

# 4

Lab

## Triển khai Active Directory trên Windows Server

Setting up Active Directory in Windows Server

**Thực hành môn Quản trị mạng và hệ thống**

GVTH: Đỗ Hoàng Hiến

**Lưu hành nội bộ**

## A. TỔNG QUAN

### 1. Mục tiêu

- Xây dựng mô hình Workgroup chia sẻ file.
- Xây dựng mô hình Domain với Active Directory (AD).
- Hiểu được sự khác nhau giữa 2 mô hình Workgroup và Domain.
- Triển khai Additional Domain Controller (ADC) và Read-Only Domain Controller (RODC) trong mô hình sử dụng Active Directory.
- Hiểu được sự khác nhau ADC và RODC trong mô hình sử dụng Active Directory.

### 2. Môi trường & công cụ

Sinh viên cần chuẩn bị trước máy tính với môi trường thực hành gồm 3 máy:

- 02 máy sử dụng Windows Server 2016/2019.

- 01 máy sử dụng Windows 7/8/10.

**Ghi chú:** Các máy trên có thể tạo trên phần mềm VMWare hoặc Virtual Box.

## B. THỰC HÀNH

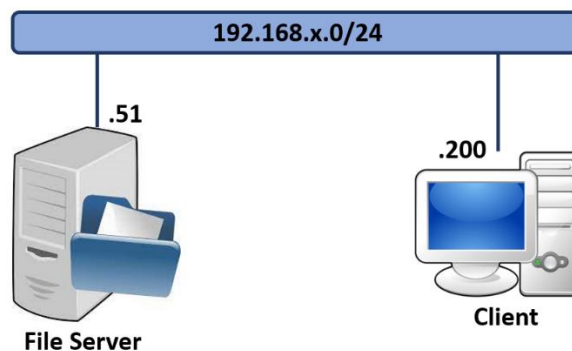
## 1. Xây dựng mô hình Workgroup

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

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

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

Mô hình cần xây dựng:

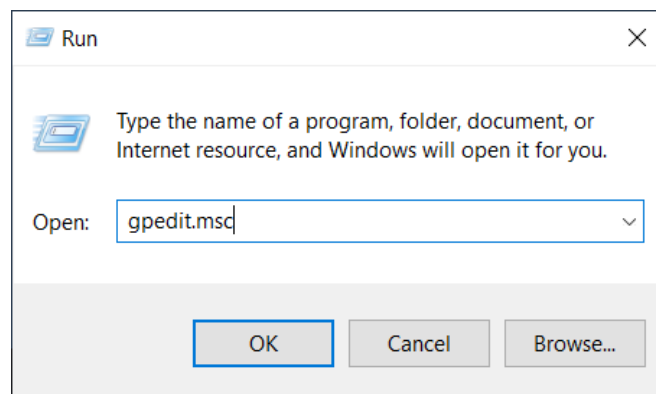


Thông tin các máy:

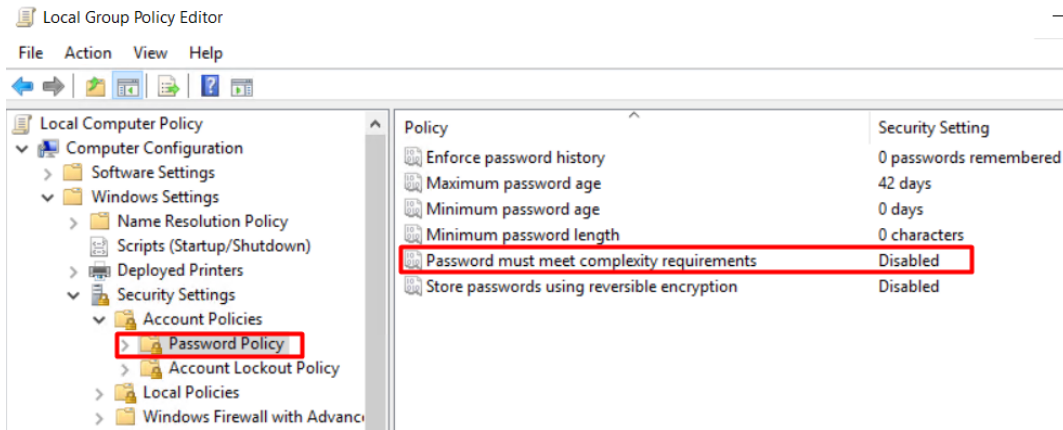
Tên máy	Hệ điều hành	Địa chỉ IP
File Server	Windows Server 2016	192.168.x.51/24
Client	Windows 7/8/10	192.168.x.200/24

Sinh viên sử dụng mạng **192.168.x.0/24**, trong đó **x** là số thứ tự nhóm đã đăng ký.

- **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 **nhomX** có mật khẩu là **123**.

**Add a user**

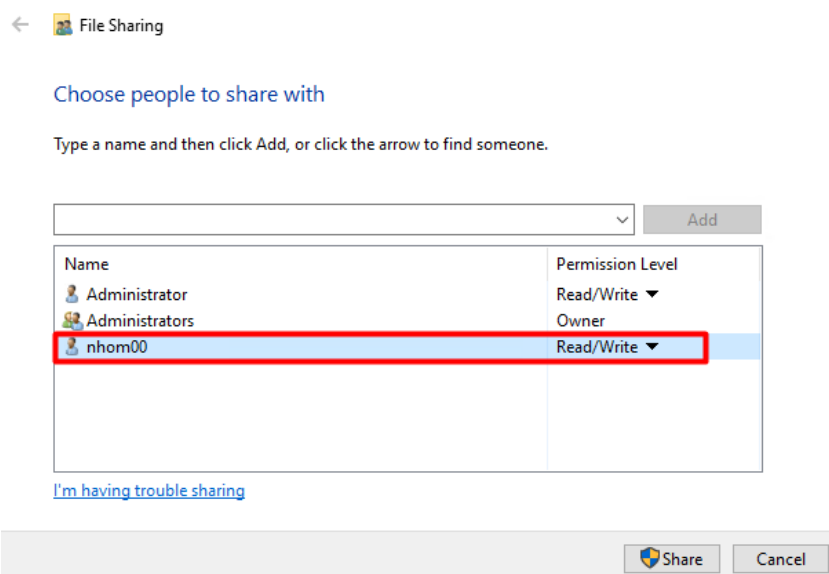
Choose a password that will be easy for you to remember but hard for others to guess. If you forget, we'll show the hint.

User name:

Password:

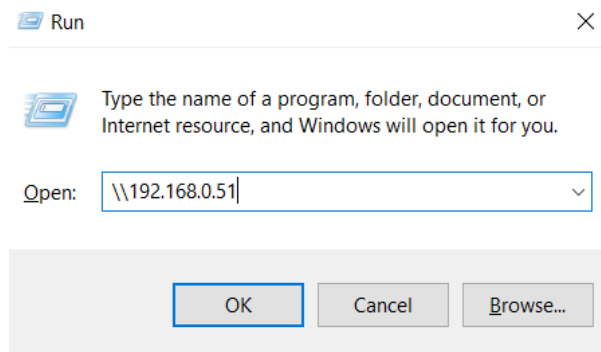
Reenter password:

- **Bước 3:** Trên ổ đĩa **C:\** của File Server, tạo 1 thư mục **folderX** (**X** là thứ tự nhóm dạng 2 chữ số) để chia sẻ dữ liệu.
- **Bước 4:** Nhấp chuột phải vào tên thư mục **folderX**, chọn **Share with > Specific people...** Thực hiện phân quyền chia sẻ trên thư mục này để user **nhomX** có quyền Read/Write.



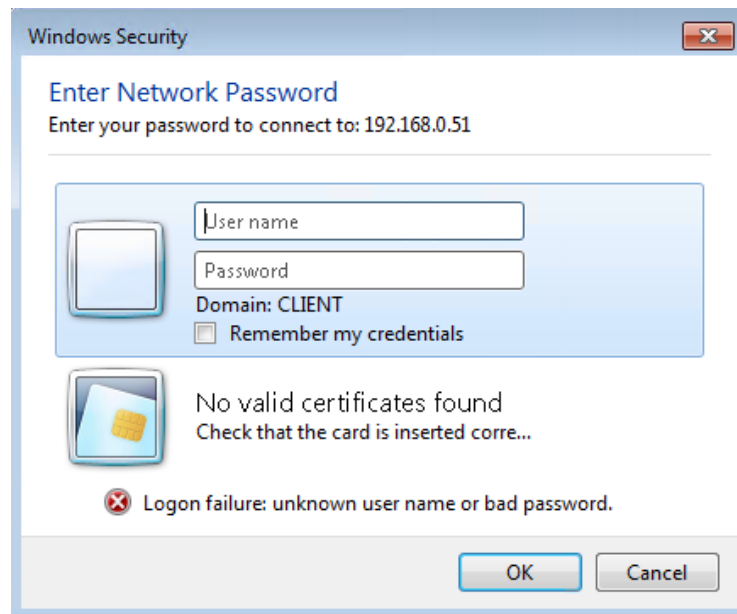
Lưu ý: nên tạm thời tắt Firewall trên File Server trước khi kết nối ở Bước 5.

- **Bước 5:** Từ máy Client, kết nối vào máy chủ File Server. Vào **Run**, gõ địa chỉ IP của máy File Server với cú pháp như bên dưới.

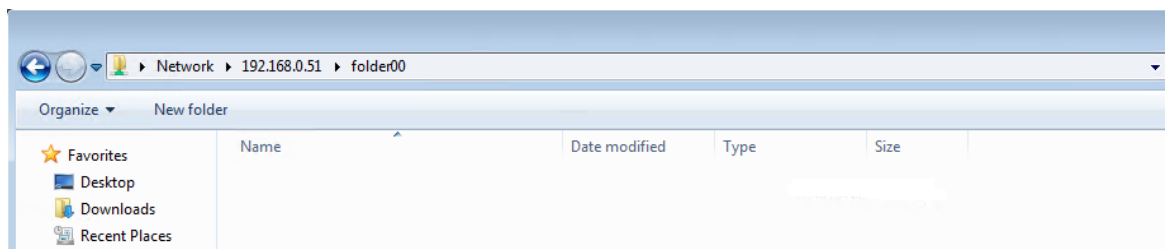


- **Bước 6:** Nhập user xác thực để truy cập vào File Server trong 2 trường hợp:
  - Sử dụng tài khoản của máy Client.
  - Sử dụng tài khoản của máy File Server (user nhómX đã tạo ở Bước 2).

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



- **Bước 7:** Sau khi truy cập thành công, trên máy Client tạo 1 tập tin tùy ý trong thư mục **folderX**. **Báo cáo và giải thích kết quả thực hiện.**



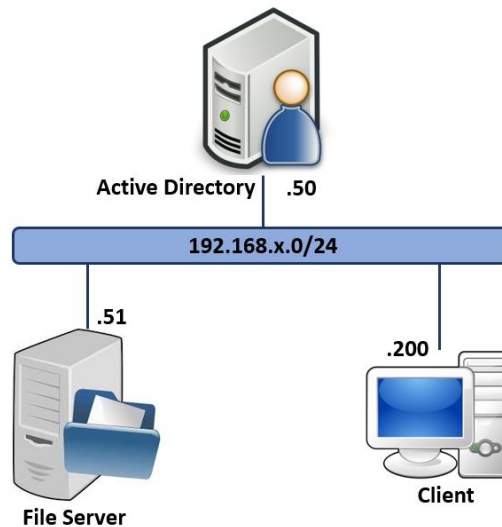
## 2. Triển khai Active Directory và xây dựng mô hình Domain

**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?

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

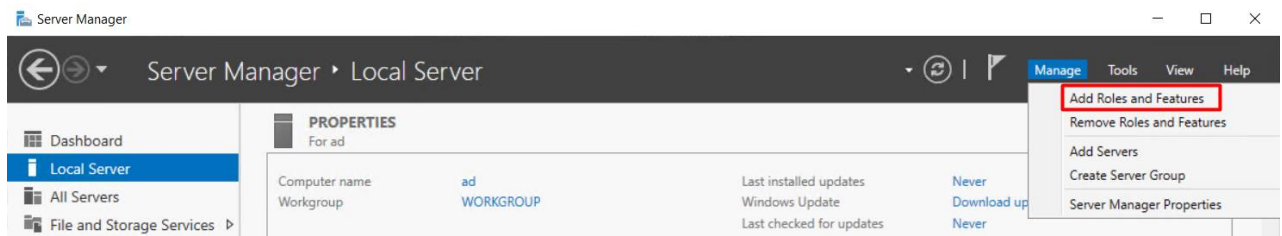
Mô hình cần xây dựng:



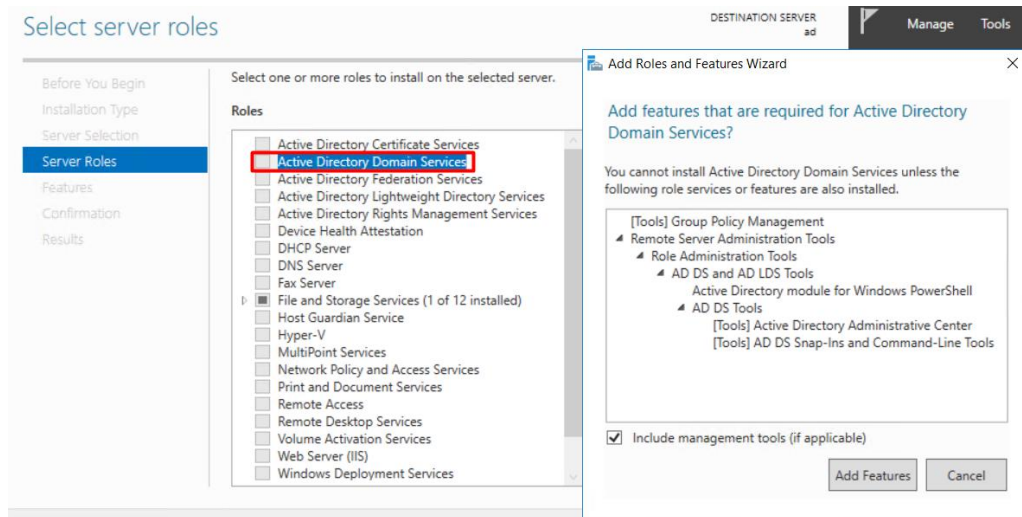
Thông tin các máy:

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
File Server	Windows Server 2016	192.168.x.51/24	192.168.x.50
Active Directory	Windows Server 2016	192.168.x.50/24	192.168.x.50
Client	Windows 7/8/10	192.168.x.200/24	192.168.x.50

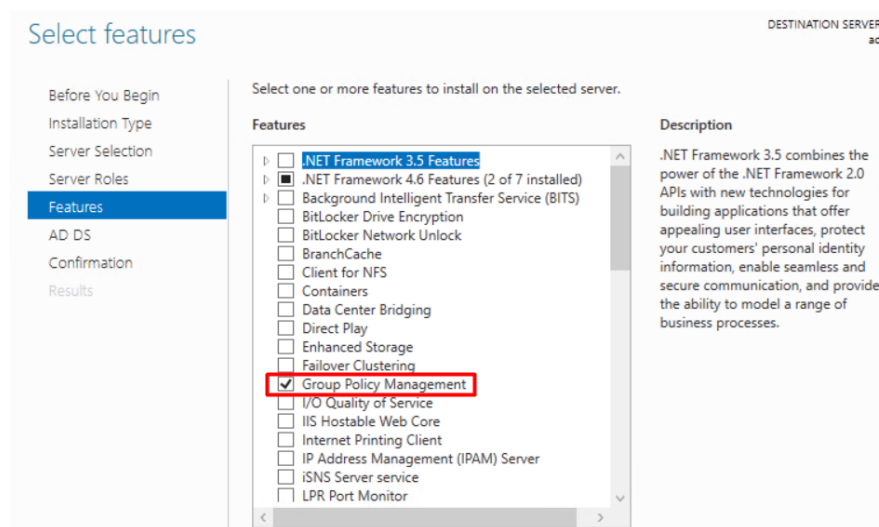
- **Bước 1:** Cài đặt Active Directory Domain Service trên máy Active Directory
- Vào **Server Manager > Manage > Add Roles and Features**



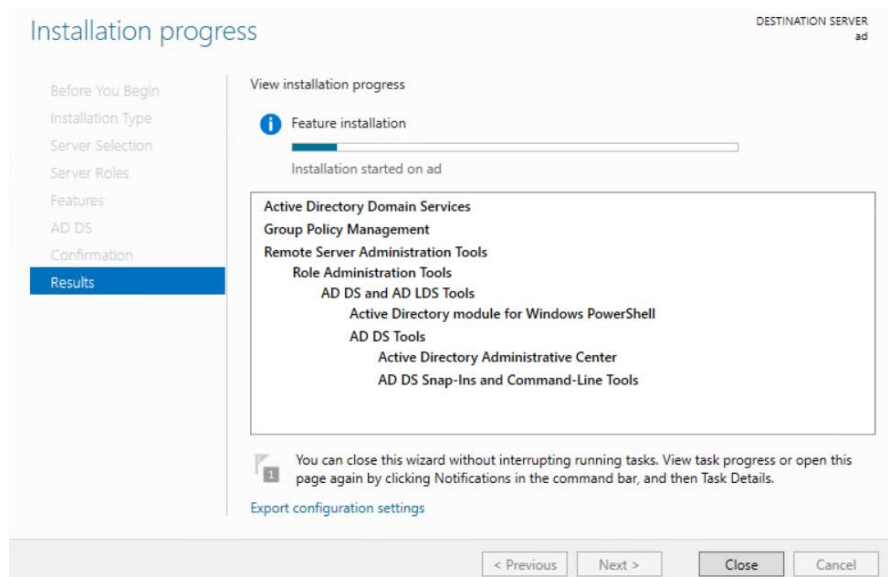
- Chọn **Next** tại các bước **Before You Begin, Installation Type, Server Selection**
- Tại bước **Server Roles**, chọn **Active Directory Domain Services**.



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

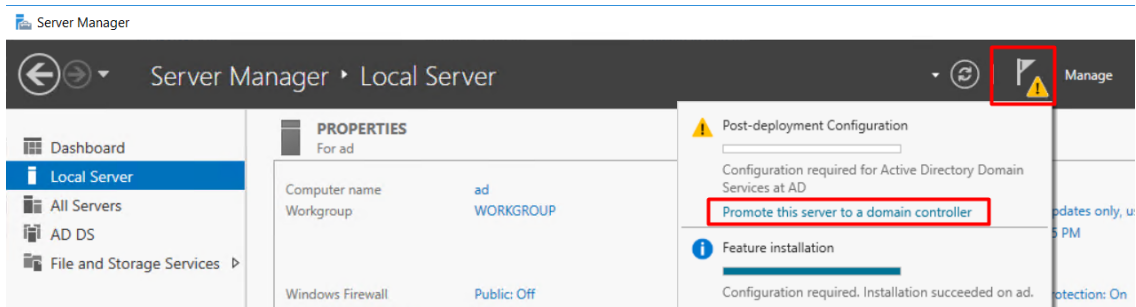


- Ở bước **AD DS**, chọn **Next**.
- Ở bước **Confirmation**, xác nhận lại thông tin và chọn **Install**.
- Chờ quá trình cài đặt hoàn thành và chọn **Close** để kết thúc.





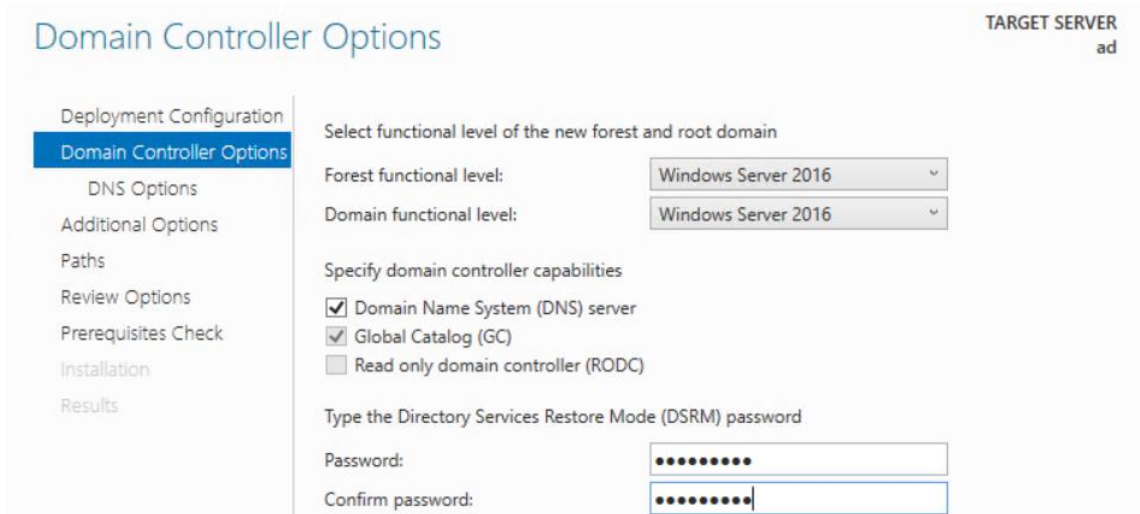
- **Bước 2:** Nâng cấp máy chủ Active Directory lên Domain Controller
- Vào **Server Manager** sẽ thấy biểu tượng cảnh báo, nhấn vào và chọn **Promote this server to a domain controller**.



- Chọn **Add new forest** và gõ domain **nhomX.local** vào mục Root domain.



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



- Thiết lập NetBIOS domain name





- Giữ nguyên các tùy chỉnh mặc định ở mục **Paths**

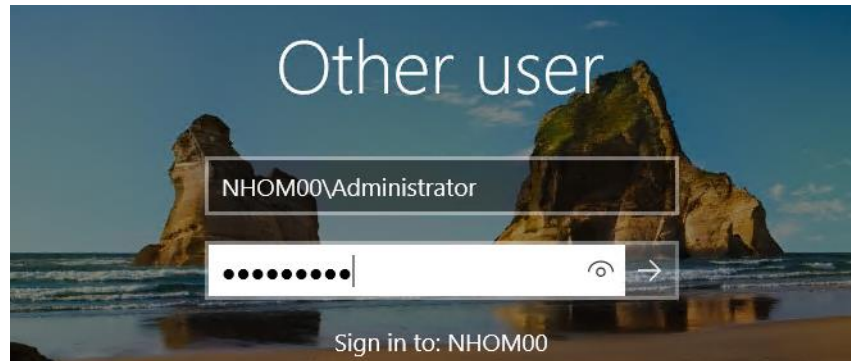
- Thực hiện bước **Prerequisites Check** hoàn thành, sau đó chọn **Install** và chờ quá trình nâng cấp hoàn tất.

Sau khi hoàn tất quá trình này, máy chủ Active Directory sẽ khởi động lại và hoàn tất quá trình nâng cấp thành Domain Controller.

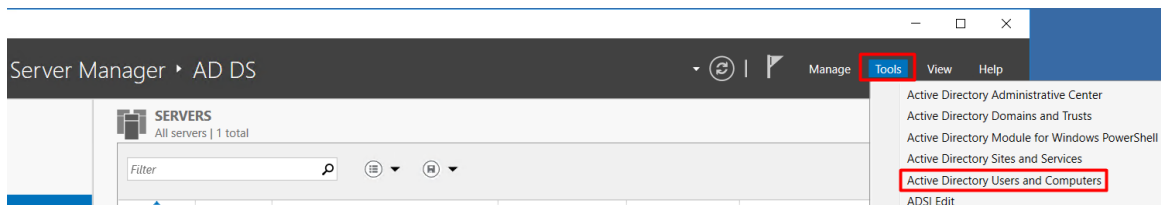
### • Bước 3: Tạo user trong domain

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.

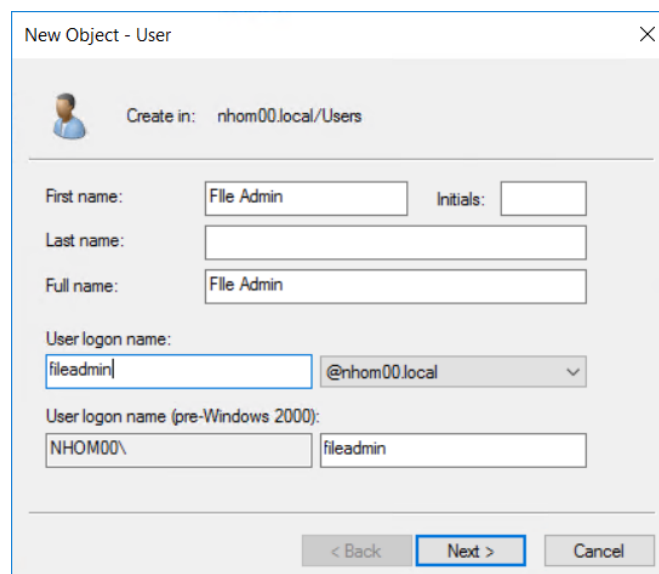
- Đăng nhập vào máy chủ Active Directory với tài khoản **NHOMX\Administrator** (tài khoản trong domain).



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



- Trong **nhomX.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**.

### • Bước 4: Thêm File Server vào domain đã tạo.

**Lưu ý:** Để thêm một máy tính vào domain, cần chú ý DNS của máy tính đó phải trỏ về DNS Server quản lý Domain, ở đây là IP của máy Active Directory.

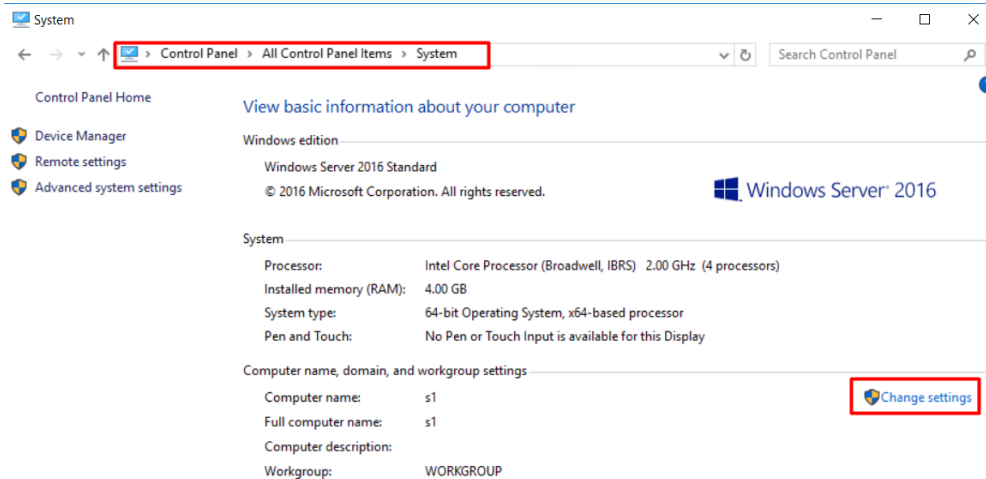
- Trên máy File Server, kiểm tra kết nối đến domain.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

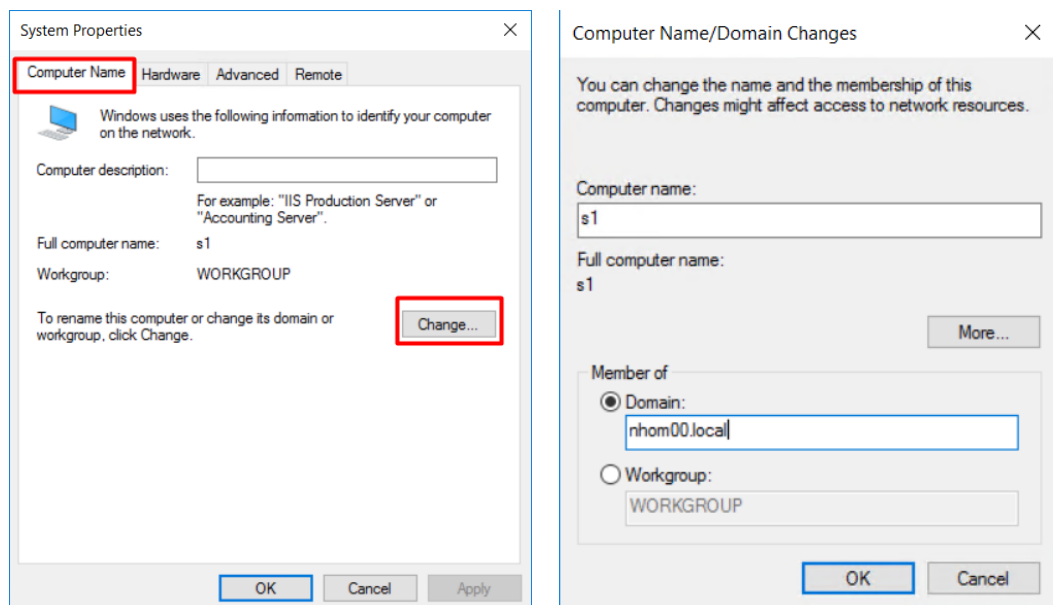
C:\Users\Administrator>ping nhom00.local

Pinging nhom00.local [192.168.0.50] with 32 bytes of data:
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
Reply from 192.168.0.50: bytes=32 time=1ms TTL=128
```

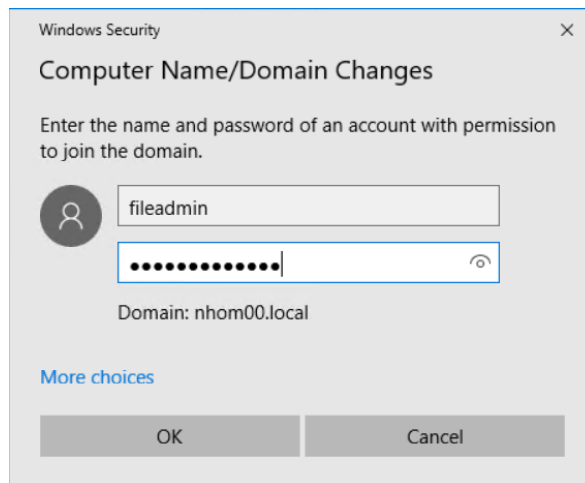
- Vào mục **System** trong **Control Panel**, chọn **Change settings**.



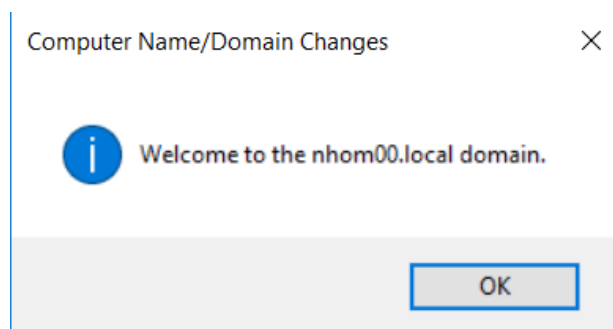
- Trong cửa sổ **System Properties**, tab **Computer Name**, chọn **Change**. Sau đó tại trường **Member of**, chọn **Domain** và nhập tên domain muốn tham gia.



- 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.**

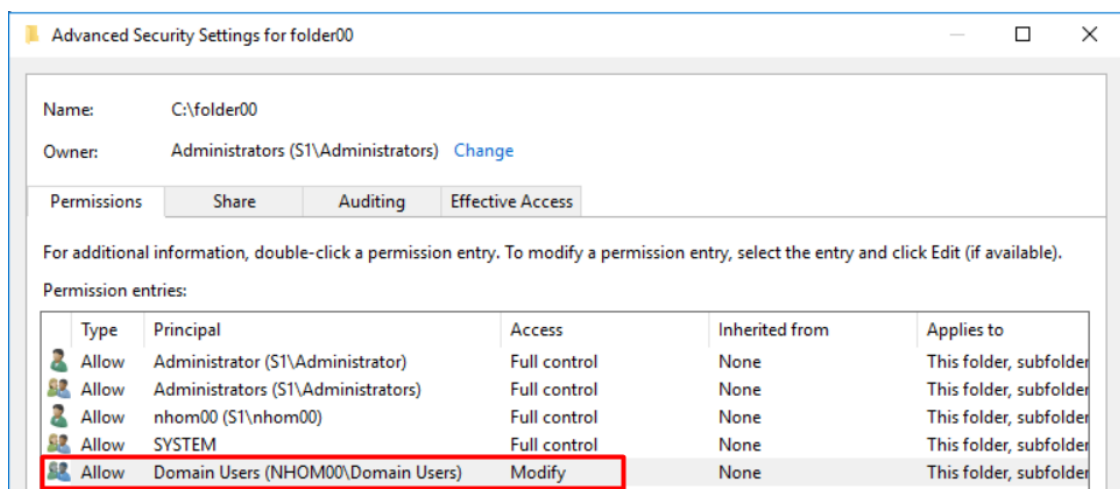
Thực hiện quá trình tương tự Bước 4 để thêm máy client vào domain.

• **Bước 6: Phân quyền và chia sẻ file từ File Server**

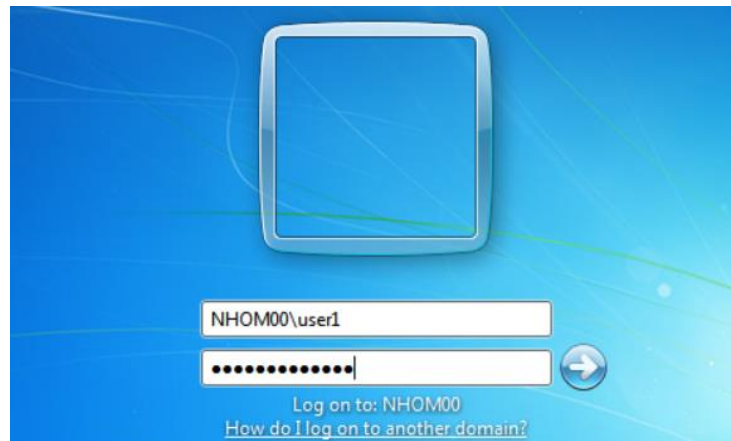
- Đăng nhập lại vào File Server và thực hiện phân quyền lại **folderX** của **File Server**.

*Lưu ý: việc phân quyền có thể yêu cầu cần xác thực với 1 tài khoản user có quyền administrator trong domain (ví dụ administrator của AD).*

Sinh viên phân quyền cho nhóm **Domain Users** trong domain như bên dưới.



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

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

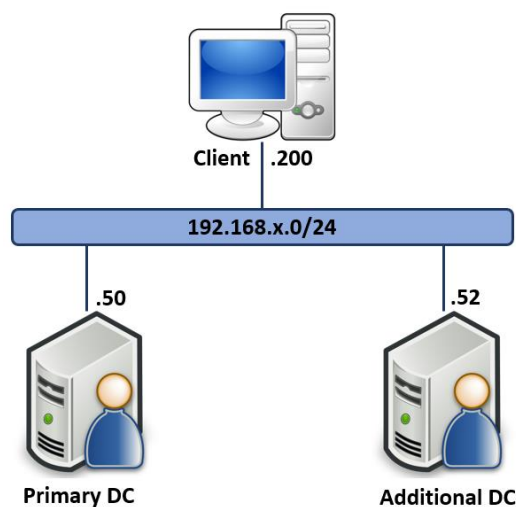
### 3. Xây dựng mô hình Additional Domain Controller cho dịch vụ Active Directory

**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?

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

**Mô hình cần xây dựng:**



Thông tin các máy:

Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7/8/10	192.168.x.200/24	192.168.x.50 192.168.x.52
Primary DC	Windows Server 2016	192.168.x.50/24	192.168.x.50 192.168.x.52
Additional DC	Windows Server 2016	192.168.x.52/24	192.168.x.52 192.168.x.50

- **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.

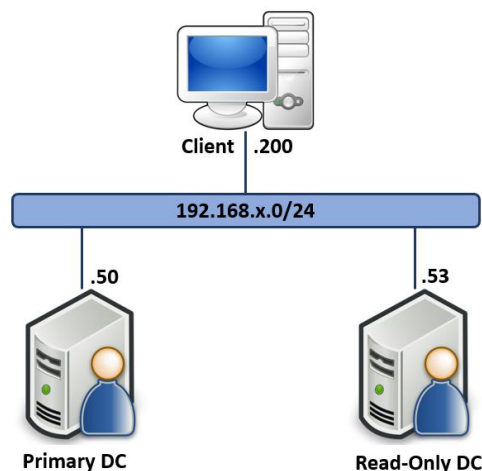
#### 4. Xây dựng mô hình Read-only Domain Controller

**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?

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

Mô hình cần xây dựng:



Thông tin các máy



Tên máy	Hệ điều hành	Địa chỉ IP	DNS server
Client	Windows 7/8/10	192.168.x.200/24	192.168.x.53 192.168.x.50
Primary DC	Windows Server 2016	192.168.x.50/24	192.168.x.50 192.168.x.53
Read-Only DC	Windows Server 2016	192.168.x.53/24	192.168.x.53 192.168.x.50

- **Bước 3:** Triển khai mô hình Read-Only Domain Controller (RODC) với thông tin như trên.
- **Bước 4:** 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.

### C. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên thực hiện bài thực hành theo **nhóm**. Sinh viên thực hiện theo quy trình được hướng dẫn.
- Sinh viên có thể chọn 1 trong 2 hình thức để báo cáo:
  - o Hình thức 1: Báo cáo trên lớp trong buổi thực hành, GVTH sẽ chấm điểm trực tiếp. Dựa trên kết quả sinh viên thực hiện, có thể không cần nộp báo cáo.
  - o Hình thức 2: Nộp file báo cáo **.pdf** trên moodle. Báo cáo cần mô tả đầy đủ và có hình ảnh minh chứng các lệnh được thực hiện/các điều chỉnh trong file cấu hình và kết quả kiểm tra ở từng bước cài đặt, cấu hình.

Tên file: **[NT132.M11.ANTT.2]-Lab4\_NhomX\_MSSV1-MSSV2-MSSV3.pdf**

### D. TÀI LIỆU THAM KHẢO

- [1] "Xây dựng Additional Domain Controller trên Windows Server 2016", <https://adminvietnam.org/xay-dung-additional-domain-controller-tren-windows-server-2016/1598/>
- [2] "Triển khai Read-Only Domain Controller trên Windows Server 2016", <https://adminvietnam.org/read-only-domain-controller-tren-windows-server-2016/1667/>

**HẾT**

*Chúc các bạn hoàn thành tốt!*