

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



**BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 1.3
CÀI ĐẶT LINUX SERVER VÀ CÁC DỊCH VỤ**

Sinh viên thực hiện:

B22DCAT251 Đặng Đức Tài

Giảng viên hướng dẫn: TS. Phạm Hoàng Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

MỤC LỤC.....	2
DANH MỤC CÁC HÌNH VẼ.....	3
CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH	4
1.1 Mục đích.....	4
1.2 Tìm hiểu lý thuyết	4
1.2.1 Hệ điều hành Ubuntu Server	4
1.2.2 Tìm hiểu dịch vụ chia sẻ file	7
CHƯƠNG 2. NỘI DUNG THỰC HÀNH	10
2.1 Chuẩn bị môi trường	10
2.2 Các bước thực hiện.....	12
2.2.1 Cài đặt Ubuntu Server	12
2.2.2 Cài đặt dịch vụ OpenSSH.....	16
2.2.3 Cài đặt và cấu hình dịch vụ Samba	19
2.2.4 Cài đặt và cấu hình dịch vụ SELinux	24
TÀI LIỆU THAM KHẢO	26

DANH MỤC CÁC HÌNH VẼ

Hình 1 Mô phỏng hệ điều hành Ubuntu	4
Hình 2 Giao diện dòng lệnh của hệ điều hành Ubuntu Server	6
Hình 3 Giao diện của hệ điều hành Ubuntu Desktop	7
Hình 4 Nguyên lý hoạt động của Samba	8
Hình 5 Nguyên lý hoạt động của Selinux	10
Hình 6 Chuẩn bị máy ảo Ubuntu Server	11
Hình 7 Máy ảo Windows 10 22H2.....	11
Hình 8 Chuẩn bị phần mềm VMWare Workstation Pro 17	12
Hình 9 Cài đặt đường dẫn	12
Hình 10 Kiểm tra & Kết thúc cài đặt	13
Hình 11 Tắt chế độ đồ họa	14
Hình 12 Cấu hình mạng cho máy ảo	14
Hình 13 Tùy chỉnh ổ đĩa cho máy ảo	15
Hình 14 Cấu hình file system cho máy ảo	15
Hình 15 Thiết lập tài khoản người dùng	16
Hình 16 Giao diện hệ điều hành Ubuntu Server	16
Hình 17 Cài đặt dịch vụ OpenSSH.....	17
Hình 18 Cài đặt PuTTY	17
Hình 19 Ping kết nối giữa máy trạm với server	18
Hình 20 Kết nối tới Ubuntu Server bằng PuTTY	18
Hình 21 Kết nối thành công tới Ubuntu Server.....	19
Hình 22 Cài đặt dịch vụ Samba.....	19
Hình 23 Tạo tài khoản User	20
Hình 24 Tạo tài khoản admin	20
Hình 25 Cấu hình file smb.conf	21
Hình 26 Khởi động lại dịch vụ	21
Hình 27 Xử lý ngoại lệ chia sẻ file.....	22
Hình 28 Truy cập vào thư mục chia sẻ.....	22
Hình 29 Truy cập vào thư mục user	22
Hình 30 Ngắt kết nối tới máy chủ Samba	23
Hình 31 Truy cập vào thư mục admin.....	24
Hình 32 Cài đặt SELinux trên Ubuntu Server.....	24
Hình 33 Kích hoạt SELinux	24
Hình 34 Cài đặt thành công SELinux.....	25
Hình 35 Cấu hình SELinux cho dịch vụ FTP.....	25

CHƯƠNG 1. GIỚI THIỆU CHUNG VỀ BÀI THỰC HÀNH

1.1 Mục đích

- Rèn luyện kỹ năng cài đặt và quản trị HĐH máy chủ Linux Server với các dịch vụ cơ bản

1.2 Tìm hiểu lý thuyết

1.2.1 Hệ điều hành Ubuntu Server

1.2.1.1 Ubuntu Server là gì?

- Ubuntu Server là một hệ điều hành dựa trên Ubuntu, được thiết kế chuyên biệt để vận hành trên các máy chủ. Máy chủ thường có hai dạng chính: dạng rackmount và dạng tower. Máy chủ dạng tower về cơ bản có hình dáng giống một máy tính để bàn thông thường, nhưng các linh kiện bên trong lại được thiết kế khác biệt, tập trung vào độ bền, sự ổn định và tính bảo mật cao. Chẳng hạn, máy chủ dạng tower thường sử dụng RAM sửa lỗi (ECC), trong khi hầu hết máy tính để bàn thông thường không được trang bị loại RAM này. Ngoài ra, một điểm khác biệt quan trọng là máy chủ không nhất thiết phải đi kèm các thiết bị ngoại vi như màn hình, bàn phím hay chuột. Khi vận hành máy chủ mà không sử dụng các thiết bị này, người ta gọi đó là thiết lập "không đầu". Phần mềm dành cho máy chủ bao gồm hệ điều hành, phần mềm máy chủ (chẳng hạn như Apache để lưu trữ trang web hoặc CUPS để quản lý in ấn) và các công cụ bảo mật cần thiết.



Hình 1 Mô phỏng hệ điều hành Ubuntu

1.2.1.2 Đặc điểm nổi bật của Ubuntu Server

- Ubuntu Server là một trong những hệ điều hành máy chủ phổ biến nhất hiện nay, được biết đến với sự ổn định, bảo mật và khả năng mở rộng cao. Được phát triển bởi

Canonical, Ubuntu Server cung cấp một môi trường mạnh mẽ và linh hoạt cho các doanh nghiệp, tổ chức cũng như cá nhân có nhu cầu triển khai hệ thống máy chủ.

- Một trong những đặc điểm nổi bật của Ubuntu Server là tính miễn phí và mã nguồn mở. Điều này cho phép người dùng tùy chỉnh, sửa đổi hệ điều hành theo nhu cầu riêng mà không bị ràng buộc bởi các chi phí bản quyền. Bên cạnh đó, Ubuntu Server cũng có một cộng đồng lớn mạnh, luôn sẵn sàng hỗ trợ và chia sẻ kinh nghiệm, giúp việc khắc phục sự cố trở nên dễ dàng hơn.
- Về hiệu suất, Ubuntu Server được tối ưu hóa để hoạt động mượt mà trên cả các hệ thống phần cứng cũ lẫn các máy chủ hiện đại. Hệ điều hành này hỗ trợ nhiều kiến trúc phần cứng, bao gồm x86, ARM và POWER, giúp mở rộng phạm vi ứng dụng từ máy chủ truyền thống đến các nền tảng điện toán đám mây và IoT.
- Bảo mật là một yếu tố quan trọng khác khiến Ubuntu Server trở thành lựa chọn hàng đầu. Hệ điều hành này được cập nhật thường xuyên với các bản vá bảo mật, đi kèm với cơ chế bảo vệ nâng cao như AppArmor và hỗ trợ mã hóa mạnh mẽ. Ngoài ra, Ubuntu Server cũng tích hợp tốt với các công cụ quản lý hệ thống như Landscape, giúp quản trị viên dễ dàng giám sát và bảo trì máy chủ từ xa.
- Một ưu điểm đáng chú ý nữa của Ubuntu Server là sự hỗ trợ mạnh mẽ cho các công nghệ đám mây. Hệ điều hành này tương thích tốt với các nền tảng như OpenStack, Kubernetes và Docker, giúp triển khai và quản lý các ứng dụng container nhanh chóng, hiệu quả. Không chỉ vậy, Ubuntu Server còn được các nhà cung cấp dịch vụ đám mây lớn như AWS, Google Cloud và Microsoft Azure tin dùng.
- Tổng kết lại, Ubuntu Server là một lựa chọn lý tưởng cho các hệ thống máy chủ nhờ vào sự kết hợp giữa tính ổn định, bảo mật, hiệu suất cao và khả năng mở rộng.

```
Ubuntu 20.04 LTS tecmint-appserver1 tty1

tecmint-appserver1 login: tecmint
Password:
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-26-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of Fri 24 Apr 2020 10:48:23 AM UTC

System load:  0.0               Processes:            106
Usage of /:   5.9% of 74.96GB   Users logged in:     0
Memory usage: 20%              IPv4 address for enp0s3: 10.42.0.218
Swap usage:   0%

0 updates can be installed immediately.
0 of these updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

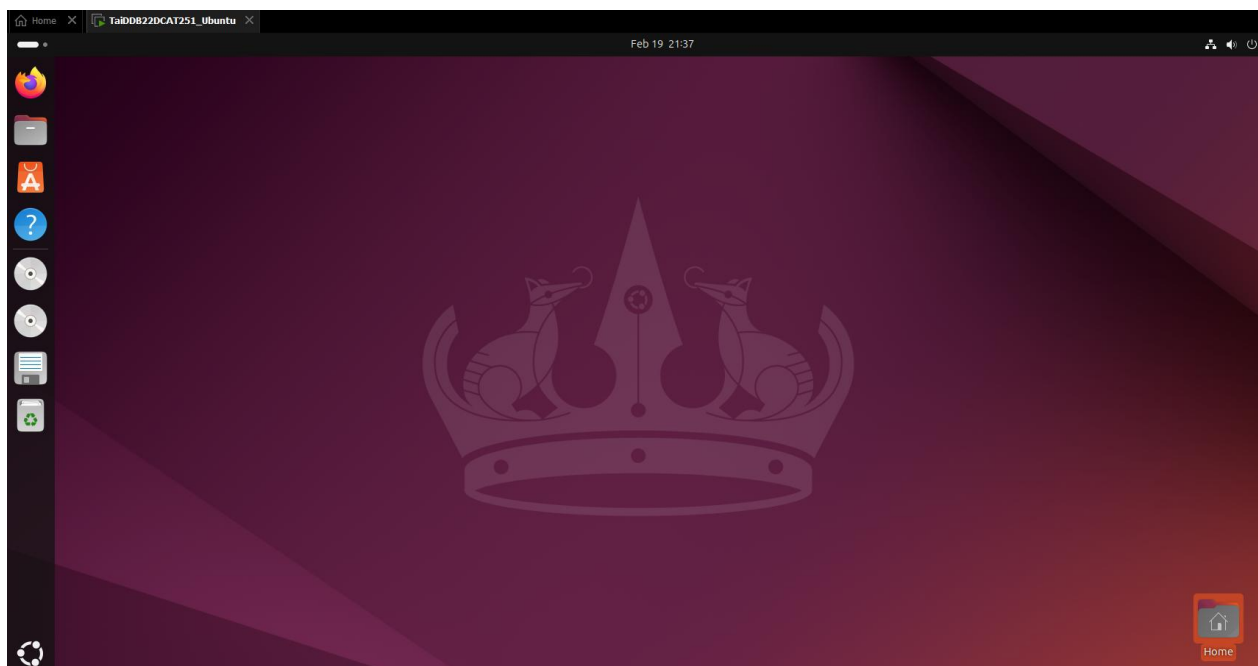
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

tecmint@tecmint-appserver1:~$ _
```

Hình 2 Giao diện dòng lệnh của hệ điều hành Ubuntu Server

1.2.1.3 So sánh Ubuntu Server với Ubuntu Desktop (máy trạm)

- Ubuntu Server và Ubuntu Desktop đều là các phiên bản của hệ điều hành Ubuntu, nhưng chúng được thiết kế để phục vụ những mục đích khác nhau. Ubuntu Server hướng đến việc vận hành các hệ thống máy chủ, trong khi Ubuntu Desktop phù hợp cho người dùng cá nhân và doanh nghiệp với giao diện đồ họa trực quan.
- Một trong những điểm khác biệt quan trọng giữa hai phiên bản này là giao diện người dùng. Ubuntu Server không đi kèm môi trường đồ họa mặc định, thay vào đó, nó hoạt động chủ yếu thông qua giao diện dòng lệnh (CLI – Command Line Interface). Điều này giúp tối ưu hóa tài nguyên và đảm bảo hiệu suất cao khi vận hành các dịch vụ nền. Ngược lại, Ubuntu Desktop được tích hợp giao diện đồ họa GNOME hoặc các biến thể khác như KDE, XFCE, giúp người dùng dễ dàng thao tác và làm việc mà không cần sử dụng dòng lệnh.
- Về ứng dụng mặc định, Ubuntu Server được trang bị sẵn các công cụ hỗ trợ vận hành máy chủ như OpenSSH, Apache, MySQL, Docker và OpenStack, giúp triển khai các dịch vụ web, cơ sở dữ liệu và nền tảng đám mây một cách hiệu quả. Trong khi đó, Ubuntu Desktop đi kèm với nhiều ứng dụng phục vụ công việc văn phòng và giải trí như trình duyệt web, bộ ứng dụng LibreOffice, trình phát nhạc và các phần mềm chỉnh sửa hình ảnh.
- Ubuntu Server cũng có lợi thế về hiệu suất do không cần chạy các thành phần đồ họa, từ đó giảm mức tiêu thụ tài nguyên hệ thống và đảm bảo sự ổn định trong thời gian dài. Điều này đặc biệt quan trọng đối với các hệ thống máy chủ, nơi mà khả năng hoạt động liên tục là yếu tố then chốt. Ngược lại, Ubuntu Desktop yêu cầu nhiều tài nguyên hơn để hỗ trợ giao diện đồ họa và các ứng dụng nền, điều này có thể ảnh hưởng đến hiệu suất khi sử dụng trên phần cứng giới hạn.
- Về mặt bảo mật, Ubuntu Server được thiết kế với các cơ chế bảo vệ nâng cao như AppArmor, tường lửa UFW và các bản cập nhật bảo mật thường xuyên. Nó cũng hỗ trợ quản lý từ xa thông qua SSH, giúp quản trị viên có thể điều khiển hệ thống mà không cần truy cập trực tiếp. Trong khi đó, Ubuntu Desktop dù vẫn có các tính năng bảo mật mạnh mẽ, nhưng do sử dụng giao diện đồ họa và nhiều ứng dụng nền, hệ thống có thể dễ bị tấn công hơn so với một máy chủ chuyên dụng.
- Ubuntu Server còn được tối ưu cho các môi trường điện toán đám mây và ảo hóa, cho phép triển khai trên quy mô lớn với các công nghệ như Docker, Kubernetes hay OpenStack. Ngược lại, Ubuntu Desktop chủ yếu được thiết kế để chạy trên các máy tính cá nhân hoặc doanh nghiệp nhỏ, không phù hợp cho việc triển khai trên cụm máy chủ lớn.
- Tổng kết lại, Ubuntu Server là lựa chọn lý tưởng cho các hệ thống máy chủ, nơi yêu cầu sự ổn định, bảo mật và hiệu suất cao. Trong khi đó, Ubuntu Desktop phù hợp hơn với các nhu cầu làm việc hàng ngày, cung cấp giao diện thân thiện và nhiều công cụ hỗ trợ cho người dùng cá nhân và doanh nghiệp nhỏ. Việc lựa chọn phiên bản phù hợp phụ thuộc vào mục đích sử dụng và yêu cầu cụ thể của hệ thống.



Hình 3 Giao diện của hệ điều hành Ubuntu Desktop

1.2.2 Tìm hiểu dịch vụ chia sẻ file

1.2.2.1 Samba

A. Samba Server là gì?

- Samba Server là một máy chủ tập tin, hay còn được gọi là File Server, được sử dụng trong mạng nội bộ.
- Đây là nơi tập trung lưu trữ thông tin của tổ chức hoặc doanh nghiệp cụ thể và có thể được triển khai trên cả hệ điều hành Windows và Linux. Ngoài ra, Samba Server chủ yếu hoạt động dựa trên giao thức SMB, được công bố lần đầu vào năm 1984 trong một tài liệu kỹ thuật của IBM, với mục đích ban đầu là thiết kế một giao thức mạng để đặt tên và duyệt.

B. Lịch sử hình thành và phát triển của Samba Server

- Samba Server bắt nguồn từ nhu cầu kết nối các hệ thống máy tính chạy hệ điều hành Unix/Linux với mạng Windows. Dự án Samba Server bắt đầu vào những năm đầu của thập kỷ 1990, khi Andrew Tridgell, một nhà phát triển phần mềm người Úc, tìm cách giải quyết vấn đề này.
- Trong quá trình nghiên cứu, Tridgell đã phân tích giao thức SMB (Server Message Block), một giao thức mạng mà hệ điều hành Windows sử dụng để chia sẻ tệp qua mạng. Dựa trên việc hiểu về SMB, ông đã phát triển Samba Server, một phần mềm mã nguồn mở cho phép hệ thống Unix/Linux tham gia vào mạng Windows và chia sẻ tệp.
- Samba Server đã trải qua nhiều phiên bản và cải tiến qua các năm. Sự phát triển của nó không chỉ dừng lại ở việc hỗ trợ các phiên bản mới của giao thức SMB/CIFS mà còn mở rộng chức năng và tính năng để đáp ứng nhu cầu ngày càng phức tạp của các môi trường mạng hiện đại.

- Trong suốt quá trình phát triển, cộng đồng người dùng và các nhà phát triển đã đóng góp vào Samba Server, làm cho nó trở thành một trong những giải pháp chia sẻ tệp phổ biến nhất và mạnh mẽ nhất trong các môi trường mạng hỗn hợp giữa Unix/Linux và Windows.

C. Cách thức hoạt động của Samba Server

- Giao thức SMB của Samba Server được phát triển từ giao thức CIFS (Common Internet File System). Giao thức này được triển khai trên mạng Internet và phụ thuộc vào giao thức TCP/IP. Nó cung cấp cho người dùng các quyền khác nhau khi tạo tập tin, bao gồm quyền Đọc và Ghi (Read-Write), Chỉ Đọc (Read Only), cũng như khả năng đặt mật khẩu và khóa tập tin. Ngoài ra, SMB còn hỗ trợ các tính năng sau:
 - Hỗ trợ Unicode.
 - Xử lý các thuộc tính mở rộng của file.
 - Thông báo về sự thay đổi trong file và thư mục.
 - Xác thực truy cập vào file và thư mục được chia sẻ.
 - Phát hiện các Server sử dụng SMB trên mạng (browse network).
 - Đàm phán và điều chỉnh để đảm bảo tương thích giữa các phiên bản của SMB.



Hình 4 Nguyên lý hoạt động của Samba

D. Các tính năng nổi bật của Samba Server

- Các tính năng nổi bật của Samba Server bao gồm:

- Chia sẻ File và Thư mục: Samba Server cho phép chia sẻ file và thư mục từ máy chủ Linux sang các thiết bị và máy tính khác trong mạng, bao gồm cả các thiết bị chạy hệ điều hành Windows.
- Tương thích với Windows: Samba Server hỗ trợ giao thức SMB/CIFS, giúp máy chủ Linux hoạt động như một máy chủ file Windows, cho phép các máy tính Windows truy cập và sử dụng tài nguyên từ máy chủ Linux.
- Quản lý Tài nguyên: Samba Server cung cấp các công cụ quản lý để tạo, sửa đổi và xóa các tài nguyên được chia sẻ trên máy chủ, bao gồm cả quản lý quyền truy cập.
- Tính Bảo mật: Samba Server hỗ trợ các cơ chế bảo mật như xác thực người dùng, mã hóa dữ liệu qua mạng, kiểm soát truy cập dựa trên quyền hạn và tích hợp với các hệ thống quản lý tài khoản người dùng.
- Hỗ trợ các Giao thức Mạng: Samba Server hỗ trợ nhiều giao thức mạng bao gồm SMB/CIFS, FTP, và HTTP, giúp tối ưu hóa việc chia sẻ và truy cập tài nguyên trong mạng.
- Tích hợp với các Hệ thống Directory: Samba Server có thể tích hợp với các hệ thống quản lý người dùng và nhóm như LDAP, Active Directory, giúp quản lý người dùng và quyền truy cập hiệu quả hơn.
- Đa nền tảng: Samba Server không chỉ hỗ trợ các máy tính chạy Linux mà còn có thể tích hợp với các hệ điều hành khác như macOS, Unix và Windows, tạo ra một môi trường chia sẻ tài nguyên đa nền tảng.

→ Những tính năng này giúp Samba trở thành một giải pháp mạnh mẽ và linh hoạt cho việc chia sẻ tài nguyên trong mạng nội bộ hoặc mạng doanh nghiệp.

1.2.2.2 SELinux

A. SELinux Là Gì?

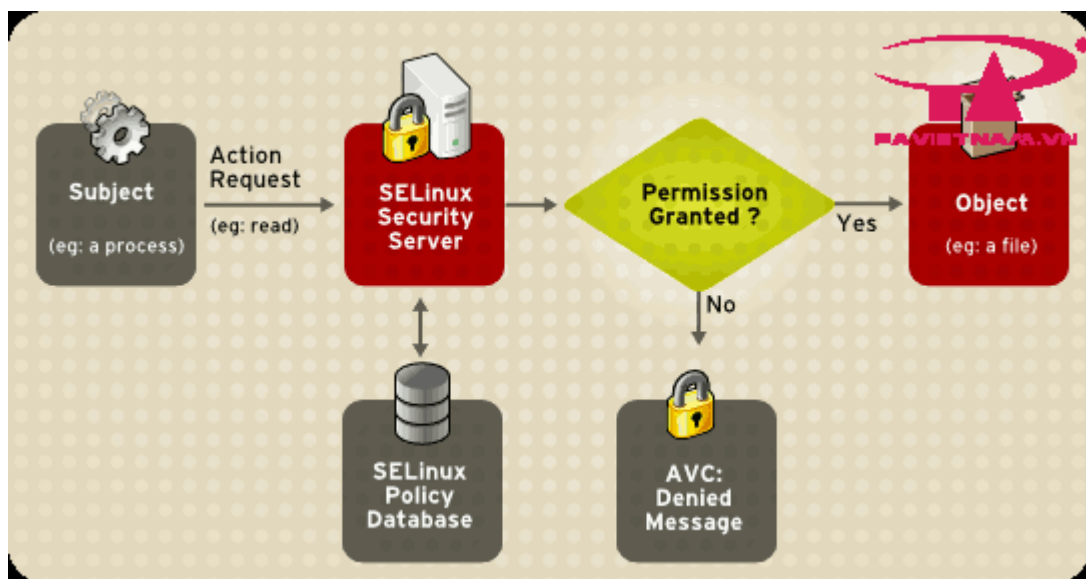
- SELinux được viết tắt từ cụm từ tiếng anh Security Enhanced Linux là một kiến trúc bảo mật nâng cao cho Linux Kernel của hệ điều hành Linux nhằm gia tăng khả năng bảo mật cho hệ thống. SELinux cho phép quản trị viên có quyền thực thi, kiểm soát các chính sách tài nguyên, xác định mức độ truy cập của người dùng, chương trình và dịch vụ trên hệ thống của hệ điều hành.

B. Các trạng thái của SELinux

- SELinux chạy ở 3 chế độ khác nhau bao gồm: Enforcing, Permissive và Disabled
- Enforcing: Đây là chế độ mặc định sẽ cho phép và thực thi các chính sách bảo mật của SELinux trên hệ thống, từ chối các hành động truy cập và ghi nhật ký. Trong chế độ Enforcing này, hệ thống sẽ thi hành các chính sách bảo mật một cách khắc khe, bắt buộc các ứng dụng và người dùng phải tuân thủ theo chính sách đó.
- Permissive: Ở chế độ này SELinux được kích hoạt nhưng sẽ không thực thi chính sách bảo mật, chỉ gửi các cảnh báo đến người dùng.
- Disabled: SELinux sẽ bị vô hiệu hóa các chính sách bảo mật, đây là chế độ không được khuyến khích nếu bạn không biết cách bảo mật hệ thống Linux của mình.

C. Cơ chế bảo mật của SELinux

- SELinux là một thực thi của cơ chế bảo mật MAC- Mandatory Access Controls tạm dịch là điều khiển truy cập bắt buộc. Nó được xây dựng trong Linux kernel và được kích hoạt mặc định trên Fedora, CentOS, RHEL và một vài bản phân phối Linux khác. Đây là cơ chế bảo mật nhiều mức (multiple level). Được dùng để bảo vệ một khối lượng dữ liệu lớn cần được bảo mật cao trong một môi trường mà các dữ liệu và người dùng đều có thể được phân loại rõ ràng.
- SELinux đặt các hạn chế đối với từng đối tượng theo từng chính sách cụ thể – khác với cơ chế bảo mật tùy quyền DAC-Discretionary Access Control – là một cơ chế bảo mật Unix/Linux truyền thống. Người dùng có thể bảo vệ những gì thuộc về mình; Chủ của dữ liệu sẽ có toàn quyền trên dữ liệu đó; Chủ của dữ liệu có quyền định nghĩa các loại truy cập đọc/ghi/thực thi (read/write/execute/...) và gán những quyền đó cho những người dùng khác.



Hình 5 Nguyên lý hoạt động của Selinux

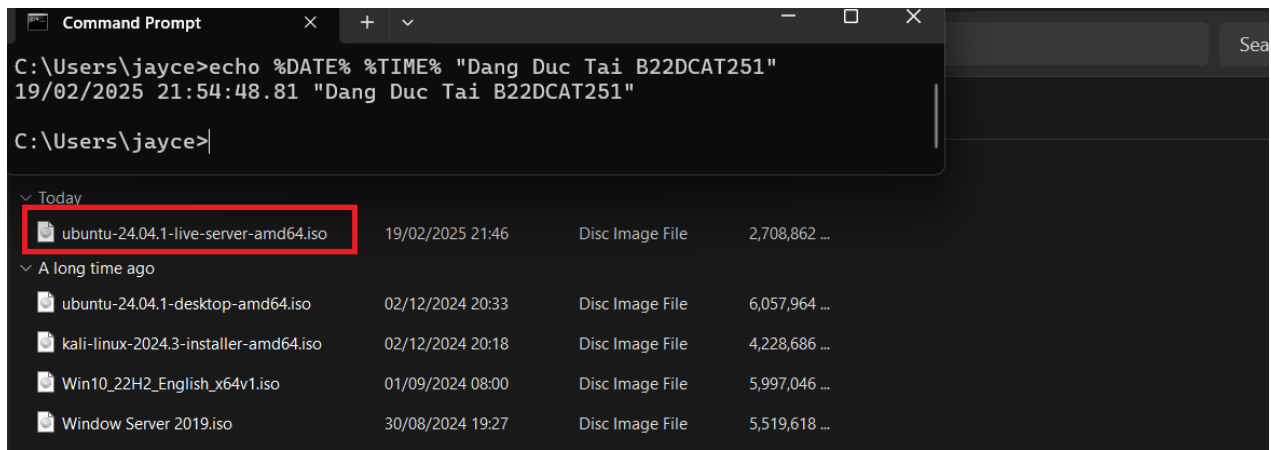
D. Ưu / Nhược điểm của SELinux

- Ưu điểm:
 - Là cơ chế điều khiển truy xuất có tính bảo mật cao trong việc ngăn chặn truy cập dữ liệu hoặc các chương trình trái phép.
 - Bảo vệ máy chủ chống lại việc khai thác. Tránh tình trạng leo thang đặc quyền.
- Nhược điểm:
 - Có những trường hợp SELinux lại gây ra sự phiền phức khi bạn muốn cài một phần mềm mà phần mềm đó lại cần can thiệp sâu vào hệ thống Linux. Do đó bạn cần phải vô hiệu hóa tính năng của SELinux

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

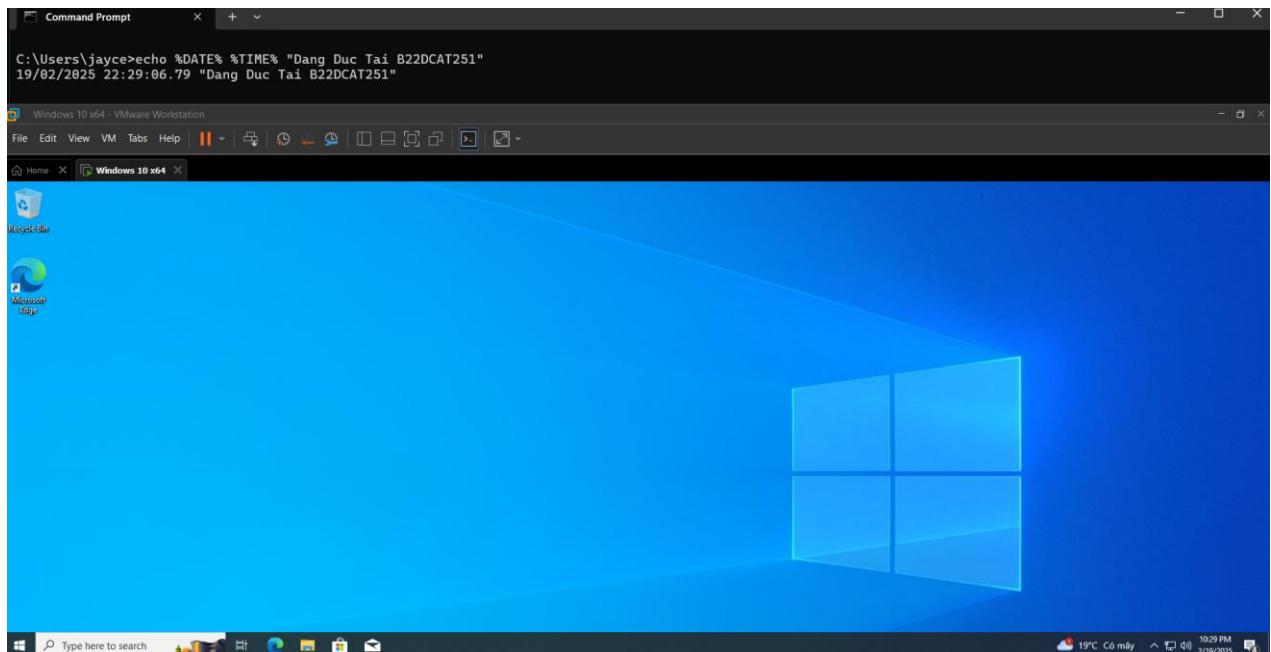
2.1 Chuẩn bị môi trường

- File cài đặt Ubuntu Server định dạng ISO.



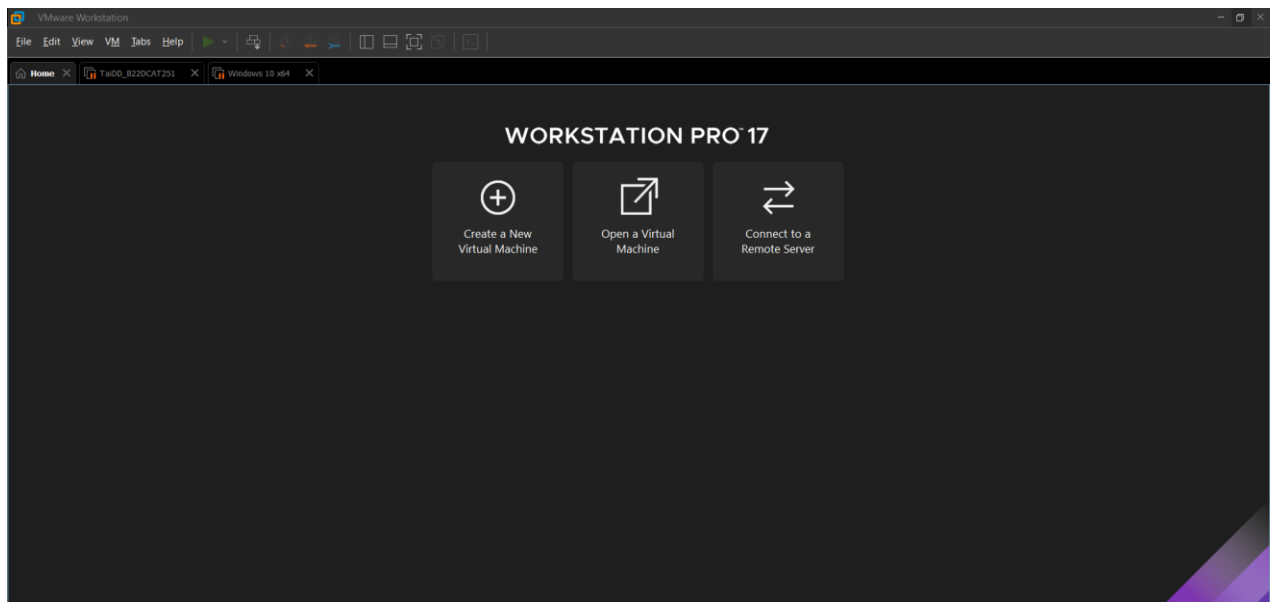
Hình 6 Chuẩn bị máy ảo Ubuntu Server

- Máy trạm Windows 7 (hoặc Windows 10/11). Trong bài này sử dụng máy trạm windows 10.



Hình 7 Máy ảo Windows 10 22H2

- Phần mềm máy ảo
- Trong bài thực hành này sử dụng phần mềm ảo hóa VMWare Workstation Pro 17.

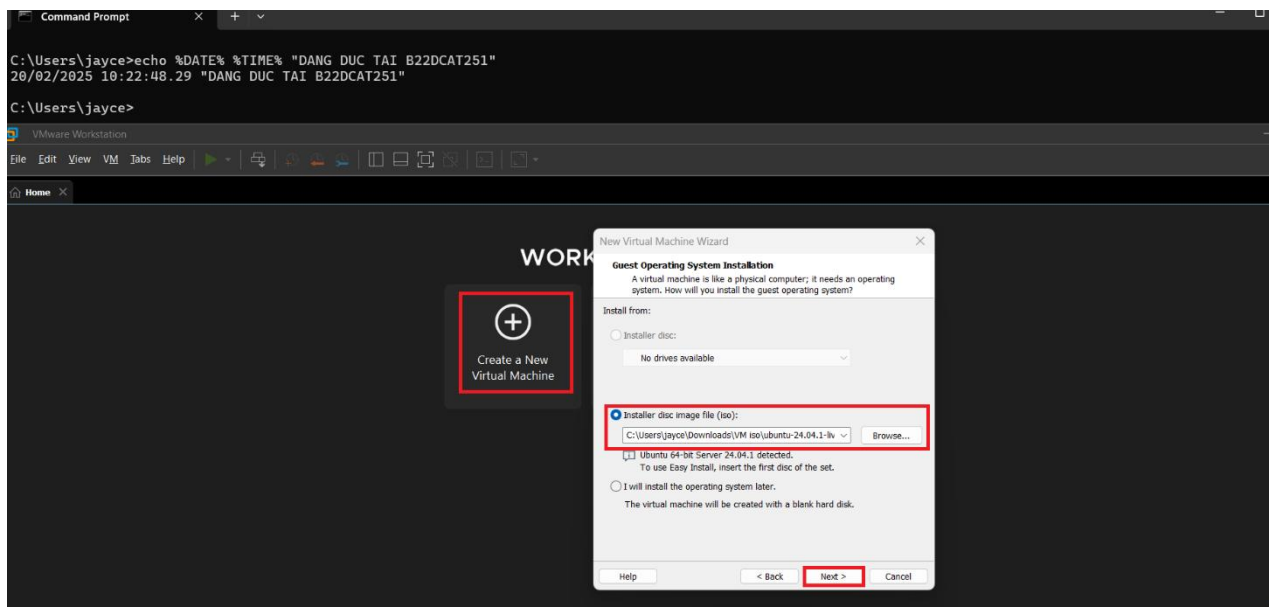


Hình 8 Chuẩn bị phần mềm VMWare Workstation Pro 17

2.2 Các bước thực hiện

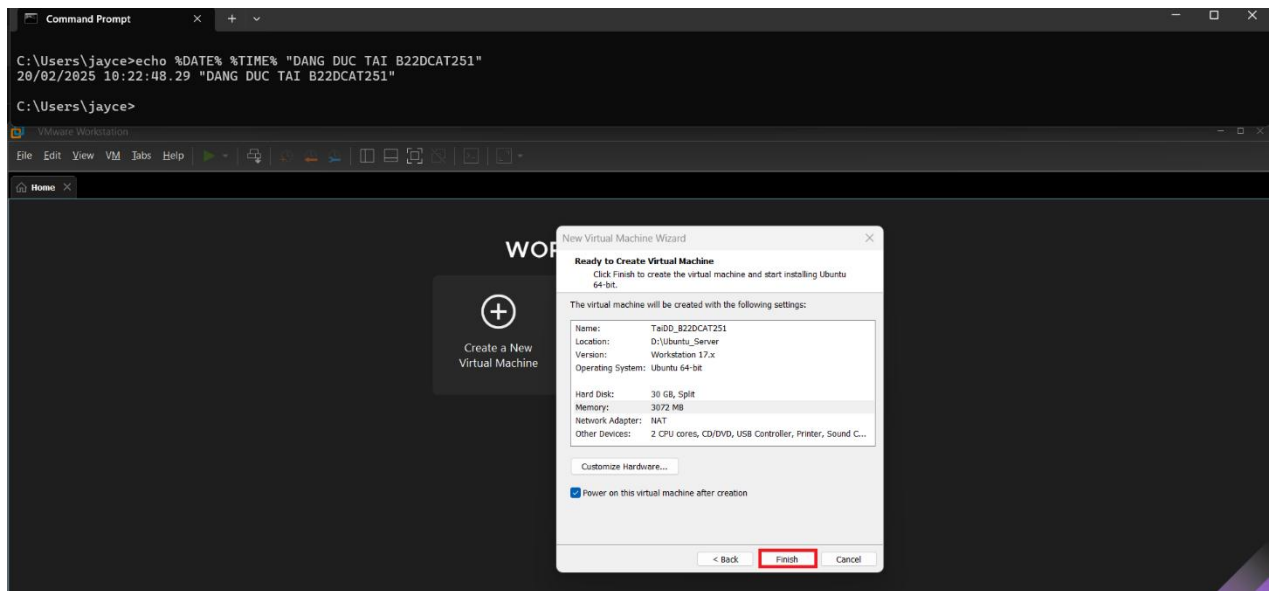
2.2.1 Cài đặt Ubuntu Server

- Bấm vào Create a New Virtual Machine → Load file iso → Next.



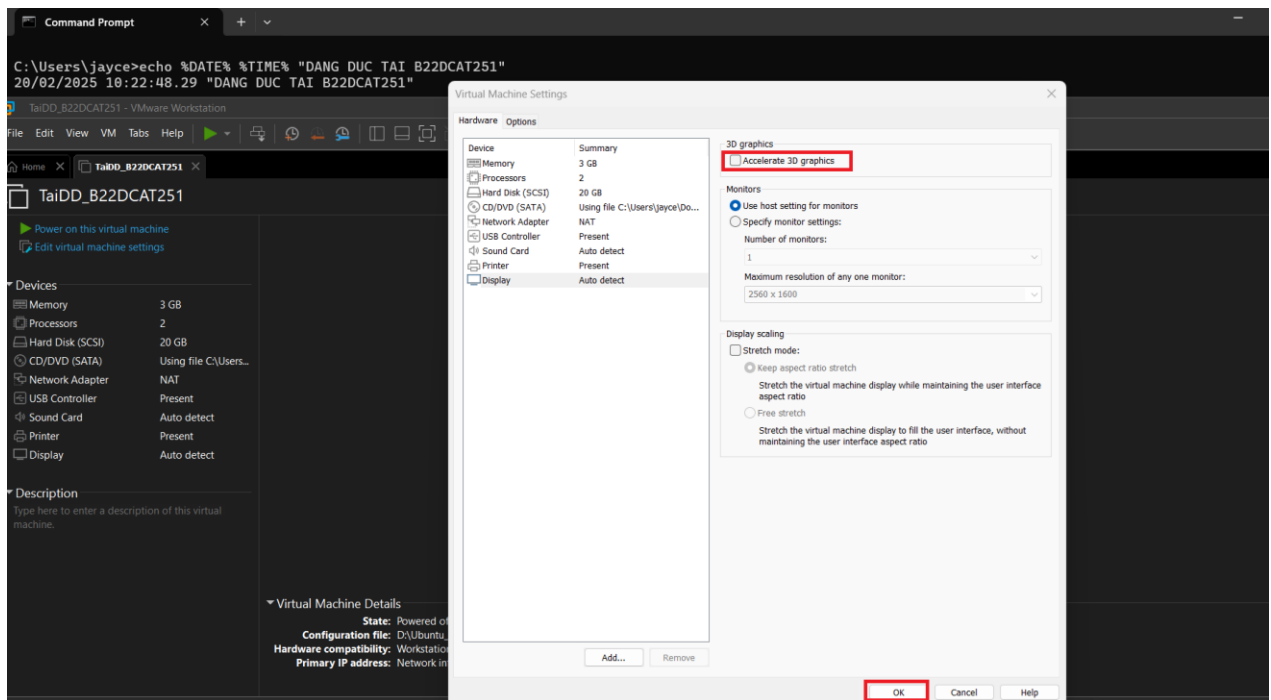
Hình 9 Cài đặt đường dẫn

- Có thể chỉnh lại cấu hình bằng cách Customize Hardware → Finish



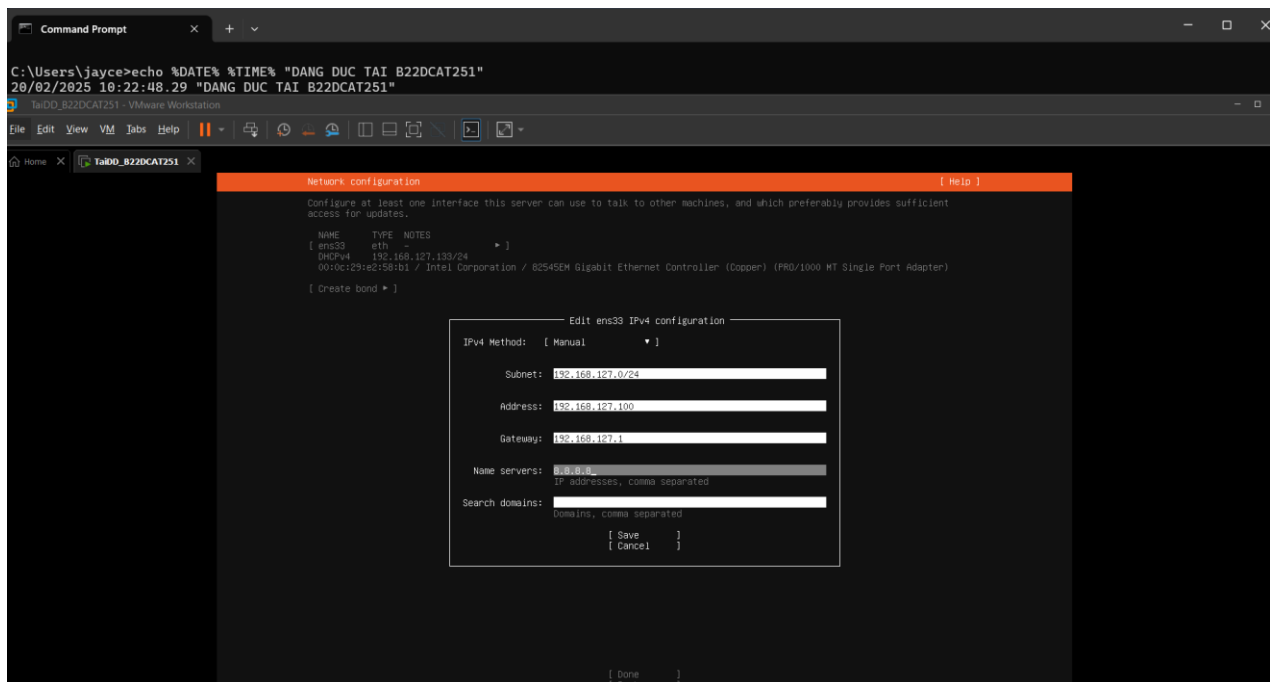
Hình 10 Kiểm tra & Kết thúc cài đặt

- Xử lý ngoại lệ (1): Tắt chế độ Accelerate 3D graphics (trên Vmware).
 → Cần phải tắt tính năng này vì Ubuntu Server không dùng chế độ đồ họa (graphics), nó còn giúp xử lý lỗi gây ra treo máy hoặc lỗi **VMware Workstation unrecoverable error: (svga)**.
 → Mở VMware Workstation → Máy ảo → Edit virtual machine settings → Display
 → Bỏ Accelerate 3D Graphics → Ok.



Hình 11 Tắt chế độ đồ họa

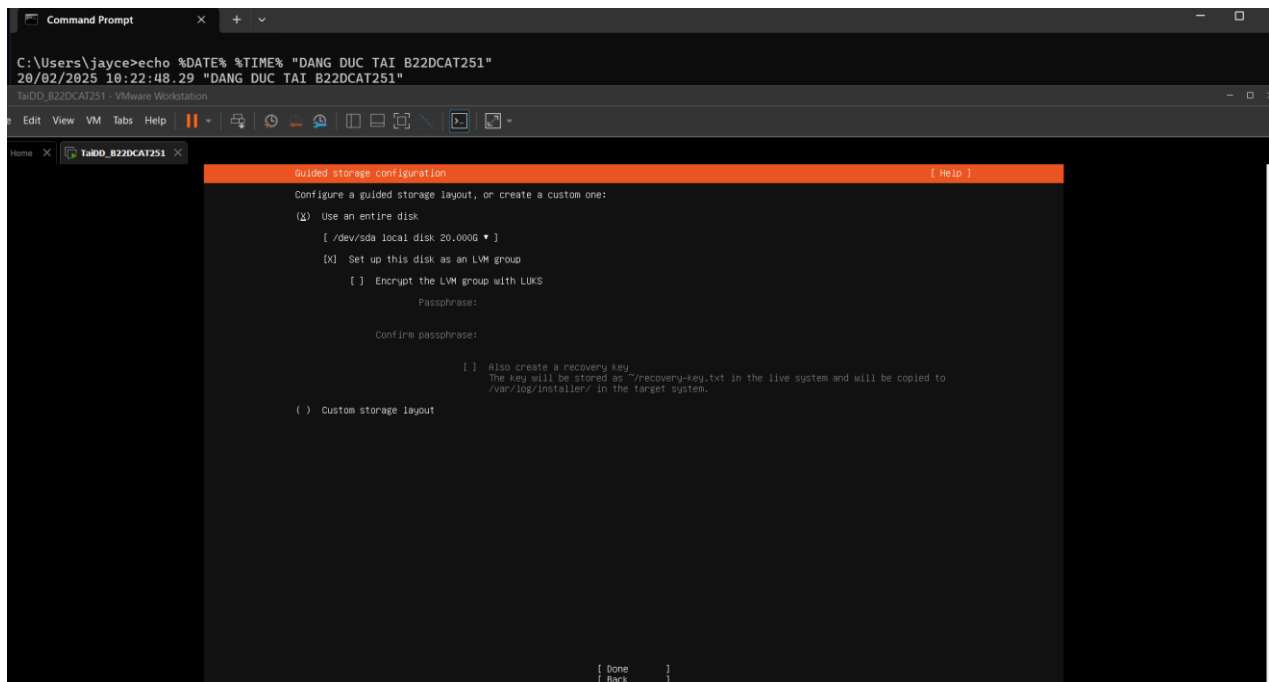
- Sau khi boot, tiến hành cấu hình địa chỉ mạng cho Ubuntu Server.
→ Chọn card mạng ens33 → Manual → Nhập địa chỉ ip cho máy ảo → Done.
- **Lưu ý:** gateway của máy ảo Ubuntu Server phụ thuộc vào chế độ mạng (card mạng) của Vmware.
→ Chế độ NAT (Network Address Translation) có gateway là 192.168.xxx.2.
→ Chế độ Bridged (Cầu nối) có gateway Chính là gateway của mạng LAN.



Hình 12 Cấu hình mạng cho máy ảo

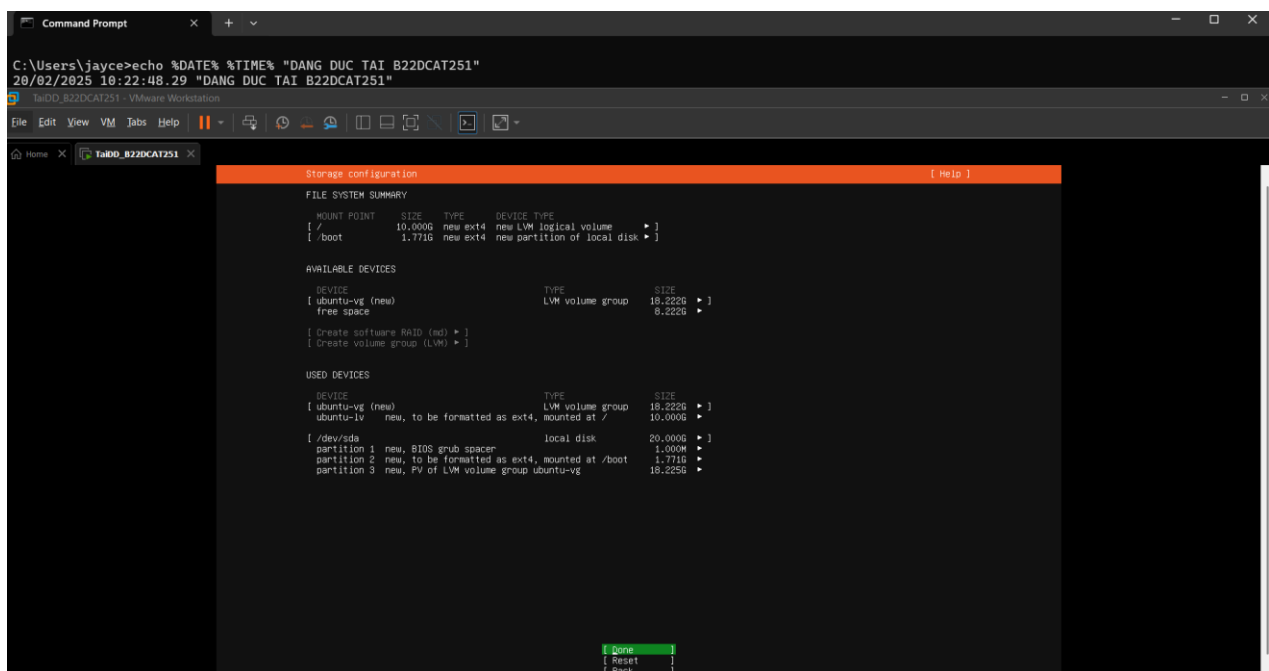
→ Thông tin máy ảo Ubuntu Server có địa chỉ ip là 192.168.127.100, Gateway là 192.168.127.2.

- Tùy chỉnh ổ đĩa disk cho máy ảo (Có thể tùy chỉnh bằng cách chọn mục Custom storage layout) nếu không thì chọn Done.



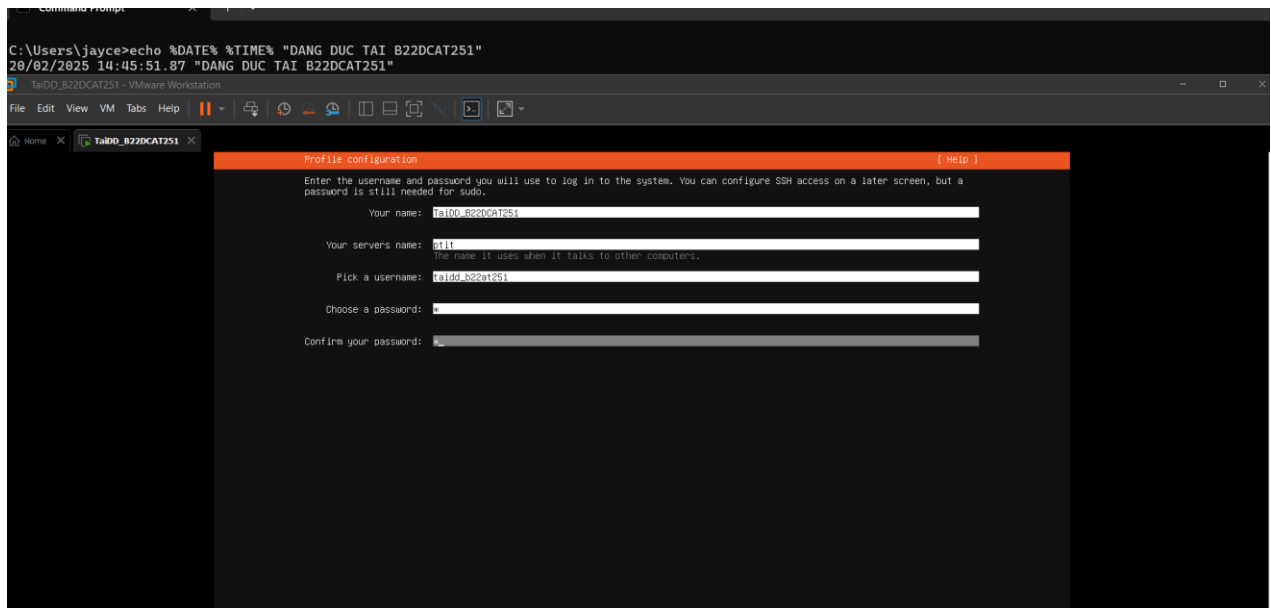
Hình 13 Tùy chỉnh ổ đĩa cho máy ảo

- Cấu hình file system cho máy ảo → Done.



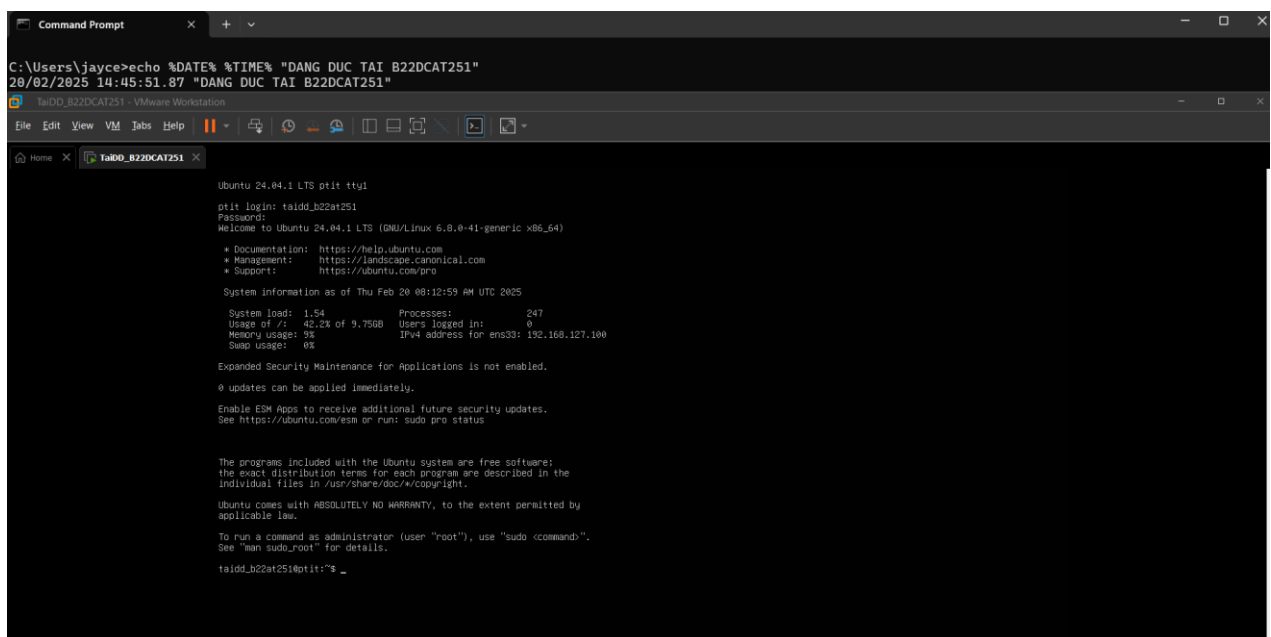
Hình 14 Cấu hình file system cho máy ảo

- Thiết lập tài khoản người dùng → Done.



Hình 15 Thiết lập tài khoản người dùng

- Cài đặt thành công, giao diện của hệ điều hành Ubuntu Server.



Hình 16 Giao diện hệ điều hành Ubuntu Server

2.2.2 Cài đặt dịch vụ OpenSSH

- Cài đặt dịch vụ OpenSSH bằng câu lệnh:
`sudo apt update && sudo apt upgrade -y` # Cập nhật các gói cần thiết
`sudo apt install openssh-server -y` # Cài đặt dịch vụ OpenSSH
- Sử dụng câu lệnh sau để kiểm tra cài đặt
`sudo systemctl status ssh`
 → Hiện thị trạng thái Active, tức là đã cài đặt thành công.


```
C:\Users\jayce>echo %DATE% %TIME% "DANG DUC TAI B22DCAT251"
20/02/2025 14:45:51.87 "DANG DUC TAI B22DCAT251"

TaDD_B22DCAT251 - VMware Workstation

File Edit View VM Tabs Help

TaDD_B22DCAT251

Installing previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu2.24.04.1_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up openssh-sftp-server (1:9.6p1-3ubuntu13.8) ...
Setting up ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up libunwind-dev (4.0-0ubuntu2) ...
Setting up ncurses-term (6.4+20240113-1ubuntu2) ...
Setting up openssh-server (1:9.6p1-3ubuntu13.8) ...

Creating config file /etc/ssh/sshd_config with new version
Created symlink /etc/systemd/system/sockets.target.wants/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Created symlink /etc/systemd/system/ssh.service.requires/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Processing triggers for ufw (0.36-2.6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
Scanning processes...
Scanning candidates...
Scanning linux images...

Pending kernel upgrade!
Running kernel version:
6.8.0-41-generic
Diagnostics:
The currently running kernel version is not the expected kernel version 6.8.0-53-generic.

Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.

Restarting services...

Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
taidd_b22cat251 @ session #1: login[1281]
taidd_b22cat251 @ user manager service: systemd[1393]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
taidd_b22cat251@taidd:~$ sudo systemctl status ssh
● ssh.service - OpenSSH Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: inactive (dead)
   TriggeredBy: ● ssh.socket
   Docs: man:sshd(8)
          man:sshd_config(5)
taidd_b22cat251@taidd:~$
```

Hình 17 Cài đặt dịch vụ OpenSSH

- Cài đặt PuTTY bằng Chocolatey trên PowerShell
→ *choco install putty*

```
File Edit Format View Help
Dang Duc Tai
B22DCAT251

Ln 1, Col 1 100% Windows (CRLF) UTF-8

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\Users\jayce> choco install putty -y
Chocolatey v2.4.2
Usage of the --trace option is only allowed when running from an elevated session.
3 validations performed, 2 success(es), 1 warning(s), and 0 error(s).

Validation Warnings:
- A pending system reboot request has been detected, however, this is being ignored due to the current Chocolatey configuration. If you want to halt when this occurs, then either set the global feature using:
  choco feature enable --name="exitOnRebootDetected"
  or pass the option --exit-when-reboot-detected.

Chocolatey detected you are not running from an elevated command shell (cmd/powershell).

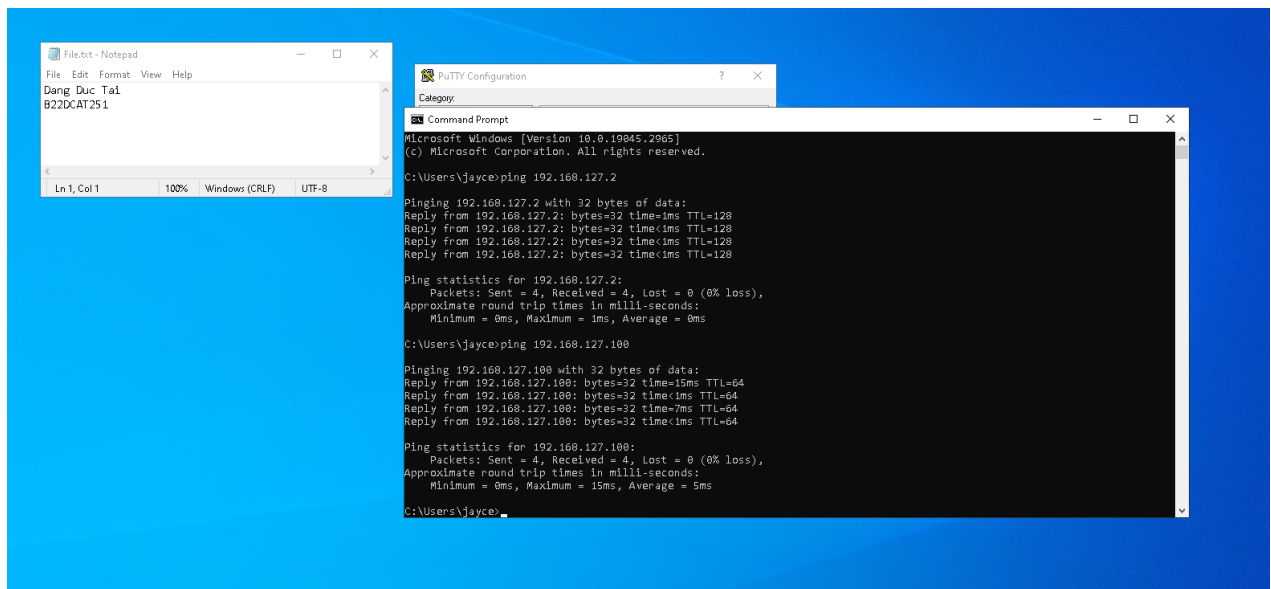
You may experience errors - many functions/packages require admin rights. Only advanced users should run choco w/out an elevated shell. When you open the command shell, you should ensure that you do so with "Run as Administrator" selected. If you are attempting to use Chocolatey in a non-administrator setting, you must select a different location other than the default install location. See https://docs.chocolatey.org/en-us/choco/setup#non-administrative-install for details.

For the question below, you have 20 seconds to make a selection.

Do you want to continue? ([Y]es/[N]o):
Timeout or your choice of '' is not a valid selection.
Installing the following packages:
putty
By installing, you accept licenses for the packages.
Downloading package from source 'https://community.chocolatey.org/api/v2/'
Progress: Downloading putty.portable 0.83.0... 100%
```

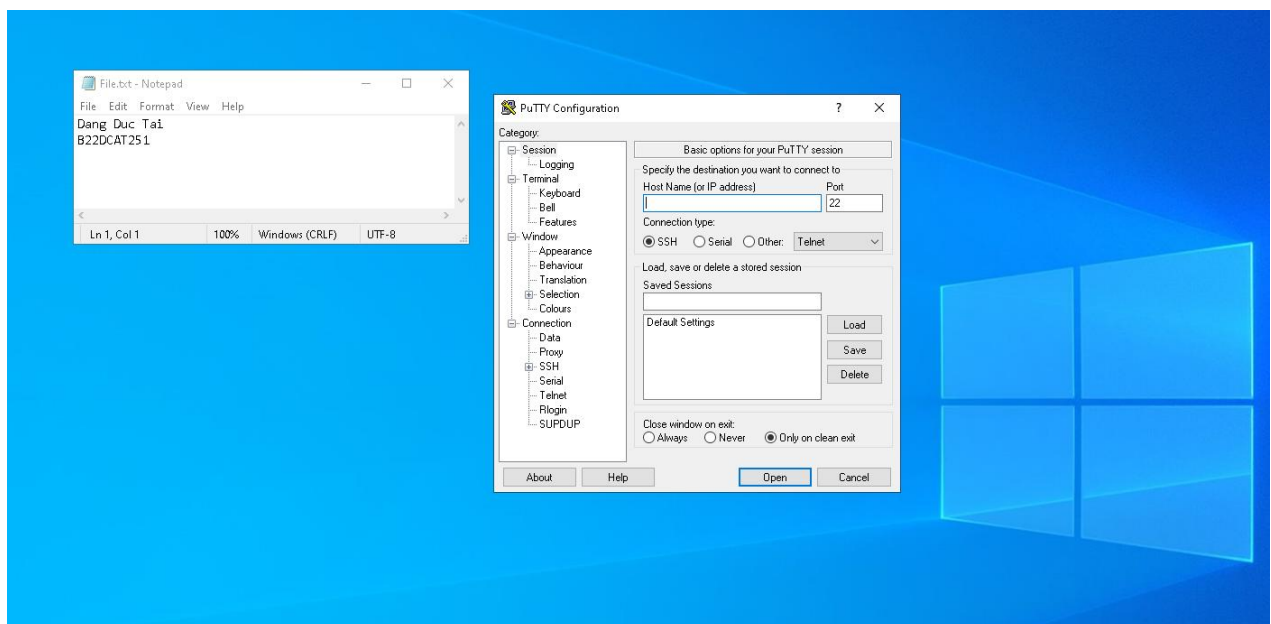
Hình 18 Cài đặt PuTTY

- Kết nối đến Ubuntu Server bằng PuTTY. Trước hết thử ping kết nối.
ping 192.168.127.2 #Gateway Server
ping 192.168.127.100 #Ip Server



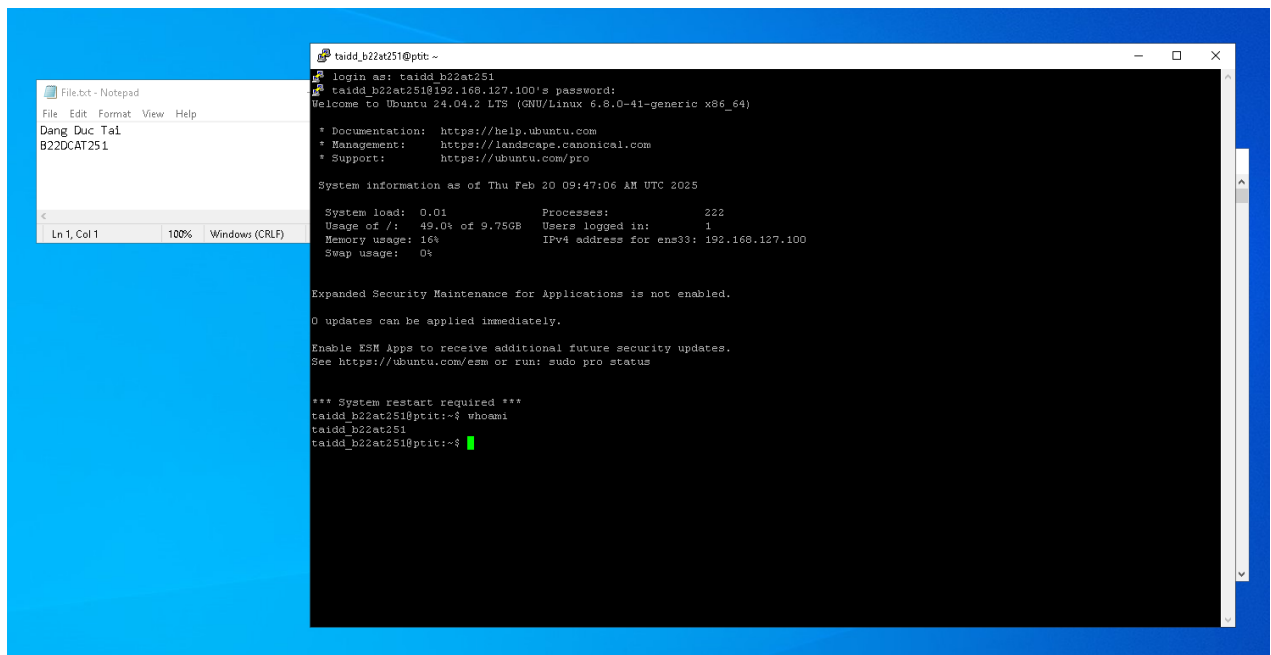
Hình 19 Ping kết nối giữa máy trạm với server

- Nhập ip của máy chủ Ubuntu vào mục Host Name, điều chỉnh Connection Type là SSH, port 22 → Open.



Hình 20 Kết nối tới Ubuntu Server bằng PuTTY

- Kết nối bằng tài khoản username:password của Server.
- Kết nối thành công, nhập câu lệnh *whoami* để kiểm tra.



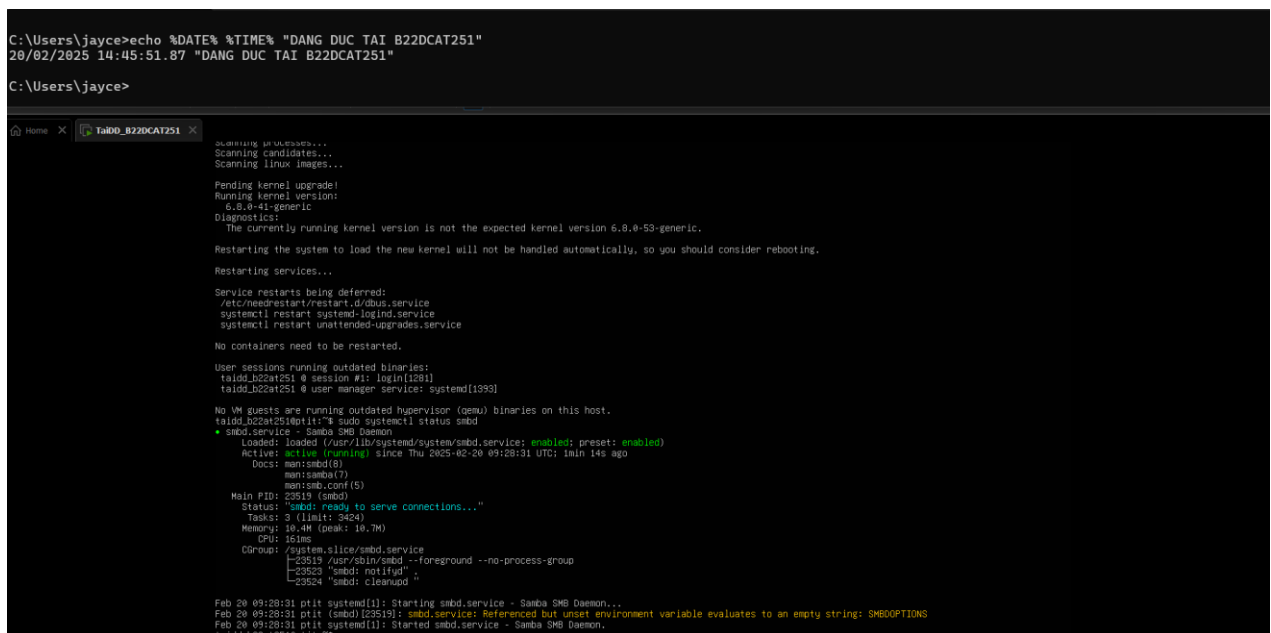
Hình 21 Kết nối thành công tới Ubuntu Server

2.2.3 Cài đặt và cấu hình dịch vụ Samba

- Cài đặt dịch vụ samba bằng câu lệnh

sudo apt install samba -y

→ Hiện thị trạng thái Active, tức là cài đặt thành công.



Hình 22 Cài đặt dịch vụ Samba

- Tạo tài khoản User.

sudo mkdir -p /home/TaiDDB22AT251/share

sudo chown TaiDDB22AT251:TaiDDB22AT251 /home/TaiDDB22AT251/share

sudo chmod 770 /home/TaiDDB22AT251/share

```
Command Prompt
C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
20/02/2025 20:58:18.35 "Dang Duc Tai B22DCAT251"

me X  TaiDD_B22DCAT251 X  Windows 10 x64 X
taidd_b22at251@ptit:~$ sudo mkdir -p /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$ sudo chown TaiDDB22AT251:TaiDDB22AT251 /home/TaiDDB22AT251/share
chown: cannot access '/home/TaiDDB22AT251/share': Permission denied
taidd_b22at251@ptit:~$ sudo chown TaiDDB22AT251:TaiDDB22AT251 /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$ sudo chmod 770 /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$
```

Hình 23 Tạo tài khoản User

- Tạo tài khoản Admin, tương tự

```
Command Prompt
C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
20/02/2025 20:58:18.35 "Dang Duc Tai B22DCAT251"

me X  TaiDD_B22DCAT251 X  Windows 10 x64 X
taidd_b22at251@ptit:~$ sudo mkdir -p /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$ sudo chown TaiDDB22AT251:TaiDDB22AT251 /home/TaiDDB22AT251/share
chown: cannot access '/home/TaiDDB22AT251/share': Permission denied
taidd_b22at251@ptit:~$ sudo chown TaiDDB22AT251:TaiDDB22AT251 /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$ sudo chmod 770 /home/TaiDDB22AT251/share
taidd_b22at251@ptit:~$
```

Hình 24 Tạo tài khoản admin

- Thêm dòng sau vào cuối file /etc/samba/smb.conf

[TaiDDB22AT251]

path = /home/TaiDDB22AT251/share

valid users = TaiDDB22AT251

read only = no

browsable = yes

create mask = 0770

directory mask = 0770

[admin]

path = /home/admin/share

valid users = admin

read only = no

browsable = yes

create mask = 0770

directory mask = 0770

```

Command Prompt

C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
20/02/2025 20:58:18.35 "Dang Duc Tai B22DCAT251"

TaID0B22AT251]
path = /home/TaID0B22AT251/share
valid users = TaID0B22AT251
read only = no
browsable = yes
create mask = 0770
directory mask = 0770
admin]
path = /home/admin/share
valid users = admin
read only = no
browsable = yes
create mask = 0770
directory mask = 0770
File Name to Write: /etc/samba/smb.conf
[ Help          M-D DOS Format      M-A Append      M-B Backup File
[ Cancel        M-M Mac Format      M-P Prepend     M-T Browse

```

Hình 25 Cấu hình file smb.conf

- Khởi động lại dịch vụ:
`sudo systemctl restart smbd`
`sudo systemctl restart nmbd`

```

Command Prompt

C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
20/02/2025 20:58:18.35 "Dang Duc Tai B22DCAT251"

taidd_b22at251@pitit:~$ sudo systemctl restart smbd
taidd_b22at251@pitit:~$ sudo systemctl restart nmbd

```

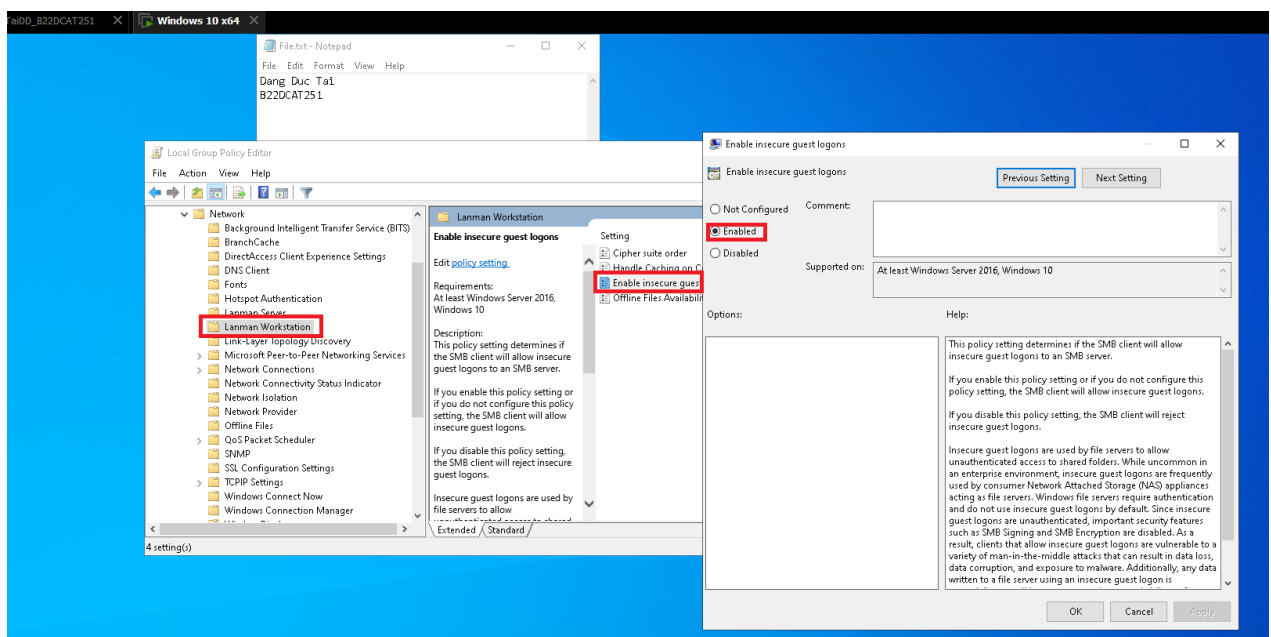
Hình 26 Khởi động lại dịch vụ

- Xử lý ngoại lệ (2): Lỗi “You can’t access this shared folder because your organization’s security policies block unauthenticated guest access”.

→ Lỗi này xảy ra khi sử dụng máy tính windows 10 truy cập share folder, kết nối máy in trong mạng nội bộ.

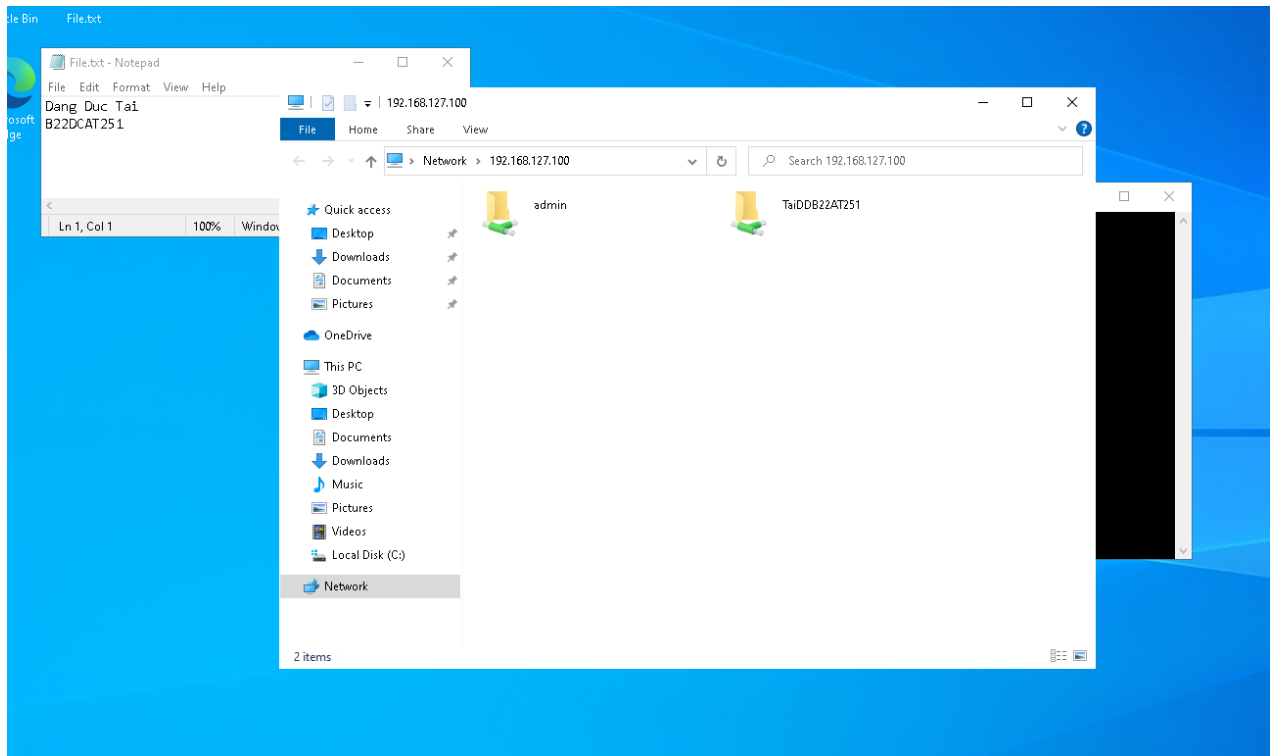
→ Cách khắc phục: Mở file Computer Configuration → Administrative Templates

→ Network → Lanman Workstation → Enable insecure guest → Enabled.



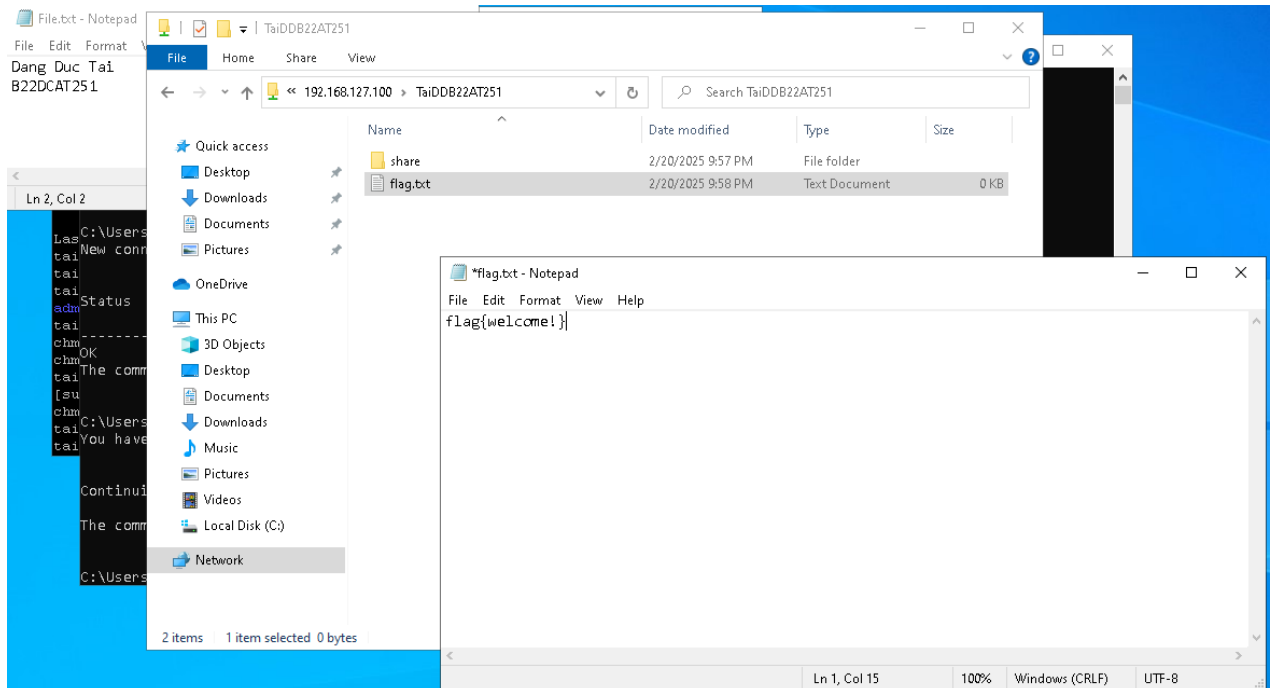
Hình 27 Xử lý ngoại lệ chia sẻ file

- Truy cập vào đường dẫn mạng tới thư mục chia sẻ.
`\\192.168.127.100`



Hình 28 Truy cập vào thư mục chia sẻ

- Nhập mật khẩu để truy cập vào thư mục, thử tạo/đọc file/thư mục trên đó.



Hình 29 Truy cập vào thư mục user

- Xử lý ngoại lệ (3): Lỗi xảy ra do Windows không cho phép một người dùng kết nối đến cùng một máy chủ Samba với nhiều tài khoản khác nhau.
→ Cách khắc phục: Ngắt kết nối kết nối cũ đến máy chủ Samba, sau đó kết nối tới tài khoản mới.

net use #Xem kết nối hiện tại

*net use * /delete /y* #Ngắt kết nối đến máy chủ Samba

```

C:\Users\jaye>net use
New connections will be remembered.

Status           Local        Remote              Network
-----
OK                \\192.168.127.100\TaiIDDB22AT251
                  Microsoft Windows Network

The command completed successfully.

C:\Users\jaye>net use * /delete /y
You have these remote connections:

                \\192.168.127.100\TaiIDDB22AT251
Continuing will cancel the connections.

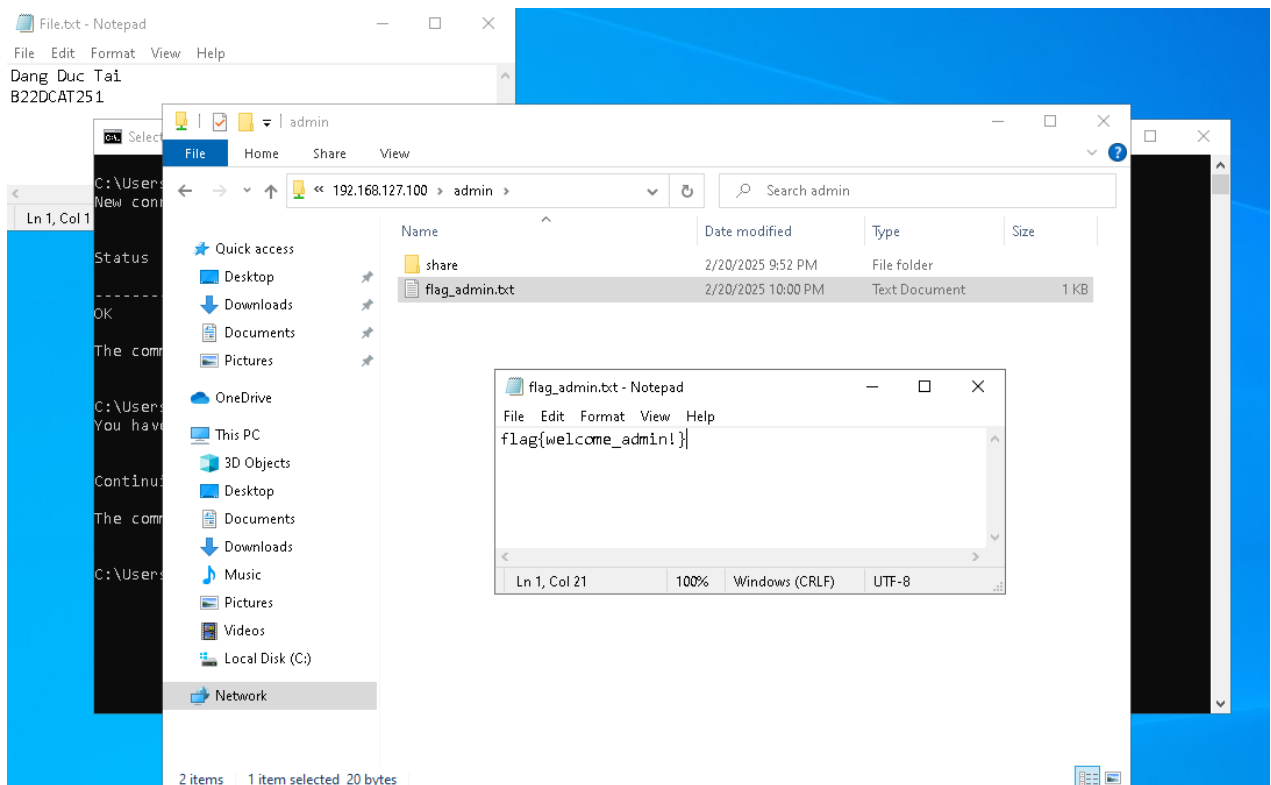
The command completed successfully.

C:\Users\jaye>

```

Hình 30 Ngắt kết nối tới máy chủ Samba

- Truy cập lại vào thư mục admin.

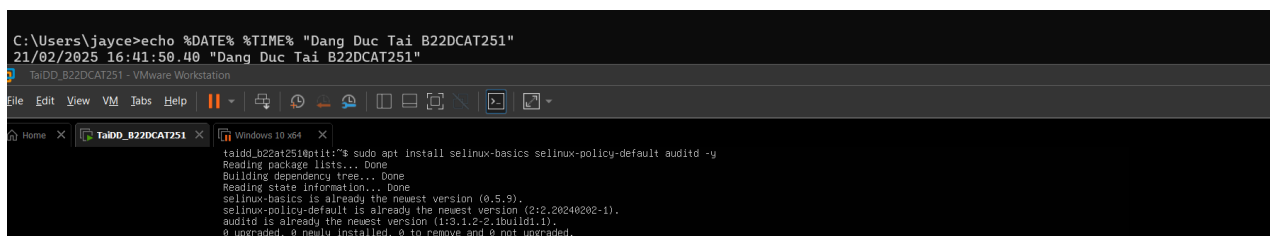


Hình 31 Truy cập vào thư mục admin

2.2.4 Cài đặt và cấu hình dịch vụ SELinux

- Cài đặt dịch vụ SELinux

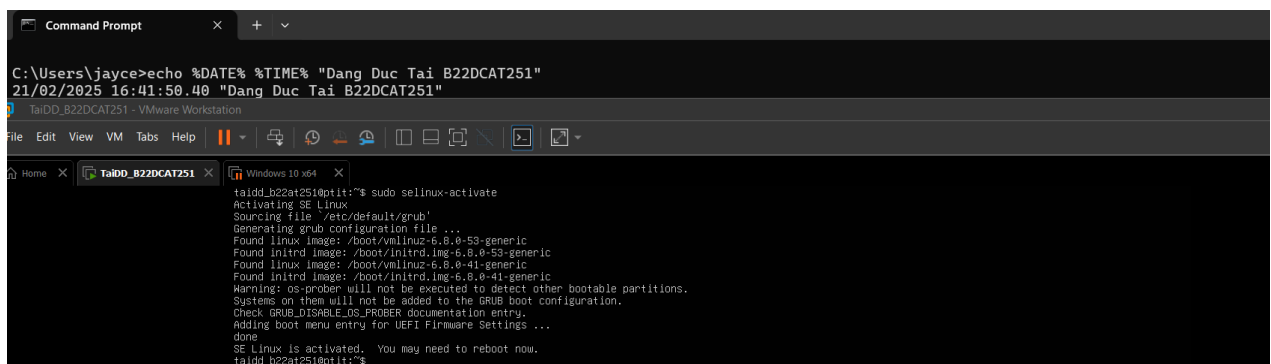
`sudo apt install selinux-basics selinux-policy-default auditd -y`



Hình 32 Cài đặt SELinux trên Ubuntu Server

- Sau khi cài đặt, cần bật SELinux bằng câu lệnh.

`sudo selinux-activate`

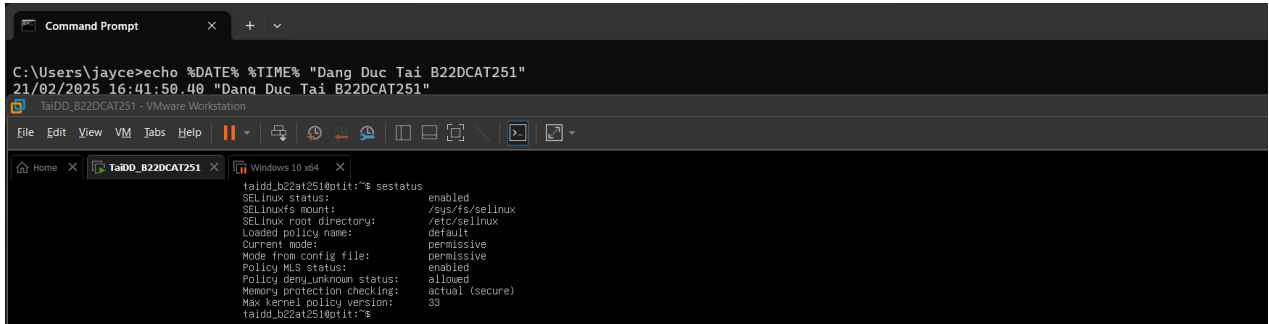


Hình 33 Kích hoạt SELinux

- Reboot server, kiểm tra trạng thái hoạt động. Câu lệnh trả về kết quả **SELinux status: enabled** tức là cài đặt thành công.

sudo reboot

sestatus



```

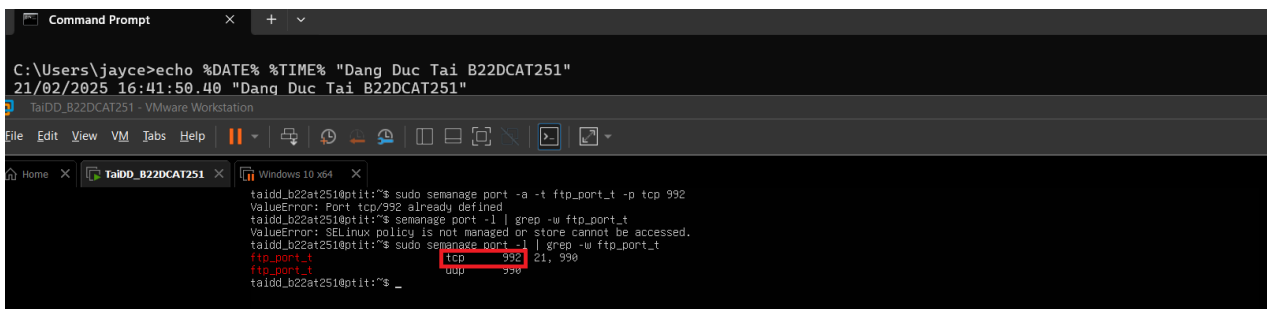
C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
21/02/2025 16:41:50.40 "Dang Duc Tai B22DCAT251"

taidd_b22cat251@taidd_b22cat251:~$ sestatus
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:       /etc/selinux
Loaded policy name:            default
Current mode:                  permissive
Mode from config file:         permissive
Policy MLS status:             enabled
Policy deny_unknown status:    allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     33
taidd_b22cat251@taidd_b22cat251:~$

```

Hình 34 Cài đặt thành công SELinux

- Cấu hình SELinux để thêm protocol TCP cổng 992 vào dịch vụ FTP
- Sử dụng lệnh sau để thêm protocol TCP cổng 992 vào dịch vụ FTP:
sudo semanage port -a -t ftp_port_t -p tcp 992
(Nếu gặp lỗi, **semanage: command not found**, hãy cài đặt gói polycoreutils)
sudo apt install polycoreutils -y
- Kiểm tra thành công bằng câu lệnh
semanage port -l | grep -w ftp_port_t
→ ftp_port_t hiển thị cổng tcp 992, tức là đã cài đặt thành công.



```

C:\Users\jayce>echo %DATE% %TIME% "Dang Duc Tai B22DCAT251"
21/02/2025 16:41:50.40 "Dang Duc Tai B22DCAT251"

taidd_b22cat251@taidd_b22cat251:~$ sudo semanage port -a -t ftp_port_t -p tcp 992
ValueError: Port tcp/992 already defined
taidd_b22cat251@taidd_b22cat251:~$ sudo semanage port -l | grep -w ftp_port_t
ValueError: SELinux policy is not managed or store cannot be accessed.
taidd_b22cat251@taidd_b22cat251:~$ sudo semanage port -l | grep -w ftp_port_t
ftp_port_t      tcp      992    21, 990
ftp_port_t      udp      992    990
taidd_b22cat251@taidd_b22cat251:~$

```

Hình 35 Cấu hình SELinux cho dịch vụ FTP

TÀI LIỆU THAM KHẢO

- [1] Phạm Hoàng Duy, Bài giảng Hệ điều hành Windows và Linux/Unix, Học viện Công Nghệ Bưu Chính Viễn Thông, 2016.
- [2] Tom Carpenter, Microsoft Windows Server Operating System Essentials, Sybex, 2011.
- [3] Wale Soyinka, Linux Administration A Beginners Guide, McGraw-Hill Osborne Media, 2012.