**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**

CÀI ĐẶT WINDOW SERVER VÀ DỊCH VỤ THƯ MỤC ACTIVE DIRECTORY TRONG WINDOW SERVER

Họ và tên sinh viên: Lê Anh Tuấn

Mã số sinh viên: B21DCAT205

Họ và tên giảng viên: TS. Đinh Trường Duy

Hà Nội 9 năm 2023

MỤC LỤC

[I. GIỚI THIỆU BÀI THỰC HÀNH 3](#_Toc145970116)

[1. Mục đích 3](#_Toc145970117)

[2. Yêu cầu 3](#_Toc145970118)

[II. CƠ SỞ LÝ THUYẾT 3](#_Toc145970119)

[1. Kiến trúc của Windows server 3](#_Toc145970120)

[1.1 Kiến trúc chung của windows 4](#_Toc145970121)

[1.2 Kiến trúc Windows NT: 5](#_Toc145970122)

[1.3 Kiến trúc Windows server 2003: 7](#_Toc145970123)

[2. Dịch vụ thư mục Active Directory 13](#_Toc145970124)

[a) Active Directory Objects 13](#_Toc145970125)

[b) Active Directory Schema 13](#_Toc145970126)

[c) Active Directory Components 13](#_Toc145970127)

[3. Domain Controller 14](#_Toc145970128)

[*a)* Domain Controller là gì? 14](#_Toc145970129)

[*b)* Chức năng và vai trò của Domain controller 14](#_Toc145970130)

[*c)* Nguyên tắc hoạt động của DC 14](#_Toc145970131)

[*d)* Cách triển khai Domain controller 14](#_Toc145970132)

[III. THỰC HÀNH 15](#_Toc145970133)

[1. Chuẩn bị môi trường 15](#_Toc145970134)

[2. Thực hành cài máy ảo 15](#_Toc145970136)

[ *Cài đặt Windows server 2019* 15](#_Toc145970137)

[ Nâng cấp Sever thành Domain Controller 23](#_Toc145970138)

# GIỚI THIỆU BÀI THỰC HÀNH

* 1. **Mục đích**

Giúp sinh viên có thể tự tạo một máy chủ Windows Server với chức năng Domain

* 1. **Yêu cầu**

Sinh viên đã nắm được nội dung lý thuyết.

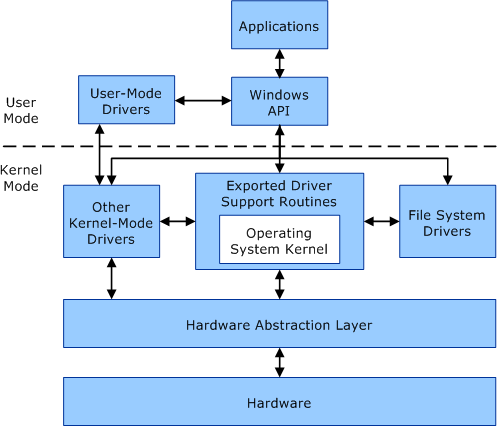
# CƠ SỞ LÝ THUYẾT

* 1. **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. **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 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

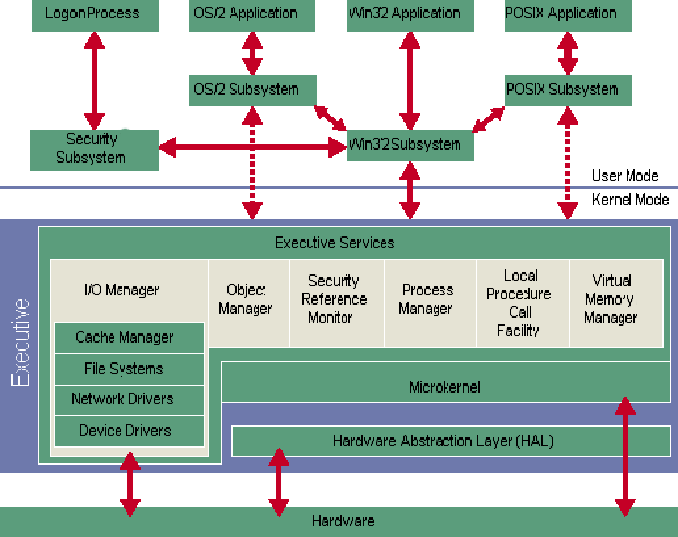
* 1. **Kiến trúc Windows NT:**

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 nguyêntrên hệ thống máy tính.

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

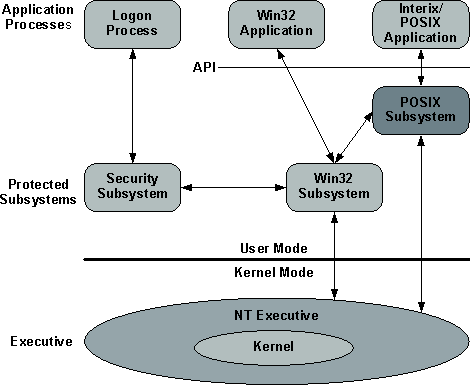
Hệ thống con (Subsystem) Win 32 và các hệ thống con về môi trường, chẳng hạn như DOS/Win 16.0S/2 và hệ thống con POSIX chạy dưới chế độ user. Bằng cách đặt các hệ thống con này trong chế độ user, các nhà thiết kế Windows NT có thể hiệu chỉnh chúng dễ dàng hơn mà không cần thay đổi các thành phần được 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 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. 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)
  1. **Kiến trúc Windows server 2003:**



Hình 3: Kiến trúc cơ bản của Windows server 2003

- Kiến trúc cơ bản:

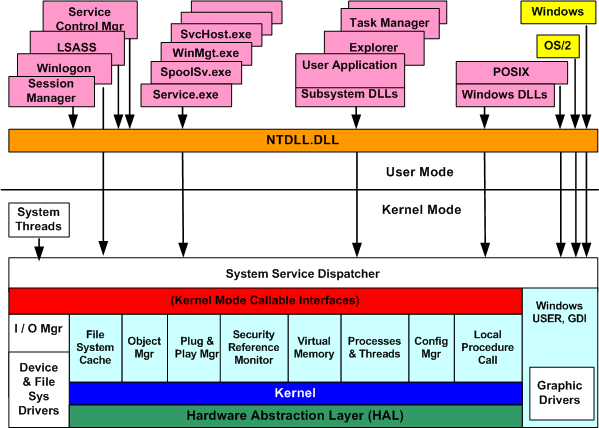
Cũng tương tự như kiến trúc cơ bản windows, kiến trúc Windows server 2003 gồm 2 mode: user mode và kernel mode.

* Use mode bao gồm các application processes mà thường là các chương trình Windows (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 lâp 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 chuân 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).

- 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: 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.

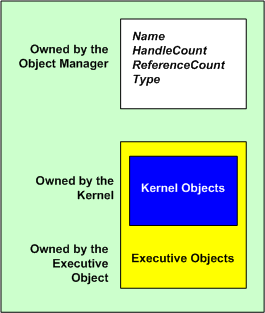
Những phần chính:

* 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

***Hình 5: Windows Object***



* Executive Object (EO)
* 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 trườnghợp

* + 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

o 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.

* 1. **Dịch vụ thư mục Active Directory**

[**Active Directory**](https://fptcloud.com/active-directory/) là 1 kiến trúc độc quyền trên thị trường của Microsoft. Theo đó nó là 1 kiến trúc không thể nào thiếu trên Windows Server và có thể được hiểu là 1 dịch vụ thư mục. Đặc biệt nó có khả năng quản trị và tập trung hoàn hảo người dùng, những nguồn tài nguyên trong cùng hệ thống mạng.

Một máy chủ nếu như chạy AD DS - Active Directory Domain Service sẽ gọi là domain controller. Theo đó nó sẽ ủy quyền và xác thực cho toàn bộ máy tính cũng như người dùng trong mạng loại Windows gán, thực thi những chính sách về bảo mật cho toàn bộ những cài đặt, máy tính hay cập nhật phần mềm. Cấu trúc 3 phần của Active Directory

### Active Directory Objects

Dữ liệu trong Active Directory ví dụ thông tin users, database, groups, computers, security policies, máy in và server sẽ được tổ chức như những objects (đối tượng). Mỗi một object sẽ có các thuộc tính riêng và đặc trưng cho một object đó.

Cụ thể ví dụ object user có những thuộc tính liên quan như Logon Name, First Name, Last Name,... và Computer Object có những thuộc tính ví dụ như computer name cùng description.

Theo đó một số những object đặc biệt gồm có nhiều object khác nhau bên trong sẽ gọi là những “container”, ví dụ domain là 1 container gồm có nhiều computer account và user.

### Active Directory Schema

Database lưu trữ trong Active Directory, chính là AD Schema. Theo đó Schema sẽ định nghĩa những đối tượng lưu trữ trong Active Directory. Tuy nhiên Schema sẽ lưu trữ những đối tượng như thế nào?

Schema thực chất là 1 danh sách những định nghĩa xác định những loại đối tượng cũng như những loại thông tin liên quan tới đối tượng lưu trữ thuộc Active Directory. Schema về bản chất cũng được lưu trữ tương tự như một object.

#### **Schema Class objects**

Schema Class objects có chức năng tương tự như 1 template tạo mới những đối tượng trong AD. Mỗi một Schema Class là 1 tập hợp những thuộc tính của đối tượng. Nếu như tạo 1 đối tượng thuộc về 1 loại Schema Class thì khi đó Schema Attribute sẽ tiến hành lưu trữ những thuộc tính trong đối tượng đó tương ứng loại Schema Class trong đối tượng.

#### **Schema Attribute**

Là định nghĩa những Schema Class tương ứng cùng với nó. Mỗi một thuộc tính theo đó chỉ được định nghĩa 1 lần trong Active Directory và đồng thời có thể thuộc nhiều những Schema Class với quan hệ 1 nhiều (1-m).

1 tập hợp những Schema Attribute và Schema Class mặc định được đóng gói sẵn chung cùng **Active Directory**. Nhưng Schema trong Active Directory đã mở ra 1 khả năng về phát triển mở rộng những Schema Class trên những Attribute có sẵn hoặc tạo mới những Attribute Schema.

### Active Directory Components

Trong một mô hình mạng doanh nghiệp hiện nay, những components của Active Directory đang được sử dụng cũng như áp dụng nhằm xây dựng nên những mô hình phù hợp cho nhu cầu của những doanh nghiệp. Nếu như xem xét về mô hình kiến trúc AD sẽ phân làm hai loại là Logical và Physical.

#### **Logical Structure**

Trong AD hiện tại việc tổ chức tài nguyên sẽ dựa theo cơ chế là Logical Structure và được ánh xạ qua mô hình domains, forest, OUs và trees. Nhóm những tài nguyên sẽ được tổ chức 1 cách luận lý và cho phép người dùng truy xuất dễ dàng tới tài nguyên hơn phải nhớ vị trí vật lý cụ thể của nó.

#### **Physical Structure**

Nếu như xét về physical component của AD hiện tại sẽ bao gồm hai phần là Domain Controllers và Sites. Tùy thuộc chủ yếu vào mô hình tổ chức trong công ty mà người quản trị sẽ sử dụng những components để thiết kế phù hợp.

* 1. **Domain Controller**

### Domain Controller là gì?

Domain là một hệ thống các tên miền website khác nhau của một cá nhân, tổ chức, doanh nghiệp trên nền tảng internet.

Domain controller (DC) là một hệ thống máy chủ có vai trò quản lý hoạt động, an ninh mạng và các dữ liệu của một Domain nào đó. Có thể ví Domain controller như một người canh gác và chịu các trách nhiệm xác thực quyền truy cập người dùng và vấn đề liên quan đến tài nguyên dữ liệu của Domain. Một Domain có thể được quản lý bởi nhiều DC

### Chức năng và vai trò của Domain controller

**Domain Controller** có vai trò lưu trữ các dữ liệu, thông tin liên quan của một domain mà nó được cài đặt. DC giúp quá trình lưu trữ dễ dàng và nhanh chóng hơn. Bên cạnh đó, nhờ tính năng Backup dữ liệu mà người dùng không sợ bị mất dữ liệu nấu thế thống gặp vấn đề.  
Sau khi cài đặt DC, các đối tượng domain không nằm trong danh sách được cài đặt nhưng vẫn được tiến hành lưu trữ bản sao miền hoàn chỉnh.

### Nguyên tắc hoạt động của DC

**Domain Controller** sẽ đóng vai trò như một người gác cổng. Các yêu cầu của dùng dùng sẽ được thông qua bởi Domain Controller để xác thực danh tính và ủy quyền đăng nhập. Cách xác thực thường là dùng username và mật khẩu người dùng.  
Sau khi thực hiện các thao tác xác thực trên, người dùng có thể sử dụng tài nguyên website như bình thường.

### Cách triển khai Domain controller

Một mô hình Domain Controller không tự có sẵn mà người quản trị hệ thống cần cài đặt để tích hợp các tính năng vào hệ thống. Các bước để cài đặt như sau:

* Bước 1: Cài đặt IP tĩnh cho máy được chọn làm DC
* Bước 2: cài đặt controller lên máy Server đã chọn ở bước 1
* Bước 3: Tạo user cho client trong DC
* Bước 4: Đặt địa chỉ IP và thêm các Client
* Bước 5: Đăng nhập máy Client để kiểm tra

# THỰC HÀNH

## Chuẩn bị môi trường

1 máy ảo Windows Server 2019

1 máy ảo Windows 7

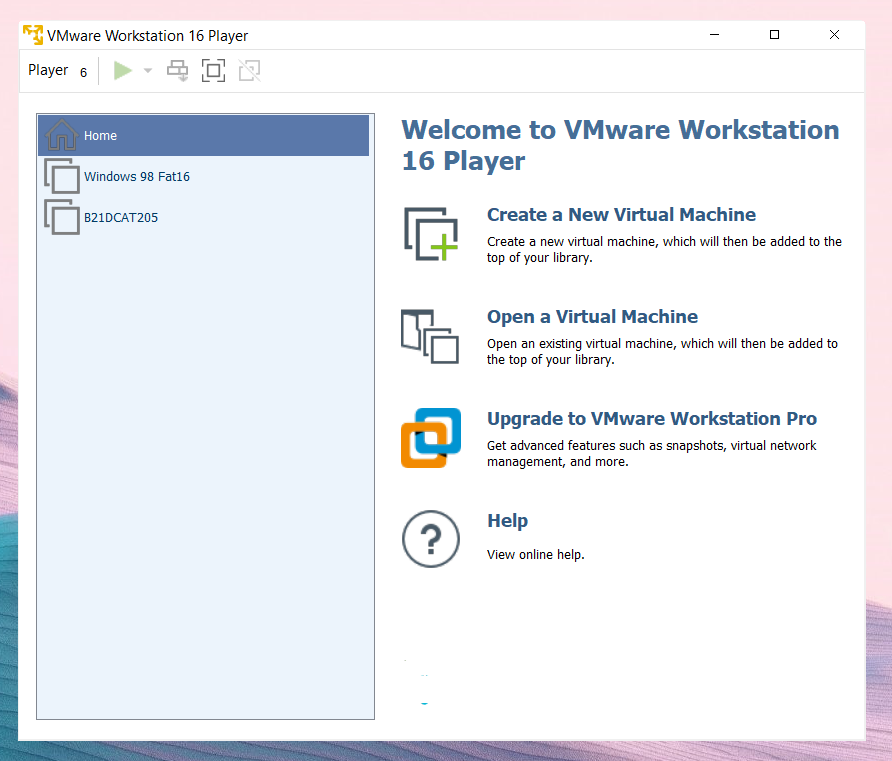


### 

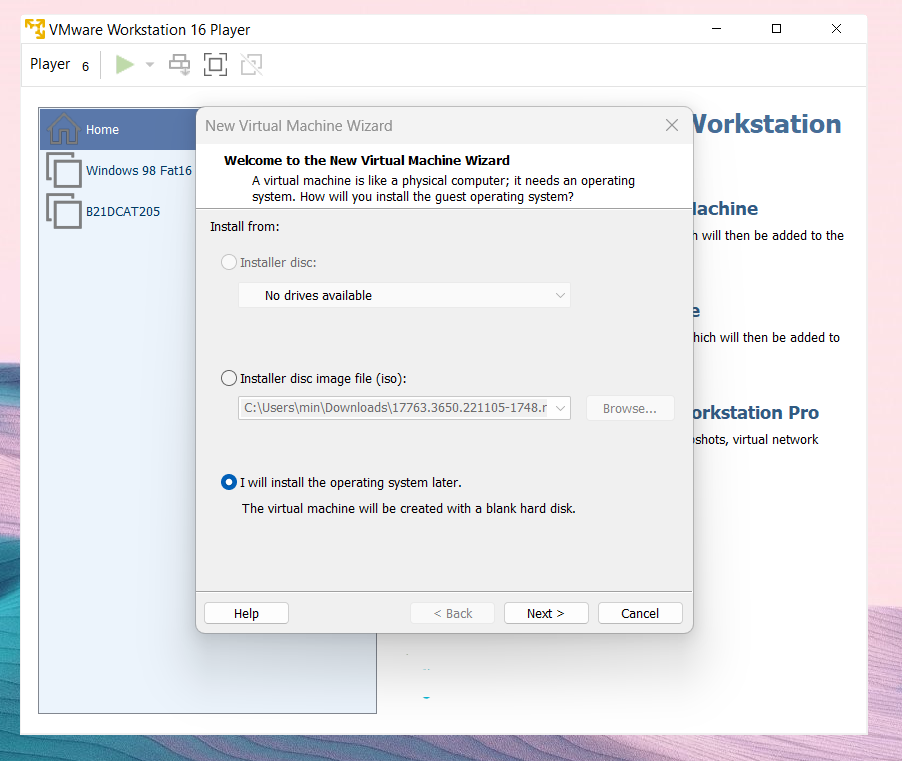


## Thực hành cài máy ảo

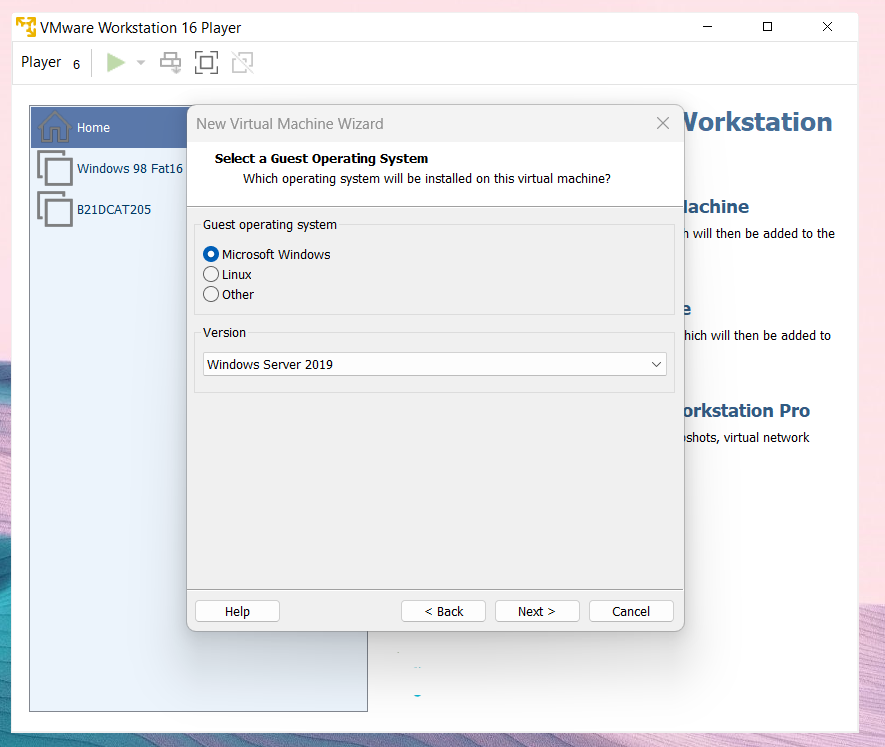
* + - ***Cài đặt Windows server 2019***
* Ở đây mình sử dụng bản VM WARE 16.2.4
* Chọn Create a New Virtual Machine

******

* Chọn I will install the operating system later -> Next



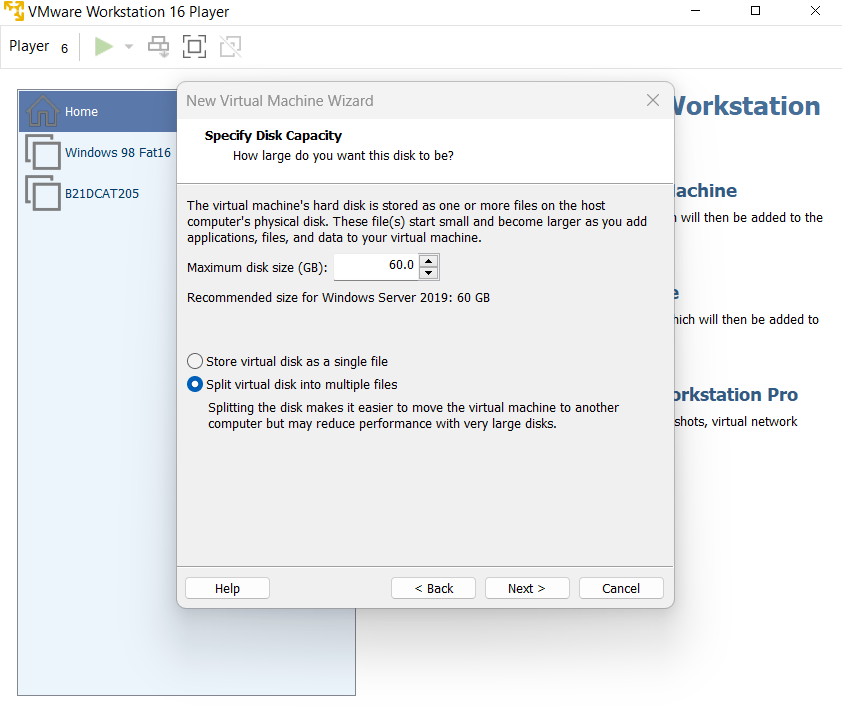
* Chọn Version: Windows Server 2019 ->Next



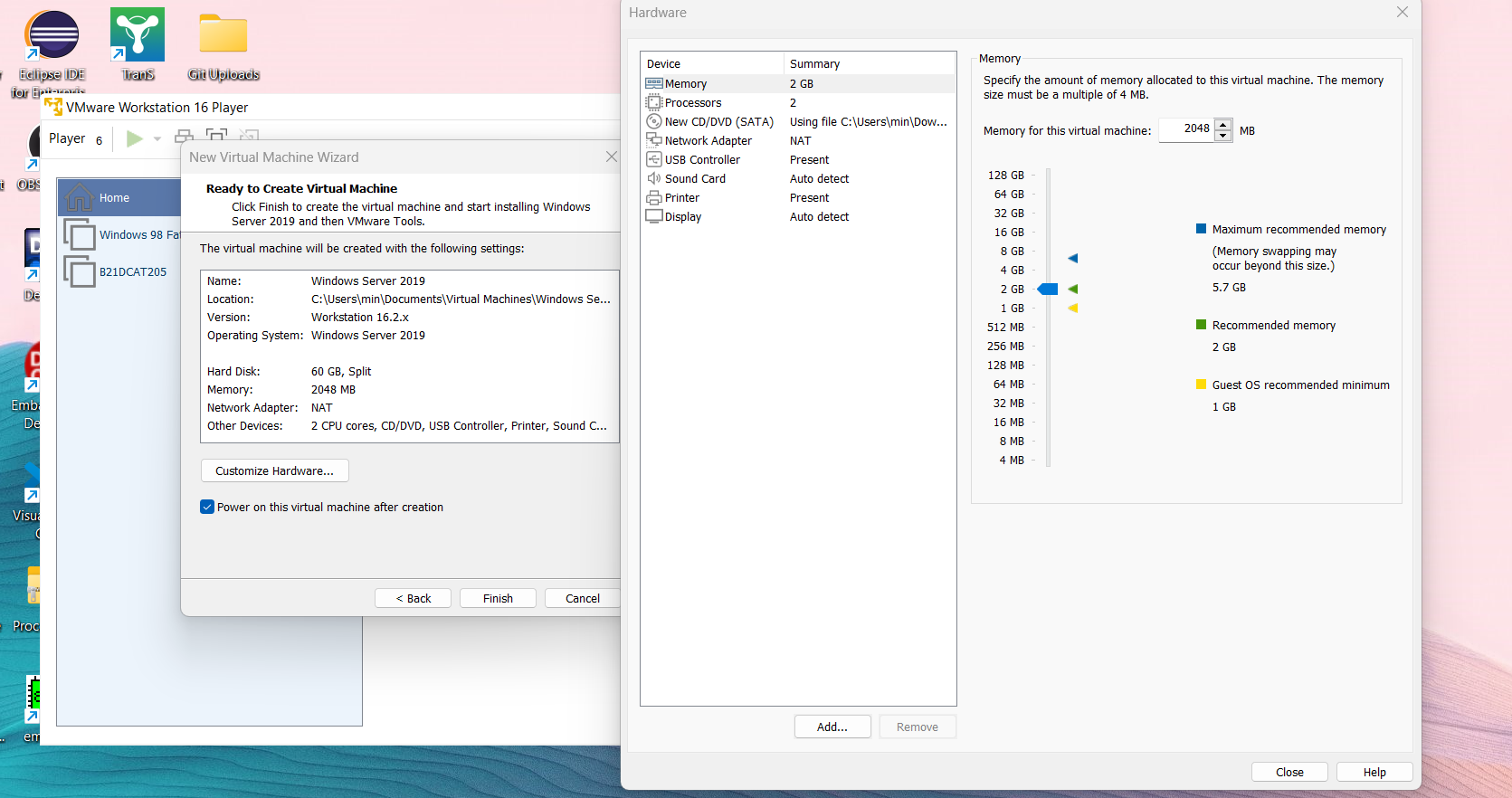
* Chọn nơi lưu trữ Windows Server -> Next

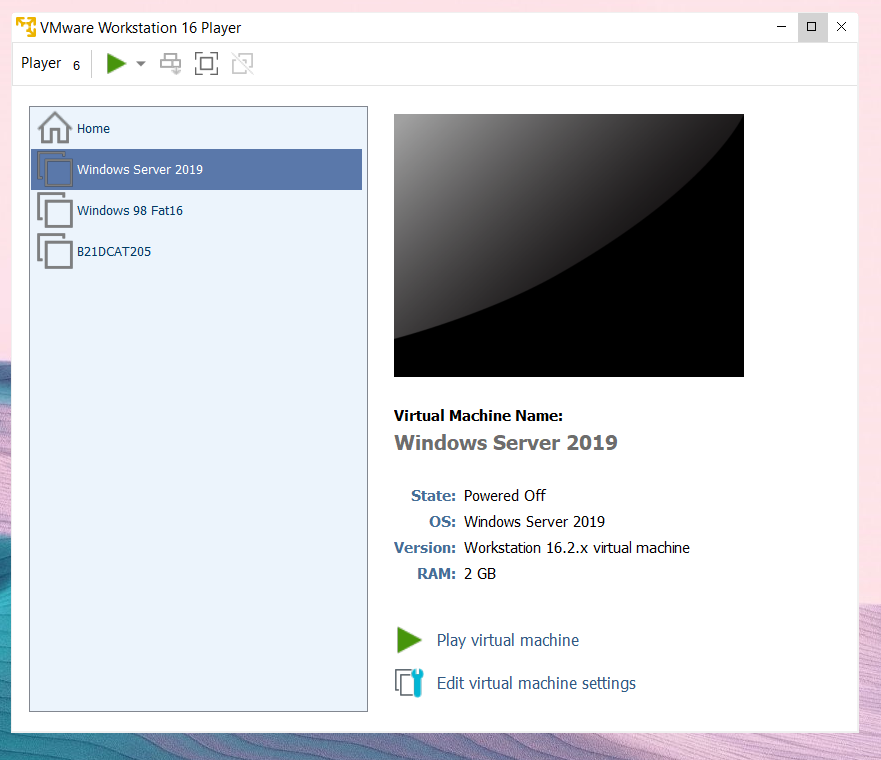


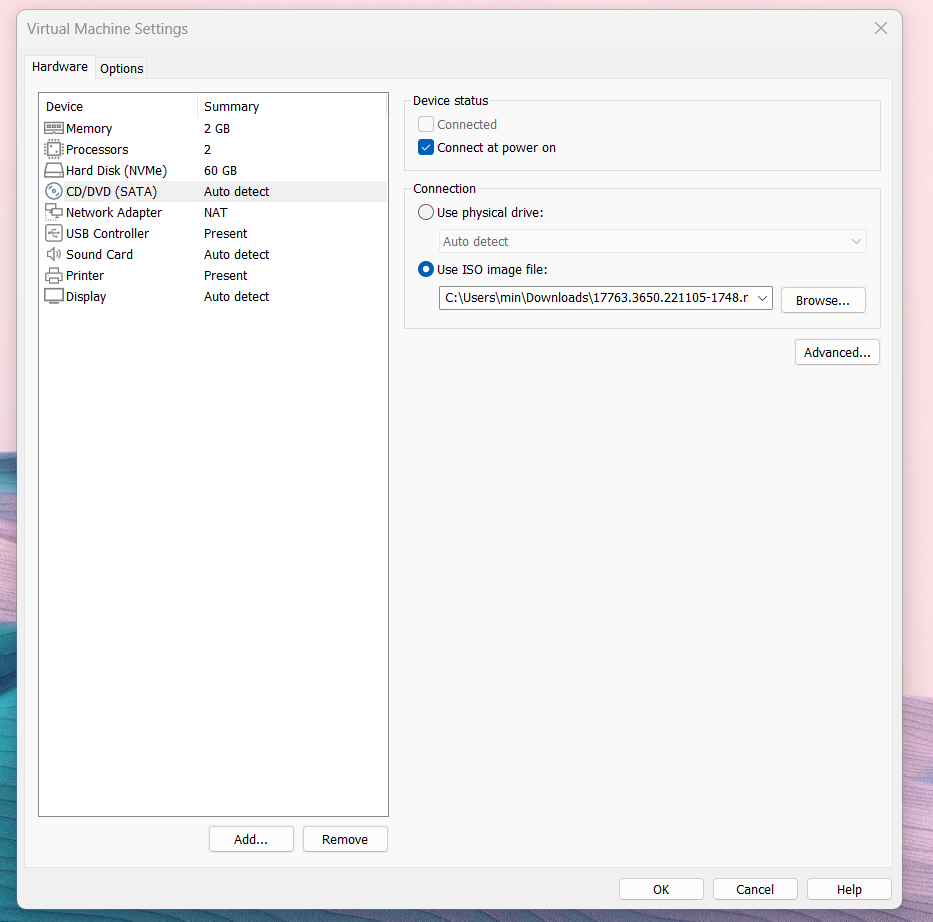
* Chọn dung lượng bộ nhớ là 60 GB (mặc định)-> Next

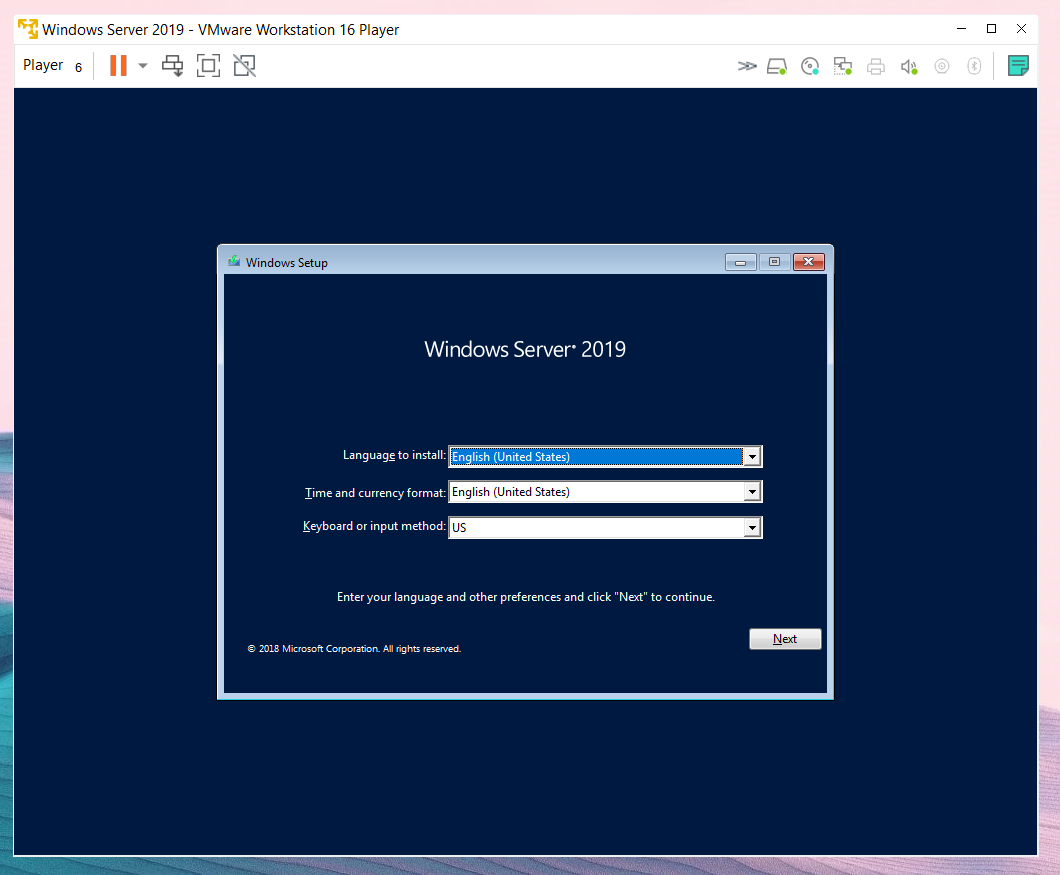


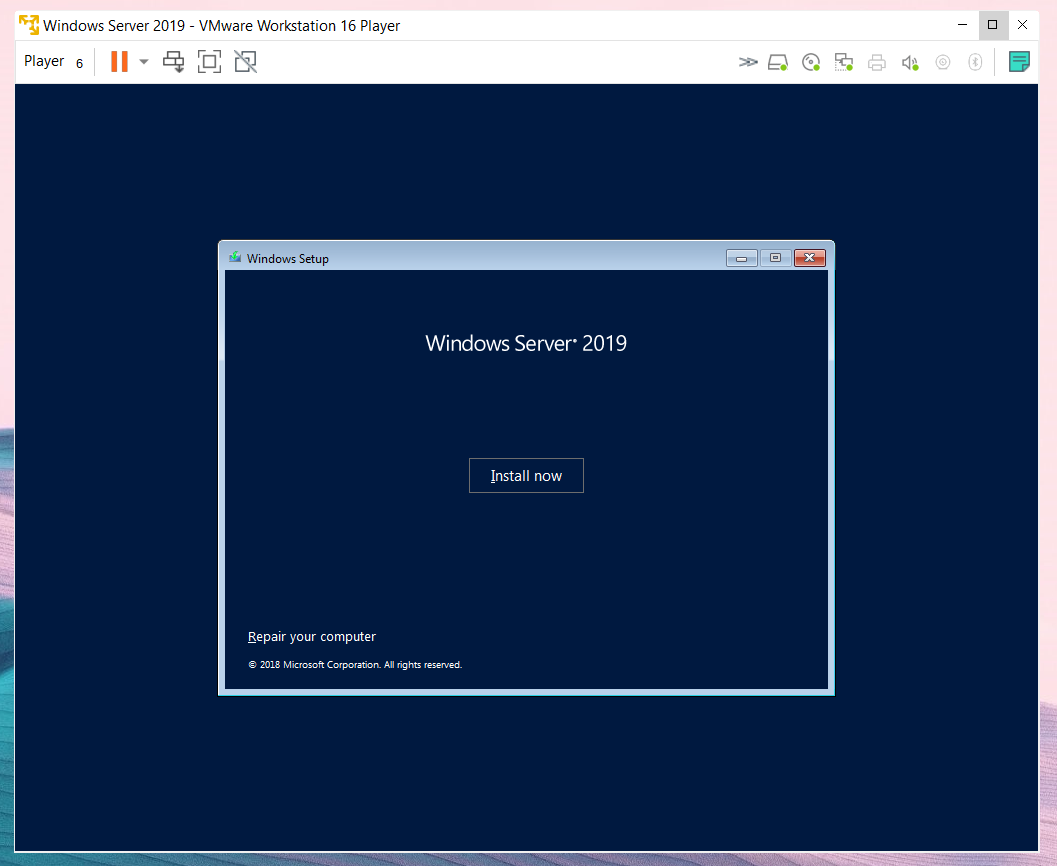
* Chọn Customize Hardware… ,ở đây ta có thể chỉnh một vài thông số như tinh chỉnh Memory .Sau đó ấn close Hardware ->Finish.

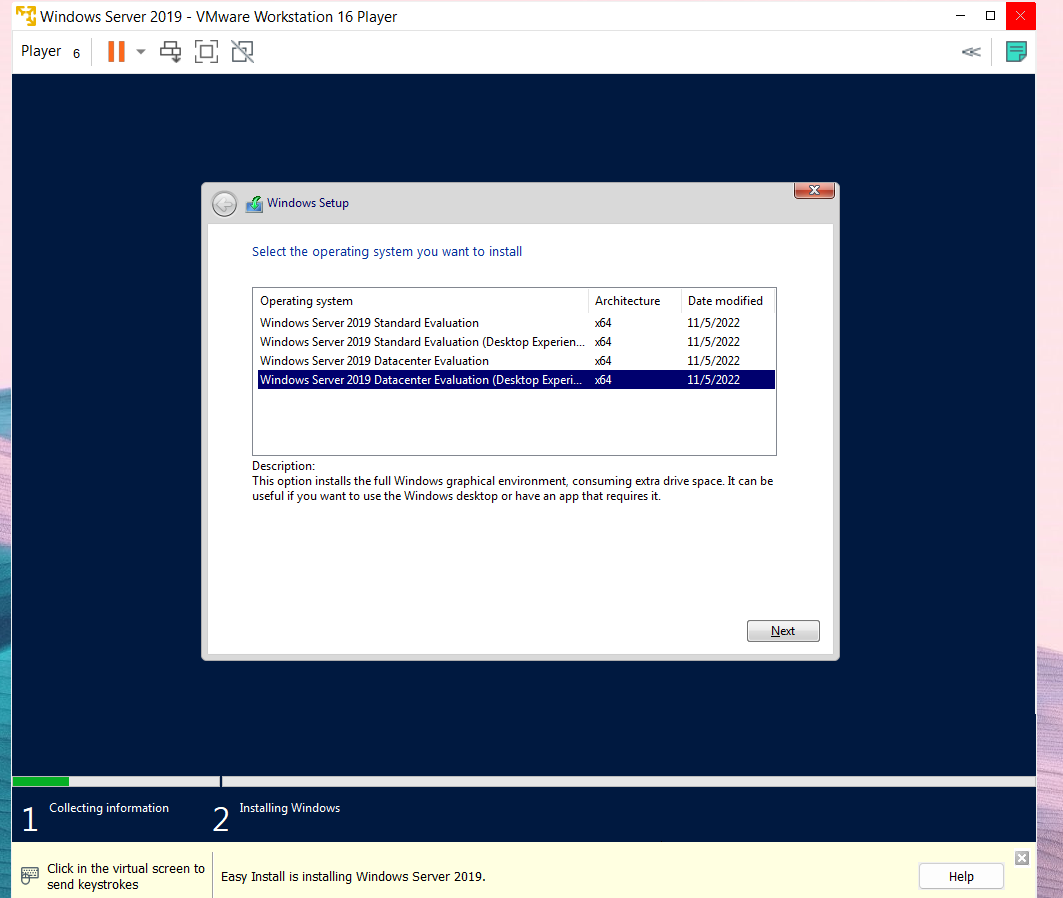


* Ta đã tạo thành công được một máy ảo có tên “Windows Server 2019 như hình dưới” .
* Ấn vào Edit virtual machine settings và thêm file ISO Windows Server 2019 đã chuẩn bị vào rồi ấn OK

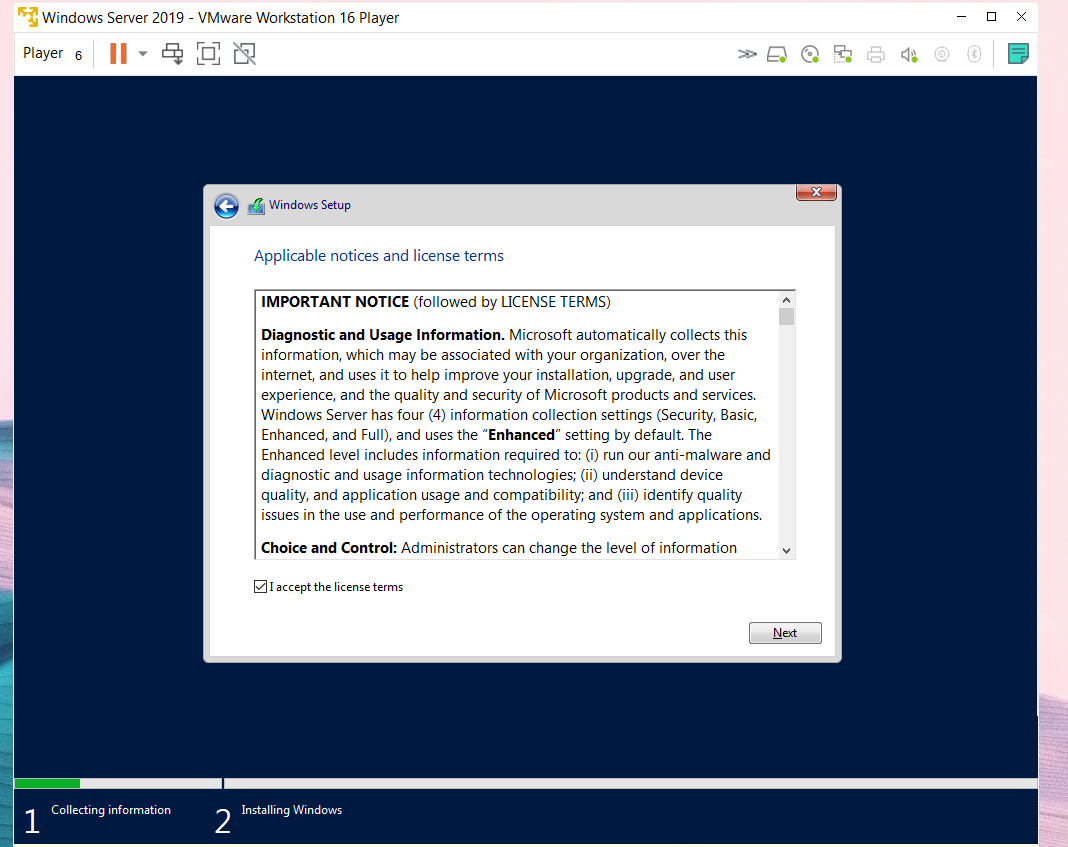


* Chọn Play a virtual machine để khởi động máy ảo, ấn Next.
* Chọn Install now





* Ấn “I accept the license terms” -> Next.

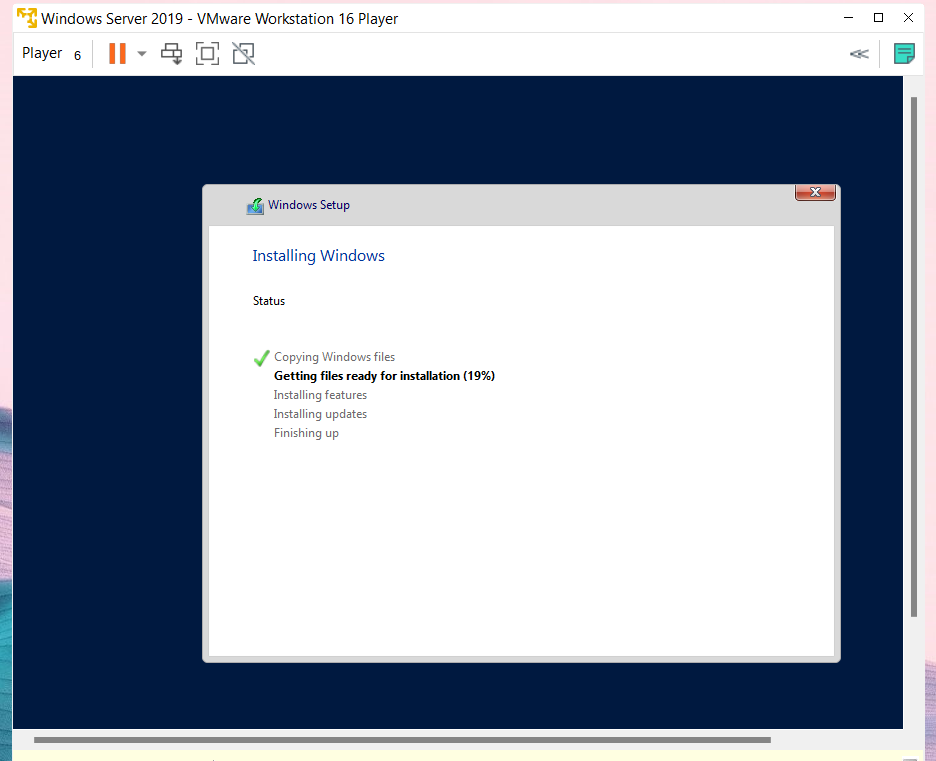


* Chọn Custom: Intall Windows only (advanced)

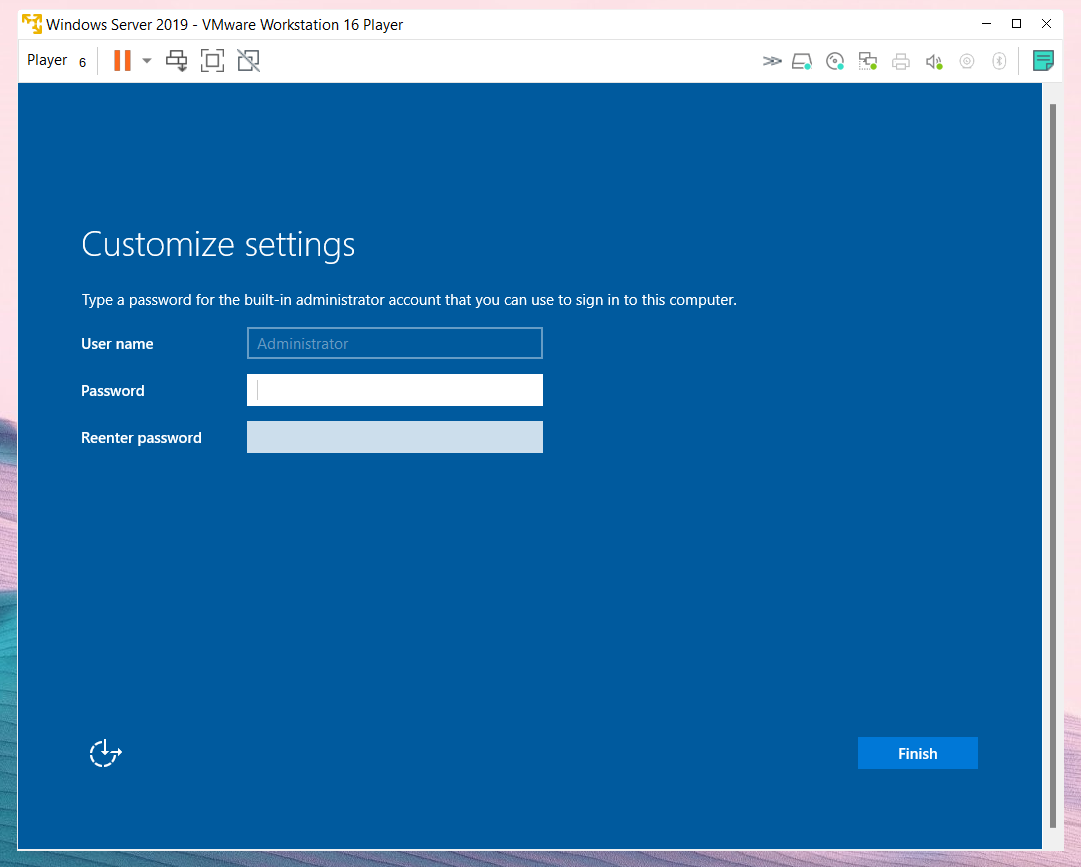


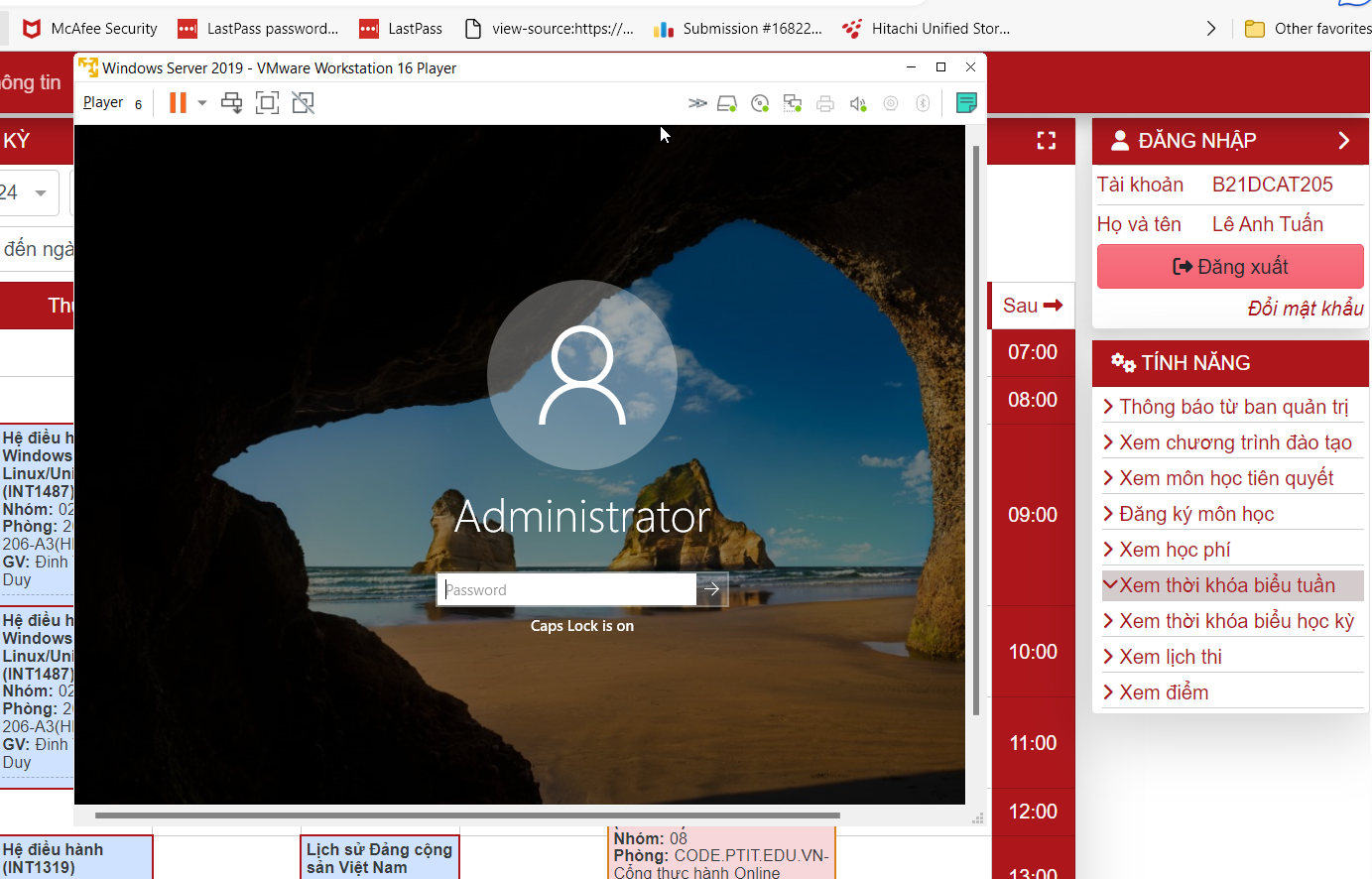
* Chọn next





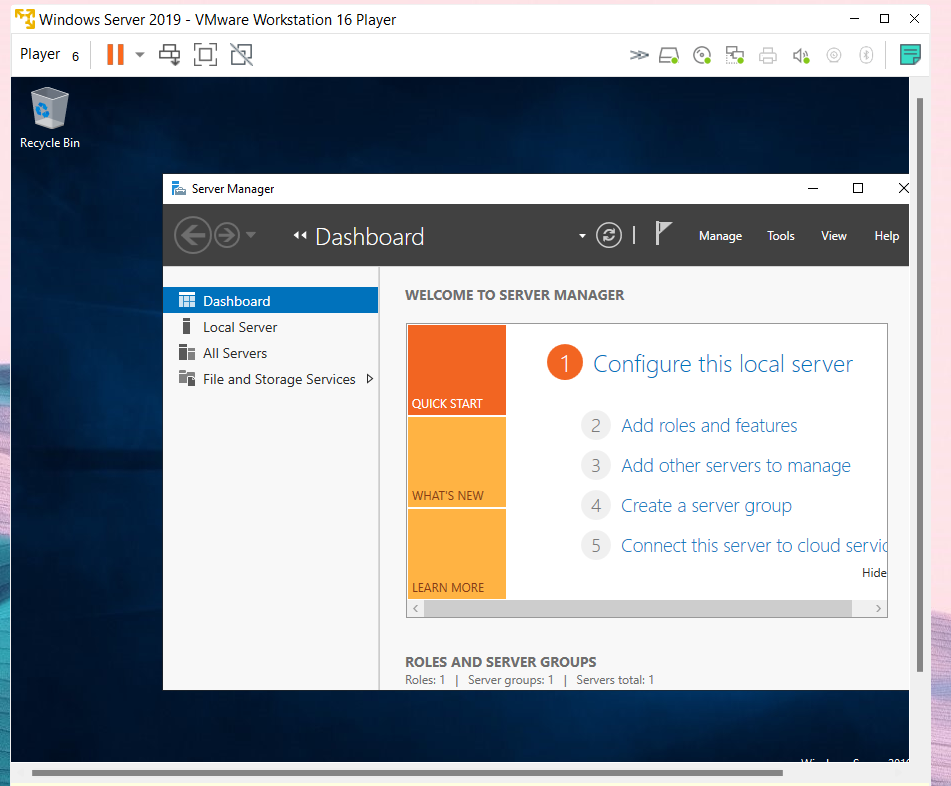
* Tiến hành thêm mật khẩu cho máy và ấn Finish



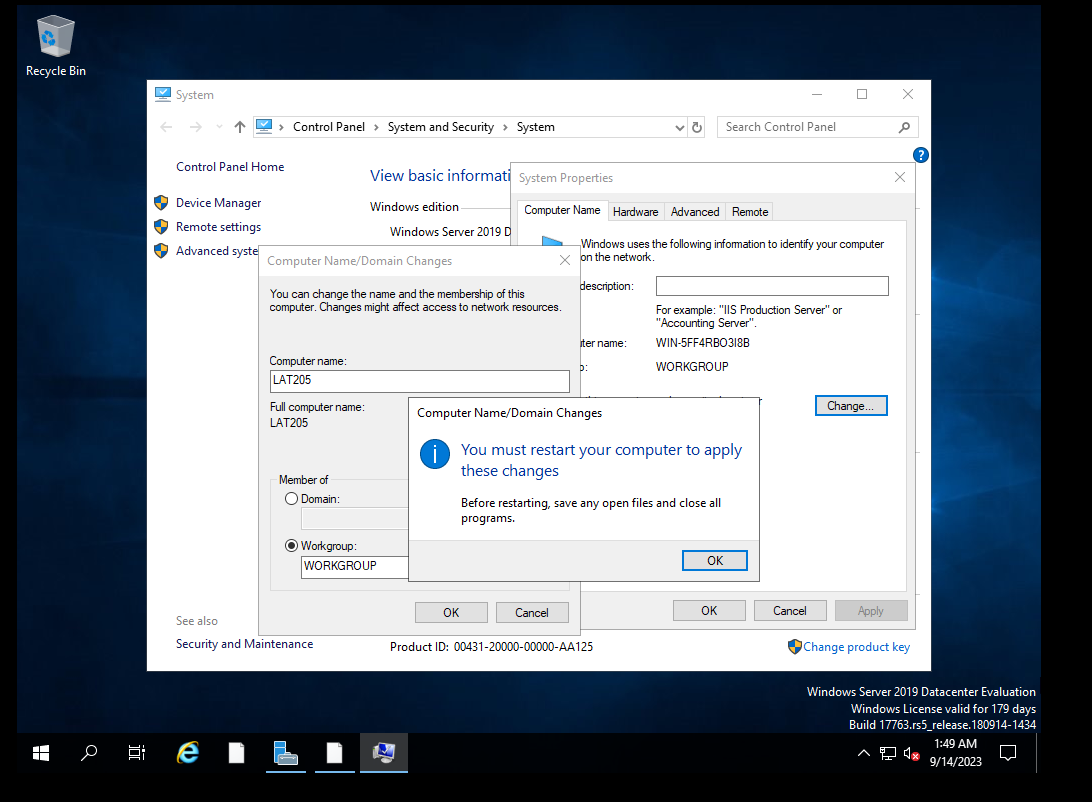


* + **Nâng cấp Sever thành Domain Controller**
* Đổi tên Server (Lê Anh Tuấn – MSV:B21DCAT205 thành LAT205)

- Khởi động máy ảo và nhập mật khẩu

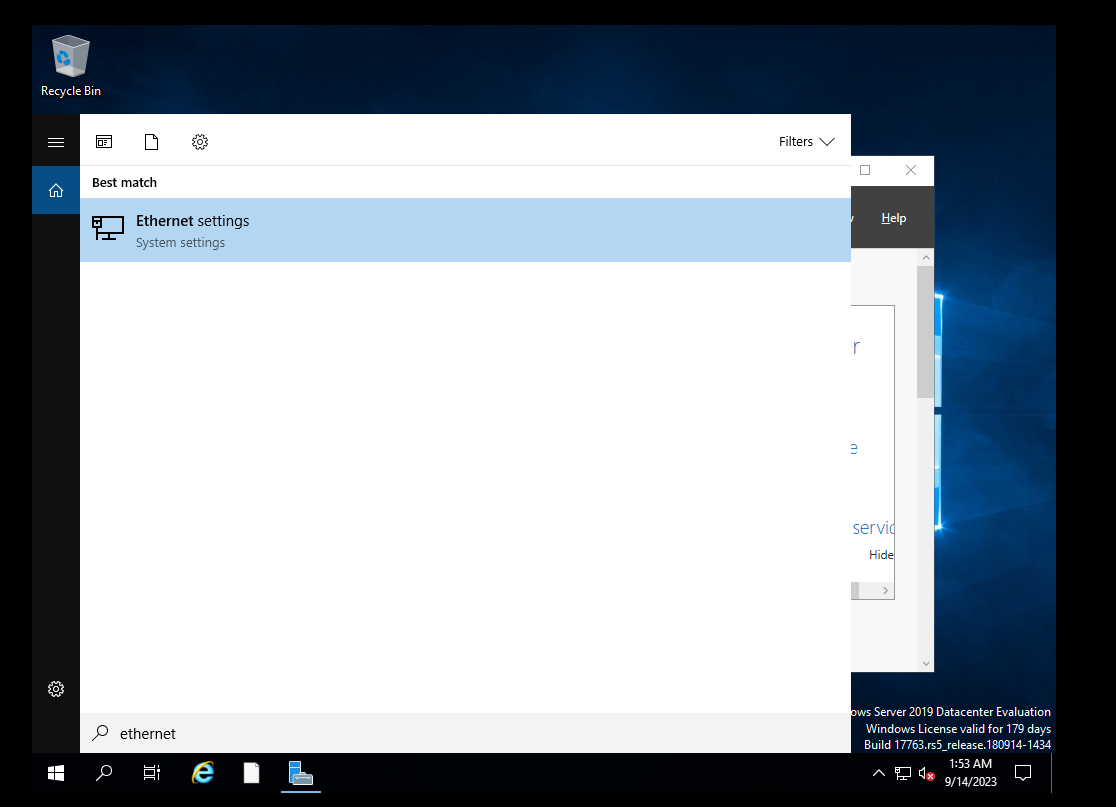


* Sau đó vào mục System and Security -> System , chọn Advanced system settings, rồi vào mục Computer Name -> Change để tiến hành đổi tên Computer.
* Sau khi đổi tên thì yêu cầu phải restart lại máy tính.

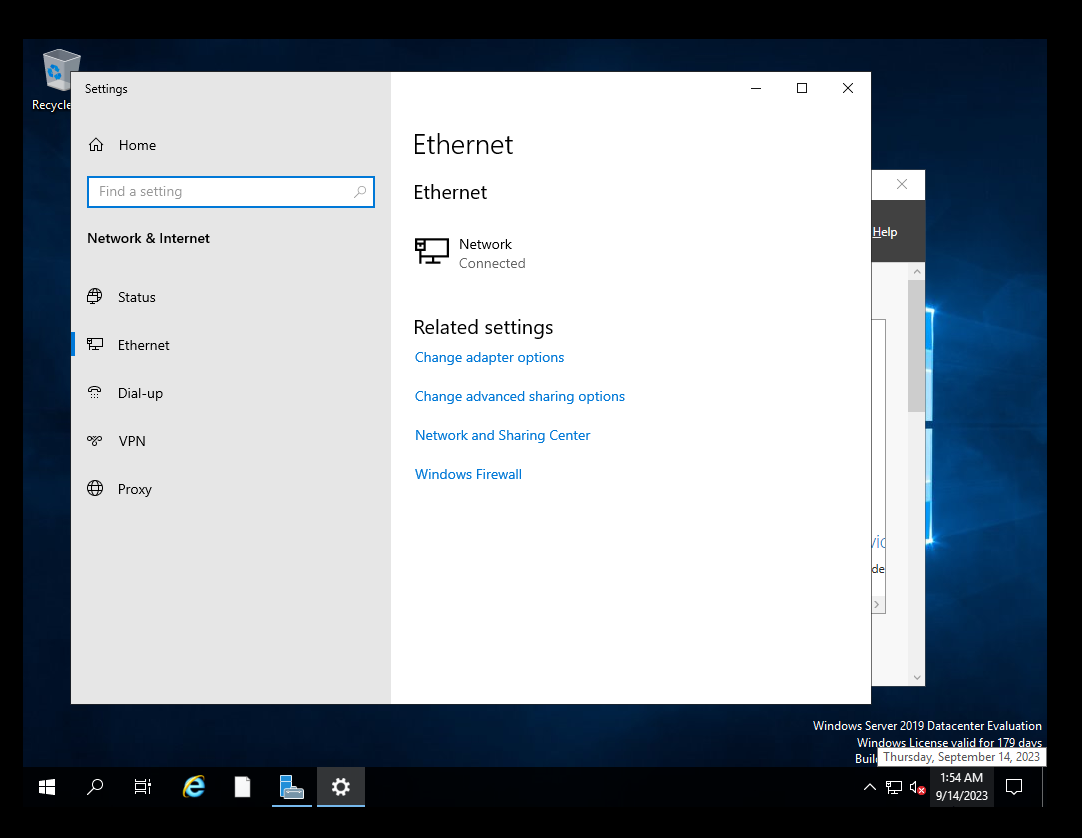


#### Cài đặt static IP

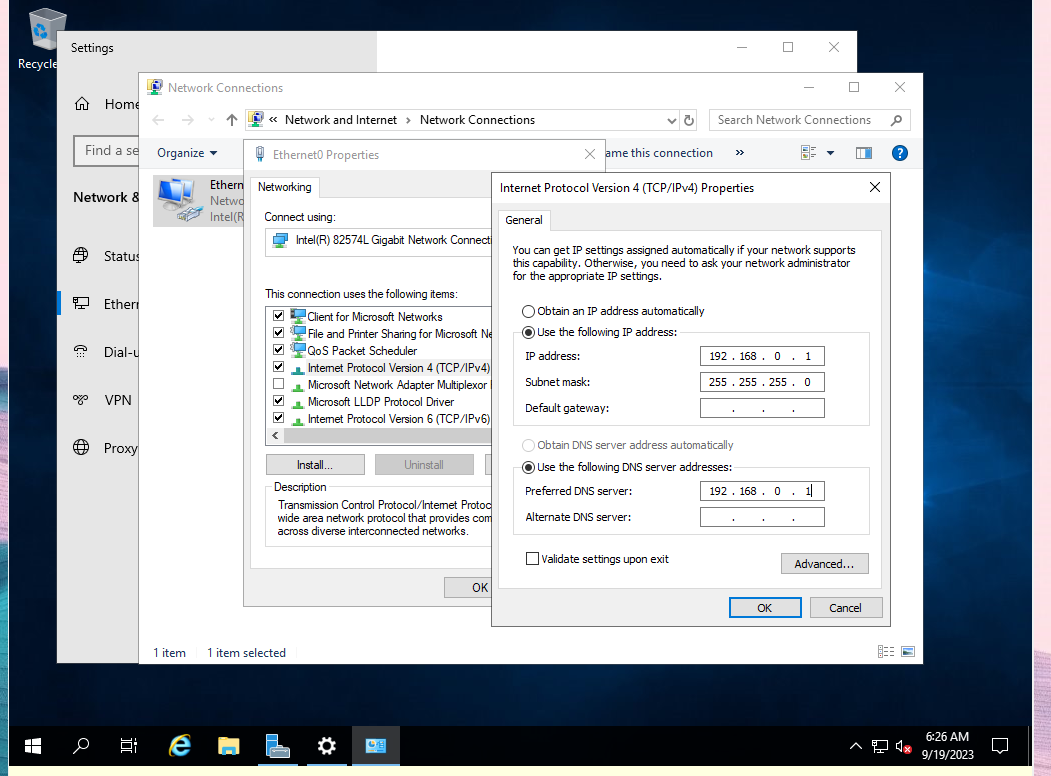
* Tìm kiếm ethernet



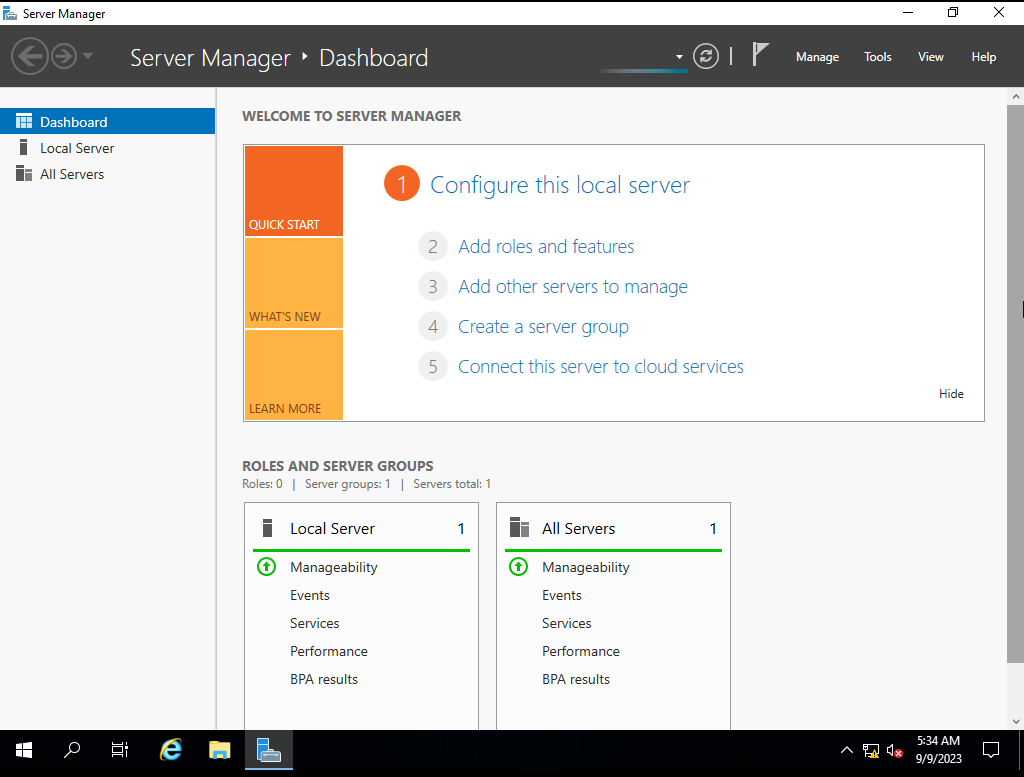
* Ấn change adapter options

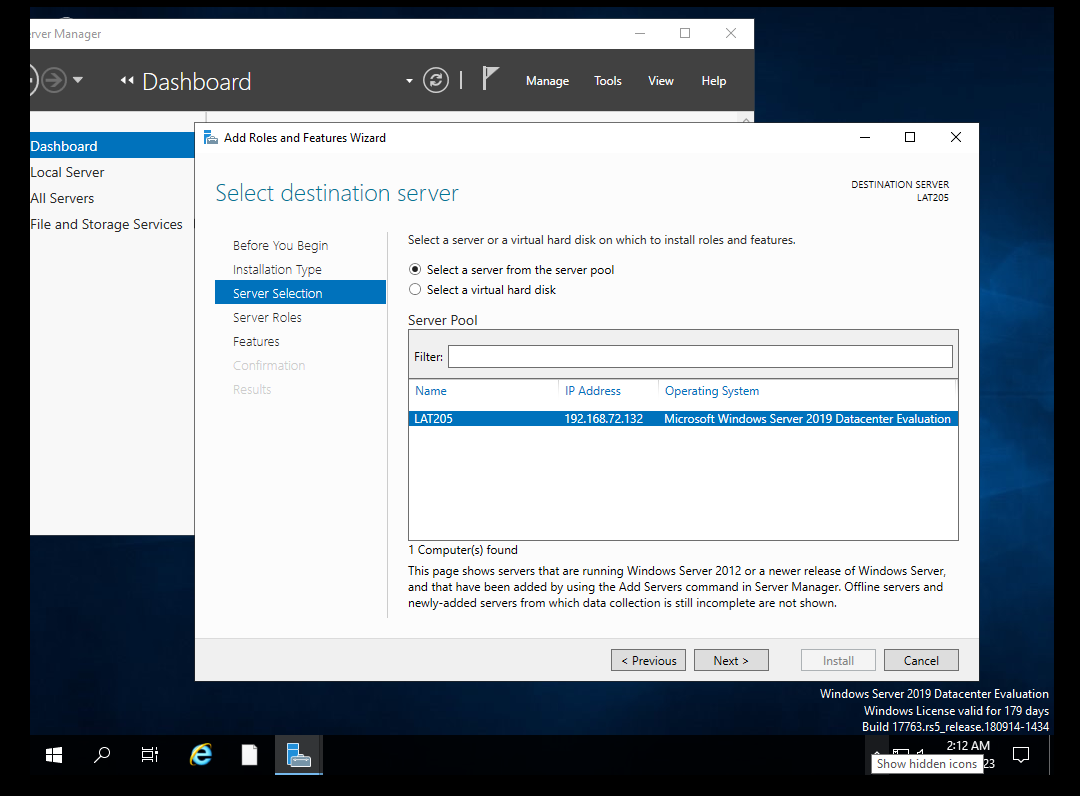


* Trong Ethernet0 Properties -> Internet Protocal Version 4(TCP/IPv4).

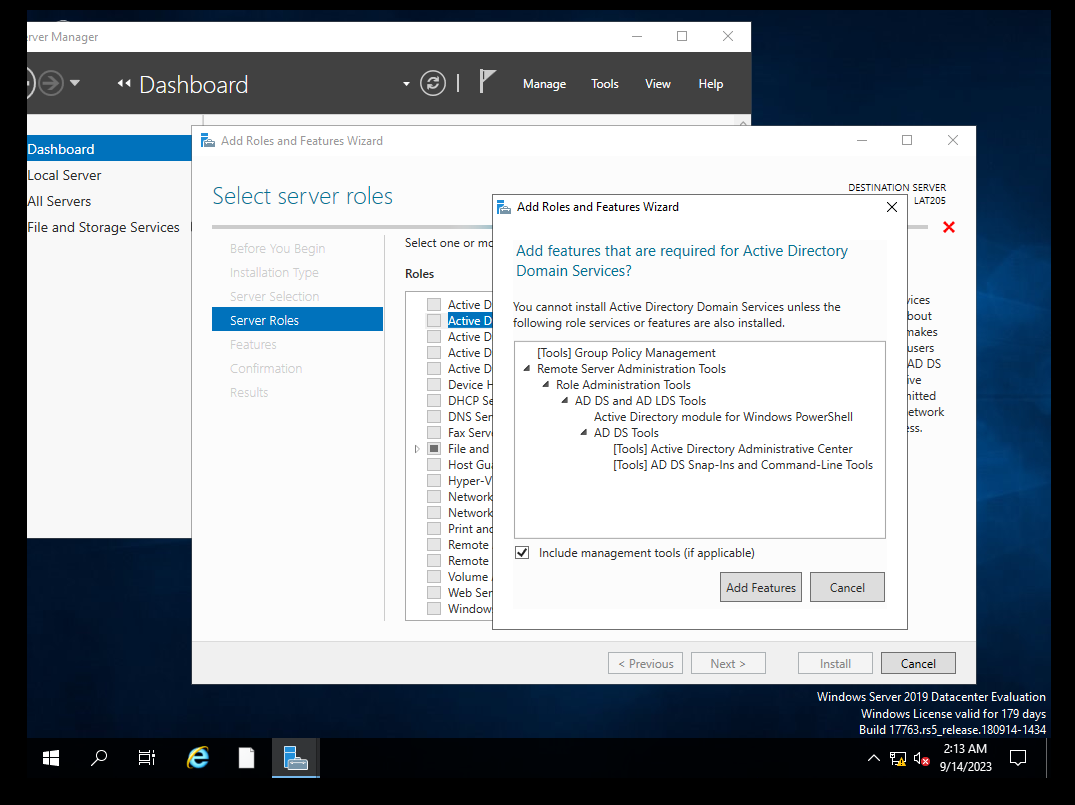


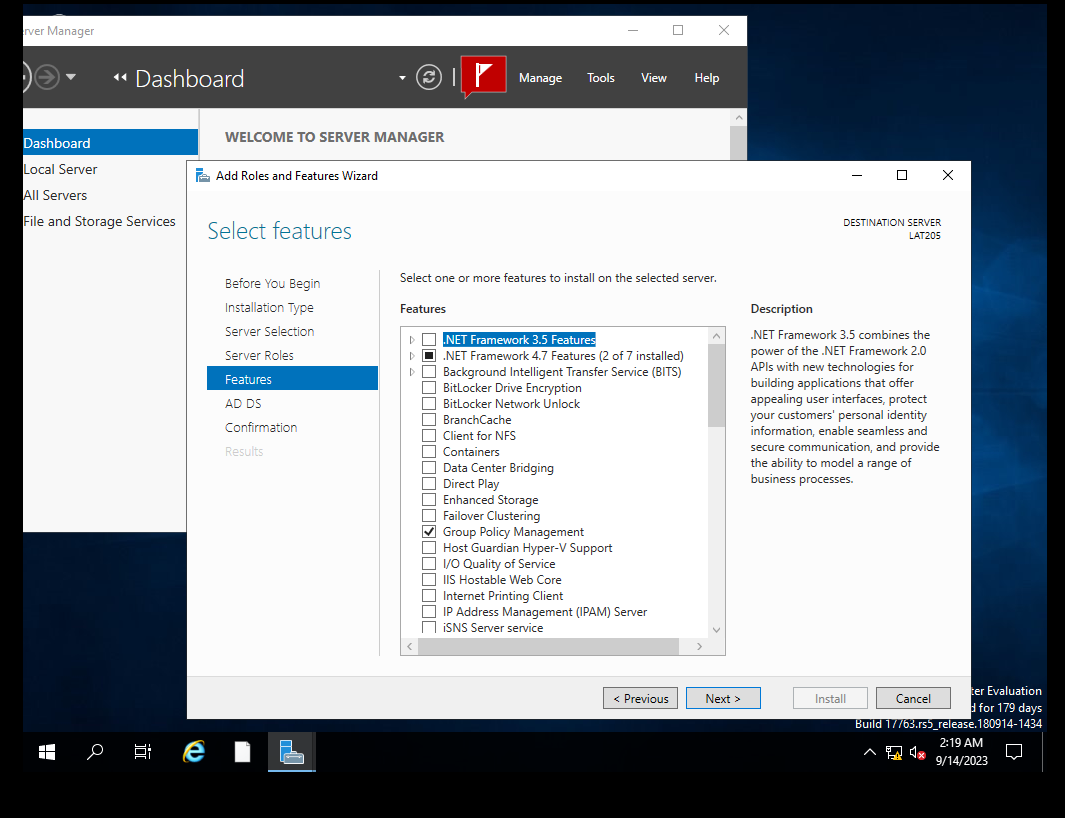
Cài đặt server role trong Server Manager

* Trên Dashboard của Server Manager, chọn vào Add roles and features

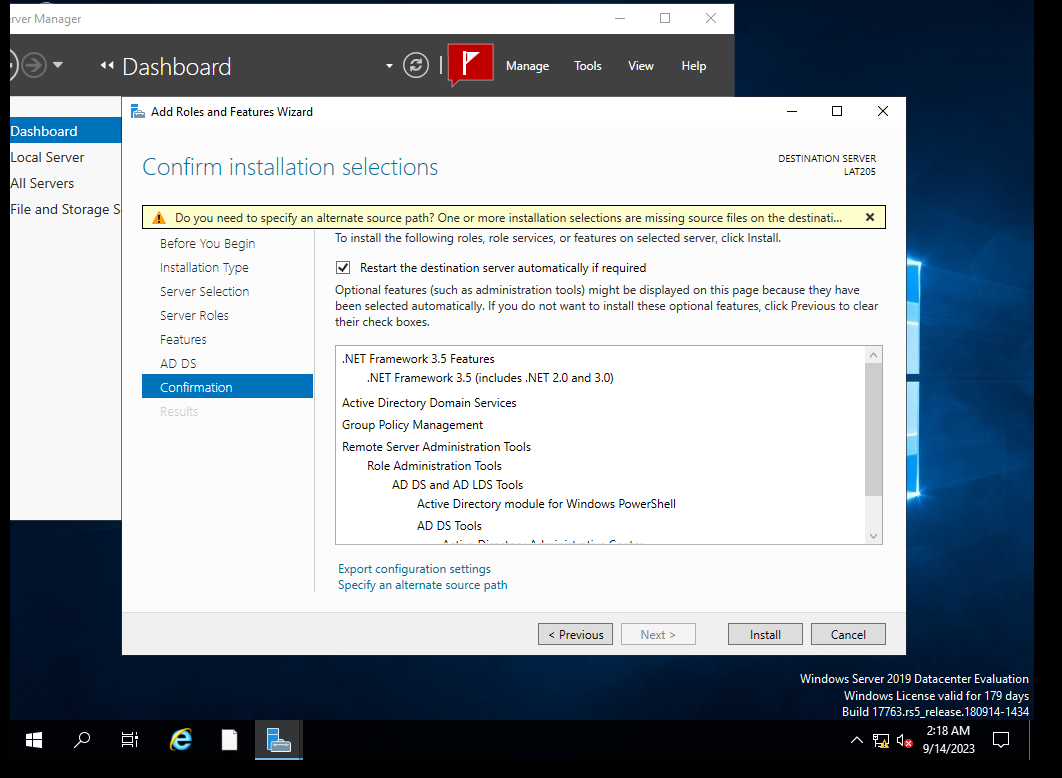


* Chọn Active Directory Domain Services - > Add Features

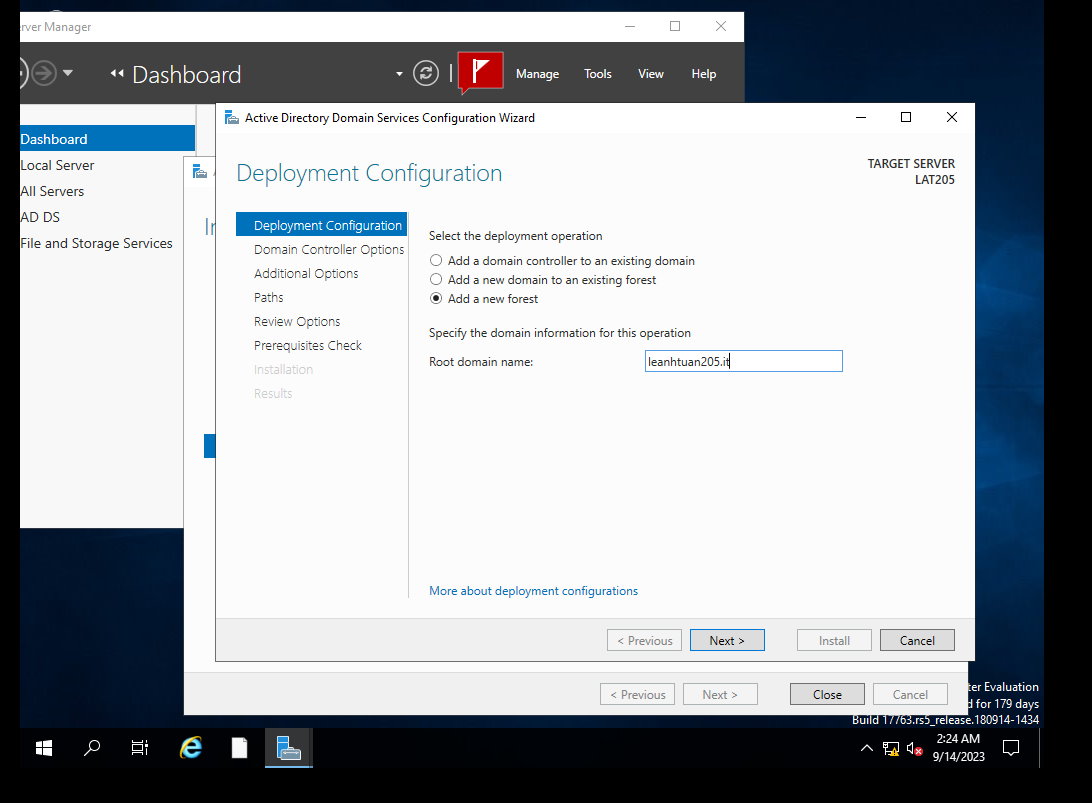




- Bấm vào Install để tiến hành cài đặt những dịch vụ cần thiết trong Domain Controller.

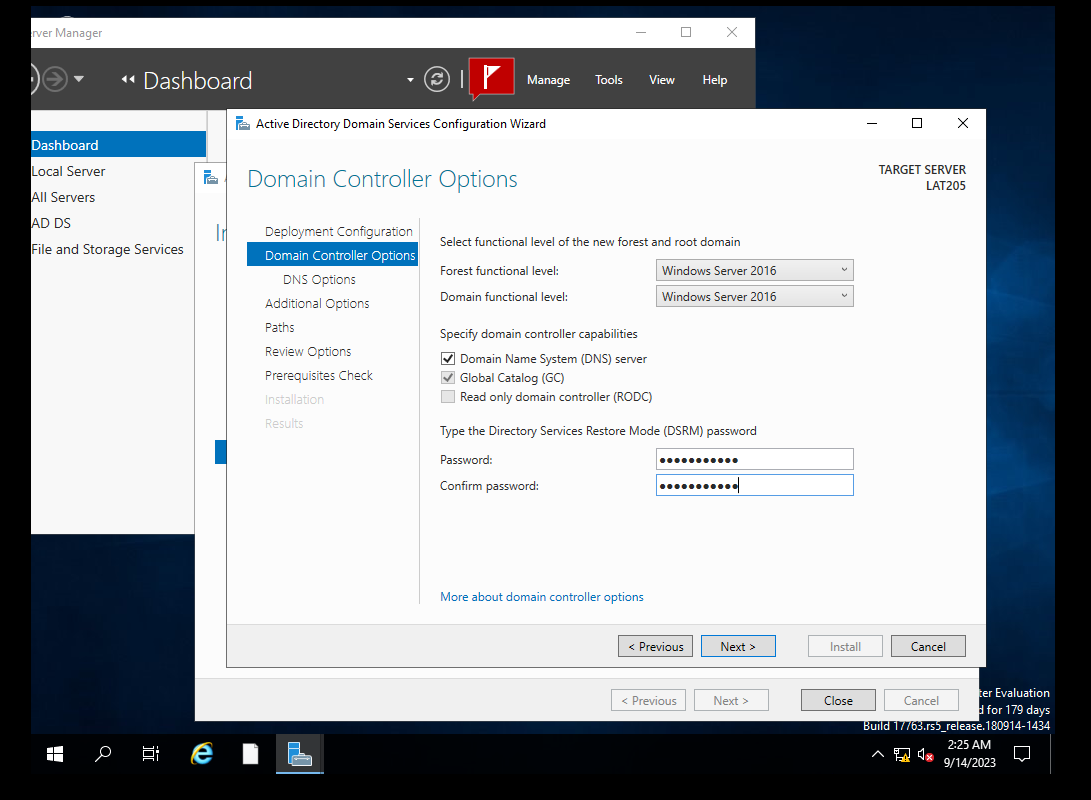


* Sau khi tải xong ấn vàopromote this server to a domain controller
* Trên Deployment Configuration sẽ có ba tùy chọn là: Thêm 1 ADC vào domain đã có sẵn, xây dựng domain mới tại forest đã có sẵn, xây dựng máy Domain Controller đầu tiên của forest. Tại đây sẽ tạo 1 forest mới với tên leanhtuan205.it:

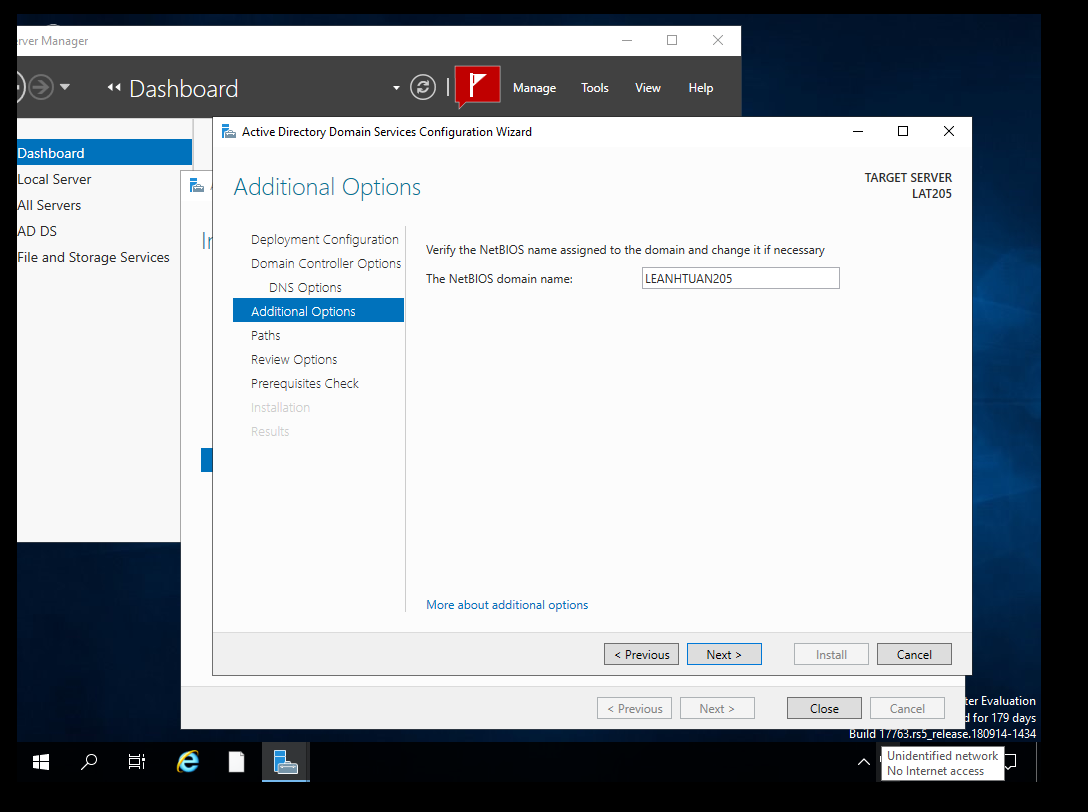


**Khôi phục AD với chế độ Restore Mode**

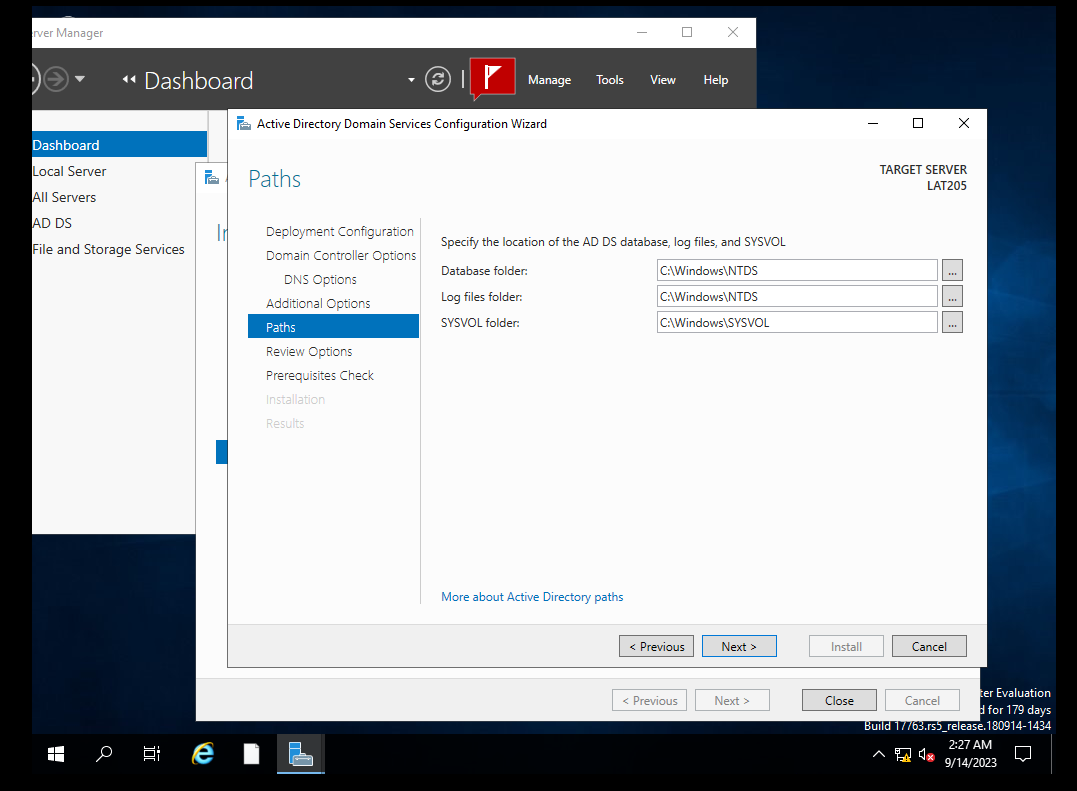
Tại Domain Controller Options, nhập vào mật khẩu ở mục Type the Directory Services Restore Mode password. Theo đó đây là mật khẩu được sử dụng để có thể khôi phục AD với chế độ Restore Mode.



* Sau đó Click Next tới màn hình Additional Options, lựa chọn tên NetBIOS domain. Tại đây sẽ để mặc định là:



- Tại Paths, chọn vào đường dẫn lưu database PAD, SYSVOL và logs. Chọn mặc định:



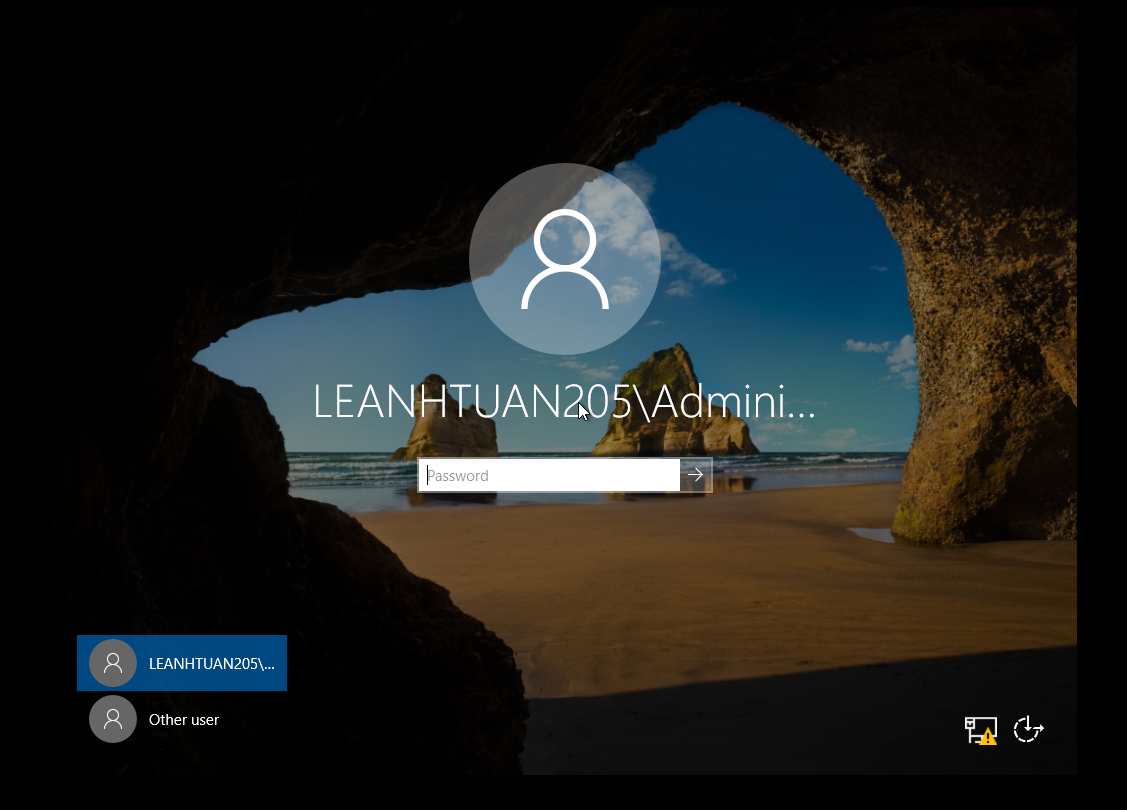
#### Bắt đầu cài đặt

Nhấn vào Next tới màn hình Prerequisites Check, ở đây sẽ kiểm tra những điều kiện để tiến hành cài đặt DC. Chọn vào Install để có thể bắt đầu quá trình cài đặt:

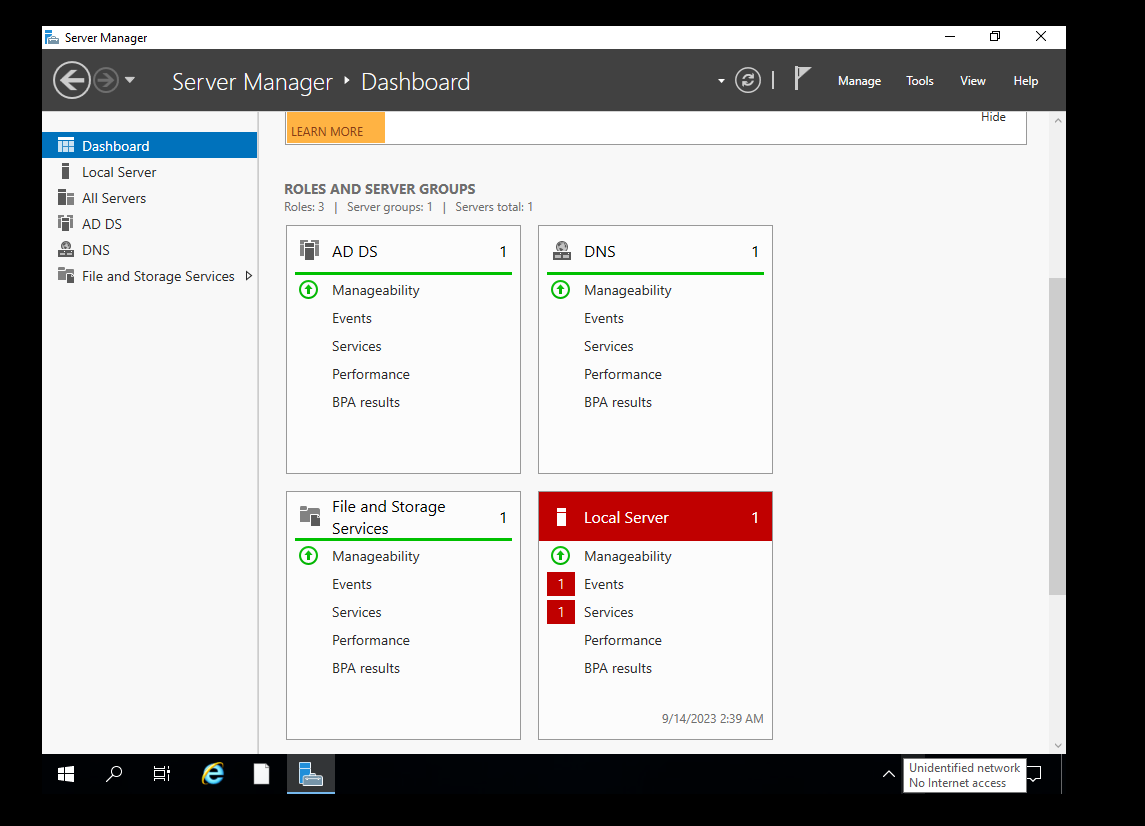


* Ngay sau khi đã hoàn tất quá trình cài đặt thì restart lại máy.

#### Kiểm tra



* 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

