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: Hoàng Trung Kiên
Mã số sinh viên: B20DCAT098
Họ và tên giảng viên:TS. Đinh Trường Duy

Hà Nội ngày……..tháng……. năm…….

1. GIỚI THIỆU BÀI THỰC HÀNH

a, Mục đích

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

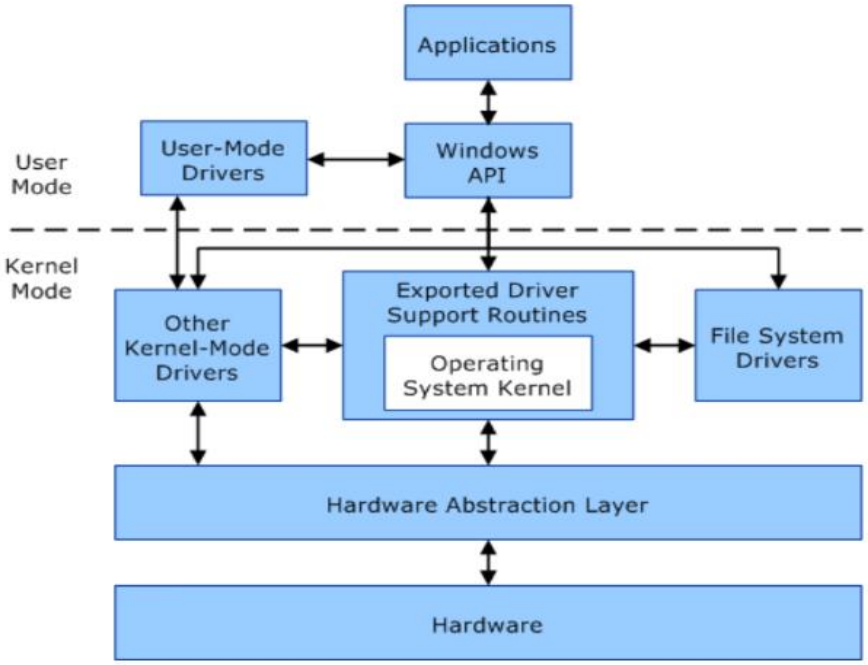
b, Yêu cầu

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

2. CƠ SỞ LÝ THUYẾT

a, 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



Hình 1:Kiến trúc chung của windows

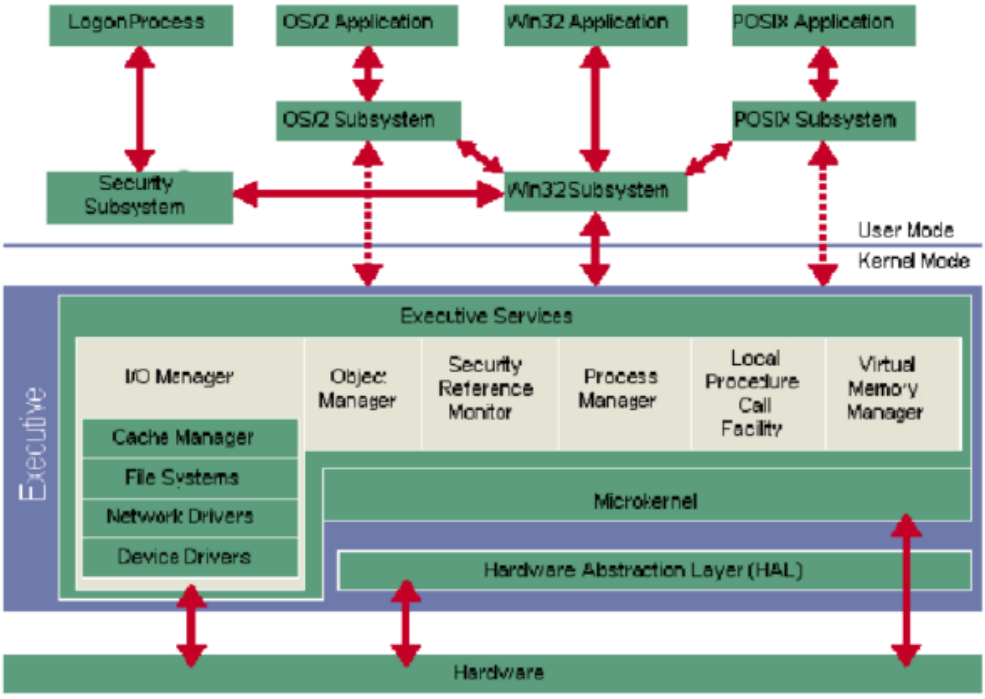
Nhánh này bao gồm các hệ điều hành sau:

- 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

- 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.

b, Kiến trúc Windows NT:

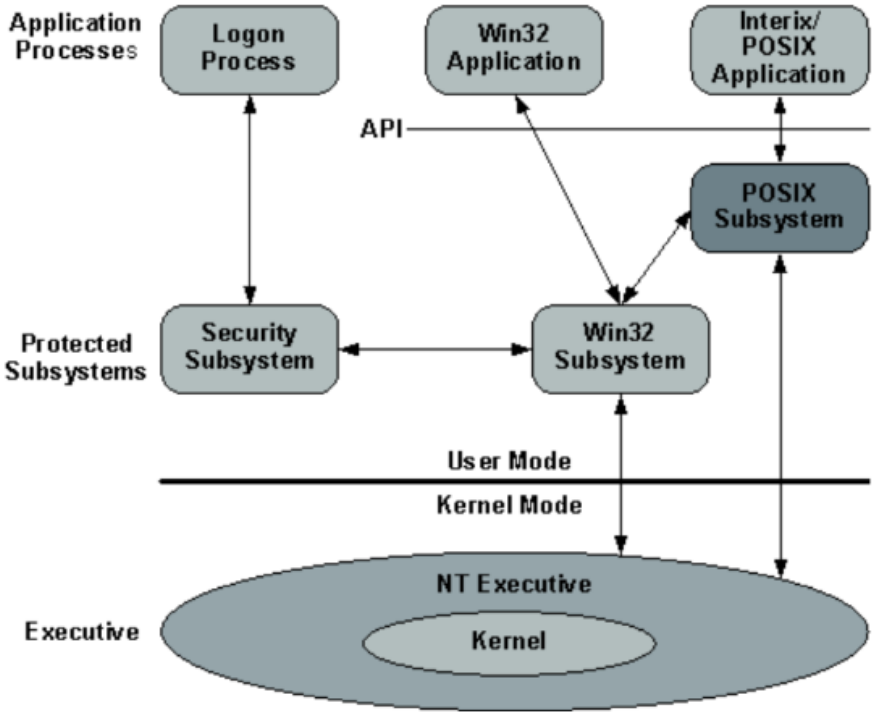
-Windows NT được thiết kế sử dụng cách tiếp cận theo đơn thể (modular). Các đơn thể khác nhau (còn được gọi là các bộ phận, thành phần) của Windows NT được trình bày trong hình 1. Các bộ phận của Windows NT có thể chạy dưới hai chế độ: User (người sử dụng) và Kernel (nhân). Khi một thành phần của hệ 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 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:
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)

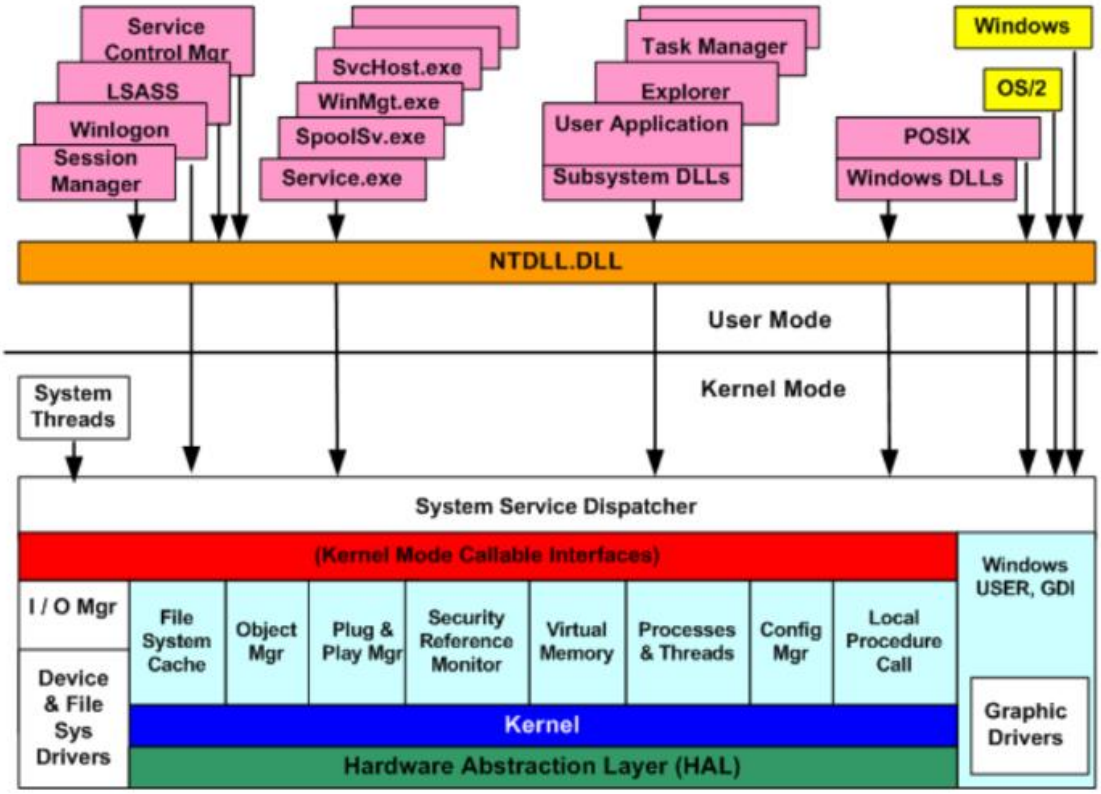
c, Kiến trúc Windows server 2003



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).
o Application process là tập hợp các chương trình các ứng dụng chạy trên Windows có thể là win32 application hoặc là các POSIX application.
o 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.
o 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
o Kernel kiểm soát hệ điều hành sử dụng các vi xử lý. Hoạt động của nó bao gồm lậpkế 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 vàquản 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:



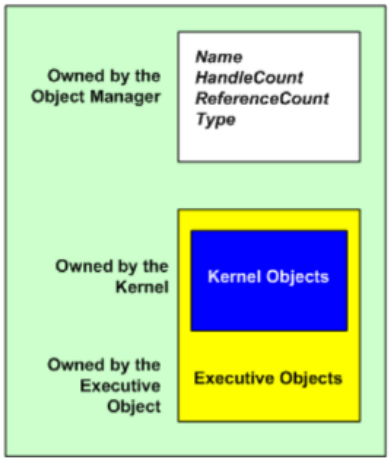
Hình 4: Chi tiết kiến trúc Windows server 2003

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: 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.

+Những phần chính:
o Configuration Manager: Quản lý Registry System.
o Process and Thread Manager: Tạo/ngắt Processes & Threads, hỗ trợ Processes &
Threads thực thi trong Kernel.
o 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
o Object Manager.
o Cache Manager.
o Memory Manage .
o 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:
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
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
+ 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

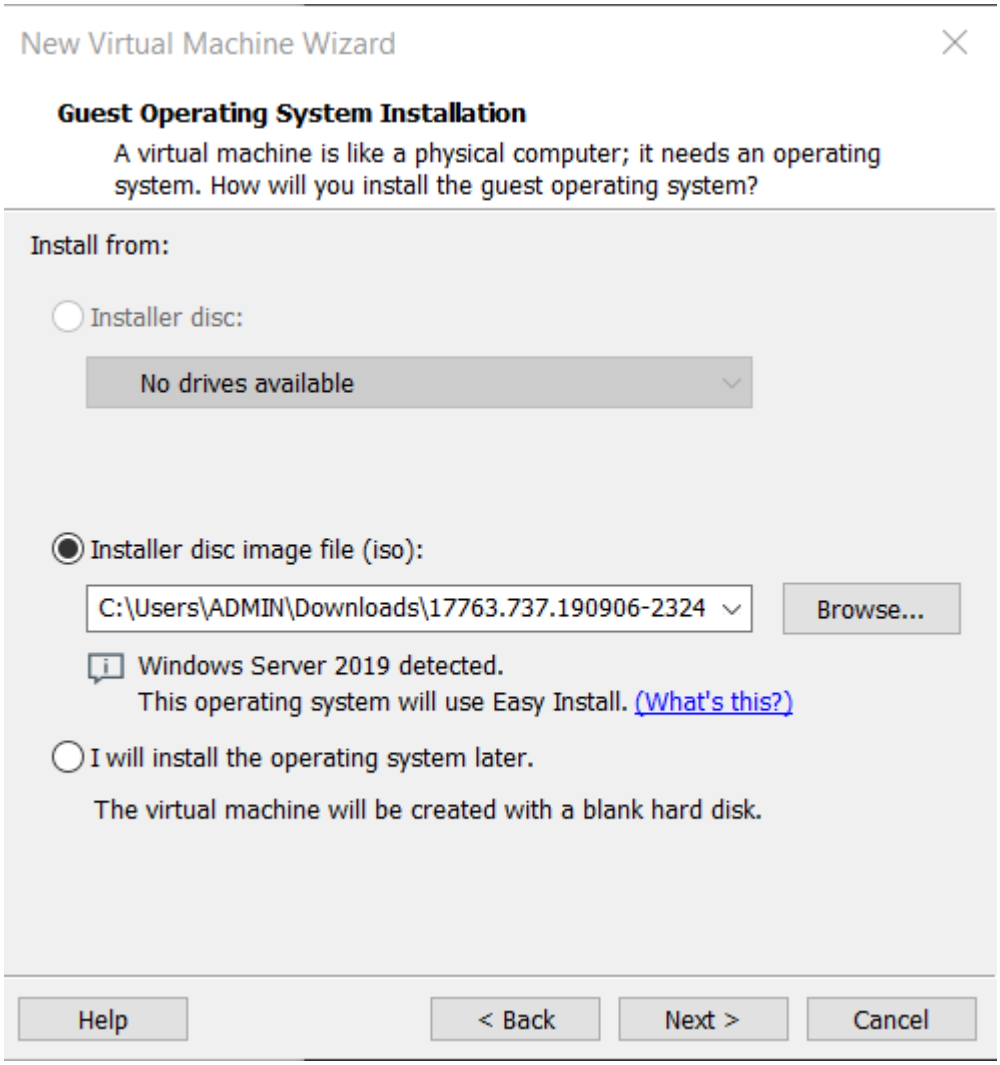
o Chủ yếu viết trên C và Assembly Code dành riêng cho các tác vụ yêu cầu truy nhập
với các chỉ lệnh vi xử lý cụ thể
+ Device Drivers: là một thành phần quan trọng được tải từ Kernel, thường kết thúc
bằng .sys. Đa phần được viết bằng C/C++. Chạy trong Kernel mode ở 1 trong 3 trường
hợp
o User Process 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
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)

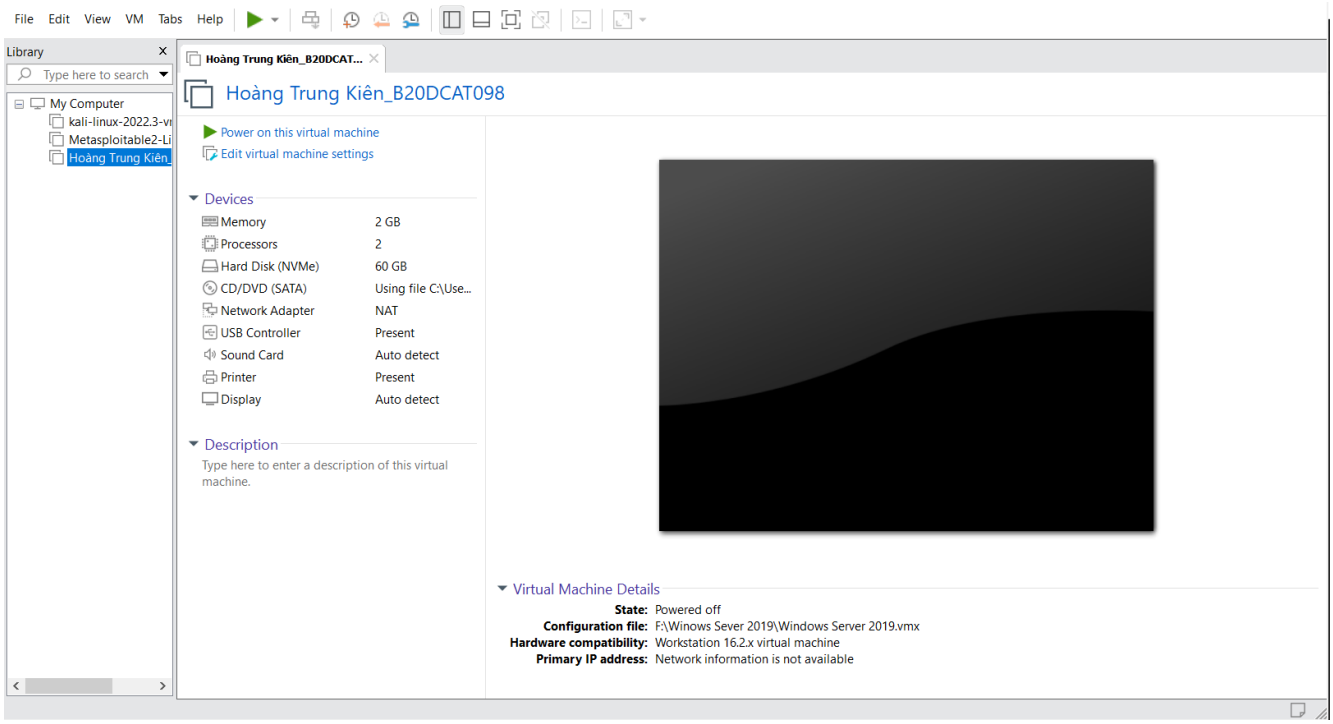
+ Local Security Authority Subsystem nằm ở \Windows\System32\Lsass.exe. Lsass gọi gói tin xác thực thích hợp (i.e. DLL) để kiểm tra Password có phù hợp với Data được lưu trong Security Accounts Manager (SAM) File. Sau khi xác thực thành công, Lsass gọi 1 hàm trong SRM (i.e.NtCreateToken) để tạo ra 1 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.

3. NỘI DUNG THỰC HÀNH

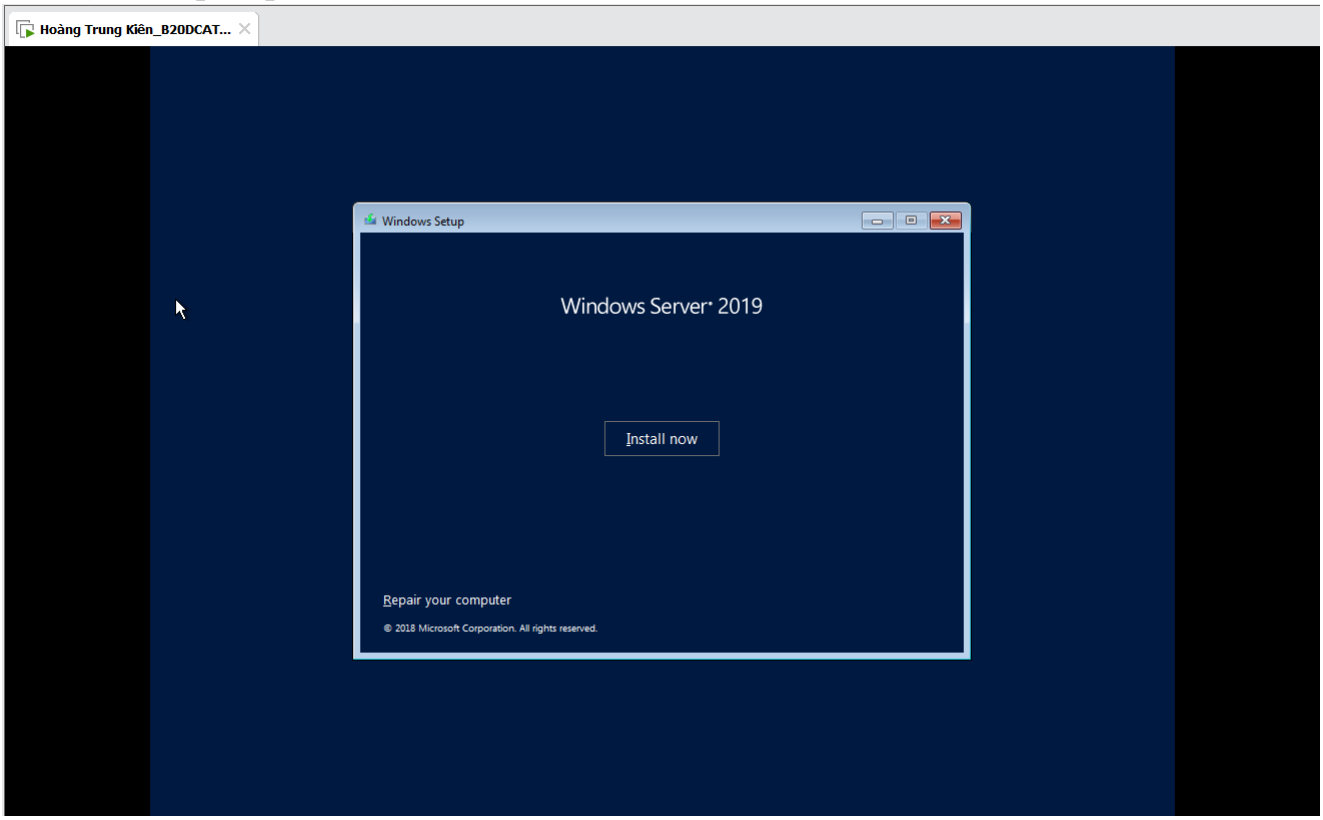
Bước 1: Cài đặt Windows Sever 2019 trên VMWare Workstation

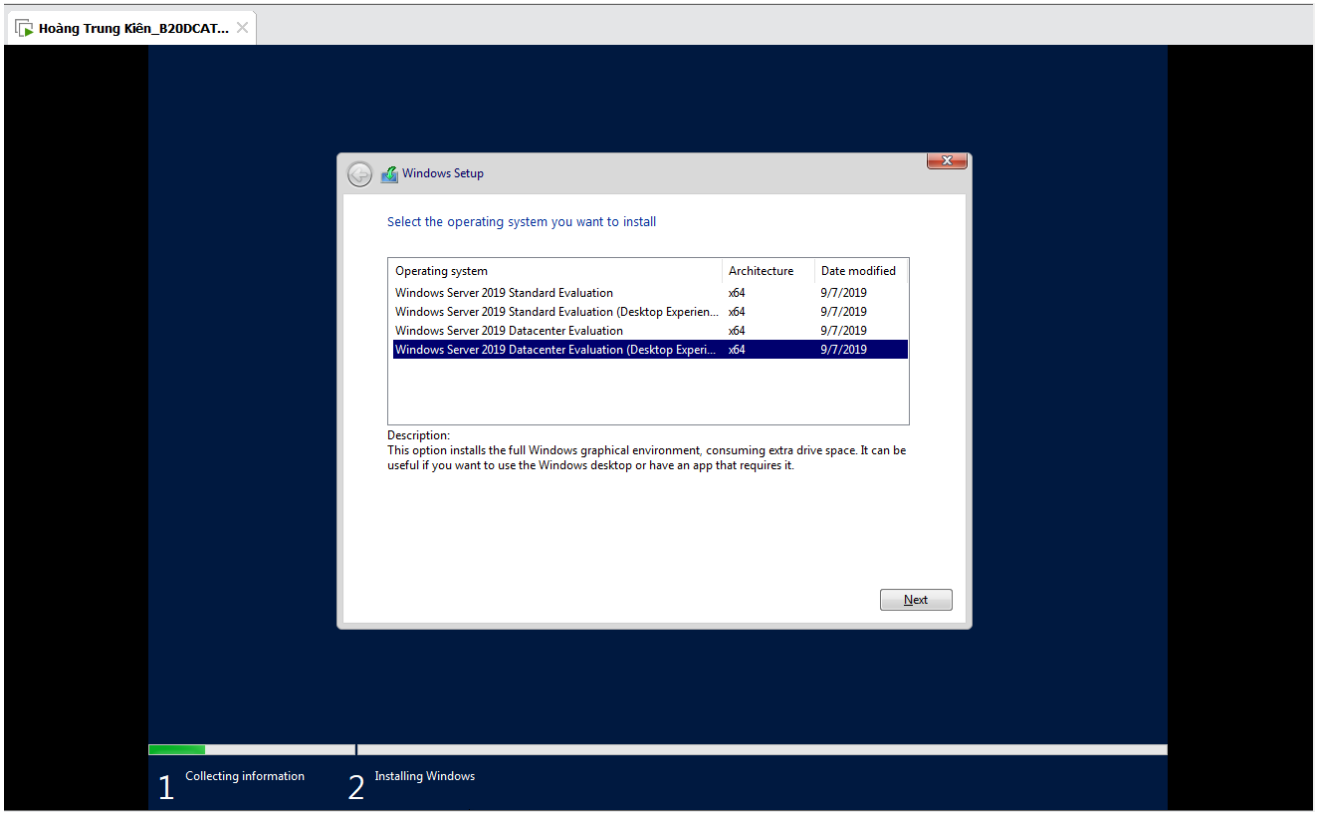
Ctrl+N -> chọn Typical -> Next -> chọn Install disc image file (iso) -> Next

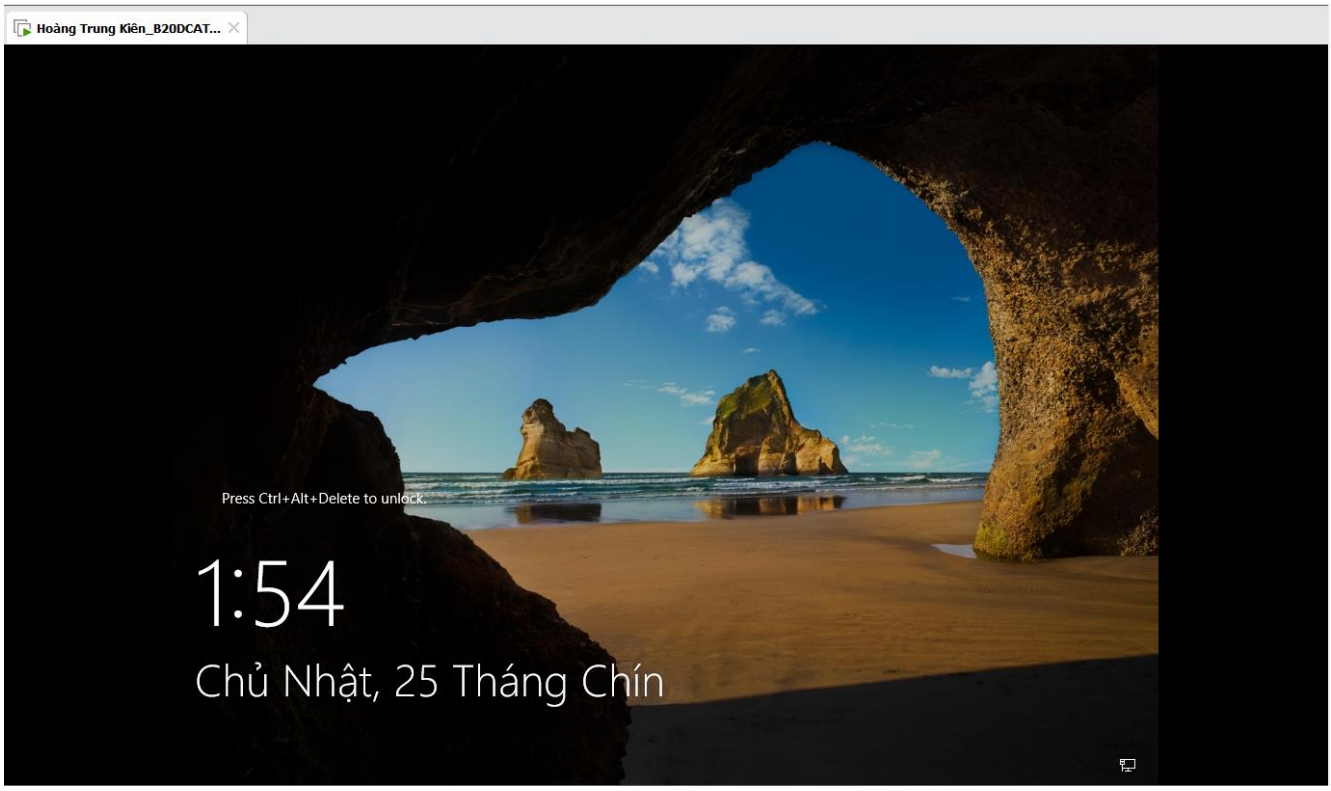

New Virtual Machine Wizard
Guest Operating System Installation
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
No drives available
Installer disc image file (iso):
C:\Users\ADMIN\Downloads\17763.737.190906-2324
Browse...
Windows Server 2019 detected.
This operating system will use Easy Install. (What's this?)
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel


File Edit View VM Tabs Help
Library
Type here to search
My Computer
kali-linux-2022.3-vr
Metasploitable2-Li
Hoàng Trung Kiên_
Hoàng Trung Kiên_B20DCAT...
Hoàng Trung Kiên_B20DCAT098
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 2 GB
Processors 2
Hard Disk (NVMe) 60 GB
CD/DVD (SATA) Using file C:\Use...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Printer Present
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: F:\Winows Sever 2019\Windows Server 2019.vmx
Hardware compatibility: Workstation 16.2.x virtual machine
Primary IP address: Network information is not available

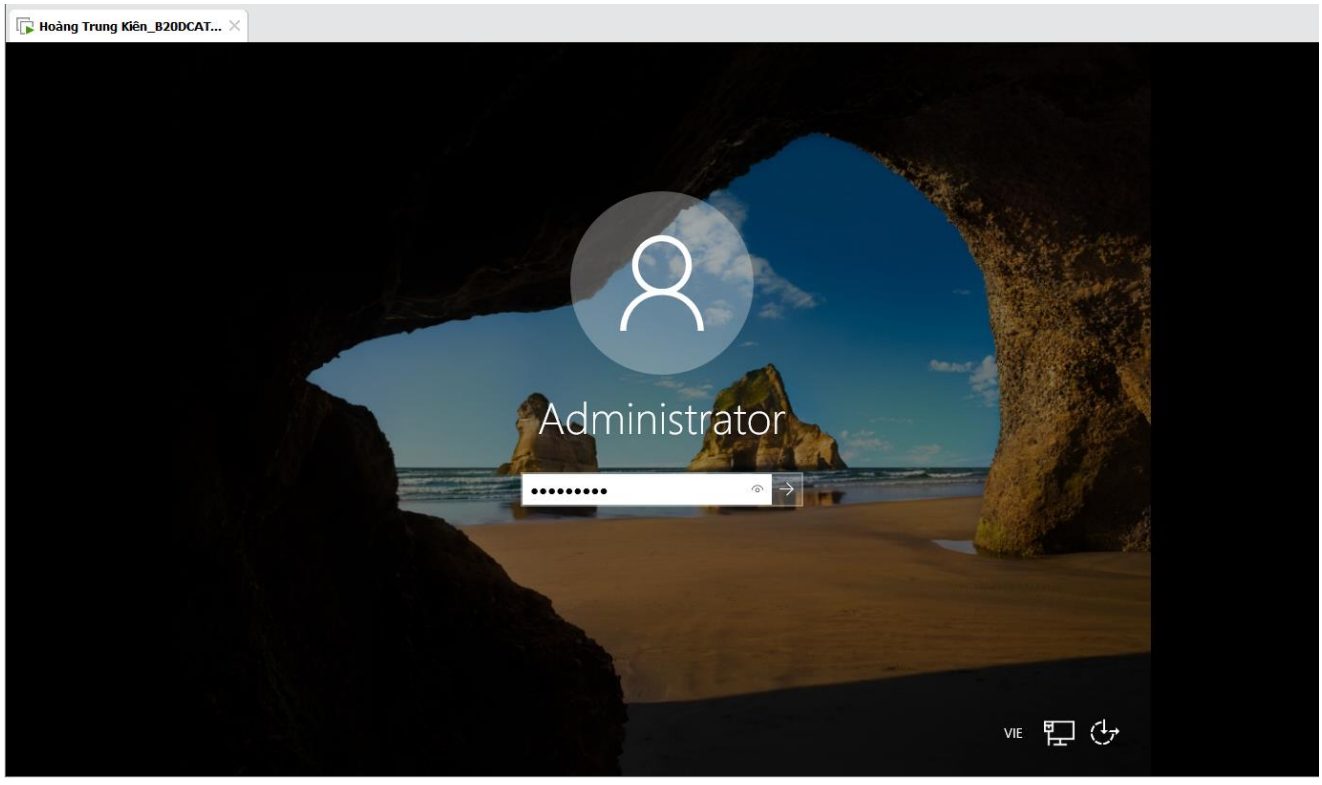
Chọn Install Now -> Windows Server 2019 Datacenter Evaluation (Desktop Experien…)

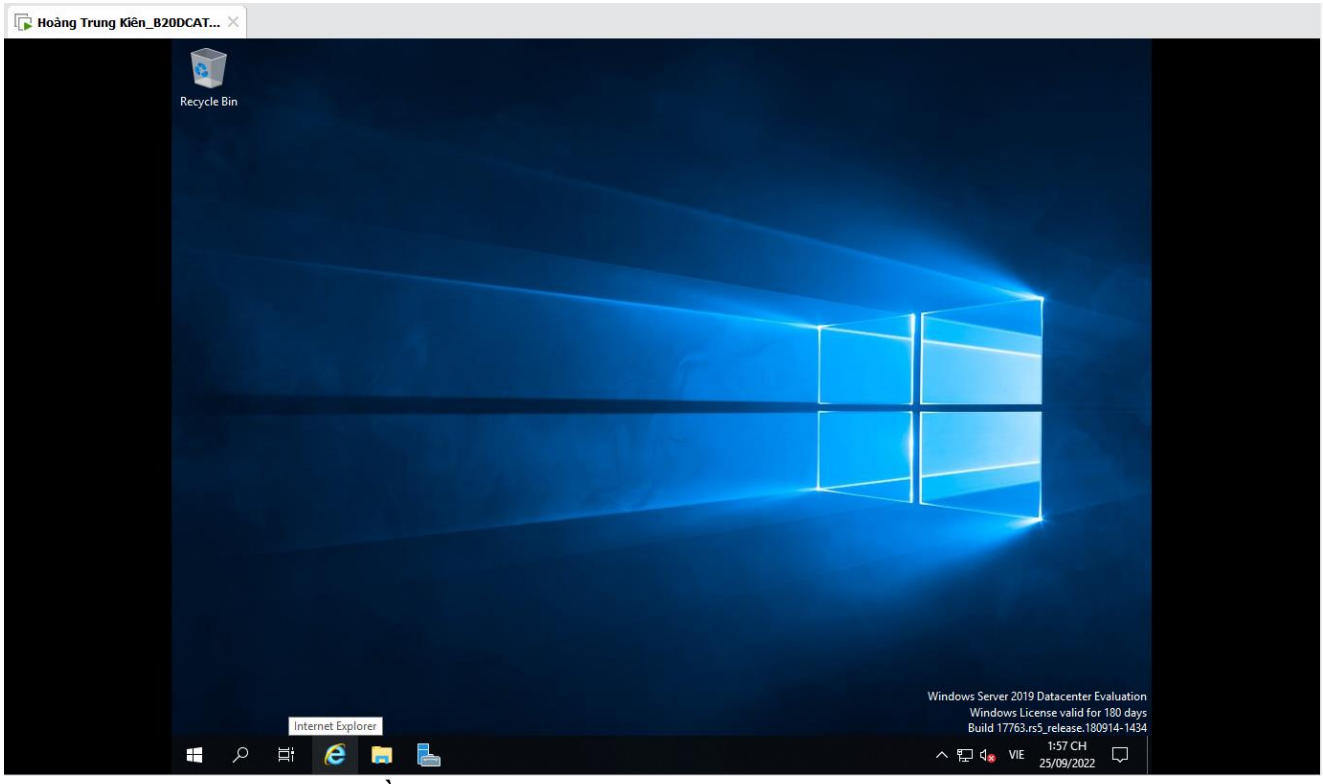






-Tiến hành đăng nhập bằng tài khoản đã cấu hình ở bước trước, đăng nhập thành công giao diện chính của Windows Server 2019



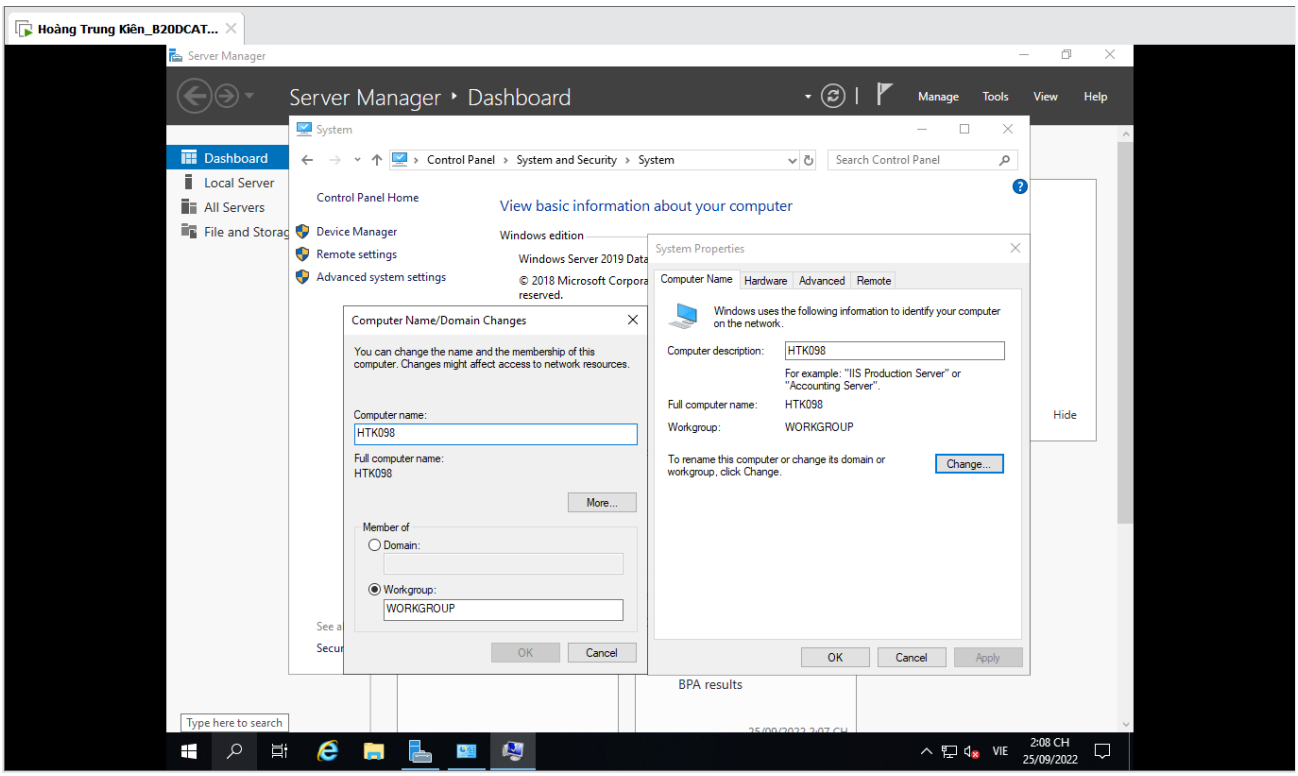


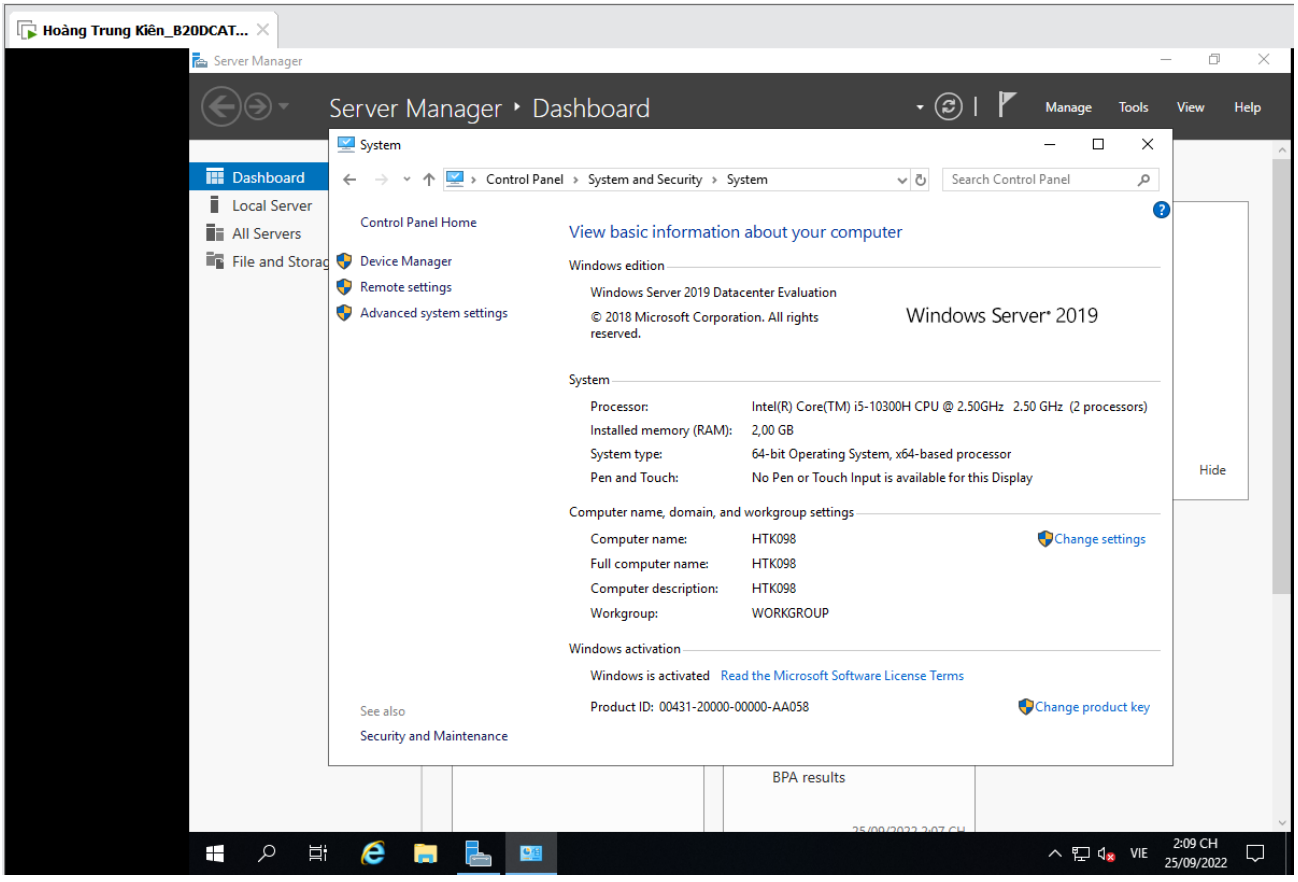
-Cài đặt thành công hệ điều hành Windows Server 2019 trên máy ảo VMWare.

Bước 2: Nâng cấp Server thành Domain Controller

-Kiểm tra tên và đổi tên của sever

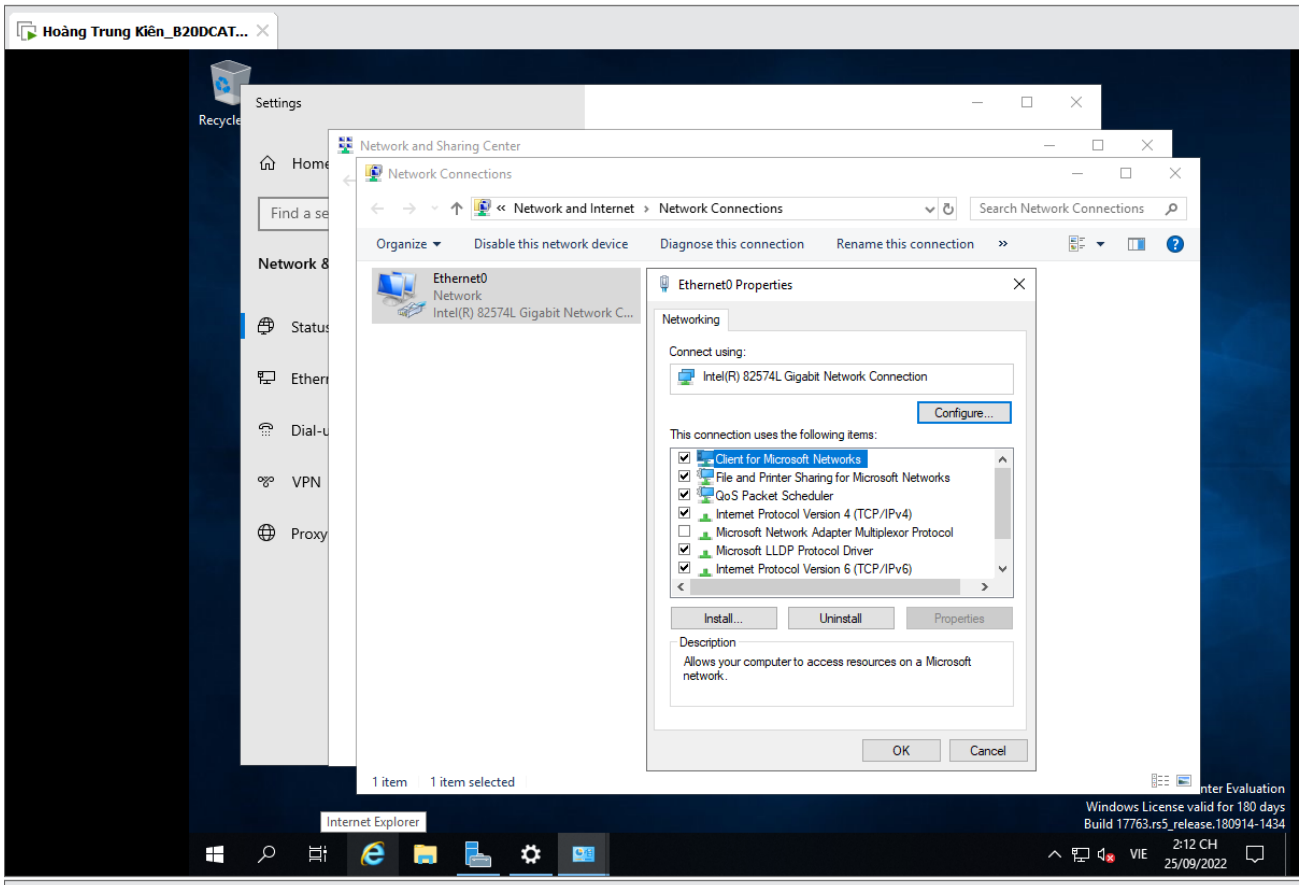
+This PC (chuột phải) -> Properties -> Advanced System Setting -> Computer Name ->Kiểm tra đúng/sai hoặc Thay đổi (change).

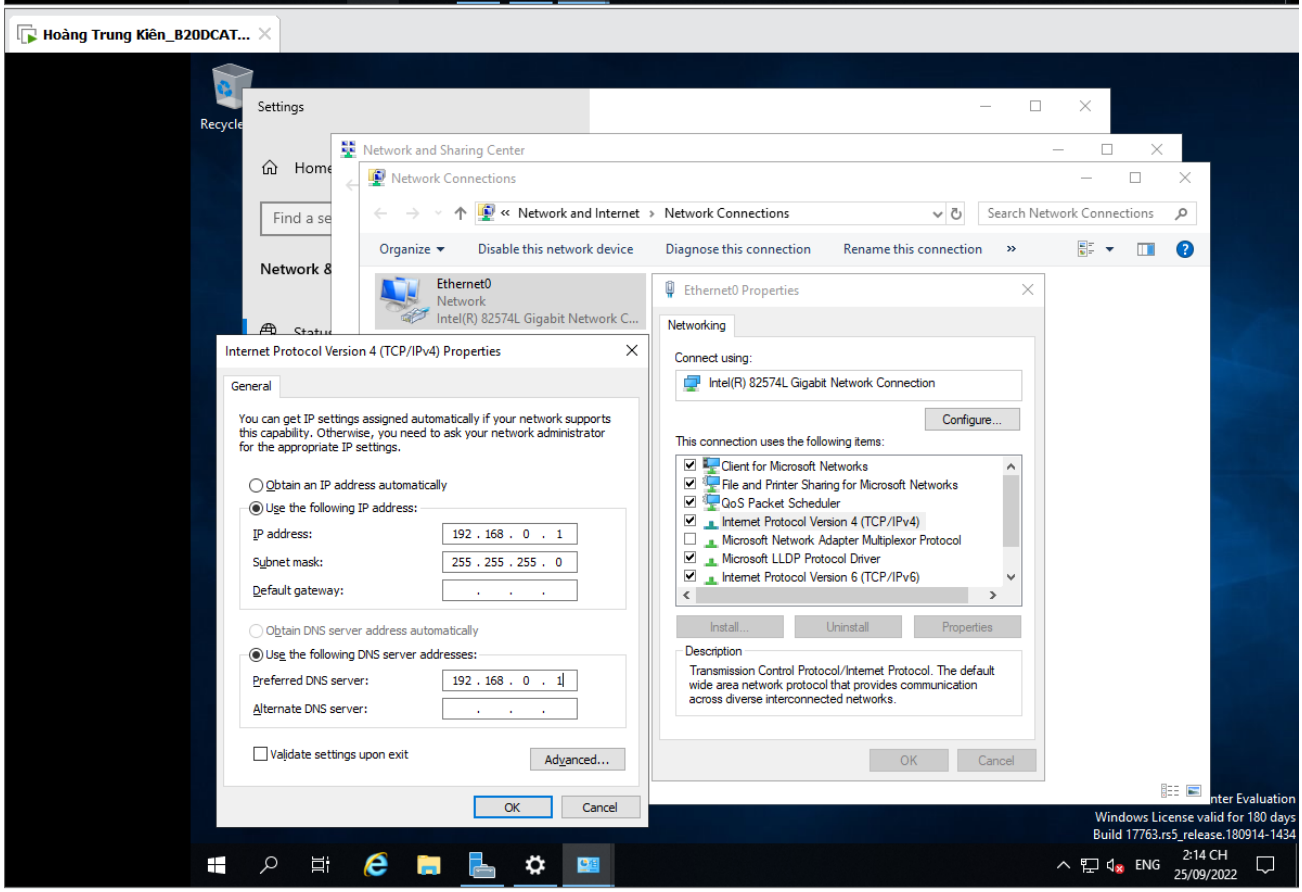




- Cài đặt static IP

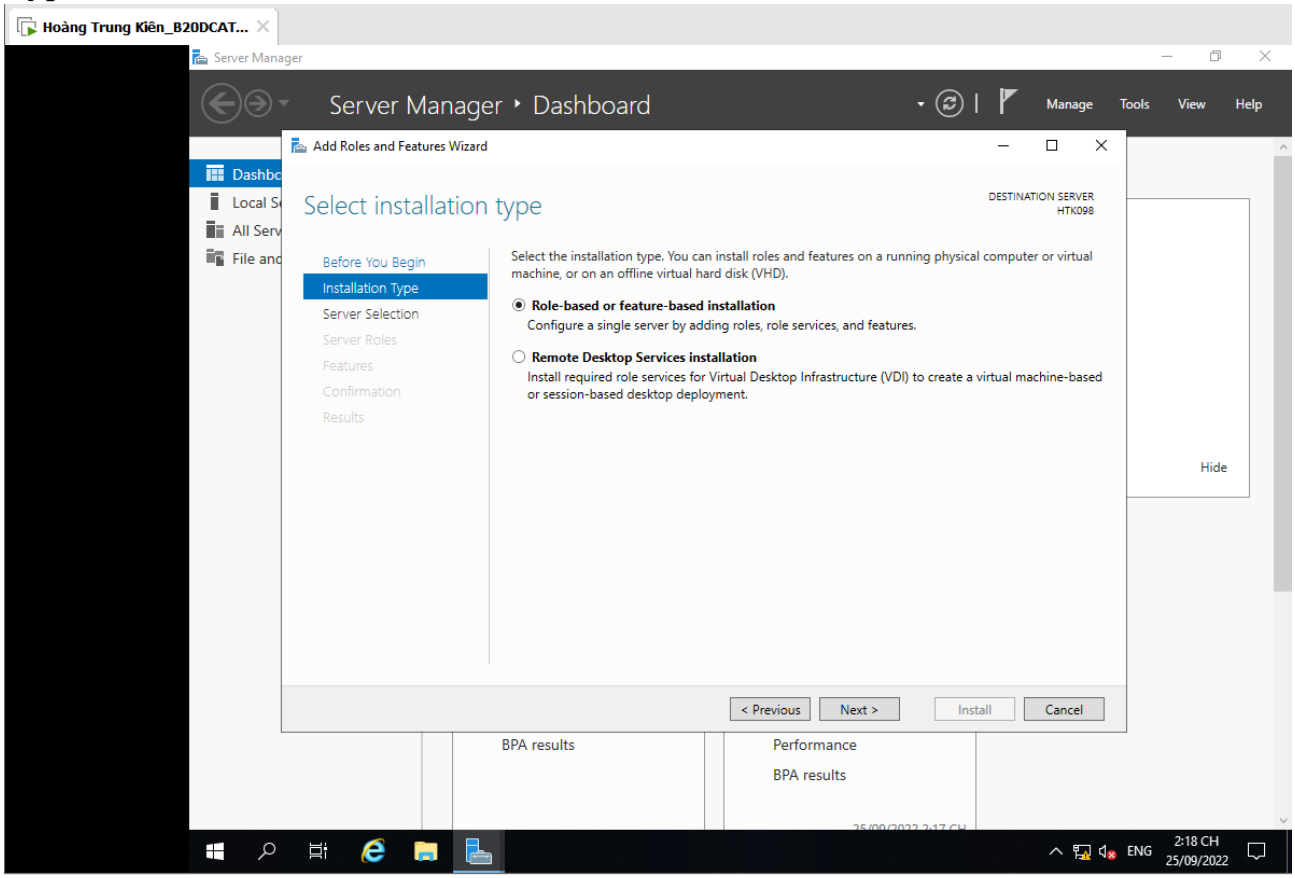
+Open Network and Sharing Center (Chuột phải) -> Change Adapter Settings -> Ethernet0 (Chuột phải)-> Properties-> Internet Protocol Version 4 (TCP/IP) Properties -> Use the following IP address -> Restart


Hoàng Trung Kiên_B20DCAT...
Recycle
Settings
Network and Sharing Center
Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet0
Network
Intel(R) 82574L Gigabit Network C...
Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
OK
Cancel
1 item
1 item selected
Internet Explorer
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
VIE
2:12 CH
25/09/2022

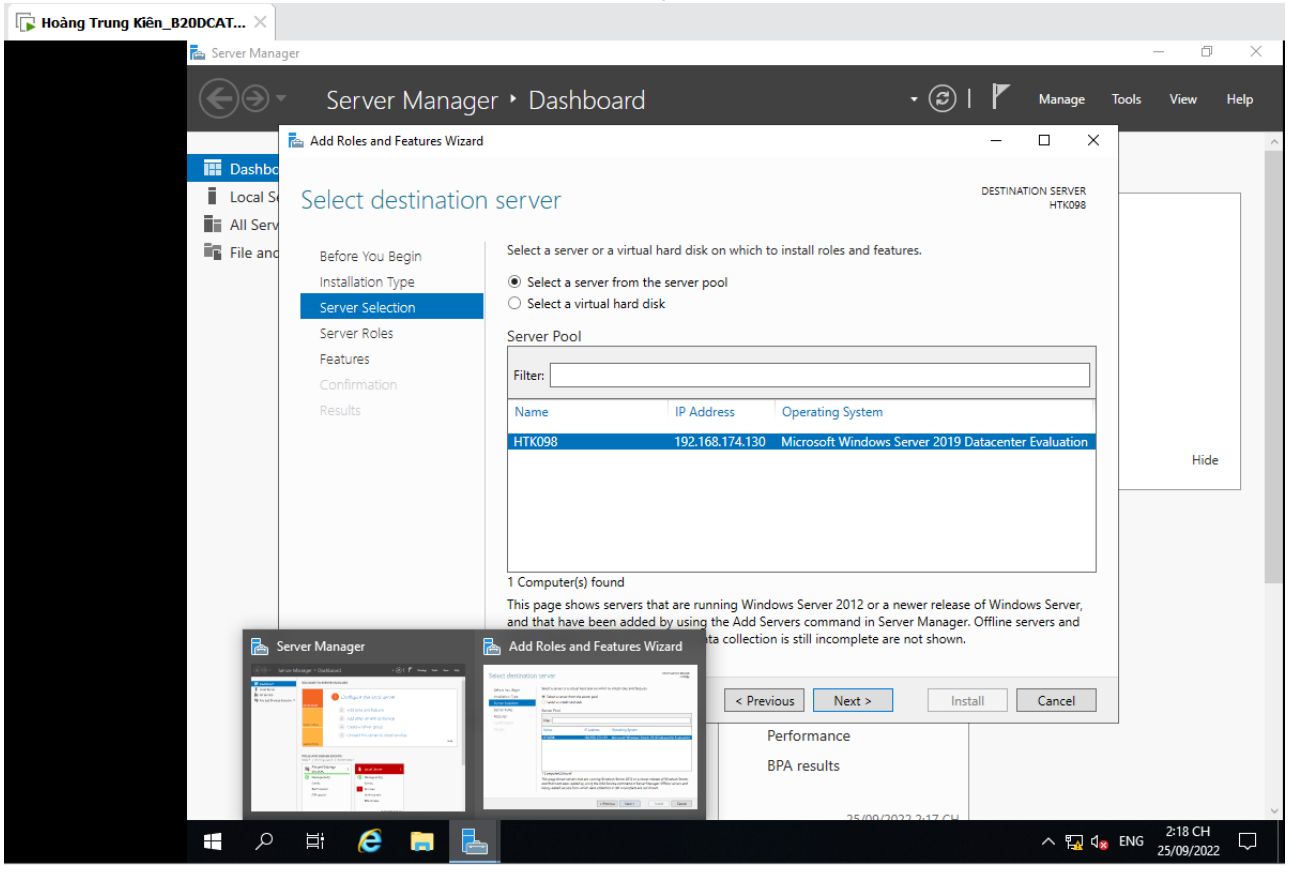

Hoàng Trung Kiên_B20DCAT...
Recycle
Settings
Network and Sharing Center
Network Connections
« Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
Ethernet0
Network
Intel(R) 82574L Gigabit Network C...
Ethernet0 Properties
Networking
Connect using:
Intel(R) 82574L Gigabit Network Connection
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 1
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
Windows License valid for 180 days
Build 17763.rs5_release.180914-1434
ENG
2:14 CH
25/09/2022

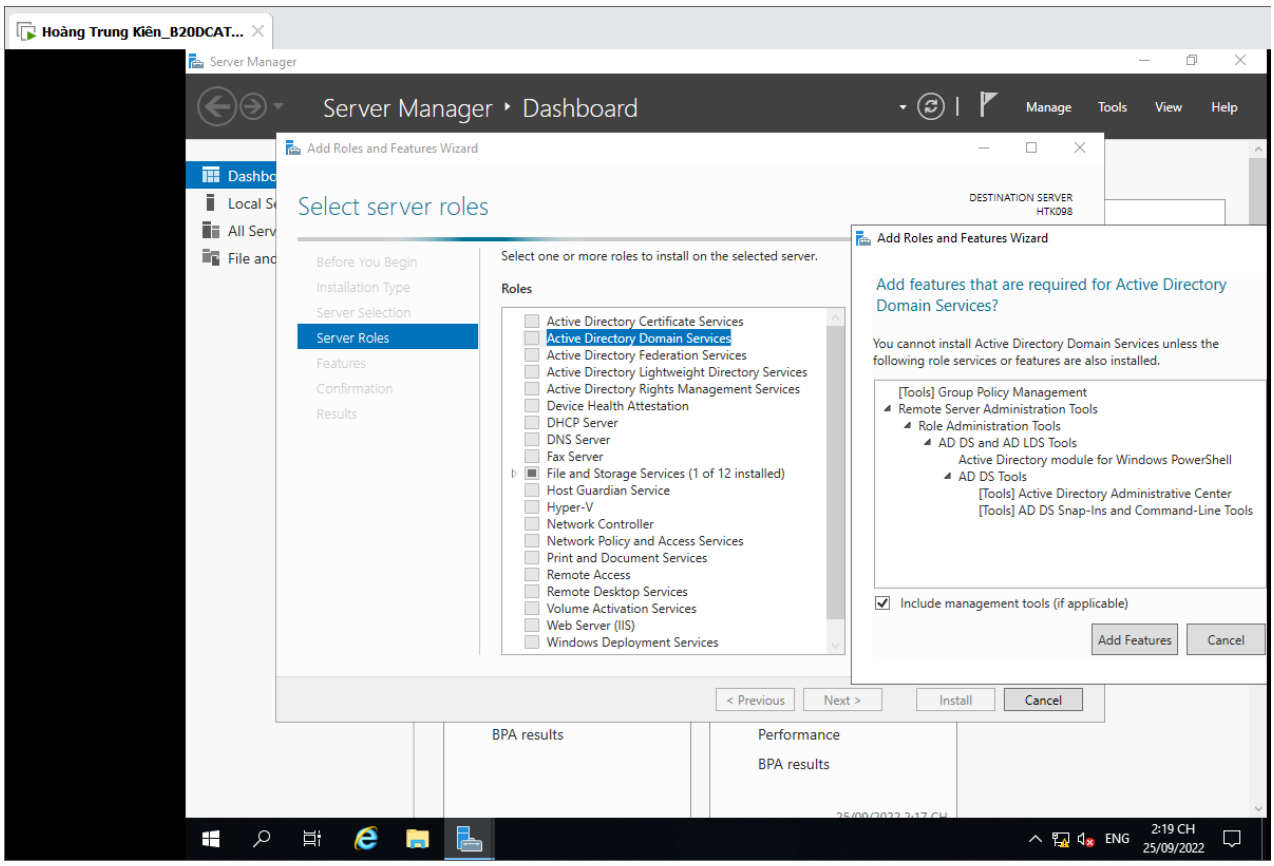
-Cài đặt server role trong Server Manager

Open Server Manager -> Manager -> Add roles and features -> Installation Type -> Chọn Roles based or features base installation -> Next



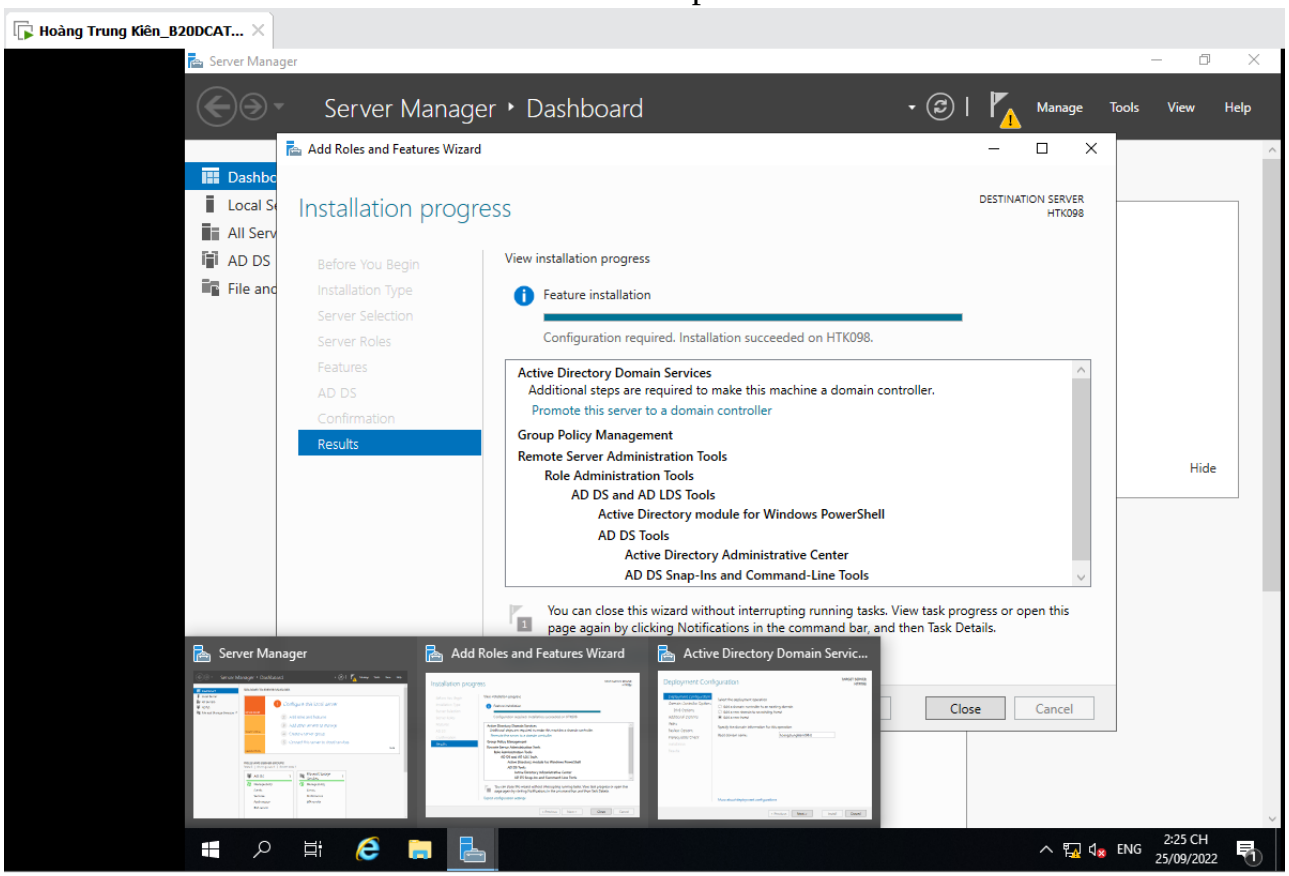
Server Selection -> Next -> Active Directory Domain Services -> Add features

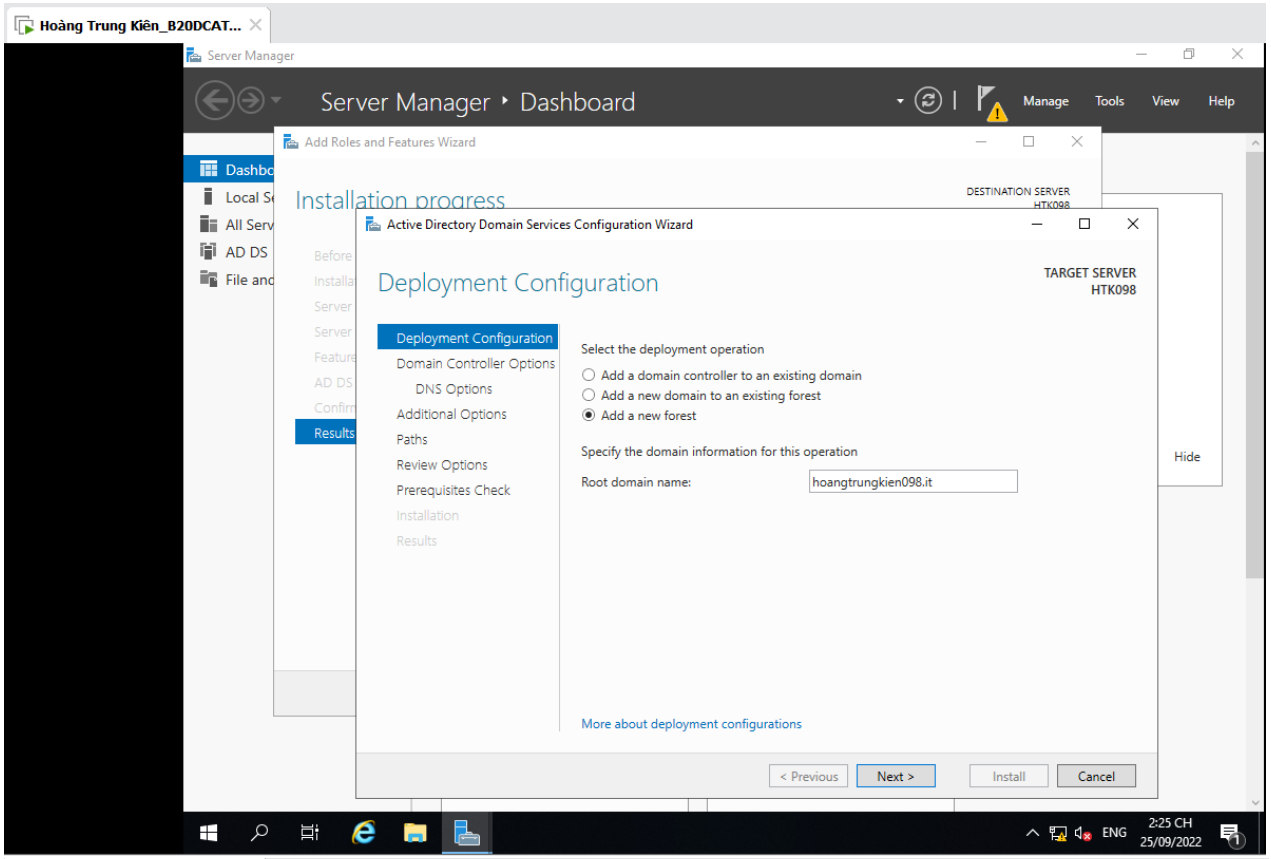


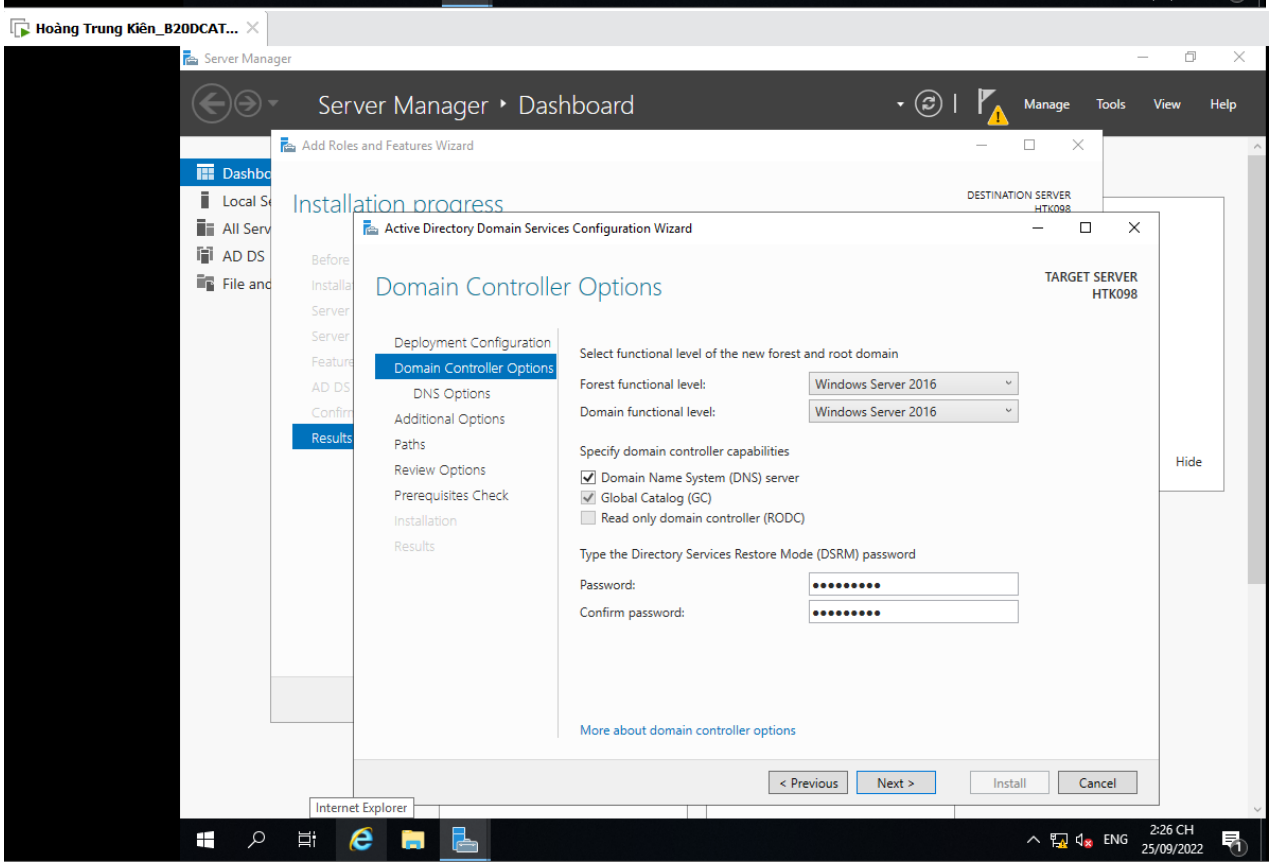


- Nâng cấp Server thành Domain Controller

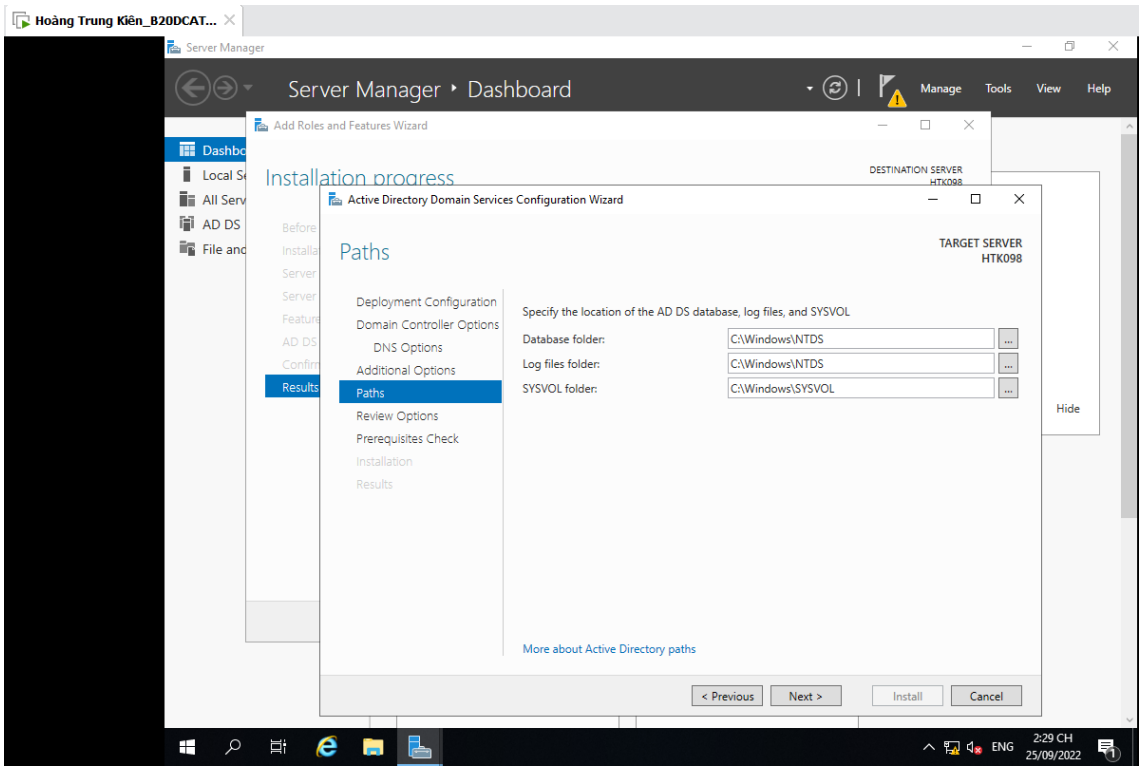
Rename root domain name -> Next -> Create password -> Next



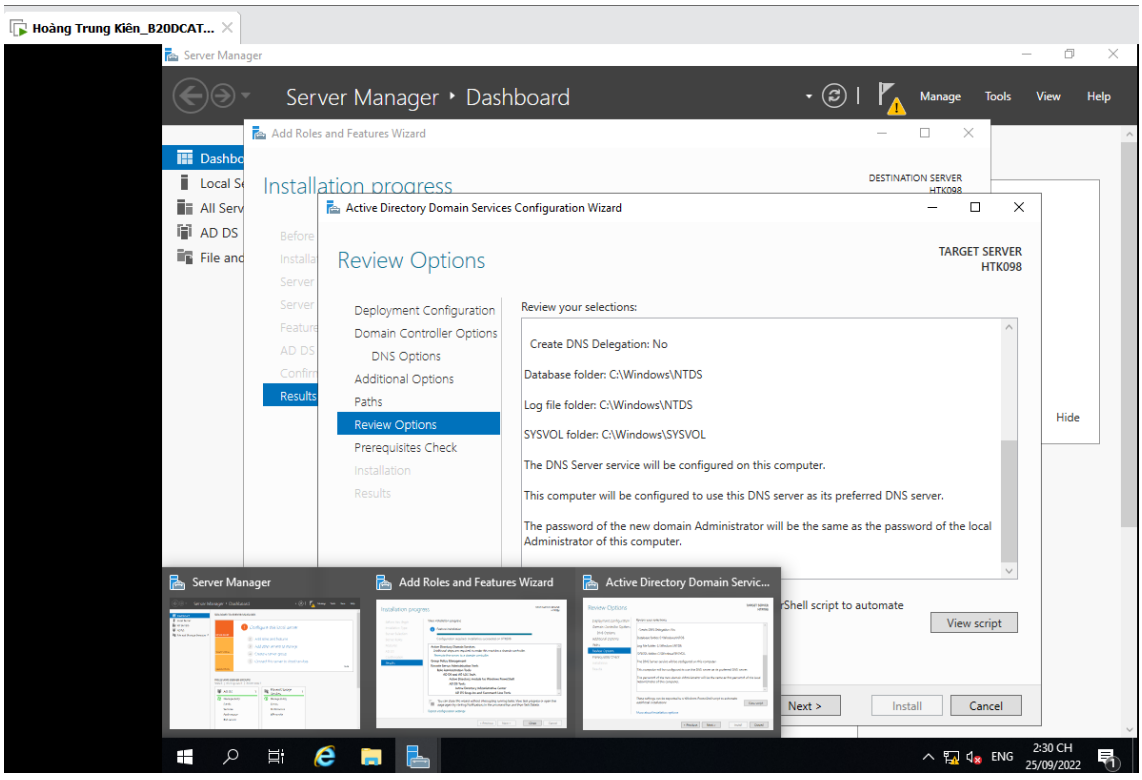

Hoàng Trung Kiên_B20DCAT...
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
HTK098
Active Directory Domain Services Configuration Wizard
Deployment Configuration
TARGET SERVER
HTK098
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select the deployment operation
Add a domain controller to an existing domain
Add a new domain to an existing forest
Add a new forest
Specify the domain information for this operation
Root domain name:
hoangtrungkien098.it
More about deployment configurations
< Previous
Next >
Install
Cancel
Hide
ENG
2:25 CH
25/09/2022

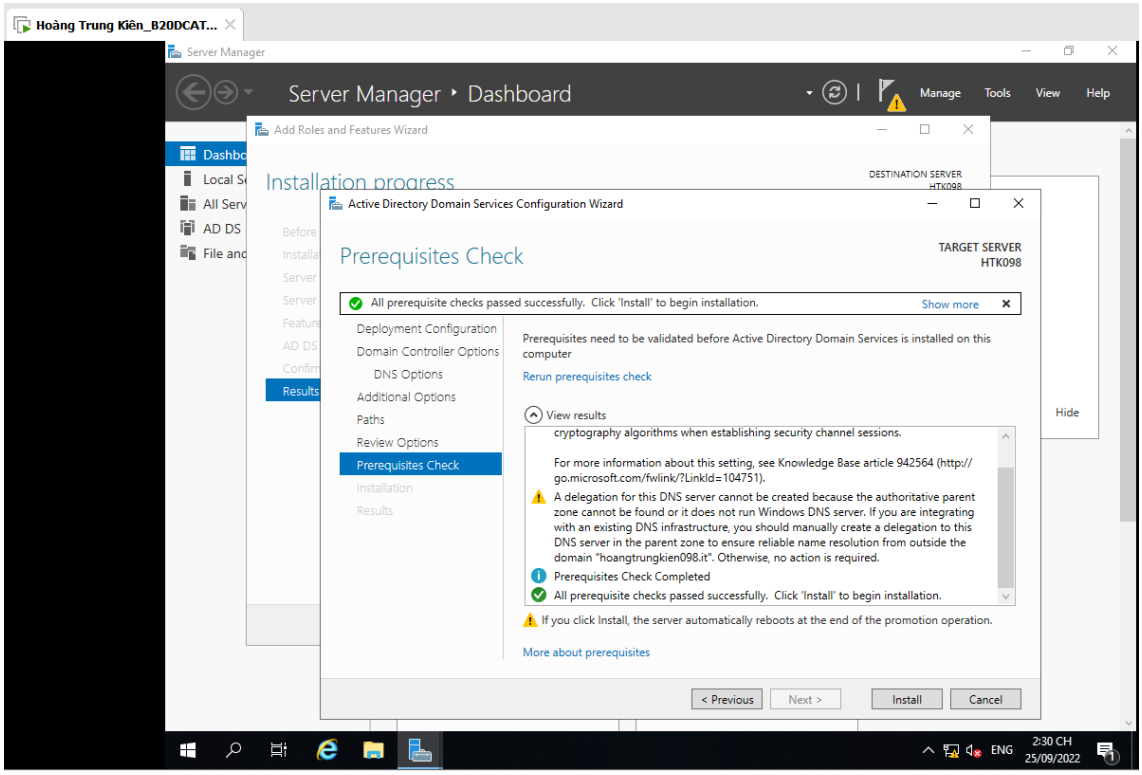

Hoàng Trung Kiên_B20DCAT...
Server Manager
Server Manager • Dashboard
Manage
Tools
View
Help
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
HTK098
Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
HTK098
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2016
Domain functional level:
Windows Server 2016
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel
Hide
Internet Explorer
ENG
2:26 CH
25/09/2022

-Lưu vị trí các Database



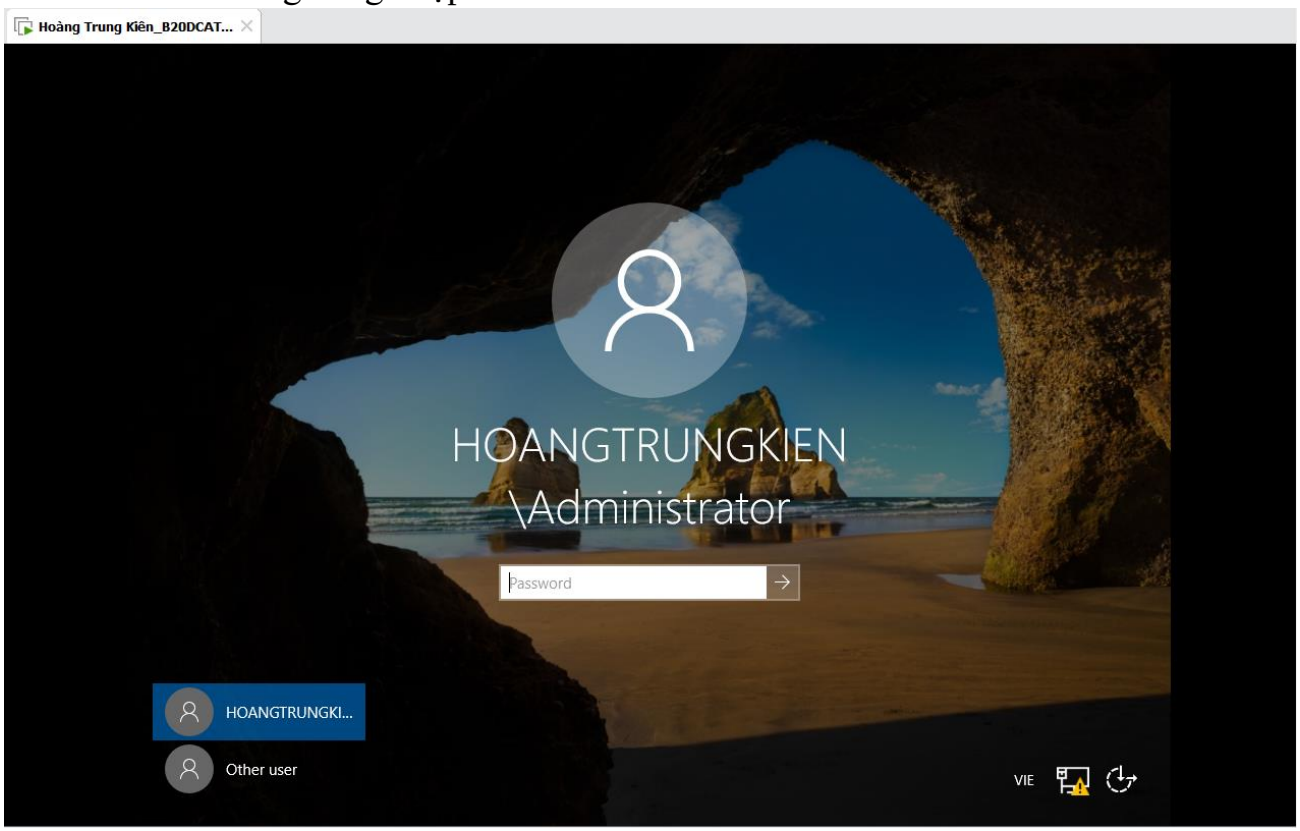
+Chọn review options -> next -> kiểm tra thành công -> install -> sau đó máy restars.





Bước 3: Kiểm tra kết quả đạt được

Sau khi install xong đăng nhập vào Windows Server



Open Control Panel -> System and Security -> System
Result: Đã nâng cấp thành công