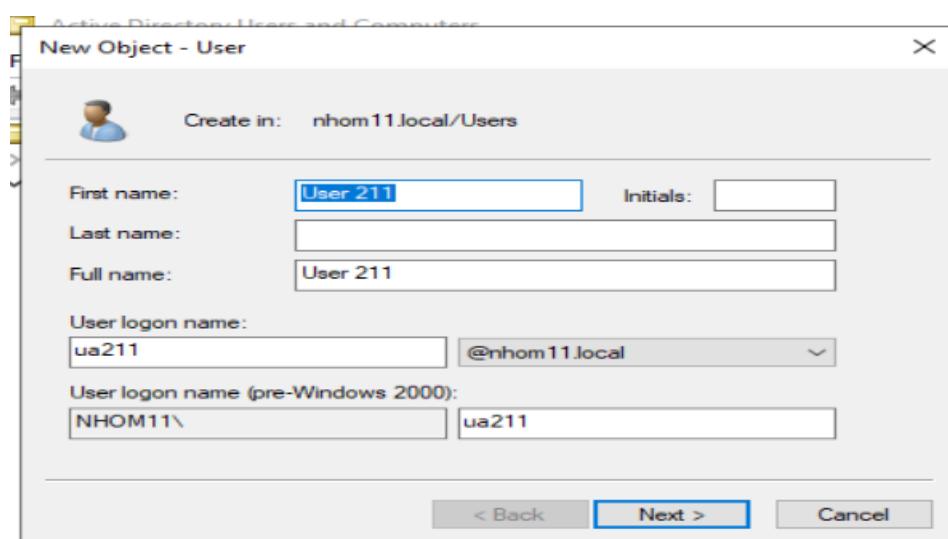
+ Truy cập ADC.

Name	Type	Description
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Builtin	Security Group...	Designated administrato...
Computers	Security Group...	All workstations and ser...
Domain Contro...	Security Group...	All domain controllers i...
Domain Con...	Security Group...	All domain guests
Domain Gue...	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...
User 1	User	
User 111	User	

ua111 đã có trên ADC.

- Tạo user ua211 trên Additional DC. Kiểm tra thông tin user này trên Primary DC.

+ Tạo ua211 trên ADC.



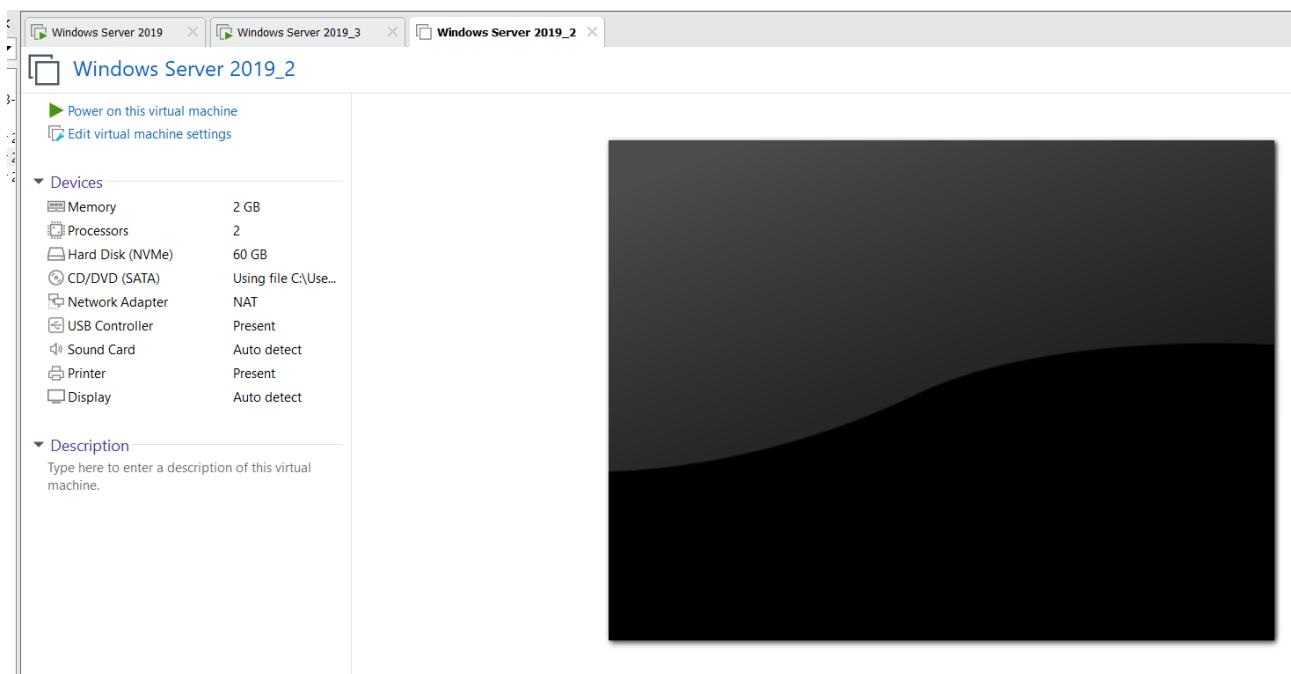
+ Truy cập PDC.

Name	Type	Description
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
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 ...
ProtectedUs...	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...
User 1	User	
User 111	User	
ua211	User	

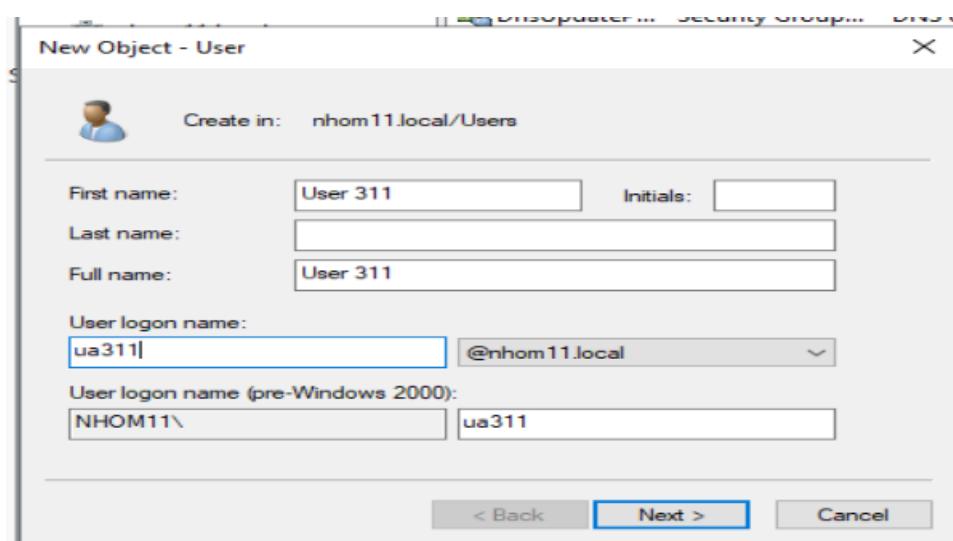
ua211 đã có trên PDC.

- 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.

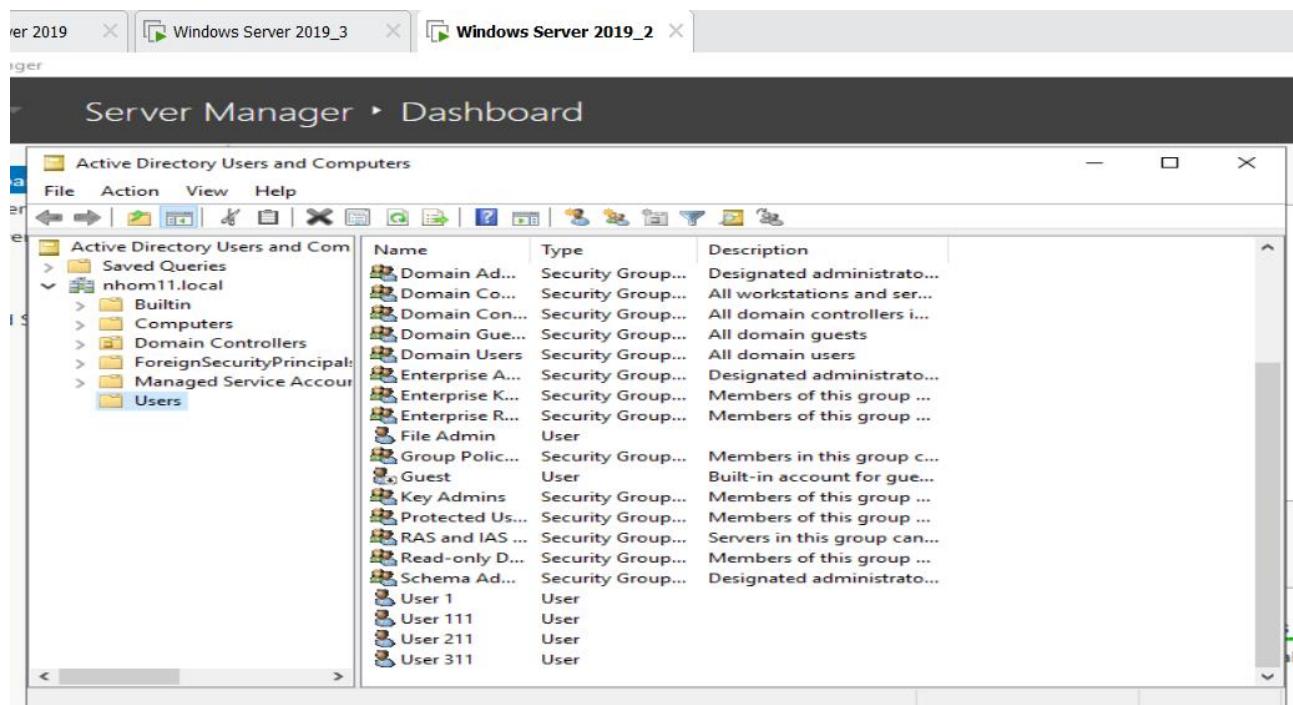
+ Tắt máy PDC.



+ Tạo ua311 trên ADC



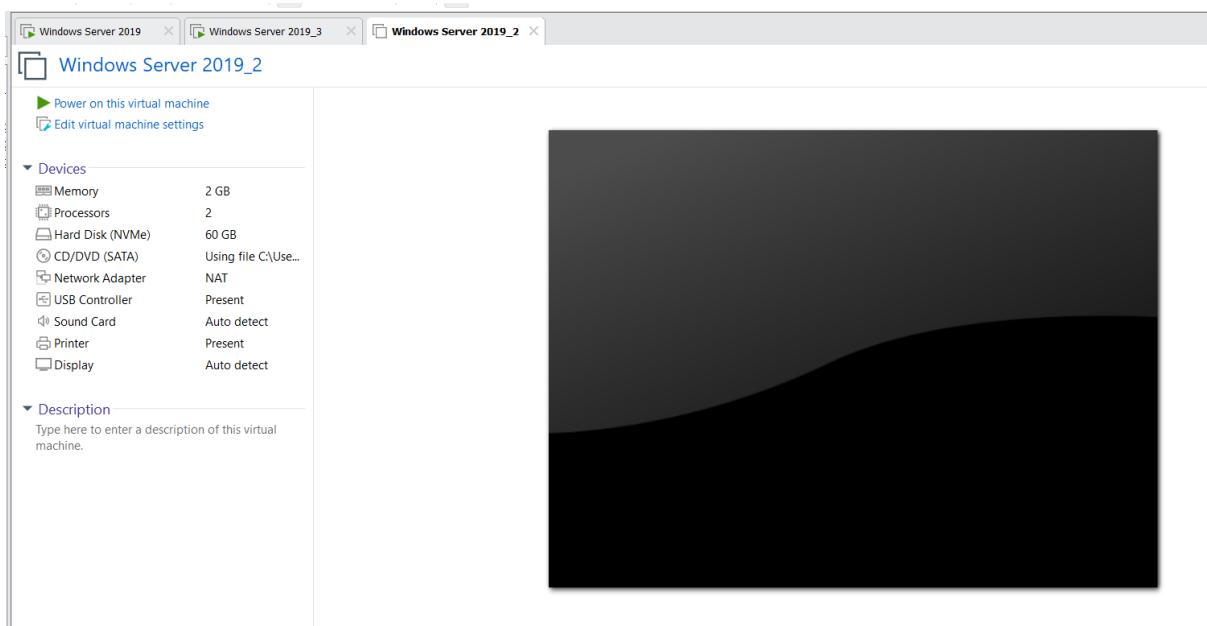
- + Mở lại PDC và kiểm tra:



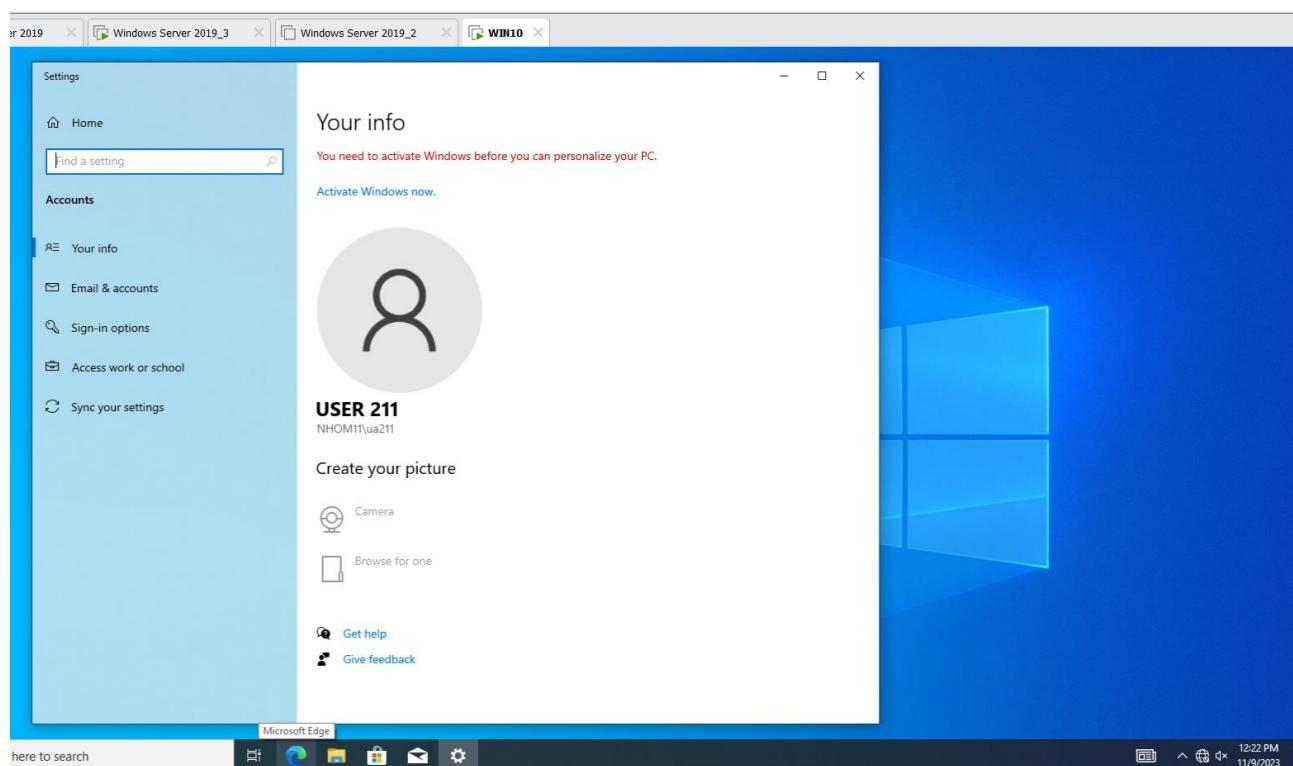
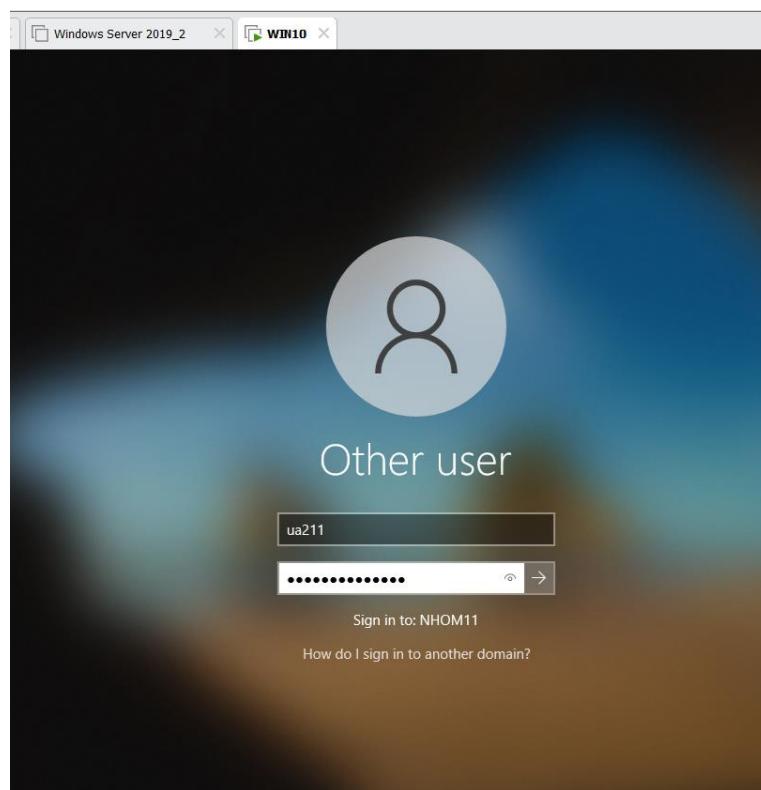
ua311 đã có trên PDC.

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

- + Tắt PDC.



+ Ta đăng nhập máy client bằng account ua211.



Kết quả đăng nhập thành công.

➔ **Kết luận:** ta đăng nhập vào ua211 thành công do ta đã thêm 1 ADC nên khi tắt PDC thì ADC có nhiệm vụ xác thực thay cho PDC.

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

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

→ Read-Only Domain Controller (RODC) 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 .

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

→ 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 hoạt động thì chúng ta phải khai báo, lưu trữ dữ liệu người dùng thông qua một policy riêng của RODC.

### 3. Khi nào cần sử dụng RODC?

→ 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. Hơn nữa, nếu chúng ta không để RODC lưu trữ thông tin về tài khoản được tạo bản sao thì cho dù đánh cắp được RODC thì cũng không thể sử dụng thông tin mà họ lấy được từ nó.

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

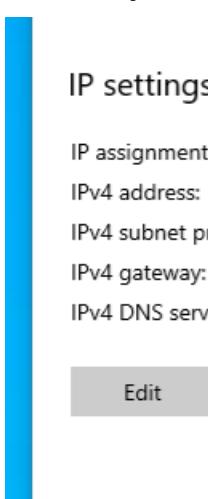
Tính chất	Mô hình ADC	Mô hình RODC
Độ truy cập	- Hoạt động như các máy chủ chính trong môi trường AD và có quyền truy cập và chỉnh sửa toàn bộ dữ liệu AD.	- Chỉ có quyền đọc dữ liệu từ AD, không thể thay đổi dữ liệu.
Tính năng chính	- Dùng để quản lý, lưu trữ và cung cấp dịch vụ xác thực, quản lý tài khoản, và phân quyền trong môi trường AD.	- Triển khai trong các vị trí vật lý hoặc địa lý có yêu cầu bảo mật cao, nơi mà sự truy cập đầy đủ vào dữ liệu AD có thể không an toàn.
Đồng bộ hóa dữ liệu	- ADCs tham gia vào quá trình đồng bộ hóa dữ liệu giữa các domain controller trong môi trường AD.	- RODCs nhận dữ liệu từ các ADCs và không tham gia vào quá trình đồng bộ hóa dữ liệu.
Bảo mật	- Cần được bảo vệ cẩn thận vì có quyền truy cập đầy đủ vào dữ liệu AD và có thể thay đổi dữ liệu.	- RODCs có tính bảo mật cao hơn vì không thể thay đổi dữ liệu AD và chỉ có quyền đọc.
Triển khai	- Tại các vị trí thông thường trong mạng AD.	- Thường triển khai ở các vị trí có nguy cơ bảo mật cao hoặc kết nối mạng không đáng tin cậy.

Hiệu suất	- Có thể tạo áp lực về hiệu suất trên hệ thống do quyền truy cập đầy đủ và hoạt động chính trong môi trường AD.	- RODCs có ít áp lực về hiệu suất hơn vì chỉ có quyền đọc.
Lợi ích bảo mật	- Không phải là một mô hình bảo mật cao vì có quyền truy cập đầy đủ vào dữ liệu AD.	- Cung cấp một lớp bảo mật bổ sung bằng cách giảm khả năng thay đổi dữ liệu trên RODCs.

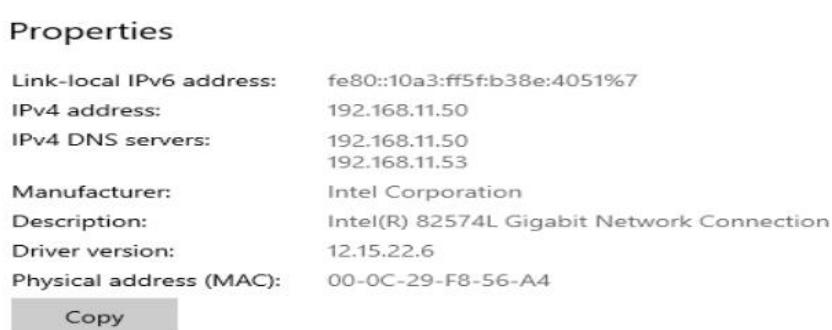
**Yêu cầu 4.2.** Sinh viên triển khai mô hình Read-Only Domain Controller theo yêu cầu bên dưới.

Tương tự yêu cầu 3, ta tận dụng client và PDC, chỉ cấu hình lại IP static.

- Cấu hình IP máy client.

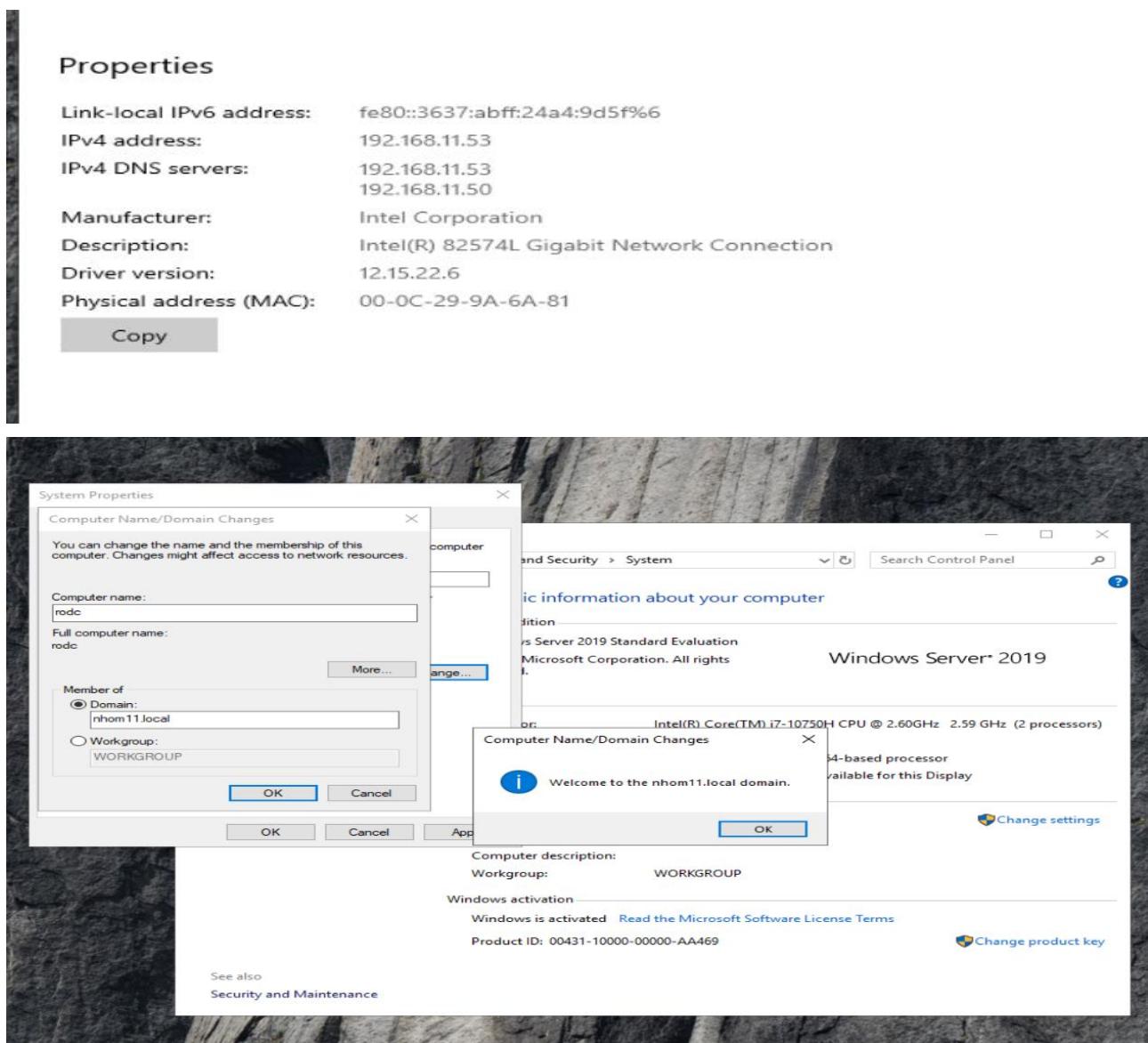


- Cấu hình IP máy PDC.

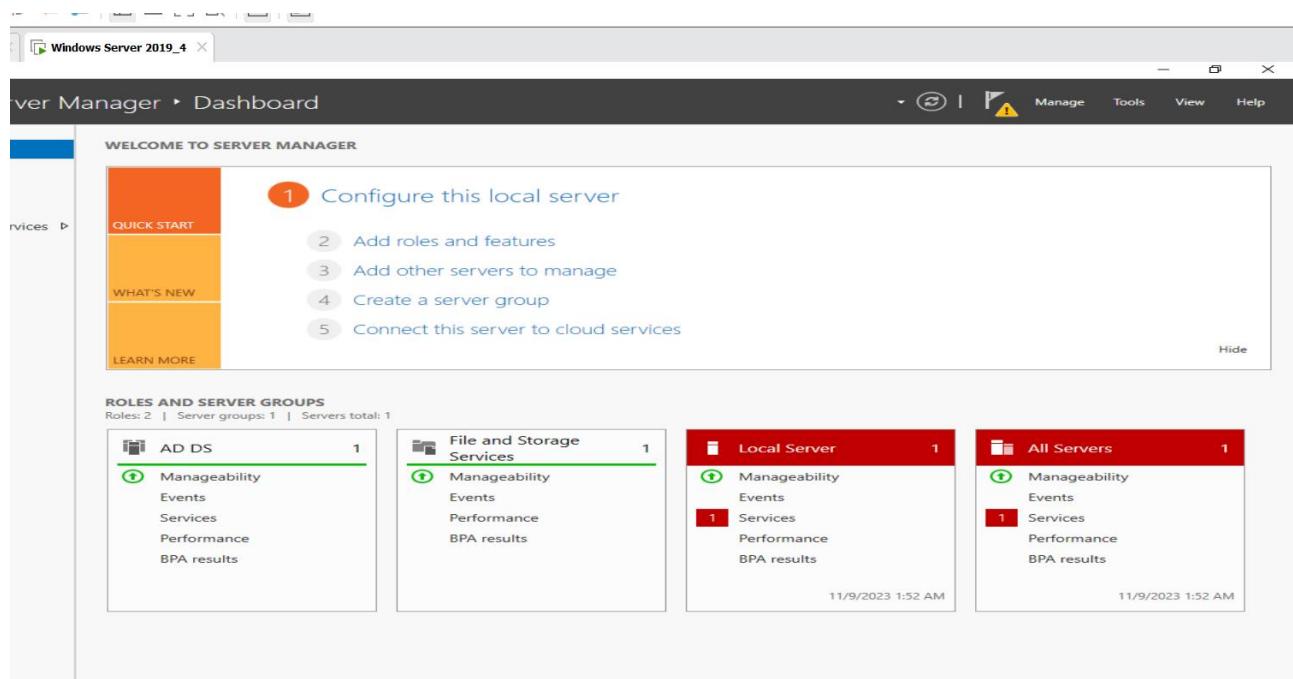


- Cài đặt ADC trên 1 Window Server mới.

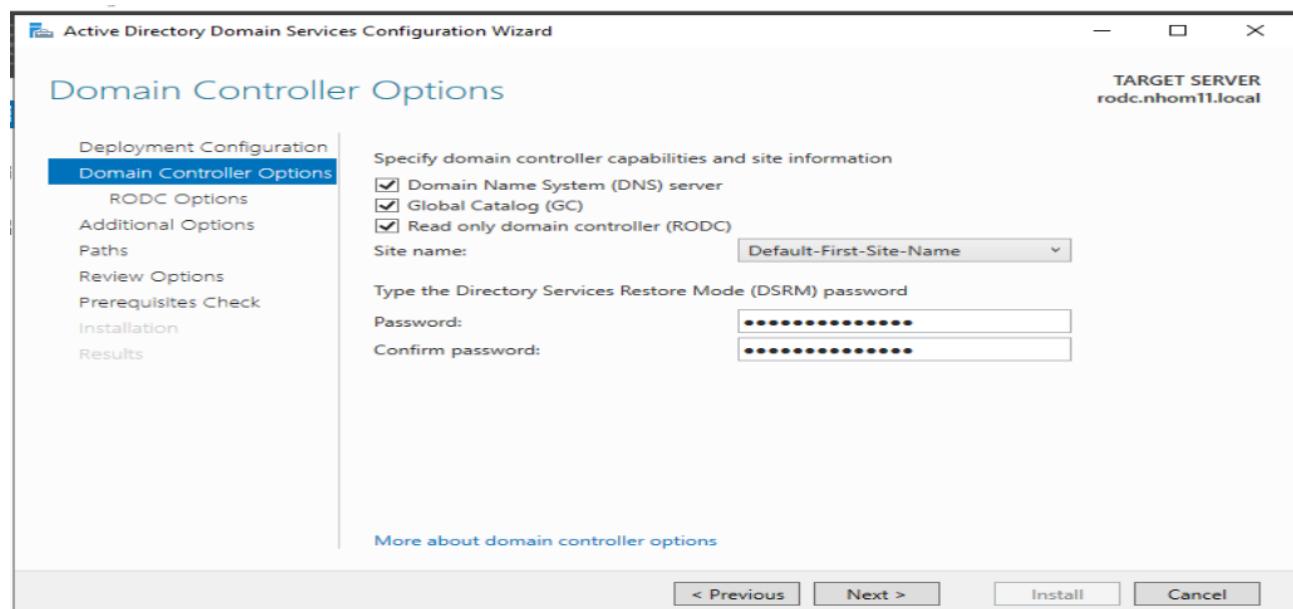
B1: Ta thiết lập trước IP tĩnh, DNS Server, Computer Name.



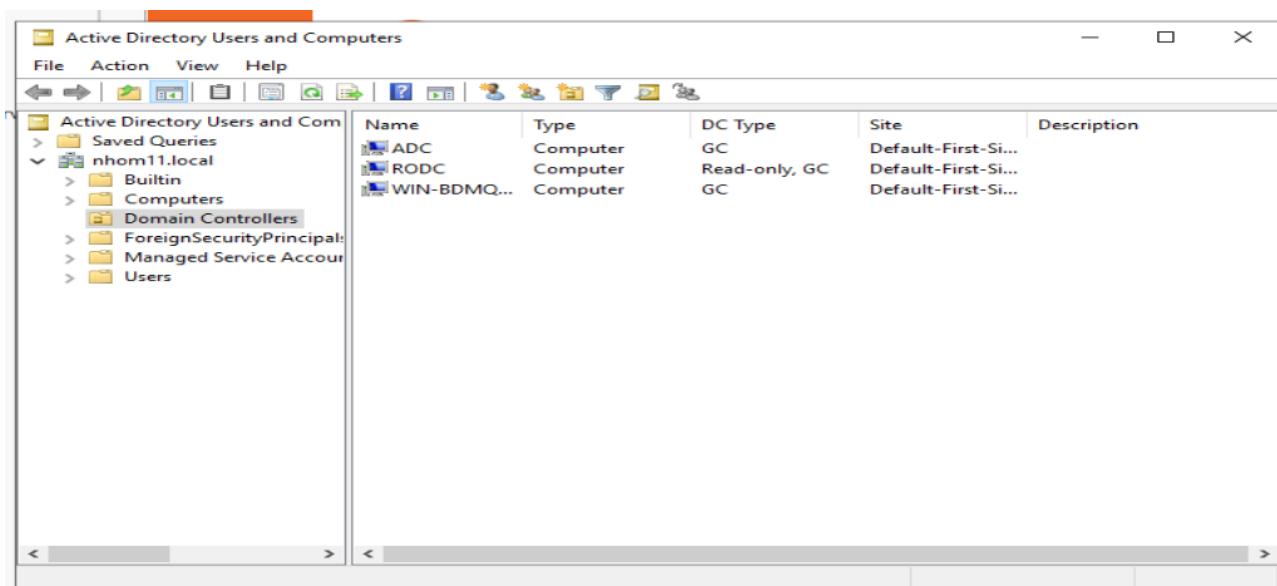
Kết quả thêm máy Windows Server mới vào domain.

**B2:** Cài đặt AD DS tương tự như PDC ở yêu cầu 2.

Kết quả cài đặt AD DS.

**B3:** Nâng cấp lên ADC cũng tương tự như các bước ở yêu cầu 3, nhưng ở bước “Domain Controller Options”, ta phải click thêm “Read only domain controller (RODC)”.

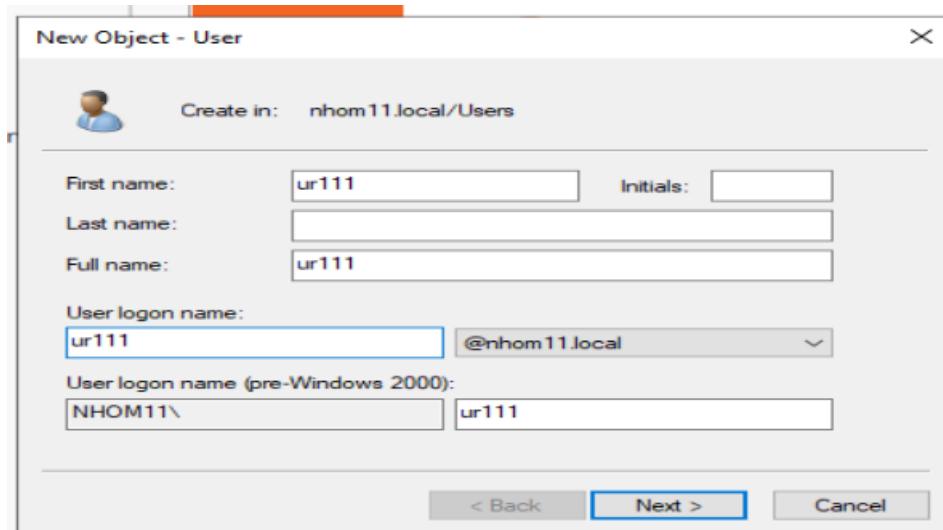
- Ở những bước còn lại, tương tự như hướng dẫn ở yêu cầu 2.



RODC đã có trong Domain Controllers.

→ Ta đã triển khai xong mô hình ADC. Để kiểm tra tính đúng đắn, ta thực hiện các tasks sau:

- **Tạo user ur1X trên Primary DC. Kiểm tra thông tin user này trên Read-Only DC.**
- + Tạo ur111 trên PDC.



- + Truy cập máy RODC và kiểm tra:

The screenshot shows the Windows Server 2019 Dashboard. In the center, there is a table titled "Active Directory Users and Computers" listing various users and groups. One user, "ur111", is listed under the "Users" section. The table includes columns for Name, Type, and Description.

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	Members in this group c...
Group Polic...	Security Group...	Built-in account for gue...
Guest	User	Members of this group ...
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 Adm...	Security Group...	Designated administrato...
ur111	User	
User 1	User	
User 111	User	
User 211	User	
User 311	User	

ur111 đã có trên RODC.

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

- + Tạo ur211 trên RODC.

The screenshot shows the "New Object - User" creation wizard in the Server Manager. The "Create in" dropdown is set to "nhom11.local/Users". The "First name" field is filled with "ur211". The "User logon name" field is also filled with "ur211", and the dropdown next to it shows "@nhom11.local". The "User logon name (pre-Windows 2000)" fields show "NHOM11\" and "ur211". At the bottom, there are "Next >" and "Cancel" buttons.

- + Truy cập PDC và kiểm tra:

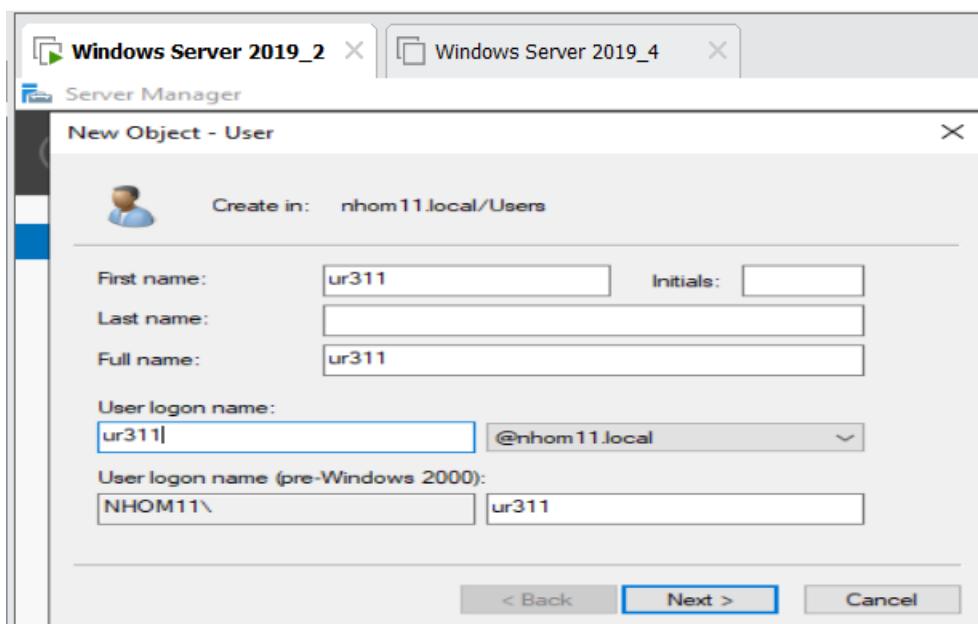
Name	Type	Description
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...
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...
ur111	User	
ur211	User	
User 1	User	
User 111	User	
User 211	User	
User 311	User	

ur211 đã có trên máy PDC.

- **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 RODC.

+ Tạo ur311 trên PDC.



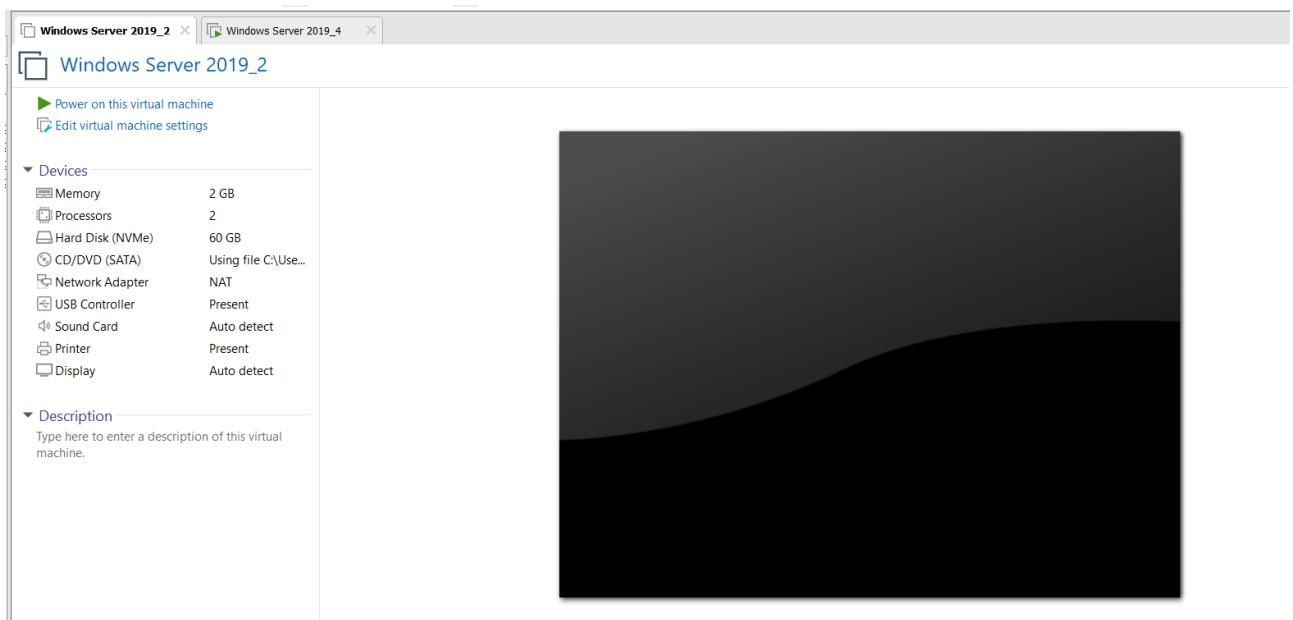
+ Mở lại RODC và kiểm tra:

Name	Type	Description
Domain Guest	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise Admins	Security Group...	Designated administrato...
Enterprise Replicators	Security Group...	Members of this group ...
File Admins	User	
Group Policies	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Users	Security Group...	Members of this group ...
RAS and IAS	Security Group...	Servers in this group can...
Read-only Domain Controllers	Security Group...	Members of this group ...
Schema Administrators	Security Group...	Designated administrato...
ur111	User	
ur211	User	
ur311	User	
User 1	User	
User 111	User	
User 211	User	
User 311	User	

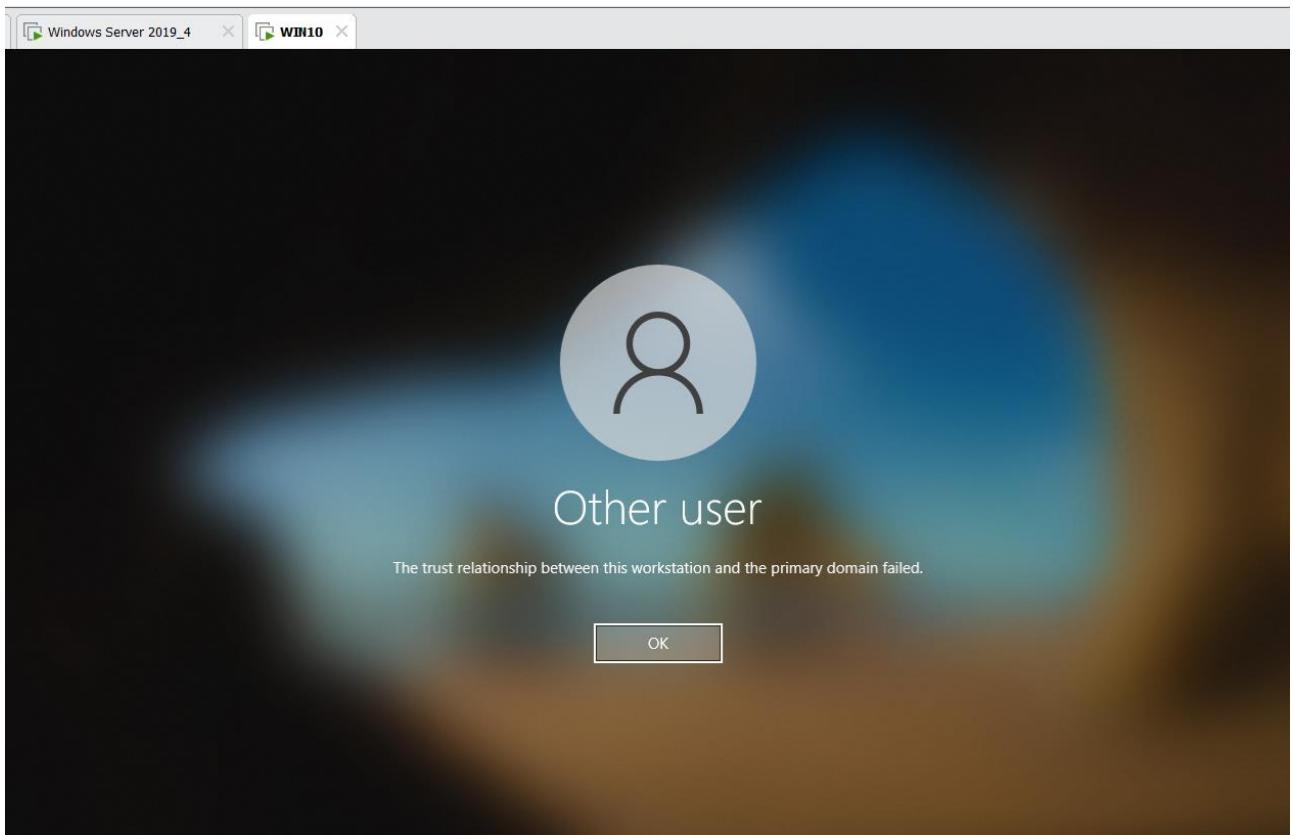
ur311 đã có trên RODC.

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

+ Tắt máy PDC.



+ Login account ur211 trên client.

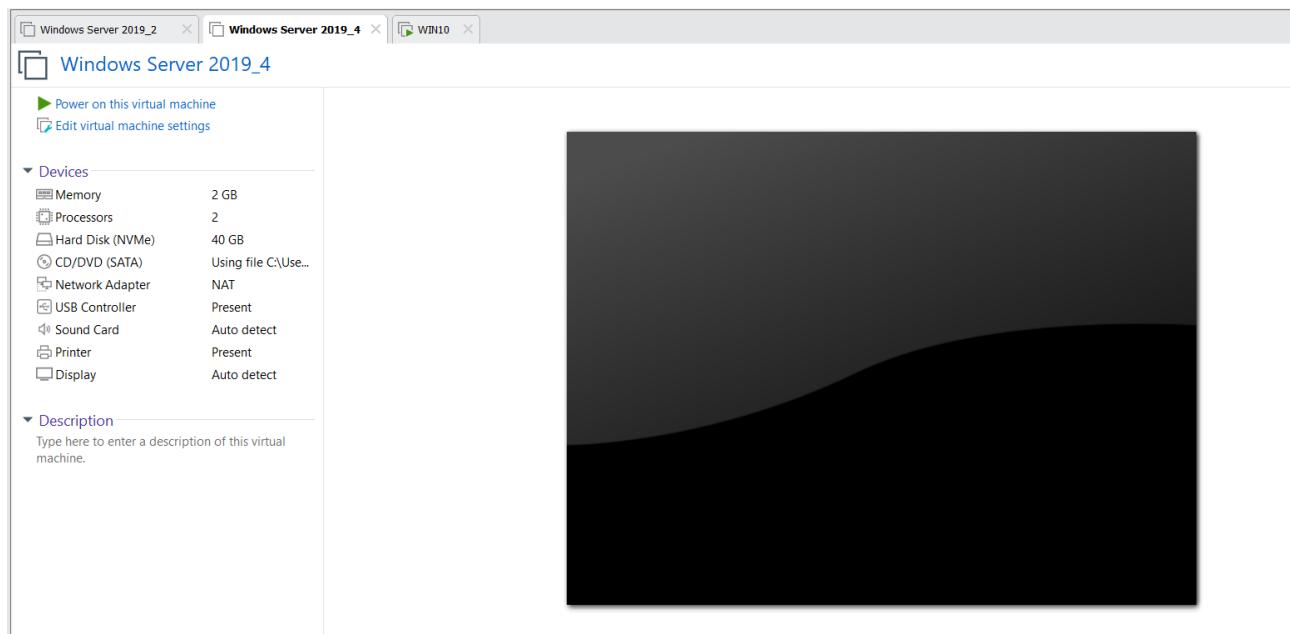


Kết quả đăng nhập không thành công.

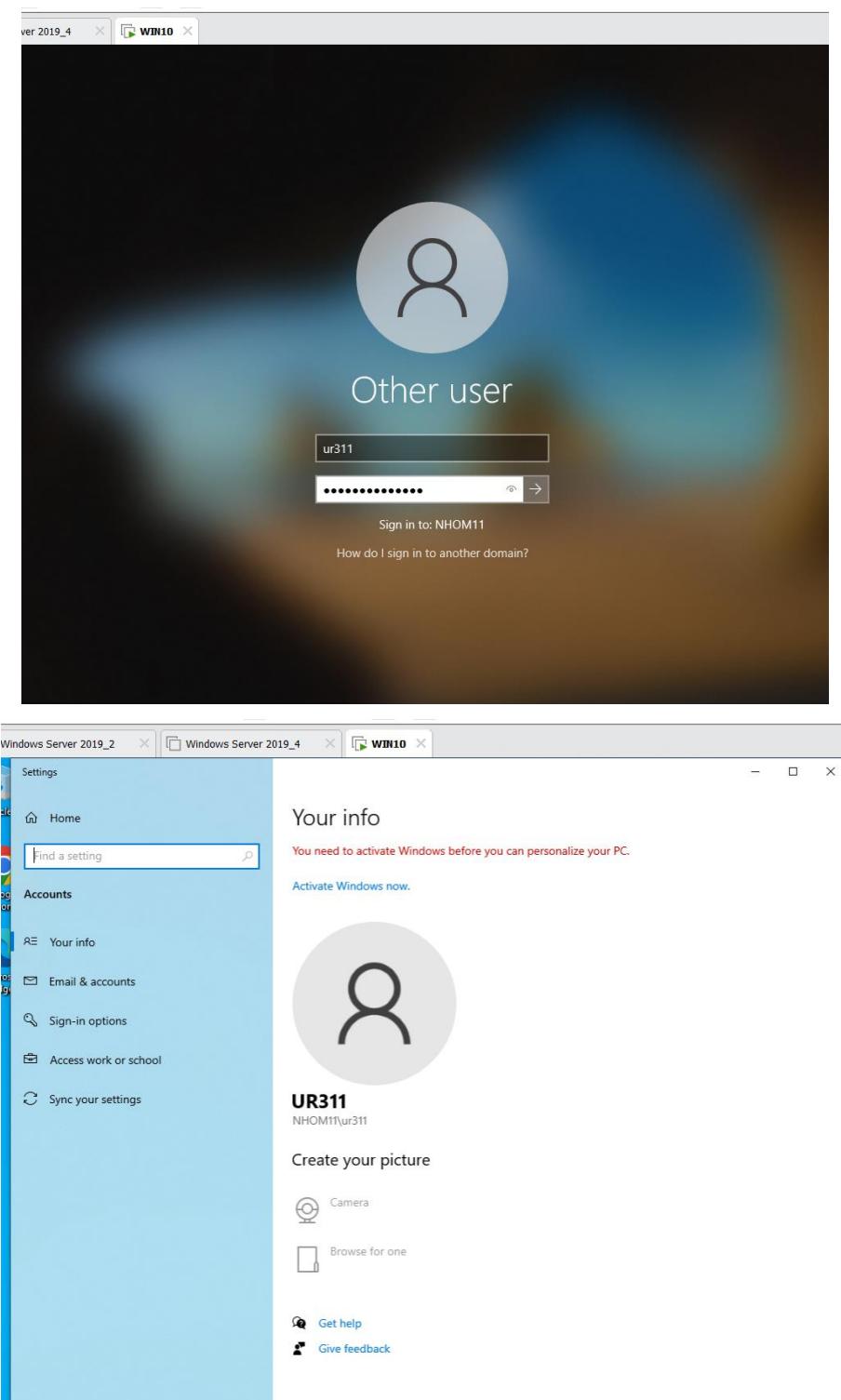
→ Kết quả: đăng nhập không thành công. Do RODC mặc định không lưu trữ dữ liệu người dùng mà nó đọc dữ liệu từ PDC thông qua cơ chế Replication giữa các Domain Controller, nên khi ta tắt PDC thì RODC cũng không hoạt động được. Dẫn đến không thể xác thực được account ur211.

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

+ Tắt máy RODC.



+ Login ur311 trên client.



Kết quả đăng nhập thành công.

➔ Kết quả: đăng nhập thành công do PDC xác thực account bình thường (không bị tác động khi tắt RODC).

## YÊU CẦU CHUNG

- Sinh viên tìm hiểu và thực hành theo hướng dẫn.
- Nộp báo cáo kết quả chi tiết những việc (**Report**) bạn đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Sinh viên báo cáo kết quả thực hiện và nộp bài.

### Báo cáo:

- File **.DOCX** và **.PDF**. Tập trung vào nội dung, không mô tả lý thuyết.
- Nội dung trình bày bằng **Font chữ Times New Romans/ hoặc font chữ của mẫu báo cáo này (UTM Neo Sans Intel/UTM Viet Sach)** – cỡ **chữ 13**. **Canh đều (Justify) cho văn bản. Canh giữa (Center) cho ảnh chụp.**
- Đặt tên theo định dạng: [Mã lớp]-SessionX\_GroupY. (trong đó X là Thứ tự buổi Thực hành, Y là số thứ tự Nhóm Thực hành đã đăng ký với GVHD-TH).

*Ví dụ: [NT101.K11.ATCL]-Session1\_Group3.*

- Nếu báo cáo có nhiều file, nén tất cả file vào file **.ZIP** với cùng tên file báo cáo.
- **Không đặt tên đúng định dạng – yêu cầu, sẽ KHÔNG chấm điểm bài Lab.**
- Nộp file báo cáo trên theo thời gian đã thống nhất tại [courses.uit.edu.vn](http://courses.uit.edu.vn).

**Đánh giá:** Sinh viên hiểu và tự thực hiện được bài thực hành. Khuyến khích:

- Chuẩn bị tốt.
- Có nội dung mở rộng, ứng dụng trong kịch bản phức tạp hơn, có đóng góp xây dựng bài thực hành.

*Bài sao chép, trễ, ... sẽ được xử lý tùy mức độ vi phạm.*

**HẾT**