

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

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

Họ và tên sinh viên:

Vũ Thành Long

Mã số sinh viên:

B21DCAT012

Họ và tên giảng viên:

TS. Đinh Trường Duy

Bài 1: Cài đặt Windows Server và dịch vụ thư mục Active Directory trong Windows Server

1 GIỚI THIỆU BÀI THỰC HÀNH

1.1 Mục đích

- Giúp sinh viên có thể tự tạo một máy chủ Windows 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 Nhóm thực hành

- 1 sinh viên.

2 CƠ SỞ LÝ THUYẾT

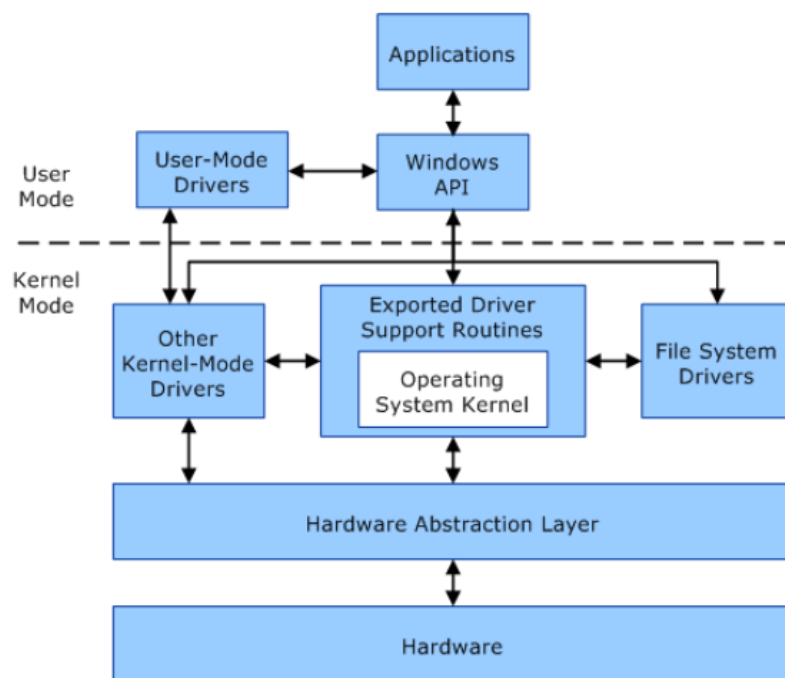
Kiến trúc của Windows server

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

2.1 Kiến trúc chung của windows



Hình 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)

- User mode như trên mình gồm 3 thành phần chính

Người dùng tương tác với hệ thống thông qua các Applications

Các application thực hiện chức năng thông qua Windows API và được điều khiển bởi UserMode Drivers

- Kernel mode làm việc với hardware thông qua Hardware Abstraction Layer

Trên nữa là các drivers hỗ trợ làm việc với hardware cũng như kết nối Windows API và driver user-mode ở lớp trên

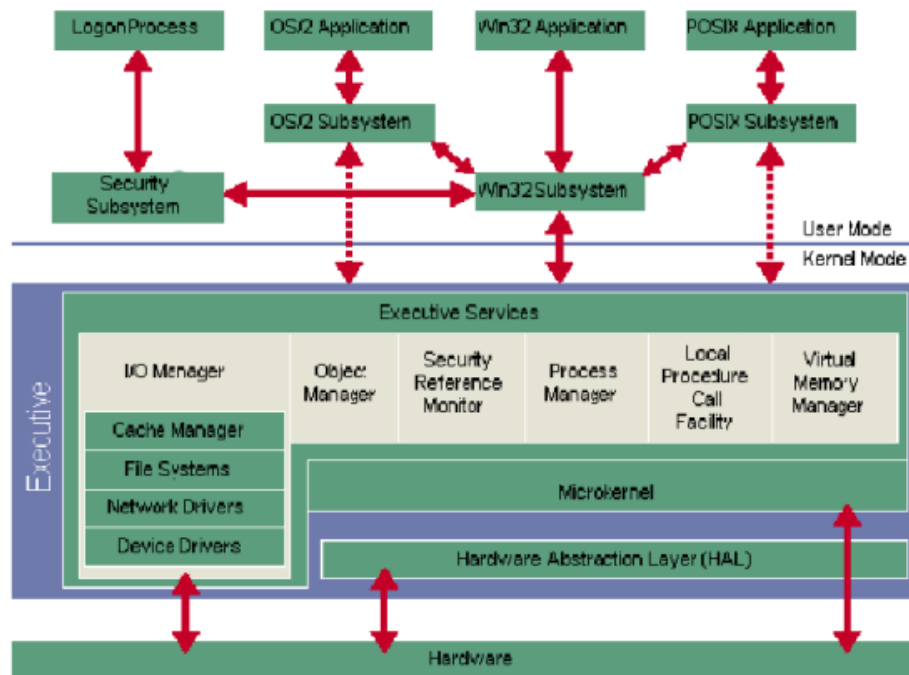
2.2 Kiến trúc Windows NT:

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. Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (nhân). Khi một thành phần của hệ điều hành chạy dưới chế độ Kernel, nó truy cập đầy đủ các chỉ thị máy cho bộ xử lý đó và có thể truy cập tổng quát toàn bộ tài nguyên trên hệ thống máy tính

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. Bằng cách đặt các

hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được thiết kế để chạy dưới chế độ Kernel.



Hình 2: Kiến trúc Windows NT

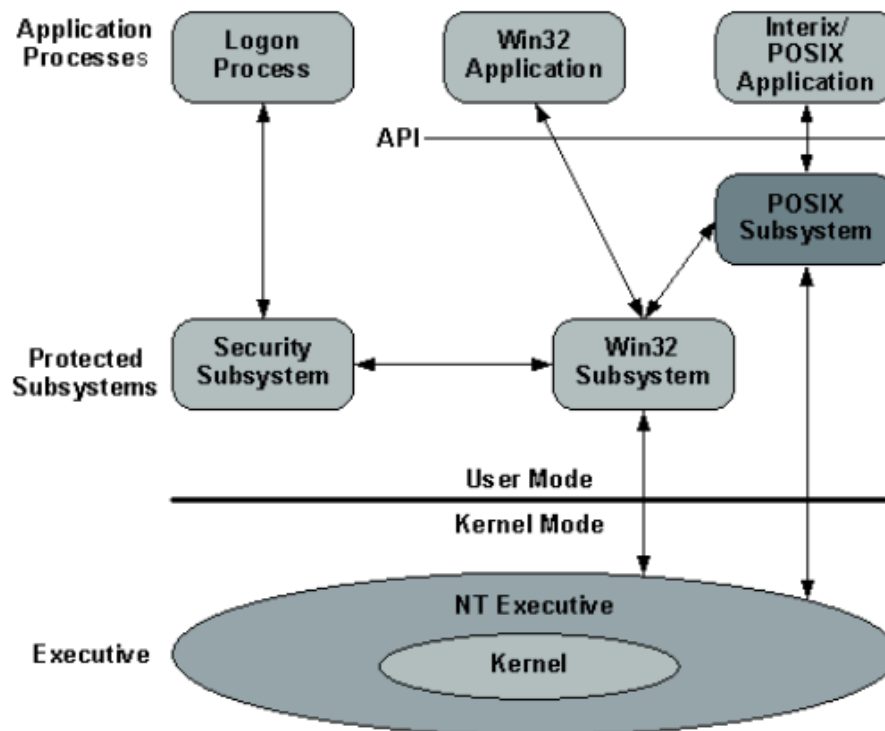
Các lớp chính của hệ điều hành WINDOWS NT SERVER gồm:

- Lớp phần cứng trừu tượng (Hardware Astraction 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. Phần lớn Kernel sử dụng HAL để truy cập các tài nguyên máy tính. Điều này có nghĩa là Kernel và tất cả các thành phần khác phụ thuộc vào Kernel có thể dễ dàng xuất (Ported) thông qua Microsoft đến các nền (Platform) phần cứng khác. Một thành phần nhỏ trong Kernel, cũng như bộ quản lý Nhập/Xuất truy cập phần cứng máy tính trực tiếp mà không cần bao gồm HAL.
- Lớp Kernel: Cung cấp các chức năng cơ bản của hệ điều hành được sử dụng bởi các thành phần thực thi khác. Thành phần Kernel tương đối nhỏ và cung cấp các thành phần cốt yếu cho những chức năng của hệ điều hành. Kernel chủ yếu chịu trách nhiệm quản lý luồng, quản lý phần cứng và đồng bộ đa xử lý.

Các thành phần Executive: Là các thành phần hệ điều hành ở chế độ Kernel thi hành các dịch vụ như:

- Quản lý đối tượng (object manager)
- Bảo mật (security reference monitor)
- Quản lý tiến trình (process manager)
- Quản lý bộ nhớ ảo (virtual memory manager)
- Thủ tục cục bộ gọi tiện ích, và quản trị nhập/xuất (I/O Manager)

2.3 Kiến trúc Windows server 2003:



Hình 3: Kiến trúc cơ bản của Windows server 2003

2.3.1 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).
 - Application process là tập hợp các chương trình các ứng dụng chạy trên Windows có thể là win32 application hoặc là các POSIX application.
 - Subsystem:
 - Protected subsystems được gọi như vậy bởi vì mỗi hệ thống con trong đó đều được xây dựng với một process riêng biệt với không gian riêng bảo vệ địa chỉ của nó. Trong đó win32 subsystem là một thành phần quan trọng trong đó cung cấp nhiều chức năng cho windows
 - Windows không thể chạy nếu không có phân hệ này. Luôn có trên các Server System mà không cần có sự tương tác của Login User.
 - Giao diện lập trình ứng dụng (application programming interface - API) là thành phần trung gian hỗ trợ các application, rất hữu ích trong phát triển các ứng dụng trên nền Windows 32bit và 64 bit.
- 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. Kerner mode còn được gọi là

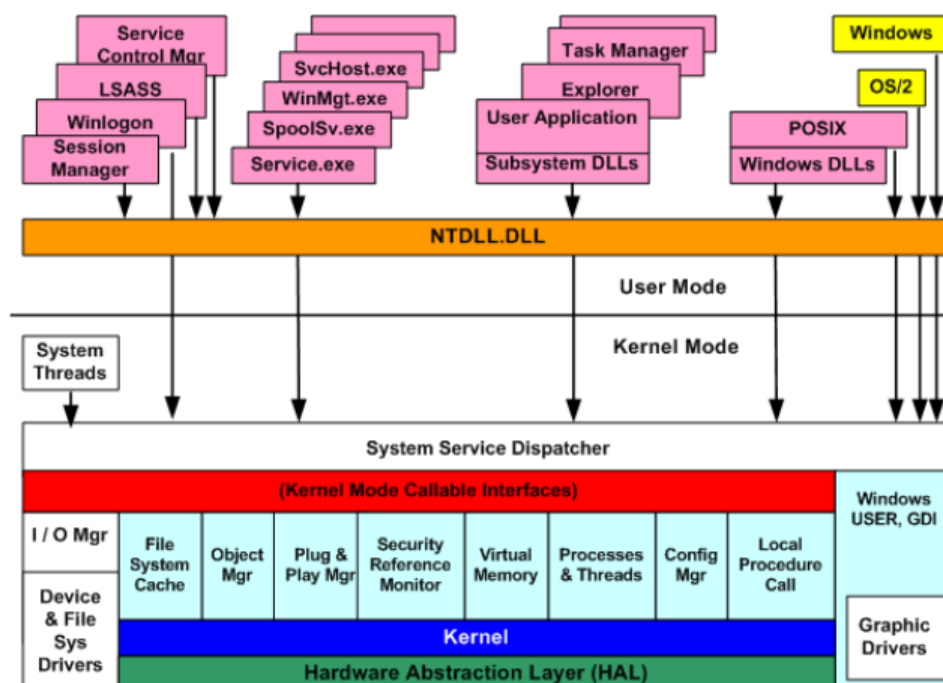
supervisor mode, protected mode. Kernel mode của Windows server 2003 bao gồm: Windows NT executive cũng như system kernel.

- Windows NT executive thực thi các dịch vụ chung mà protected subsystems ở lớp trên gọi từ đó có được các dịch vụ hệ điều hành cơ bản. Chẳng hạn như hoạt động của tập tin, dữ liệu vào/ra (I/O), và các dịch vụ đồng bộ hóa. Phân vùng các protected subsystems và system kernel giúp đơn giản hóa thiết kế hệ điều hành cơ bản và cho phép mở rộng các tính năng protected subsystems mà không ảnh hưởng đến system kernel
- Kernel kiểm soát hệ điều hành sử dụng các vi xử lý. Hoạt động của nó bao gồm lập kế hoạch, đồng bộ hóa đa năng và cung cấp các đối tượng mà NT executive có thể sử dụng hoặc export sang các ứng dụng

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).

2.3.2 Chi tiết kiến trúc Windows server 2003



Hình 4: Chi tiết kiến trúc Windows server 2003

Tìm hiểu cụ thể và chi tiết hơn các thành phần của 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

- Được xuất ra qua NtDll.dll
- Đa số các dịch vụ có thể được truy nhập thông qua các hàm API của Windows

Các hàm điều khiển thiết bị

- Được gọi qua hàm DeviceIoControl
- 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.

Những phần chính:

- Configuration Manager: Quản lý Registry System.
- Process and Thread Manager: Tạo/ngắt Processes & Threads, hỗ trợ Processes & Threads thực thi trong Kernel.
- Security Reference Monitor (SRM):
 - ☐ Là 1 phần của Ntoskrnl.exe
 - ☐ Thực thi Secure Policies trên Local Host
 - ☐ Bảo vệ System Resources
 - ☐ Kểm toán và bảo vệ Objects
- Object Manager.
- Cache Manager.
- Memory Manage .
- Input/Output Manager.

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:

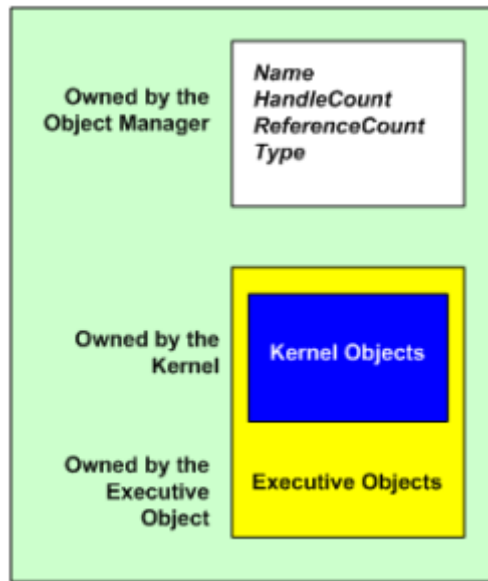
- Tạo, xóa, bảo vệ và theo dõi Objects
- Cung cấp một cơ chế thống nhất, phổ biến cho việc sử dụng System Resources
- Phân tách Objects bảo vệ trong 1 Domain của OS, tuân thủ C2 Criteria

Windows có 2 kiểu Object là

- Executive Object (EO)
- Kernel Object

Kernel Object

- Không hiển thị trong Code ở User mode



Hình 5: Windows Object

- Được tạo ra và chỉ sử dụng bên trong Executive
- EOs chứa đựng (gói gọn) KOs
- ❖ 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:
 - Được sử dụng bởi các thành phần thực thi
 - Hỗ trợ kiến trúc phần cứng ở mức thấp (Interrupts)
 - Có sự khác nhau trên mỗi Processor Architecture
 - 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
 - User Process bắt đầu thực hiện 1 chức năng Input/Output
 - System Process trong Kernel mode
 - Kết quả của xử lý Interrupt
- System Processes
 - Phân hệ quản lý phiên (Session Manager Subsystem - Smss.exe)
 - Tiến trình quản lý đăng nhập (Winlogon.exe)
 - Phân hệ thẩm quyền an toàn cục bộ (Local Security Authority Subsystem – Lsass.exe)
 - Dịch vụ kiểm soát truy nhập (Service Control Manager - Services.exe)
 - 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:

- Mở các tập tin bổ sung
- Đổi tên tập tin và xóa các tác vụ
- Tạo các biến môi trường hệ thống

Chạy các tiến trình hệ thống con và tiến trình đăng nhập Winlogon để tiến trình này lần lượt tạo ra các phần còn lại của các tiến trình hệ thống. Sau khi thực thi các bước khởi tạo tiến trình chính trong Smss sẽ chờ để lấy kết quả xử lý của Csrss và Winlogon. Khi 1 trong Processes này chấm dứt đột ngột Smss sẽ làm treo 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. Các khía cạnh định danh và xác thực của tiến trình đăng nhập được thực thi trong DLL có khả năng thay thế Graphical Identification and Authentication (GINA). GINA tiêu chuẩn là Msgina.dll, thực hiện giao diện đăng nhập Windows mặc định. Developers có thể cung cấp GINA DLL để thực thi các cơ chế định danh và xác thực khác với kỹ thuật sử dụng cặp Name/Password để xác thực của Windows (i.e. Voice)
- 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. Ngoài ra, tham khảo chương 1, chương 2 trong tài liệu “Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016”

3 NỘI DUNG THỰC HÀNH

3.1 Thực hành cài đặt hệ điều hành Windows Server 2019

3.1.1 Chuẩn bị môi trường

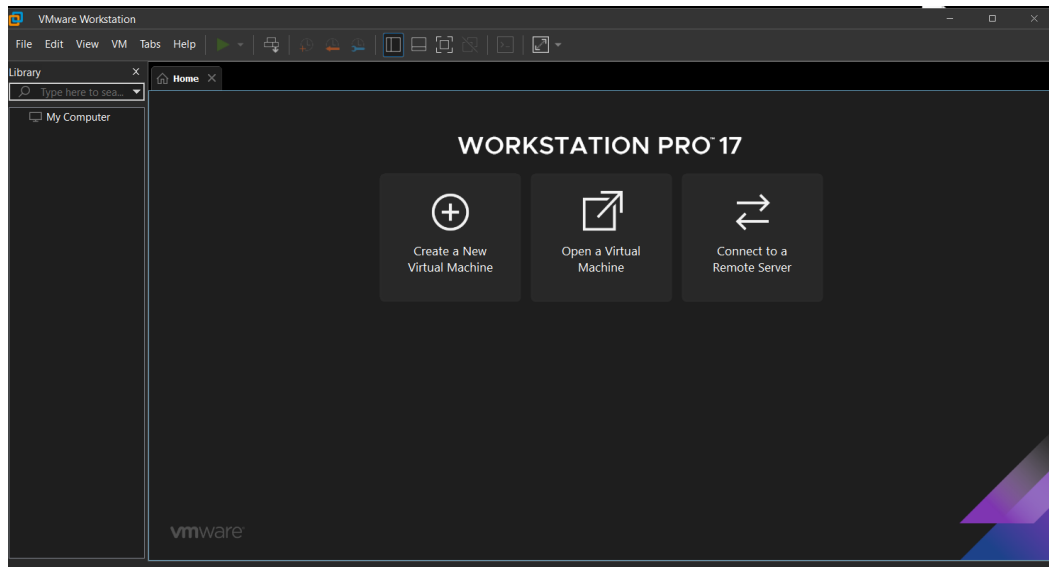
- 1 máy ảo Windows Server 2019

- 1 máy ảo Windows 7

3.1.2 Các bước thực hiện

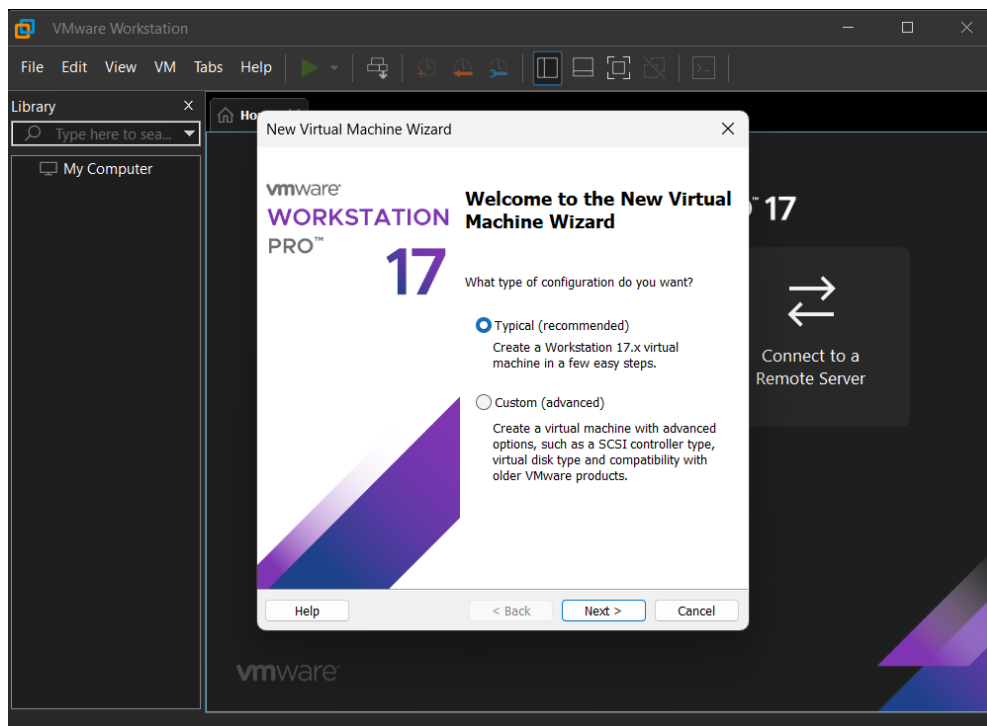
3.1.2.1 Trên VMWare Workstation

- Khởi động chương trình VMWare Workstation, giao diện chính sẽ hiện ra (Xem Hình 3.1).



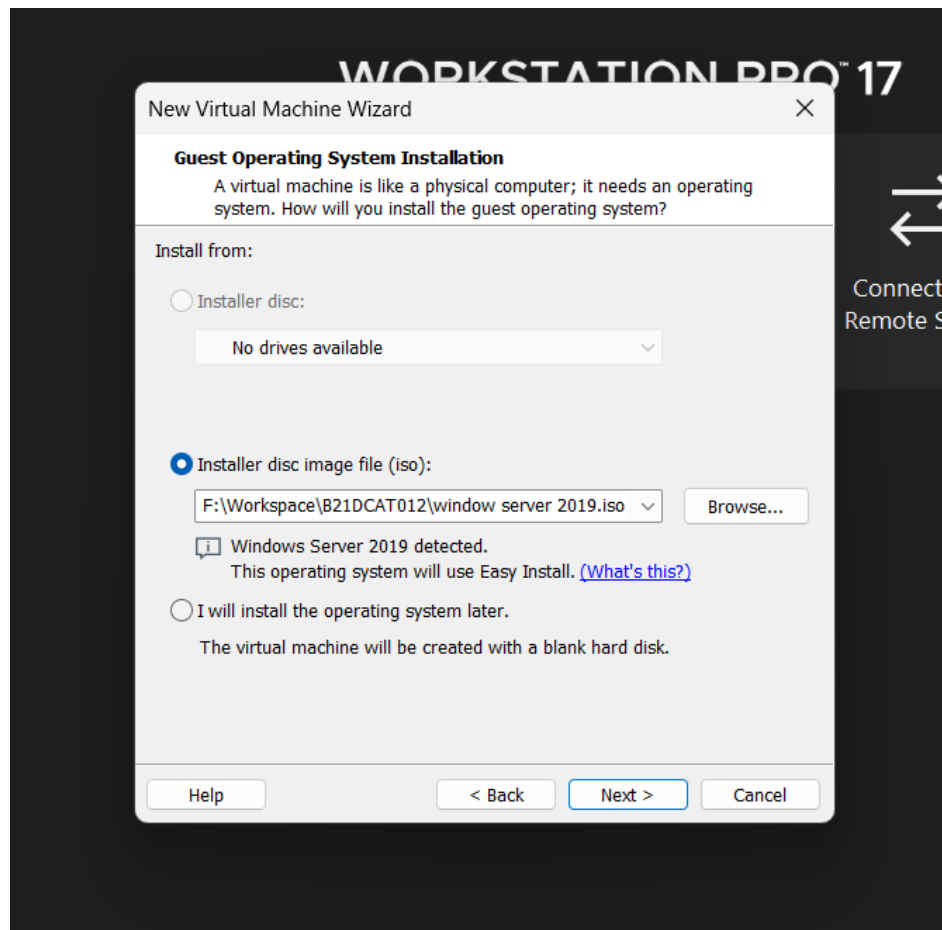
Hình 3.1: Giao diện chính của chương trình VMWare

- Chọn **File -> New Virtual Machine** của sổ cài đặt máy ảo mới sẽ hiện ra (Xem Hình 3.2).



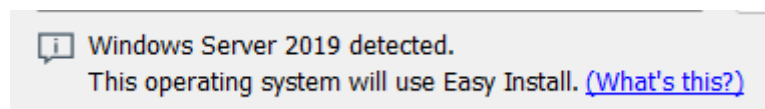
Hình 3.2: Cài đặt máy ảo

- 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 3.3) .
- File iso Windows Server 2019 có thể tải trực tiếp từ trang chủ Microsoft



Hình 3.3: Cấu hình đường dẫn chứa file cài đặt

- Trong trường hợp này VMWare thông báo là phát hiện file iso vừa chọn là của Windows Server 2019 và việc cài đặt sẽ sử dụng cơ chế **Easy Install** giúp cho việc cài đặt diễn ra nhanh chóng hơn (Xem Hình 3.4). Ấn **Next** để tiếp tục.



Hình 3.4: VMWare tự động phát hiện hệ điều hành

- Trong cửa sổ tiếp theo sẽ là tùy chọn về key bản quyền Windows tên người dùng, tên đăng nhập và mật khẩu. Tiến hành nhập đầy đủ (key bản quyền nếu không có, có thể không nhập) và ấn **Next** (Xem Hình 3.5)

New Virtual Machine Wizard

Easy Install Information
This is used to install Windows Server 2019.

Windows product key

Version of Windows to install
Windows Server Datacenter Core

Personalize Windows

Full name: B21DCAT012

Password: (optional)

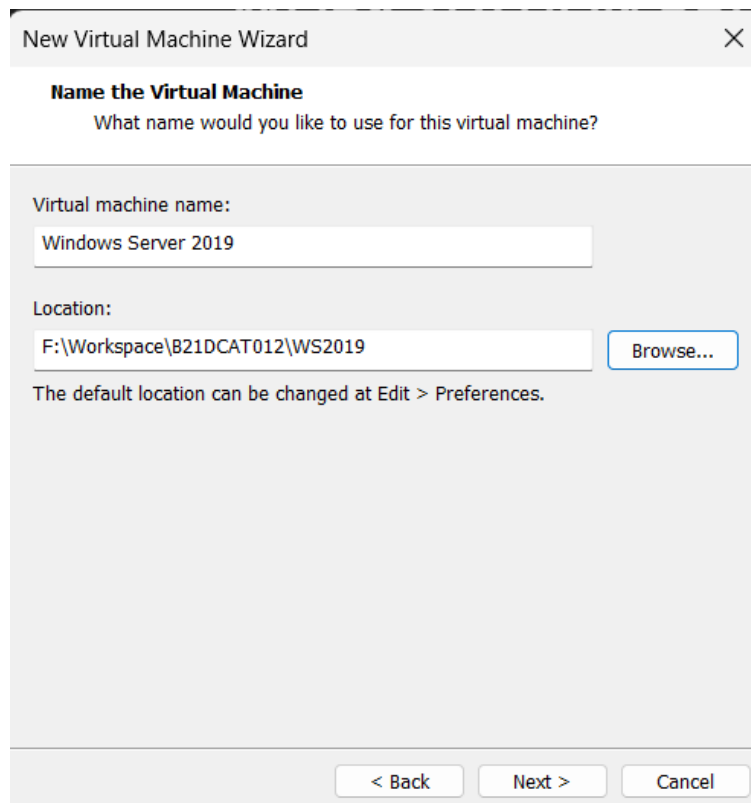
Confirm:

☐ Log on automatically (requires a password)

Help < Back Next > Cancel

Hình 3.5: Cấu hình tên đăng nhập và mật khẩu

- 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 3.6).



New Virtual Machine Wizard

Name the Virtual Machine
What name would you like to use for this virtual machine?

Virtual machine name:
Windows Server 2019

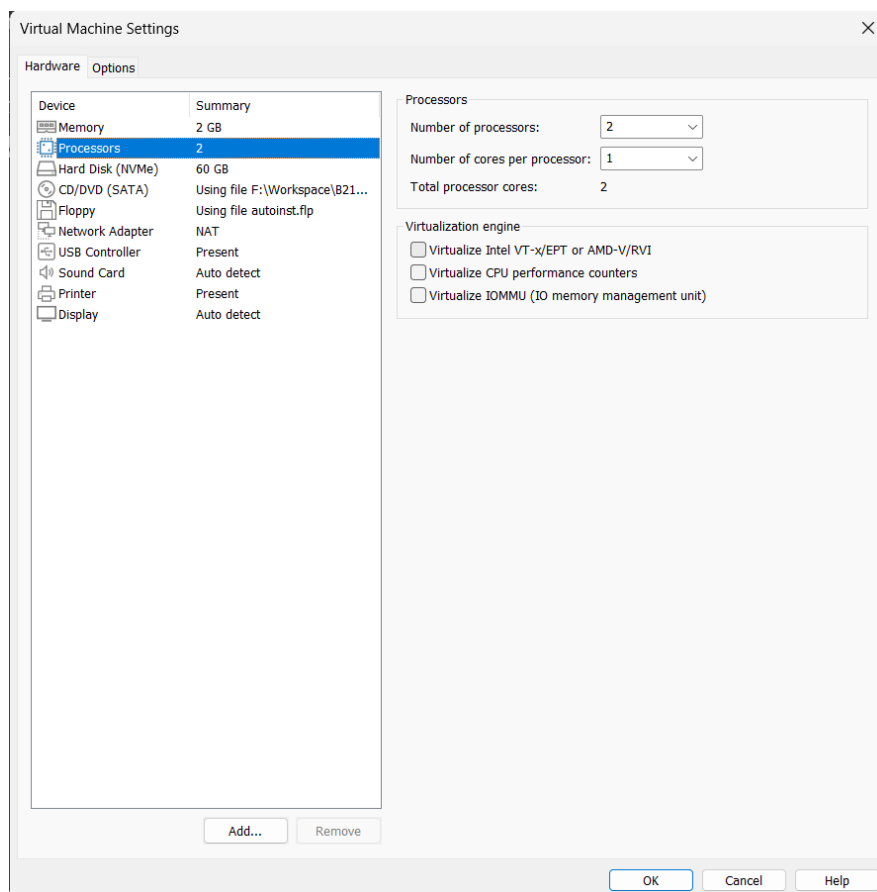
Location:
F:\Workspace\B21DCAT012\WS2019 Browse...

The default location can be changed at Edit > Preferences.

< Back Next > Cancel

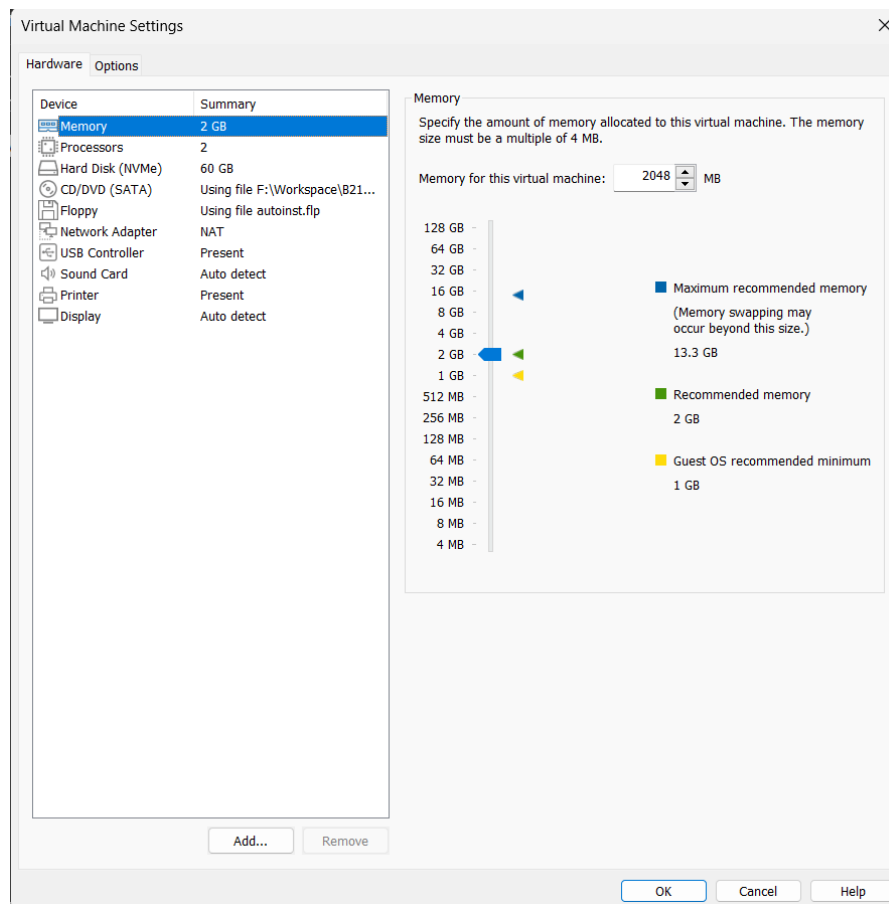
Hình 3.6: Cấu hình đường dẫn lưu máy ảo

- 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 3.7).



Hình 3.7: 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 3.8).

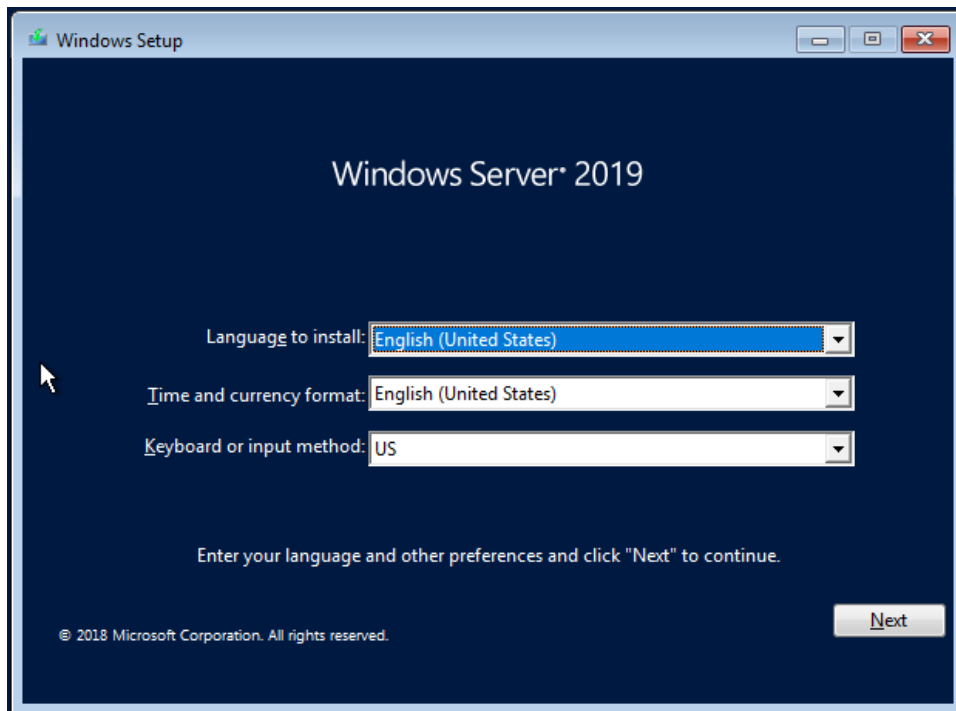


Hình 3.8: Cấu hình dung lượng RAM cấp cho máy ảo

- 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.

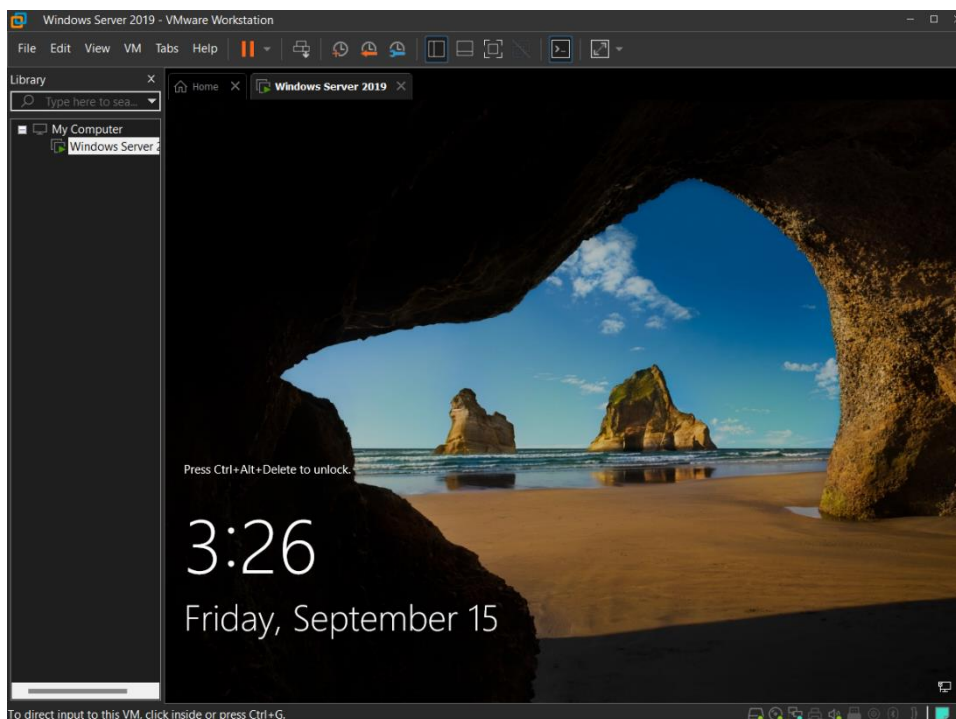
3.1.2.2 Trên máy ảo Windows Server 2019

- 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 3.9).



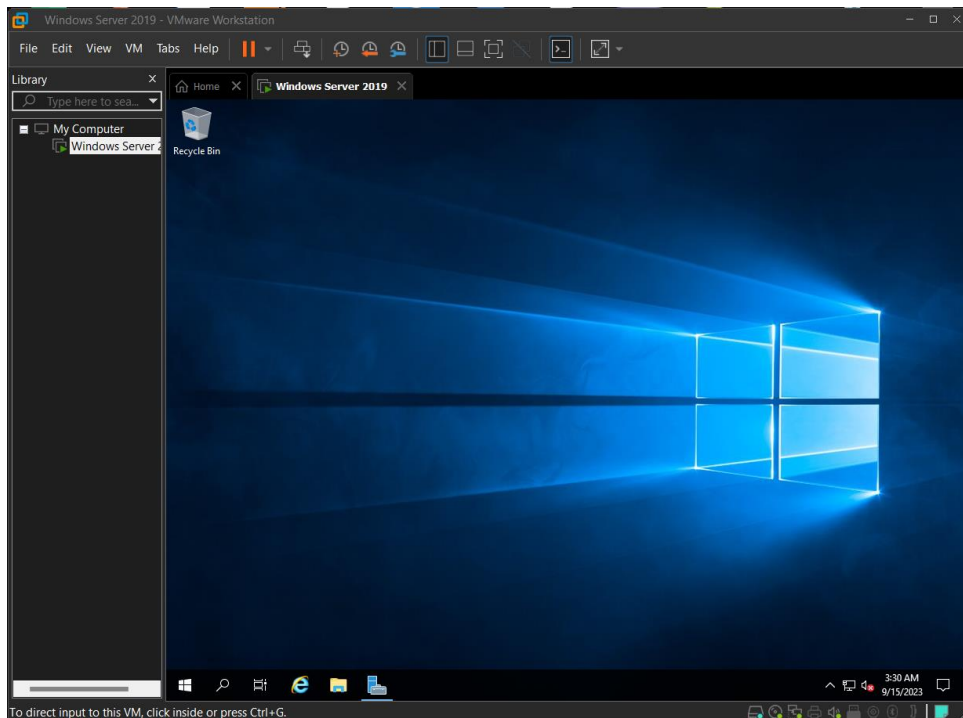
Hình 3.9: Giao diện cài đặt Windows Server 2019

- ❑ Quá trình cài đặt sẽ diễn ra trong một vài phút, sau đó giao diện đăng nhập sẽ được hiển thị (Xem Hình 3.10) .



Hình 3.10: Giao diện đăng nhập 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 3.11).



Hình 3.11: Giao diện màn hình chính của Windows Server 2019

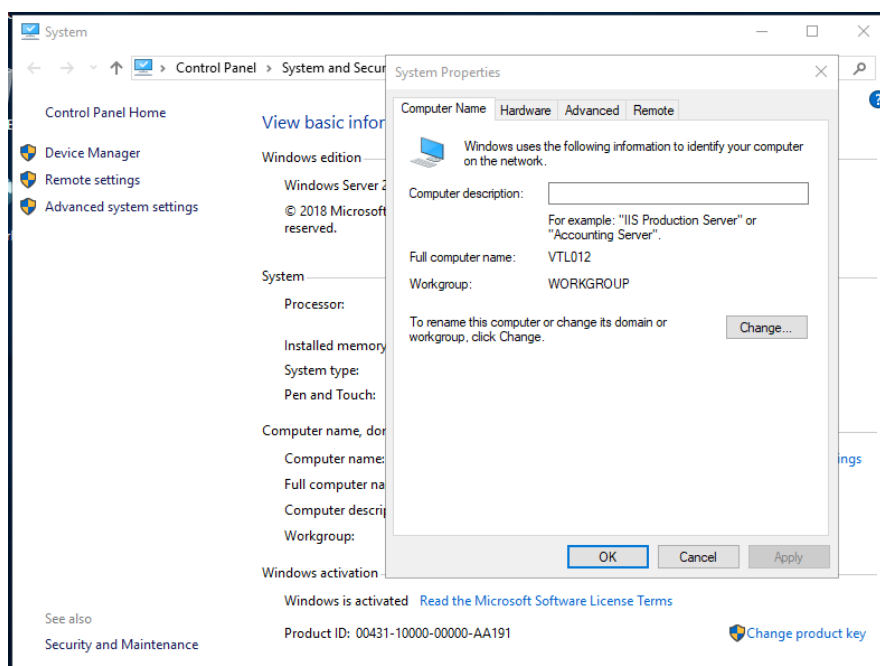
3.1.3 Kết luận

- Cài đặt thành công hệ điều hành Windows Server 2019 trên máy ảo VMWare .

3.2 Nâng cấp Server thành Domain Controller

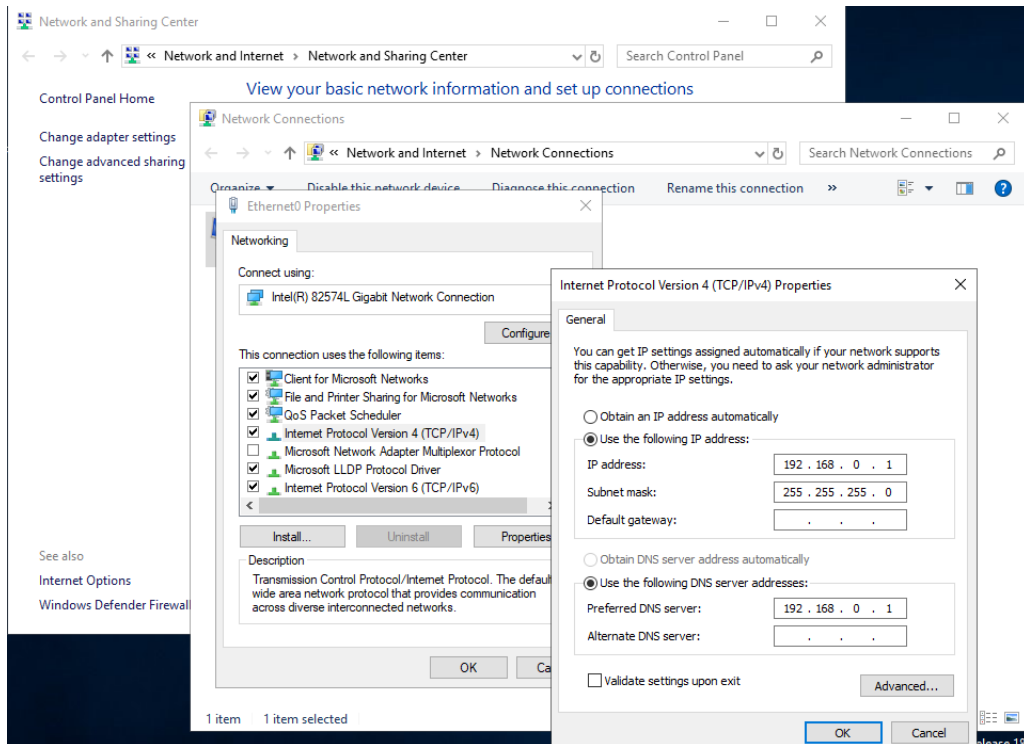
3.2.1 Kiểm tra tên của server

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

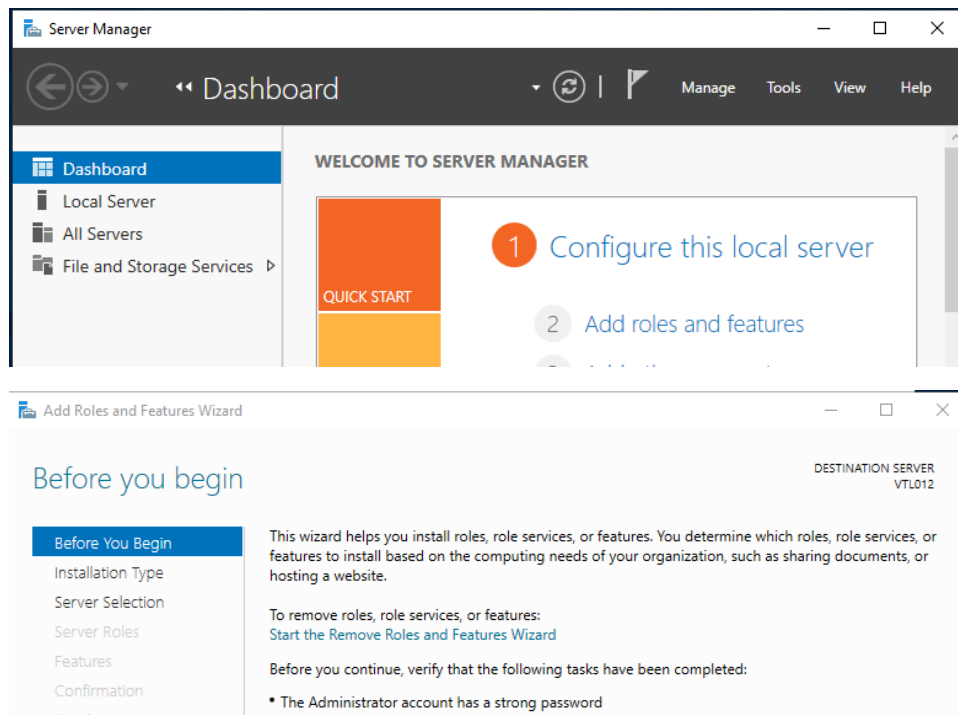


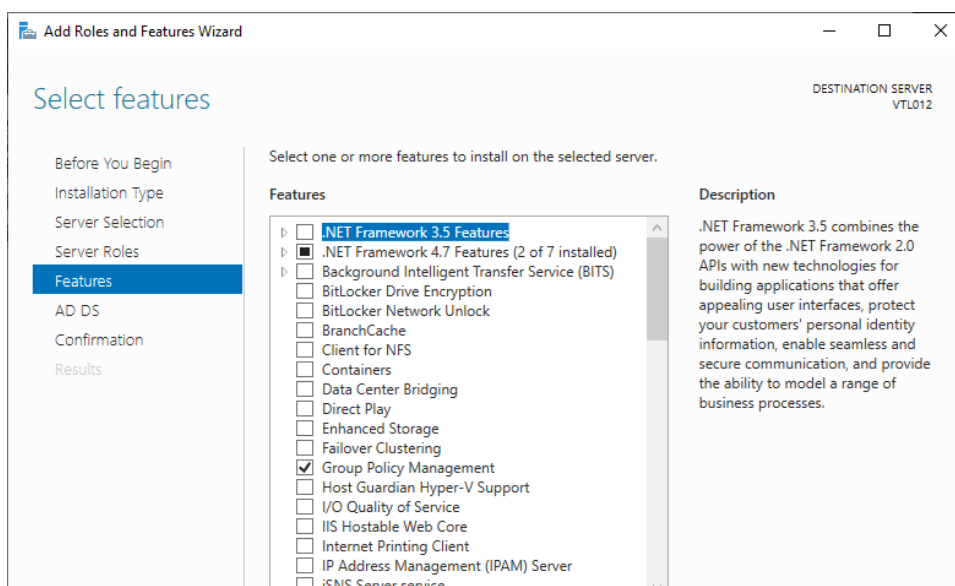
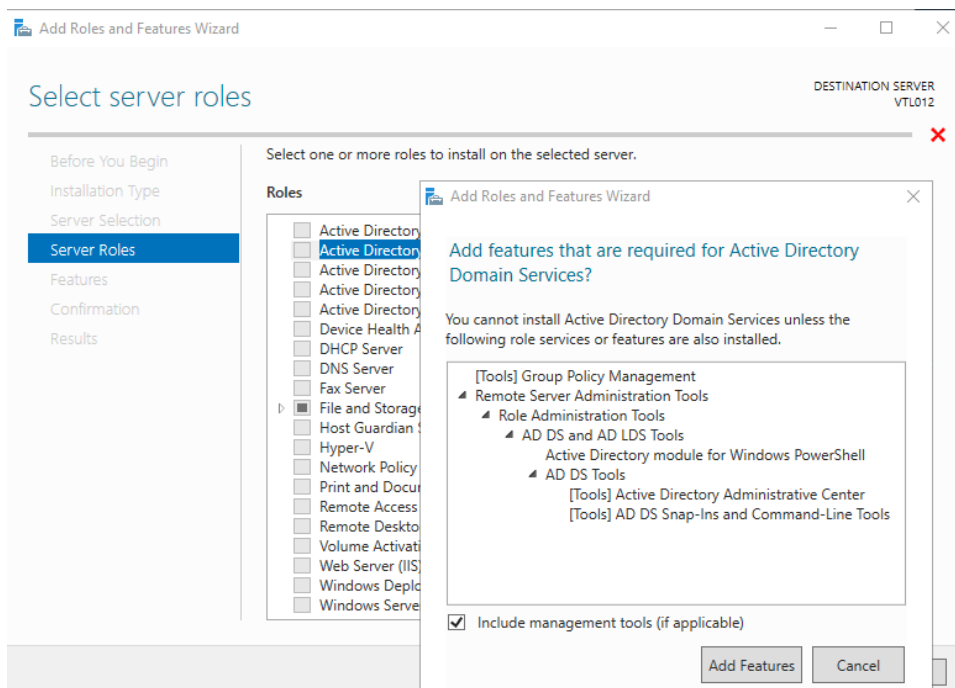
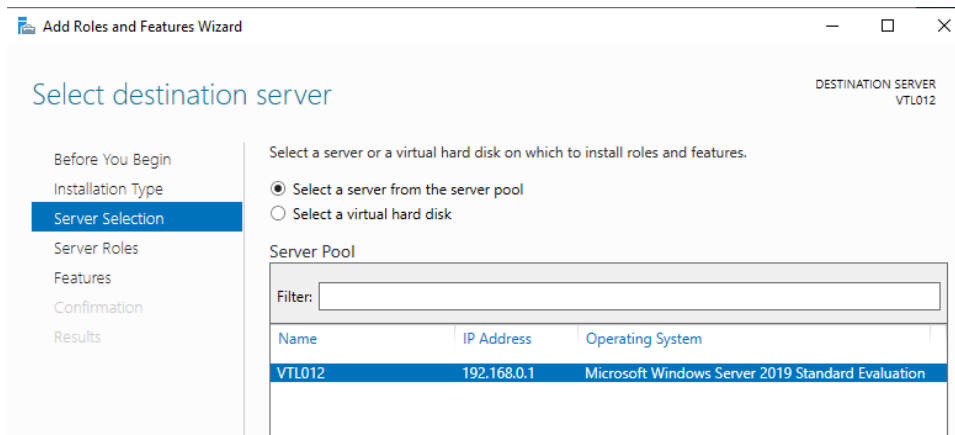
3.2.2 Cài đặt static IP

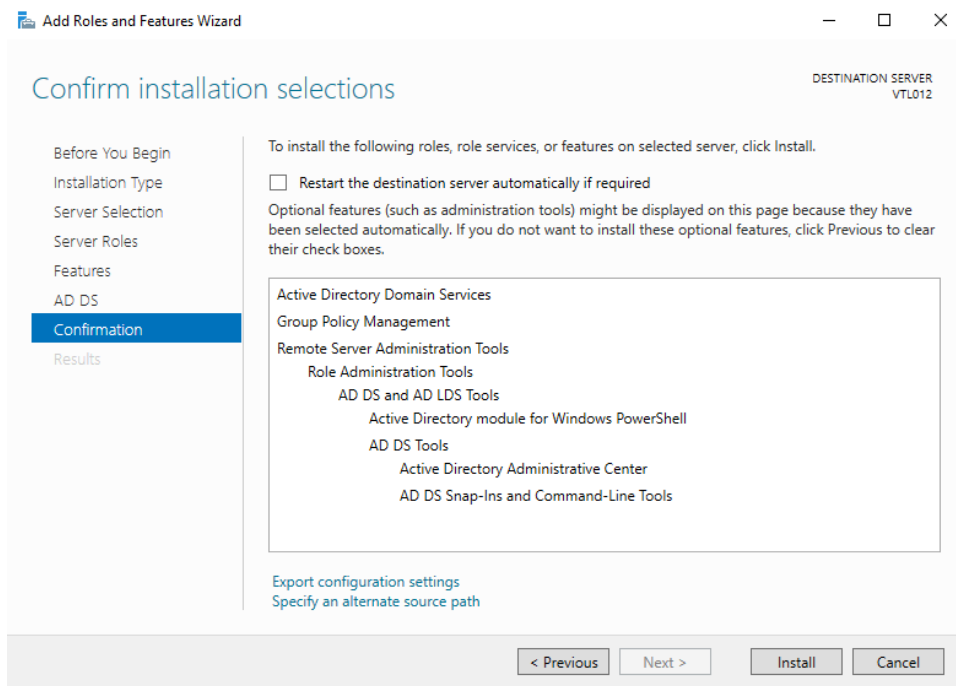
Open Network and Sharing Center (Chuột phải) → Change Adapter Settings
→ Ethernet0 (Chuột phải) → Properties → Internet Protocol Version 4 (TCP/IP)
Properties → Use the following IP address → Restart.



3.2.3 Cài đặt server role trong Server Manager

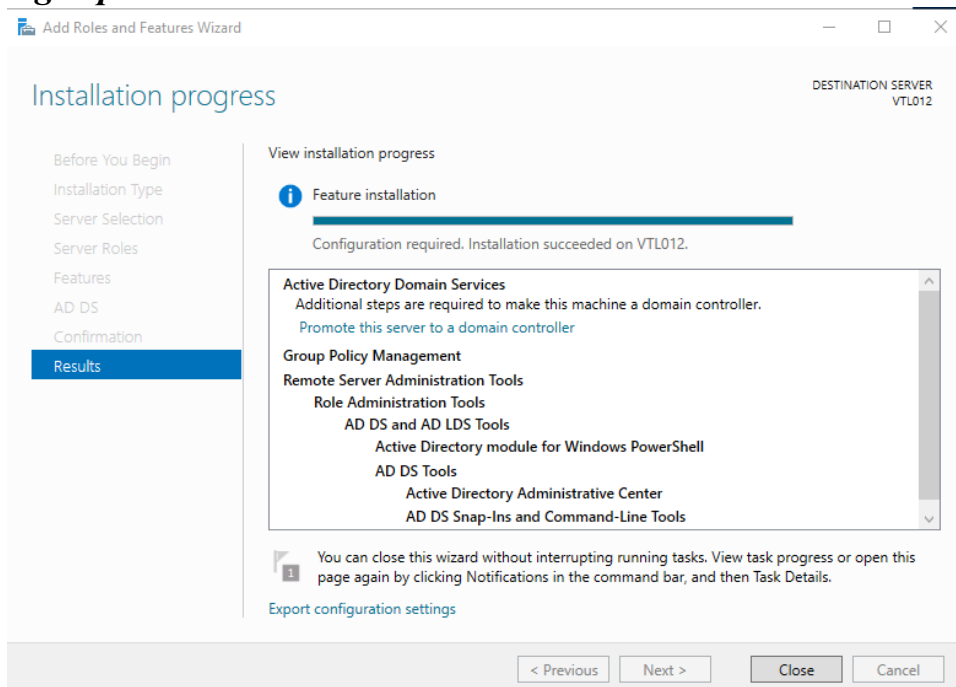


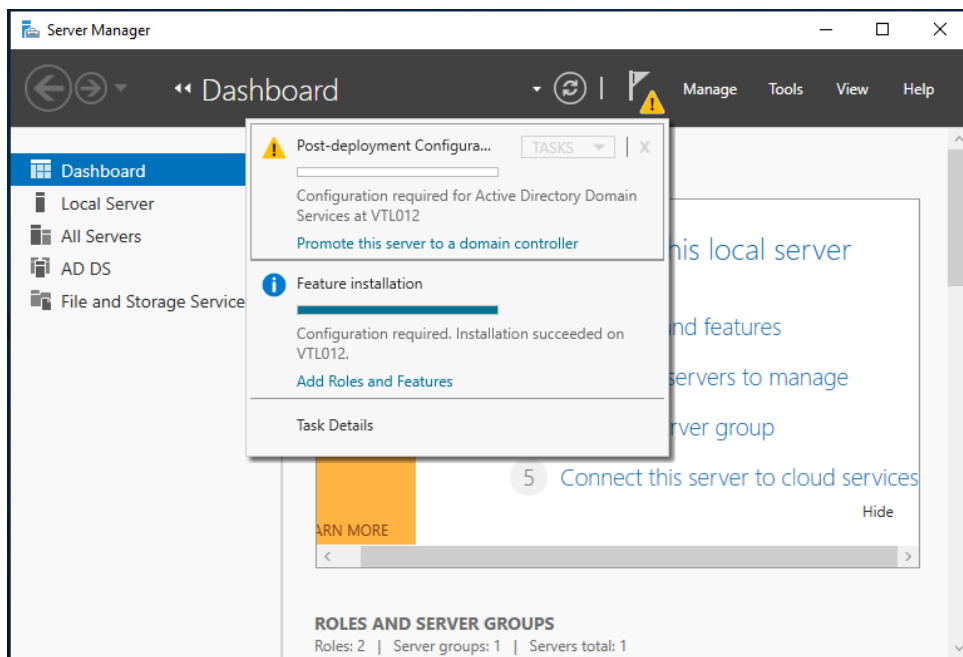




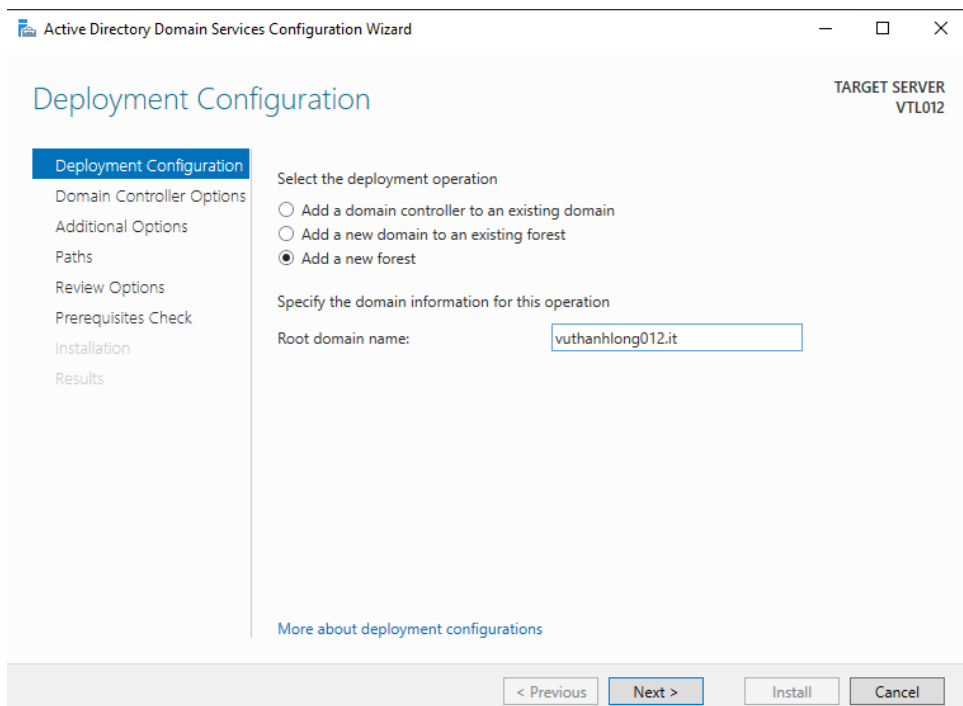
Đây chưa hẳn đã là cài đặt Active Directory → Nó chỉ cài đặt role, cho phép chúng ta nâng cấp server thành Domain Controller.

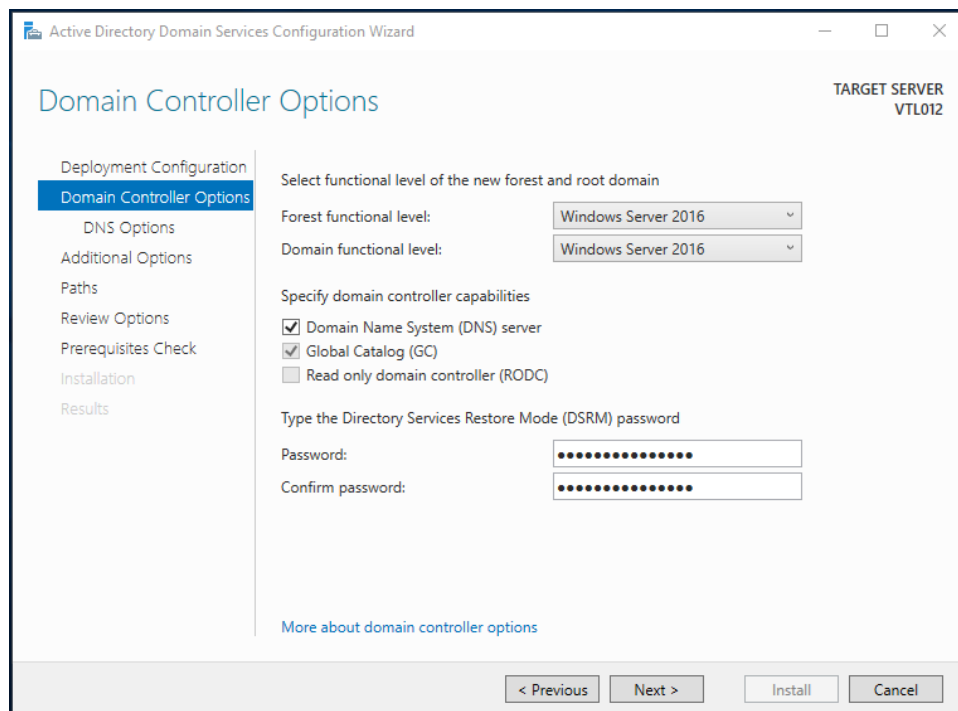
3.2.4 Nâng cấp Server thành Domain Controller



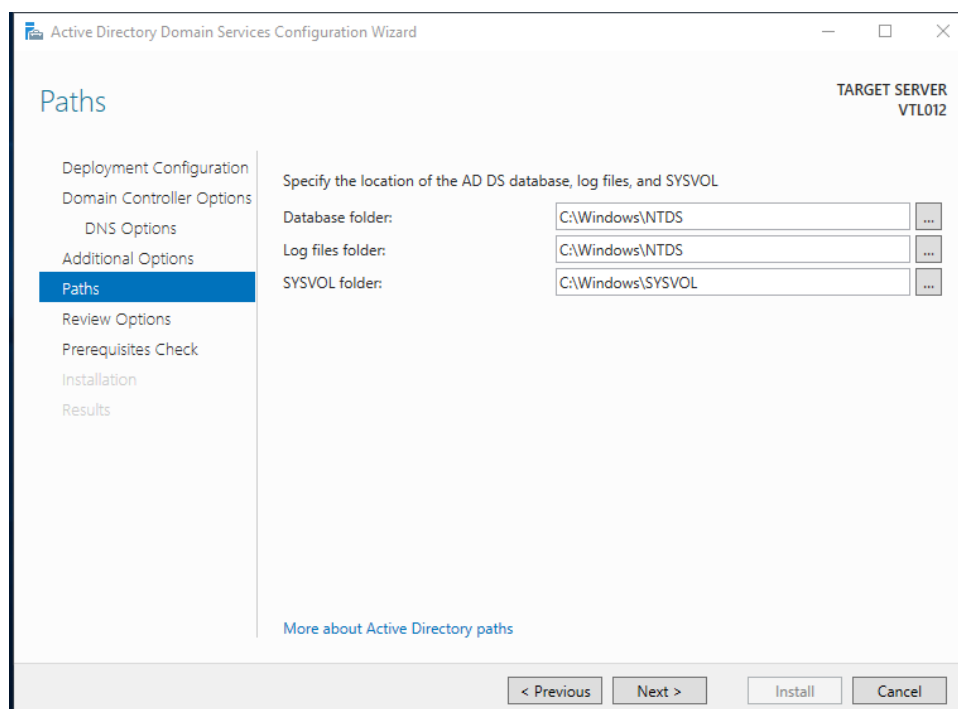


Nếu bạn tắt cửa sổ trước khi promote, thì có thể chọn biểu tượng lá cờ (notifications) trong server manager → Promote this server to a domain controller.

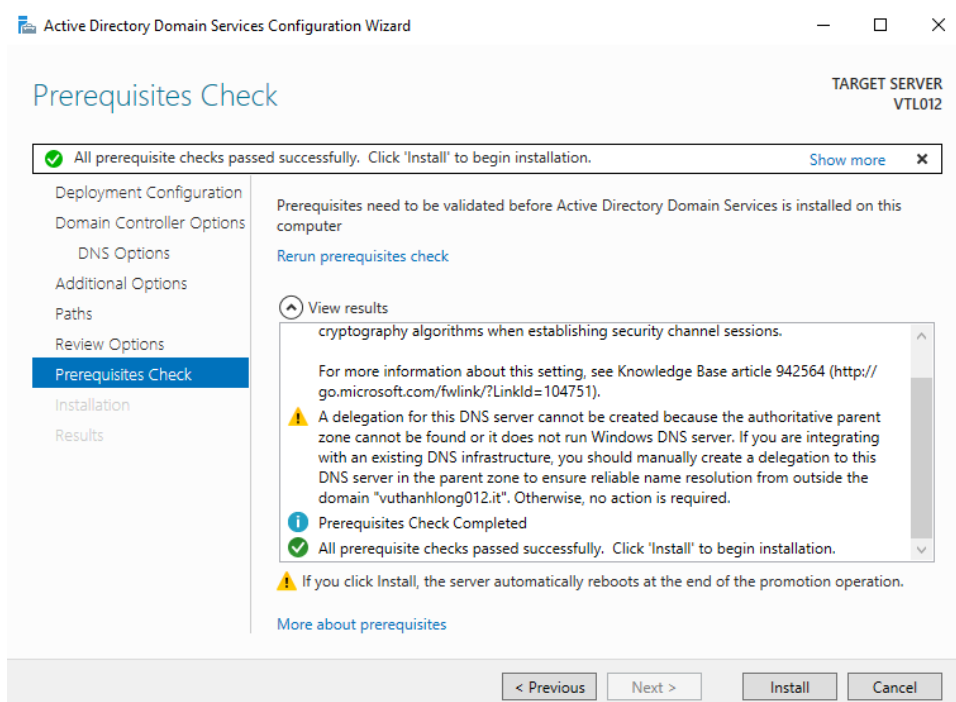




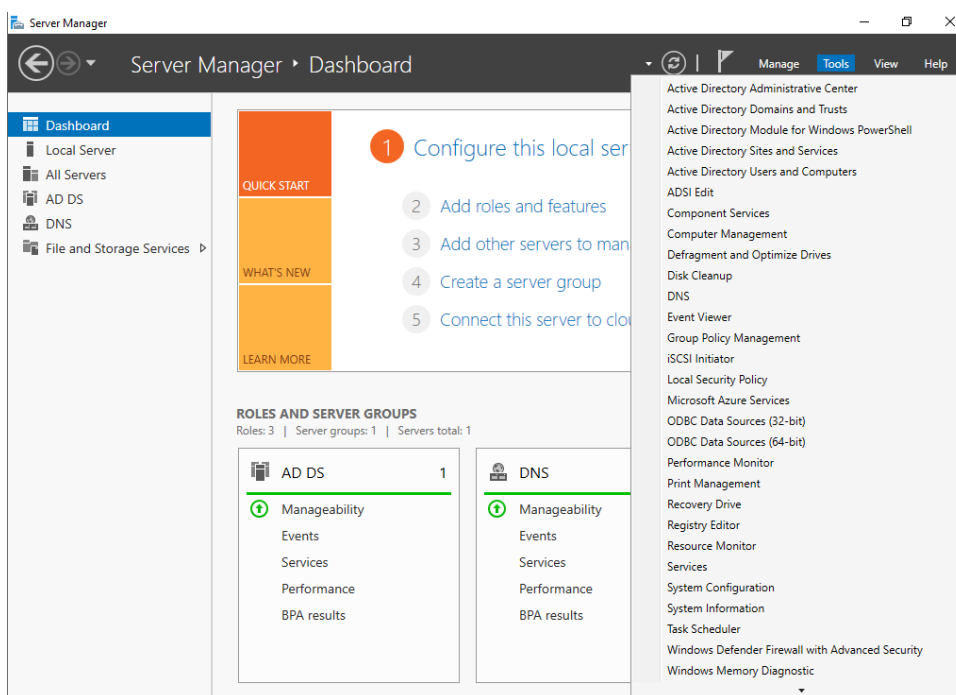
Lưu ý: Bỏ qua cảnh báo về DNS option và chọn tên NETBIOS (Chọn Next)



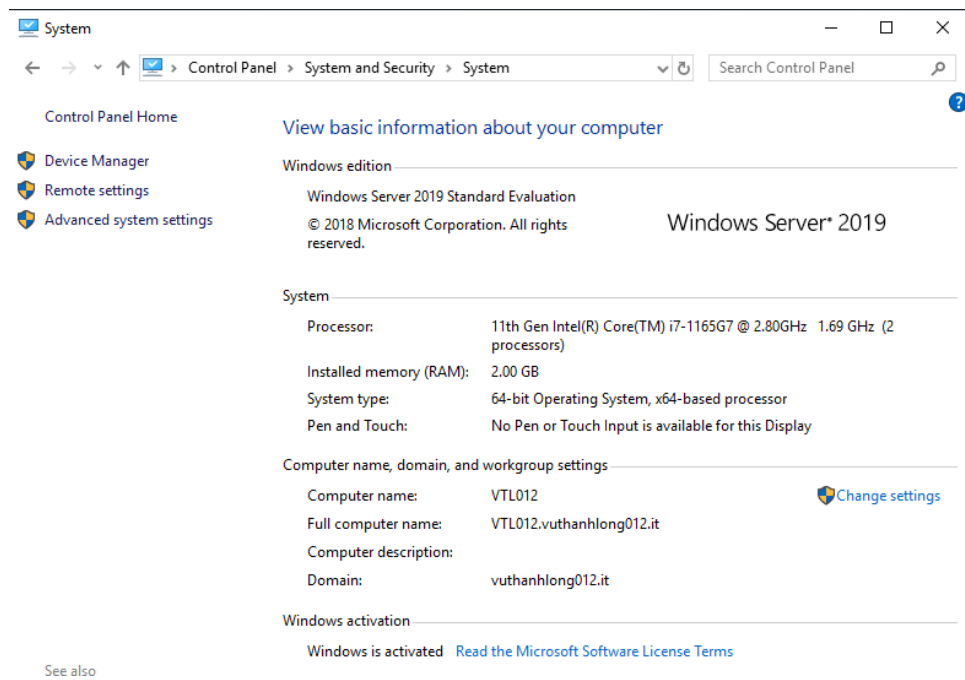
Đây là bước lựa chọn vị trí lưu trữ các database. Sau bước này sẽ đến phần review options (Chọn Next)



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.



Kiểm tra trong hệ thống máy đã thay đổi domain.

3.3 Kết luận

- Nâng cấp thành công máy Windows Server thành DC