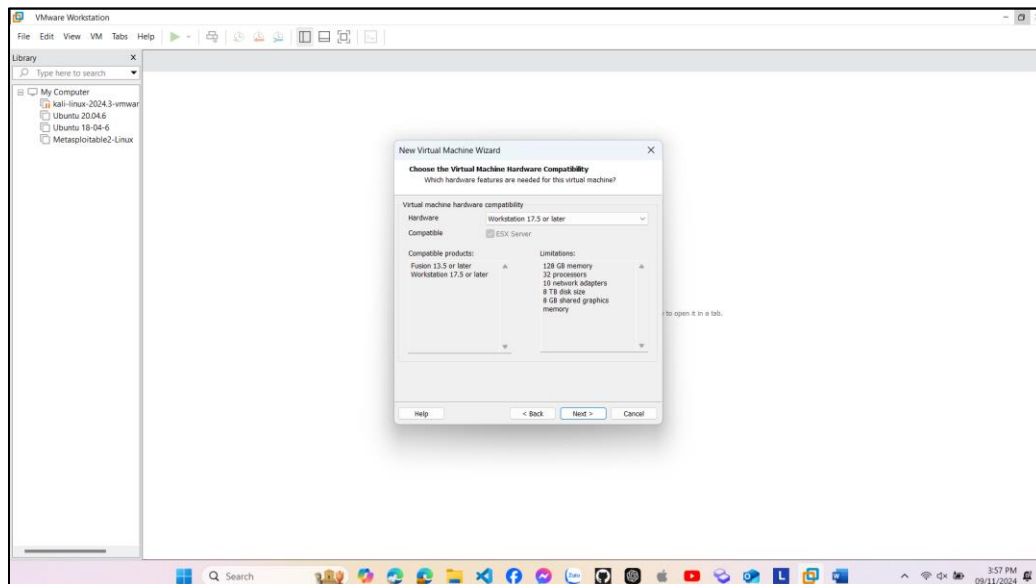
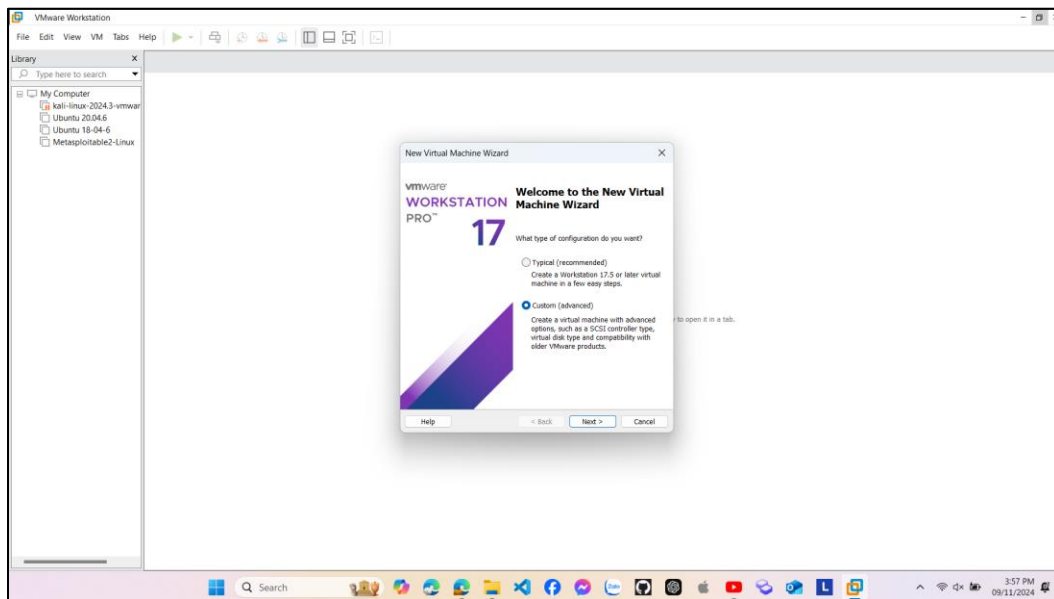


# BÁO CÁO

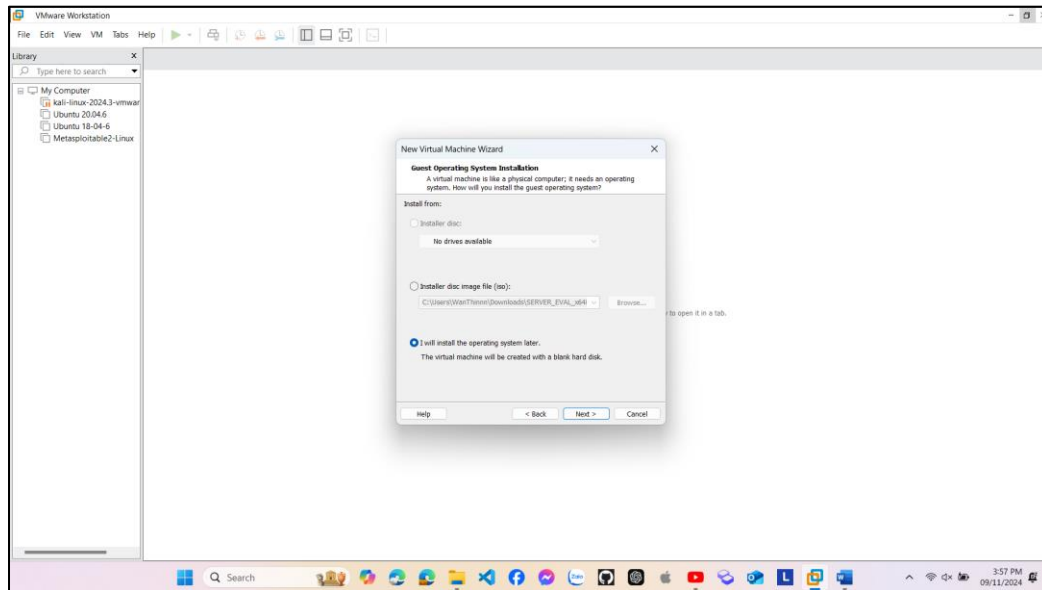
## Bài tập 8.1. Thực hiện các cấu hình trên Windows Server

### I. Cấu hình các thông số cần thiết trên VMWare Workstation Pro 17 cho Windows Server 2022

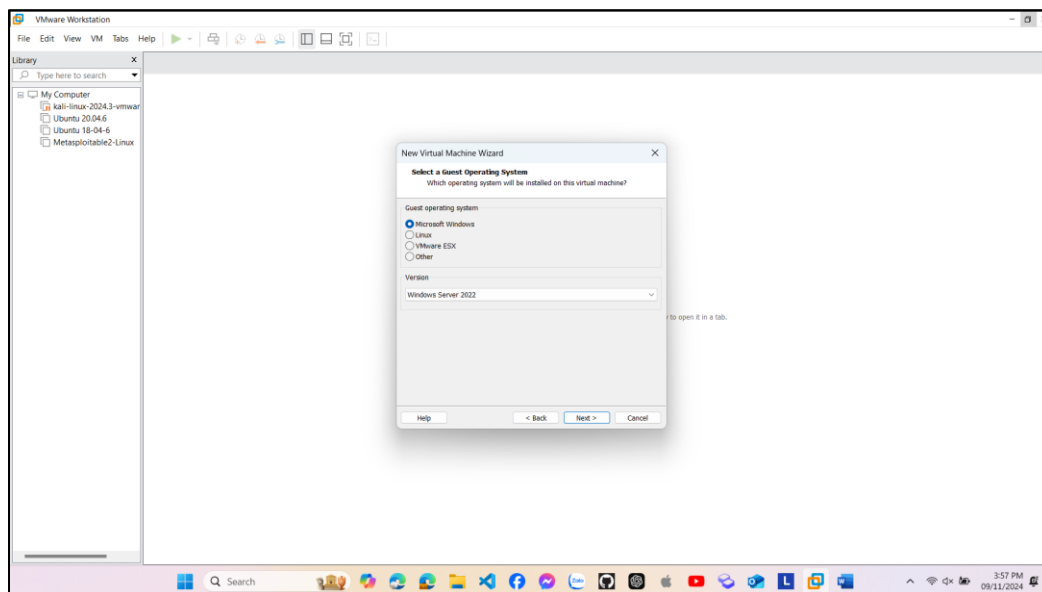
- Mở app VMWare Workstation Pro 17, tại Home -> Create a New Virtual Machine
- Tại cửa sổ này, chúng ta chọn config là Custom để tiện cho việc config nhiều thông số hơn.



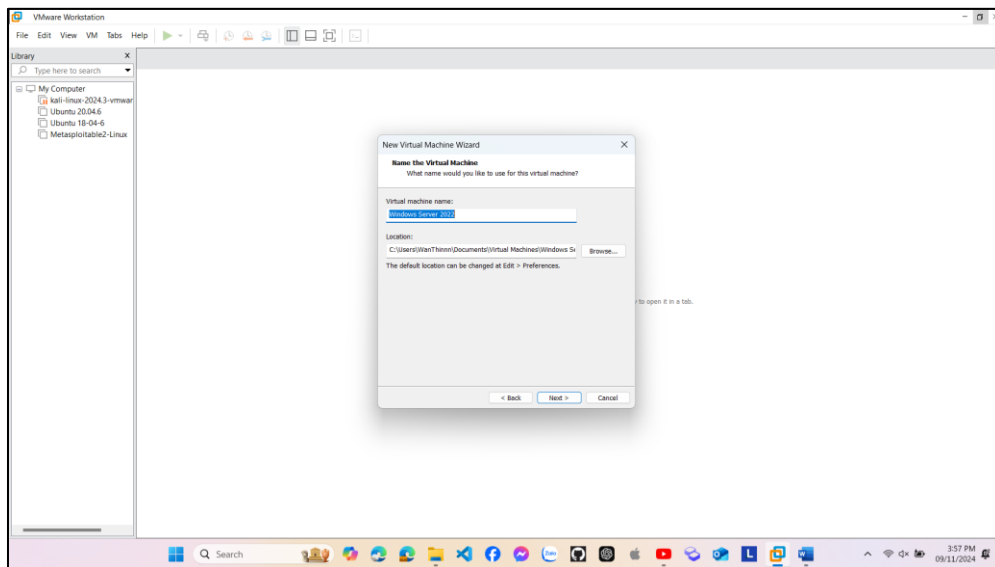
- Chỗ này ta chọn “I will install the operating system later” để tiện cho việc config thông số phần cứng, sau khi config xong thì import file iso vào sau.



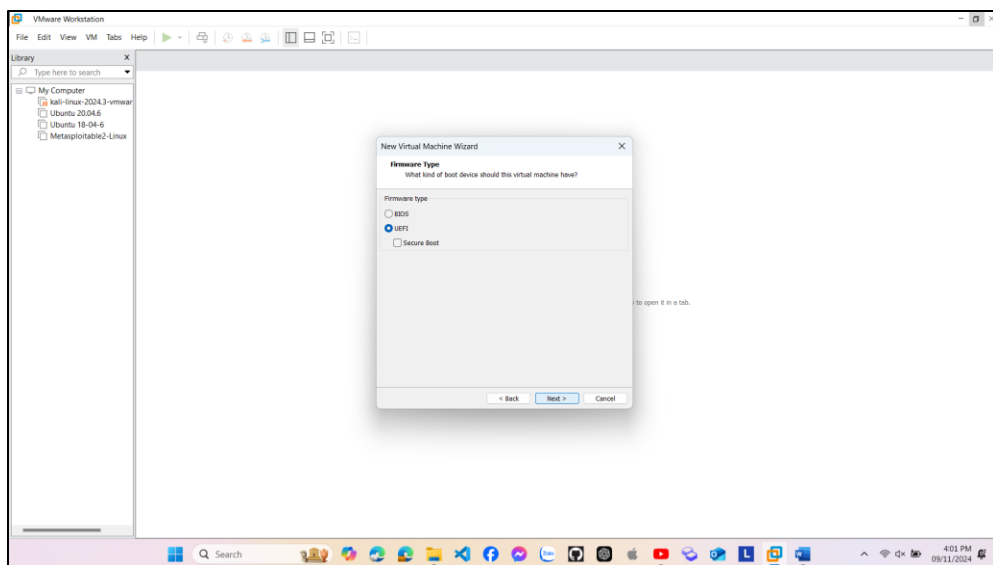
- Chọn OS là Microsoft Windows với Version là Windows Server 2022.

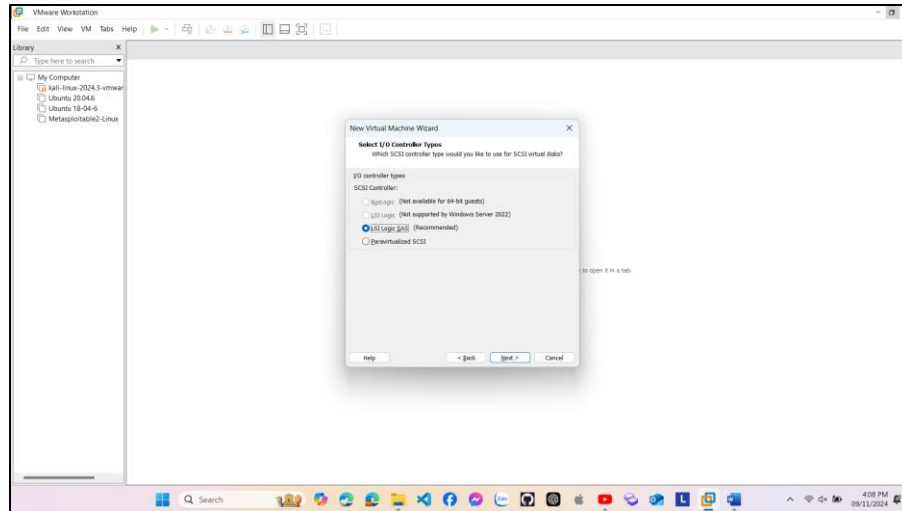


- Đặt tên cho máy ảo và thư mục lưu trữ máy ảo đó.

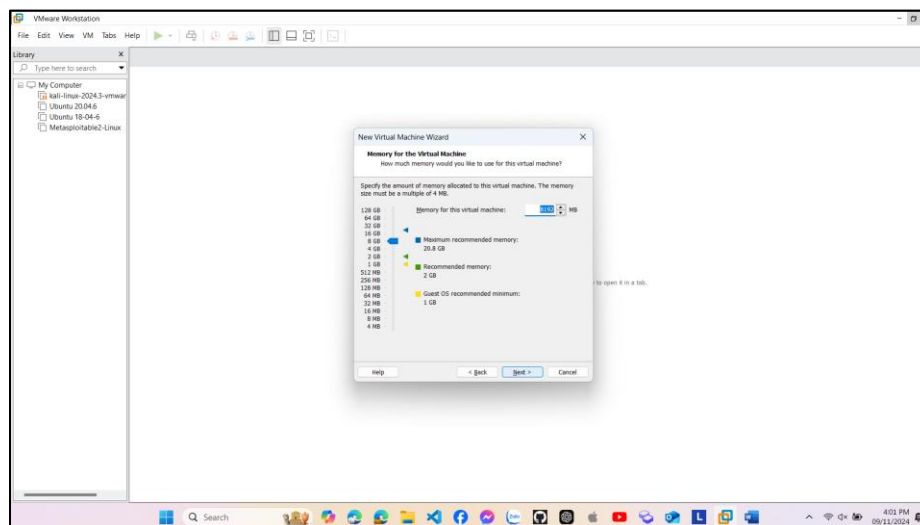
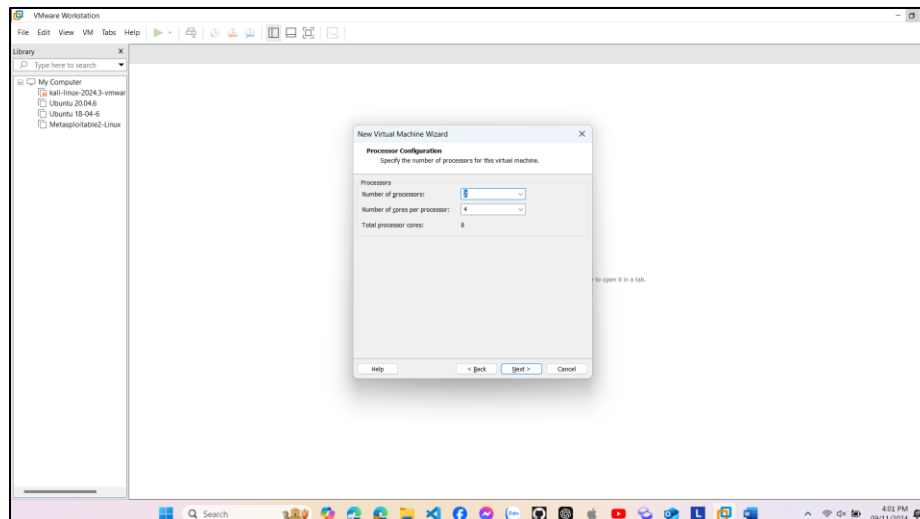


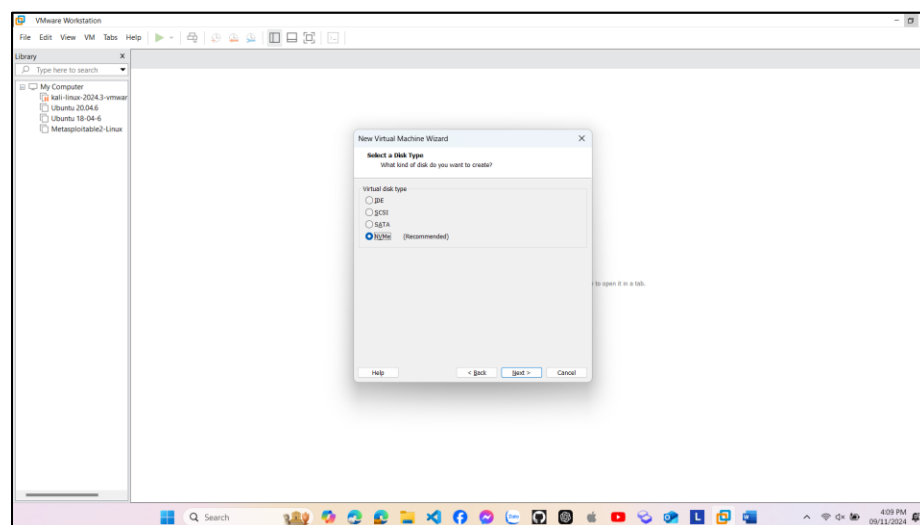
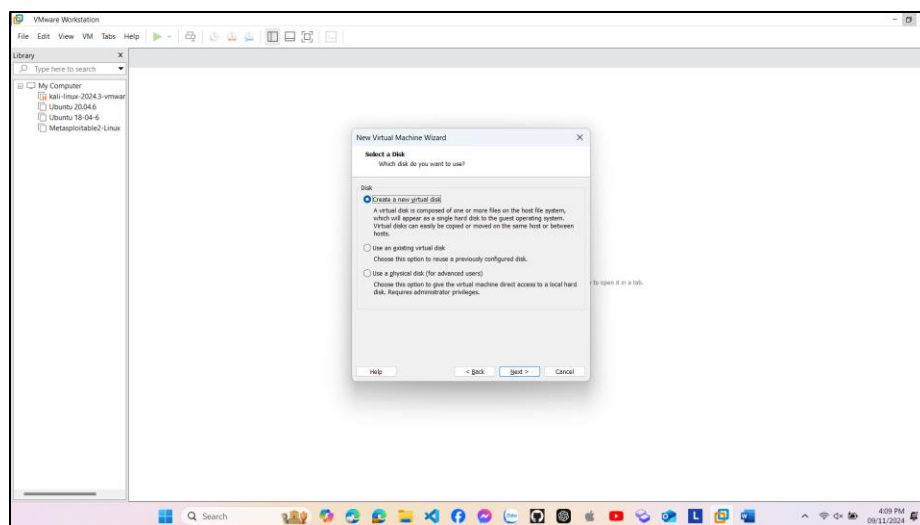
- Cấu hình các thông số cần thiết cho máy ảo:



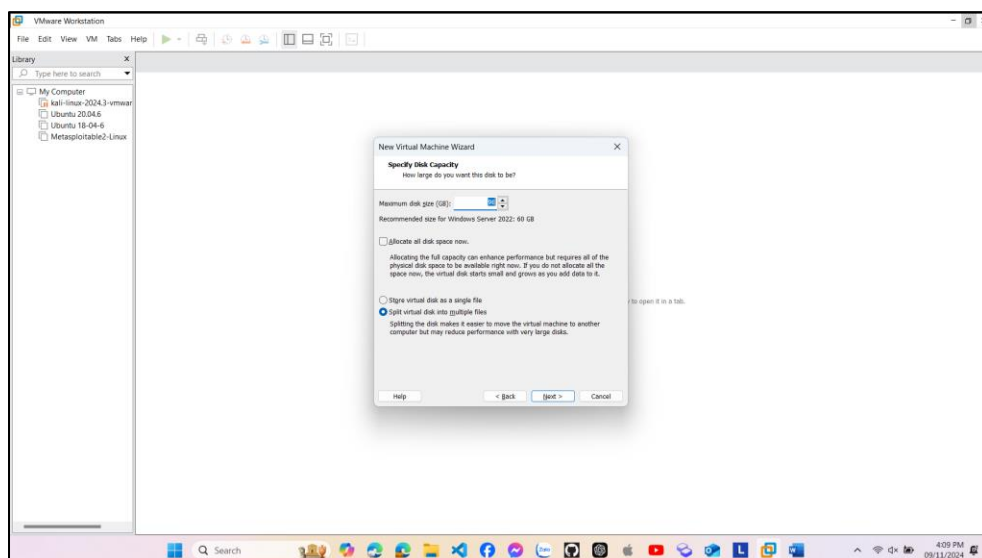


- Thông số của máy thật: Lenovo LOQ 2024:
  - + Ram 24GB DDR5 – Dual Channel - 4800 MHz
  - + 512 GB SSD NVMe PCIe
  - + NVIDIA GeForce RTX 3050, 6 GB
  - + Intel Core i5 Alder Lake - 12450HX - 8 nhân 12 luồng
- Dựa vào thông số của máy thật, ta có thể cấp phát cho máy ảo như sau:
  - + 4GB Ram
  - + 8 nhân Processor
  - + Sử dụng mạng NAT
  - + Các thông số còn lại để mặc định theo đề xuất của Vmware

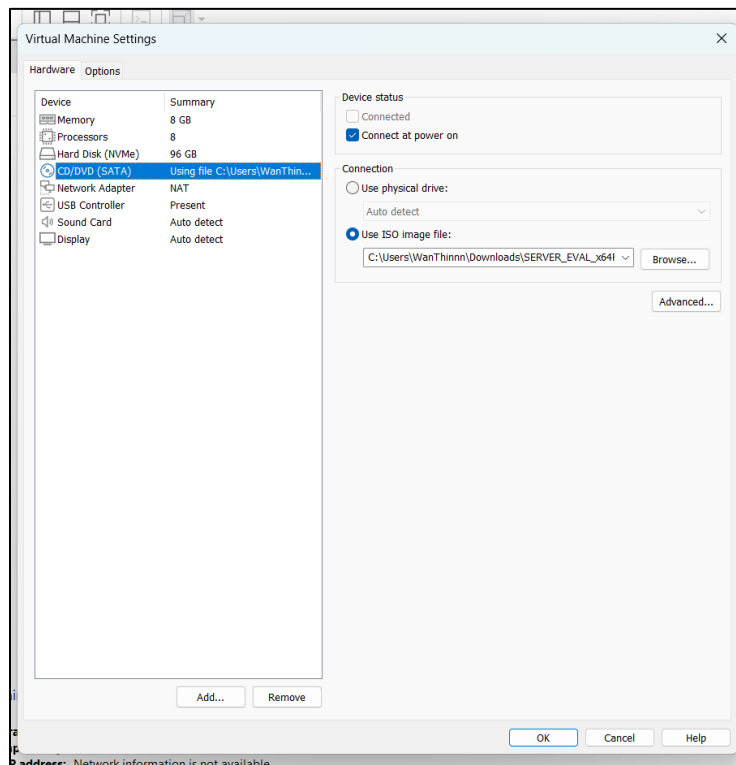




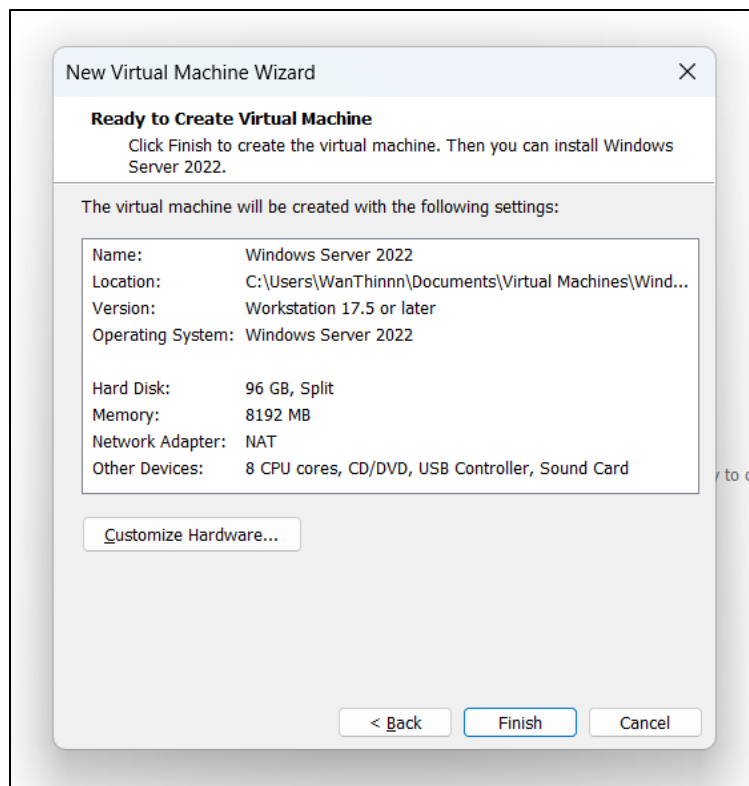
- Cấp dung lượng cho máy ảo là 96GB.



- Tại đây, ta chọn luôn file iso của Windows Server 2022:

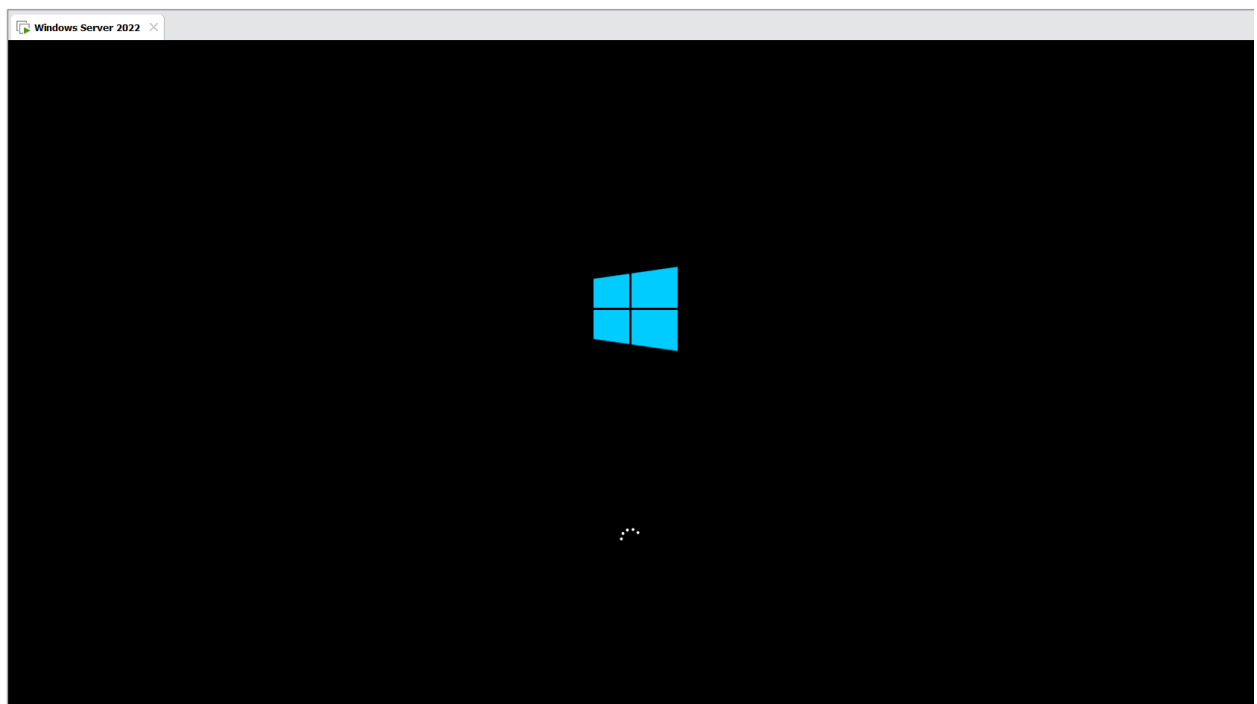
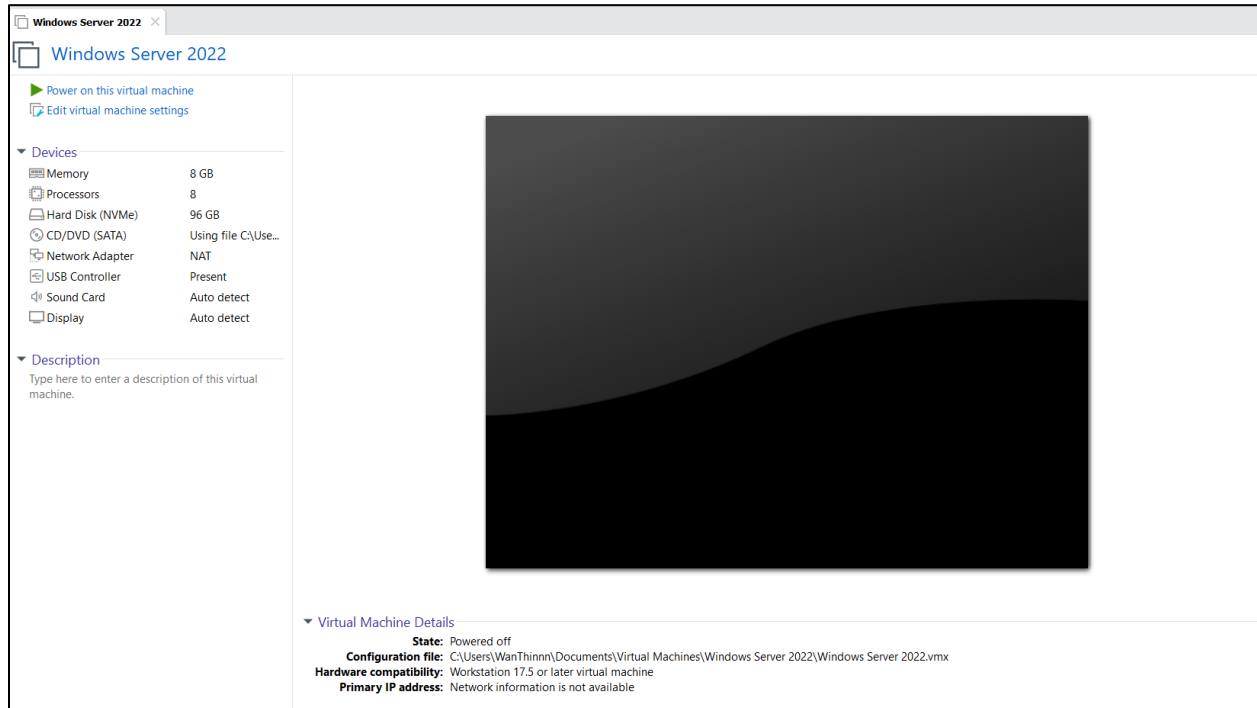


- Kết quả sau khi config xong:



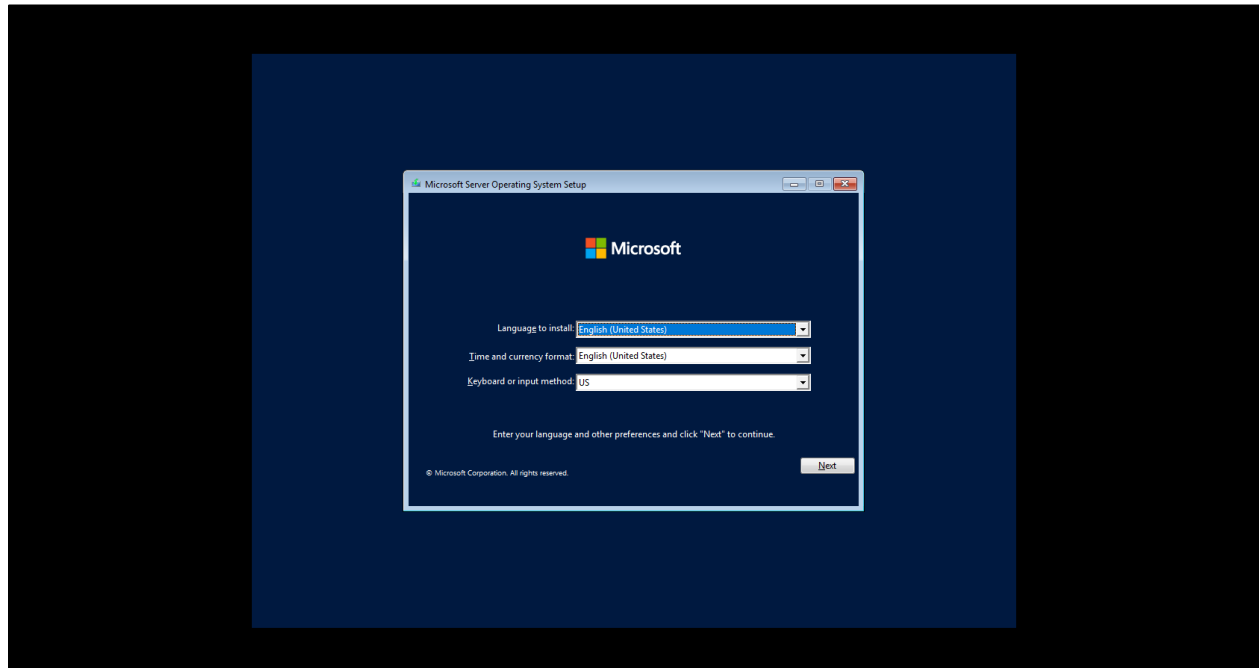
## II. Cài đặt máy ảo Windows Server 2022:

- Khởi động máy ảo, ta sẽ thấy màn hình GUI như bên dưới hiện lên,:

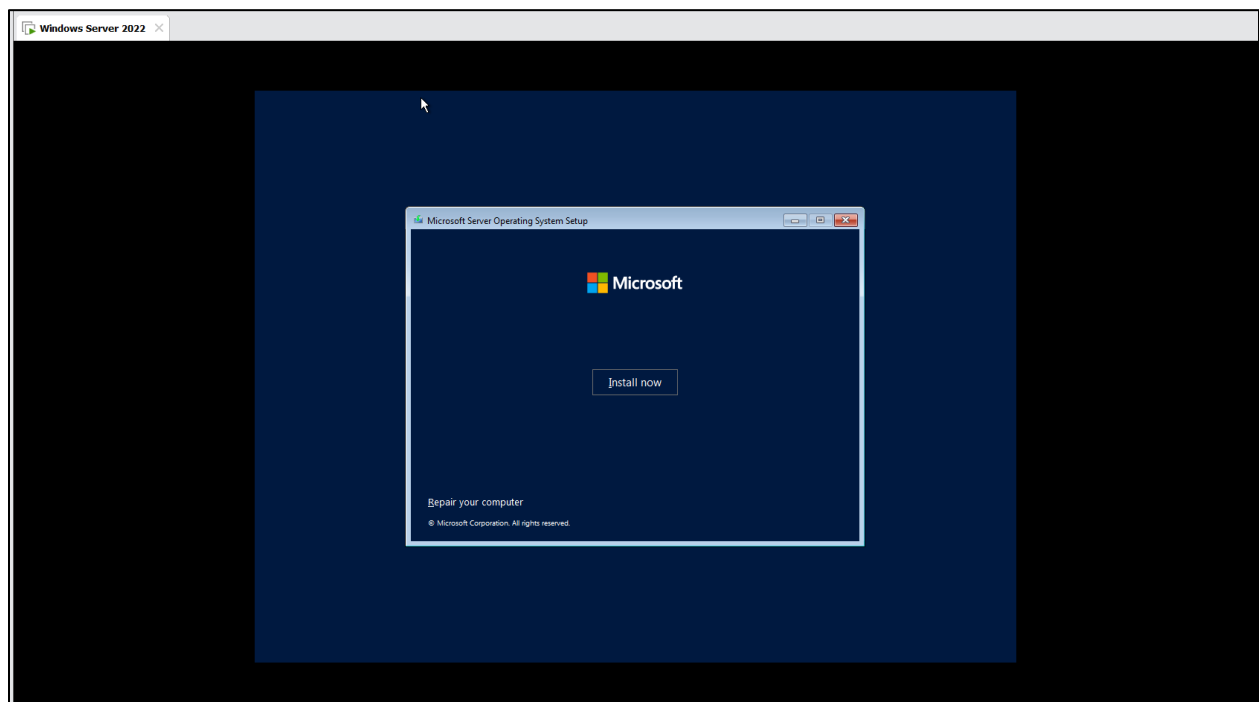




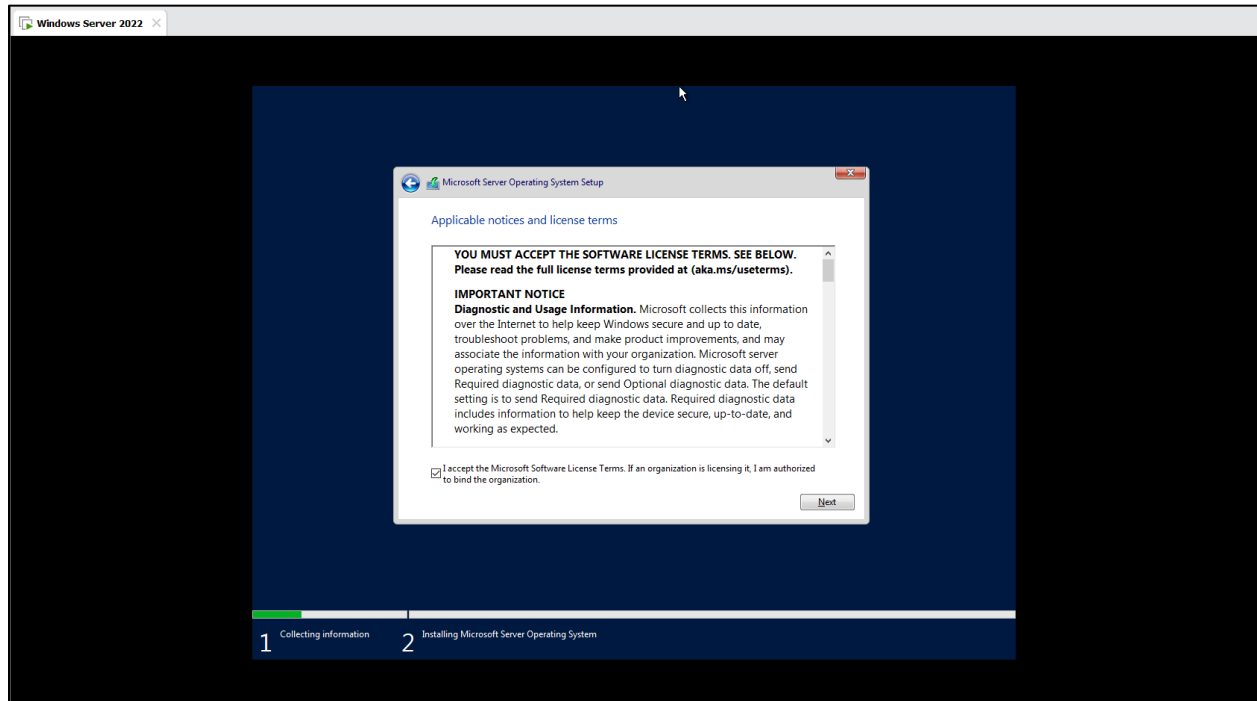
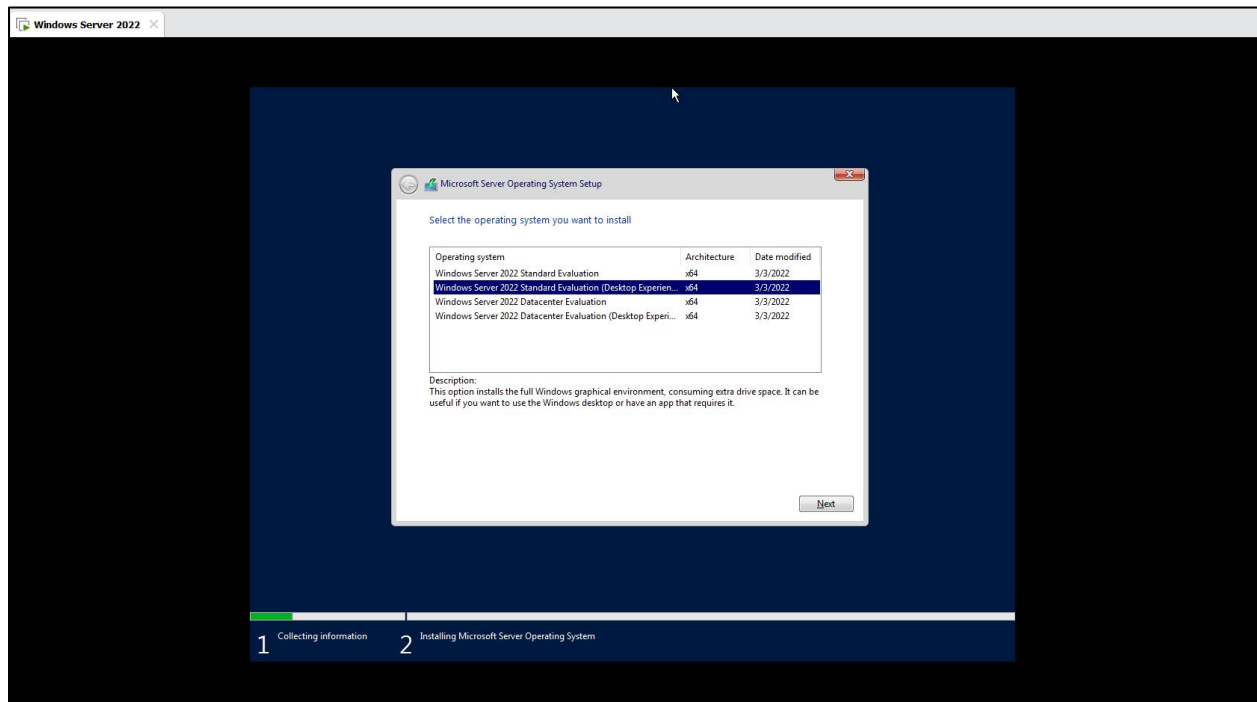
- Chọn ngôn ngữ là Tiếng Anh:



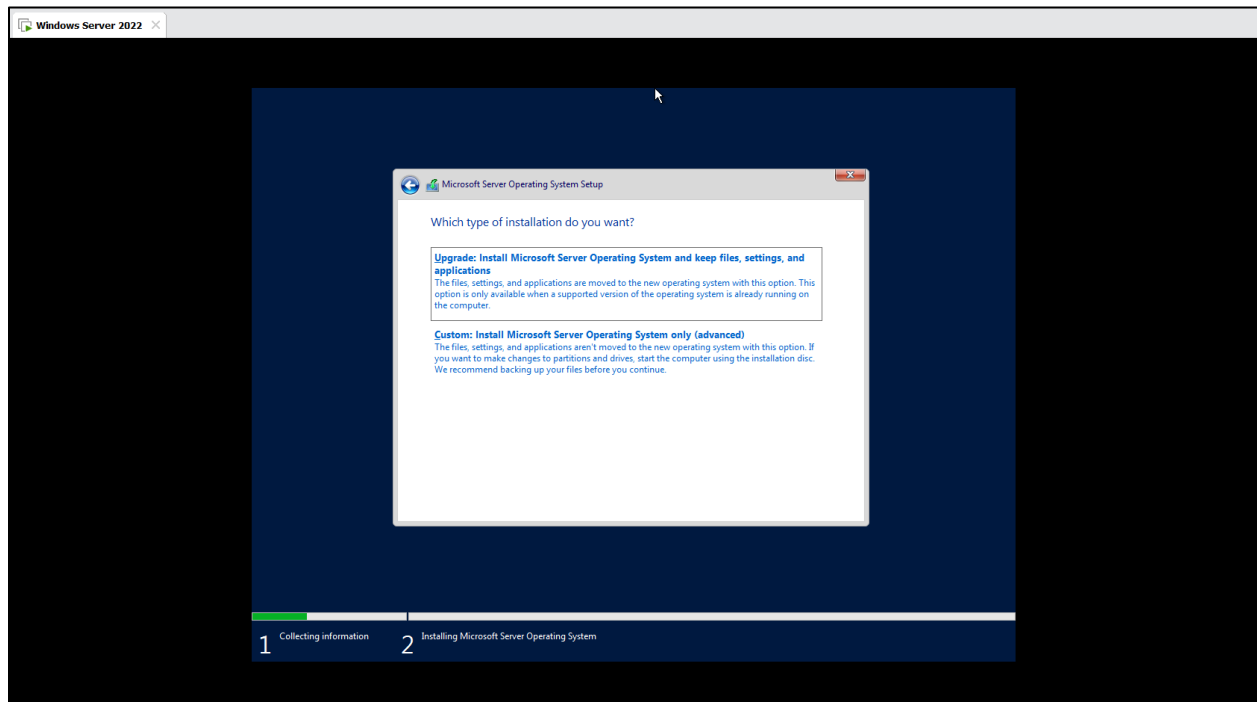
- Tiến hành cài đặt Windows Server 2022:



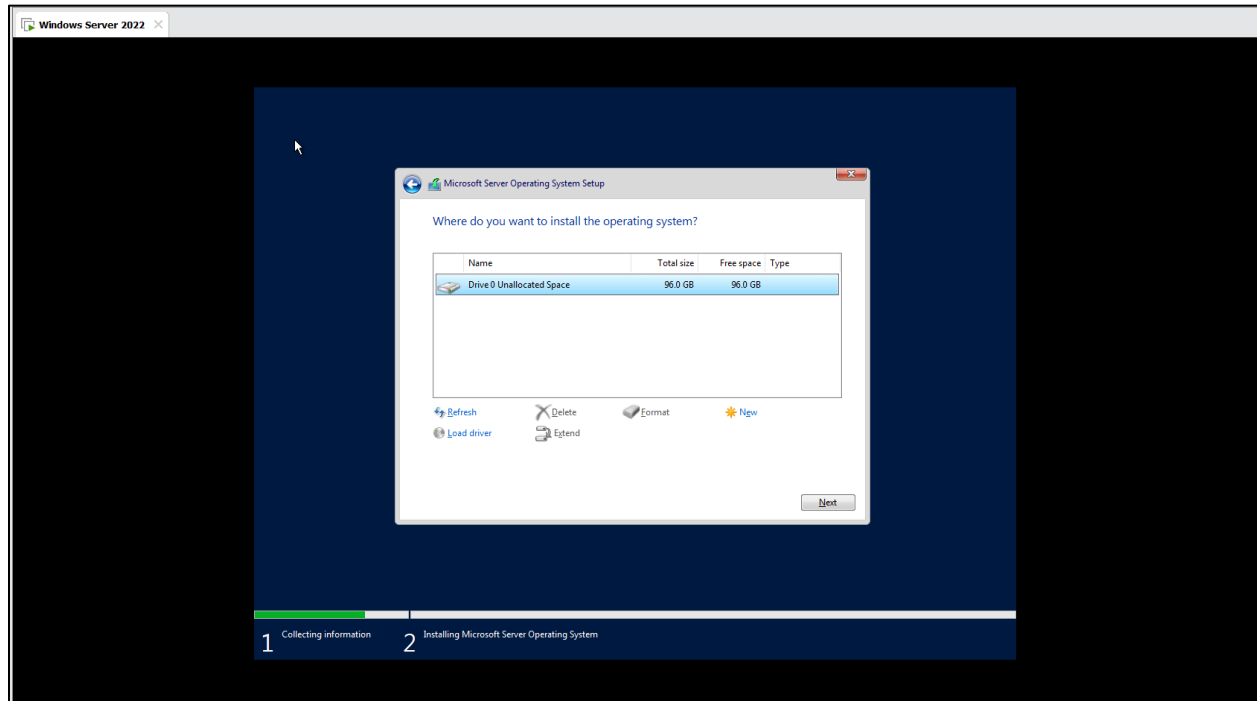
- Chọn phiên bản Windows Server GUI:



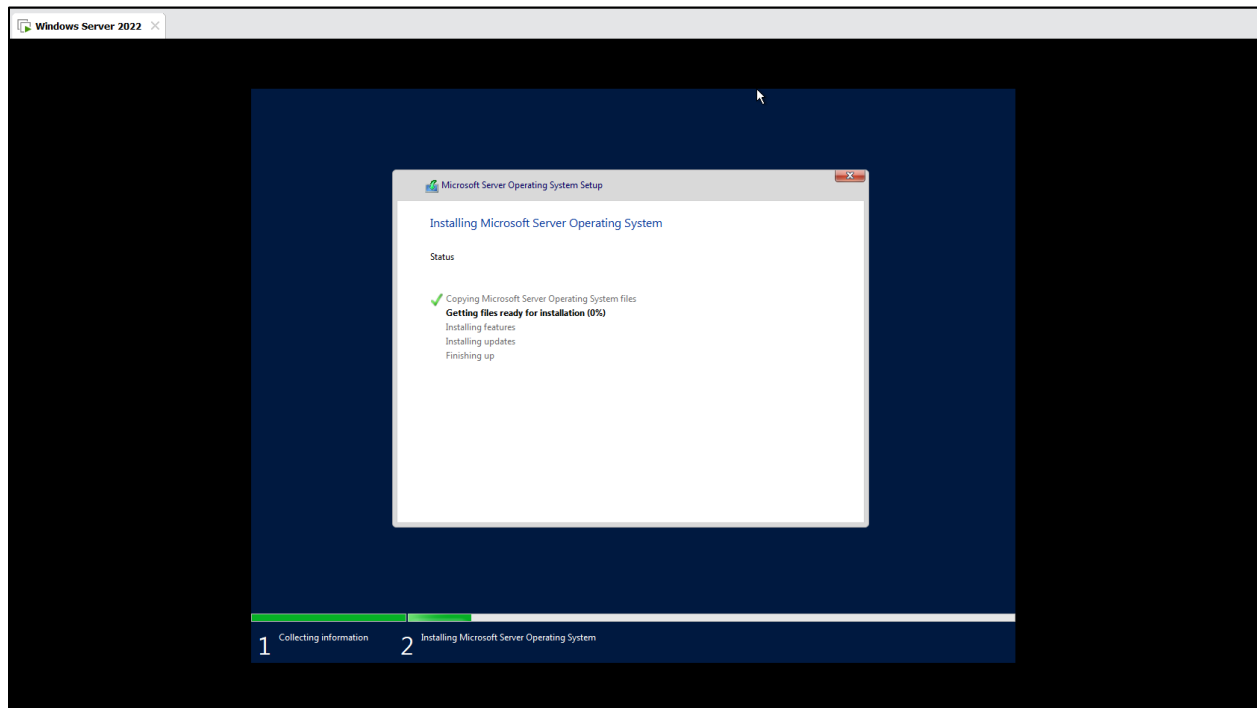
- Chọn “Custom”:



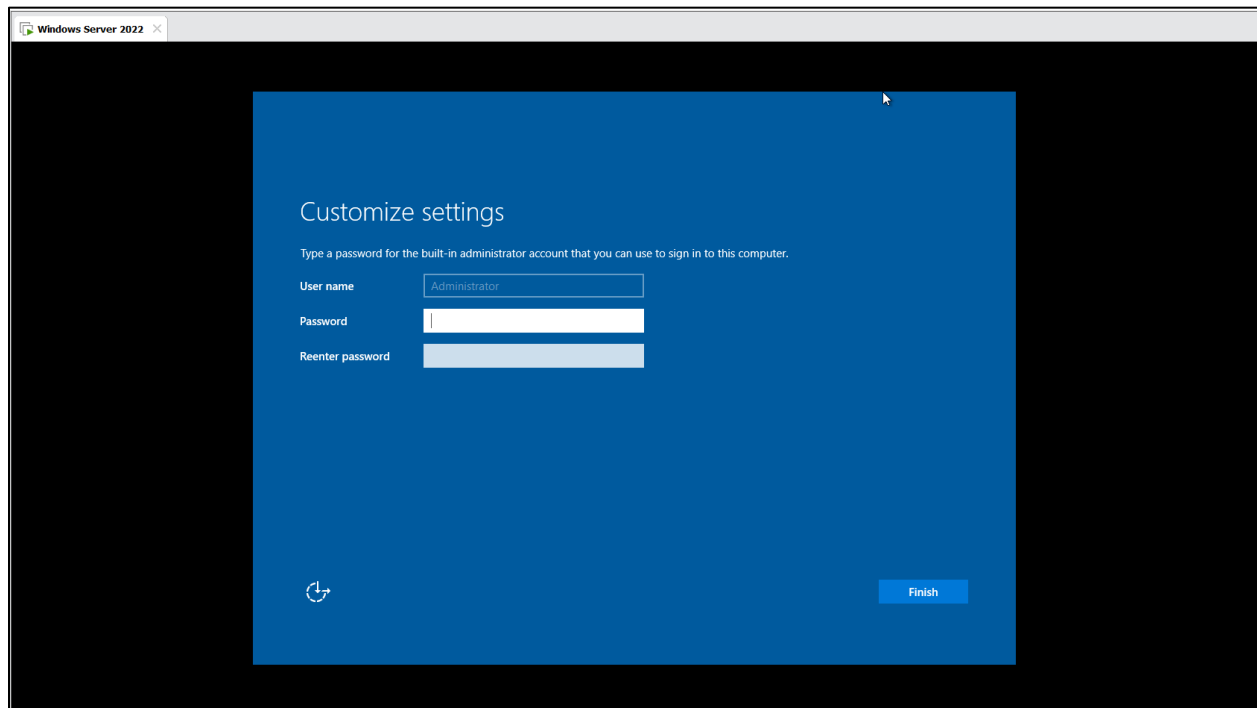
- Chọn ổ đĩa ảo để cài đặt Windows Server 2022 lên:



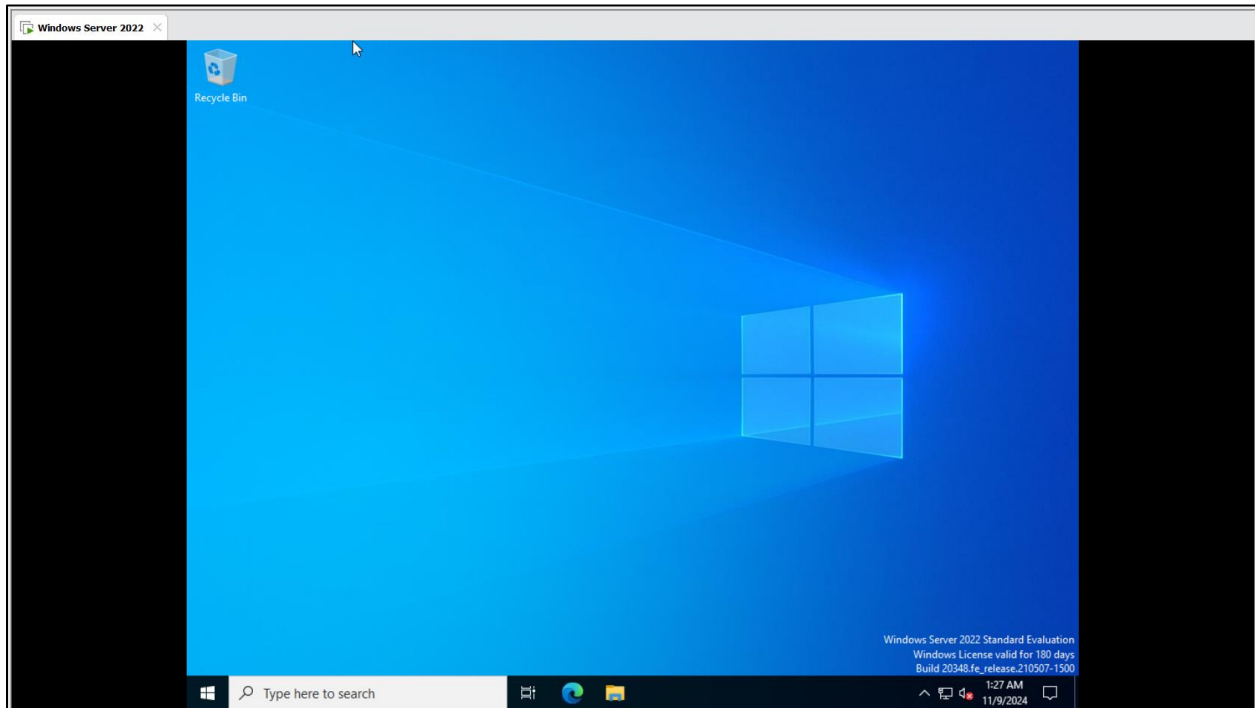
- Quá trình cài đặt bắt đầu:



- Sau khi cài đặt xong, ta tiến hành đặt Username và Password cho máy ảo:



- Cài đặt thành công:



### III. Thực hiện các cấu hình sau trên Windows Server 01:

#### 1. Bật/tắt tường lửa.

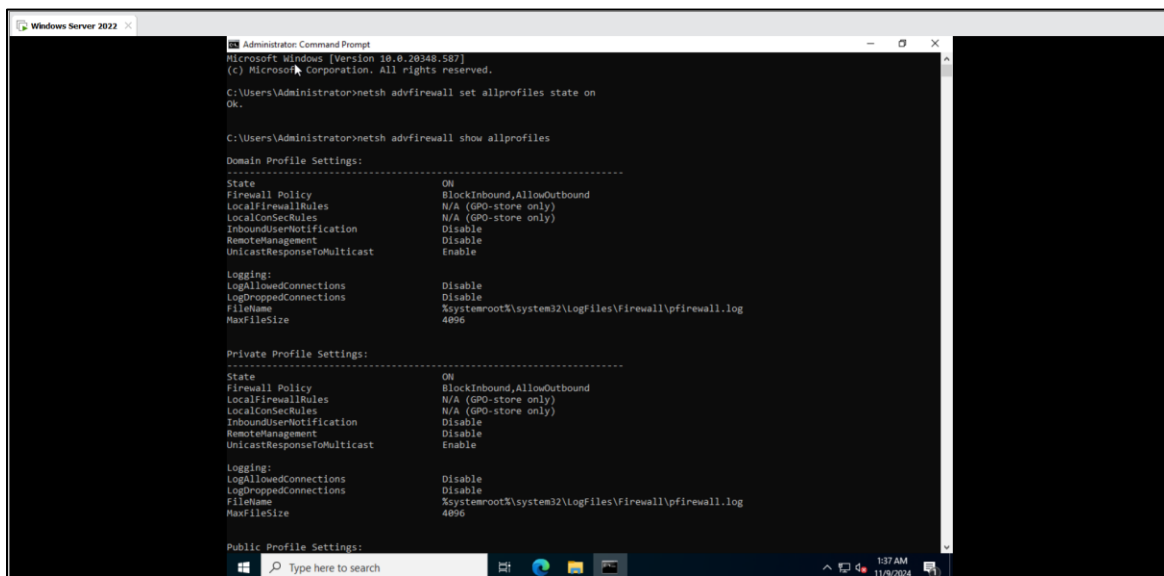
- Mở Command Prompt với quyền admin và sử dụng lệnh sau:

+ Để bật tường lửa: **netsh advfirewall set allprofiles state on**

+ Để tắt tường lửa: **netsh advfirewall set allprofiles state off**

+ Để kiểm tra trạng thái tường lửa: **netsh advfirewall show allprofiles**

- Bật tường lửa:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>netsh advfirewall set allprofiles state on
Ok.

C:\Users\Administrator>netsh advfirewall show allprofiles

Domain Profile Settings:
-----
State                ON
Firewall Policy       BlockInbound,AllowOutbound
LocalFirewallRules    N/A (GPO-store only)
LocalConSecRules      N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement     Disable
UnicastResponseToMulticast Enable

Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

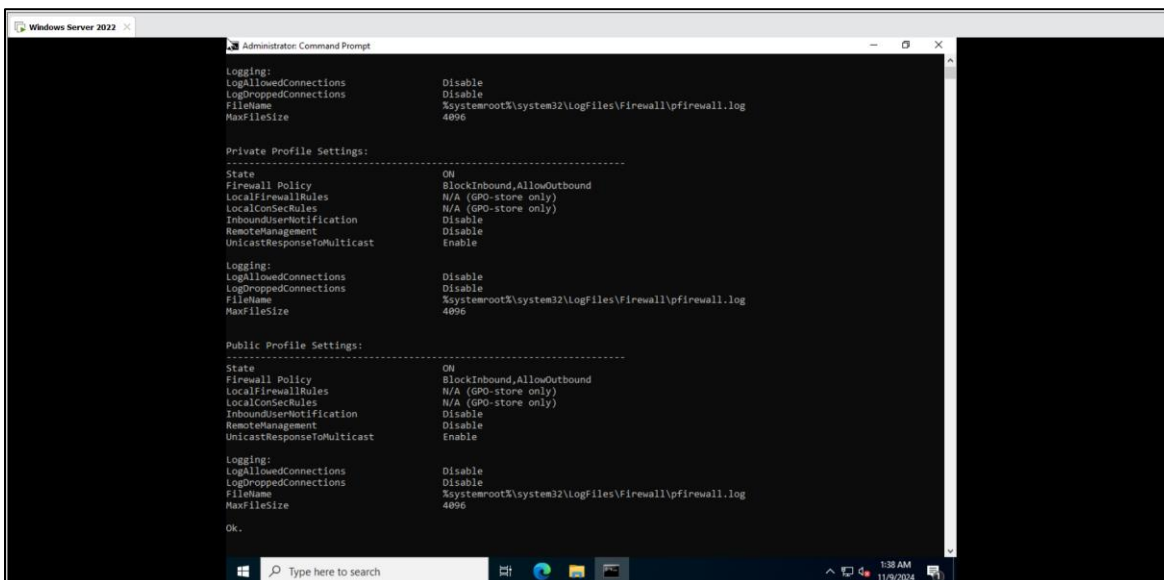
Private Profile Settings:
-----
State                ON
Firewall Policy       BlockInbound,AllowOutbound
LocalFirewallRules    N/A (GPO-store only)
LocalConSecRules      N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement     Disable
UnicastResponseToMulticast Enable

Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

Public Profile Settings:
-----
State                ON
Firewall Policy       BlockInbound,AllowOutbound
LocalFirewallRules    N/A (GPO-store only)
LocalConSecRules      N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement     Disable
UnicastResponseToMulticast Enable

Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

Ok.
```



```
Administrator: Command Prompt

Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

Private Profile Settings:
-----
State                ON
Firewall Policy       BlockInbound,AllowOutbound
LocalFirewallRules    N/A (GPO-store only)
LocalConSecRules      N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement     Disable
UnicastResponseToMulticast Enable

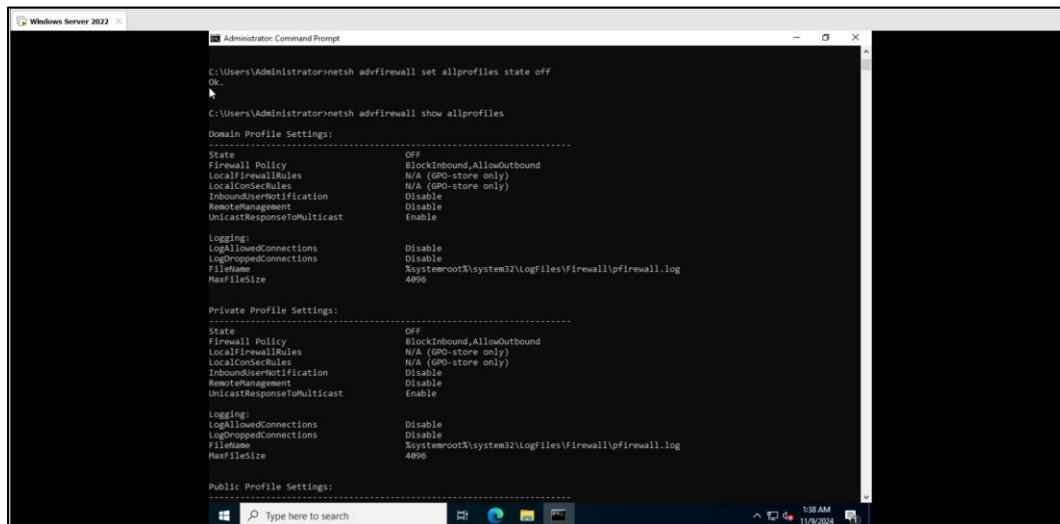
Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

Public Profile Settings:
-----
State                ON
Firewall Policy       BlockInbound,AllowOutbound
LocalFirewallRules    N/A (GPO-store only)
LocalConSecRules      N/A (GPO-store only)
InboundUserNotification Disable
RemoteManagement     Disable
UnicastResponseToMulticast Enable

Logging:
LogAllowedConnections Disable
LogDroppedConnections Disable
FileName              %systemroot%\system32\LogFiles\Firewall\pfirewall.log
MaxFileSize           4096

Ok.
```

- Tắt tường lửa:



The screenshot shows a Windows Server 2022 Administrator Command Prompt window. The user has entered the command `netsh advfirewall set allprofiles state off`, which has been executed successfully, returning `Ok.`. The user then enters `netsh advfirewall show allprofiles`, which displays the following settings:

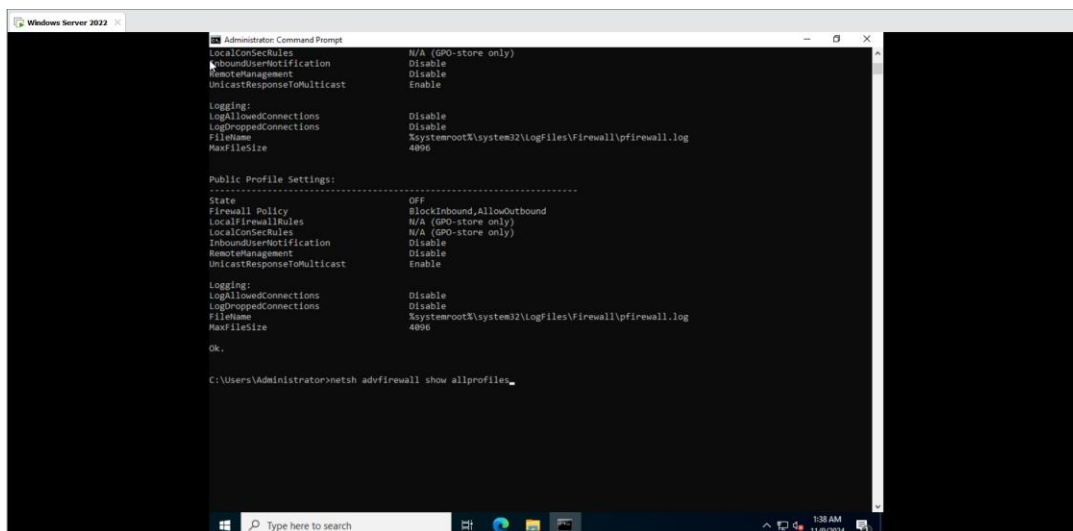
```
Domain Profile Settings:
-----
State: OFF
Firewall Policy: BlockInbound,AllowOutbound
LocalFirewallRules: N/A (GPO-store only)
LocalConSecRules: N/A (GPO-store only)
InboundUserNotification: Disable
RemoteManagement: Disable
UnicastResponseToMulticast: Enable

Logging:
LogAllowedConnections: Disable
LogDroppedConnections: Disable
LogDroppedConnections: %systemroot%\system32\Logfiles\Firewall\pfirewall.log
FileShare:
MaxFileSize: 4096

Private Profile Settings:
-----
State: OFF
Firewall Policy: BlockInbound,AllowOutbound
LocalFirewallRules: N/A (GPO-store only)
LocalConSecRules: N/A (GPO-store only)
InboundUserNotification: Disable
RemoteManagement: Disable
UnicastResponseToMulticast: Enable

Logging:
LogAllowedConnections: Disable
LogDroppedConnections: Disable
LogDroppedConnections: %systemroot%\system32\Logfiles\Firewall\pfirewall.log
FileShare:
MaxFileSize: 4096

Public Profile Settings:
-----
```



This screenshot is a continuation of the previous one, showing the end of the `netsh advfirewall show allprofiles` output. The settings for the Public Profile are shown, followed by `Ok.` and the user entering the command `netsh advfirewall show allprofiles` again.

```
Public Profile Settings:
-----
State: OFF
Firewall Policy: BlockInbound,AllowOutbound
LocalFirewallRules: N/A (GPO-store only)
LocalConSecRules: N/A (GPO-store only)
InboundUserNotification: Disable
RemoteManagement: Disable
UnicastResponseToMulticast: Enable

Logging:
LogAllowedConnections: Disable
LogDroppedConnections: Disable
LogDroppedConnections: %systemroot%\system32\Logfiles\Firewall\pfirewall.log
FileShare:
MaxFileSize: 4096

Ok.

C:\Users\Administrator>netsh advfirewall show allprofiles
```

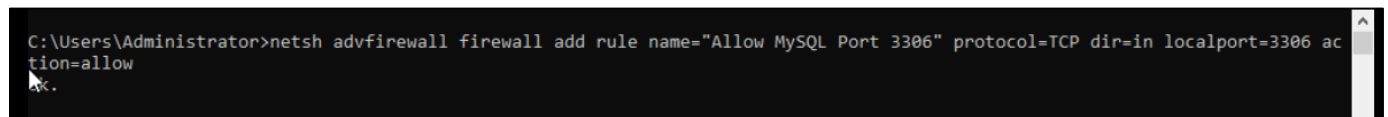
## **2. Thêm 1 rule mới trên tường lửa để cho phép người dùng từ bên ngoài truy cập và cổng 3306.**

- Để thêm một rule mới cho phép truy cập vào cổng 3306 trên tường lửa của Windows Server thông qua CMD, ta mở CMD với quyền Admin và chạy lệnh:

**netsh advfirewall firewall add rule name="Allow MySQL Port 3306" protocol=TCP dir=in localport=3306 action=allow**

- Giải thích:

- + name="Allow MySQL Port 3306": Đặt tên cho rule là "Allow MySQL Port 3306".
- + protocol=TCP: Chỉ định giao thức TCP.
- + dir=in: Áp dụng rule cho các kết nối đến (inbound).
- + localport=3306: Chỉ định cổng là 3306 (cổng mặc định của MySQL).
- + action=allow: Cho phép truy cập vào cổng này.



```
C:\Users\Administrator>netsh advfirewall firewall add rule name="Allow MySQL Port 3306" protocol=TCP dir=in localport=3306 action=allow
OK.
```

- Để kiểm tra xem rule cho cổng 3306 đã được thêm vào tường lửa thành công chưa, ta sử dụng lệnh sau:

**netsh advfirewall firewall show rule name="Allow MySQL Port 3306"**

- Lệnh này sẽ hiển thị thông tin chi tiết của rule "Allow MySQL Port 3306" nếu rule đã được thêm thành công. Bạn có thể kiểm tra các mục như:

- + Action: Xác nhận là "Allow".
- + LocalPort: Đảm bảo là 3306.
- + Protocol: Kiểm tra giao thức là TCP.

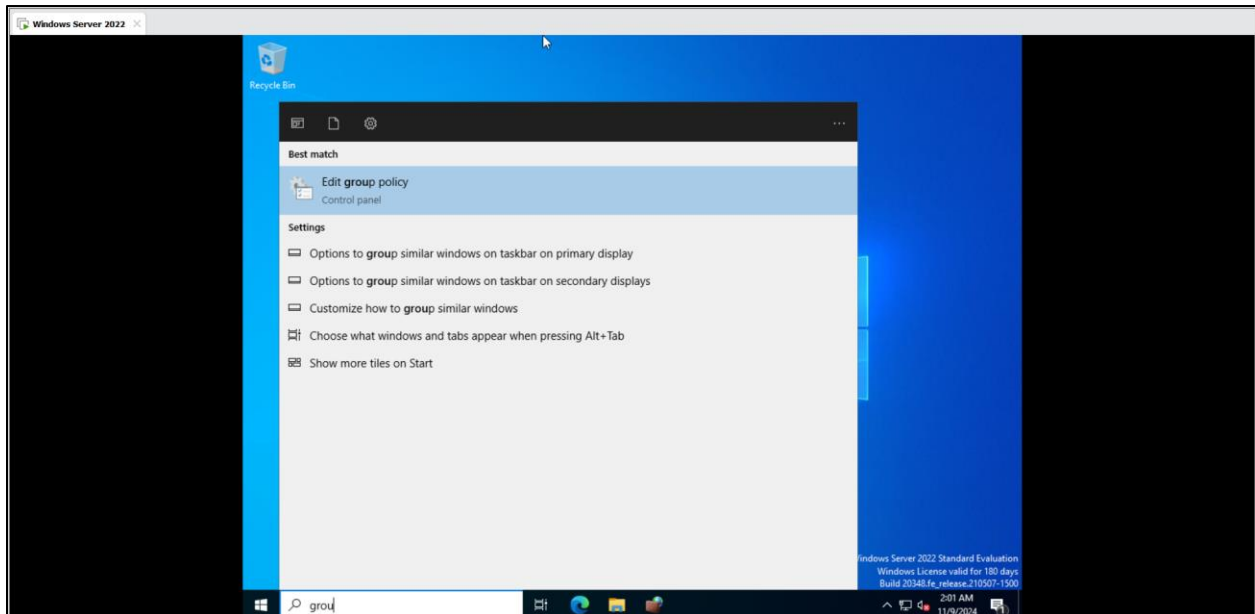


```
C:\Users\Administrator>netsh advfirewall firewall show rule name="Allow MySQL Port 3306"

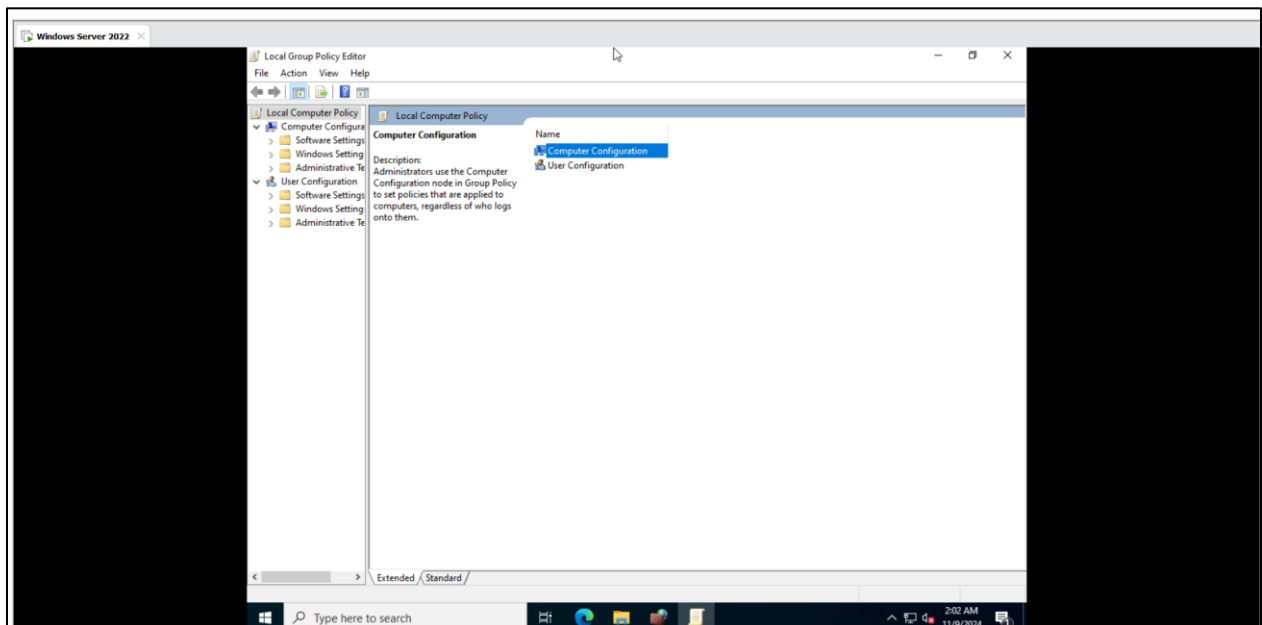
Rule Name: Allow MySQL Port 3306
-----
Enabled: Yes
Direction: In
Profiles: Domain,Private,Public
Grouping:
LocalIP: Any
RemoteIP: Any
Protocol: TCP
LocalPort: 3306
RemotePort: Any
Edge traversal: No
Action: Allow
Ok.
```

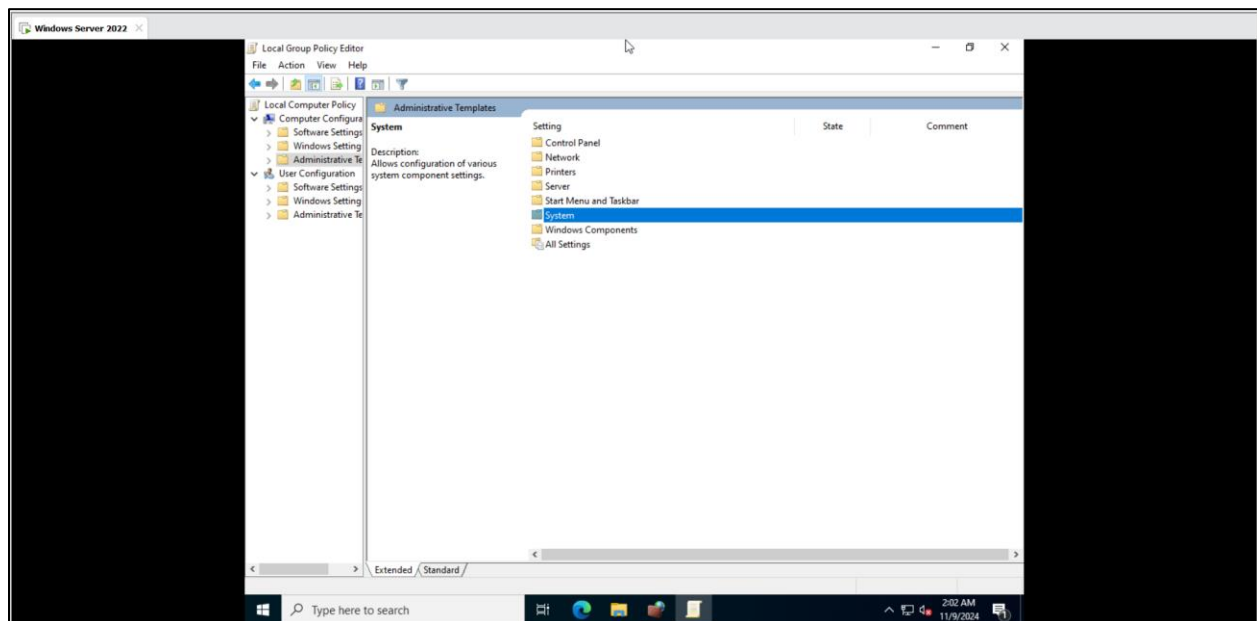
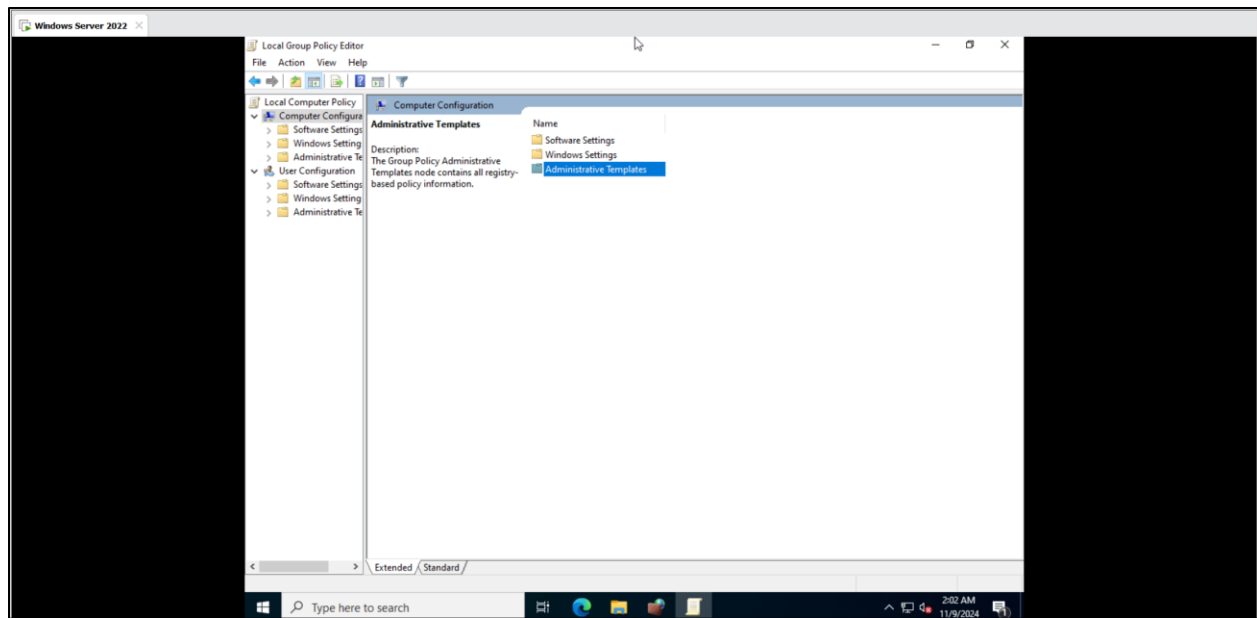
### 3. Cấu hình Group Policy để chặn sử dụng USB

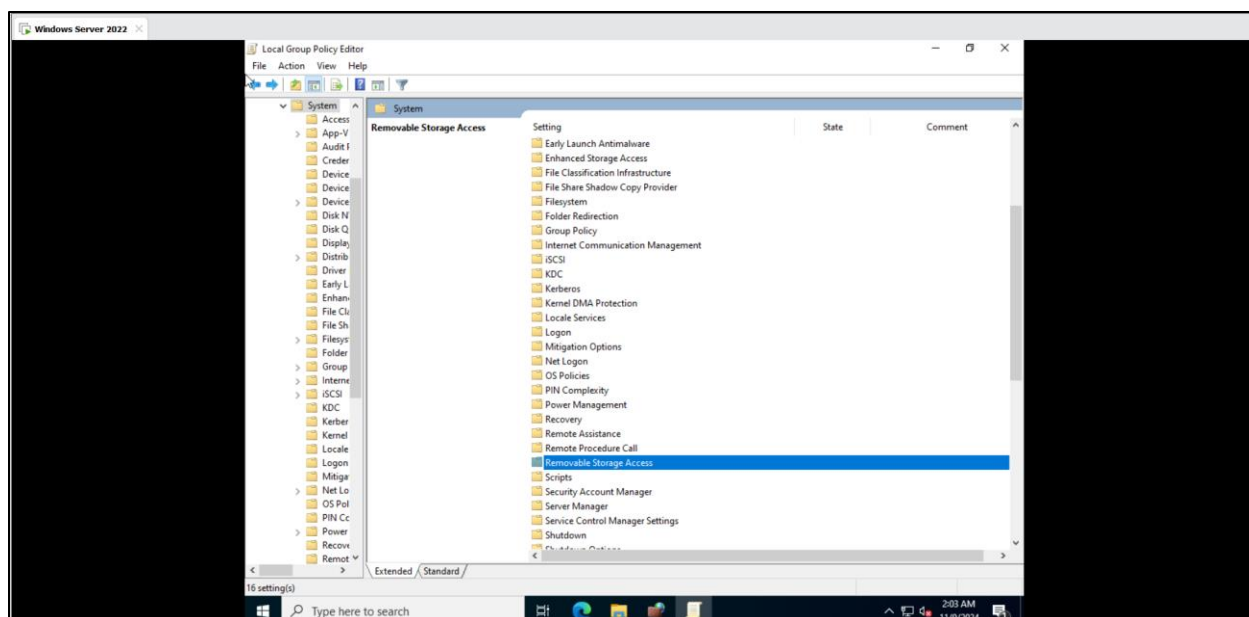
- Mở Edit Group Policy:



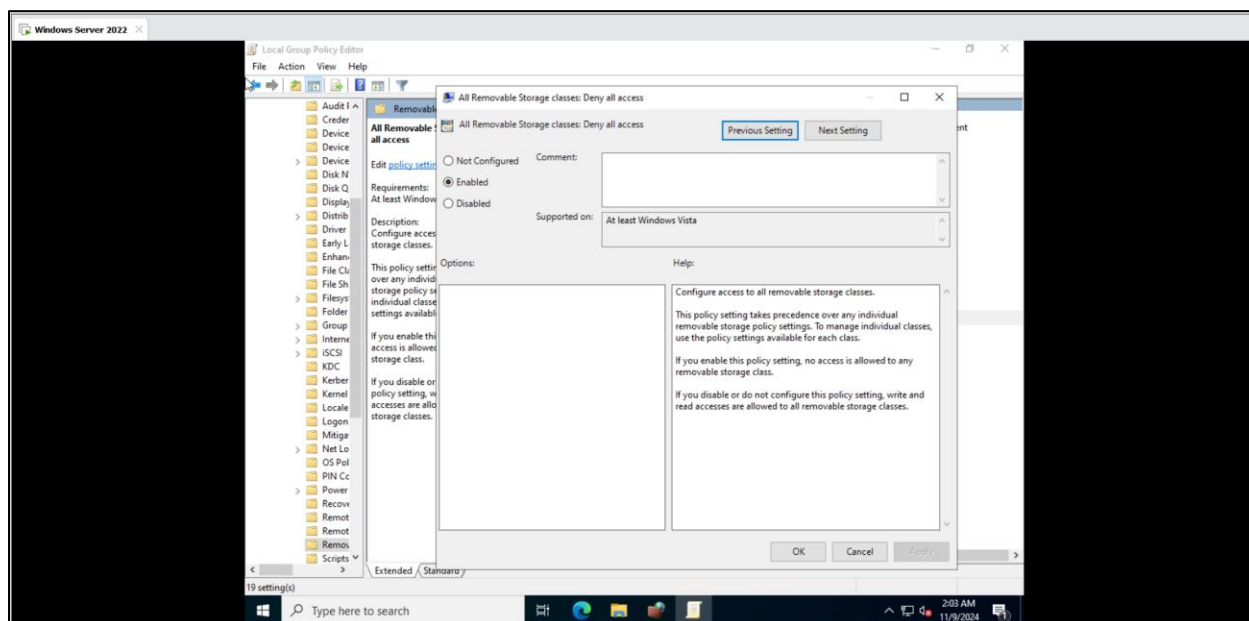
- Điều hướng đến: Computer Configuration > Administrative Templates > System > Removable Storage Access.



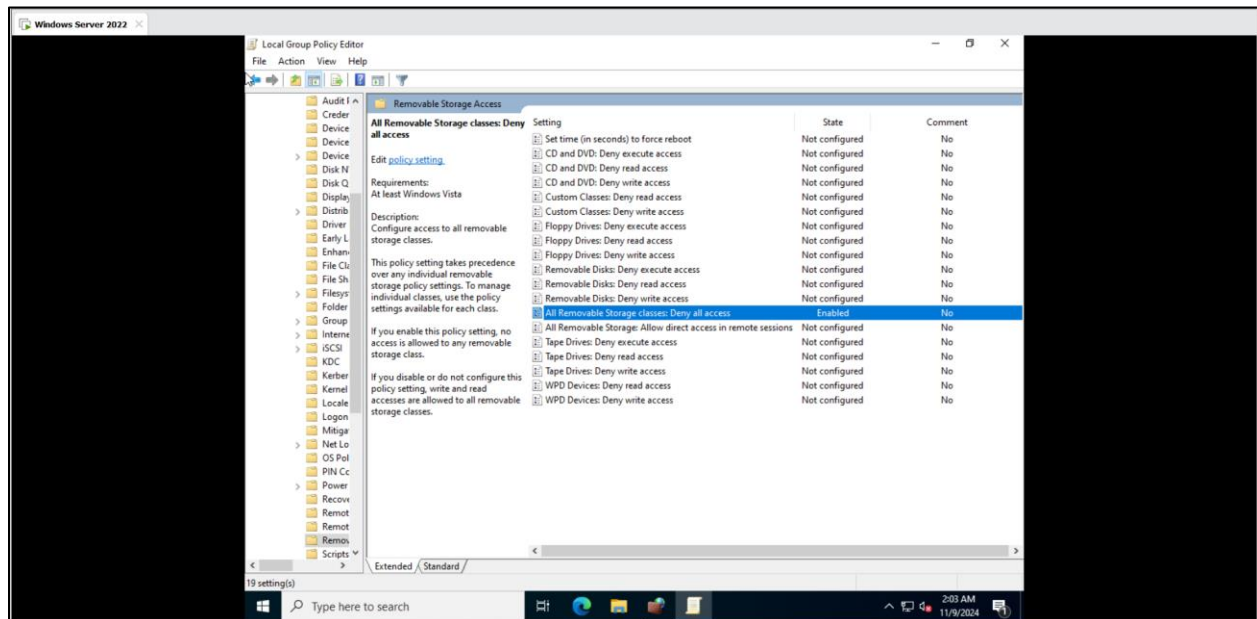




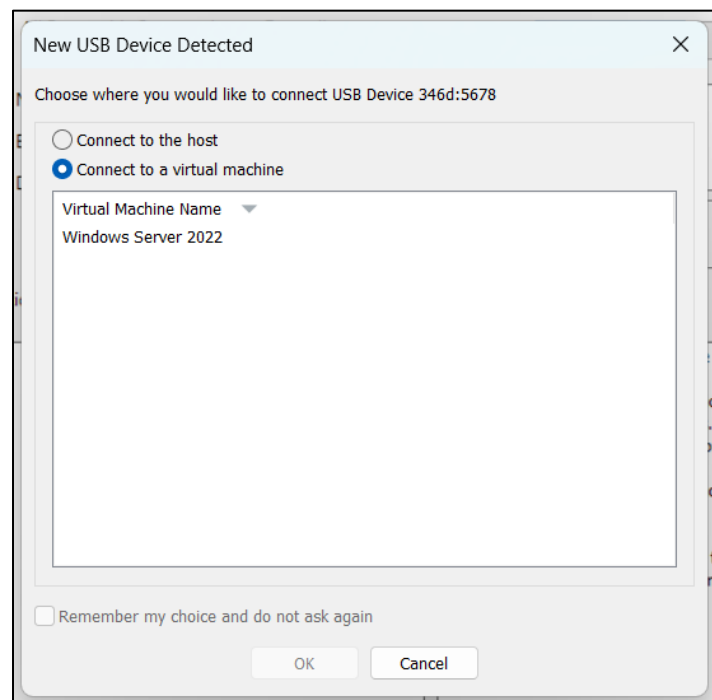
- Tại đây ta chọn “Enabled”:



- Kết quả:



- Kiểm tra bằng việc kết nối USB vào:



- Có thể thấy USB bị chặn sử dụng:

