

Nhóm 9:

Nguyễn Bùi Kim Ngân - 205206  
Nguyễn Bình Thục Trâm - 20520815

## Yêu cầu 1.1

### 1. Mô hình Workgroup hoạt động như thế nào?

- Một nhóm máy tính mạng cùng chia sẻ tài nguyên như file,... Các máy tính có quyền hạn ngang nhau, có quyền chia sẻ tài nguyên ngang nhau mà không cần chỉ định của server
- Mỗi máy có chức năng vừa là server vừa là client, tự duy trì những tài khoản, quản trị và chính sách bảo mật riêng.

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

Ưu:

- Cài đặt dễ dàng, thiết kế đơn giản
- Thích hợp cho số lượng máy nhỏ
- Không yêu cầu controller

Nhược:

- Kém an toàn
- Không phù hợp với số lượng máy lớn
- Triển khai được ít dịch vụ mạng
- Các tài nguyên không được quản lý tập trung, khó tìm kiếm và sử dụng

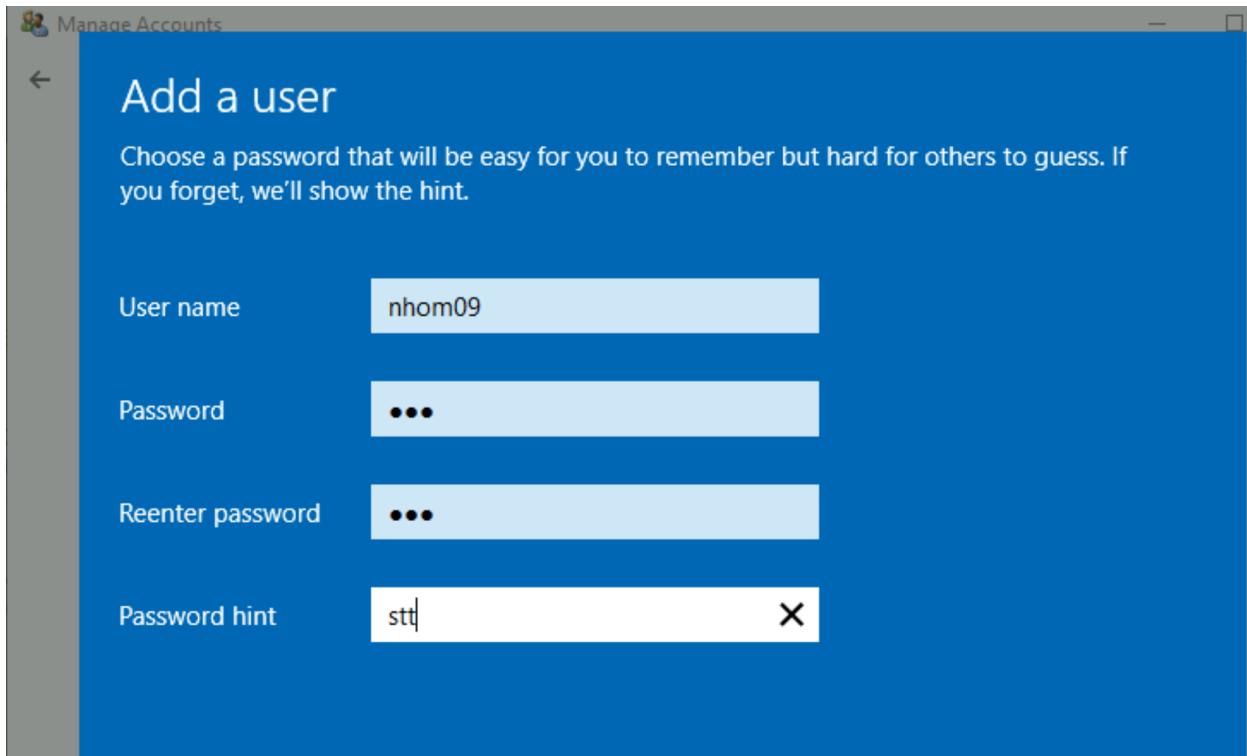
## Yêu cầu 1.2

- Thiết lập disable cho Password must meet complexity requirements:

The screenshot shows the Local Group Policy Editor window. The left pane displays the navigation tree under 'Computer Configuration' with 'Security Settings' expanded, showing 'Accounts' and 'Passwords'. The right pane lists policy settings with their current security settings:

Policy	Security Setting
Enforce password history	0 passwords remembered
Maximum password age	42 days
Minimum password age	0 days
Minimum password length	0 characters
Minimum password length audit	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

- Tạo tài khoản nhom09, pass 123



- Tạo folder09 và phân quyền read/write cho user nhom09

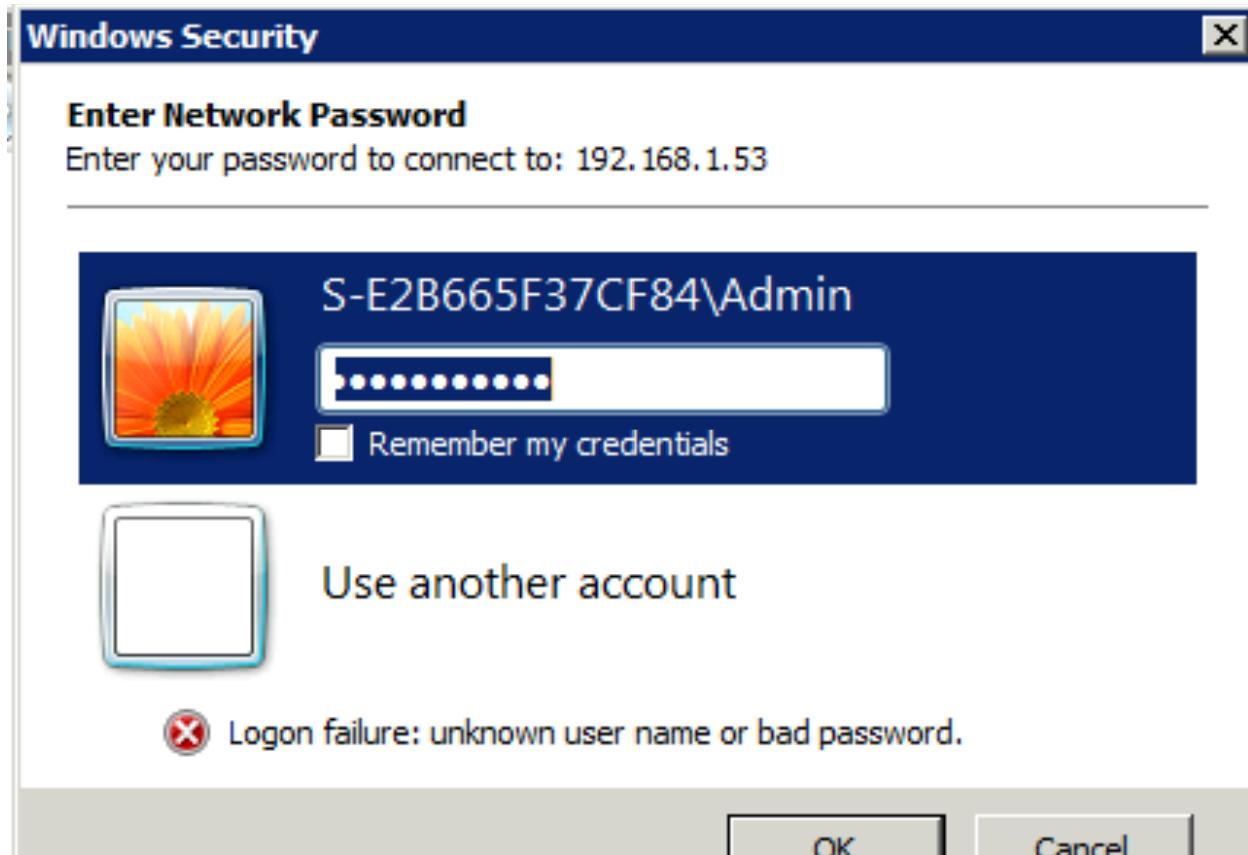
The screenshot shows the Windows File Explorer interface. On the left, there's a sidebar with icons for PerfLogs, Program Files, Program Files (x86), ProgramData, Users, Windows, and folder09. The current view is 'Network access' under 'Sharing and security'. A large blue header says 'Choose people to share with' with the sub-instruction 'Type a name and then click Add, or click the arrow to find someone.' Below this is a search bar and an 'Add' button. A table lists users and their permission levels:

Name	Permission Level
Administrator	Read/Write ▾
Administrators	Owner
nhom09	Read/Write ▾

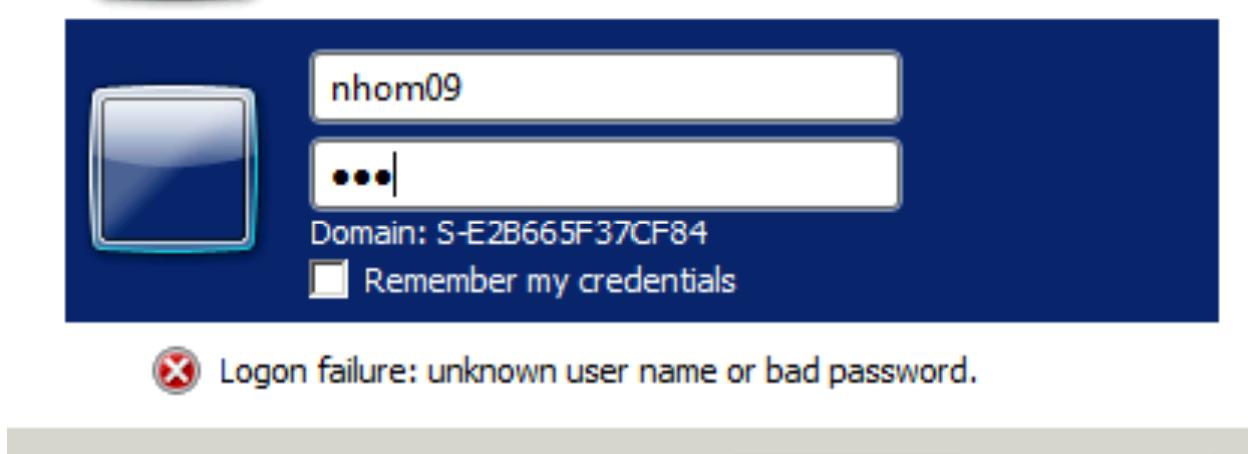
- Tại máy client, kết nối tới máy chủ File Server bằng tài khoản của máy client

The screenshot shows a 'Windows Security' dialog box titled 'Enter Network Password'. It prompts the user to enter a password to connect to the IP address 192.168.1.53. The dialog includes fields for the username ('Admin'), password (represented by a series of dots), and domain ('Domain: S-E2B665F37CF84'). There is also a 'Remember my credentials' checkbox. Below the dialog is an error message: 'Logon failure: unknown user name or bad password.' At the bottom are 'OK' and 'Cancel' buttons.

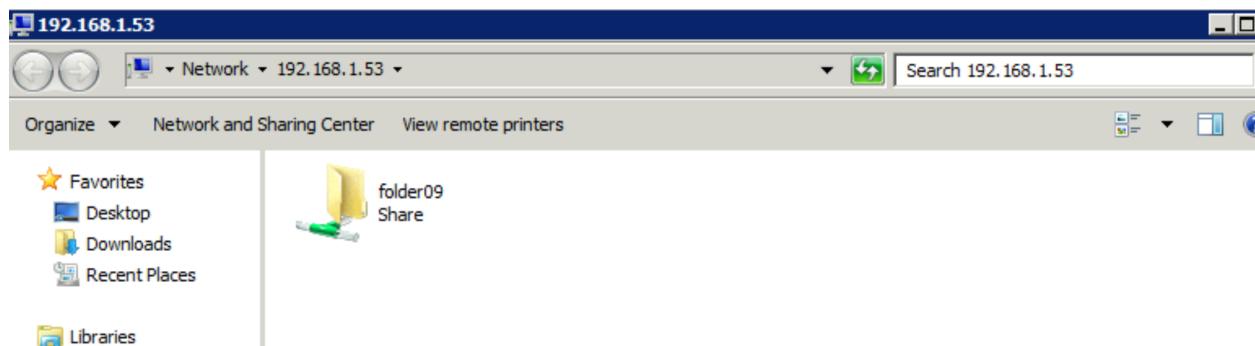
- Kết quả không thành công. Do tài khoản trên là tài khoản local của máy client, không nằm trong tài khoản của file server



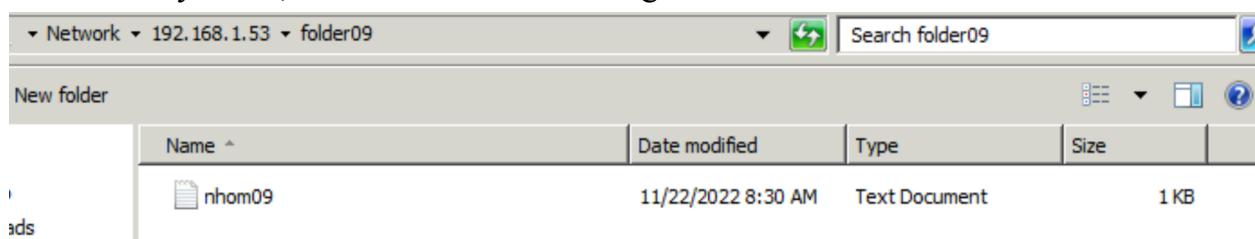
- Thử lại bằng tài khoản nhom09 tạo từ bước trước



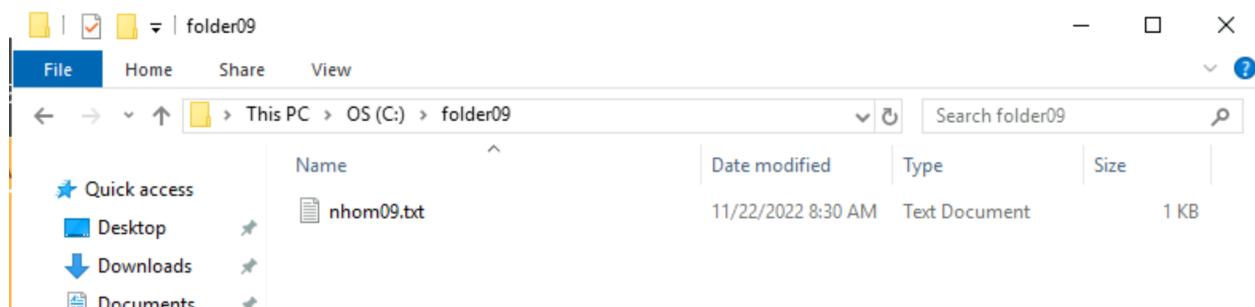
- Kết quả kết nối thành công và tìm được folder đã chia sẻ



- Ở máy client, tạo file text nhom09 trong thư mục



- Kiểm tra trên File Server, file vừa tạo đã hiện lên



## 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?

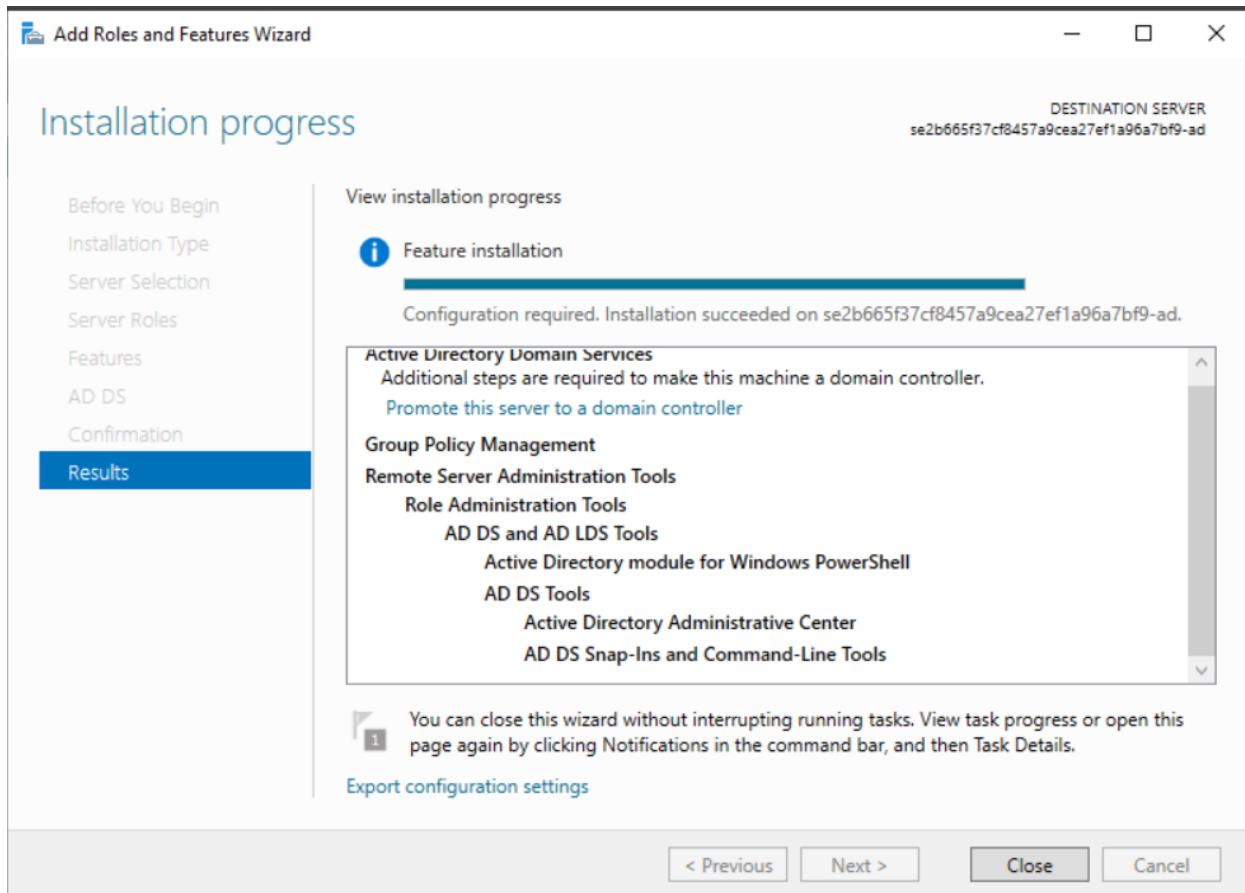
=> Là một dịch vụ thư mục được Microsoft phát triển cho các mạng sử dụng Windows domain. Một máy chủ chạy Active Directory Domain Service (AD DS) được gọi là domain controller. Nó xác thực và ủy quyền cho tất cả người dùng và máy tính trong mạng loại Windows gán và thực thi các chính sách bảo mật cho tất cả các máy tính và cài đặt hoặc cập nhật phần mềm.

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

Domain Controller	Workgroup
<ul style="list-style-type: none"><li>- Set up phức tạp, chi phí cao.</li><li>- Có domain controller server.</li><li>- Sẽ có một trong số các máy thuộc hệ thống trở thành domain account để quản lý.</li><li>- Để sử dụng, máy tính cần phải join vào domain.</li><li>- Các máy có thể không cùng mạng.</li><li>- Có thể cho phép hàng ngàn máy join vào domain cùng lúc =&gt; Phù hợp build hệ thống lớn.</li><li>- Mọi máy tính thuộc domain đều có thể được đăng nhập vào bằng account được quản lý bởi domain controller.</li><li>- Chỉ có admin mới có thể thực hiện các thay đổi quan trọng liên quan đến group policy.</li></ul> <p>=&gt; An toàn hơn và có thể dùng để share các dữ liệu nhạy cảm.</p>	<ul style="list-style-type: none"><li>- Set up đơn giản, chi phí thấp.</li><li>- Không có hệ thống server quản lý.</li><li>- Sẽ không có máy nào trong hệ thống có quyền quản lý các máy còn lại =&gt; Peer - to - peer.</li><li>- Máy tính không cần join vào domain.</li><li>- Các máy bắt buộc phải cùng mạng.</li><li>- Chỉ phù hợp sử dụng build hệ thống nhỏ khoảng 20 máy tính hoặc ít hơn.</li><li>- Mỗi máy tính có nhiều tài khoản được liên kết với nó. Mỗi tài khoản chỉ có thể đăng nhập vào máy tính có trong liên kết.</li><li>- Có thể thay đổi group policy trong nhóm cục bộ mà không cần quyền admin.</li></ul> <p>=&gt; Kém an toàn hơn.</p>

Triển khai:

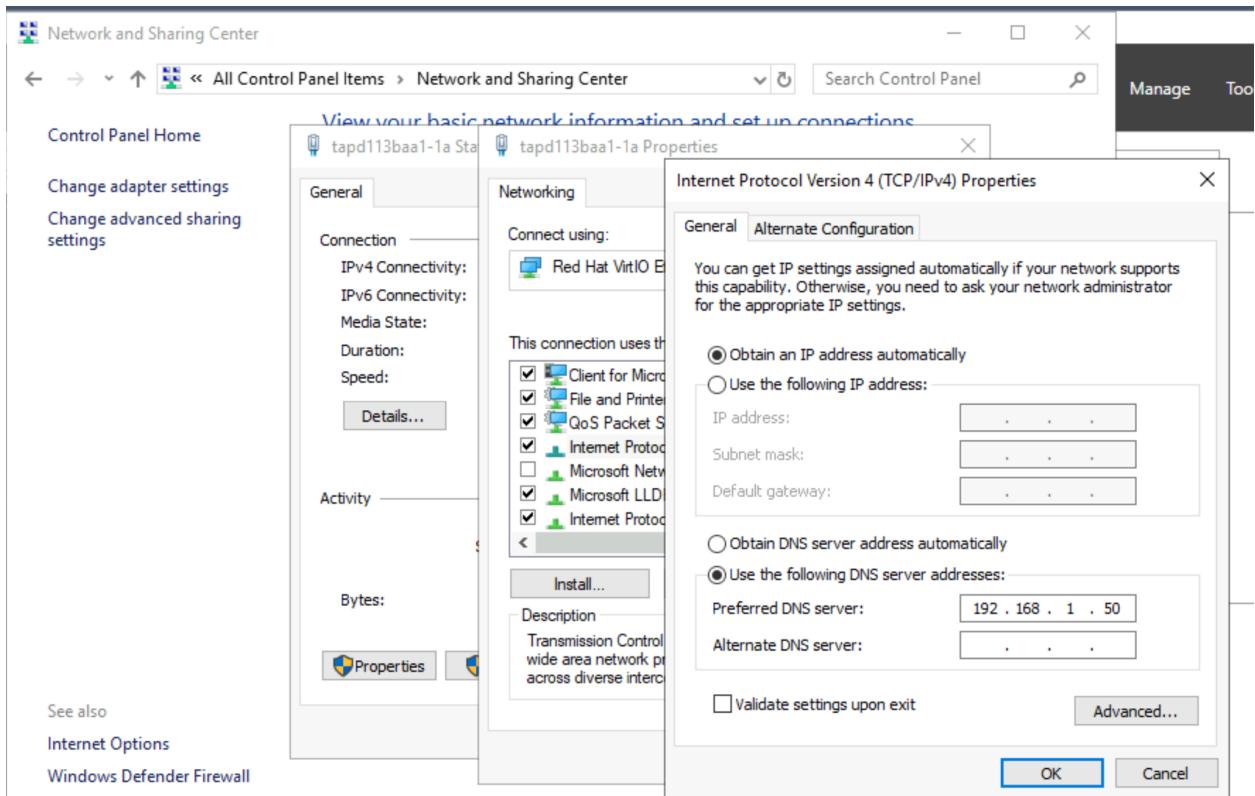
Setup các option và install



Tạo các user trong domain. Password: Bingt0n!

User	Type	Description
Guest	User	BUILT-IN ACCOUNT FOR gue...
fileadmin	User	
<b>user1</b>	User	

Configure DNS để add máy vào domain



Test ping

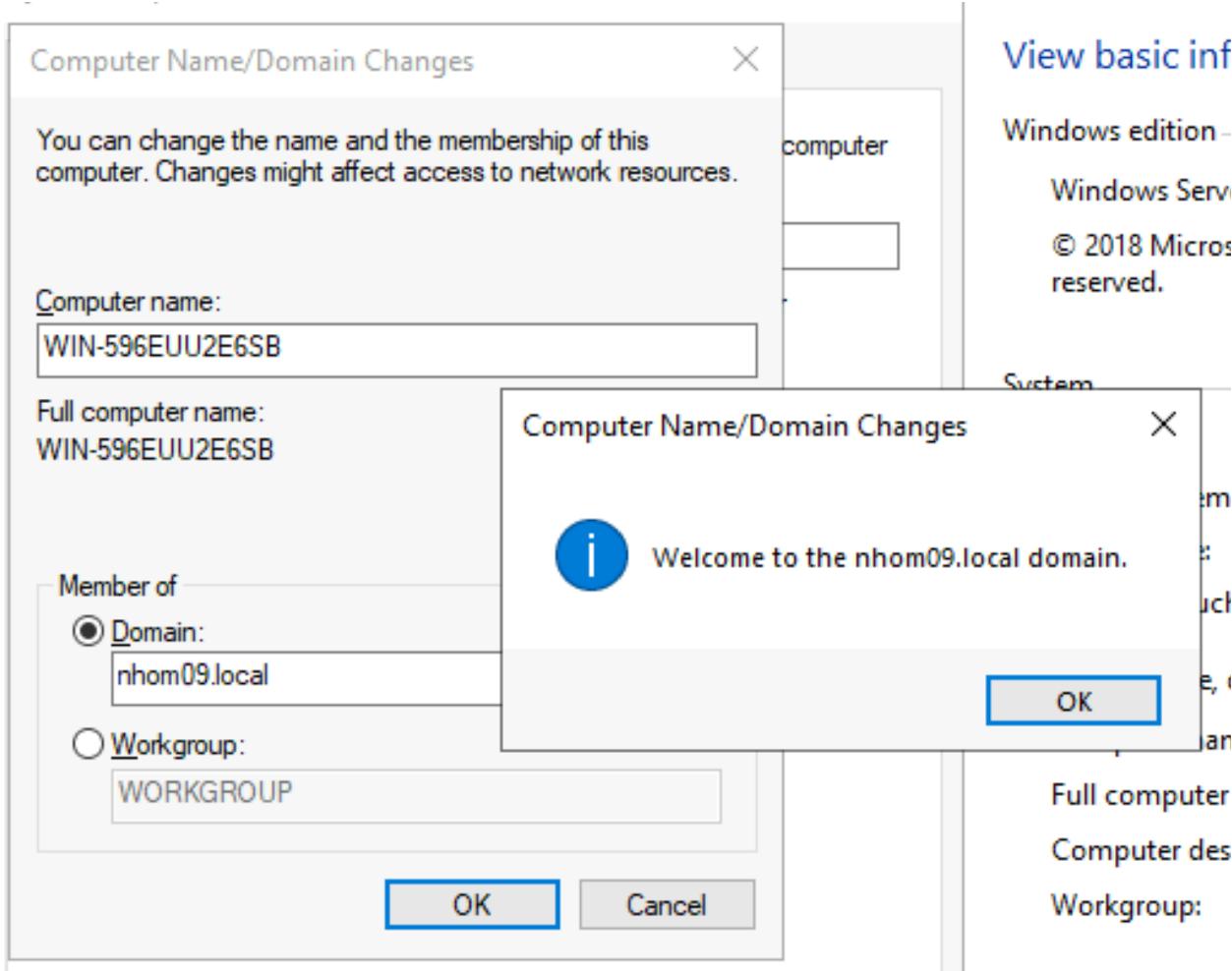
```
C:\Users\Administrator>ping nhom09.local

Pinging nhom09.local [192.168.1.50] with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time=1ms TTL=128

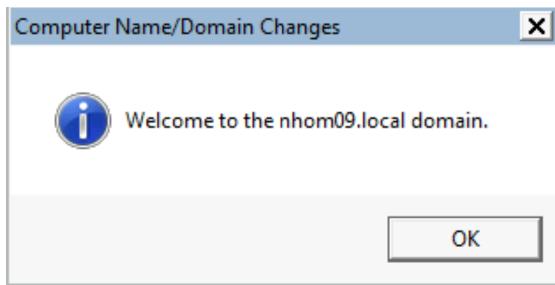
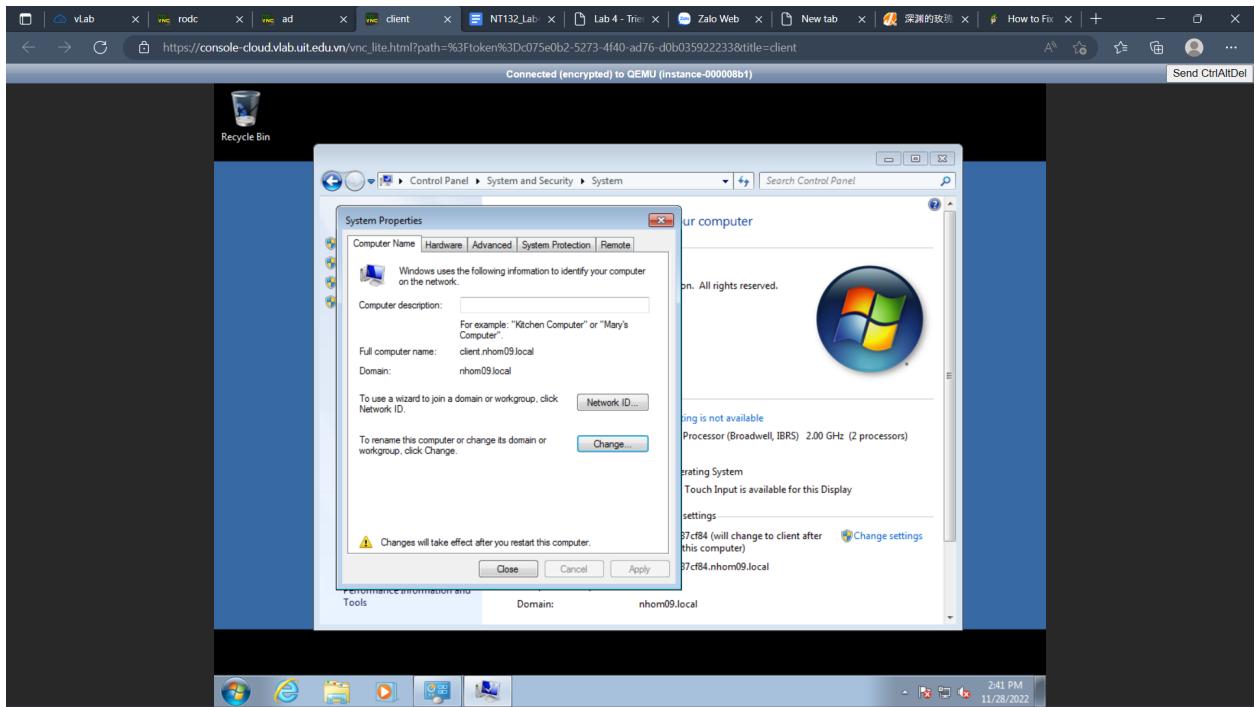
Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

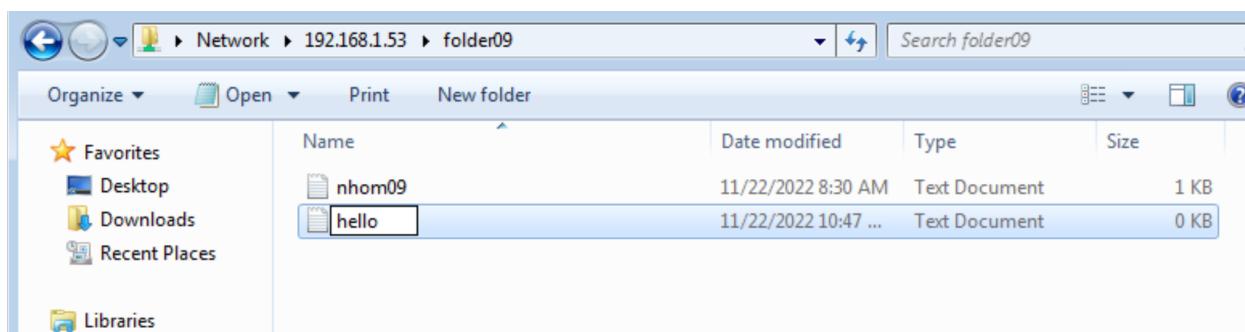
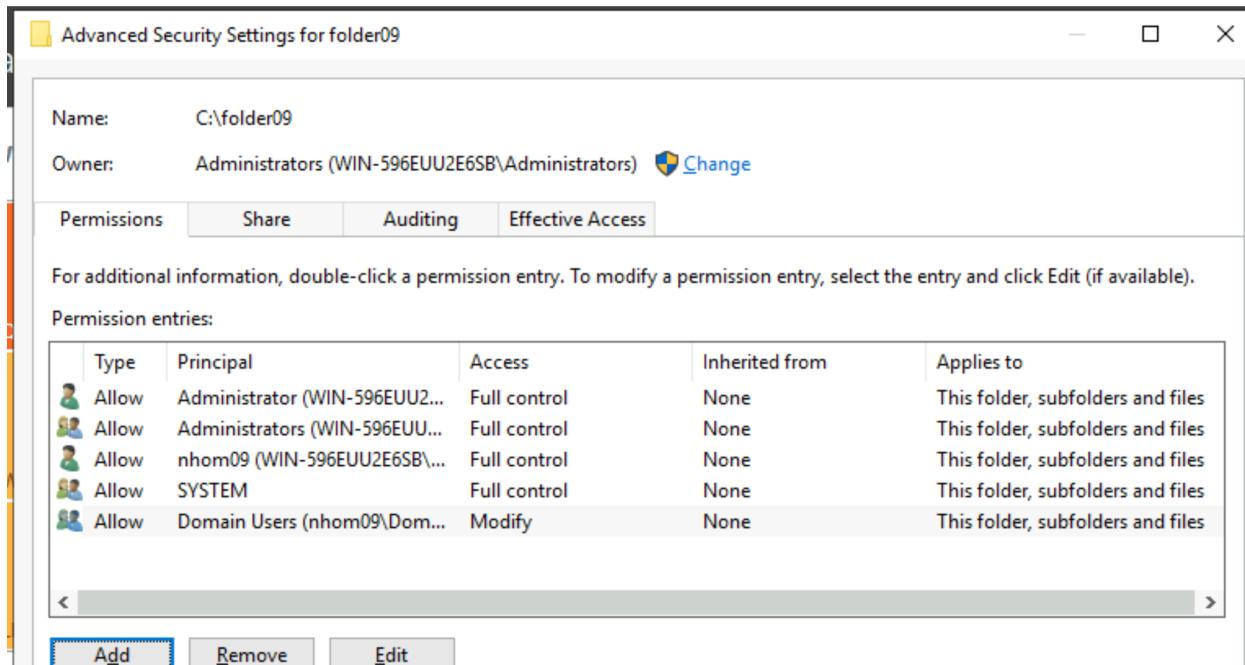
C:\Users\Administrator>
```

Thành công add máy đóng vai trò File Admin vào domain



Thành công add user1 vào domain





### 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?

=> Additional domain controller được dùng để cân bằng tải giữa các domain controller hiện có. Nếu chẳng may Domain Controller bị lỗi thì vẫn có các additional domain controller để duy trì hệ thống.

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

=> Dữ liệu chứng thực người dùng, DNS... của Domain được đồng bộ giữa Primary Domain Controller (PDC) và các Additional Domain Controller (ADC). Về khả năng chứng thực và phân giải DNS thì các ADC và PDC đều có khả năng như nhau do giữa các

server đồng bộ dữ liệu cho nhau. Trong trường hợp có một trong những server bị chết sẽ không ảnh hưởng đến việc hoạt động đột ngột của domain, ngoài ra hệ thống cũng có thể phân bổ việc chứng thực cho các server.

### 3. Khi nào cần sử dụng ADC?

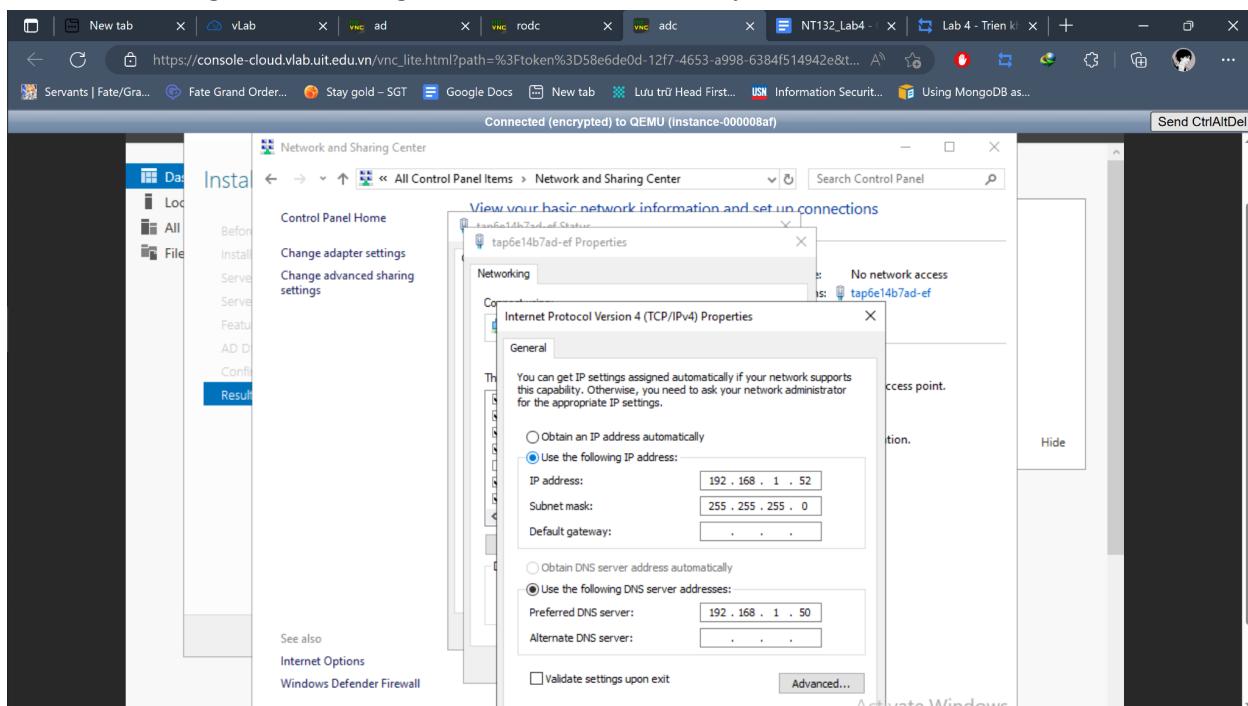
Mô hình ADC thường được sử dụng trong các trường hợp sau đây:

- Hệ thống có nhiều Site.
- Hệ thống chỉ có 1 site nhưng có số lượng user lớn. Khi log on, DC sẽ bị quá tải và gây ra tình trạng nghẽn mạng.
- Hệ thống chỉ có 1 site và chỉ có 1 PDC, hệ thống nhỏ. Toàn bộ hệ thống hiện đang chạy ổn định. Nhưng một ngày nào đó PDC gặp sự cố, thì hệ thống công ty sẽ bị tê liệt. Thời gian khôi phục sẽ mất khá nhiều thời gian. Vì vậy sử dụng ADC để phòng ngừa là một giải pháp.

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

##### Các bước thiết lập:

Đầu tiên, chúng ta cần config DNS để có thể add máy ADC vào domain:



Ping để test thử giữa các máy:

Connected (encrypted) to QEMU (instance-000008ae)

Administrator: Command Prompt

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

C:\Users\Administrator>ping 192.168.1.52

Pinging 192.168.1.52 with 32 bytes of data:
Reply from 192.168.1.52: bytes=32 time=2ms TTL=128
Reply from 192.168.1.52: bytes=32 time=1ms TTL=128
Reply from 192.168.1.52: bytes=32 time=1ms TTL=128
Reply from 192.168.1.52: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.1.52:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Users\Administrator>
```

Events

Connected (encrypted) to QEMU (instance-000008b0)

Administrator: Command Prompt - ping 192.168.1.50

```
C:\Users\Administrator>ping 192.168.1.50

Pinging 192.168.1.50 with 32 bytes of data:
Reply from 192.168.1.50: bytes=32 time=zms 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
```

Performance

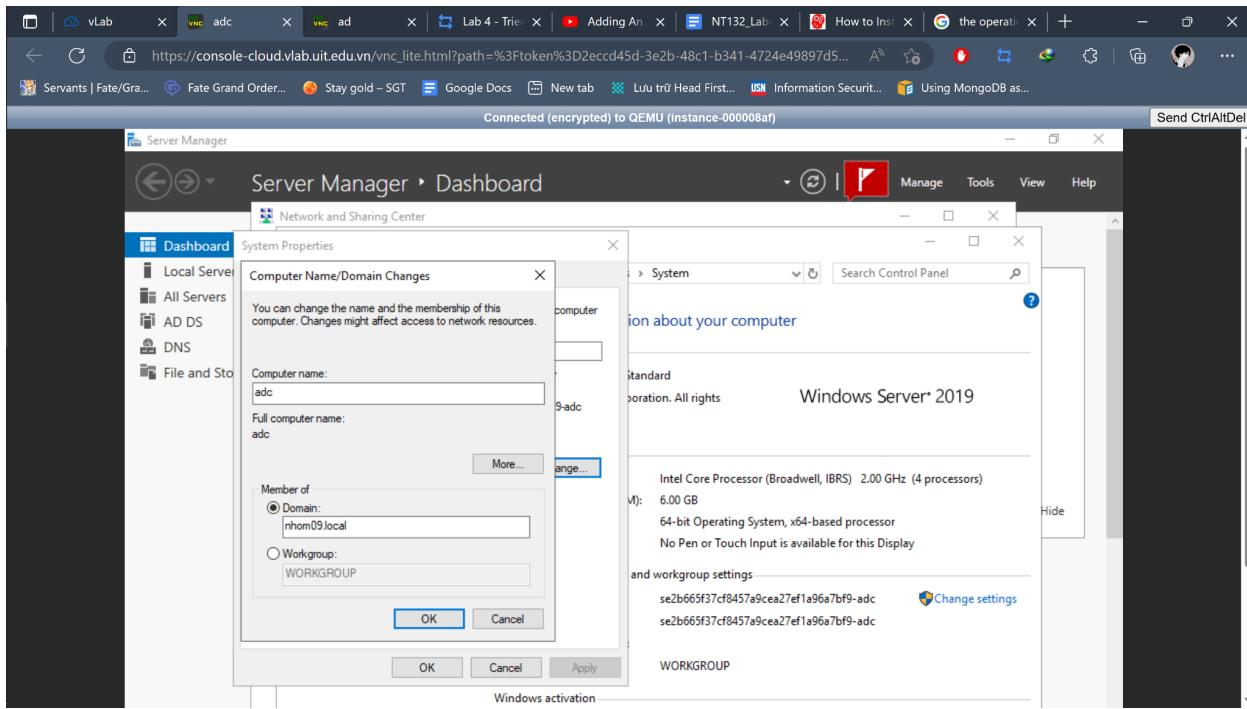
BPA results

Performance

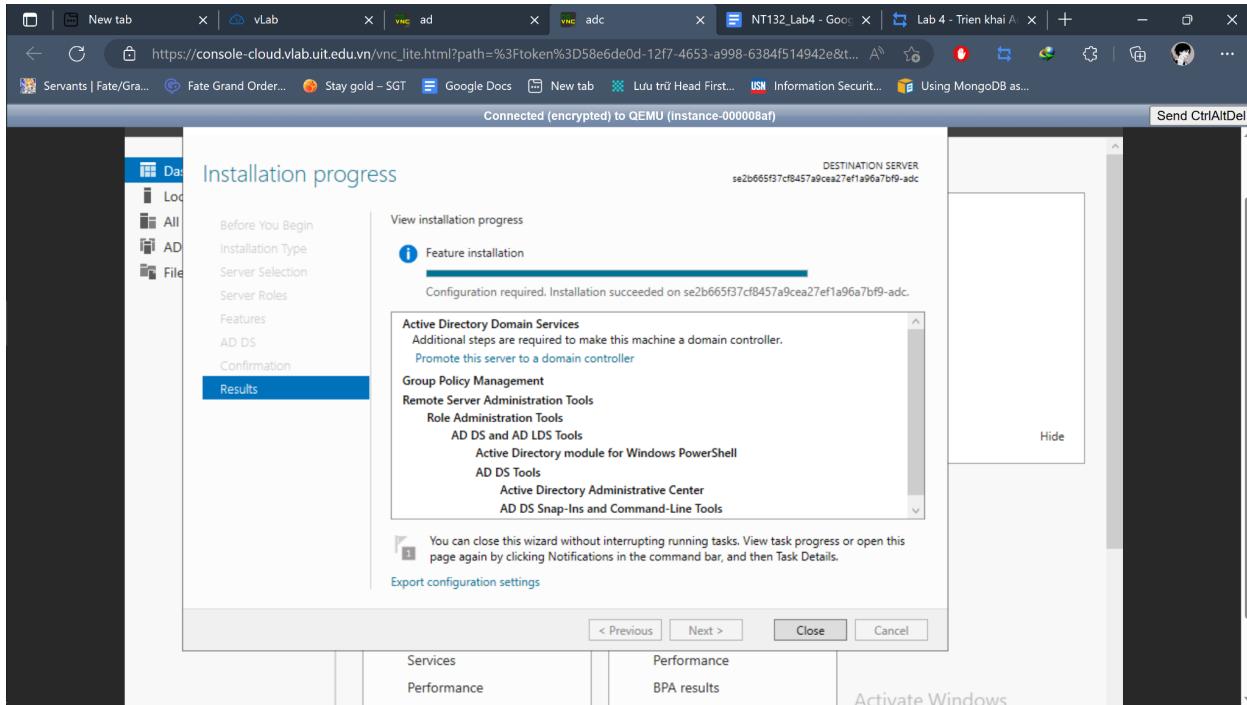
BPA results

Activate Windows  
Go to Settings to activate Windows.

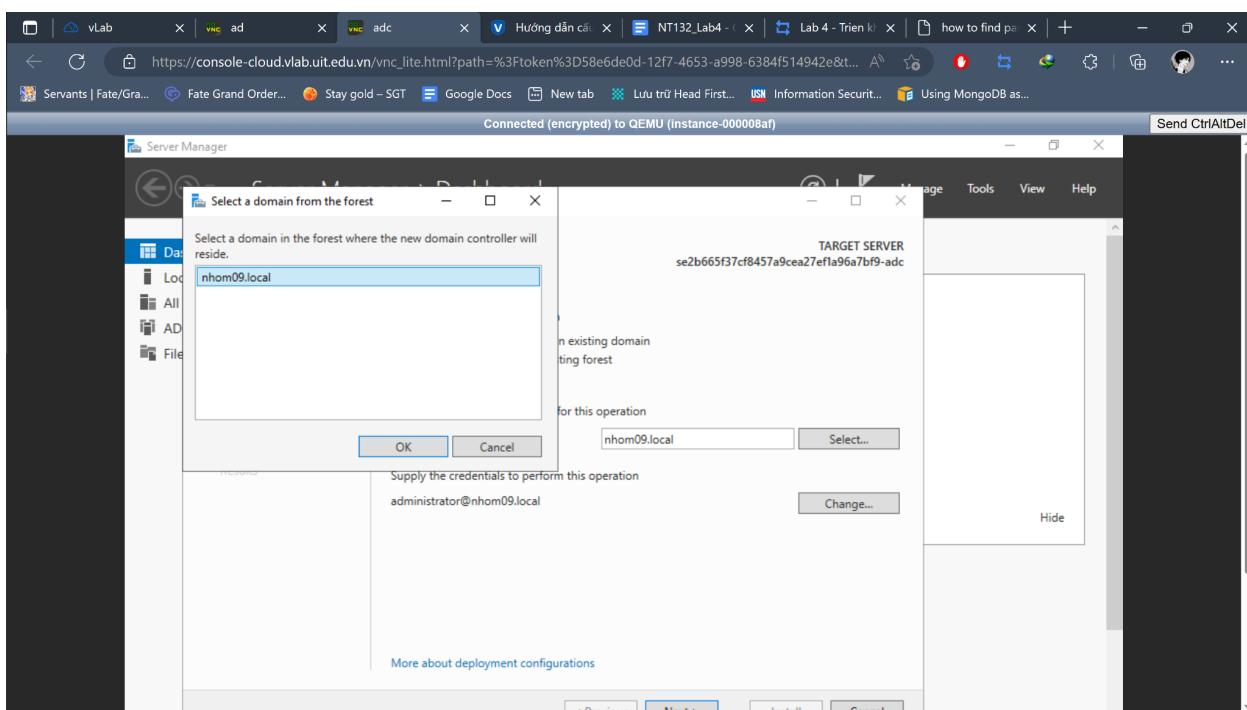
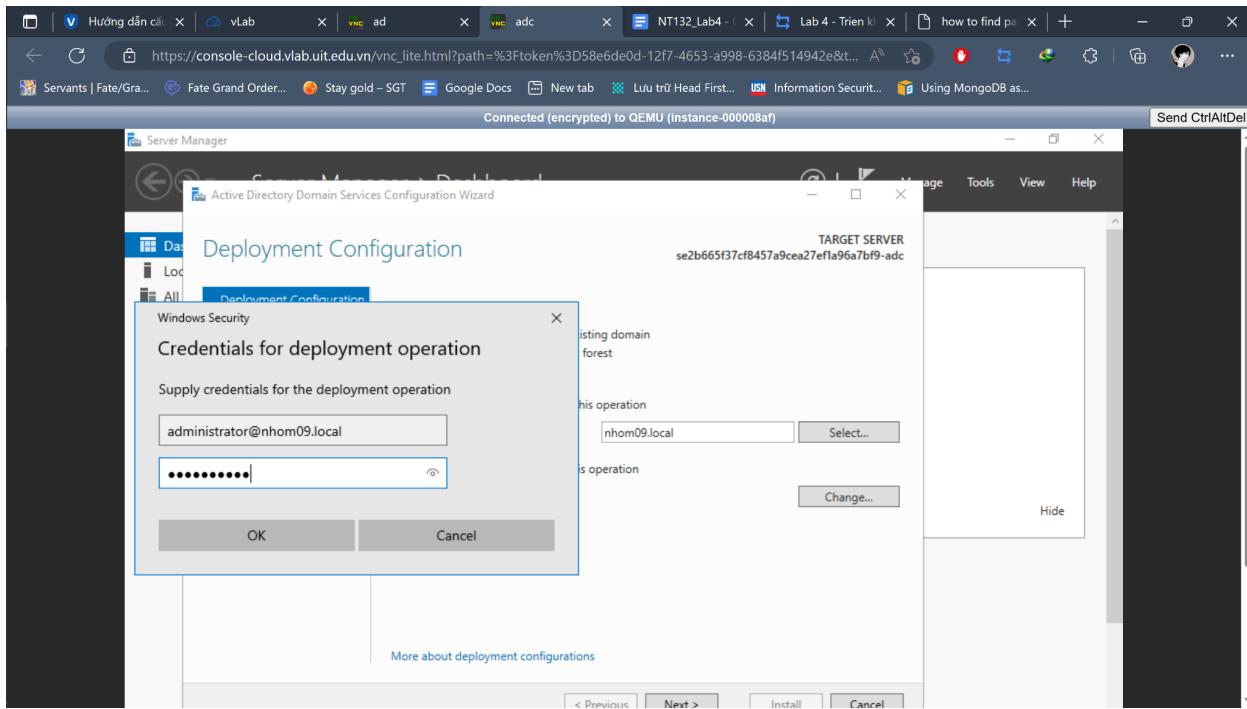
Tiếp theo, ta đổi tên computer trong domain và thực hiện add máy vào domain bằng tài khoản administrator.



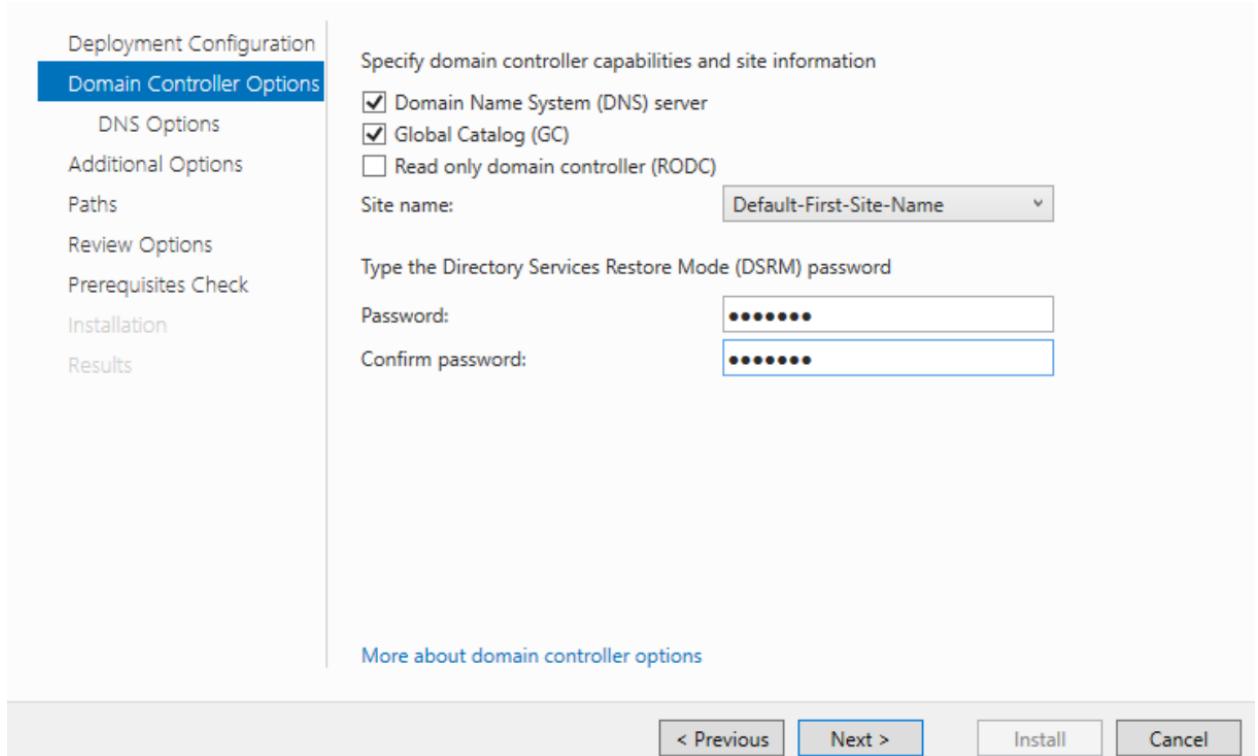
Sau đó, ở máy ADC, ta vào Add roles and feature, chọn add Active directory domain service để set up ADC với các option như hình dưới.



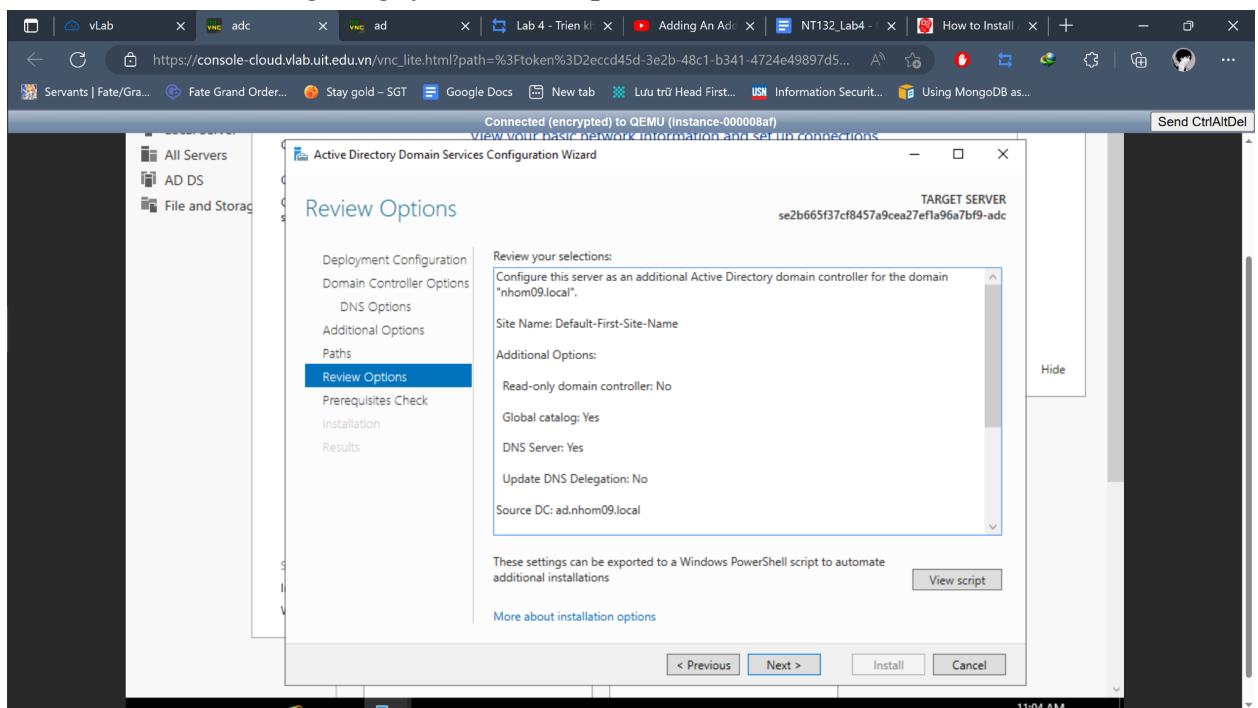
Sau khi cài đặt hoàn tất, ta vào Deployment Configuration để tiếp tục setup. Ở tab đầu tiên tick vào mục Add a domain controller to an existing domain, sau đó chọn select, nhập user password của tài khoản admin vào để chọn domain nhom09.local

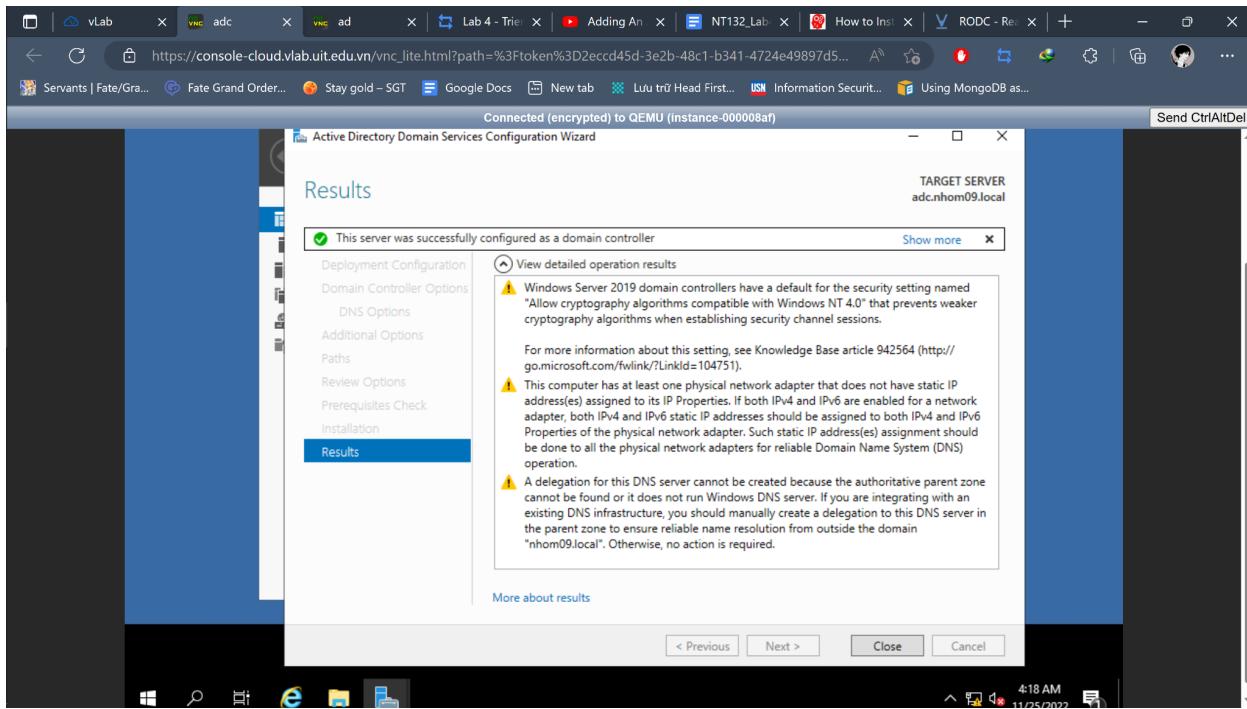


Ở Domain Controller Options, ta tick và nhập pass như hình dưới.

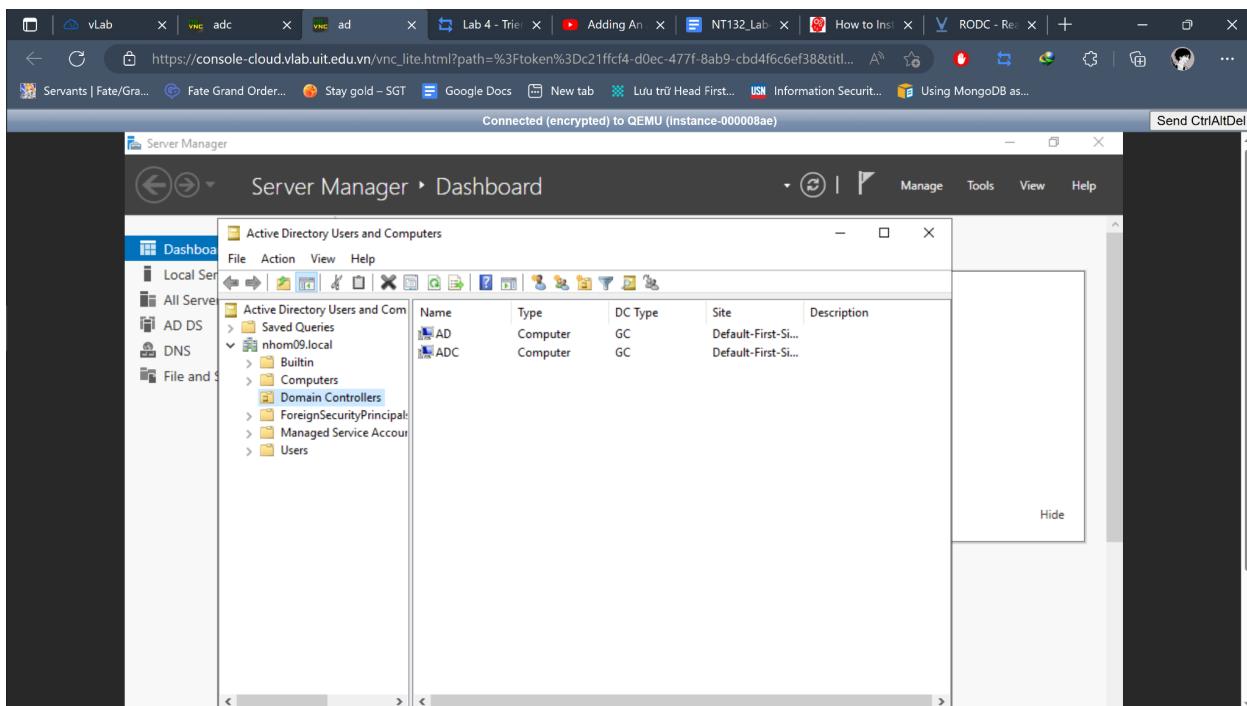


Ở các mục còn lại, ta giữ nguyên default option và thực hiện install.



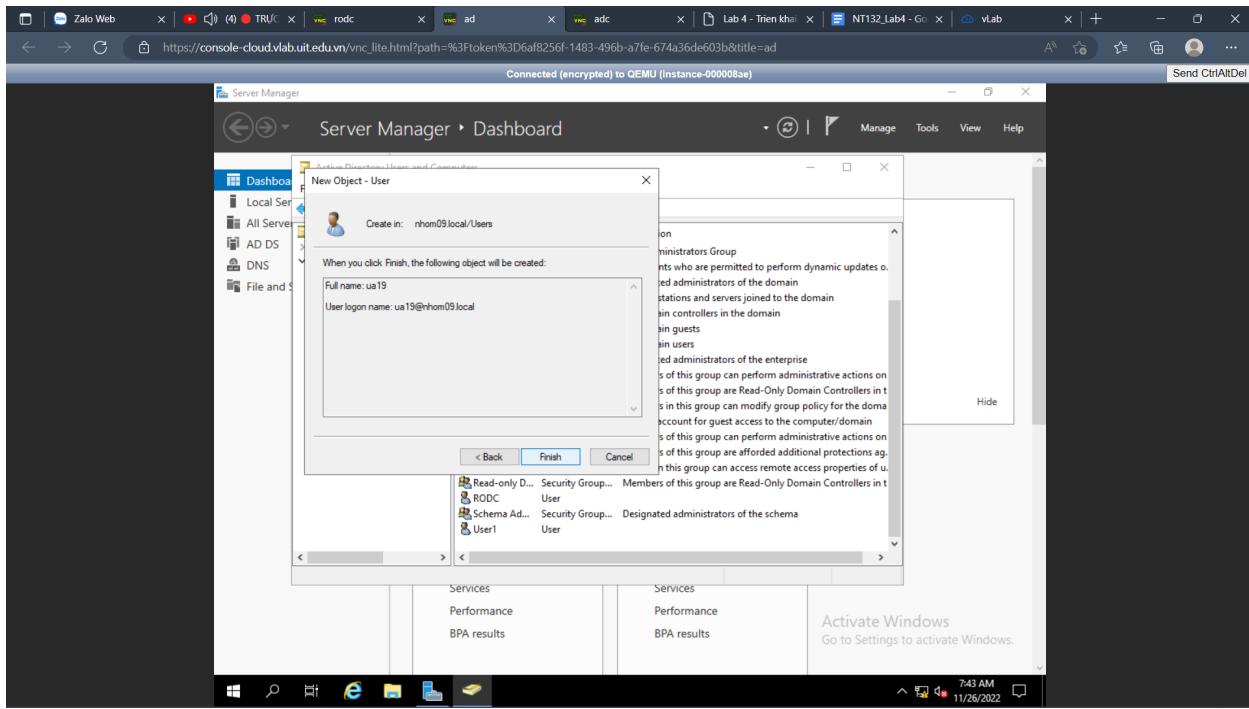


Sau khi hoàn thành, ta có thể thấy được trong phần Domain Controller xuất hiện thêm máy ADC, đóng vai trò là Additional Domain Controller.

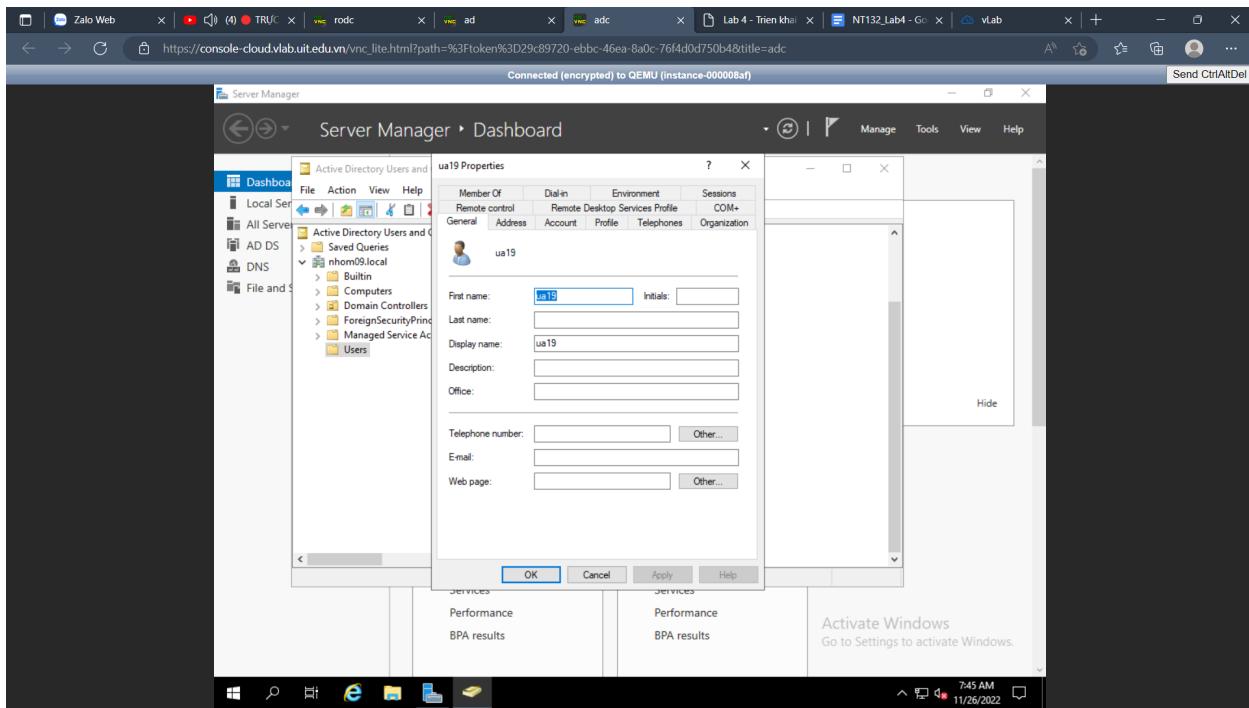


Thực hiện các công việc sau và kiểm tra kết quả (X là số thứ tự nhóm)

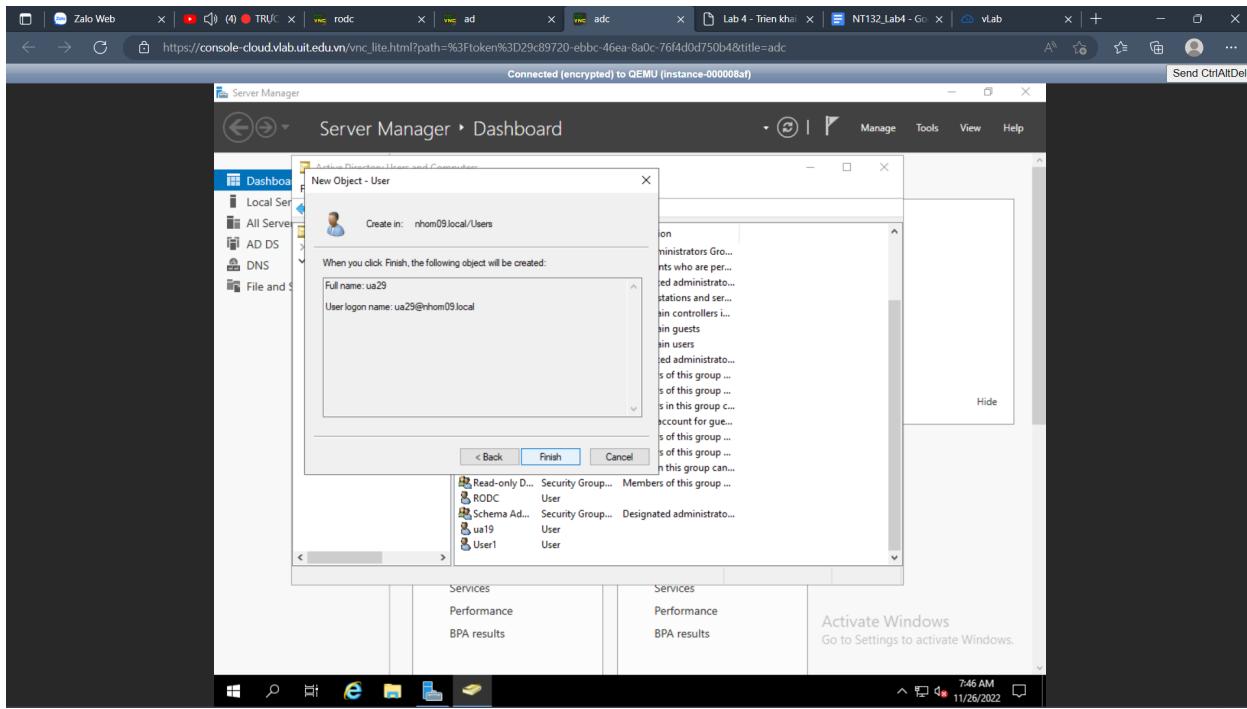
- Tạo user ua1X trên Primary DC. Kiểm tra thông tin user này trên Additional DC.



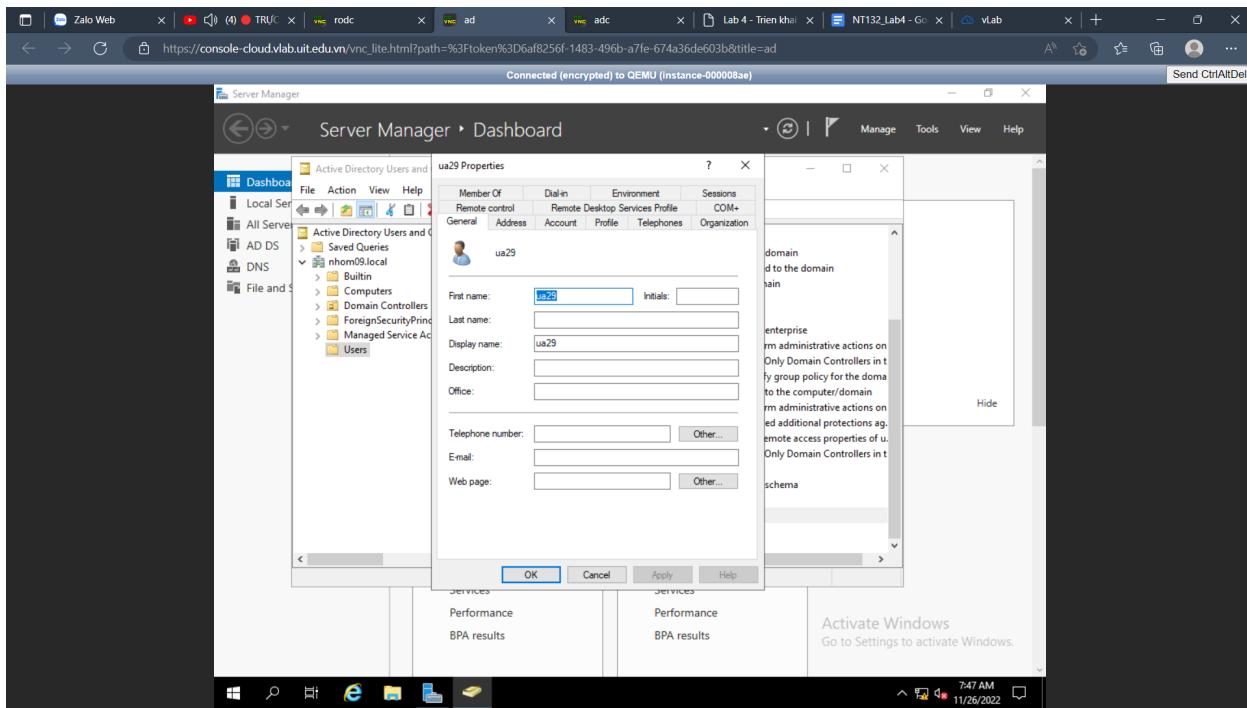
Sau đó ta hoàn toàn có thể vào kiểm tra user này trong máy ADC.



- Tạo user ua2X trên Additional DC. Kiểm tra thông tin user này trên Primary DC.

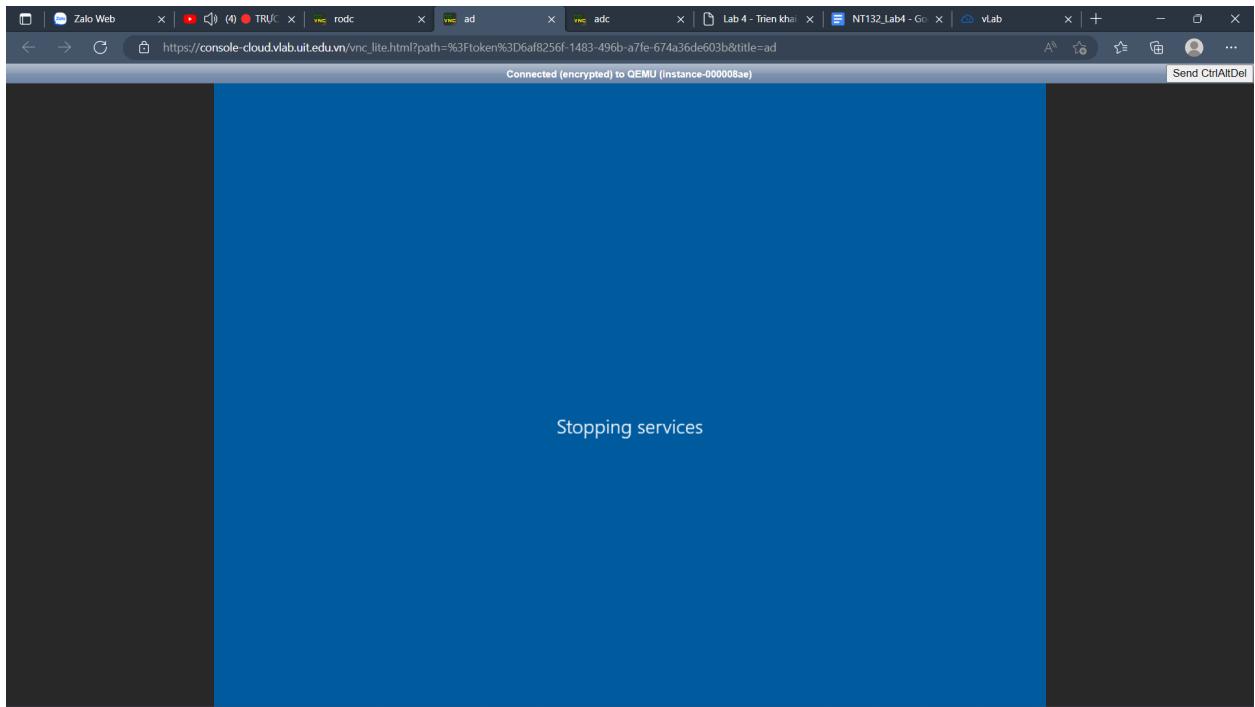


Ta cũng có thể click vào và xem thông tin của user

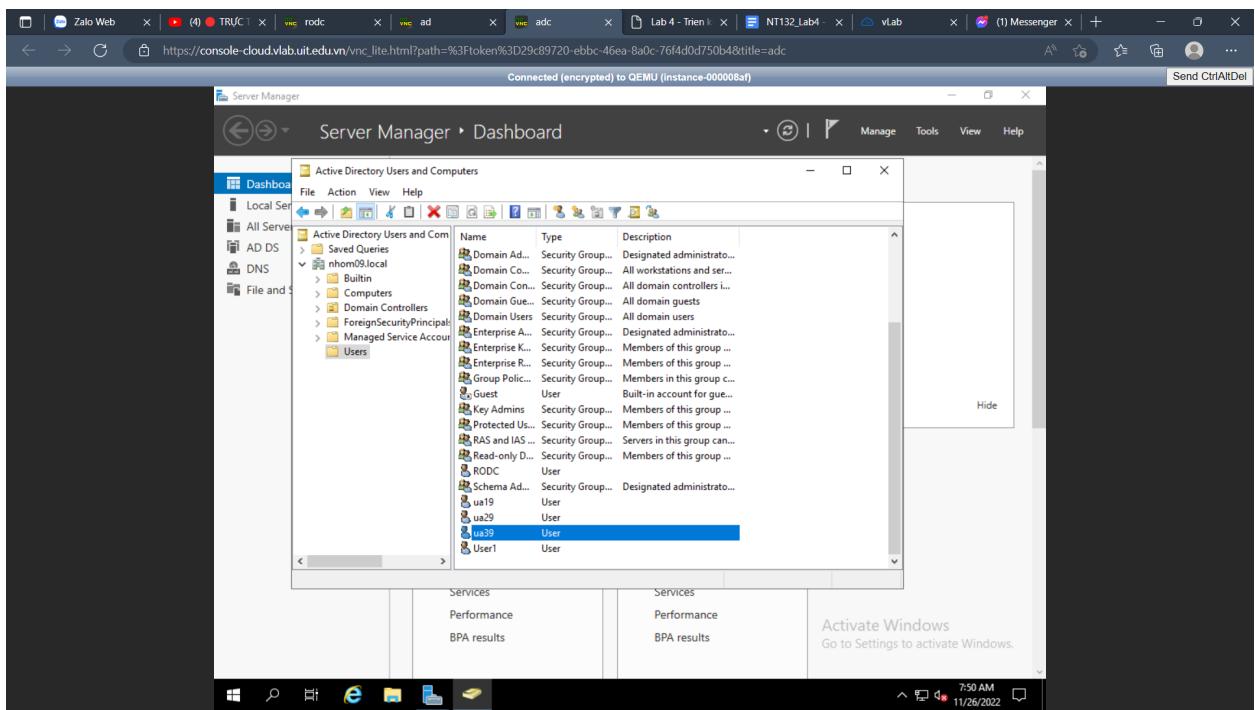


- Tắt máy Primary DC, thêm user ua3X trên Additional DC. Sau đó mở lại Primary DC và kiểm tra thông tin user này trên Primary DC.

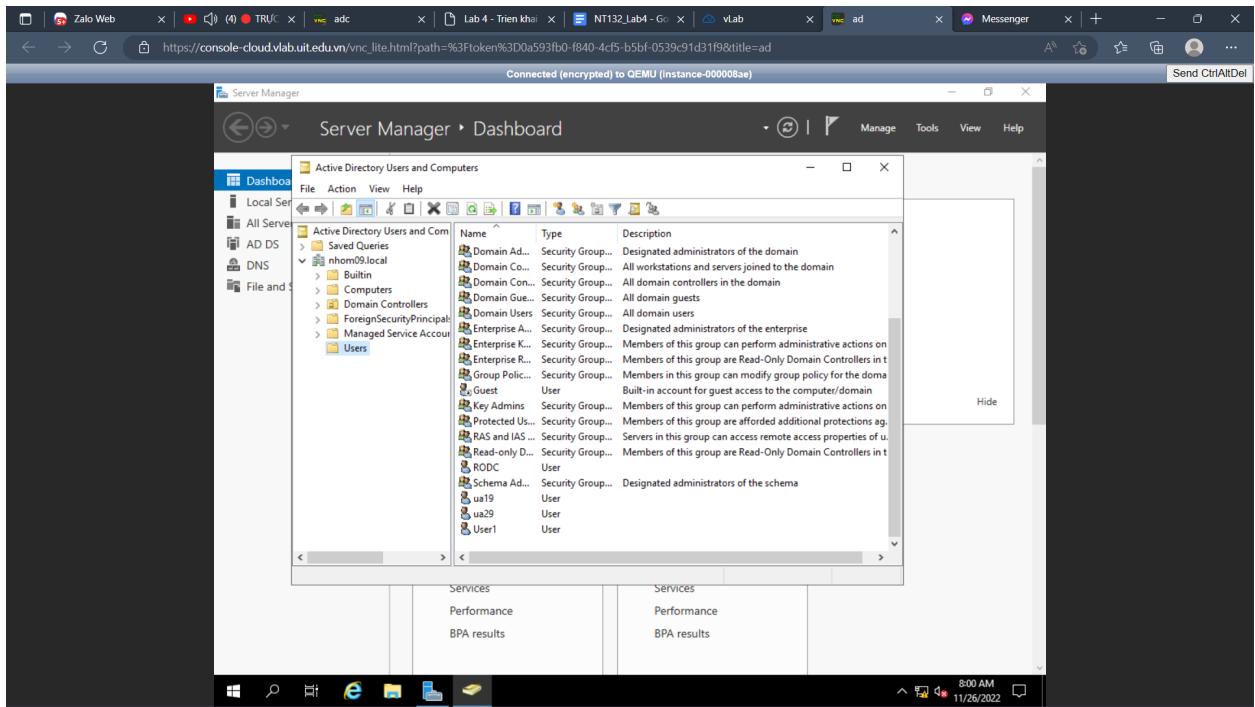
Ta shut down máy AD trước:



Sau đó, thực hiện add user trên máy ADC:

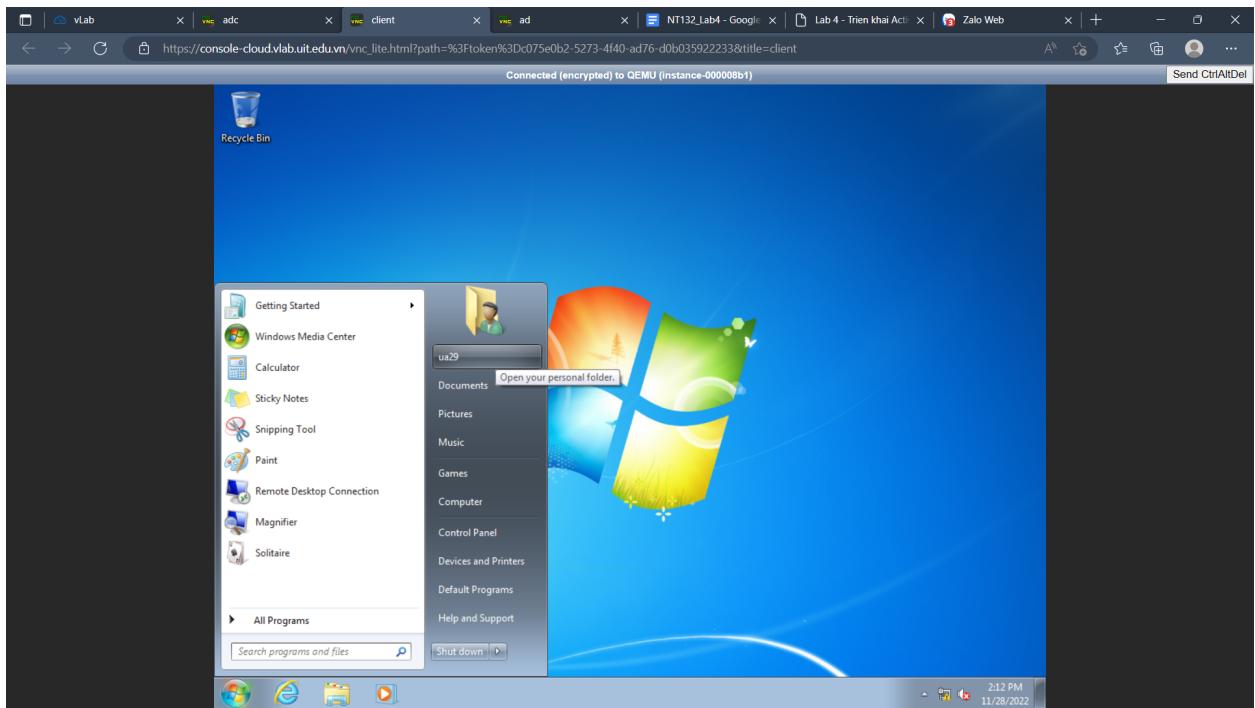


Trên máy AD, ta ko nhìn thấy ua39



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

Sau khi tắt máy PDC (máy AD) thì vẫn có thể vào được user ua29 như bình thường vì vẫn còn máy ADC là additional domain controller, vẫn có khả năng xác thực cho các user account.



#### **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?**

=> Read Only Domain Controller hay còn gọi là RODC, là một tính năng của Microsoft window server, đối với 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.

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

=> Read-Only Domain Controller (RODC) chỉ cho phép chứa bản sao của Database của AD DS từ các máy Fully Writable Domain Controller. Mặc định, các thông tin xác thực của Users và Computers không được sao chép tới RODC. Để sử dụng một RODC tăng cường cho việc xác thực người dùng, bạn cần cấu hình tính năng Password Replication Policy (PRP) để chỉ định thông tin xác thực của những người dùng nào mà bạn cho phép lưu trữ trong bộ nhớ Cache của RODC.

##### **3. Khi nào cần sử dụng RODC?**

=> Mục đích chính của RODC là để cung cấp an ninh trong các văn phòng chi nhánh. Ở các văn phòng chi nhánh thường rất khó để có được sự giúp đỡ cho những vấn đề cơ sở hạ tầng IT, đặc biệt là Domain Controllers chứa những dữ liệu nhạy cảm. Thông thường một DC có thể tìm thấy dưới một chiếc bàn ở văn phòng. Nếu một người nào đó có thể truy cập vật lý vào DC, không khó để tác động vào hệ thống và có thể truy cập vào dữ liệu. RODC có thể giải quyết những vấn đề này.

Bên cạnh đó, RODC cũng có thể giảm thiểu chi phí cho các công ty khi set up, vì nó không cho phép ghi dữ liệu nên chỉ tốn chi phí ở chiều sao chép dữ liệu, nhờ đó giúp các công ty tiết kiệm hơn.

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

Additional Domain Controller	Read-Only Domain Controller
<ul style="list-style-type: none"> <li>- Fully Writable Domain Controller (Domain Controller có thể ghi được liệu vào Database của AD DS)</li> <li>- Set up phức tạp và chi phí cao hơn.</li> <li>- Không thể triển khai ở một vị trí</li> </ul>	<ul style="list-style-type: none"> <li>- Read-Only Domain Controller (RODC) chỉ cho phép chứa bản sao của Database của AD DS từ các máy Fully Writable Domain Controller</li> <li>- Set up đơn giản và chi phí thấp hơn.</li> <li>- Có thể triển khai ở một vị trí không</li> </ul>

không quá bảo mật.

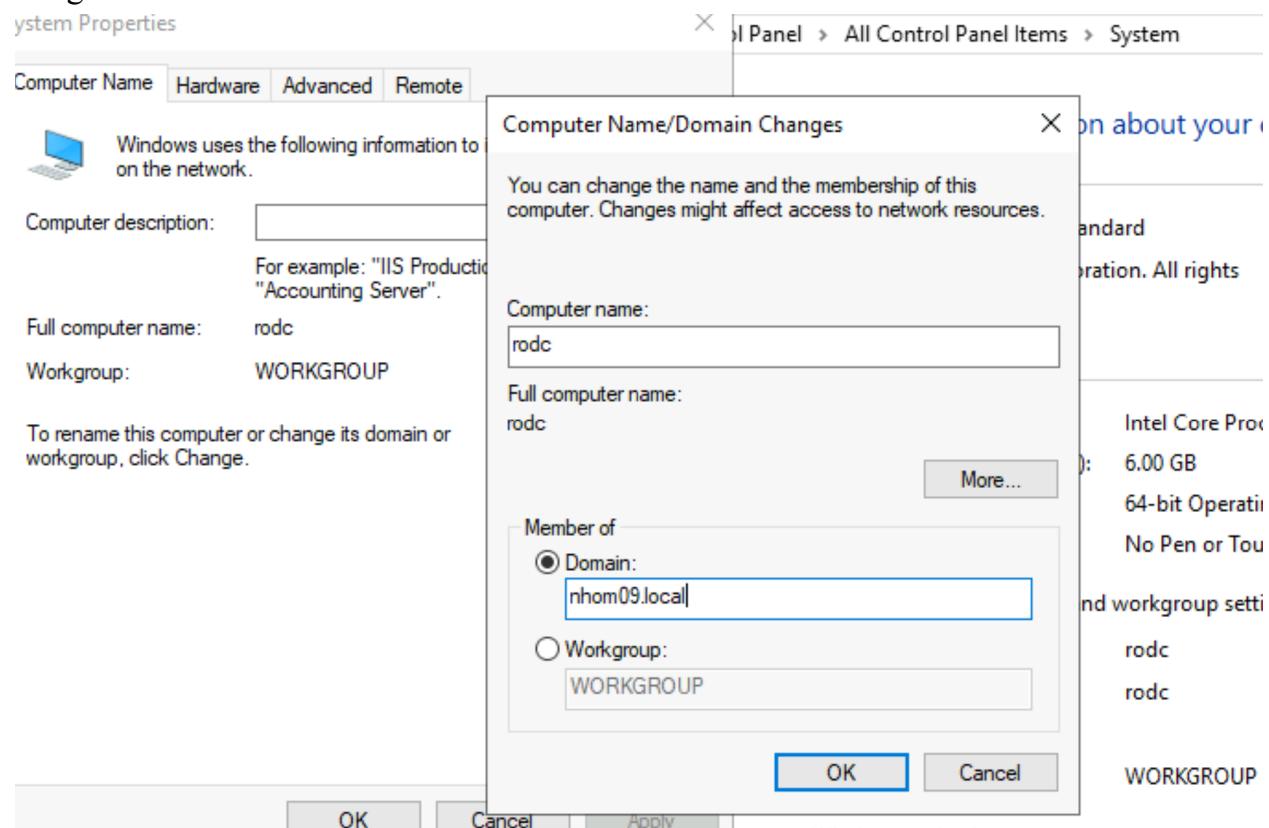
quá bảo mật.

=> Có tính bảo mật cao hơn.

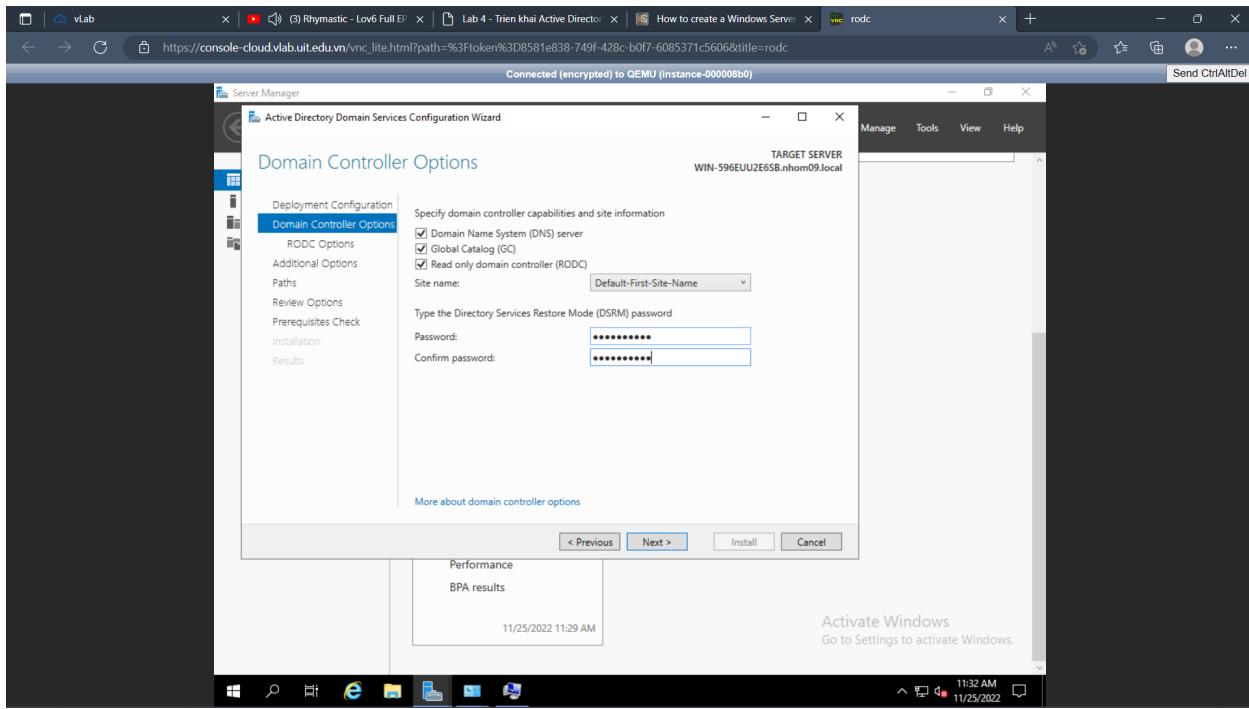
## Yêu cầu 4.2 Sinh viên triển khai mô hình Read-Only Domain Controller theo yêu cầu bên dưới.

### Các bước thiết lập.

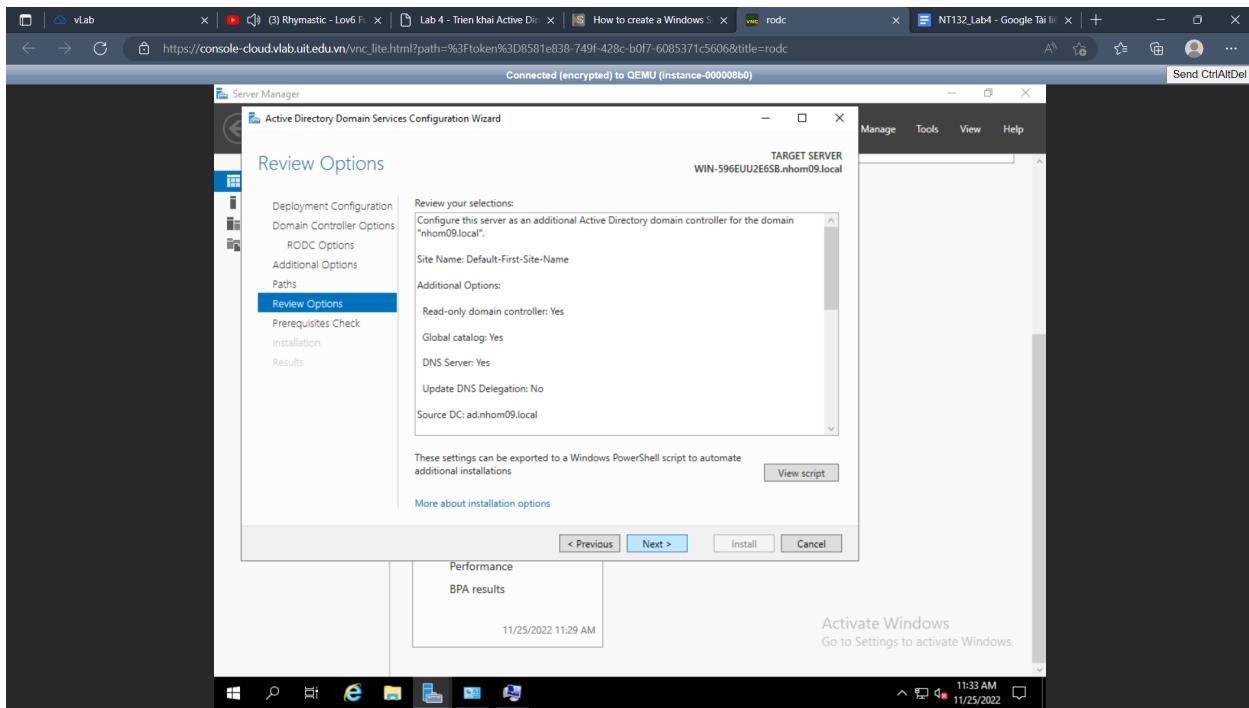
Ta thực hiện add máy RODC vào domain với tài khoản admin, đồng thời đổi tên cho máy trong domain:



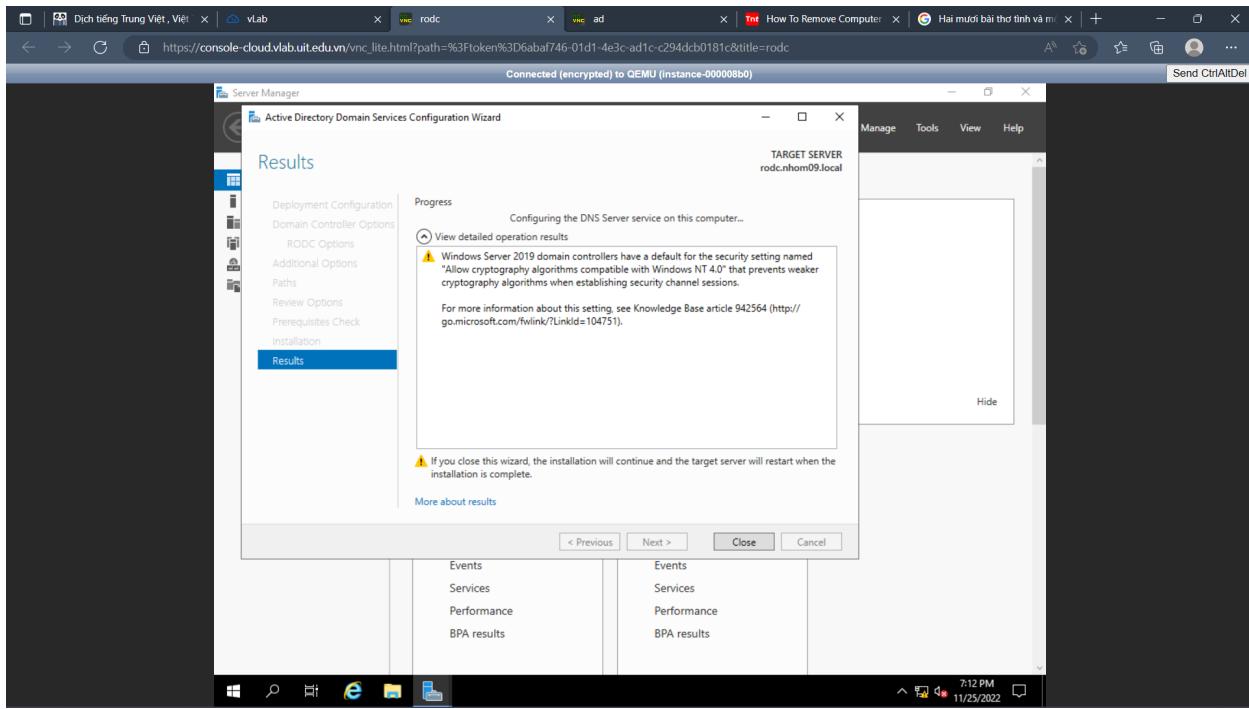
Sau đó thực hiện Add roles and features. Ta sẽ add Active Directory tương tự với những phần trước đó. Riêng ở phần Domain Controller Options, ta sẽ tick thêm vào ô Read only domain controller như hình dưới.



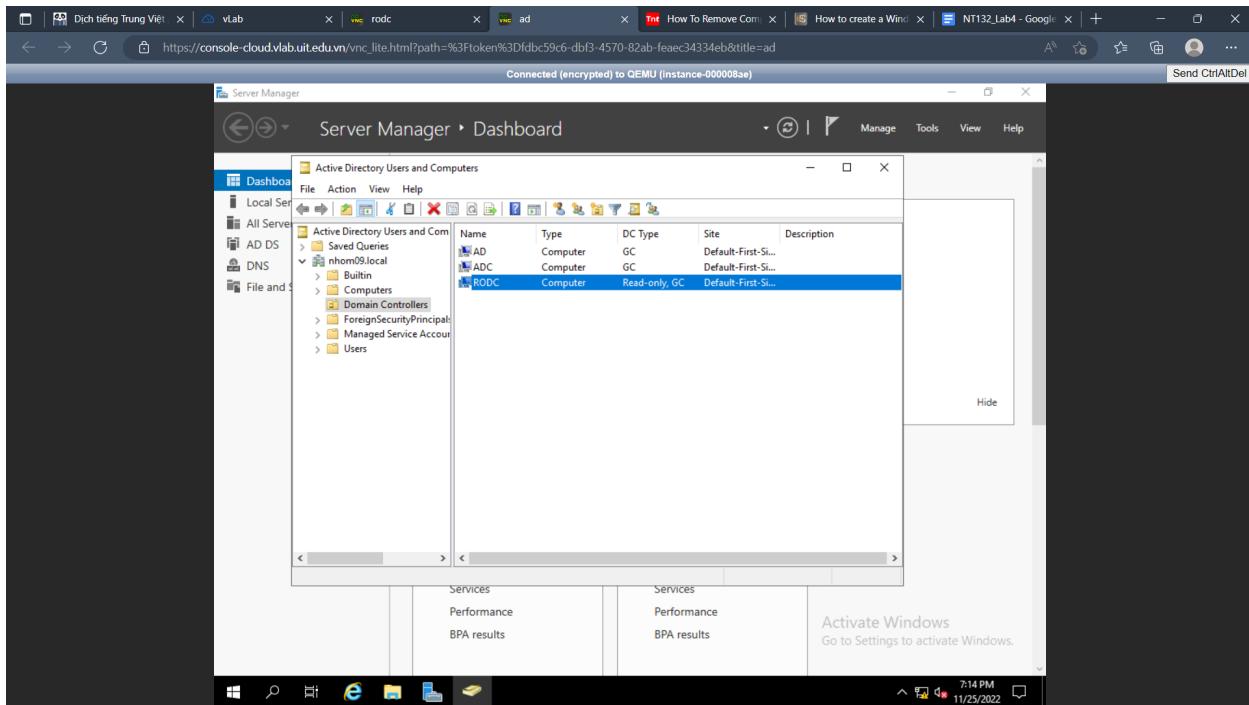
Các phần còn lại tương tự, có thể thấy trong phần review option bên dưới.



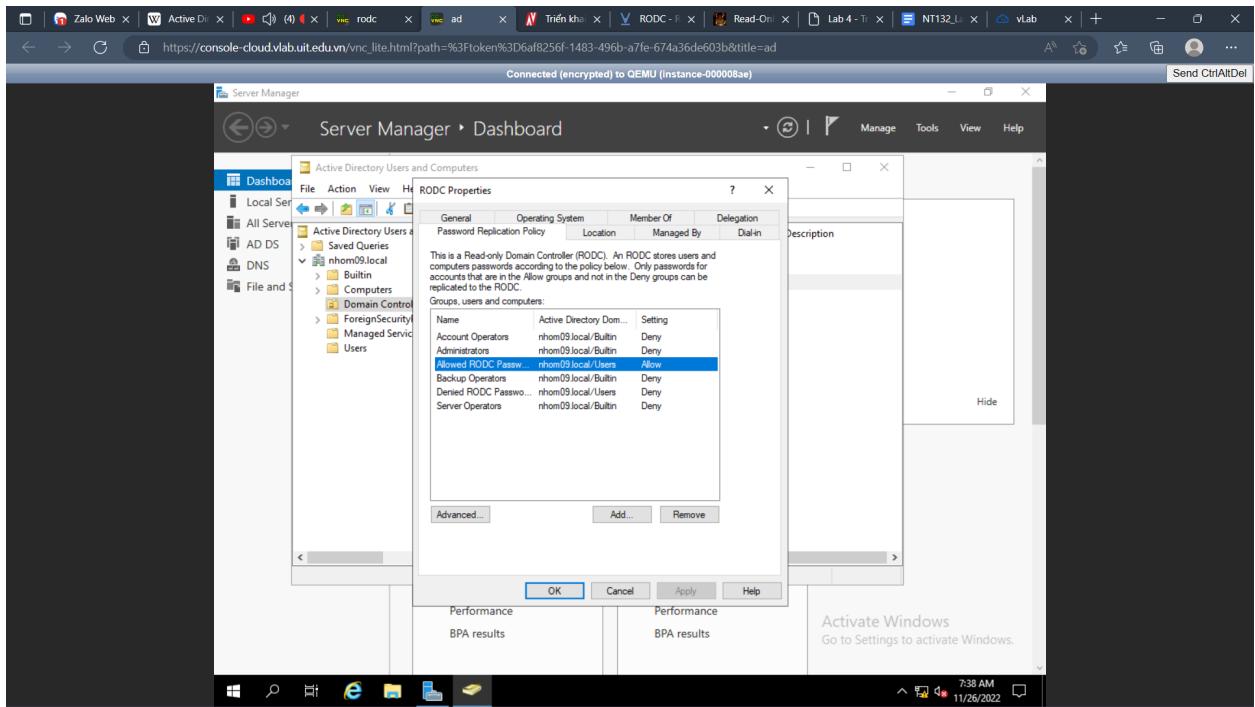
Sau đó ta hoàn thành việc cài đặt.



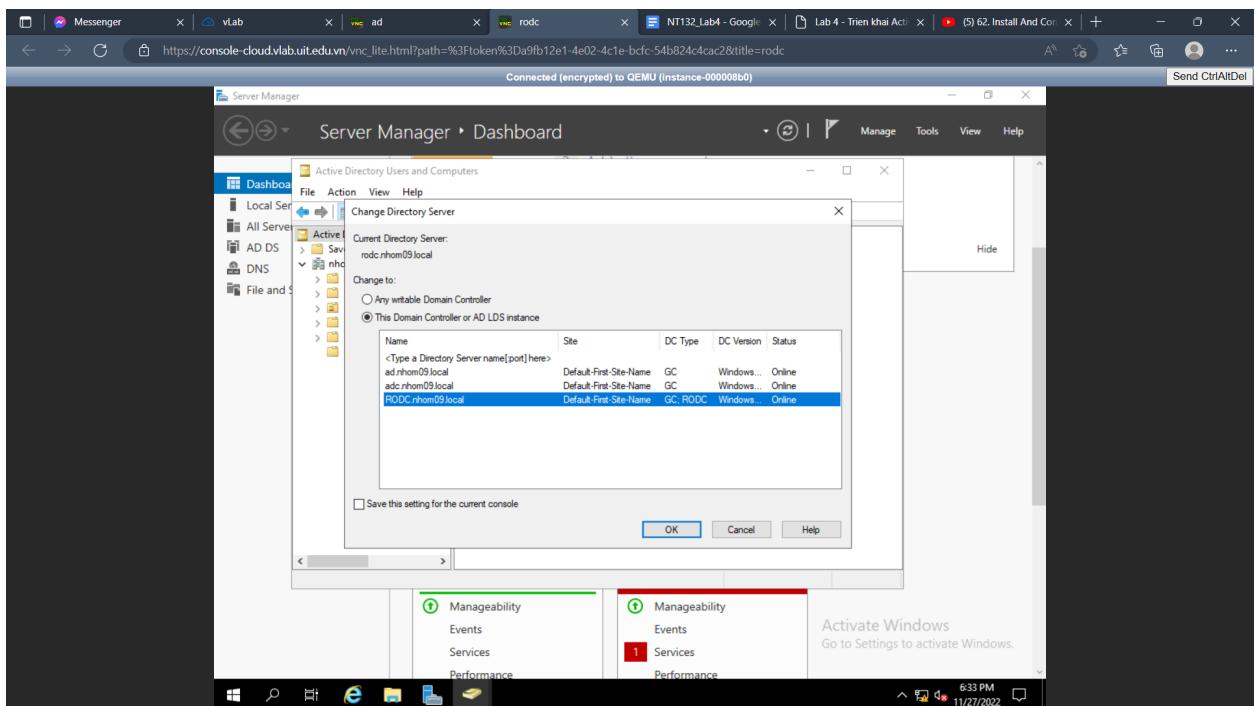
Sau khi cài đặt xong, ta có thể thấy được trong phần Domain Controller xuất hiện máy RODC, ở DC Type sẽ khác với các DC khác, hiển thị chỉ chế độ Read only.



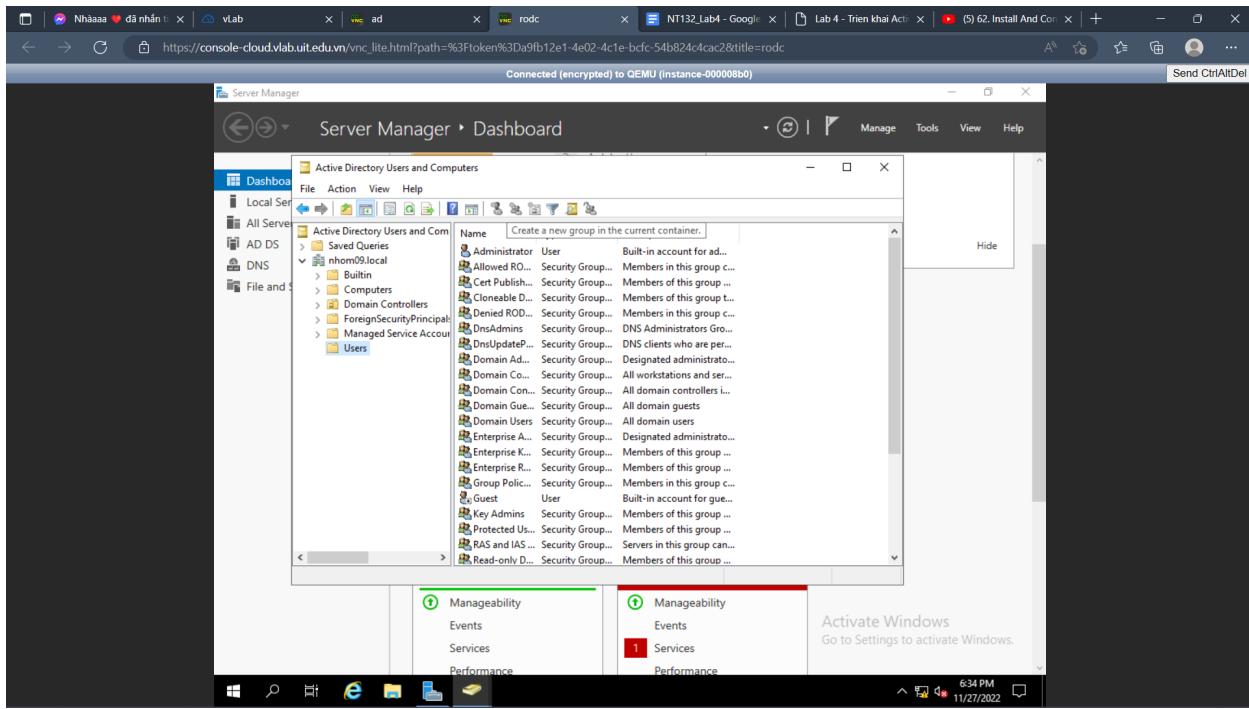
Trong properties của RODC, ta có thể thấy 2 group allow và deny password, phân ra các user nào RODC có quyền xác thực.



Ta sang máy RODC, vào Tool -> Active Directories Users and Computers, chuột phải vào cây thư mục và chọn change domain server sang RODC.

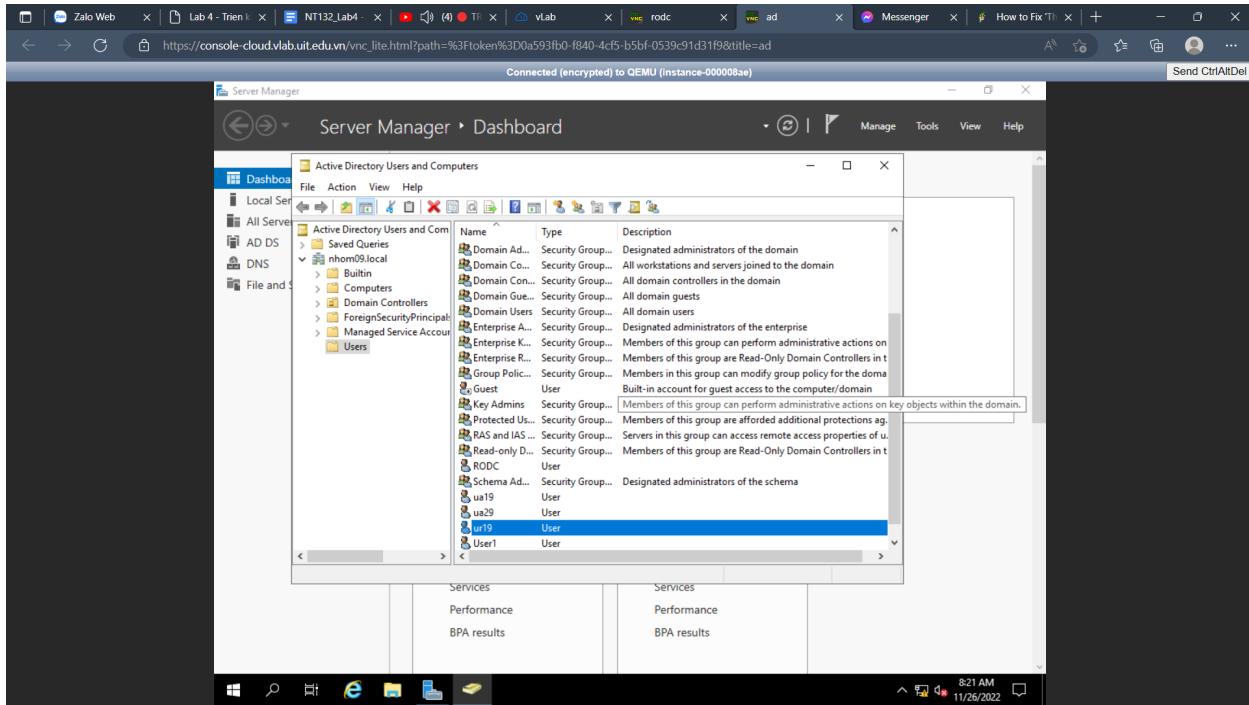


Khi đó, domain của chúng ta ở chế độ Read Only, các mục thay đổi đều không thể thực hiện (hiện màu xám.)

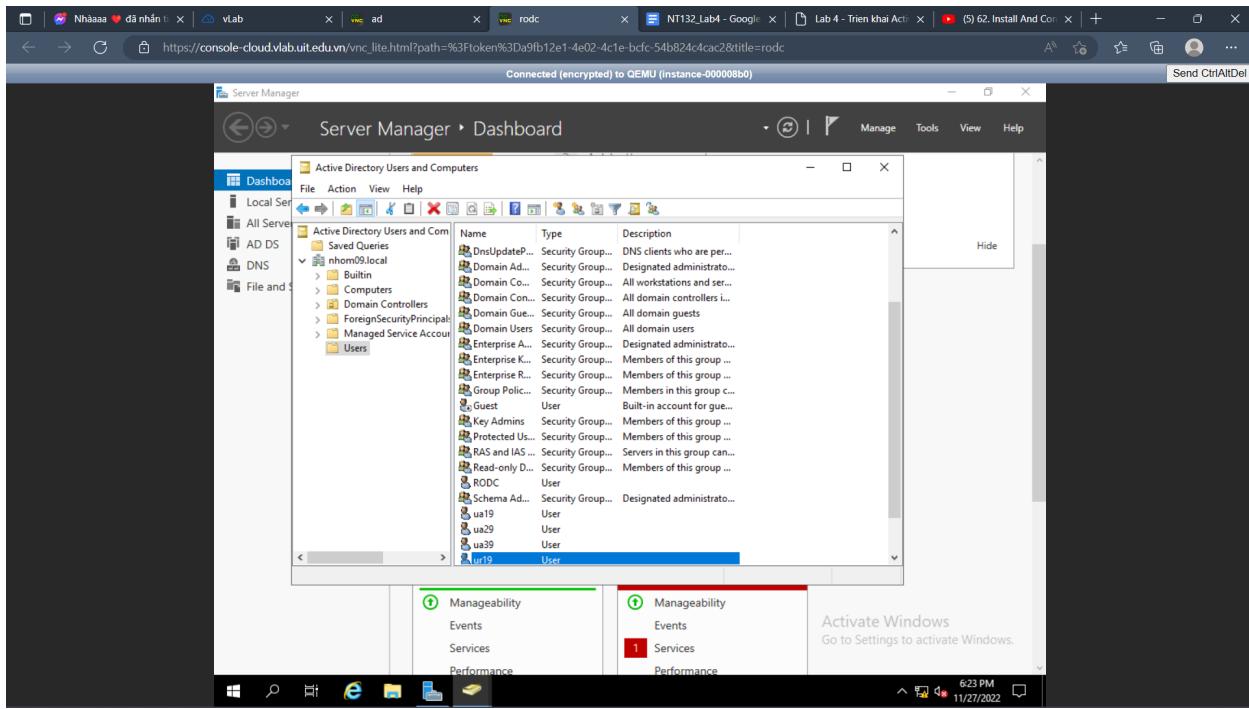


Thực hiện các công việc sau và kiểm tra kết quả (X là số thứ tự nhóm)

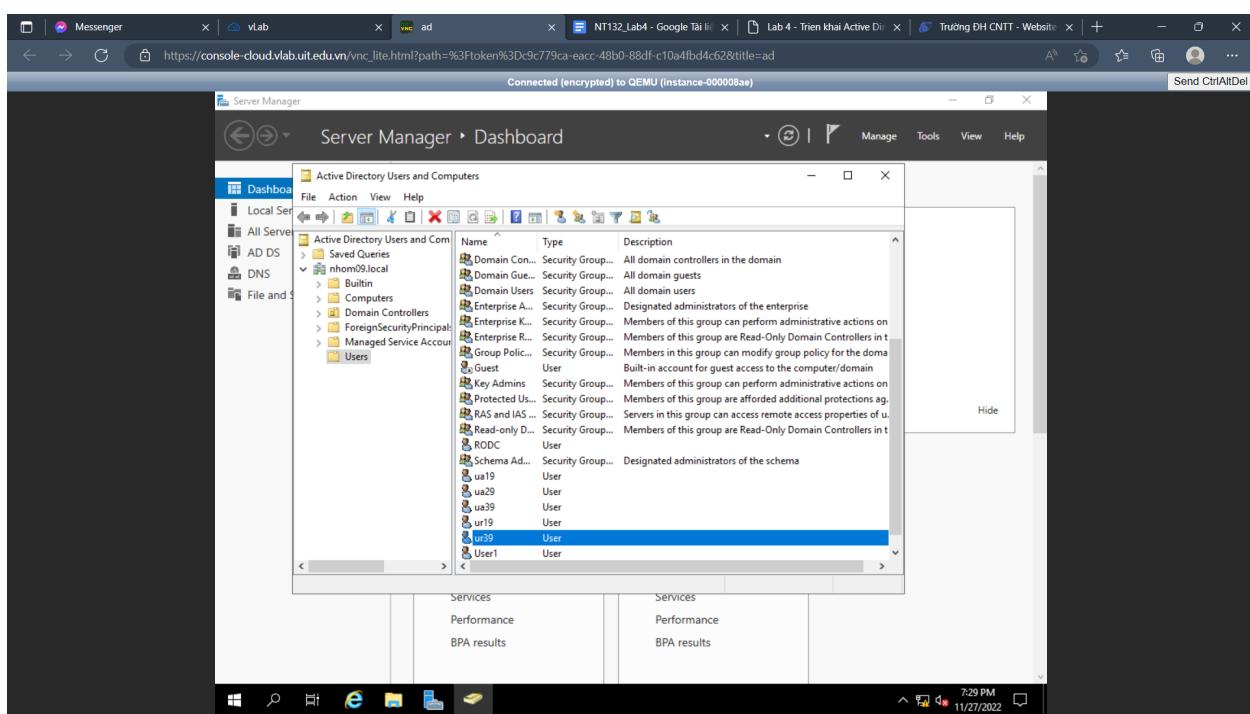
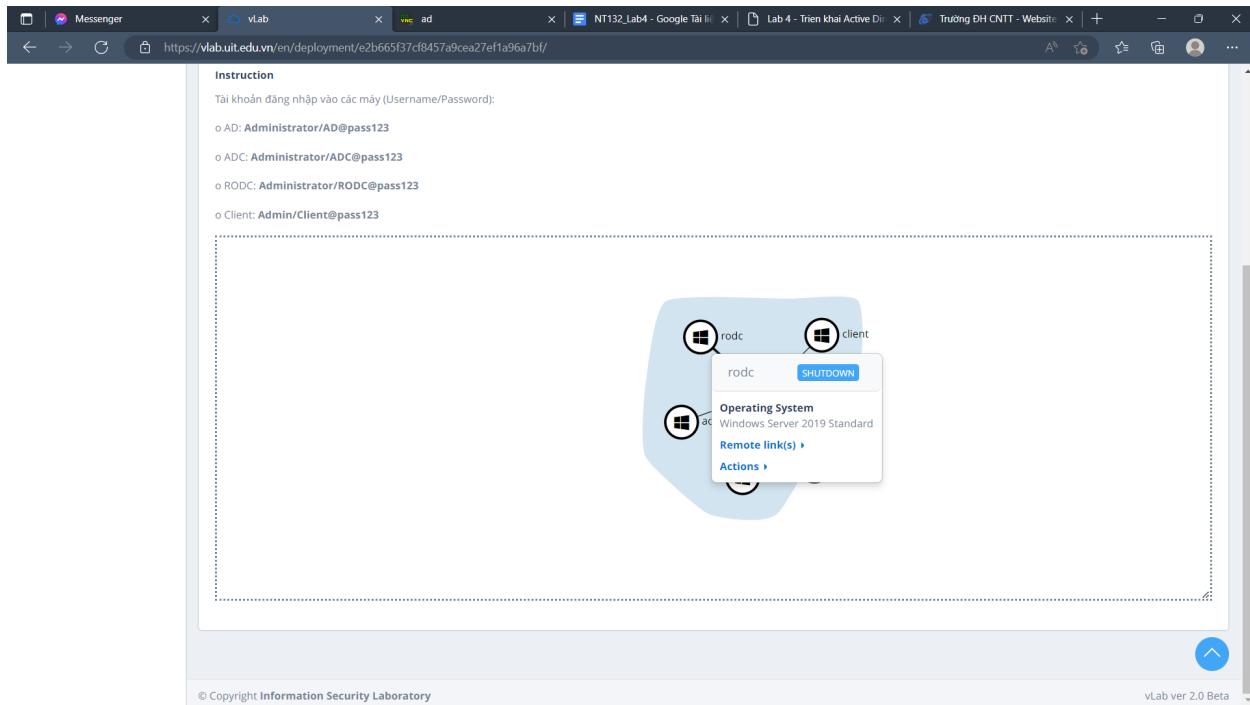
- Tạo user ur1X trên Primary DC. Kiểm tra thông tin user này trên Read-Only DC.  
Tạo ur19 trên máy AD.

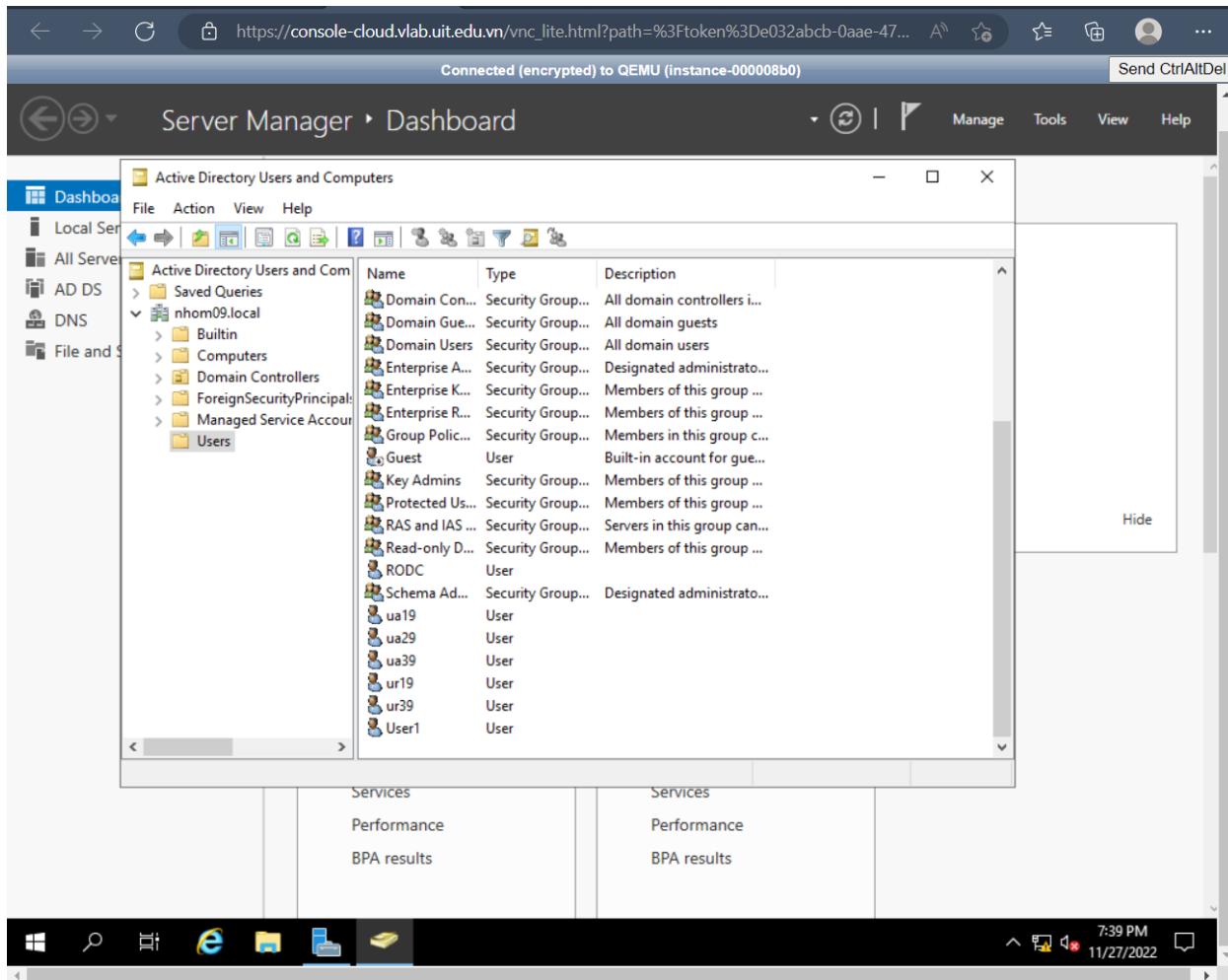


Có thể kiểm tra thông tin ur19 trên máy RODC:



- Tạo user ur2X trên Read-Only DC. Kiểm tra thông tin user này trên Primary DC.  
=> Không tạo được ur29 trên RODC do domain này là domain Read only, vì vậy không thể ghi và thay đổi dữ liệu.
- 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 và tạo ur39





- Tắt máy Primary DC, login ur2X trên máy Client. Giải thích kết quả.  
=> Không thể tạo được ur29.

- Tắt máy Read-Only DC, login ur3X trên máy Client. Giải thích kết quả.  
Khi tắt máy RODC thì vẫn có thể login ur39 trên máy client vì vẫn còn domain controller là máy AD đang chạy.

