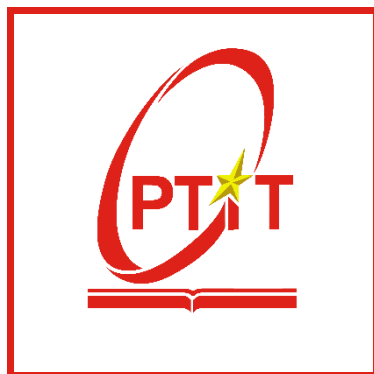


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**  
**KHOA AN TOÀN THÔNG TIN**

---



**THỰC TẬP CƠ SỞ**  
**Bài 4: Cài đặt và cấu hình Windows Server**

Sinh viên	Nguyễn Duy Đạt
MSV	B21DCAT056
Giảng viên	Vũ Minh Mạnh

**Hà Nội – 2024**

## Môn học Thực tập cơ sở

### Bài 4: Cài đặt và cấu hình Windows Server

#### I. Lý thuyết

##### 1. Tìm hiểu về Windows Server

Windows Server là một hệ điều hành đa năng được thiết kế dành riêng cho môi trường máy chủ. Nó cung cấp sự ổn định, khả năng kết nối mạng tiên tiến, tính năng bảo mật mạnh mẽ, khả năng mở rộng và các công cụ quản lý toàn diện.

Windows Server đảm bảo hoạt động đáng tin cậy và không bị gián đoạn của các ứng dụng và quy trình kinh doanh quan trọng. Nó cung cấp các tính năng mạng nâng cao như bộ điều khiển miền, Active Directory và dịch vụ DHCP để quản lý mạng và xác thực người dùng hiệu quả.

Bảo mật là ưu tiên hàng đầu trong Windows Server, với các tính năng như kiểm soát truy cập chi tiết, kiểm tra và Chính sách nhóm. Nó hỗ trợ các giải pháp bảo mật bổ sung như tường lửa và phần mềm chống vi-rút để tăng cường khả năng bảo vệ tổng thể.

Windows Server có khả năng mở rộng cao, đáp ứng nhu cầu của các doanh nghiệp đang phát triển và nhu cầu công nghệ ngày càng phát triển. Nó cung cấp nhiều vai trò và tính năng máy chủ khác nhau, bao gồm Máy chủ Web, Quản lý cơ sở dữ liệu, Hỗ trợ ảo hóa và Dịch vụ máy tính từ xa.

So sánh Windows Server với Windows Workstation:

Windows Server	Windows Workstation
Được thiết kế cho môi trường máy chủ	Được thiết kế cho máy tính cá nhân, máy tính xách tay và máy tính bảng
Cung cấp các công cụ quản lý, khả năng mở rộng và hiệu suất cao	Cung cấp giao diện thân thiện với người dùng và các tính năng trực quan
Tập trung vào sự ổn định, khả năng tương thích và dịch vụ lâu dài	Sử dụng chu kỳ phát hành thường xuyên với các tính năng mới 6 tháng một lần

Hỗ trợ nhiều ứng dụng máy chủ và phần mềm doanh nghiệp	Tương thích với hầu hết các ứng dụng tiêu dùng và kinh doanh
Nhắm mục tiêu các chuyên gia CNTT, quản trị viên hệ thống và tổ chức	Hướng tới người tiêu dùng cá nhân, tổ chức giáo dục và doanh nghiệp
Cung cấp khả năng kết nối mạng tiên tiến và kiểm soát tập trung các tài nguyên	Nhấn mạnh vào bảo mật cấp độ người dùng và các tác vụ điện toán cá nhân
Kết hợp các biện pháp bảo mật mạnh mẽ và hỗ trợ các giải pháp bổ sung	Bao gồm các tính năng bảo mật như Windows Defender Antivirus
Thích hợp cho môi trường máy chủ cấp doanh nghiệp	Thích hợp cho các tác vụ tính toán cá nhân và kết nối mạng quy mô nhỏ
Cung cấp các công cụ quản lý toàn diện cho quản lý máy chủ	Cung cấp các công cụ quản lý thân thiện với người dùng và cập nhật thường xuyên để thuận tiện cho người dùng
Nâng cao năng suất, khả năng mở rộng và độ tin cậy cho các hoạt động kinh doanh quan trọng	Nâng cao trải nghiệm người dùng, khả năng sáng tạo và khả năng kết nối giữa các thiết bị

## 2. Tìm hiểu về Web Server, FTP Server và Remote Desktop Users

- ❖ Trong môi trường máy chủ Windows, dịch vụ Web được cung cấp thông qua dịch vụ thông tin Internet IIS (Internet Information Services). Ngoài dịch vụ Web, người quản trị có thể cài đặt dịch vụ truyền file và gửi thư điện tử thông qua dịch vụ thông tin này.

Để kiểm soát việc truy nhập tới các trang chủ Web, người quản trị có thể đặt hạn chế về địa chỉ mạng thông qua chức năng thiết lập luật hạn chế (Add Allow Restriction Rule) của máy chủ IIS. Mặt khác, có thể thiết lập các cơ chế xác thực để xác định người dùng được phép truy nhập vào trang web. Có một số cách thức như sau:

- Nặc danh (Anonymous): cho phép bất cứ người dùng nào cũng được truy nhập mà không cần xác thực.
- Xác thực cơ bản (Basic Authentication): yêu cầu người dùng cung cấp tên và mật khẩu hợp lệ. Tuy nhiên cách này không mã hóa thông tin nên chứa đựng rủi ro an toàn.

- Xác thực số (Digest Authentication): dùng máy chủ miền xác thực.
- Xác thực Windows (Windows Authentication): sử dụng giao thức NTLM hay Kerberos để xác thực.

❖ Dịch vụ file cho phép người dùng lưu trữ và chia sẻ các dữ liệu, chương trình với người dùng khác trong mạng. Việc truy nhập thành công các file chia sẻ phải căn cứ vào quyền truy nhập mà người dùng có được. Trong môi trường Windows có thể áp dụng hai hình thức đảm bảo an ninh

- Quyền với thư mục chia sẻ. Hình thức này chỉ áp dụng với thư mục và các quyền của người dùng giới hạn: Đọc/Ghi/Sở hữu
- Đặt quyền file/thư mục sử dụng cách thức phân quyền NTFS để kiểm soát việc truy nhập. Hình thức này cho phép giám sát tốt hơn và các quyền chi tiết hơn.

Việc thực hiện chia sẻ file có thể được thực hiện trực tiếp từ trình duyệt file của Windows. Khi này hình thức chia sẻ là chia sẻ thư mục đòi hỏi người dùng phải có tài khoản và quyền phù hợp trên máy tính chia sẻ. Nói cách khác, người dùng và quyền chỉ có giá trị cục bộ trên máy tính chia sẻ.

Khi thực hiện việc chia sẻ qua thư mục động thì hình thức kiểm soát truy nhập sử dụng cơ chế giống NTFS. Như vậy người dùng cần phải có tài khoản và quyền phù hợp trong thư mục động đó.

❖ Dịch vụ truy nhập từ xa cho phép người dùng kết nối từ bên ngoài vào máy chủ dịch vụ bên trong để truy nhập dữ liệu và các ứng dụng như làm việc trên máy tính thông thường. Cùng với sự phát triển của các công nghệ truyền dữ liệu tốc độ cao dịch vụ truy nhập từ xa trở nên tiện dụng hơn.

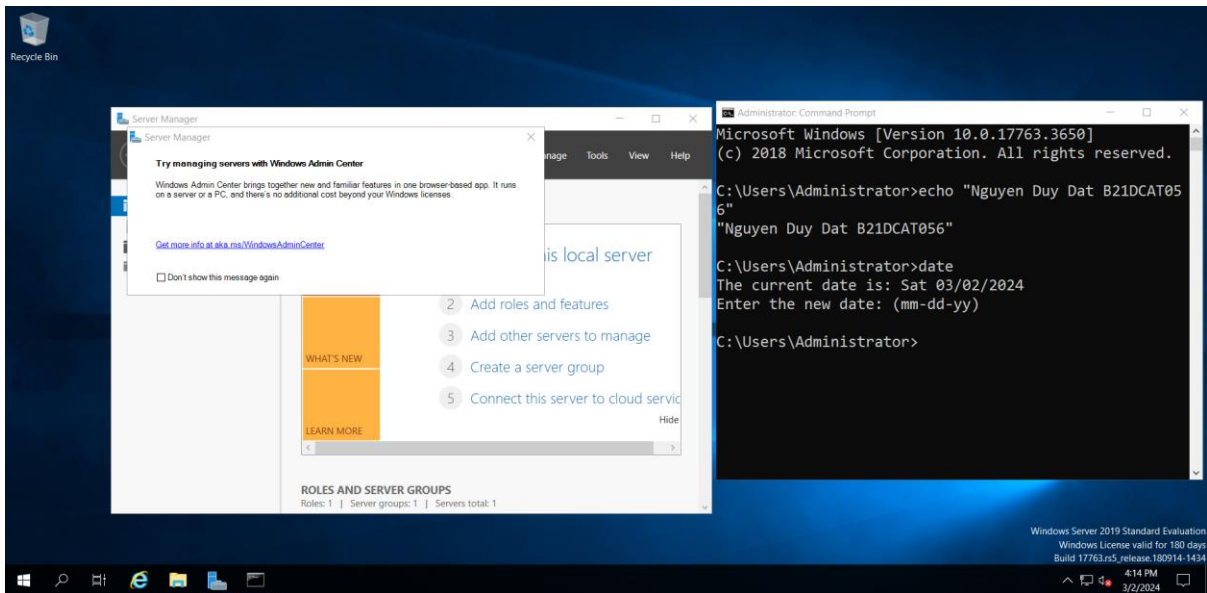
Dịch vụ truy nhập từ xa thường sử dụng mạng riêng ảo VPN (Virtual Private Networks) hỗ trợ các giao thức:

- Point-to-Point Tunneling Protocol (PPTP): Đơn giản khi triển khai song tính bảo mật yếu
- Layer 2 Tunneling Protocol (L2TP): Dùng chuẩn IPSec.
- Secure Socket Tunneling Protocol (SSTP): dùng giao thức http bảo mật

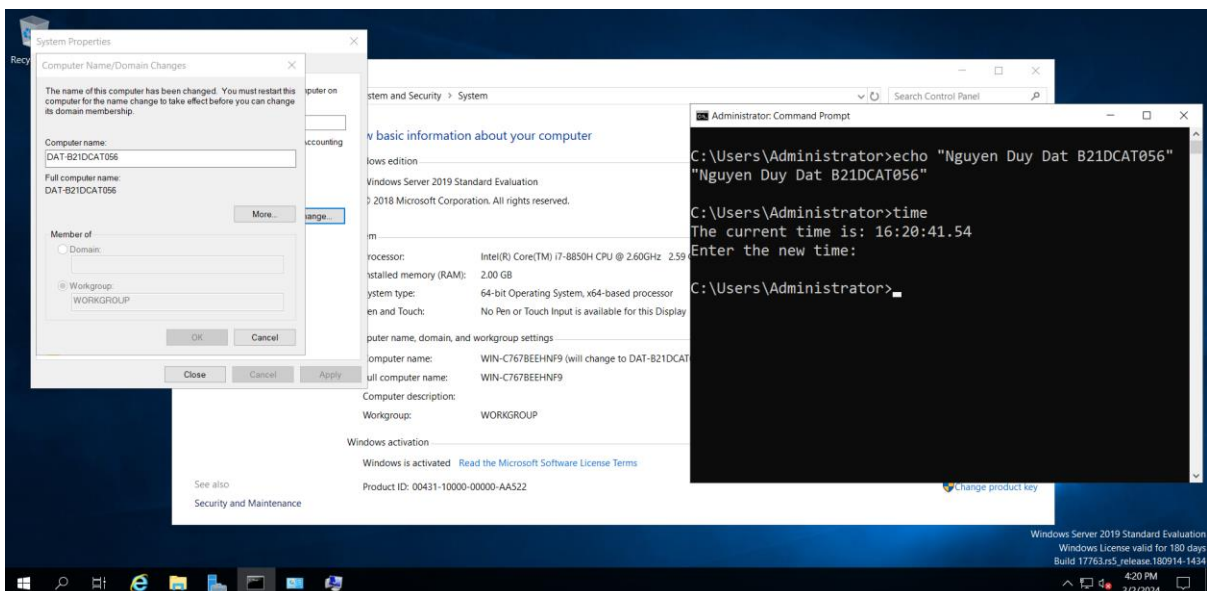
## II. Cài đặt

### 1. Cài đặt Windows Server

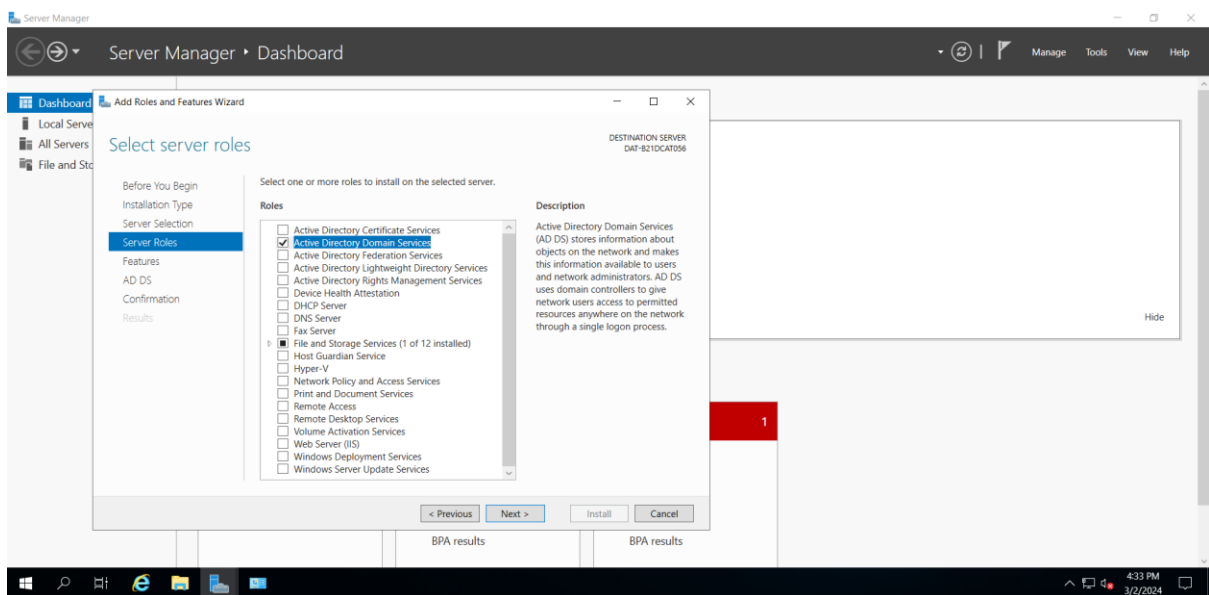
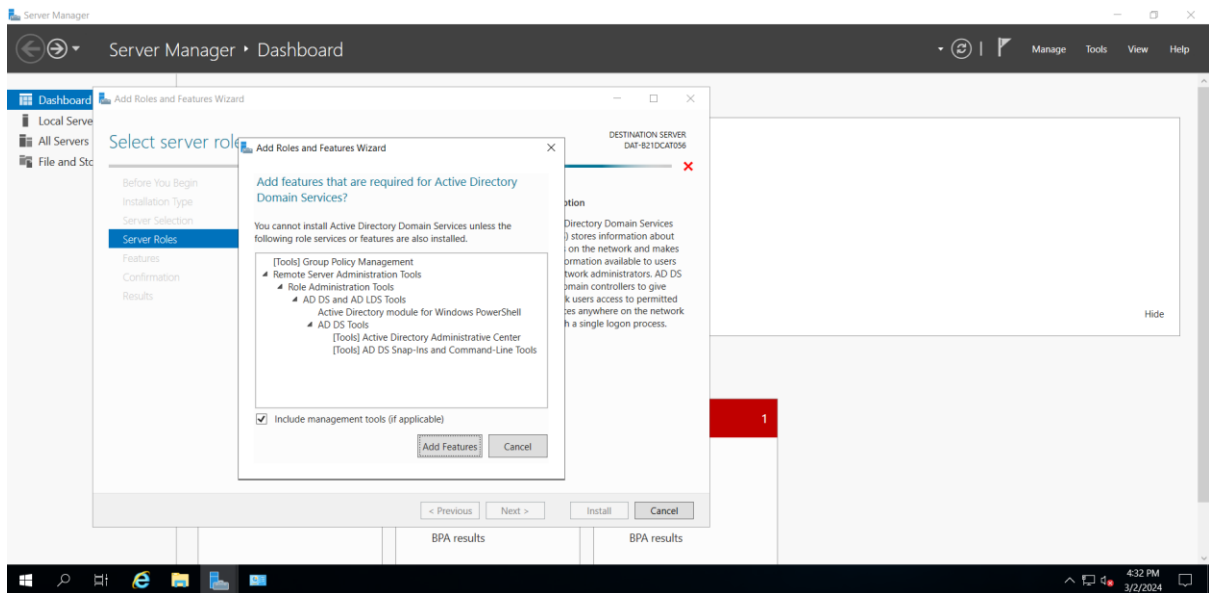
#### - Cài đặt Windows Server thành công



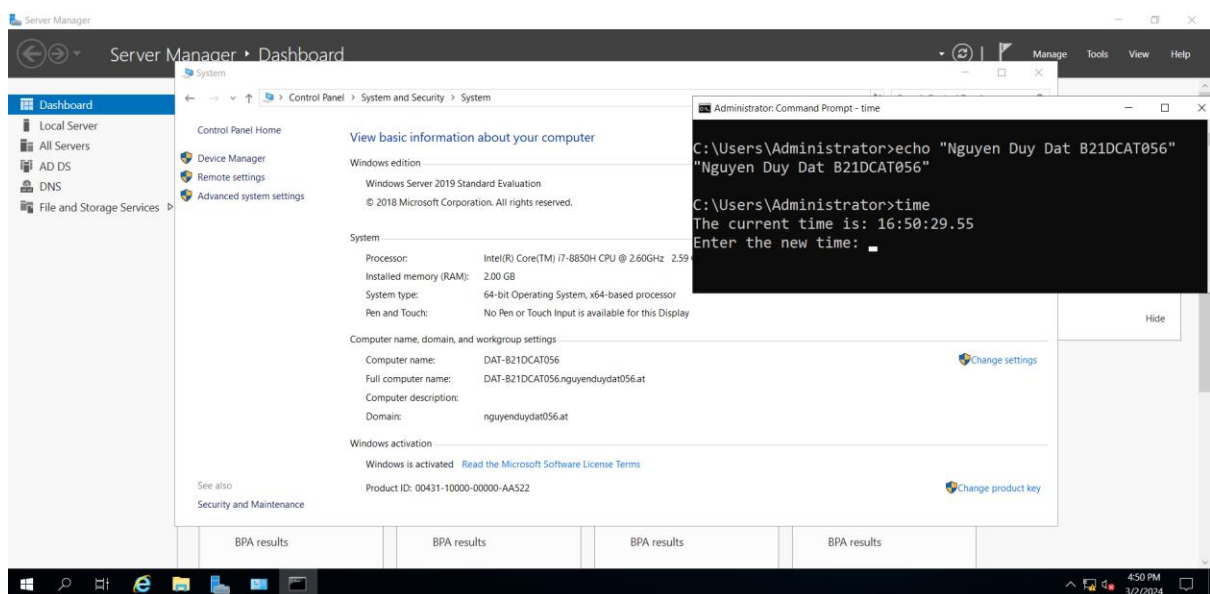
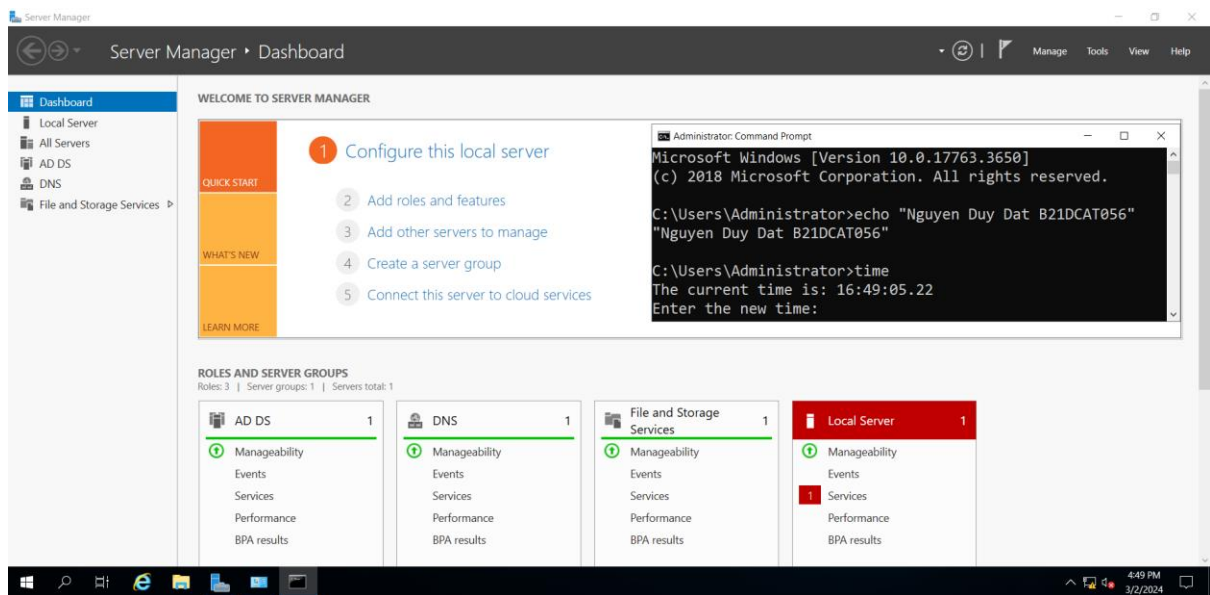
#### - Đổi tên Server thành: DAT-B21DCAT056



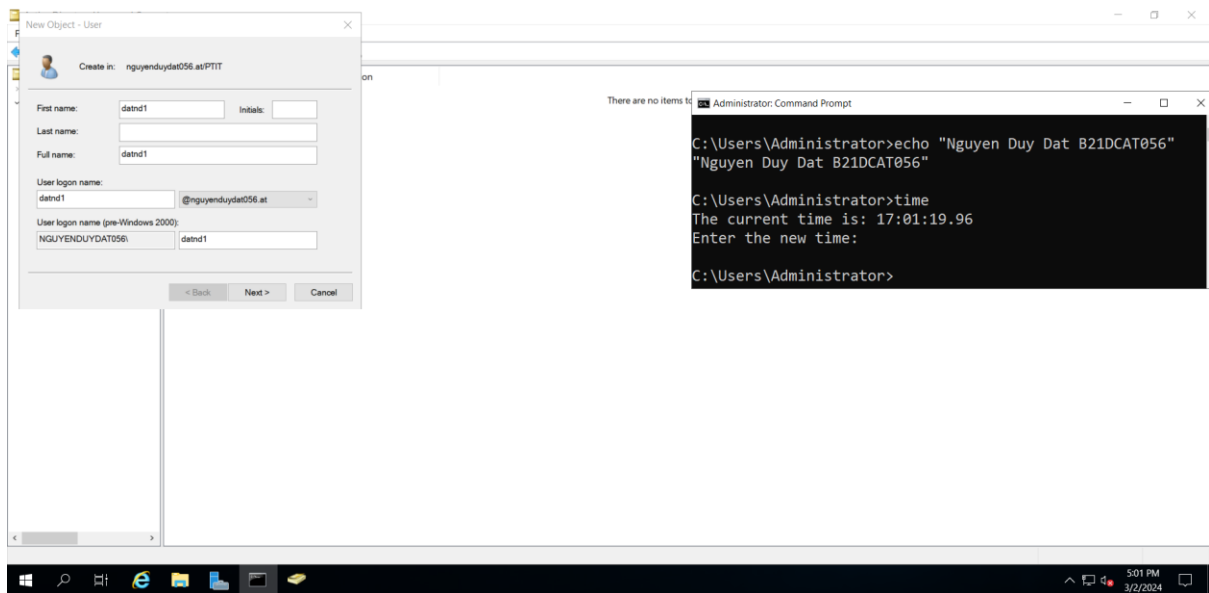
## - Cài đặt server role trong Server Manager



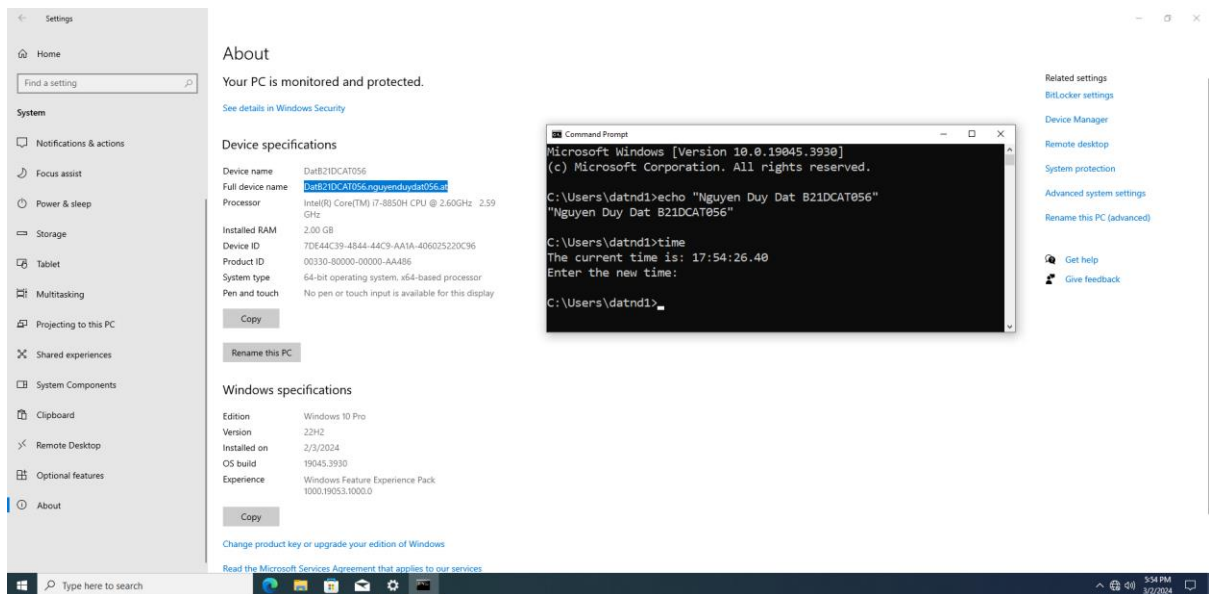
## - Nâng cấp Server thành Domain Controller



## - Tạo User trong OU PTIT



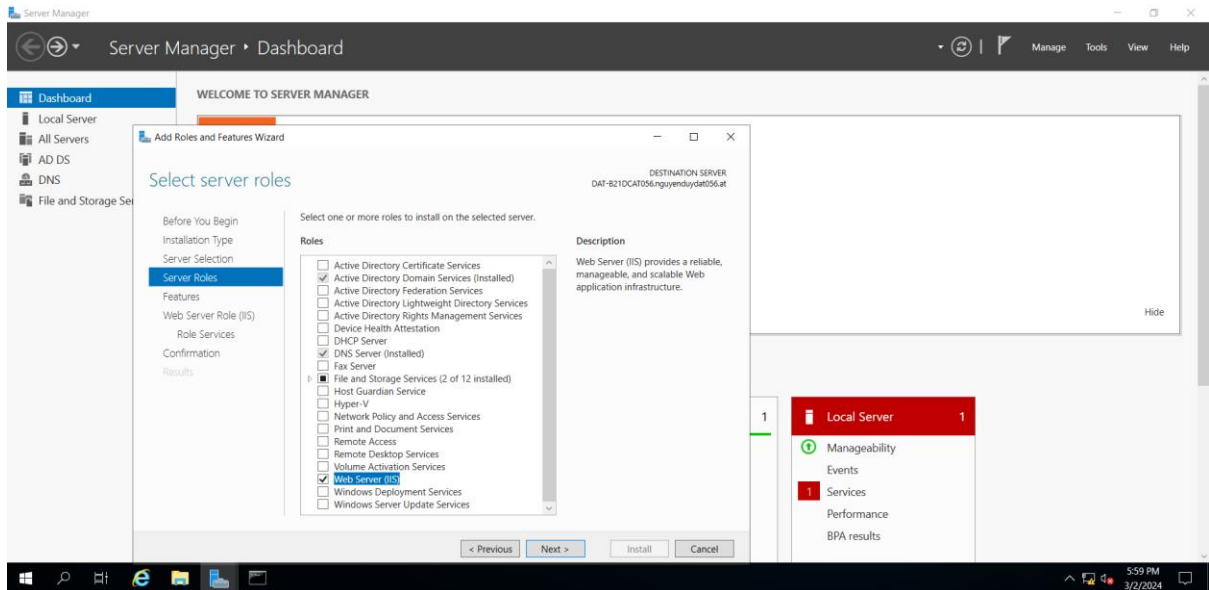
## - Máy trạm Windows gia nhập vào domain vừa tạo được



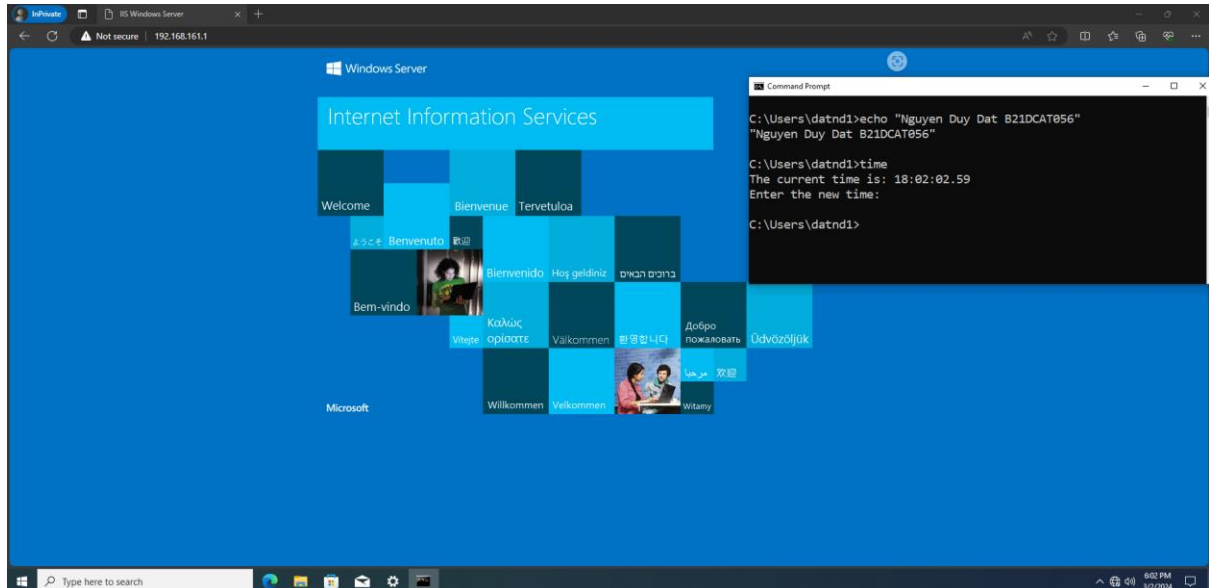


## 2. Cài đặt Web

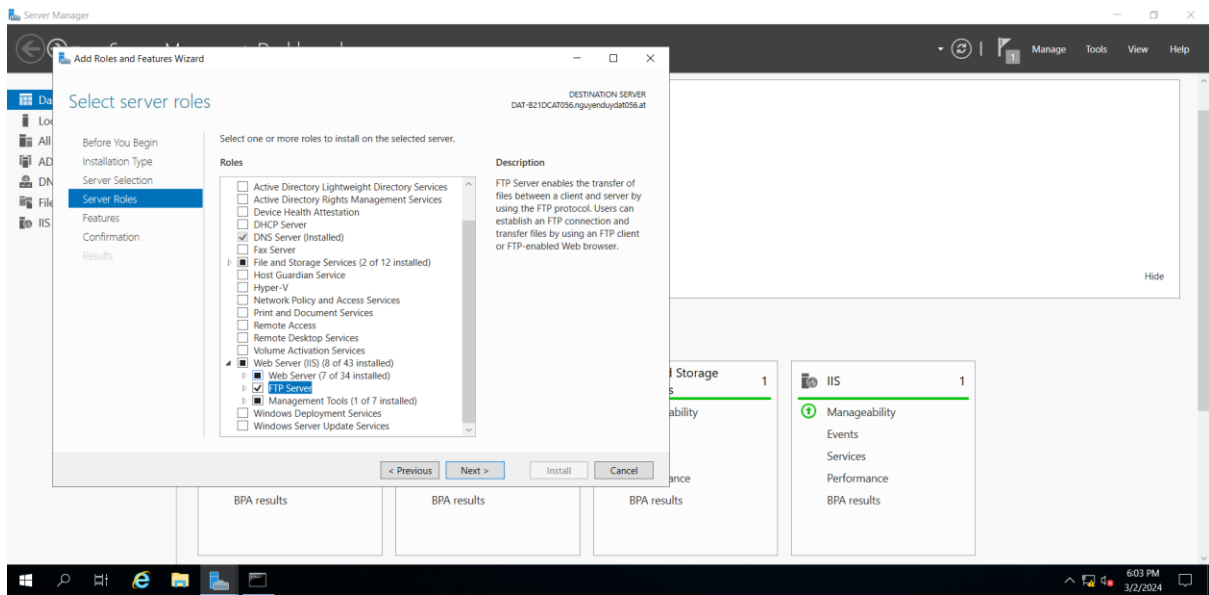
### - Cài đặt Web Server (IIS) trong Server Manager



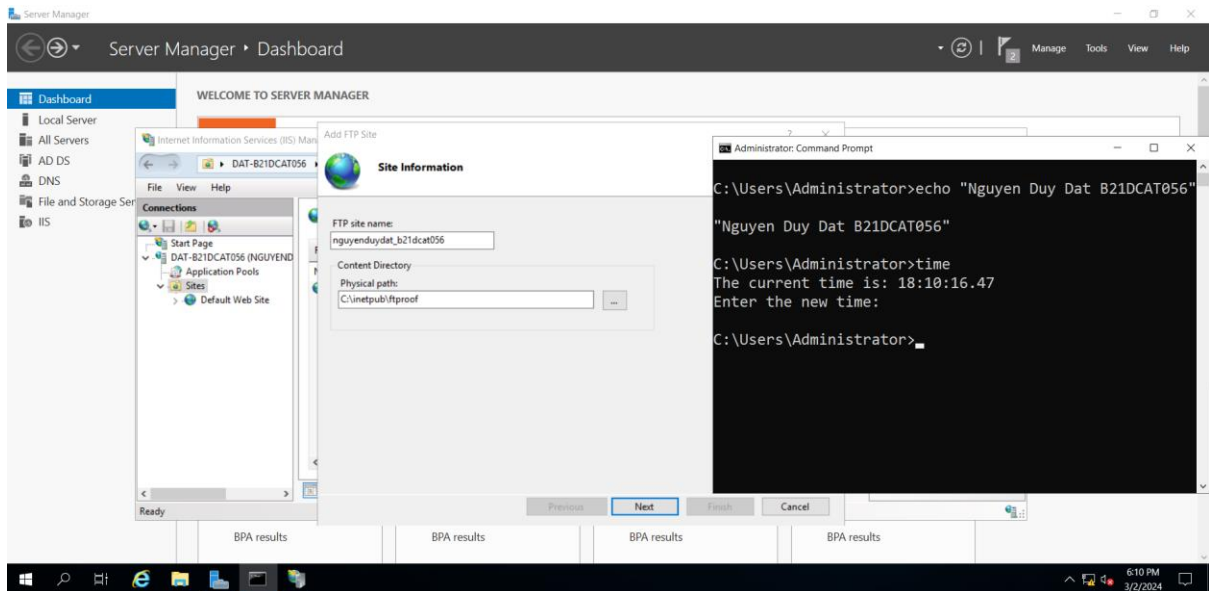
### - Truy cập thành công web từ máy trạm



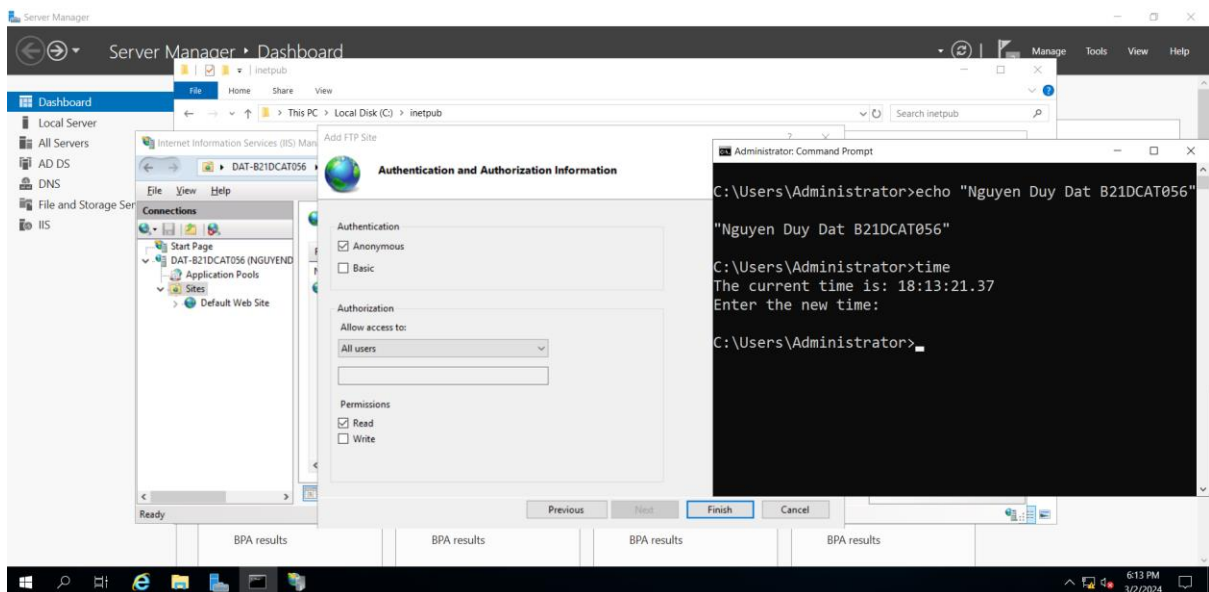
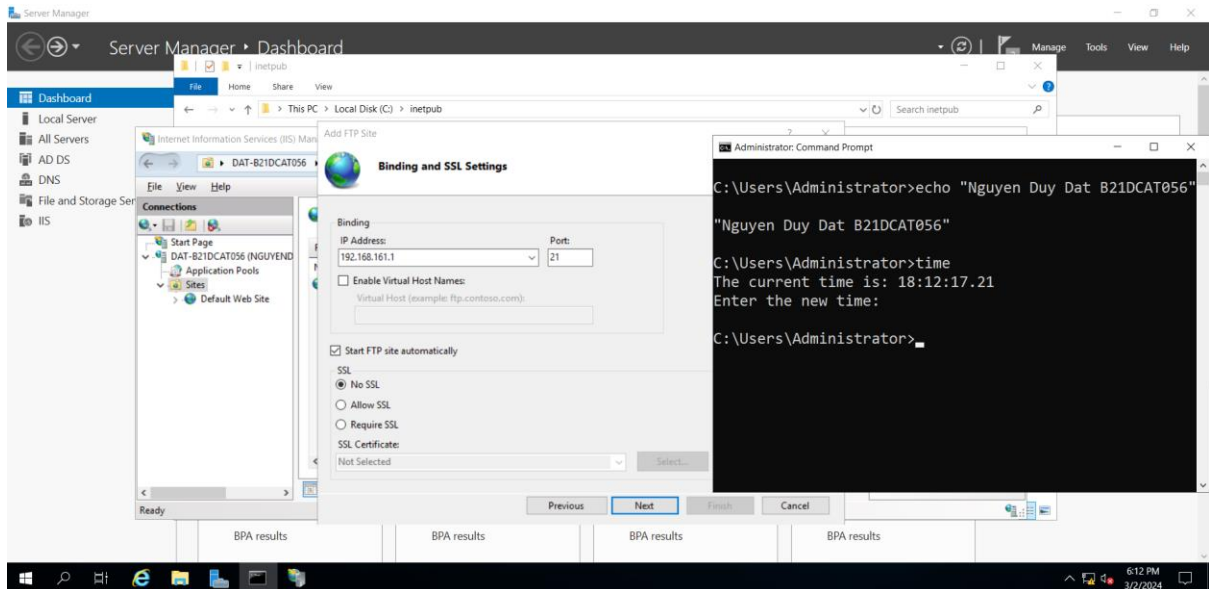
## - Cài đặt FTP Server trong Web Server



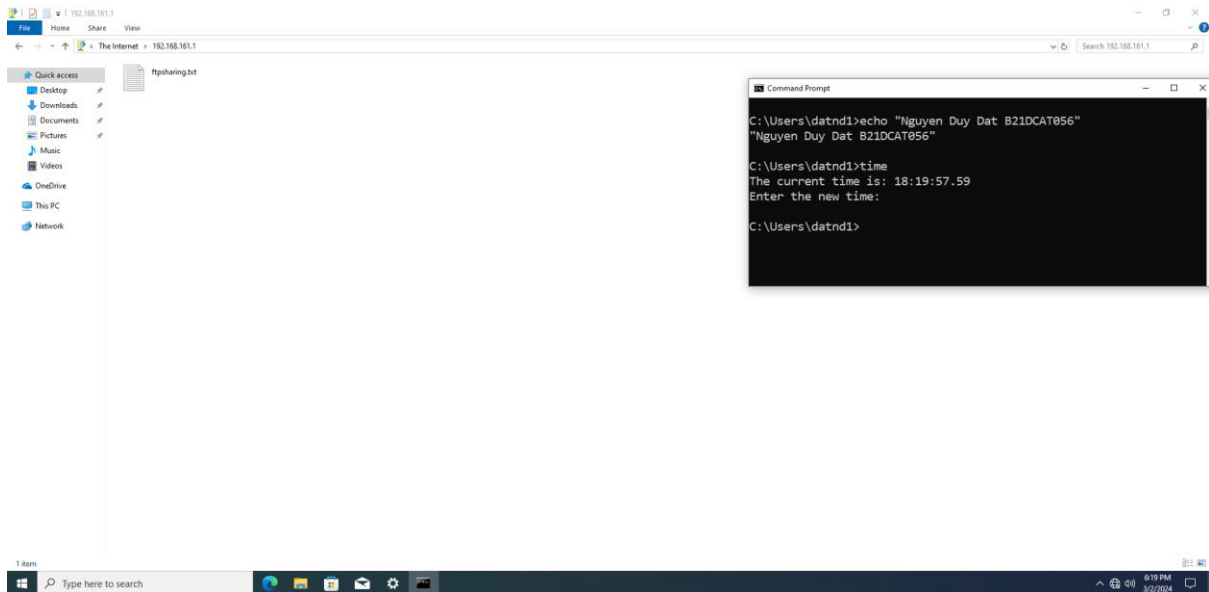
## - Add ftpsite trong mục Sites với tên là: nguyenduydat\_b21dcat056



- Cấu hình FTP Site: Ip address: 192.168.161.1; port: 21; chọn No SSL.
- Tiếp theo chọn Authentication: Anonymous; Permissions: Read.

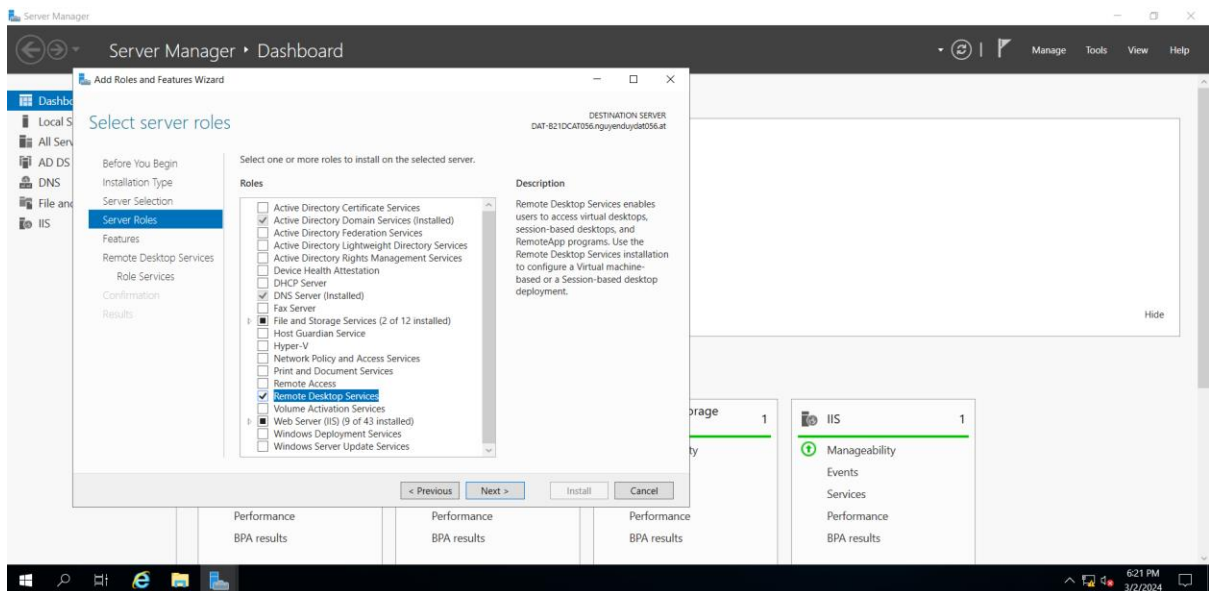


- Khởi động máy Windows 7 đã cài đặt sau đó vào my computer và nhập vào phần đường dẫn “ftp://192.168.161.1” → đã truy cập được file ftpsharing

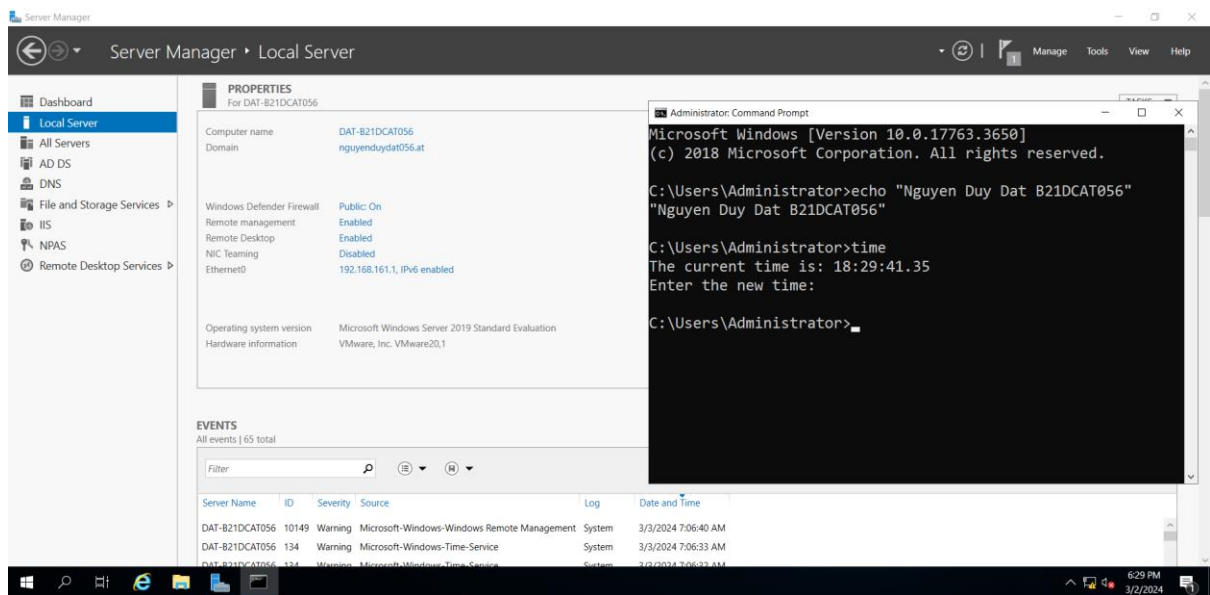


### 3. Cài đặt Remote

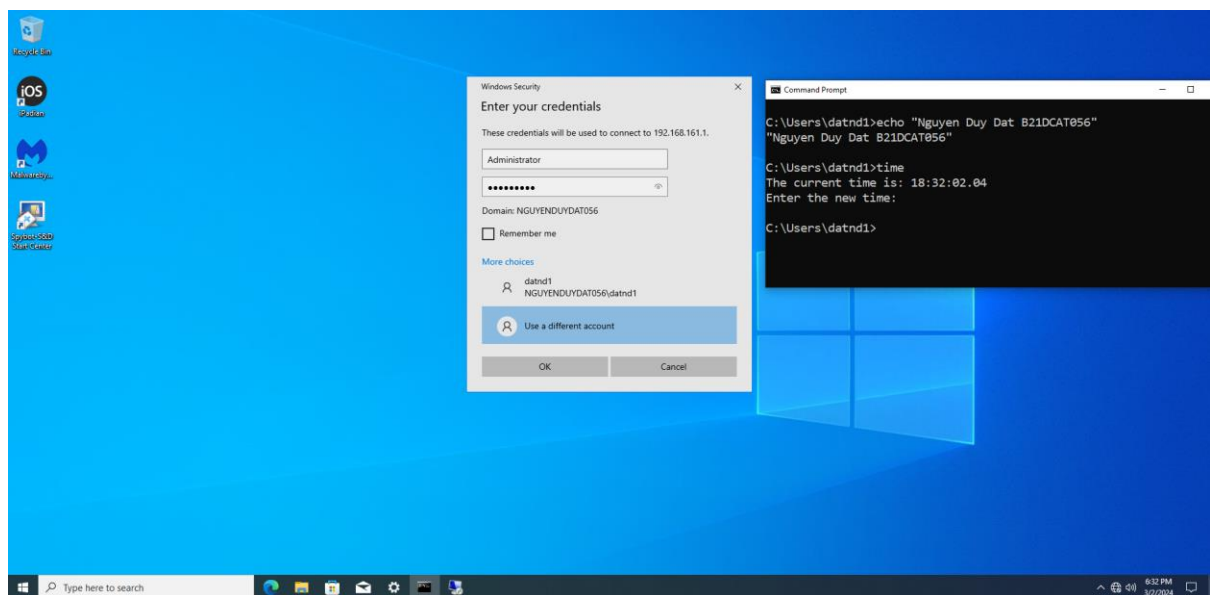
- Cài đặt Remote Desktop trong Server Manager



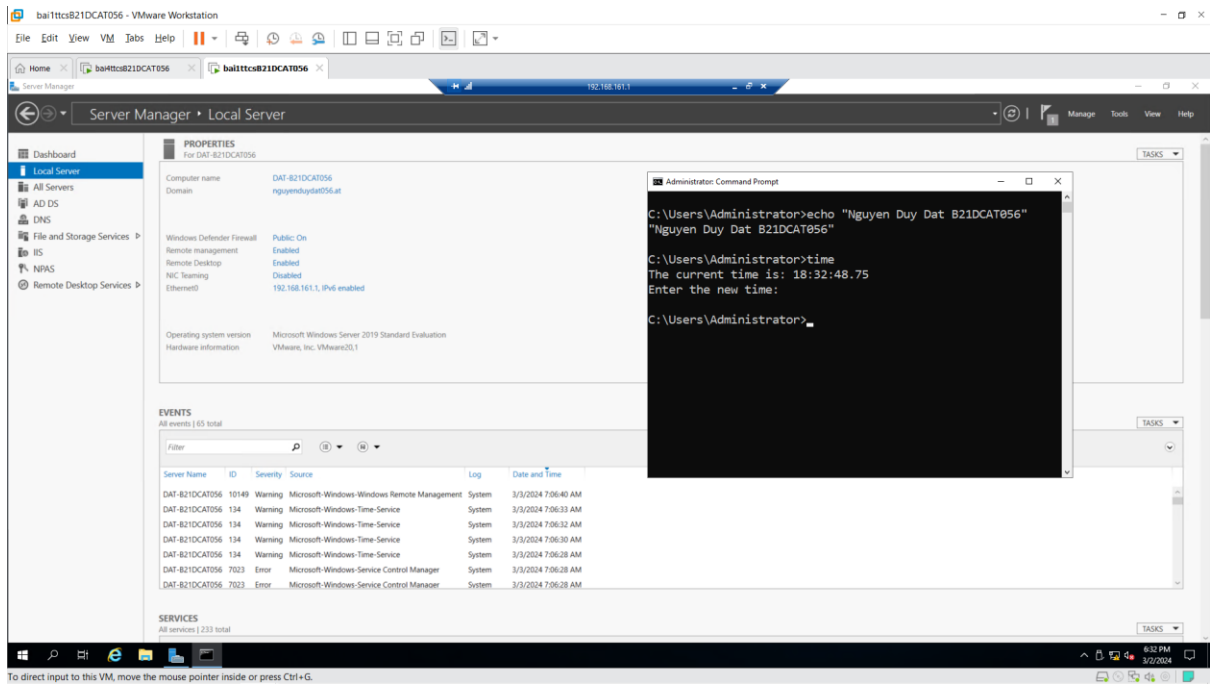
- Local Server : Remote Desktop đã enable



- Khởi động máy trạm Windows, bật phần mềm Remote Desktop Connection, nhập IP, tài khoản (administrator) và mật khẩu của máy Server.

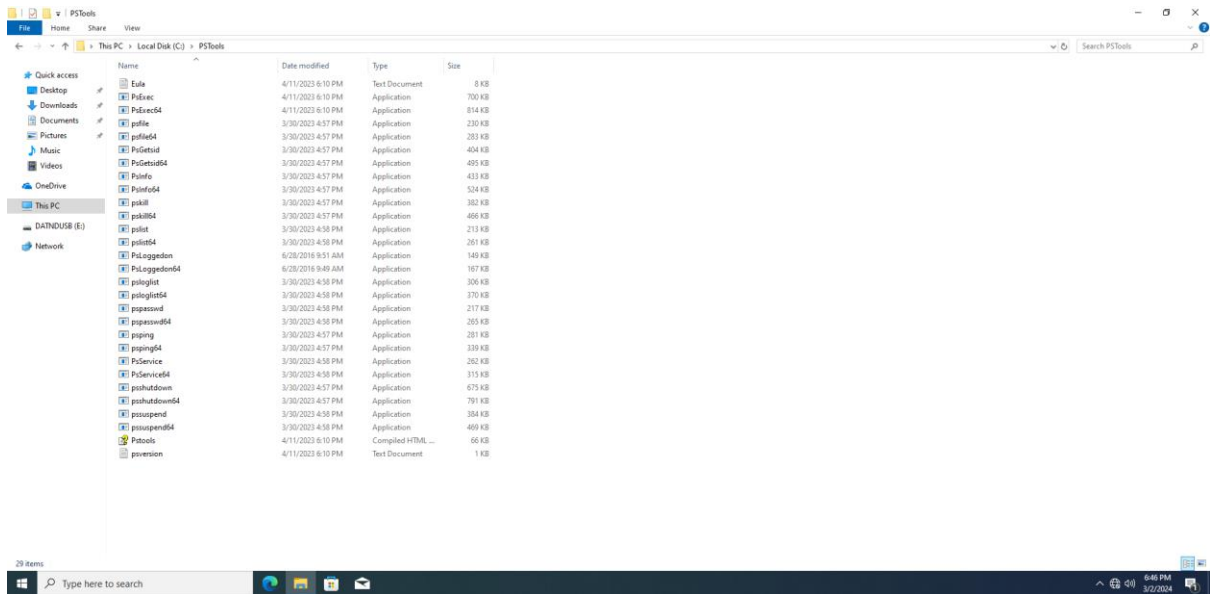


- Truy cập thành công vào máy Server

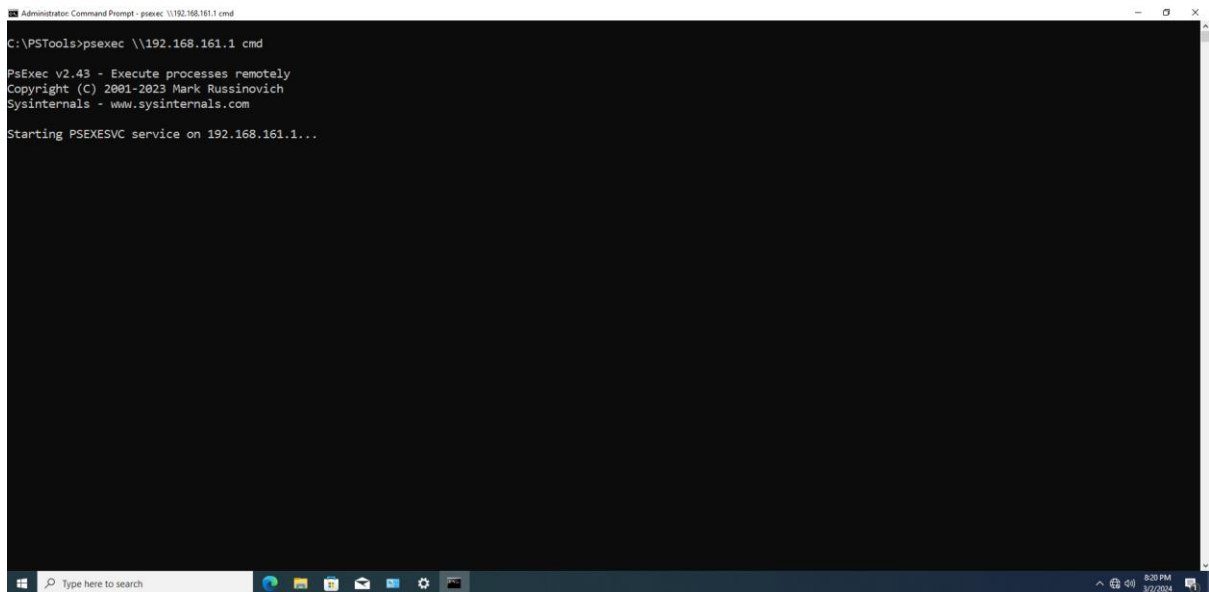


## 4. Cài đặt Pstool

- Tải công cụ PSTools. Giải nén trong máy trạm Windows

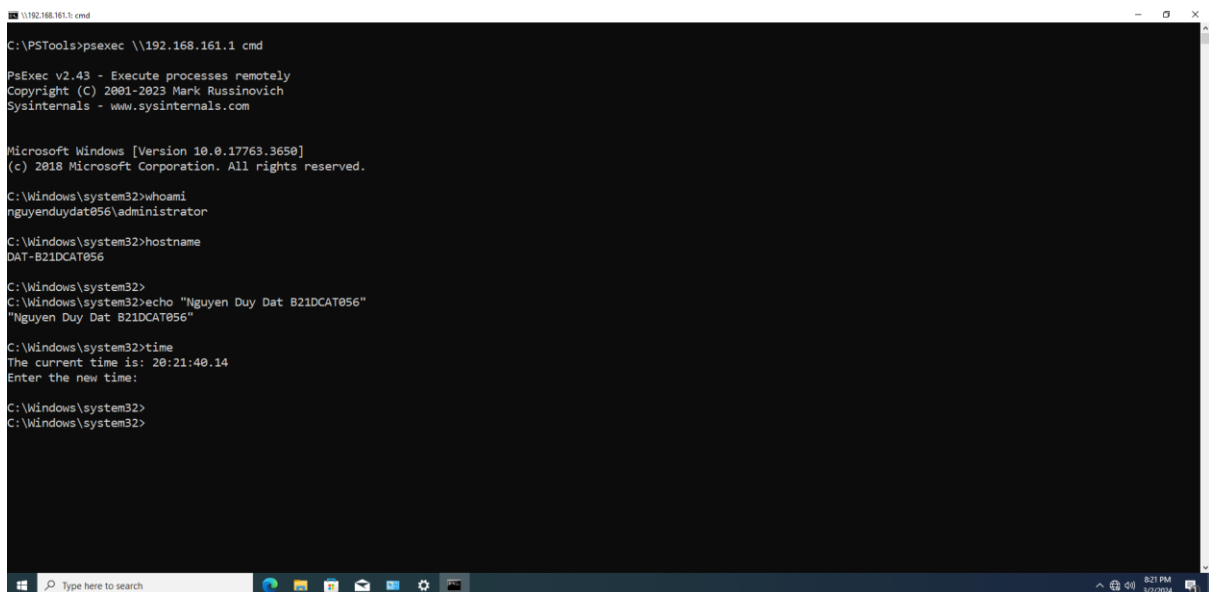


- Sử dụng công cụ PStools với cmd để kết nối tới máy Server theo lệnh: **psexec \\192.168.161.1 cmd**



```
Administrator: Command Prompt - psexec \\192.168.161.1 cmd
C:\PSTools>psexec \\192.168.161.1 cmd
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
Starting PSEXESVC service on 192.168.161.1...
```

- Kết nối thành công đến Server



```
\\192.168.161.1: cmd
C:\PSTools>psexec \\192.168.161.1 cmd
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
nguyenduydat056\administrator

C:\Windows\system32>hostname
DAT-B21DCAT056

C:\Windows\system32>
C:\Windows\system32>echo "Nguyen Duy Dat B21DCAT056"
"Nguyen Duy Dat B21DCAT056"

C:\Windows\system32>time
The current time is: 20:21:40.14
Enter the new time:

C:\Windows\system32>
C:\Windows\system32>
```