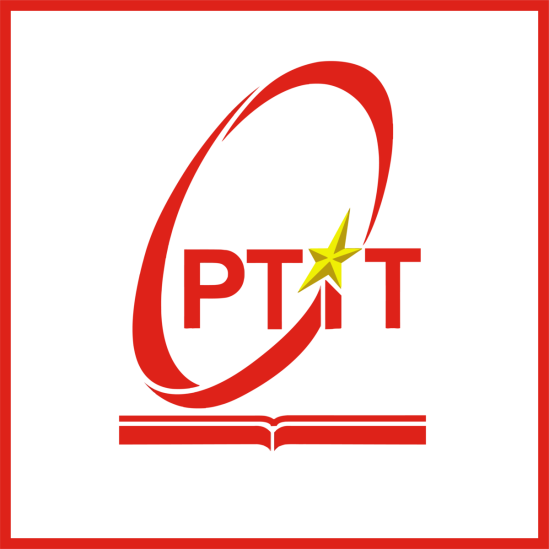
**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA CÔNG NGHỆ THÔNG TIN 1**



Môn: HỆ ĐIỀU HÀNH WINDOWS VÀ LINUX/UNIX

**BÁO CÁO BÀI THỰC HÀNH SỐ 2**

Họ và tên sinh viên:

Đỗ Tiến Sĩ

Mã số sinh viên:

B20DCAT153

Họ và tên giảng viên:

TS. Đinh Trường Duy

I. Giới thiệu chung.

1. Mục đích:

- Tạo được một máy chủ Windows Server với chức năng Domain.

2. Mô tả lý thuyết:

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**

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 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 đươc điều khiển bởi User-Mode 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 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. Từ đó, 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.

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 đươc 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.

- Lớp Kernel: 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:

* 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:**

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.

\* Use mode bao gồm các application processes mà thường là các chương trình Windows 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 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: tâp 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) và Kernel Object. Kernel Object

+ Không hiển thị trong Code ở User mode.

+ 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 tiển 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.

**2.4. Domain Controller**

Miền (Domain) là đơn vị lô-gíc các máy tính và tài nguyên mạng xác định ranh giới an ninh. Miền sử dụng một cơ sở dữ liệu miền động đơn lẻ để chia sẻ thông tin chung về an ninh và người dùng cho phép quản lý tập trung toàn bộ người dùng, nhóm và tài nguyên mạng.

Trong mỗi miền của thư mục động có máy chủ đặc biệt gọi là máy chủ miền (Domain controller) chịu trách nhiệm lưu bản sao thông tin tài khoản và an ninh của miền. Để chống lỗi có thể sử dụng nhiều máy chủ miền. Tất cả các máy chủ miền trong một miền nhận các thay đổi và sao chép các sửa đổi này vào phần miền được lưu trong toàn bộ các máy chủ còn lại. Kết quả, tất các các máy chủ miền đều ngang hàng với nhau và cùng quản lý việc sao lưu.

Máy chủ danh mục toàn cục (global catalog) là máy chủ miền lưu bản sao đầy đủ của toàn bộ các đối tượng của thư mục động của miền mà máy chủ hoạt động. Các ứng dụng và người dùng truy vấn danh mục toàn cục để xác định bất kỳ đối tượng nào trong thư mục động. Danh mục này được tạo ra một các tự động khi cài đặt máy chủ miền đầu tiên.

Máy chủ miền chỉ đọc là máy chủ miền đặc biệt dùng cho các nhánh phòng ban của tổ chức và các máy chủ đặt trong môi trường an ninh kém. Máy chủ miền này chỉ lưu trữ bản sao không sửa được của thư mục động.

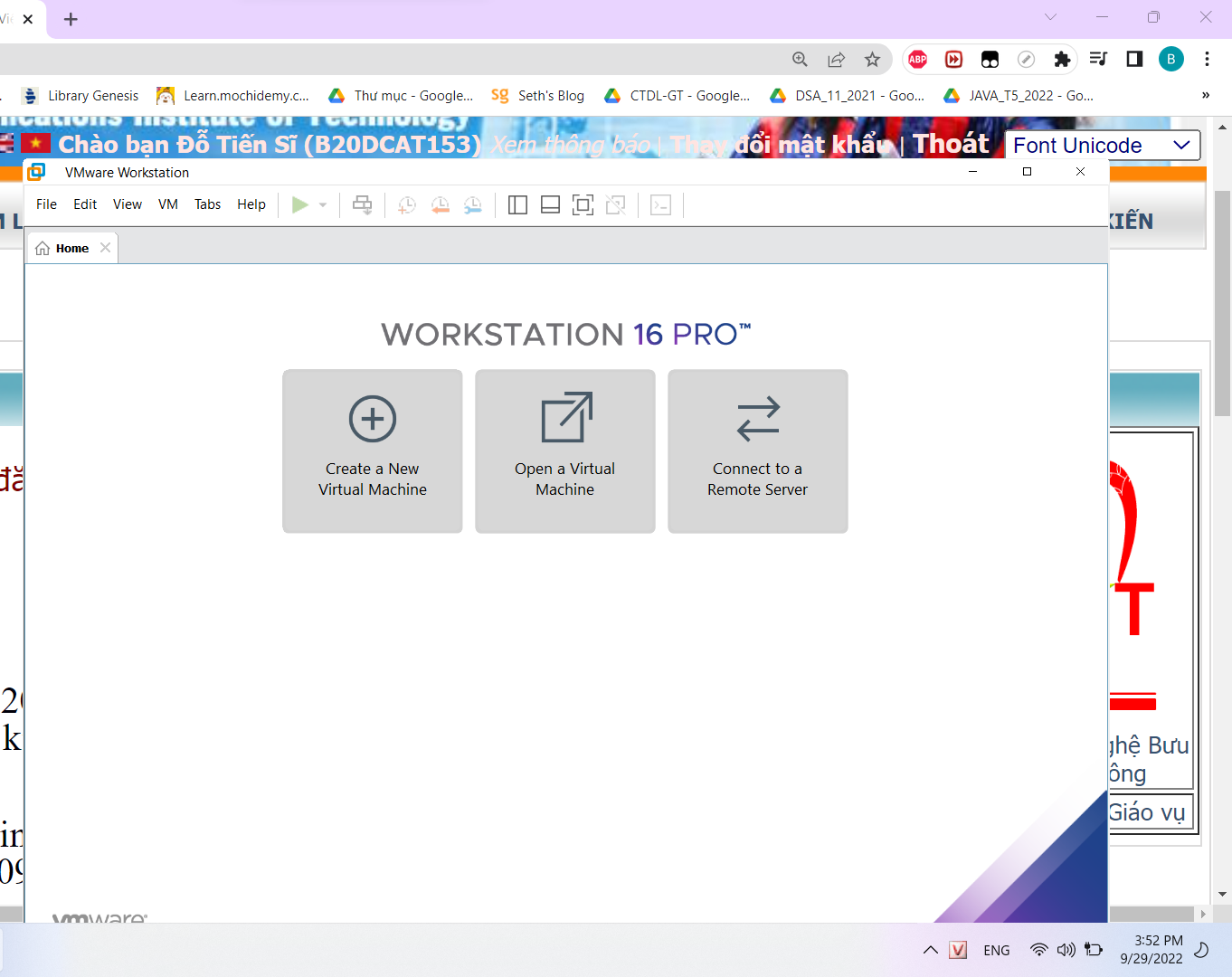
Máy chủ miền duy trì danh mục toàn cục (Global catalog) chứa đựng thông tin của từng đối tượng trong cây và rừng. Danh mục toàn cục giúp truy nhập các đối tượng giữa các miền khác nhau cũng như lưu các thuộc tính được tìm kiếm thường xuyên như tên người dùng, tên máy tính. Danh mục này được tự động tạo ra khi triển khai máy chủ miền đầu tiên của rừng (forest). Mặt khác danh mục toàn cục được dùng khi người dùng đăng nhập giúp liệt kê thành viên nhóm và xác định định danh người dùng.

Miền thư mục động (Active Directory Domain Services): Lưu thông tin về người quản trị, máy tính và các thiết bị khác trong mạng. Ngoài ra, dịch vụ này giúp người quản trị quản lý các thông tin trên an toàn và làm thuận tiện cho việc chia sẻ và phối hợp giữa các người quản trị.

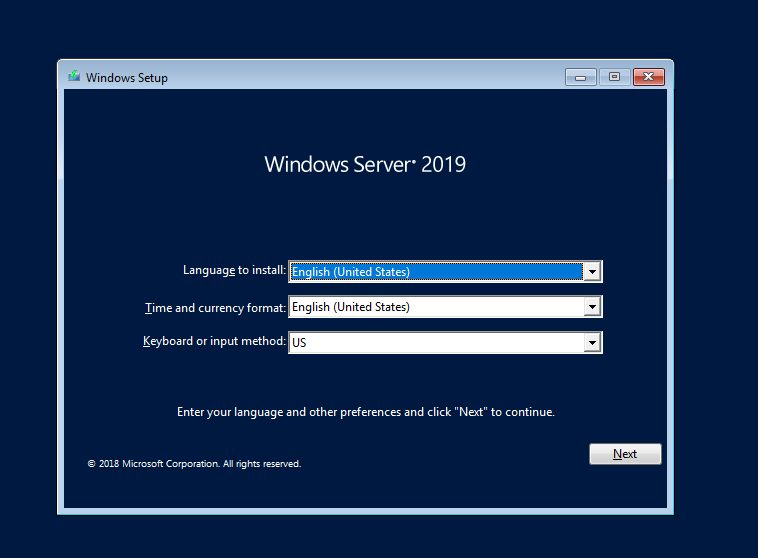
**II. Các bước thực hành.**

1. **Cài đặt hệ điều hành Windows Server 2019**
2. Trên VMware Workstation:

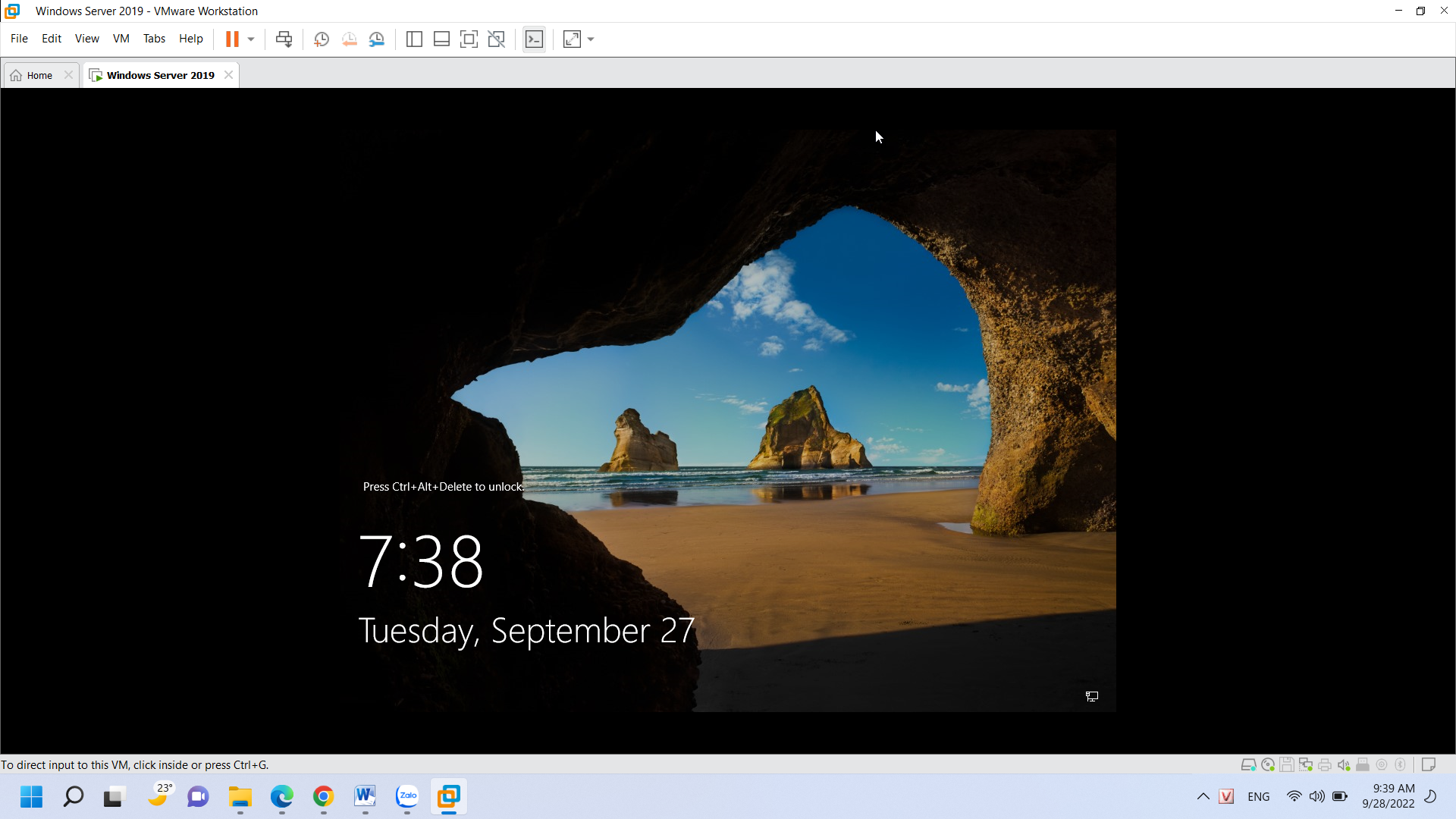
* Sau khi cài chương trình VMware Workstation, ta khởi động chương trình, giao diện chính sẽ hiện ra như hình dưới đây:



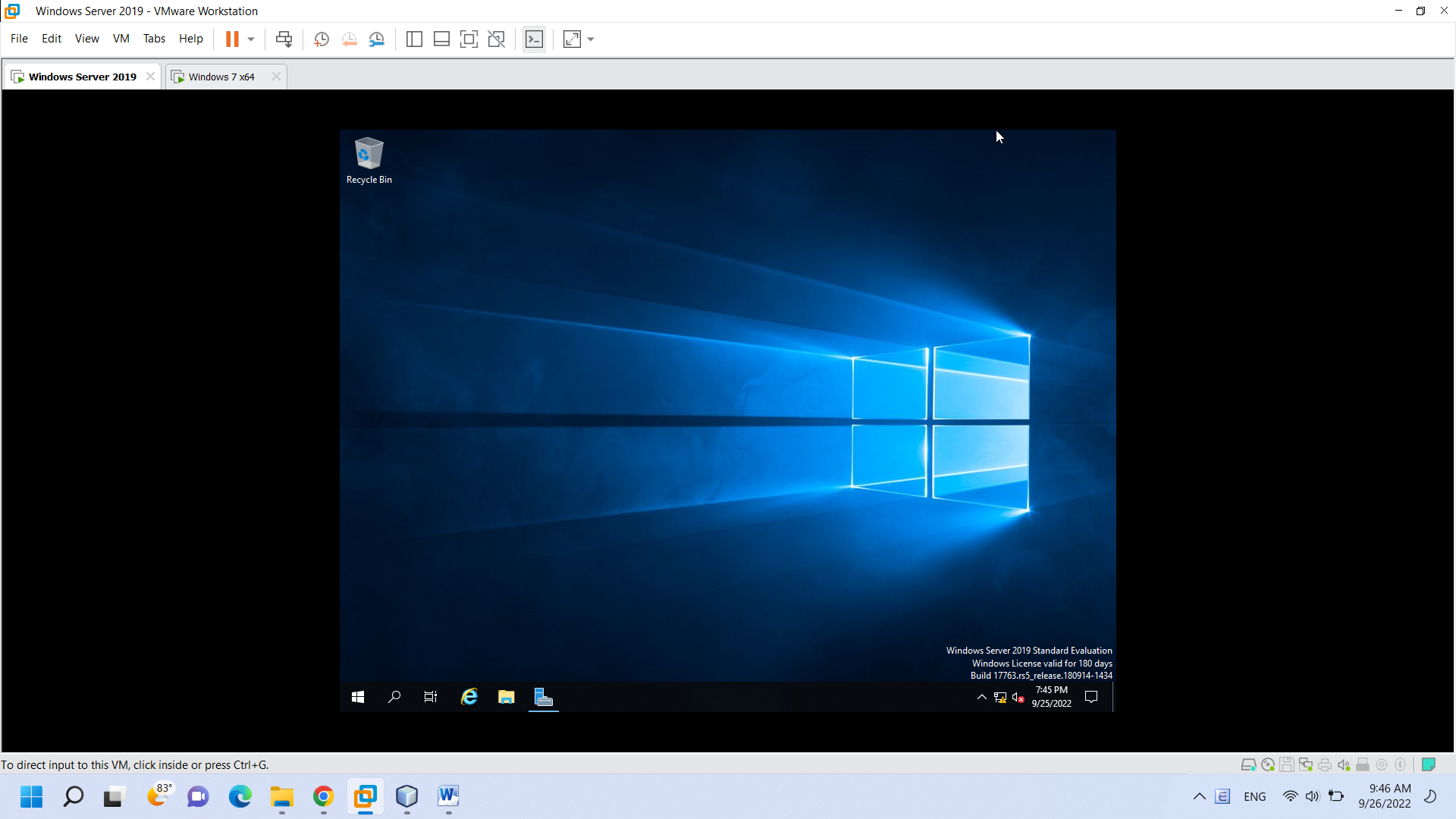
Sau một số bước cài ta được giao diện cài đặt của window server 2019



* Sau quá trình cài đặt ta được giao diện đăng nhập:



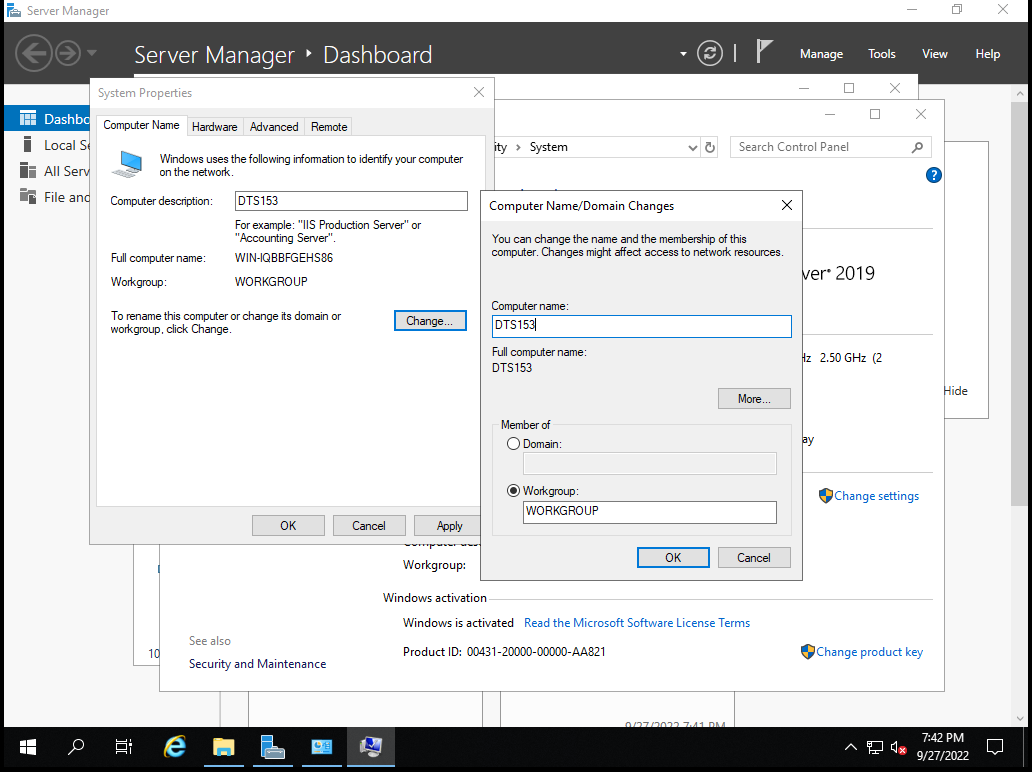
* Giao diện chính của window server 2019



1. Nâng cấp Server thành Domain Controller

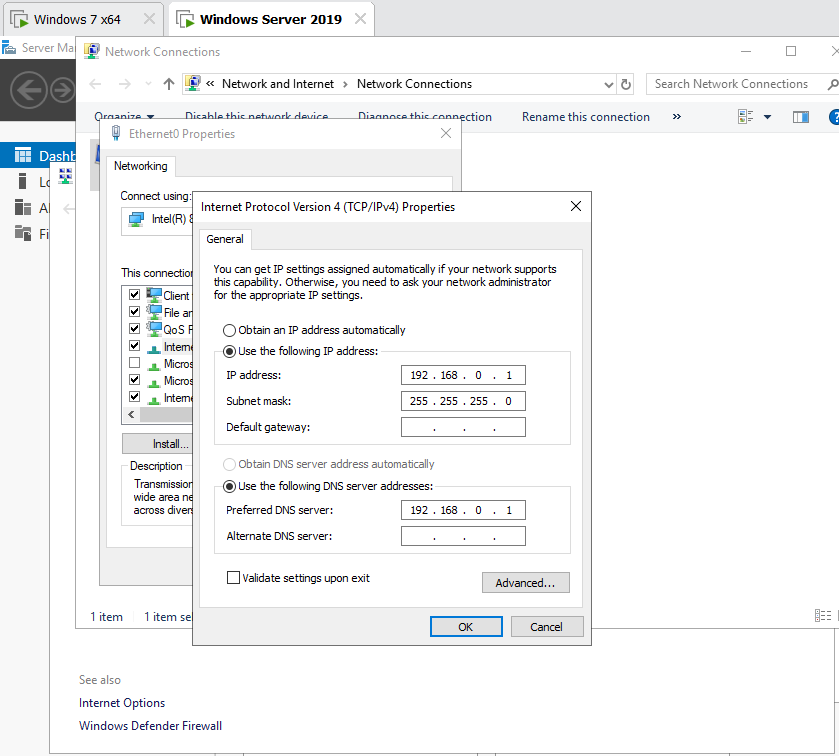
a, kiểm tra tên của Server

This PC (chuột phải) → Properties Advanced System Setting → Computer Name → Thay đổi tên (Change).

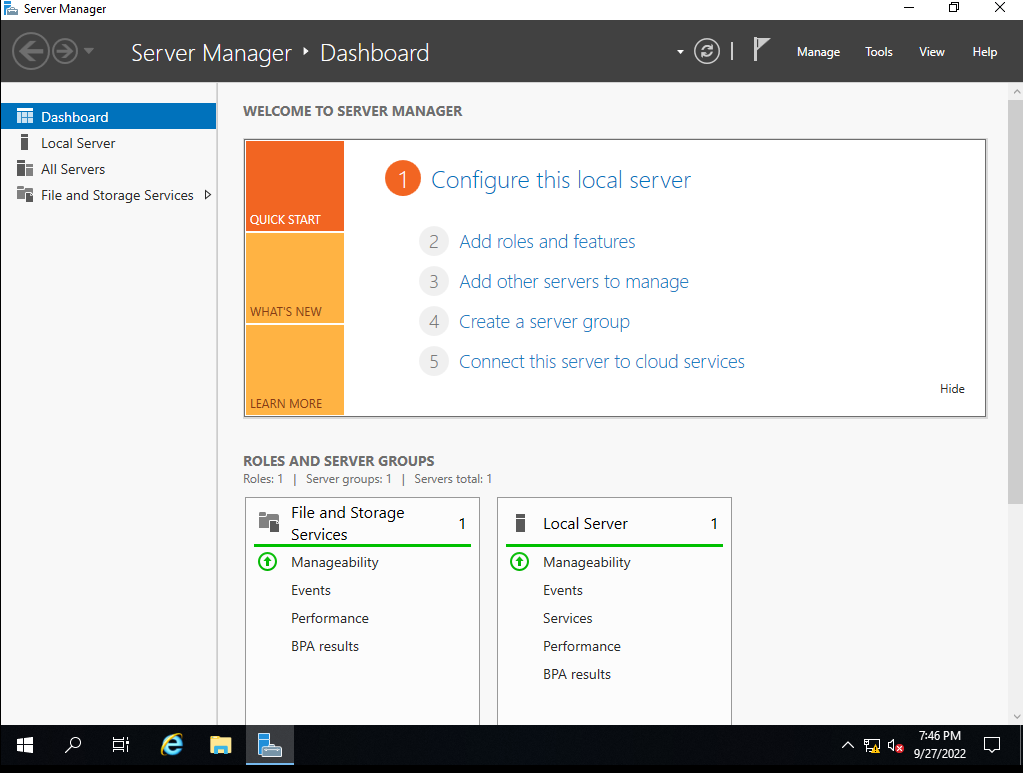


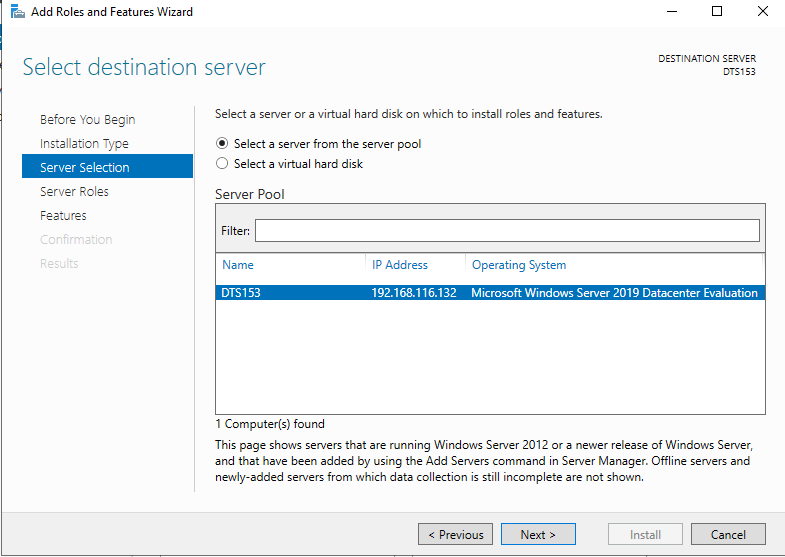
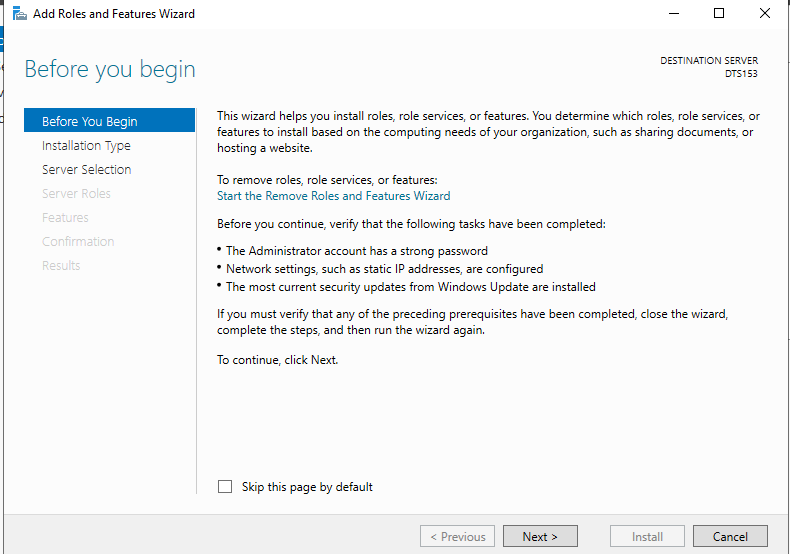
Đổi tên thành công

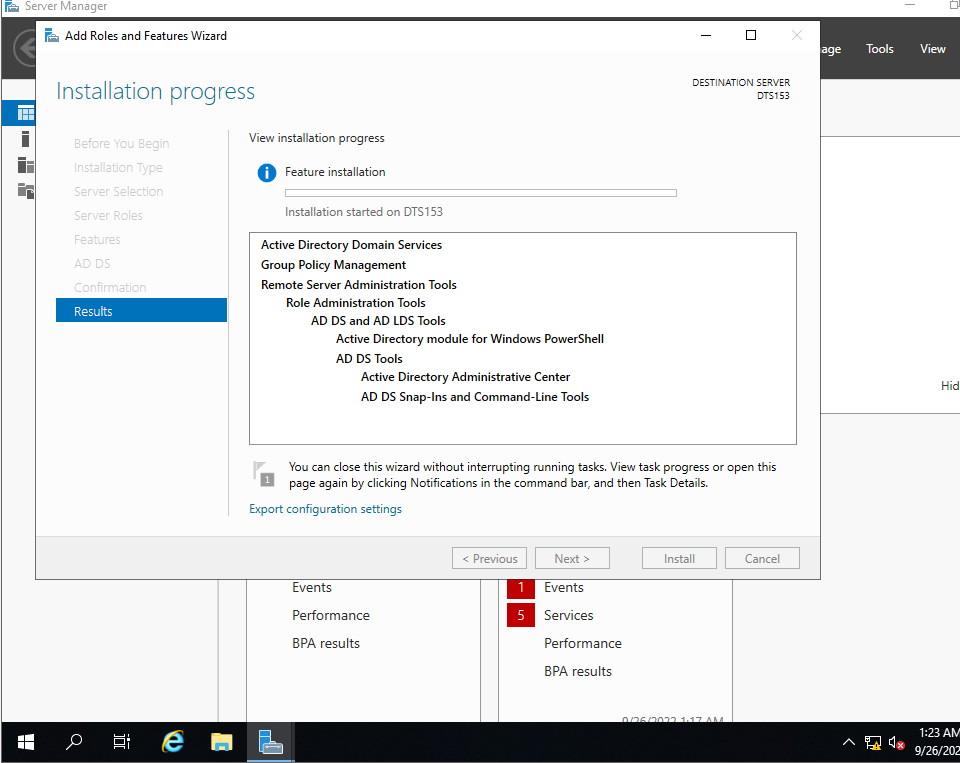
b, Cài đặt Static IP Open Network and Sharing Center (Chuột phải) → Change Adapter Settings → Ethernet0 (Chuột phải) → Properties → Internet Protocol Version 4 (TCP/IP) → Properties → Use the following IP address → Restart



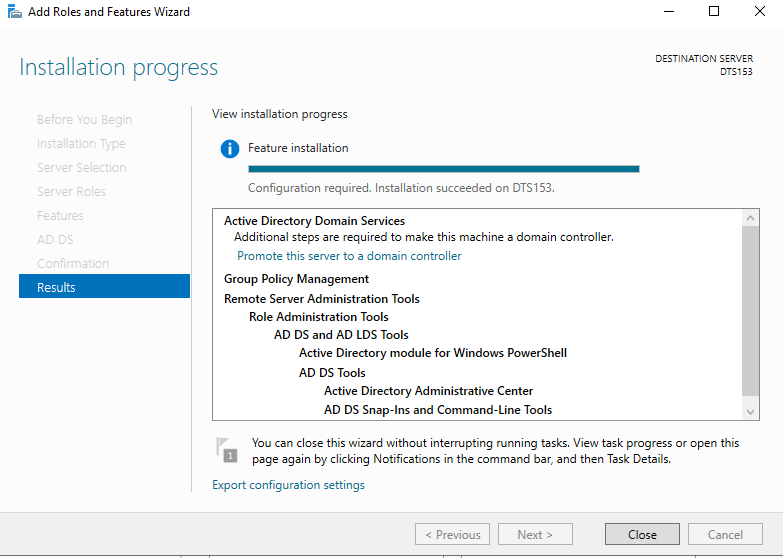
c, cài đặt server role trong server manager.

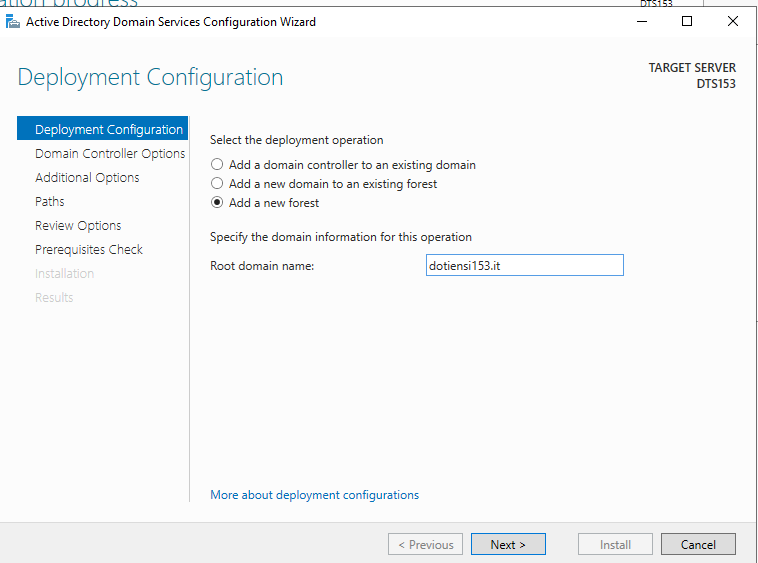




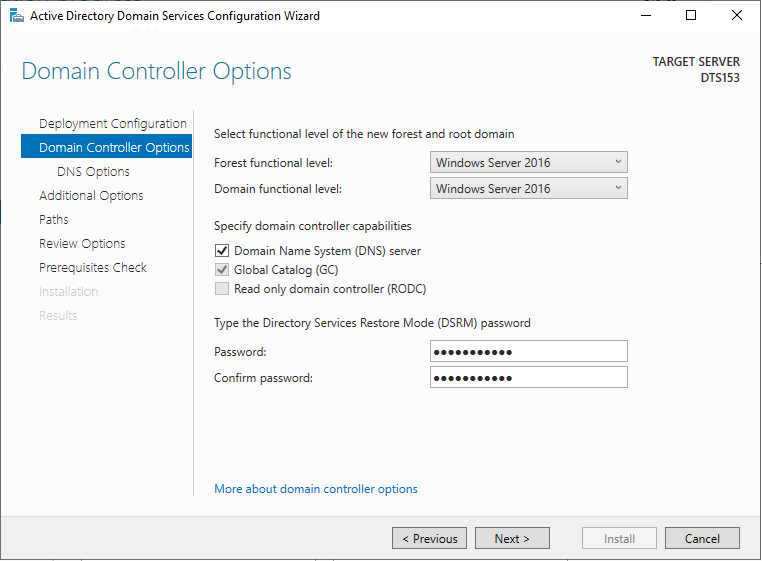


d, nâng cấp server thành domain controller

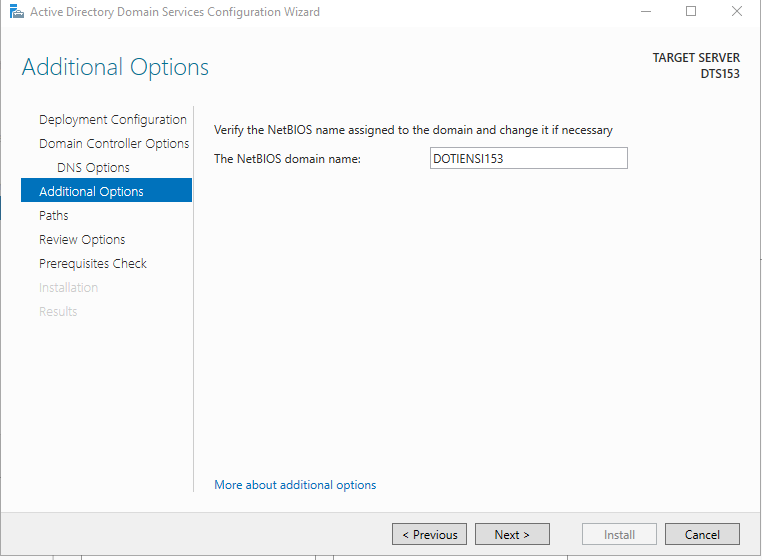


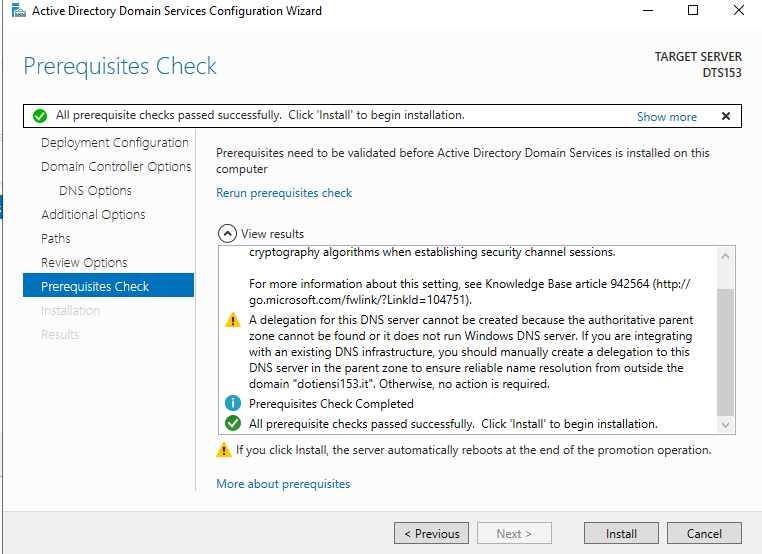
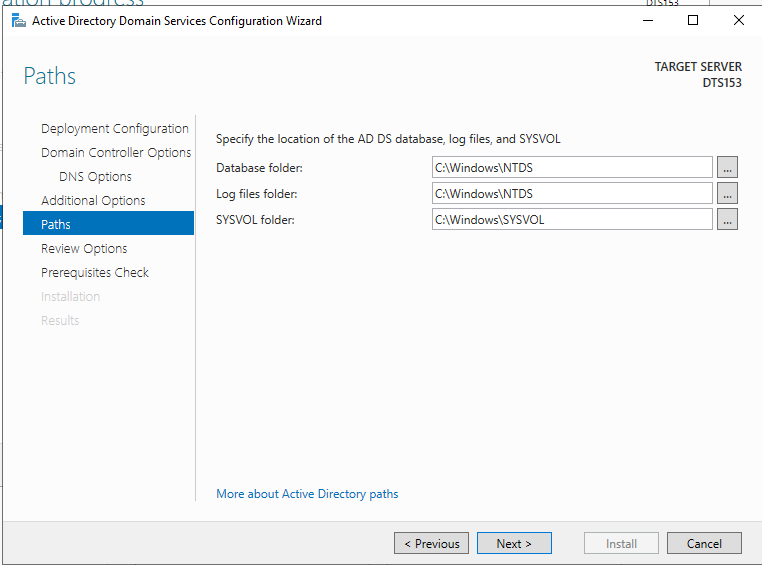


* Đặt tên cho domain name dotiensi153.it

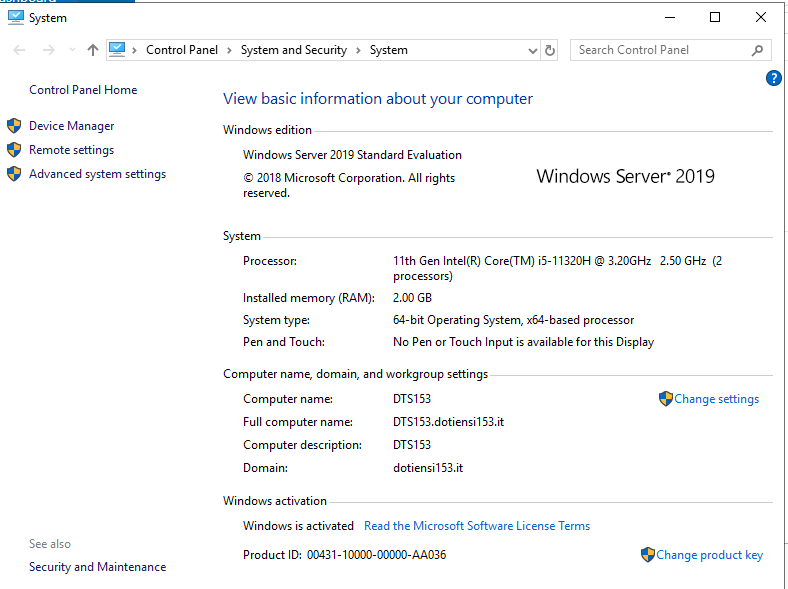


* Cài dặt mật khẩu.





* Ta kiểm tra trong hệ thống máy tính.



**Kết quả: nâng cấp thành công window serve thành Domain Controller**