

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA CÔNG NGHỆ THÔNG TIN 1**

**Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ  
LINUX/UNIX**  
**BÁO CÁO BÀI THỰC HÀNH SỐ 1**

Họ và tên sinh viên:      Ninh Chí Hường

Mã số sinh viên:          B20DCAT094

Họ và tên giảng viên:      TS. Đinh Trường Duy

Hà Nội 9/2022 (tháng/năm)

## Table of Contents

<b>I. Giới thiệu chung về bài thực hành</b>	<b>3</b>
<b>1.1 Mục đích</b>	<b>3</b>
<b>1.2 Yêu cầu</b>	<b>3</b>
<b>1.3 Cơ sở lý thuyết</b>	<b>3</b>
1.3.1 Kiến trúc chung của windows	3
1.3.2 Kiến trúc Windows NT:	4
1.3.3 Kiến trúc Windows server 2003:	5
1.3.3.1 Kiến trúc cơ bản:	5
1.3.3.2 Chi tiết kiến trúc Windows server 2003	6
<b>2 Tiến hành thực hiện</b>	<b>8</b>
<b>2.1 cài đặt hệ điều hành Windows Server 2019</b>	<b>9</b>
2.1.2 Trên VMWare Workstation	9
2.1.3 Trên máy ảo Windows Server 2019	12
<b>2.2 Nâng cấp Server thành Domain Controller</b>	<b>13</b>
2.2.1 Kiểm tra tên server	13
<b>2.2.2 Cài đặt static IP</b>	<b>14</b>
2.2.3 Cài đặt server role trong Server Manager	15
2.2.4 Nâng cấp Server thành Domain Controller	16

# I. Giới thiệu chung về bài thực hành

## 1.1 Mục đích

- tạo được một máy chủ Window Server với chức năng Domain .

## 1.2 Yêu cầu

- Sinh viên đã nắm được nội dung lý thuyết.
- Sinh viên về cơ bản biết cách sử dụng hệ điều hành Ubuntu.

## 1.3 Cơ sở lý thuyết

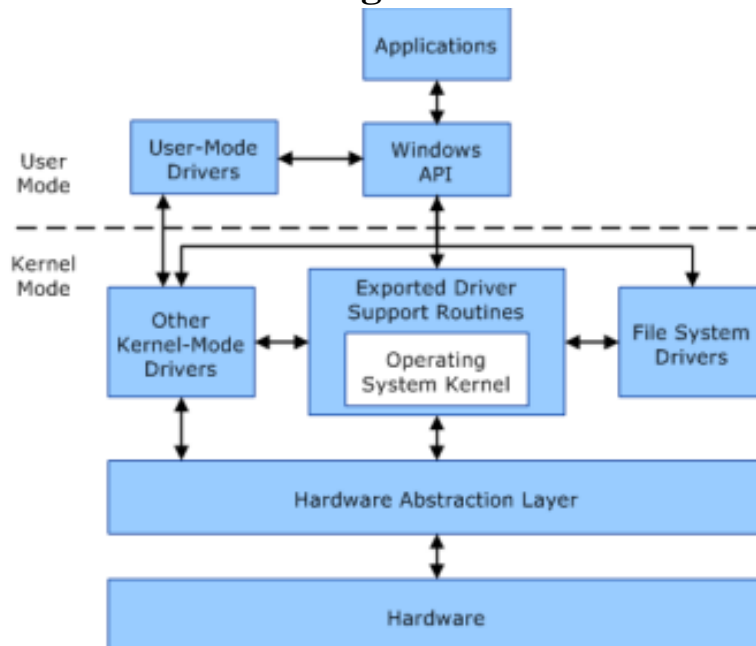
Kiến trúc của Windows server

Windows Server là một nhánh của hệ điều hành máy chủ được sản xuất bởi tập đoàn Microsoft. Phiên bản đầu tiên của Windows server là Windows server NT ra đời năm 1994, hiện tại đã có phiên bản Windows server 2019

Nhánh này bao gồm các hệ điều hành sau:

- Windows Server NT
- Windows 2000 Server
- Windows Server 2003
- Windows Server 2008
- Windows HPC Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019

### 1.3.1 Kiến trúc chung của windows



Hình 1.1: Kiến trúc chung của windows

Về cơ bản kiến trúc Windows gồm 2 mode: User mode (người sử dụng) và kernel mode (cốt lõi của hệ điều hành)

Người dùng tương tác với hệ thống thông qua các Applications

Kernel mode làm việc với hardware thông qua Hardware Abstraction Layer

### 1.3.2 Kiến trúc Windows NT:

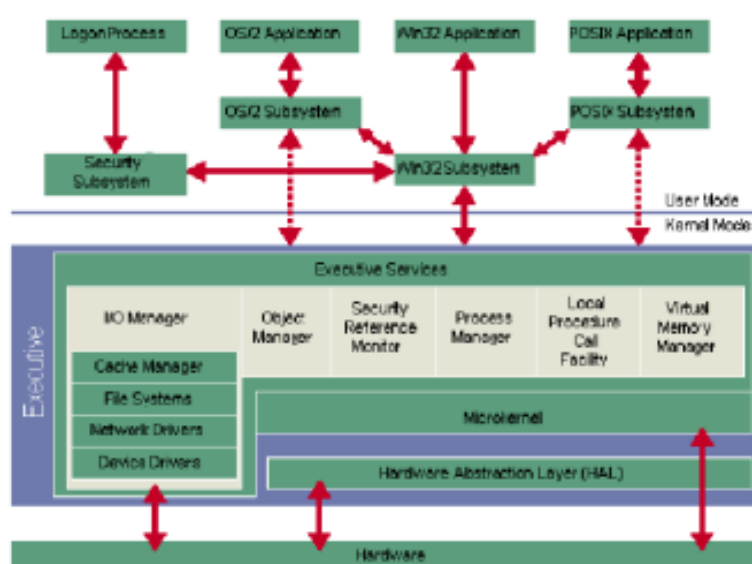
Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular).

Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của

Windows NT được trình bày trong hình 1.1. Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (nhân).

Trong Windows NT: Executive Services, Kernel và HAL chạy dưới chế độ Kernel.

Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user.

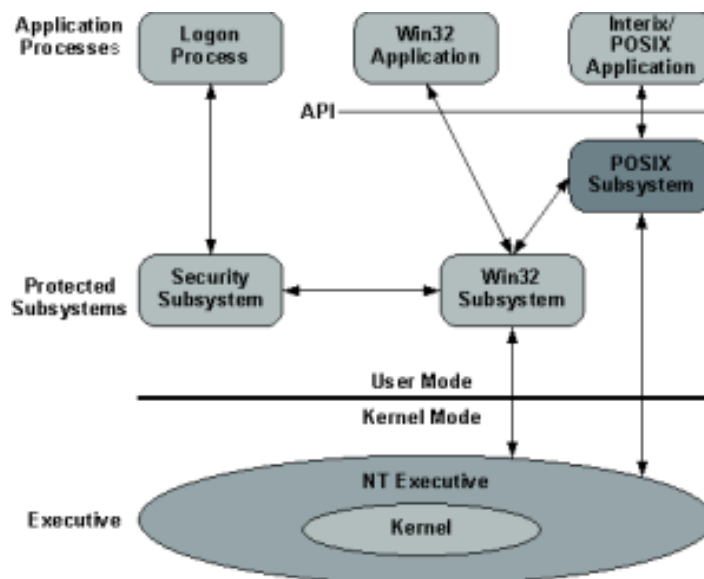


Hình 1.2 :Kiến trúc Windows NT

Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:

- Lớp phần cứng trừu tượng (Hardware Abstraction Layer - HAL): Là phần cứng máy tính mà Kernel có thể được ghi vào giao diện phần cứng ảo, thay vì vào phần cứng máy tính thực sự.
- Lớp Kernel: Cung cấp các chức năng cơ bản của hệ điều hành được sử dụng bởi các thành phần thực thi khác.
- Các thành phần Executive: Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như:
  - o Quản lý đối tượng (object manager)
  - o Bảo mật (security reference monitor)
  - o Quản lý tiến trình (process manager)
  - o Quản lý bộ nhớ ảo (virtual memory manager)
  - o Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

### 1.3.3 Kiến trúc Windows server 2003:



Hình 1.3 Kiến trúc windows server 2003

#### 1.3.3.1 Kiến trúc cơ bản:

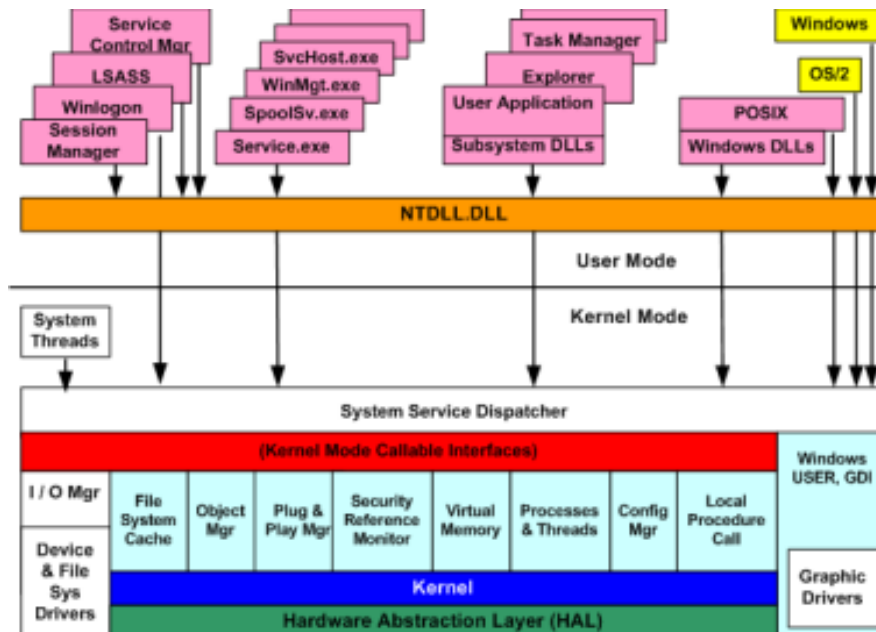
Cũng tương tự như kiến trúc cơ bản windows, kiến trúc Windows server 2003 gồm 2 mode: user mode và kernel mode.

- User mode bao gồm các application processes mà thường là các chương trình Windows (Windows program) và tập hợp các hệ thống con bảo vệ (protected subsystems)
- Kernel mode là chế độ đặc quyền trong đó các chương trình có thể truy cập trực tiếp đến bộ nhớ ảo. Nó bao gồm các không gian địa chỉ của tất cả các quá trình các chế độ người dùng và các ứng dụng phần cứng. Kernel mode còn được gọi là supervisor mode, protected mode. Kernel mode của Windows server 2003 bao gồm: Windows NT executive cũng như system kernel

Hệ điều hành Windows hỗ trợ các tính năng sau:

- Đa nhiệm.
- Tính linh hoạt để chọn một giao diện lập trình (user and kernel APIs).
- Một giao diện người dùng đồ họa (GUI) và một giao diện dòng lệnh cho người dùng và quản trị viên (The default UI is graphical.)
- Tích hợp kết nối mạng.( theo tiêu chuẩn TCP/IP)
- Quy trình dịch vụ hệ thống liên tục được gọi là "Windows Services" và các dịch vụ quản lý của Windows - Service Control Manager (SCM).

### 1.3.3.2 Chi tiết kiến trúc Windows server 2003



Hình 1.4: chi tiết kiến trúc windows server 2003

❖ Environment Subsystems and Subsystem DLLs: đây là thành phần rất quan trọng trong Windows nói chung và Windows server nói riêng. Windows không thể chạy nếu không có phân hệ này. Chúng luôn có trên các Server System mà không cần có sự tương tác của Login User.

❖ Executive: tập hợp các kiểu hàm chức năng.

Các hàm chức năng (các dịch vụ hệ thống) có khả năng gọi từ chế độ User Mode.

o Được xuất ra qua Ntdll.dll

o Đa số các dịch vụ có thể được truy nhập thông qua các hàm API của Windows. Các hàm điều khiển thiết bị.

o Được gọi qua hàm DeviceIoControl

o Cung cấp 1 giao diện chung từ User mode tới Kernel mode để thực hiện gọi các hàm trong các trình điều khiển thiết bị.

Windows Object Manager: Windows dùng Object Model để cung cấp truy nhập phù hợp và an toàn tới các dịch vụ nội bộ khác nhau khi điều hành System. Windows Object Manager được thiết kế để đáp ứng:

o Tạo, xóa, bảo vệ và theo dõi Objects

o Cung cấp một cơ chế thống nhất, phổ biến cho việc sử dụng System Resources

o Phân tách Objects bảo vệ trong 1 Domain của OS, tuân thủ C2 Criteria. Windows có 2 kiểu Object là

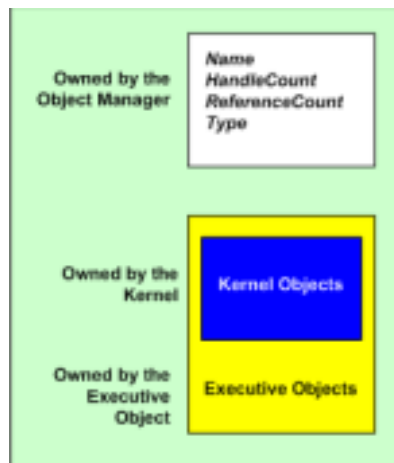
o Executive Object (EO)

o Kernel Object

o Không hiển thị trong Code ở User mode

o Được tạo ra và chỉ sử dụng bên trong Executive

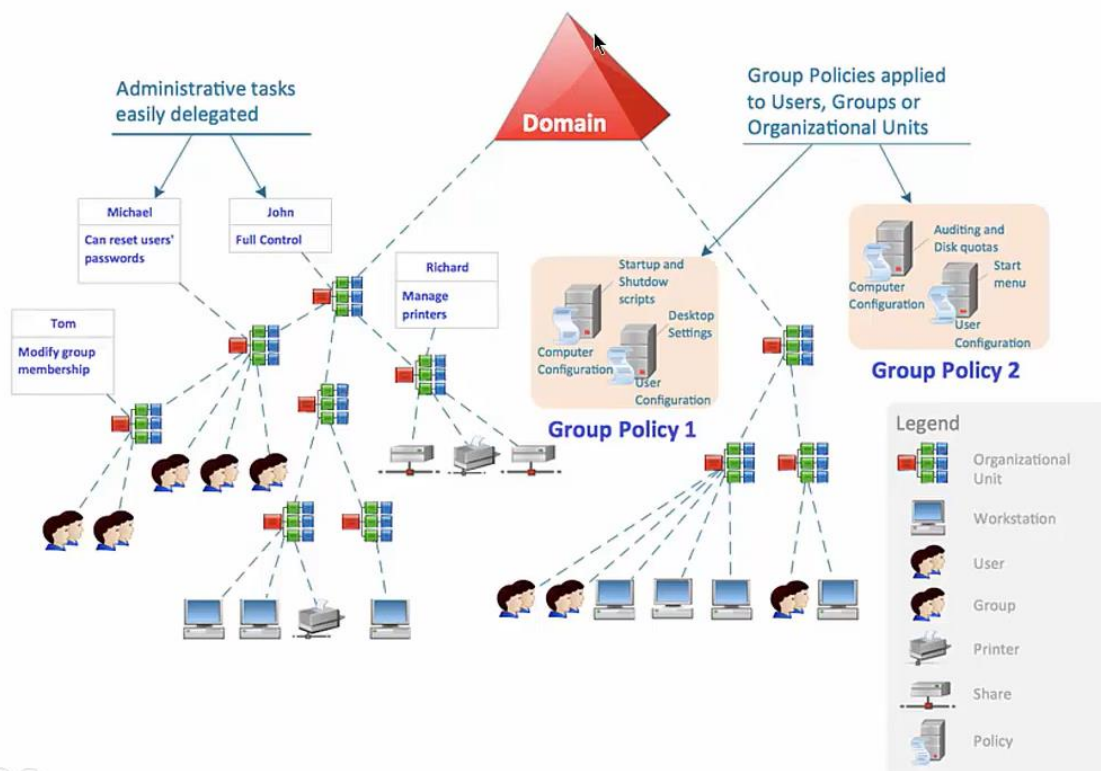
- o EOs chứa đựng (gói gọn) KOs



Hình 1.5 window object

- ❖ Kernel: Tập hợp các chức năng trong Ntoskrnl.exe cung cấp các cơ chế cơ bản: Điều phối Process và các dịch vụ đồng bộ hóa  
Một số đặc điểm của kernel:
  - o Được sử dụng bởi các thành phần thực thi
  - o Hỗ trợ kiến trúc phần cứng ở mức thấp (Interrupts)
  - o Có sự khác nhau trên mỗi Processor Architecture
  - o Chủ yếu viết trên C và Assembly Code dành riêng cho các tác vụ yêu cầu truy nhập với các chỉ lệnh vi xử lý cụ thể
- ❖ Device Drivers: là một thành phần quan trọng được tải từ Kernel, thường kết thúc bằng .sys. Đa phần được viết bằng C/C++. Chạy trong Kernel mode ở 1 trong 3 trường hợp
  - o User Process bắt đầu thực hiện 1 chức năng Input/Output
  - o System Process trong Kernel mode
  - o Kết quả của xử lý Interrupt
- System Processes
  - o Phân hệ quản lý phiên (Session Manager Subsystem - Smss.exe)
  - o Tiến trình quản lý đăng nhập (Winlogon.exe)
  - o Phân hệ thẩm quyền an toàn cục bộ (Local Security Authority Subsystem – Lsass.exe)
  - o Dịch vụ kiểm soát truy nhập (Service Control Manager - Services.exe)
  - o Phân hệ ứng dụng thời gian thực Client/Server (Client /Server Runtime Subsystem - Csrss.exe)
- ❖ Session Manager Subsystem: nằm ở Windows\System32\Smss.exe.  
Process đầu tiên trong User mode được tạo ra trong System.  
Nhiệm vụ chính của Session Manager Subsystem:
  - o Mở các tập tin bổ sung
  - o Đổi tên tập tin và xóa các tác vụ
  - o Tạo các biến môi trường hệ thống

- Winlogon nằm ở Windows\System32\Winlogon.exe. Thực hiện chức năng xử lý tương tác với User khi đăng nhập và đăng xuất System. Winlogon được kích hoạt bất cứ khi nào nó chặn tổ hợp phím chuỗi gây chú ý về bảo mật (Secure Attention Sequence – SAS) nhập từ từ Keyboard. SAS mặc định trên Windows là sự kết hợp của Ctrl+Alt+Delete. SAS bảo vệ User trước các chương trình chụp ảnh trộm Password
- Local Security Authority Subsystem nằm ở \Windows\System32\Lsass.exe. Lsass gọi gói tin xác thực thích hợp (i.e. DLL) để kiểm tra Password có phù hợp với Data được lưu trong Security Accounts Manager (SAM) File. Sau khi xác thực thành công, Lsass gọi 1 hàm trong SRM (i.e.NtCreateToken) để tạo ra 1 Object (thẻ truy nhập – Access Token) lưu hồ sơ an ninh (Secure Profile) của User. Access Token sau đó được Winlogon dùng tạo các tiến trình ban đầu cho User Session
- Cơ sở dữ liệu chính sách Lsass (Lsass Policy Database) Database lưu các cài đặt chính sách an toàn cục bộ
- Service Control Manager nằm ở \Windows\System32\Services.exe chức năng chính khởi động, dừng và tương tác với Processes.



Hình 1.6 : mô hình Active Directory Domain Server

## 2 Tiến hành thực hiện



## 2.1 cài đặt hệ điều hành Windows Server 2019

Trước tiên ta cần tải về file iso của windows server 2019



### Windows Server 2019

Overview Get started for free Description Prerequisites Resources Supporting products

#### Overview

In addition to your trial experience of Windows Server 2019, you can download a new feature on demand for Server Core, la aplicación Compatibilidad FOD. improve the compatibility of Server Core for aplicaciones and tools used for troubleshooting and debugging. Windows features on demand can be added to the DISM command.

Learn more about the [Server Core App Compatibilidad FOD](#). Download this [FOD](#).

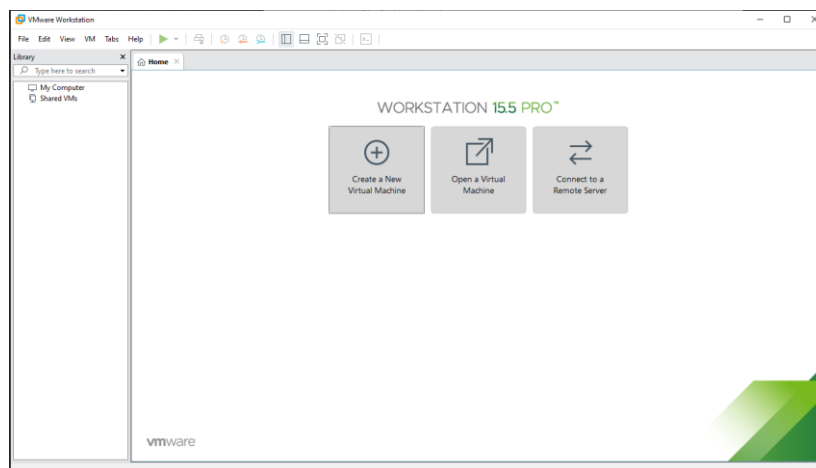
To learn more about FODs in general, and the DISM command, please visit [DISM Capabilities Package Servicing](#).

#### Get started for free

Please select your product experience:

[Try Windows Server on Azure >](#) [Download the ISO >](#) [Download the VHD >](#)

### 2.1.2 Trên VMWare Workstation



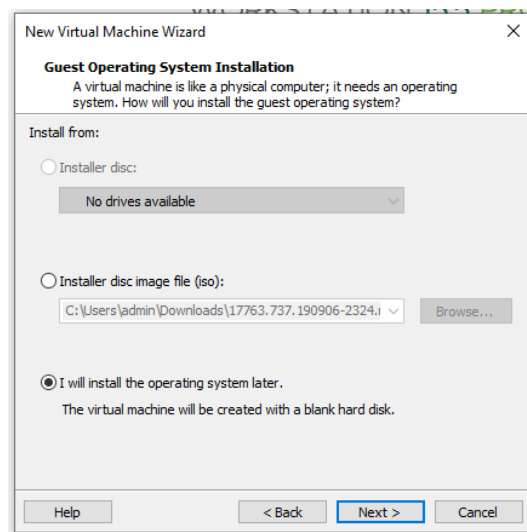
Hình 2.1 giao diện chính của chương trình VMWare

- Chọn **File -> New Virtual Machine** của sổ cài đặt máy ảo mới sẽ hiện ra (Xem Hình 2.2).



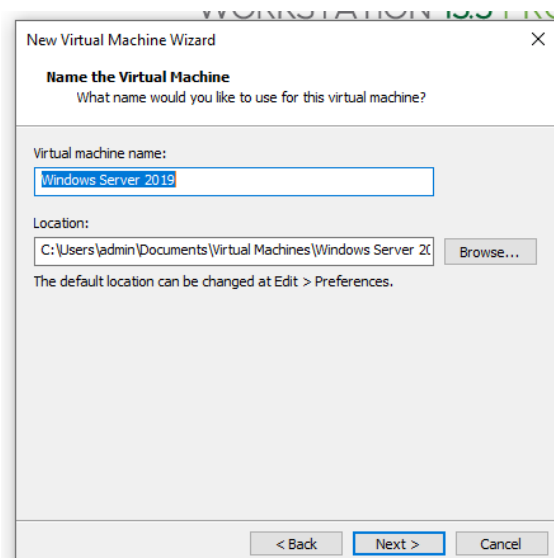
### Hình 2.2 : Cài đặt máy ảo

- Chọn **Typical (recommended)** để thực hiện cài đặt nhanh hoặc chọn **Custom (advanced)** để cài đặt với nhiều tùy chỉnh chuyên sâu. Trong bài thực hành này sẽ sử dụng chế độ **Typical**, chọn **Typical** và ấn **Next**.
- Bước tiếp theo để mặc định và **Next**.
- Giao diện lựa chọn hệ điều hành sẽ hiện ra, lựa chọn **Installer disc image file (iso)** và chọn file iso đã chuẩn bị từ đầu (Xem Hình 2.3).

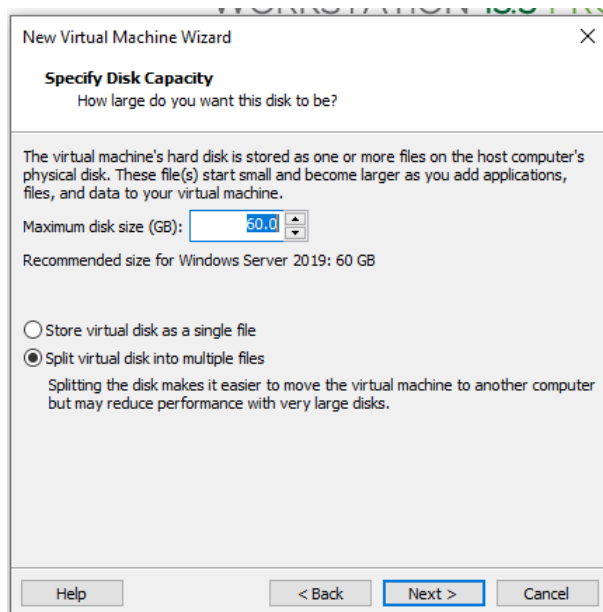


Hình 2.3: Cấu hình đường dẫn chứa file cài đặt

- Bước tiếp theo sẽ là tùy chọn tên của máy ảo hiển thị trong VMWare và đường dẫn lưu máy ảo. Nhập thông tin tùy chỉnh rồi ấn **Next** (Xem Hình 2.4).

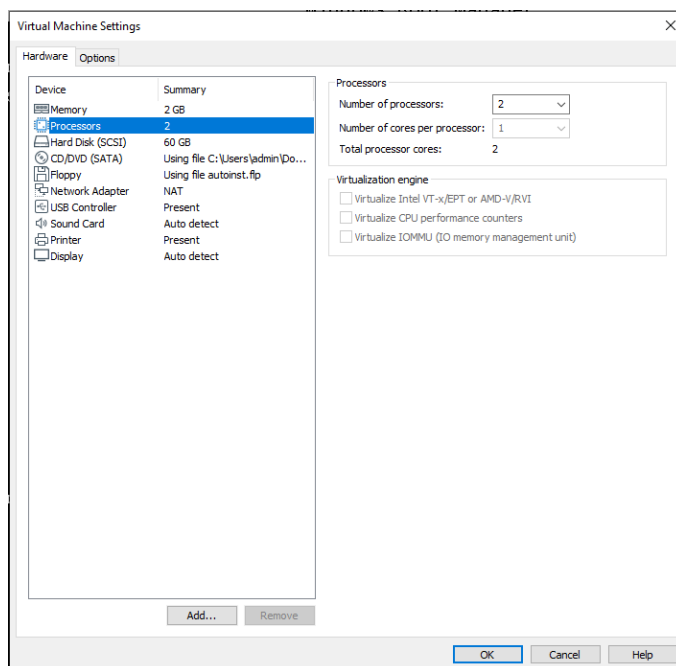


Hình 2.4 :Cấu hình đường dẫn lưu file máy ảo



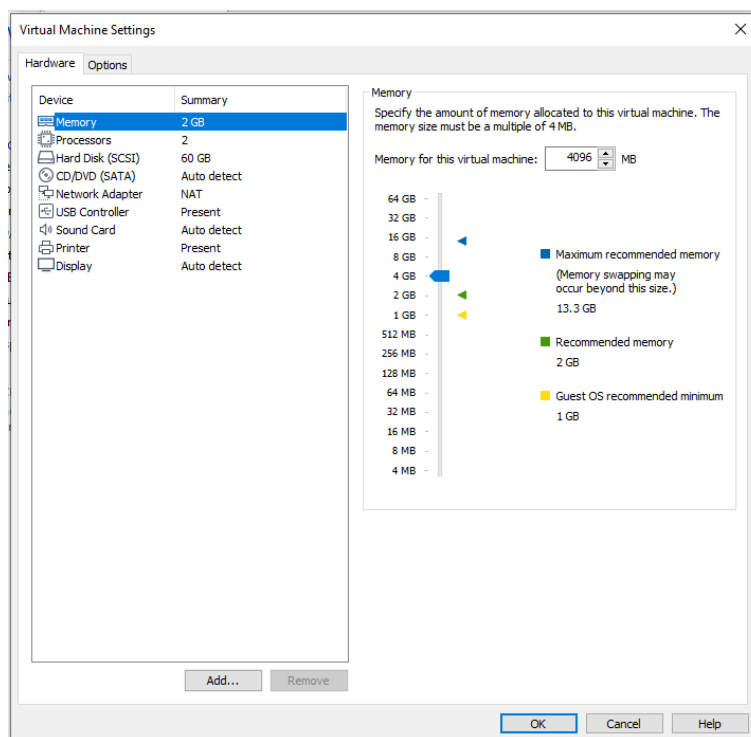
*Hình 2.5: tùy chọn kích thước ổ đĩa cho máy ảo*

- Lựa chọn số nhân cho máy ảo, trong trường hợp này khuyến nghị nên chọn 1 nhân và 2 luồng sẽ giúp cho máy ảo chạy ổn định hơn. Ấn **Next** để tiếp tục (Xem Hình 2.6).



*Hình 2.6: Cấu hình số nhân CPU cấp cho máy ảo*

- Lựa chọn dung lượng ram cấp cho máy ảo, khuyến nghị từ 2048 MB trở lên. Ấn **Next** để tiếp tục (Xem Hình 2.7).

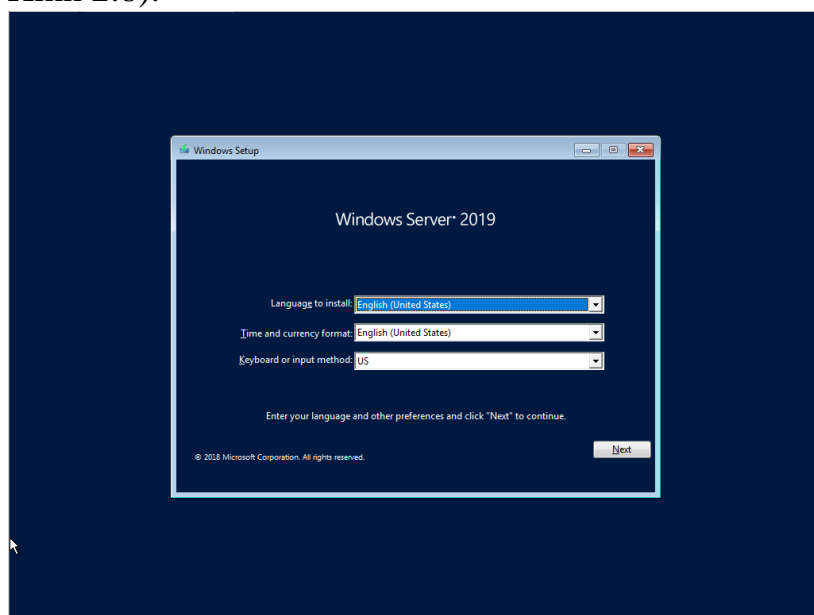


Hình 2.7 : Cấu hình dung lượng RAM cho máy ảo

- 4 bước tiếp theo để mặc định. Đến bước chọn dung lượng tối đa cấp cho máy ảo, khuyến nghị nên để lớn hơn 20GB. Ấn **Next** để tiếp tục. Các bước sau để mặc định và ấn **Finish** ở bước cuối để hoàn tất. Máy ảo sẽ tự động chạy.

### 2.1.3 Trên máy ảo Windows Server 2019

- Sau khi hoàn tất các bước cấu hình trên VMWare thì máy ảo Windows Server 2019 sẽ được khởi động, giao diện cài đặt chính như hình dưới (Xem Hình 2.8).



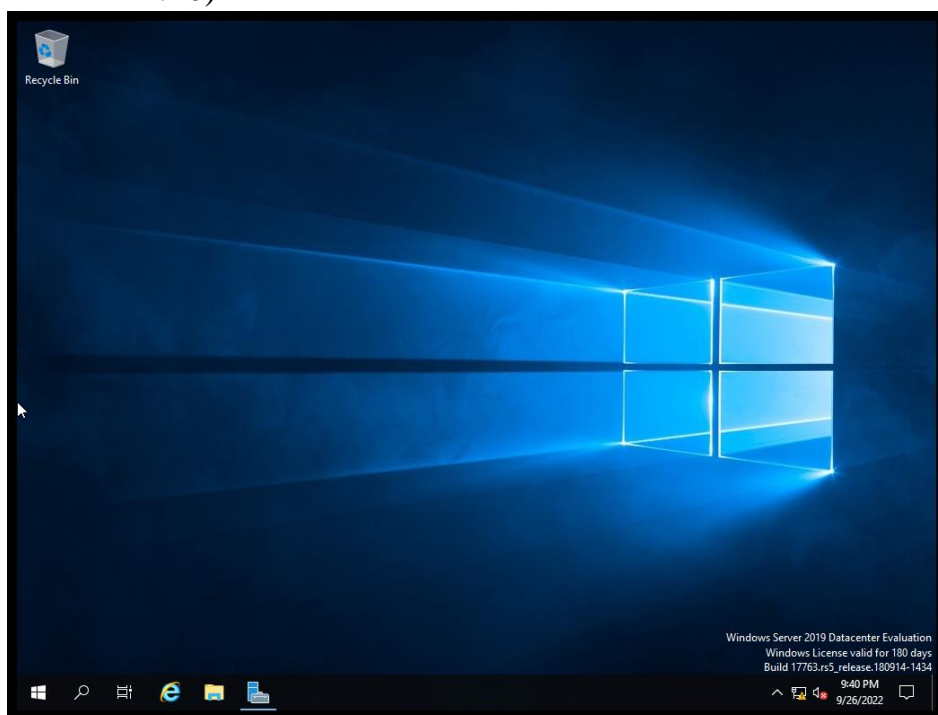
Hình 2.8: giao diện cài đặt Windows Server 2019

- Quá trình cài đặt sẽ diễn ra trong một vài phút, sau đó giao diện đăng nhập sẽ được hiển thị (Xem Hình 2.9).



*Hình 2.9 :giao diện đăng nhập vào Windows Server 2019*

- Tiến hành đăng nhập bằng tài khoản đã cấu hình ở bước trước, đăng nhập thành công giao diện chính của Windows Server 2019 sẽ được hiển thị (Xem Hình 2.10)

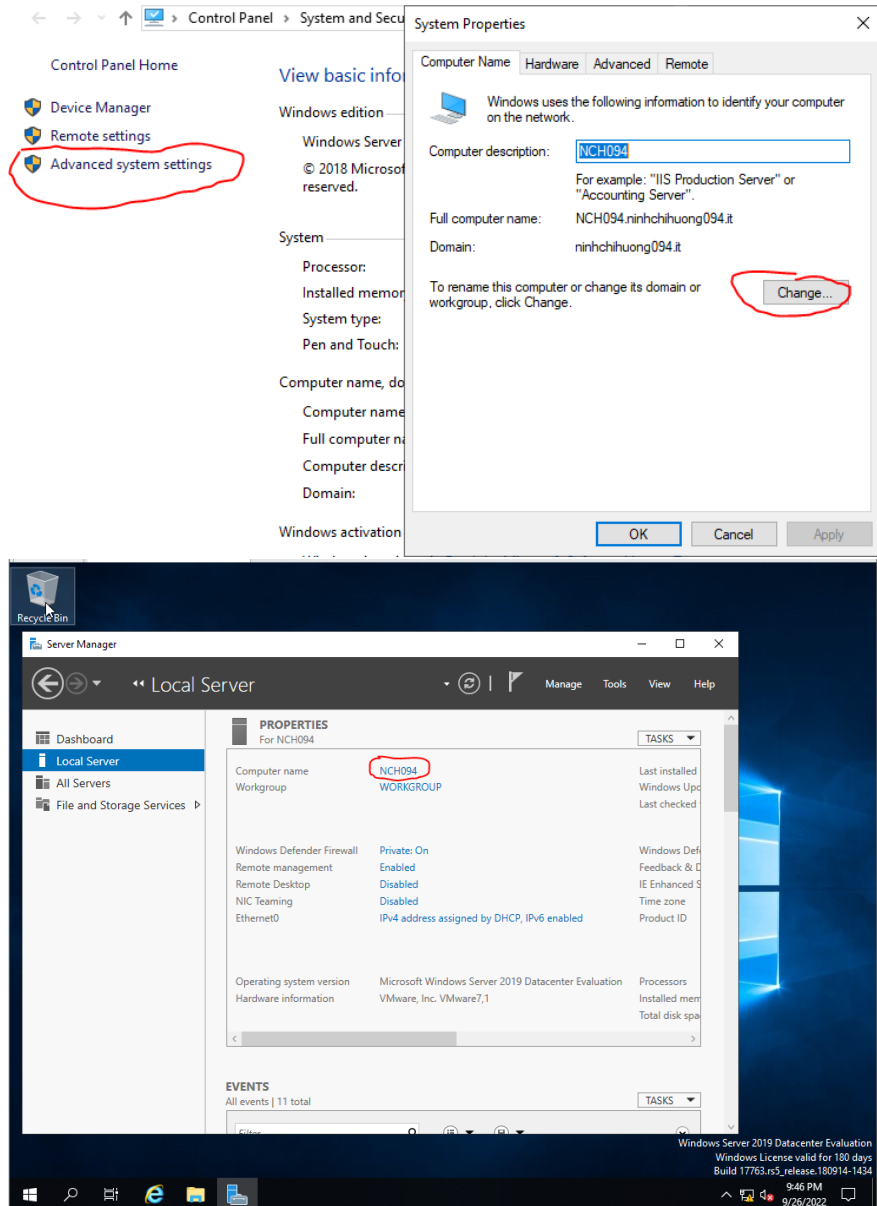


*Hình 2.10: giao diện màn hình chính của Windows Server 2019*

## **2.2 Nâng cấp Server thành Domain Controller**

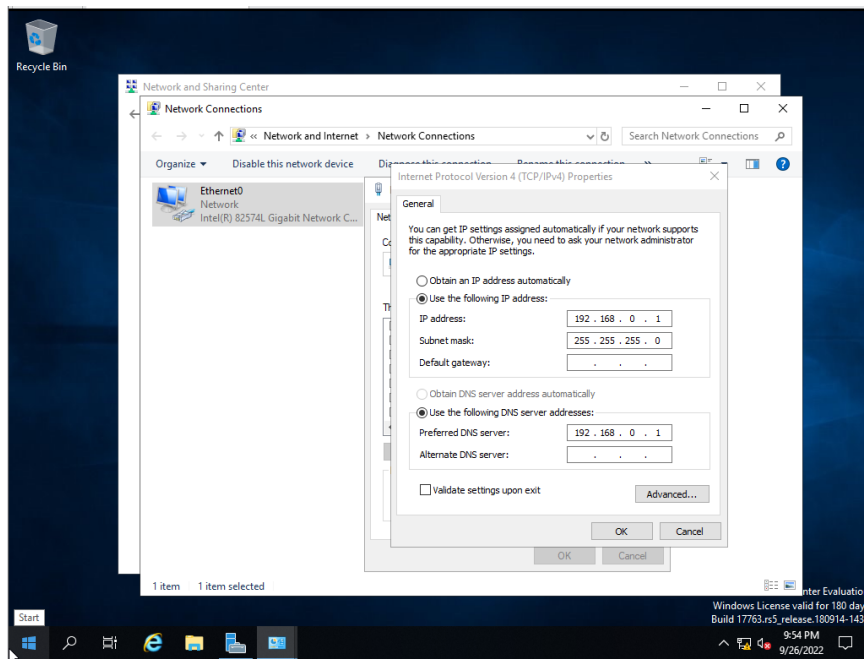
### **2.2.1 Kiểm tra tên server**

This PC (chuột phải) > Properties > Advanced System Setting > Computer Name > Kiểm tra đúng/sai hoặc Thay đổi (change).

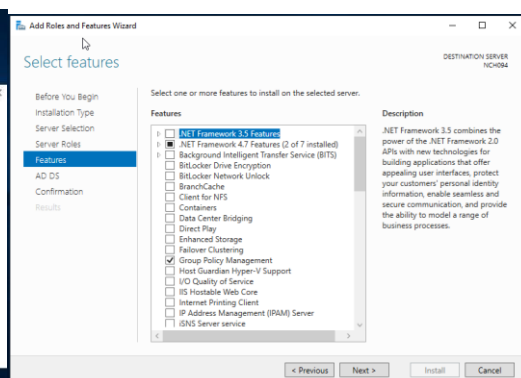
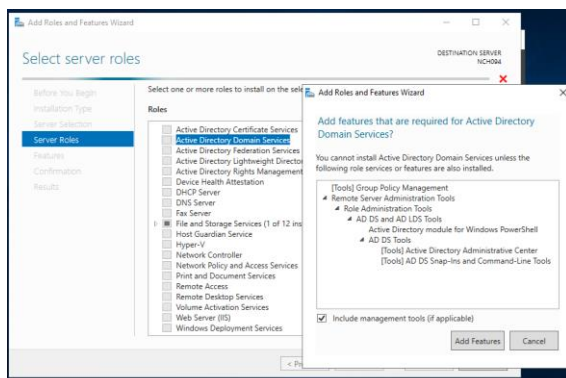
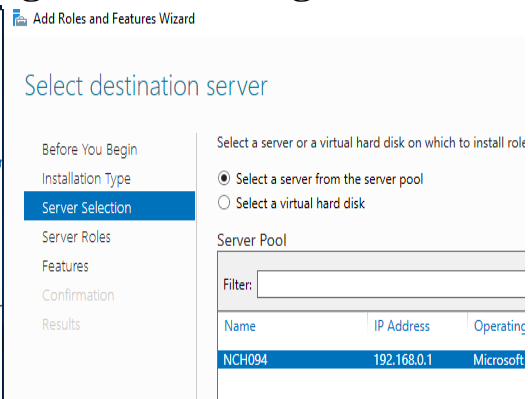
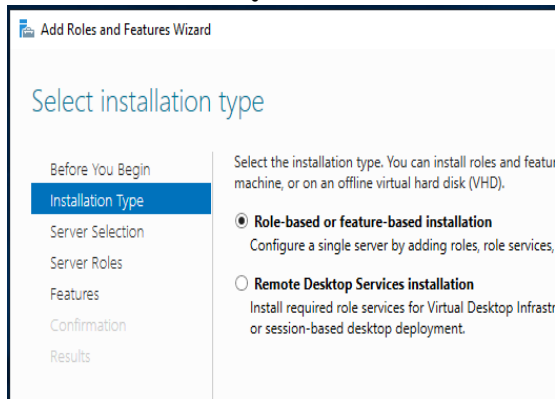


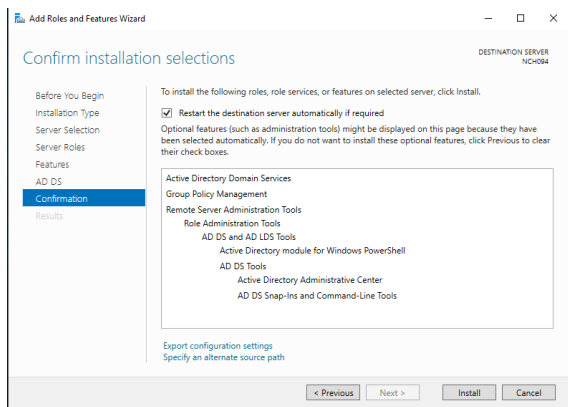
## 2.2.2 Cài đặt static IP

Open Network and Sharing Center (Chuột phải) > Change Adapter Settings > Ethernet0 (Chuột phải) > Properties > Internet Protocol Version 4 (TCP/IP) Properties > Use the following IP address > Restart



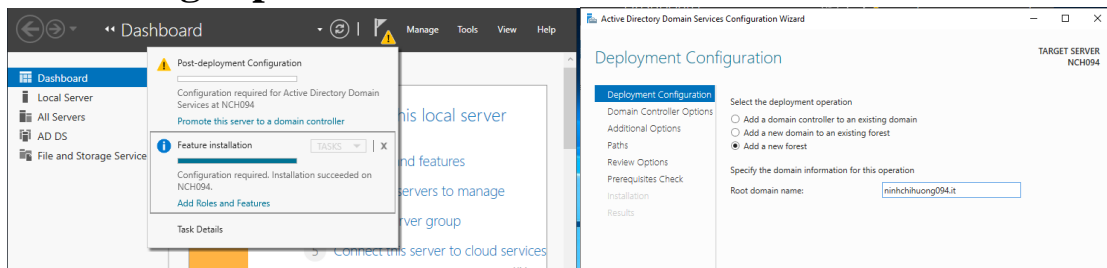
## 2.2.3 Cài đặt server role trong Server Manager



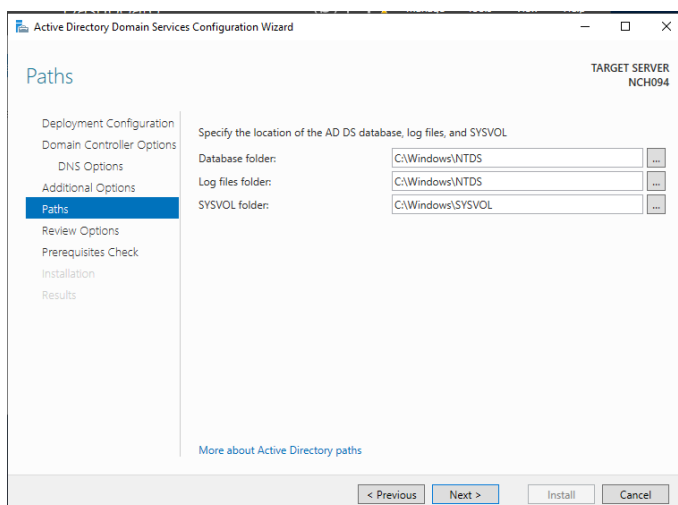


Đây chưa hẳn đã là cài đặt Active Directory ☐  
 Nó chỉ cài đặt role, cho phép chúng ta nâng cấp server thành Domain Controller.

## 2.2.4 Nâng cấp Server thành Domain Controller

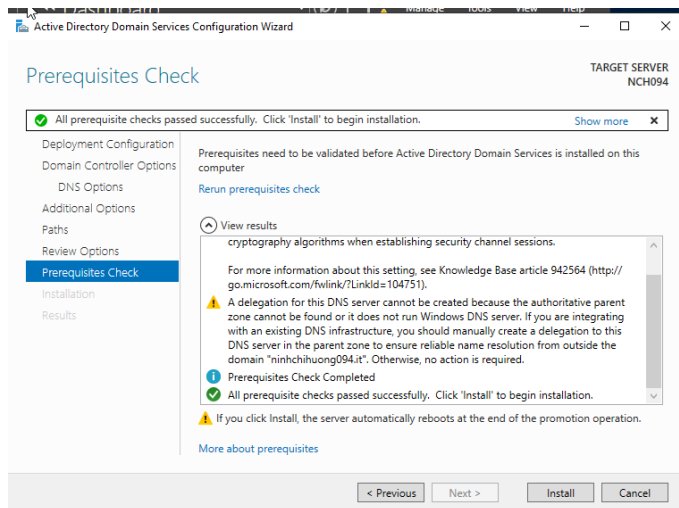


Đặt tên cho Root domain name: **Ninh Chí Hường**, mã sv **B20DCAT094** thì đặt là **ninhchihuong094.it**

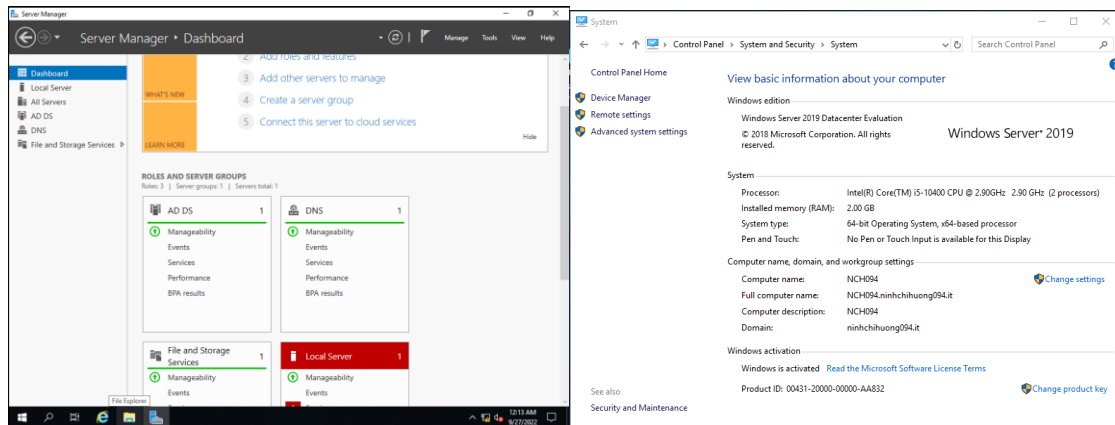


Đây là bước lựa chọn vị trí lưu trữ các database.





Sau khi yêu cầu được kiểm tra thành công ta chọn **install** để cài đặt



Sau khi máy khởi động lại, ta kiểm tra lại trong Server manager dịch vụ đã được cài đặt và kiểm tra hệ thống máy đã thay đổi domain .