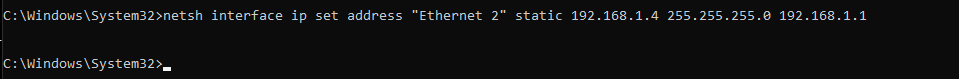
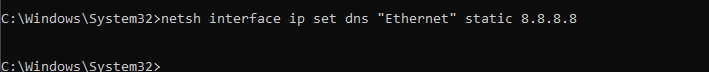
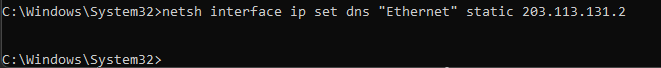
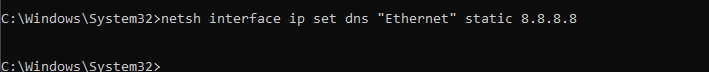
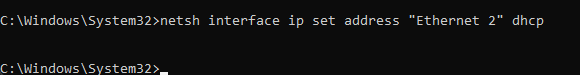
**CÂU HỎI ÔN TẬP QUẢN TRỊ MẠNG 2023**

1. **Tìm hiểu cài đặt IP cho máy tính server bằng lệnh Netsh**

+ DNS:



+DHCP:



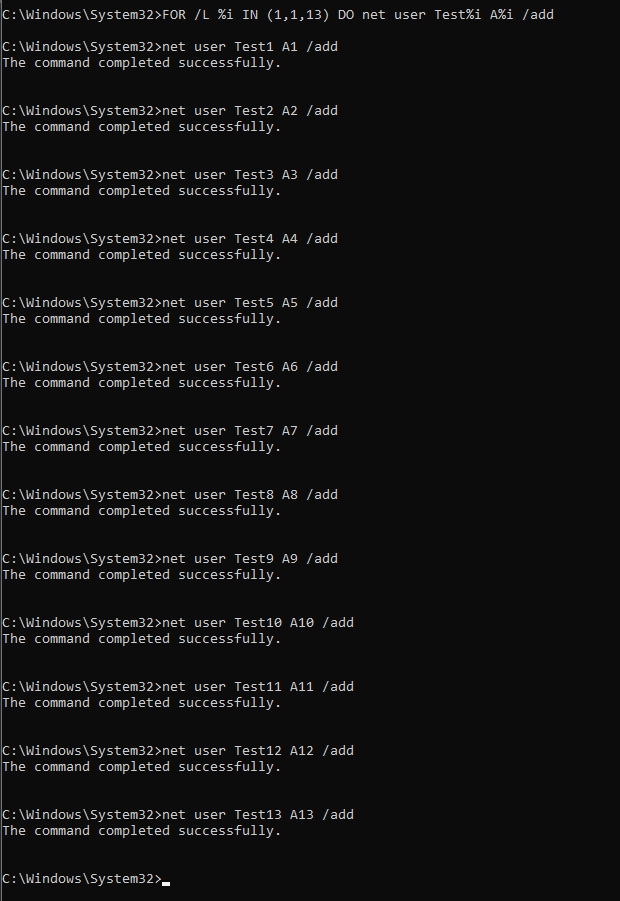
1. **Tạo user tên là Test với mật khẩu là A0 bằng lệnh net user**



1. **Cài đặt phần mềm Mremote và điều khiển Server 2019**
2. **Tạo các user trên Windows Server với thông tin sau:**

C1: net user Test01 A1 /add.

C2: FOR /L %i IN (1,1,13) tạo một vòng lặp từ 1 đến 13 với bước là 1. - %i là biến lặp được sử dụng để tạo tên người dùng và mật khẩu tương ứng. - net user Test%i A%i /add tạo người dùng với tên là "Test" theo giá trị của %i và mật khẩu là "A" theo giá trị của %i.



|  |  |
| --- | --- |
| **Username** | **Password** |
| Test01 | A1 |
| Test02 | A2 |
| Test03 | A3 |
| Test04 | A4 |
| Test05 | A5 |
| Test06 | A6 |
| Test07 | A7 |
| Test08 | A8 |
| Test09 | A9 |
| Test10 | A10 |
| Test11 | A11 |
| Test12 | A12 |
| Test13 | A13 |

1. **Tạo folder tên là DungChung sau đó tạo các folder con theo bảng sau:**

mkdir Test01

icacls "Test01" /grant "Test01:(OI)(CI)F"

mkdir Test02

icacls "Test02" /grant "Test02:(OI)(CI)F"

mkdir Test03

icacls "Test03" /grant "Test03:(OI)(CI)F"

mkdir Test04

icacls "Test04" /grant "Test04:(OI)(CI)F"

mkdir Test05

icacls "Test05" /grant "Test05:(OI)(CI)F"

mkdir Test06

icacls "Test06" /grant "Test06:(OI)(CI)F"

mkdir Test07

icacls "Test07" /grant "Test07:(OI)(CI)F"

mkdir Test08

icacls "Test08" /grant "Test08:(OI)(CI)F"

mkdir Test09

icacls "Test09" /grant "Test09:(OI)(CI)F"

mkdir Test10

icacls "Test10" /grant "Test10:(OI)(CI)F"

mkdir Test11

icacls "Test11" /grant "Test11:(OI)(CI)F"

mkdir Test12

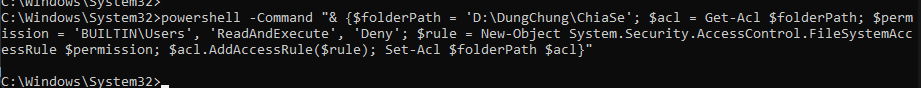
icacls "Test12" /grant "Test12:(OI)(CI)F"

mkdir Test13

icacls "Test13" /grant "Test13:(OI)(CI)F"

|  |  |
| --- | --- |
| **Username** | **Password** |
| D:\DungChung\Test01 | Phân quyền cho User Test01 |
| D:\DungChung\Test02 | Phân quyền cho User Test02 |
| D:\DungChung\Test03 | Phân quyền cho User Test03 |
| D:\DungChung\Test04 | Phân quyền cho User Test04 |
| D:\DungChung\Test05 | Phân quyền cho User Test05 |
| D:\DungChung\Test06 | Phân quyền cho User Test06 |
| D:\DungChung\Test07 | Phân quyền cho User Test07 |
| D:\DungChung\Test08 | Phân quyền cho User Test08 |
| D:\DungChung\Test09 | Phân quyền cho User Test09 |
| D:\DungChung\Test10 | Phân quyền cho User Test10 |
| D:\DungChung\Test11 | Phân quyền cho User Test11 |
| D:\DungChung\Test12 | Phân quyền cho User Test12 |
| D:\DungChung\Test13 | Phân quyền cho User Test13 |

1. **Đảm bảo user nào chỉ được truy cập duy nhất folder của user đó**



1. **Dùng Windows 10 truy cập vào Folder dùng chung để kiểm tra phân quyền.**

Tìm và nhấp đúp vào thư mục "DungChung" để mở.

Danh sách các thư mục con (Test01, Test02, ..., Test13) trong thư mục "DungChung". Nhấp đúp vào từng thư mục để mở chúng.

Để kiểm tra phân quyền của mỗi thư mục, bạn có thể nhấp chuột phải vào thư mục đó và chọn "Properties".

Trong cửa sổ Properties, chuyển sang tab "Security". Ở đây, bạn sẽ thấy danh sách các người dùng và nhóm người dùng có quyền truy cập vào thư mục đó.

Để xem chi tiết về quyền truy cập của mỗi người dùng, nhấp vào người dùng tương ứng và nhấn vào nút "Advanced". Trong cửa sổ Advanced Security Settings, bạn sẽ thấy danh sách các quyền được cấp cho người dùng đó.

1. **Tạo snapshot lưu trữ Windows 10, tìm hiểu local policy tắt Task Manager của Windows 10**
   * **Tìm hiểu local policy tắt services.msc của Windows 10**
   * **Tìm hiểu local policy tắt Control Pannel của Windows 10**
   * **Tìm hiểu local policy tắt Registry của Windows 10**
2. **Tìm hiểu lý thuyết về dịch vụ DHCP, HTTP, HTTPS, FTP (active/passive)**

DHCP (Giao thức Cấu hình Động Host):-Lý thuyết: -DHCP là một giao thức quản lý mạng được sử dụng để tự động cấp phát địa chỉ IP và thông tin cấu hình mạng khác cho các thiết bị trong mạng. Mục tiêu chính là đơn giản hóa quản lý địa chỉ IP trong một mạng.HTTP (Giao thức Truyền Tải Siêu Văn bản) - Lý thuyết:- HTTP là nền tảng của truyền thông dữ liệu trên World Wide Web. Đây là một giao thức tầng ứng dụng giúp truyền tải siêu văn bản giữa máy khách và máy chủ.

HTTPS (Giao thức Truyền Tải Siêu Văn bản An Toàn):-Lý thuyết: -HTTPS là phiên bản an toàn của HTTP sử dụng mã hóa để bảo vệ truyền tải dữ liệu giữa máy khách và máy chủ. Nó được sử dụng rộng rãi để truyền thông an toàn qua mạng máy tính, đặc biệt là trên internet. -Chế Độ Chủ Động:-Lý thuyết:-Trong chế độ chủ động của FTP, máy khách thiết lập cả hai kết nối điều khiển và dữ liệu. Máy chủ mở một cổng ngẫu nhiên để truyền dữ liệu và máy khách kết nối đến cổng này.

1. **Tìm hiểu cách mở rule Firewall để cho phép Windows 10 có thể ping tới Windows Server 2019 và ngược lại.**
2. **Tạo các user ở câu 13 bằng lệnh net user (sinh viên tìm hiểu thêm lệnh đổi password, thêm user vào group)**





1. **Sử dụng lệnh Netsh mức cơ bản**
   * **Xem IP của card mạng máy tính (netsh interface ipv4 show config)**
   * **Gán IP tĩnh card mạng máy tính (netsh interface ipv4 set address name="Wi-Fi" static 192.168.3.8 255.255.255.0 192.168.3.1)**
   * **Thiết lập DNS cho card mạng máy tính (netsh interface ipv4 set dns name="Wi-Fi" static 8.8.8.8)**
2. **Cú pháp sử dụng lệnh Net Use để map ổ đĩa ánh xạ mạng đã chia sẻ giữa các máy tính.**

net use [Ổ đĩa muốn ánh xạ] [\địa chỉ máy tính\thư mục chia sẻ] [mật khẩu] /user:[tên người dùng]

1. **Mục đích của port forwarding là gì ? DMZ là gì ?**

Mục đích chính của port forwarding là định tuyến các yêu cầu kết nối từ mạng bên ngoài tới các dịch vụ hay ứng dụng cụ thể trong mạng nội bộ.

DMZ là một khu vực đặc biệt trong mạng máy tính, được cô lập hoàn toàn hoặc một phần từ mạng nội bộ.

1. **VPN là gì ? Có mấy loại VPN? Có thể tạo VPN trên Windows 10 bằng cách nào ? Hiệu chỉnh Modem như thế nào để có thể kết nối VPN từ Internet?**

VPN (Virtual Private Network) là một công nghệ cho phép bạn tạo một kết nối mạng riêng tư và an toàn qua mạng công cộng, như Internet.

Có hai loại chính của VPN:

VPN Remote Access (Truy cập từ xa): Loại VPN này cho phép người dùng từ xa kết nối với mạng nội bộ của một tổ chức hoặc công ty từ bất kỳ đâu trên Internet. Điều này cho phép người dùng truy cập vào tài nguyên và dịch vụ trong mạng nội bộ như khi họ đang có mặt trực tiếp trong mạng đó.

VPN Site-to-Site (Từ trang web này đến trang web khác): Loại VPN này cho phép hai hoặc nhiều mạng nội bộ khác nhau kết nối với nhau thông qua Internet. Điều này cho phép các văn phòng hoặc chi nhánh của một tổ chức truy cập vào tài nguyên và dịch vụ của nhau một cách an toàn và bảo mật.

Để tạo VPN trên Windows 10, bạn có thể sử dụng tính năng VPN tích hợp của hệ điều hành. Dưới đây là cách tạo VPN trên Windows 10:

Mở "Settings" (Cài đặt) trên Windows 10.

Chọn mục "Network & Internet" (Mạng và Internet).

Trong thanh bên trái, chọn "VPN".

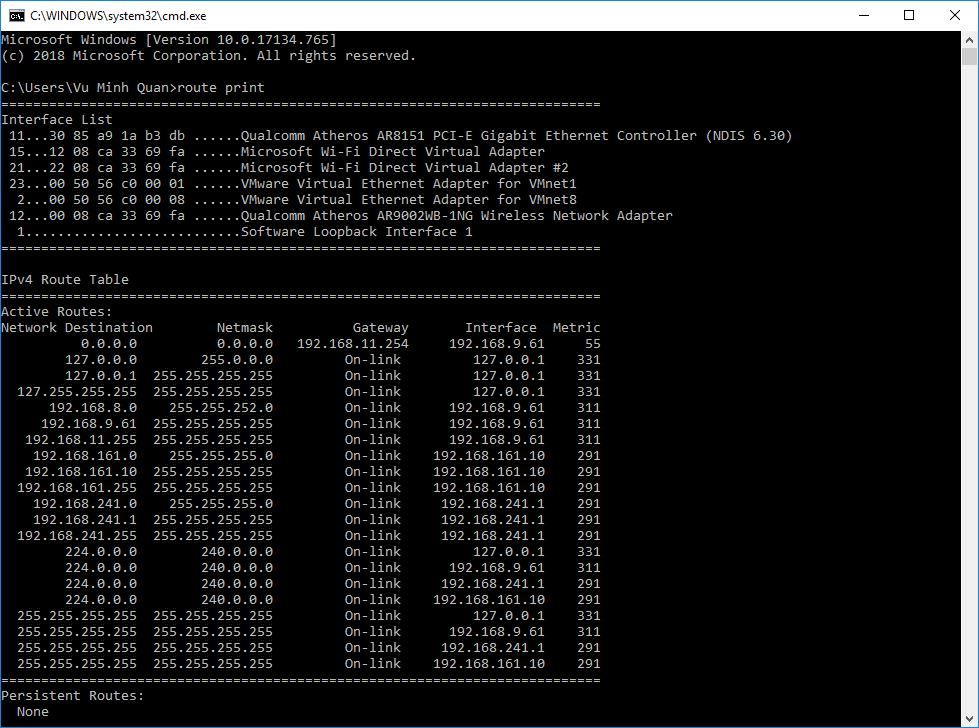
Bấm vào "Add a VPN connection" (Thêm một kết nối VPN).

Cung cấp các thông tin cần thiết cho kết nối VPN, bao gồm tên kết nối, địa chỉ máy chủ VPN và loại kết nối.

Sau khi cung cấp thông tin, bấm vào "Save" (Lưu) để tạo kết nối VPN.

Để hiệu chỉnh modem để kết nối VPN từ Internet bạn cần truy cập vào giao diện quản lý của modem bằng cách nhập địa chỉ IP của modem vào trình duyệt web. Sau khi truy cập giao diện quản lý modem, bạn cần tìm các tùy chọn liên quan đến VPN hoặc Port Forwarding. Bạn cần cấu hình modem để chuyển tiếp lưu lượng VPN đến địa chỉ IP của máy tính hoặc máy chủ VPN trong mạng nội bộ của bạn.

1. **Hãy cho biết nội dung của bảng sau là gì ? Muốn thêm một phần tử trong bảng này thì dùng lệnh nào?**

****

Bảng đưa ra kết quả của lệnh "route print" trong Command Prompt trên hệ điều hành Microsoft Windows (phiên bản 10.0.17134.765). Bảng này hiển thị thông tin về các giao diện mạng, bộ định tuyến và bảng định tuyến IPv4.

Để thêm một phần tử vào bảng định tuyến IPv4 trên hệ điều hành Windows, bạn có thể sử dụng lệnh "route add".

1. **Nêu các lỗi thường gặp khi thực hiện kết nối domain ( join domain) từ máy Windows 10 đến Windows Server 2019 không thành công?**

Lỗi không tìm thấy domain: Đây là lỗi phổ biến khi máy Windows 10 không thể tìm thấy domain trong mạng. Nguyên nhân có thể là do sai cấu hình DNS, lỗi kết nối mạng hoặc domain không tồn tại.

Lỗi không thể kết nối với domain controller: Lỗi này xảy ra khi máy Windows 10 không thể kết nối với domain controller trong domain. Nguyên nhân có thể là do lỗi kết nối mạng, domain controller không hoạt động hoặc không thể truy cập.

Lỗi xác thực: Khi thực hiện kết nối domain, có thể xảy ra lỗi xác thực khi máy Windows 10 không thể xác minh danh tính với domain controller. Lỗi này có thể do sai tên người dùng hoặc mật khẩu, chính sách xác thực không chính xác hoặc sự không phù hợp giữa phiên bản Windows của máy client và domain controller.

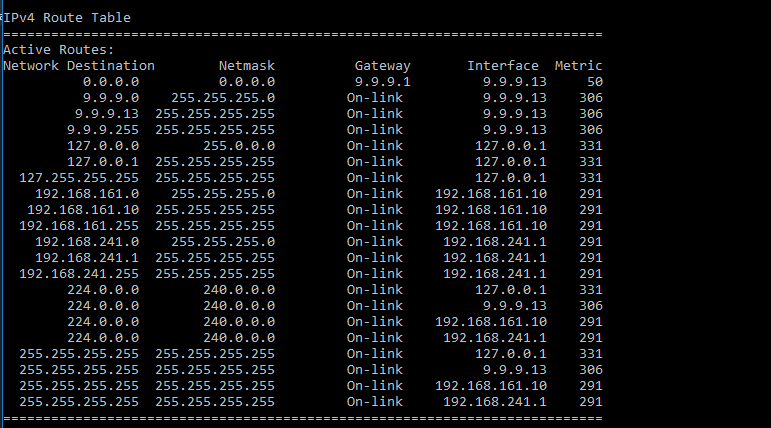
Lỗi quyền truy cập: Lỗi này xảy ra khi người dùng không có đủ quyền truy cập để thực hiện kết nối với domain. Nguyên nhân có thể là do quyền truy cập bị từ chối, tài khoản người dùng không thuộc nhóm người dùng được phép tham gia domain.

Lỗi thời gian đồng bộ: Khi máy client và domain controller có sự không đồng bộ về thời gian, có thể xảy ra lỗi kết nối domain. Điều này có thể được gây ra bởi cấu hình sai múi giờ hoặc không đồng bộ hóa thời gian với domain controller.

1. **Giải thích lệnh nslookup dùng để làm gì ? Lệnh nào cho phép xem bộ nhớ cache DNS của Windows Server 2019 ?**

Lệnh nslookup là một công cụ dòng lệnh được sử dụng để thực hiện truy vấn DNS. Nó cho phép người dùng kiểm tra và xem thông tin liên quan đến tên miền, địa chỉ IP và các bản ghi DNS khác.

Để xem bộ nhớ cache DNS của Windows Server 2019, bạn có thể sử dụng lệnh ipconfig /displaydns. Lệnh này hiển thị các bản ghi DNS đã được lưu trữ trong bộ nhớ cache của máy tính, bao gồm tên miền, địa chỉ IP và thời gian sống (TTL) của bản ghi.



1. **Hãy cho biết chức năng Routing and Remote Access của Windows Server 2019 dùng để làm gì ?**

Chức năng Routing and Remote Access của Windows Server 2019 được sử dụng để tạo các kết nối từ xa an toàn đến mạng nội bộ thông qua Internet. Điều này cung cấp quyền truy cập vào tất cả các tài nguyên mạng nội bộ, như tin nhắn, chia sẻ tệp và in ấn, và truy cập máy chủ web.

1. **Domain Controller, Active Directory là gì ? Những tính năng của Active Directory? Child Domain là gì?**

Domain Controller là một hệ thống máy chủ được thiết lập nhằm mục đích quản lý, kiểm tra domain.

Active Directory (AD) là một dịch vụ thư mục đã được Microsoft phát triển nên dành cho những mạng dùng Windows domain.

Những tính năng chính của Active Directory bao gồm:

• Cơ cấu tổ chức phân cấp.

• Xác thực Multimaster & Sao chép Multimaster.

• Khả năng truy cập và sửa đổi AD DS từ nhiều điểm quản trị.

• Một điểm truy cập duy nhất của tài nguyên mạng.

• Khả năng tạo mối quan hệ tin cậy với các mạng bên ngoài chạy các phiên bản trước đó của AD.

Child Domain là một domain con trực thuộc parents domain nằm trong cùng một forest.

1. **Cách thức cài đặt cấu hình một website trên IIS, cài đặt Wordpress trên IIS. Có thể cài đặt nhiều website trên cùng một port 80 trên IIS được không? Giải thích cách làm.**

Để cài đặt và cấu hình một website trên IIS, bạn có thể thực hiện theo các bước sau4:

1. Mở Internet Information Services (IIS) Manager.

2. Mở rộng thư mục máy tính của bạn bằng cách nhấp vào > ở bên trái của biểu tượng trong khung bên trái.

3. Nhấp chuột phải vào Các trang web và chọn Thêm trang web…

4. Đặt tên cho trang web và chỉ định đường dẫn vật lý đến thư mục chứa các tệp của trang web.

5. Đặt các tùy chọn ràng buộc như Kiểu (HTTP hoặc HTTPS), Địa chỉ IP, Hải cảng và Tên máy chủ.

6. Nhấn vào OK để hoàn thành việc tạo trang web mới.

Để cài đặt WordPress trên IIS, bạn có thể thực hiện theo các bước sau:

1. Đăng nhập vào máy chủ của bạn thông qua RDP.

2. Cài đặt IIS.

3. Mở IIS và tạo một trang web mới.

4. Tải xuống WordPress và giải nén vào thư mục của trang web mới.

5. Tạo cơ sở dữ liệu mới và người dùng quản lý cơ sở dữ liệu trong phpMyAdmin hoặc công cụ quản lý cơ sở dữ liệu tương tự.

6. Truy cập trang cài đặt WordPress thông qua trình duyệt và điền thông tin cơ sở dữ liệu và người dùng đã tạo.

7. Hoàn tất quá trình cài đặt WordPress.

Về việc cài đặt nhiều website trên cùng một port 80 trên IIS, điều này hoàn toàn khả thi910. Bạn có thể tạo nhiều website trên IIS và cấu hình chúng để sử dụng cùng một port (thông thường là port 80 cho HTTP và port 443 cho HTTPS) nhưng với các tên miền khác nhau. Khi một yêu cầu đến, IIS sẽ xác định website phù hợp dựa trên tên miền được sử dụng trong yêu cầu. Tuy nhiên, nếu bạn muốn chạy nhiều dịch vụ web server (như IIS và Apache) trên cùng một máy tính, bạn sẽ cần phải cấu hình chúng để sử dụng các port khác nhau.

1. **DHCP hoạt động thế nào ? Cách thức cấu hình DHCP trên Windows Server 2019?**

DHCP hoạt động theo các bước sau:

1. Máy tính yêu cầu địa chỉ IP từ DHCP Server.

2. DHCP Server gửi một địa chỉ IP còn trống đến máy tính.

3. Máy tính xác nhận địa chỉ IP vừa nhận được.

4. DHCP Server ghi lại thông tin về địa chỉ IP và máy tính đã sử dụng nó trong bảng quản lý.

5. Máy tính sử dụng địa chỉ IP để truy cập Internet hoặc mạng cục bộ.

Để cấu hình DHCP trên Windows Server 2019, bạn có thể thực hiện theo các bước sau:

1. Mở Server Manager -> Thông báo màu vàng -> Complete DHCP configuration.

2. Trên trang Post-Install configuration wizard nhấn chọn Next.

3. Nhấn chọn vào Authorization để đăng nhập thông tin đăng nhập AD nếu Server được kết nối với miền. Nhấn chọn Skip AD authorization nếu như DHCP Server hoạt động độc lập và không được kết nối với miền.

4. Cài đặt DHCP Server và cấu hình DHCP Server.

5. Đặt scope gồm các IP từ 10.10.10.140 đến 10.10.10.254.

6. Bật máy client và cấu hình IP động cho máy client.

7. Đợi Client nhận IP và kiểm tra. Client đã nhận IP được DHCP server cấp phát.

1. **DNS hoạt động thế nào ? Làm sao cài đặt và cấu hình dịch vụ DNS trên Windows Server ? Sinh viên cài đặt website có domain tên sinhvien.com trên dns và dùng Windows 10 client truy cập kiểm tra chức năng của DNS?**

DNS hoạt động theo cấu trúc phân cấp, bao gồm các loại server khác nhau như Root Name Server, TLD Name Server, Authoritative Name Server và DNS Recursor1. Khi bạn gõ một tên miền vào trình duyệt, DNS sẽ truy vấn các server này để tìm ra địa chỉ IP tương ứng của tên miền đó.

Để cài đặt và cấu hình dịch vụ DNS trên Windows Server, bạn cần thực hiện các bước sau:

• Gán IP tĩnh cho card mạng của máy server.

• Vào Server Manager, click chuột phải vào Role chọn Add Roles.

• Chọn Next và tích chọn DNS, sau đó chọn Next.

• Click Next và chọn Install để cài đặt DNS.

• Sau khi cài đặt xong, click Close để đóng màn hình cài đặt.

• Vào DNS Manager, click chuột phải vào máy chủ DNS và chọn New Zone.

• Chọn Zone Type là Primary Zone và chọn Next.

• Nhập tên miền của zone và chọn Next.

• Chọn Dynamic Update là None và chọn Next.

• Chọn Finish để hoàn tất tạo zone.

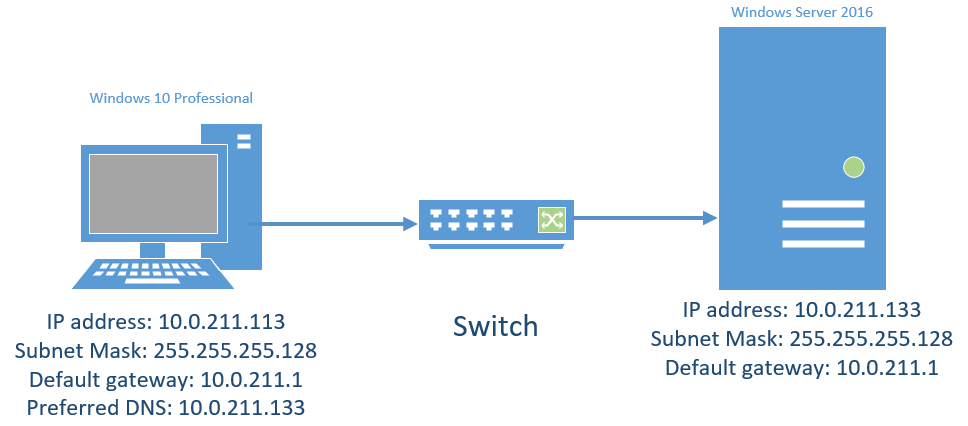
• Trong zone vừa tạo, click chuột phải và chọn New Host (A or AAAA).

• Nhập tên và địa chỉ IP của máy chủ và chọn Add Host.

• Lặp lại bước trên cho các máy chủ khác trong mạng LAN.

• Để kiểm tra dịch vụ DNS, bạn có thể sử dụng lệnh ping hoặc nslookup từ máy khách

1. **Trong hình dưới Windows 10 không thể join domain congty.com trên Windows Server 2016. Sinh viên hãy mô tả nguyên nhân của sự cố này. Biết rằng Windows 10 đã Sysprep, Server đã cài đặt DNS trỏ domain congty.com thành công.**

****

IP tĩnh của máy trạm không đúng với phạm vi mạng của domain. Bạn cần kiểm tra lại địa chỉ IP, subnet mask, gateway và DNS của máy trạm để đảm bảo chúng thuộc cùng mạng với domain controller.

• DNS server của domain controller không hoạt động hoặc không cấu hình đúng. Bạn cần kiểm tra lại dịch vụ DNS trên domain controller và đảm bảo rằng nó có thể phân giải được tên miền congty.com. Bạn cũng cần kiểm tra lại cài đặt Dynamic Update để cho phép các máy trạm cập nhật bản ghi DNS khi join domain.

• Máy trạm đã bị sysprep quá nhiều lần hoặc không được sysprep đúng cách. Bạn cần kiểm tra lại số lần sysprep của máy trạm và đảm bảo rằng nó không vượt quá giới hạn cho phép. Bạn cũng cần kiểm tra lại cách thức sysprep của máy trạm và đảm bảo rằng nó được thực hiện theo các bước hướng dẫn.

• Máy trạm đã bị cấm truy cập vào domain bởi chính sách bảo mật của domain controller. Bạn cần kiểm tra lại các chính sách bảo mật trên domain controller và đảm bảo rằng nó không có những quy định nào ngăn cản máy trạm join domain. Bạn cũng cần kiểm tra lại quyền của tài khoản được sử dụng để join domain và đảm bảo rằng nó có đủ quyền để thực hiện thao tác này

1. **Khi tạo user với mật khẩu là số 1, người quản trị gặp lỗi và không tạo thành công. Sinh viên hãy cho biết các lỗi có thể gặp của người quản trị này và trình bày giải pháp khắc phục ?**

Lỗi “Mật khẩu không đáp ứng yêu cầu bảo mật”. Đây là lỗi do mật khẩu quá đơn giản hoặc không đủ ký tự. Để khắc phục, bạn cần chọn một mật khẩu khác, có ít nhất 8 ký tự, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

• Lỗi “Tài khoản người dùng đã tồn tại”. Đây là lỗi do tên user đã được sử dụng bởi một tài khoản khác. Để khắc phục, bạn cần chọn một tên user khác, không trùng với bất kỳ tài khoản nào trên hệ thống.

• Lỗi “Bạn không có quyền tạo tài khoản người dùng”. Đây là lỗi do bạn đăng nhập bằng một tài khoản không có quyền quản trị. Để khắc phục, bạn cần đăng nhập bằng một tài khoản người quản trị hoặc yêu cầu người quản trị cấp quyền cho bạn.

1. **OU là gì ? Group là gì ? Có mấy loại group ? Tại sao sau khi tạo OU trên Active Directory User and Group của Windows 2019 không thể xóa được OU? Nếu muốn xóa thì phải chỉnh ở đâu?**

OU là viết tắt của Organizational Unit, là một đối tượng trong Active Directory. OU là nơi chứa các đối tượng khác như user, computer và group. OU có thể chứa các OU con để tạo cấu trúc phân cấp. OU được dùng để ủy quyền quản trị, áp dụng các chính sách và phân quyền cho các đối tượng bên trong.

Group là một đối tượng trong Active Directory, chứa các user hoặc group khác để tạo nhóm. Group được dùng để quản lý các user theo nhóm, cấp quyền truy cập vào các tài nguyên và phân phối email.

Có ba loại group trong Active Directory, là Domain Local Group, Global Group và Universal Group. Mỗi loại group có phạm vi và mục đích khác nhau:

• Domain Local Group: Chỉ có thể chứa các đối tượng trong cùng domain, và chỉ có thể cấp quyền truy cập cho các tài nguyên trong cùng domain.

• Global Group: Có thể chứa các đối tượng trong cùng domain, và có thể cấp quyền truy cập cho các tài nguyên trong cùng hoặc khác domain.

• Universal Group: Có thể chứa các đối tượng trong cùng hoặc khác domain, và có thể cấp quyền truy cập cho các tài nguyên trong cùng hoặc khác domain.

Tại sao sau khi tạo OU trên Active Directory User and Group của Windows 2019 không thể xóa được OU? Nếu muốn xóa thì phải chỉnh ở đâu?

Có thể bạn không thể xóa được OU vì OU có chứa các đối tượng quan trọng như user, computer hoặc group. Để xóa được OU, bạn cần chuyển các đối tượng này ra khỏi OU hoặc xóa chúng trước. Bạn cũng cần có quyền quản trị để xóa OU.

Nếu bạn muốn xóa OU, bạn cần làm như sau:

• Mở công cụ Active Directory Users and Computers.

• Tìm OU cần xóa trong cấu trúc cây bên trái.

• Click chuột phải vào OU và chọn Delete.

• Xác nhận việc xóa OU bằng cách nhấn Yes.

1. **Làm sao có thể cấm tất cả user trong domain controller không thể vào Regedit ? Hiệu chỉnh chức năng này ở đâu?**

Mở Group Policy Editor và đi tới User Configuration > Administrative Templates > System

• Sau đó bạn kích đúp vào Prevent access to registry editing tools.

• Chọn Enabled và nhấn Apply hoặc OK.

1. **Cho mô hình mạng Domain với địa chỉ IP 10.10.0.0/22 có thể tạo ra bao nhiêu mạng domain có số client Windows 10 là 50 client ?**

Địa chỉ IP 10.10.0.0/22 thuộc lớp A, có 22 bit làm network ID và 10 bit làm host ID. Do đó, số lượng mạng con có thể tạo ra là:

210 - 2 = 1022 mạng con

Số lượng host trên mỗi mạng con là:

210 - 2 = 1022 host

Nếu mỗi mạng domain có 50 client Windows 10, thì số lượng mạng domain có thể tạo ra là:

1022 / 50 = 20.44

Làm tròn xuống, ta được:

20 mạng domain

1. **Lệnh nào để thêm một User, Group, OU vào Active Directory**

Lệnh để thêm một User: dsadd user "cn=user\_name,ou=ou\_name,dc=domain\_name,dc=com" -pwd password

• Lệnh để thêm một Group: dsadd group "cn=group\_name,ou=ou\_name,dc=domain\_name,dc=com" -secgrp yes -scope global

• Lệnh để thêm một OU: dsadd ou "ou=ou\_name,dc=domain\_name,dc=com"

1. **Lệnh nào để thay đổi password của một user trong hệ thống Active Directory**

Sử dụng lệnh PowerShell: bạn mở sổ Command Promtp và nhập lệnh

net user \*username\* \*password\*

1. **Cách thức tạo và đổi mật khẩu của nhiều User từ File Excel**

Có thể sử dụng công cụ Active Directory User and Computers

Hoặc sử dụng lệnh Powershell : New-ADUser, Set-ADAccountPassword

1. **Python cơ bản:**
   * **Khai báo biến trong python ( int, str …)**

ten\_bien = gia\_tri ví dụ : a, b = 5, "Hello"

* + **Khai báo List trong python (thêm, xóa, sửa phần tử trong list)**

Để thêm list trong python ta có thể dùng: my\_list.insert

Để xóa ta có thể dùng : my\_list.remove

Sửa : my\_list

* + **Khai báo Dictionary trong python (thêm, xóa, sửa phần tử trong Dict)**

my\_dict

thêm: my\_dict[new\_key] = new\_value

xóa: del my\_dict

sửa: my\_dict['age']

* + **Cách thức đọc file txt của Python**

Để đọc một file text trong Python, bạn có thể sử dụng hàm open() để mở file và hàm read() để đọc nội dung của file

with open('ten\_file.txt', 'r') as

file:

noi\_dung = file.read()

* + **Cách thức đọc file csv của Python**
  + **Cách tách tên trong một chuỗi String cho trước, cách tách tên từ List và file csv**

Phương thức split()

input\_string = "apple,banana,orange"  
fruits = input\_string.split(",")  
print(fruits)

kết quả : [‘apple’, ‘banana’, ‘orange’]

* + **Sắp xếp một list tăng giảm**

new\_list = sorted

ví dụ:

my\_list = [4, 1, 3, 6, 2, 5]

sorted\_list = sorted(my\_list)

print(sorted\_list)

kết quả: [1, 2, 3, 4, 5, 6]

1. **Các bài tập python mà đã làm trong bài lab.**
2. **Viết chương trình python hiển thị tất cả folder trong thư muc** [**\\192.168.161.128\DungChung**](file:///\\192.168.161.128\DungChung) **(trong đó 192.168.161.128 là IP của server DC sinh viên đã cài đặt).**

Sử dụng thư viện OS trong python

import os

path = '\\\\192.168.161.128\\DungChung'

for folder\_name in os.listdir(path):

if os.path.isdir(os.path.join(path, folder\_name)):

print(f'Folder: {folder\_name}')

1. **Viết chương trình copy file từ một thư mục nguồn sang thư mục đích bằng python**

sử dụng thư viện shutil trong Python

import shutil

src\_file = '/path/to/source/file'

dst\_folder = '/path/to/destination/folder'

shutil.copy2(src\_file, dst\_folder)

import shutil

src\_folder = '/path/to/source/folder'

dst\_folder = '/path/to/destination/folder'

shutil.copytree(src\_folder, dst\_folder)

1. **Viết chương trình copy file txt từ thư mục của các user tới một thư mục đích.**

# import module

import os

source\_dir = "C:\\Users\\test"

dest\_dir = "D:\\backup"

file\_name = "Test.txt"

source\_file = os.path.join(source\_dir, file\_name)

dest\_file = os.path.join(dest\_dir, file\_name)

os.system(f"copy {source\_file} {dest\_file}")

print(f"File {file\_name} has been copied from {source\_dir} to {dest\_dir}.")

1. **Viết chương trình copy file txt từ thư mục của các user tới nhiều thư mục đích.**

import os

import shutil

src\_folder = '/path/to/source/folder'

dst\_folders = ['/path/to/destination/folder1', '/path/to/destination/folder2', ...]

for dst\_folder in dst\_folders:

os.makedirs(dst\_folder, exist\_ok=True)

for file\_name in os.listdir(src\_folder):

if file\_name.endswith('.txt'):

src\_file = os.path.join(src\_folder, file\_name)

dst\_file = os.path.join(dst\_folder, file\_name)

shutil.copy2(src\_file, dst\_file)

1. **Viết chương trình thêm một User vào Active Directory bằng Python**

import os

user\_name = "testuser"

user\_password = "test123"

user\_cmd = "net user " +

user\_name + " " + user\_password + " /add"

os.system(user\_cmd)

print("User " + user\_name + " has been added to active directory.")

1. **Viết chương trình đổi Password của nhiều User trong Active Directory bằng Python**

# Import pyad module

import pyad

# Define the domain name and the admin credentials

domain\_name = "example.com"

admin\_user = "admin"

admin\_password = "password"

1. **Viết chương trình python cho phép ánh xạ ổ địa** [**\\IP-Server\DungChung**](file:///\\IP-Server\DungChung) **cho tất cả nhân viên của congty.com**

import subprocess

# Địa chỉ IP của máy chủ và tên thư mục được chia sẻ

server\_ip = "192.168.1.100"

shared\_folder = "DungChung"

# Hàm ánh xạ thư mục mạng

def map\_network\_drive(username, password):

# Sử dụng lệnh subprocess để thực hiện ánh xạ

subprocess.run(["net", "use", f"\\\\{server\_ip}\\{shared\_folder}", f"/user:{username}", f"{password}", "/persistent:yes"])

# Duyệt qua danh sách nhân viên trong công ty congty.com

employees = ["employee1", "employee2", "employee3"]

for employee in employees:

# Gọi hàm ánh xạ thư mục cho mỗi nhân viên trong công ty

map\_network\_drive(employee, "password") # Thay "password" bằng mật khẩu của từng nhân viên

1. **Viết chương trình tìm và xóa một file theo tên của file đó**

import os

def delete\_file\_by\_name(file\_name):

# Kiểm tra xem file có tồn tại không

if os.path.exists(file\_name):

# Xóa file nếu tồn tại

os.remove(file\_name)

print(f"Đã xóa file {file\_name}")

else:

print(f"Không tìm thấy file {file\_name}")

# Thay tên file bạn muốn xóa vào đây

file\_to\_delete = "ten\_file\_can\_xoa.txt"

delete\_file\_by\_name(file\_to\_delete)

Giải thích code:

os.path.exists(file\_name): Hàm này kiểm tra xem file có tồn tại không.

os.remove(file\_name): Nếu file tồn tại, hàm này sẽ xóa file đó.

print(): Dùng để thông báo kết quả, có xóa file hay không.

1. **Tham số nào của lệnh tạo user cho phép hiệu chỉnh user đó sau khi đăng nhập lần đầu phải đổi password.**

sudo: Là quyền quản trị để chạy lệnh với quyền hạn cao.

useradd: Là lệnh để tạo người dùng mới.

-e 2023-12-31: Là tùy chọn để đặt ngày hết hạn tài khoản, trong đó 2023-12-31 là ngày hết hạn.

import subprocess

def create\_user\_with\_password\_change(username):

command = f"sudo useradd -e 2023-12-31 {username}"

subprocess.run(command, shell=True)

# Thực hiện tạo người dùng với yêu cầu thay đổi mật khẩu khi đăng nhập lần đầu

new\_username = "newuser"

create\_user\_with\_password\_change(new\_username)

1. **Để cài đặt VPN cho Windows Server 2019 phải dùng chức năng nào ? Muốn user có thể kết nối VPN thì phải chỉnh ở đâu ?**

Để cài đặt VPN trên Windows Server 2019, bạn có thể sử dụng tính năng "Remote Access" hoặc "Routing and Remote Access Services (RRAS)".

Cài đặt VPN trên Windows Server 2019:

Remote Access Role:

Bạn có thể cài đặt tính năng "Remote Access" thông qua Server Manager.

Mở Server Manager -> Chọn Add roles and features -> Chọn Remote Access để cài đặt.

Routing and Remote Access Services (RRAS):

Đây là một dịch vụ có sẵn trong Windows Server cho phép cấu hình VPN.

Mở Server Manager -> Tools -> Routing and Remote Access -> Theo hướng dẫn để cấu hình VPN.

Cho phép người dùng kết nối VPN:

Khi đã cài đặt VPN, để cho phép người dùng kết nối vào VPN trên Windows Server 2019, bạn cần:

Tạo người dùng VPN:

Mở "Computer Management" -> Users -> Tạo một người dùng mới hoặc chỉnh sửa người dùng hiện có.

Chắc chắn rằng người dùng đó được phép kết nối từ xa.

Cấu hình quyền truy cập VPN:

Trong Remote Access Management Console hoặc Routing and Remote Access, bạn có thể cấu hình quyền truy cập VPN cho từng người dùng.

Xác định quyền truy cập cho người dùng cụ thể thông qua các chính sách và phân quyền truy cập.

Cấu hình cổng và giao thức VPN:

Đảm bảo rằng cổng và giao thức được cấu hình đúng, ví dụ như PPTP, L2TP/IPsec, SSTP, hoặc OpenVPN.

Khi đã cấu hình xong, người dùng sẽ có thể kết nối vào VPN từ máy tính của họ bằng cách sử dụng thông tin đăng nhập được cấp từ máy chủ VPN Windows Server 2019.

1. **Profile của User có những kiểu nào ? Hãy giải thích chức năng của từng kiểu profile ?**

Trong hệ điều hành Windows, có ba loại chính của profile người dùng: local profiles, roaming profiles, và mandatory profiles.

Local Profiles:

Chức năng: Là profile lưu trữ trên máy tính cục bộ.

Hoạt động: Khi người dùng đăng nhập lần đầu tiên vào một máy tính, một local profile sẽ được tạo cho họ trên máy đó. Tất cả các thay đổi và tùy chỉnh (như hình nền, thiết lập ứng dụng) chỉ áp dụng cho máy tính đó cụ thể.

Roaming Profiles:

Chức năng: Cho phép người dùng truy cập profile của họ từ bất kỳ máy tính nào trong mạng.

Hoạt động: Khi người dùng đăng nhập vào một máy tính khác, profile của họ sẽ được đồng bộ từ máy chủ. Tất cả các thay đổi sẽ được lưu trữ và áp dụng khi họ đăng nhập vào bất kỳ máy tính nào trong mạng.

Mandatory Profiles:

Chức năng: Là một phiên bản "bắt buộc" của profile, không cho phép thay đổi.

Hoạt động: Mandatory profiles không lưu trữ các thay đổi được thực hiện bởi người dùng. Bất kỳ thay đổi nào cũng sẽ bị loại bỏ khi người dùng đăng xuất. Điều này thường được sử dụng trong môi trường nơi quản trị viên muốn đảm bảo rằng mọi người dùng đều có cùng một cấu hình và tùy chỉnh cố định.

Các loại profile này đều có mục tiêu khác nhau trong việc quản lý người dùng và cung cấp linh hoạt cho việc di chuyển giữa các máy tính trong mạng. Profiles cũng quyết định cách mà dữ liệu và cài đặt cá nhân được lưu trữ và sử dụng trên hệ thống Windows.

1. **Để giới hạn người dùng không được copy file quá 100MB lên ổ đĩa D: của máy tính, quản trị mạng phải cấu hình chức năng nào? Có thể cấm không cho phép người dùng chép file exe lên ổ đĩa D được không?**

Để giới hạn kích thước file được copy lên ổ đĩa D và cấm người dùng chép file exe lên đó, bạn có thể sử dụng các chức năng như Group Policy và Quotas trên hệ điều hành Windows.

Sử dụng Disk Quotas:

Chức năng: Cho phép bạn giới hạn không gian disk được sử dụng hoặc kích thước file cho từng người dùng hoặc nhóm người dùng.

Cách thức áp dụng:

Mở "Computer Management" -> "Disk Management".

Chuột phải vào ổ đĩa D: -> Chọn "Properties" -> Chuyển sang tab "Quota" -> Chọn "Enable quota management".

Bạn có thể cấu hình giới hạn kích thước tối đa cho mỗi người dùng hoặc nhóm người dùng ở đây.

Group Policy:

Chức năng: Cho phép bạn tùy chỉnh cấu hình hệ thống Windows.

Cấm người dùng chép file exe:

Mở "Local Group Policy Editor" bằng cách gõ "gpedit.msc" trong Run.

Đi đến "User Configuration" -> "Administrative Templates" -> "System" -> "Don't run specified Windows applications".

Thêm tên của các file exe mà bạn muốn cấm chạy vào danh sách.

Lưu ý rằng việc cấm người dùng chép file exe có thể gây ảnh hưởng đến các chương trình cần thiết để hoạt động, vì vậy hãy cân nhắc trước khi thực hiện. Đồng thời, sử dụng Disk Quotas để giới hạn dung lượng cho mỗi người dùng trên ổ đĩa D có thể giúp kiểm soát lưu lượng dữ liệu được lưu trữ.

Top of Form

1. **DFS trên Windows Server là chức năng gì ?**

DFS (Distributed File System) trên Windows Server là một tính năng cho phép tổ chức và quản lý các tập tin và thư mục trên mạng một cách hiệu quả. Đây là một công nghệ giúp kết hợp các tài nguyên từ nhiều máy chủ khác nhau thành một không gian lưu trữ duy nhất và có thể truy cập từ nhiều địa điểm khác nhau trên mạng.

DFS cung cấp hai dạng chính:

DFS Namespace: Đây là khái niệm giúp tổ chức các tài nguyên (thư mục, ổ đĩa) thành một không gian tên duy nhất và logic. Thay vì sử dụng đường dẫn thực tế đến từng máy chủ, người dùng có thể truy cập các tài nguyên này thông qua một đường dẫn duy nhất và thân thiện hơn.

DFS Replication: Là khả năng sao chép và đồng bộ hóa dữ liệu giữa các máy chủ DFS. Nó cho phép sao chép dữ liệu từ máy chủ nguồn đến máy chủ đích để đảm bảo dữ liệu luôn có sẵn và được đồng bộ hóa trên nhiều máy chủ.

Ưu điểm của DFS bao gồm khả năng cung cấp tính sẵn có và độ tin cậy cao, giúp tăng cường hiệu suất và khả năng mở rộng hệ thống lưu trữ trong môi trường doanh nghiệp. Nó cũng giúp người dùng truy cập tài nguyên mạng một cách dễ dàng và linh hoạt hơn.

1. **Loadbalancing là gì ? Cách thức cấu hình Server 2019 có chức năng LoadBallancing**

Load balancing là quá trình phân phối công việc và tải đều các tài nguyên của hệ thống (như các yêu cầu mạng, công việc xử lý) đến các máy chủ hoặc các thành phần hạ tầng mạng khác để tối ưu hiệu suất, tăng cường sẵn sàng và tránh quá tải tại một điểm.

Trong Windows Server 2019, bạn có thể sử dụng tính năng Network Load Balancing (NLB) để cấu hình load balancing cho các dịch vụ và ứng dụng. NLB cho phép bạn chia sẻ tải làm việc giữa nhiều máy chủ trong một cụm để cải thiện khả năng kháng cự lỗi và tăng cường hiệu suất.

Cách cấu hình Network Load Balancing trên Server 2019:

Cài đặt tính năng NLB:

Mở Server Manager -> Chọn "Add roles and features".

Chọn "Network Load Balancing" trong danh sách tính năng cần cài đặt.

Tạo cụm NLB:

Sau khi cài đặt xong, mở NLB Manager từ Tools hoặc tìm kiếm.

Chuột phải vào "Network Load Balancing Clusters" -> Chọn "New Cluster".

Thực hiện định cấu hình cụm NLB: chọn các card mạng, cấu hình IP, cổng và thuật toán cân bằng tải (như Round Robin, Least Connections).

Thêm máy chủ vào cụm NLB:

Chuột phải vào cụm vừa tạo -> Chọn "Add Host to Cluster".

Nhập địa chỉ IP của máy chủ và cấu hình các thiết lập khác nếu cần.

Kiểm tra và kiểm soát:

Kiểm tra trạng thái của cụm NLB, các máy chủ, và việc phân phối tải bằng cách sử dụng NLB Manager.

Khi hoàn thành, NLB sẽ phân phối các yêu cầu mạng đến các máy chủ trong cụm một cách cân đối, giúp tối ưu hiệu suất và tăng tính sẵn sàng của hệ thống.

1. **Tìm hiểu các dịch vụ Cloud hiện nay**

Hiện nay, có nhiều dịch vụ Cloud lớn cung cấp các giải pháp cho lưu trữ dữ liệu, tính toán, quản lý cơ sở hạ tầng, AI, IoT, và nhiều ứng dụng khác. Dưới đây là một số dịch vụ Cloud phổ biến:

1. Amazon Web Services (AWS):

Là một trong những nhà cung cấp dịch vụ Cloud lớn nhất và đa dạng nhất trên thị trường.

Cung cấp hầu hết các loại dịch vụ từ lưu trữ, tính toán, cơ sở dữ liệu, AI, IoT đến machine learning và nhiều dịch vụ khác.

2. Microsoft Azure:

Dịch vụ Cloud của Microsoft với nhiều tính năng và dịch vụ tương tự như AWS.

Cung cấp các giải pháp cho lưu trữ, tính toán, IoT, AI, DevOps, và cả dịch vụ quản lý hạ tầng như Virtual Machines, Kubernetes.

3. Google Cloud Platform (GCP):

Dịch vụ Cloud của Google với hệ thống cơ sở hạ tầng mạnh mẽ và tính linh hoạt.

Bao gồm lưu trữ, tính toán, machine learning, dịch vụ IoT và nhiều công cụ phát triển ứng dụng.

4. IBM Cloud:

Cung cấp các dịch vụ tính toán đám mây, lưu trữ, dịch vụ dành cho doanh nghiệp và công nghệ mới như AI, blockchain.

5. Alibaba Cloud:

Là một trong những nhà cung cấp dịch vụ Cloud hàng đầu tại châu Á.

Cung cấp lưu trữ, tính toán, AI, IoT và dịch vụ phát triển ứng dụng.

6. Oracle Cloud:

Chuyên về các dịch vụ Cloud dành cho doanh nghiệp, bao gồm lưu trữ, cơ sở dữ liệu, tính toán, và các ứng dụng doanh nghiệp.

7. DigitalOcean:

Tập trung vào các dịch vụ đơn giản, linh hoạt và dễ sử dụng cho các nhà phát triển, bao gồm máy chủ ảo, lưu trữ dữ liệu, và các dịch vụ phát triển ứng dụng.

Mỗi dịch vụ Cloud có các điểm mạnh riêng, phù hợp với nhu cầu và yêu cầu cụ thể của từng doanh nghiệp hoặc người dùng. Điều này tạo ra sự cạnh tranh sôi động giữa các nhà cung cấp và cung cấp nhiều lựa chọn cho người dùng.

1. **Tìm hiểu HyperV và Vmware Sphere các phần mềm này dùng làm gì ?**

Hyper-V và VMware vSphere đều là các nền tảng ảo hóa dùng để tạo và quản lý các máy ảo trên các máy chủ vật lý. Chúng đều có chức năng tương tự nhưng là của hai nhà cung cấp khác nhau.

Hyper-V (Microsoft):

Chức năng: Là một công nghệ ảo hóa tích hợp trong hệ điều hành Windows Server.

Sử dụng để: Tạo và quản lý máy ảo trên một máy chủ vật lý, cho phép chạy nhiều hệ điều hành và ứng dụng trên cùng một máy chủ.

Đặc điểm nổi bật: Cung cấp khả năng ảo hóa, cơ chế quản lý linh hoạt, tích hợp sâu trong hệ thống Windows.

VMware vSphere:

Chức năng: Là một nền tảng ảo hóa của VMware, cung cấp công cụ để tạo và quản lý môi trường ảo hóa trên nhiều máy chủ vật lý.

Sử dụng để: Tạo và quản lý các máy ảo, cung cấp các tính năng như di chuyển máy ảo, sao lưu, khôi phục, quản lý tài nguyên.

Đặc điểm nổi bật: Có khả năng mở rộng tốt, quản lý linh hoạt tài nguyên ảo hóa, hỗ trợ nhiều tính năng mạnh mẽ cho quản lý và bảo mật.

Cả Hyper-V và VMware vSphere đều cho phép bạn tạo, chạy và quản lý các máy ảo, cung cấp khả năng tận dụng tốt tài nguyên phần cứng, tăng tính linh hoạt và hiệu quả trong quản lý hạ tầng máy chủ. Sự lựa chọn giữa hai nền tảng thường phụ thuộc vào yêu cầu cụ thể của từng tổ chức, chi phí, tính năng và sự tương thích với môi trường hệ thống hiện tại.

1. **Hosting là gì ? Domain là gì ? VPS là gì ? Làm sao mua được một hosting, VPS, Domain?**

-Hosting là dịch vụ cung cấp không gian lưu trữ và tài nguyên trên máy chủ để lưu trữ các trang web và ứng dụng web. Khi bạn mua hosting, bạn thuê một phần của máy chủ để đặt dữ liệu của mình và chia sẻ tài nguyên của máy chủ đó với các người dùng khác.

- Domain (tên miền) là địa chỉ web duy nhất được sử dụng để truy cập một trang web.

- VPS (Virtual Private Server) là một dạng hosting được tạo ra bằng cách chia nhỏ một máy chủ vật lý thành nhiều máy chủ ảo độc lập. Mỗi VPS có tài nguyên và hệ điều hành riêng biệt, giống như bạn có một máy chủ riêng trong một môi trường ảo. VPS thường cung cấp tính linh hoạt cao và kiểm soát đối với hệ thống và cấu hình.

- Để mua hosting, VPS và domain, bạn có thể thực hiện các bước sau:

Chọn nhà cung cấp dịch vụ: Có nhiều nhà cung cấp trên thị trường như Bluehost, SiteGround, HostGator cho hosting; DigitalOcean, Linode, AWS cho VPS; và các công ty như Namecheap, GoDaddy cho domain.

Chọn gói dịch vụ phù hợp: Mỗi nhà cung cấp có nhiều gói dịch vụ khác nhau với các tính năng và tài nguyên khác nhau. Chọn gói dịch vụ phù hợp với nhu cầu của bạn.

Đăng ký tài khoản: Điền thông tin cần thiết và đăng ký tài khoản trên trang web của nhà cung cấp dịch vụ.

Chọn tên miền (nếu cần): Nếu bạn mua hosting, thường sẽ được cung cấp một tên miền miễn phí. Nếu chỉ mua domain, chọn tên miền mong muốn và kiểm tra tính khả dụng.

Thanh toán: Chọn phương thức thanh toán và hoàn tất quá trình thanh toán.

Cài đặt và quản lý dịch vụ: Sau khi thanh toán thành công, bạn sẽ nhận được thông tin đăng nhập và hướng dẫn để quản lý dịch vụ của mình.

1. **Cách thức chia sẻ File giữa Windows và Linux Centos**

1. Sử dụng Samba (Windows đóng vai trò Server, Linux làm Client):

Cài đặt Samba trên Linux CentOS:

sudo yum install samba samba-client

Cấu hình và khởi động dịch vụ Samba:

Sửa file cấu hình /etc/samba/smb.conf để định nghĩa các thư mục chia sẻ và quyền truy cập.

Khởi động dịch vụ Samba:

sudo systemctl start smb

Chia sẻ thư mục trong Samba:

Sử dụng lệnh smbpasswd để tạo mật khẩu cho người dùng Samba.

sudo smbpasswd -a your\_username

Truy cập từ Windows:

Trên Windows Explorer, nhập \\your\_linux\_ip và đăng nhập với tên người dùng và mật khẩu Samba.

2. Sử dụng SSH (Linux đóng vai trò Server, Windows làm Client):

Cài đặt SSH trên Linux CentOS:

sudo yum install openssh-server

Khởi động và kích hoạt dịch vụ SSH:

sudo systemctl start sshd

sudo systemctl enable sshd

Truy cập từ Windows:

Sử dụng một công cụ SCP hoặc SFTP như WinSCP hoặc FileZilla để kết nối và truy cập thư mục trên Linux.

3. Sử dụng NFS (Network File System):

Cài đặt NFS Server trên Linux CentOS:

sudo yum install nfs-utils

Cấu hình và khởi động dịch vụ NFS:

Sửa file /etc/exports để định nghĩa các thư mục chia sẻ.

Khởi động dịch vụ NFS:

sudo systemctl start nfs

Truy cập từ Windows:

Trên Windows, sử dụng tính năng "Map Network Drive" và nhập địa chỉ NFS.

1. **Làm sao có thể dùng User trên DC (domain controller) đăng nhập Centos**

1. Cài đặt và Cấu Hình SSSD:

Cài đặt Gói SSSD:

sudo yum install sssd sssd-tools sssd-client

Cấu hình File /etc/sssd/sssd.conf:

Sửa file cấu hình SSSD để đồng bộ hóa thông tin người dùng từ Active Directory hoặc LDAP.

sudo nano /etc/sssd/sssd.conf

Phân quyền Cho File Cấu Hình:

sudo chmod 600 /etc/sssd/sssd.conf

sudo chown root:root /etc/sssd/sssd.conf

Khởi động và Kích Hoạt Dịch Vụ SSSD:

sudo systemctl start sssd

sudo systemctl enable sssd

2. Cấu Hình PAM (Pluggable Authentication Modules):

Sửa File /etc/pam.d/system-auth:

sudo nano /etc/pam.d/system-auth

Thêm dòng sau ở đầu file:

auth required pam\_sss.so

account required pam\_sss.so

password required pam\_sss.so

session required pam\_sss.so

3. Kiểm Tra và Đảm Bảo:

Kiểm Tra Trạng Thái SSSD:

sudo systemctl status sssd

Kiểm Tra Đăng Nhập:

Sử dụng lệnh id để kiểm tra xem user từ AD có thể được đồng bộ hóa không.

id your\_ad\_username

Kiểm Tra Đăng Nhập SSH:

Sử dụng SSH để kiểm tra đăng nhập từ một tài khoản AD.

ssh your\_ad\_username@centos\_server\_ip

1. **Remote App là gì? Cách thức cài đặt và cấu hình Remote App.**

- RemoteApp là một tính năng trong hệ điều hành Windows Server, cho phép bạn triển khai ứng dụng Windows từ máy chủ xuống các máy tính client mà không cần cài đặt ứng dụng trên máy tính client đó. Điều này giúp đơn giản hóa quản lý ứng dụng, giảm bớt gánh nặng của việc duy trì và cập nhật ứng dụng trên nhiều máy tính.

- Cách thức cài đặt và cấu hình RemoteApp trên Windows Server:

Bước 1: Cài đặt Remote Desktop Services (RDS)

Mở Server Manager trên máy chủ Windows Server.

Chọn "Manage" -> "Add Roles and Features".

Chọn "Remote Desktop Services Installation".

Chọn "Next" và theo dõi các bước trong wizard để cài đặt Remote Desktop Services.

Bước 2: Cấu hình RemoteApp

Mở Server Manager và chọn "Remote Desktop Services" từ danh sách.

Bên trái, chọn "Collections" và tạo một mới nếu chưa có.

Chọn "RemoteApp Programs" và thêm ứng dụng bạn muốn triển khai.

Chọn "RD Web Access" để cấu hình trang web truy cập từ xa.

Bước 3: Cấu hình Remote Desktop Gateway (tùy chọn)

Nếu bạn muốn cung cấp quyền truy cập từ xa thông qua Internet, bạn có thể cài đặt và cấu hình Remote Desktop Gateway:

Trong Server Manager, chọn "Remote Desktop Services" -> "Overview".

Trong bảng "Deployment Overview", chọn "Configure RD Gateway".

Theo dõi wizard để cấu hình RD Gateway.

Bước 4: Truy cập RemoteApp từ máy tính client

Mở trình duyệt web và truy cập địa chỉ của trang RD Web Access (ví dụ: https://yourserver/rdweb).

Đăng nhập với tài khoản có quyền truy cập RemoteApp.

Chọn ứng dụng bạn muốn sử dụng và chờ cho ứng dụng được triển khai.

1. **Cách thức cài đặt Webstie ASP.net trên IIS, có thể cài đặt nopcommerce trên IIS được không ? Nếu được thì cách thức cài đặt như thế nào ?**

Cài đặt một trang web ASP.NET trên IIS:

Để cài đặt một trang web ASP.NET trên IIS, bạn có thể tuân theo các bước cơ bản sau:

Cài đặt IIS trên máy chủ:

Mở Server Manager.

Chọn "Manage" -> "Add Roles and Features".

Chọn "Web Server (IIS)" trong danh sách các tính năng và cài đặt.

Cài đặt ASP.NET trên IIS:

Mở Server Manager.

Chọn "Manage" -> "Add Roles and Features".

Trong wizard, chọn "Role-based or feature-based installation".

Chọn máy chủ cần cài đặt tính năng IIS.

Chọn "Web Server (IIS)" -> "Application Development" -> Chọn "ASP.NET".

Cấu hình một ứng dụng web:

Mở IIS Manager.

Trong trình duyệt bên trái, chọn "Sites".

Chuột phải vào "Default Web Site" (hoặc tạo một site mới) và chọn "Add Application".

Đặt Alias và chọn đường dẫn vật lý đến thư mục gốc của ứng dụng web ASP.NET.

Chạy ứng dụng web ASP.NET:

Mở trình duyệt web và nhập địa chỉ http://localhost/ten-ung-dung.

1. **Làm sao vào được firewall của Window Server nhanh nhất ? Làm sao có thể mở các cổng dịch vụ 80, 22, 23, 1723 , 3389 , 443, 1433 mà không cần phải tắt firewall ?**

Mở Firewall Settings:

Mở "Control Panel" trên máy chủ Windows Server.

Chọn "System and Security" -> "Windows Defender Firewall."

Cấu hình cổng dịch vụ:

Chọn "Advanced settings" ở phía bên trái.

Trong cửa sổ "Windows Firewall with Advanced Security", chọn "Inbound Rules."

Chuột phải và chọn "New Rule..."

Chọn "Port" và nhấn "Next."

Nhập số cổng bạn muốn mở (ví dụ: 80, 22, 23, 1723, 3389, 443, 1433) và nhấn "Next."

Chọn "Allow the connection" và nhấn "Next."

Chọn các loại mạng bạn muốn áp dụng quy tắc (thường chọn tất cả) và nhấn "Next."

Đặt tên cho quy tắc và mô tả (nếu cần) và nhấn "Finish."

Kiểm tra quy tắc đã tạo:

Trong "Windows Firewall with Advanced Security", chọn "Inbound Rules."

Bạn sẽ thấy quy tắc mới được tạo.

Sử dụng Command Prompt:

Mở Command Prompt với quyền Administrator:

Nhấn Win + X và chọn "Command Prompt (Admin)" hoặc "PowerShell (Admin)."

Sử dụng lệnh netsh:

Để mở cổng 80, sử dụng lệnh sau:

netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80

netsh advfirewall firewall add rule name="Open Port 22" dir=in action=allow protocol=TCP localport=22

netsh advfirewall firewall add rule name="Open Port 23" dir=in action=allow protocol=TCP localport=23

netsh advfirewall firewall add rule name="Open Port 1723" dir=in action=allow protocol=TCP localport=1723

netsh advfirewall firewall add rule name="Open Port 3389" dir=in action=allow protocol=TCP localport=3389

netsh advfirewall firewall add rule name="Open Port 443" dir=in action=allow protocol=TCP localport=443

netsh advfirewall firewall add rule name="Open Port 1433" dir=in action=allow protocol=TCP localport=1433

1. **GPO là gì ? Có thể tạo GPO cho 2 hoặc nhiều OU khác nhau được không ?**

GPO (Group Policy Object) là một tính năng của hệ điều hành Windows Server, được sử dụng để quản lý cấu hình và chính sách an toàn trên các máy tính và người dùng trong một môi trường Active Directory (AD). GPO giúp quản trị viên tự động hóa việc triển khai, quản lý và theo dõi các cài đặt cấu hình trên các máy tính và người dùng.

Cách tạo GPO cho 2 hoặc nhiều OU khác nhau:

Sử dụng GPMC (Group Policy Management Console):

Mở GPMC trên máy chủ Windows Server của bạn.

Chọn "Forest" -> "Domains" -> Tên domain của bạn.

Bên phải, chọn "Group Policy Objects" và chuột phải để tạo một GPO mới.

Đặt tên cho GPO và nhấn "OK."

Chọn OU mà bạn muốn liên kết GPO đó. Bạn có thể chọn nhiều OU bằng cách giữ phím Ctrl hoặc Shift trong quá trình chọn.

1. **Cách thức cài đặt phần mềm cho client từ GPO có mấy cách ?**

1. Sử dụng Group Policy Software Installation

2. Sử dụng Logon Scripts

3. Sử dụng PowerShell Scripts

4. Sử dụng MSI Deployment

1. **Các lệnh nào để vào các dịch vụ Card mạng, Active Directory, Local User And group, Programe and Features, Internet Information Service, Registry, Microsoft Management Console, Firewall, Startup, desktop chung của tất cả user, group policy.**

1. Card mạng:

Lệnh Command Prompt:

ncpa.cpl

2. Active Directory:

Lệnh MMC (Microsoft Management Console):

dsa.msc

3. Local Users and Groups:

Lệnh Command Prompt:

lusrmgr.msc

4. Programs and Features:

Lệnh Control Panel:

appwiz.cpl

5. Internet Information Services (IIS):

Lệnh Run:

inetmgr

6. Registry Editor:

Lệnh Run:

Regedit

7. Microsoft Management Console (MMC):

Lệnh Run:

Mmc

8. Firewall:

Lệnh Command Prompt:

wf.msc

9. Startup Folder:

Lệnh Run:

shell:startup

10. Desktop (chung của tất cả user):

Lệnh Run:

shell:common desktop

11. Group Policy Editor:

Lệnh Run:

gpedit.msc

1. **Làm cách nào để có thể cấm người dùng sử dụng internet download manager bằng GPO**

Việc cấm người dùng sử dụng Internet Download Manager (IDM) thông qua Group Policy Object (GPO) trong môi trường Windows có thể thực hiện được bằng cách tắt hoặc ngăn chặn một số tính năng cụ thể hoặc các loại phần mềm có thể làm tăng rủi ro bảo mật hoặc không phù hợp với chính sách tổ chức.

Dưới đây là một số biện pháp:

1. Tắt Windows Installer:

Tắt khả năng cài đặt các ứng dụng mới thông qua Windows Installer có thể giảm khả năng người dùng cài đặt IDM.

Mở Group Policy Management Console (GPMC).

Chọn hoặc tạo một Group Policy Object (GPO) và mở nó để chỉnh sửa.

Dưới Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Software Restriction Policies, bạn có thể chọn Don't allow any Windows Installer packages hoặc User Account Control: Only elevate executables that are signed and validated.

2. Quản lý Ứng Dụng và Chính Sách:

Sử dụng chính sách để quản lý ứng dụng có thể chặn IDM và các ứng dụng khác:

Mở Group Policy Management Console (GPMC).

Dưới User Configuration -> Policies -> Administrative Templates -> System, tìm và mở Don't run specified Windows applications.

Chọn "Enabled" và thêm tên tệp của IDM hoặc các ứng dụng mà bạn muốn chặn.

3. Ngăn Chặn Quyền Truy Cập vào Thư Mục Cài Đặt:

Điều này đặc biệt hữu ích nếu IDM được cài đặt trong một thư mục cụ thể. Ngăn chặn quyền truy cập đọc/ghi vào thư mục cài đặt IDM cho các người dùng không mong muốn.

Sử dụng ACLs (Access Control Lists) hoặc chính sách nhóm để kiểm soát quyền truy cập vào thư mục này.

4. Quản Lý Proxy và Firewall:

Quản lý cấu hình proxy để kiểm soát và giới hạn quyền truy cập của người dùng.

Sử dụng tường lửa để kiểm soát kết nối internet và ngăn chặn các kết nối đến các server cụ thể mà IDM có thể sử dụng.

1. **Hãy tìm cách đăng nhập Windows 10 tự động, không cần nhập mật khẩu biết rằng user của Windows 10 đã có mật khẩu.**

có thể cấu hình đăng nhập tự động vào Windows 10 mà không cần nhập mật khẩu.Hai cách để cấu hình đăng nhập tự động:

Sử dụng công cụ netplwiz: Bạn có thể sử dụng công cụ netplwiz để cấu hình đăng nhập tự động. Để làm điều này, bạn cần mở cửa sổ Run bằng cách nhấn tổ hợp phím Win + R. Nhập netplwiz và nhấn Enter. Chọn tài khoản người dùng trong tab Users. Bỏ chọn hộp kiểm Users must enter a username and password to use this computer. Nhấn Apply. [Nhập mật khẩu hai lần và nhấn OK1](https://windowsloop.com/automatically-login-on-windows-10-with-no-password/)[2](https://10scopes.com/configure-windows-10-auto-login-without-password/).

Sử dụng Registry Editor: Bạn có thể sử dụng Registry Editor để cấu hình đăng nhập tự động. Để làm điều này, bạn cần mở Registry Editor bằng cách nhấn tổ hợp phím Win + R. Nhập regedit và nhấn Enter. Điều hướng đến HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon. Tìm và chỉnh sửa giá trị AutoAdminLogon thành 1. Tạo giá trị chuỗi mới DefaultPassword và nhập mật khẩu của tài khoản người dùng vào giá trị này. Nếu giá trị DefaultPassword không tồn tại, hãy tạo giá trị chuỗi mới và đặt tên là DefaultPassword. [Khởi động lại máy tính và bạn sẽ tự động đăng nhập vào Windows 10 mà không cần nhập mật khẩu](https://www.pcmag.com/how-to/how-to-launch-windows-without-entering-a-password)

1. **Lệnh nào cho phép máy tính client Windows 10 cập nhật một địa chỉ IP mới lấy từ DHCP Server ?**

- Để cập nhật địa chỉ IP mới lấy từ DHCP Server trên máy tính client Windows 10, bạn có thể sử dụng lệnh ipconfig /renew. Lệnh này sẽ yêu cầu máy tính client gửi một yêu cầu cập nhật địa chỉ IP mới đến DHCP Server. [Sau khi nhận được yêu cầu, DHCP Server sẽ cấp phát một địa chỉ IP mới cho máy tính client](https://bing.com/search?q=L%e1%bb%87nh+n%c3%a0o+cho+ph%c3%a9p+m%c3%a1y+t%c3%adnh+client+Windows+10+c%e1%ba%adp+nh%e1%ba%adt+m%e1%bb%99t+%c4%91%e1%bb%8ba+ch%e1%bb%89+IP+m%e1%bb%9bi+l%e1%ba%a5y+t%e1%bb%ab+DHCP+Server)

1. **Server sử dụng domain qtm.com, quản trị sử dụng command dsadd user để tạo user tuy nhiên quản trị gặp lỗi ở lệnh dưới không thể tạo thành công. Sinh viên hãy tìm nguyên nhân của lỗi này?**

**dsadd user "CN=Tran Van A,OU=QTM\_01,OU=CTK38,OU=QTM,dc=com,dc=qtm" -upn atv -samid atv -pwd P@ssw0rd1410387 -memberof CN=QTM\_01 -mustchpwd yes**

dsadd user "CN=Tran Van A,OU=QTM\_01,OU=CTK38,OU=QTM,dc=com,dc=qtm" -upn atv -samid atv -pwd P@ssw0rd1410387 -memberof CN=QTM\_01 -mustchpwd yes

1. **Máy Windows Server muốn chia sẽ một thư mục ẩn đến các máy client? Làm sao để share thư mục ẩn và truy cập vào thư mục ẩn này?**

Nhấp chuột phải vào thư mục bạn muốn chia sẻ và chọn Properties.

Chọn thẻ Sharing và nhấp vào Advanced Sharing.

Chọn Share this folder và nhập tên chia sẻ của bạn.

Bỏ chọn hộp kiểm Share this folder on the network và nhập tên chia sẻ ẩn của bạn bằng cách thêm một ký tự $ vào cuối tên chia sẻ.

Nhấp vào Permissions và cấp quyền truy cập cho người dùng cần thiết.

Nhấp vào OK để lưu các thay đổi của bạn.

Để truy cập vào thư mục ẩn, bạn có thể nhập địa chỉ UNC (Universal Naming Convention) của thư mục vào thanh địa chỉ của trình duyệt tệp của bạn. Địa chỉ UNC sẽ có dạng \\servername\sharename$. Bạn sẽ được yêu cầu nhập thông tin đăng nhập để truy cập vào thư mục.

1. **Bạn hiểu thế nào là Roaming Profile và Mandatory Roaming Profile?**

Roaming Profile là một loại hồ sơ người dùng được lưu trữ trên một máy chủ mạng và cho phép người dùng truy cập vào hồ sơ của họ từ bất kỳ máy tính nào trong mạng. Khi người dùng đăng nhập vào một máy tính mới, hồ sơ của họ được tải xuống từ máy chủ mạng và được sử dụng để cấu hình máy tính đó theo cách mà người dùng đã thiết lập trước đó. Khi người dùng đăng xuất khỏi máy tính, hồ sơ của họ được tải lên máy chủ mạng để được sử dụng cho các lần đăng nhập sau.

Mandatory Roaming Profile là một loại hồ sơ người dùng bắt buộc, được lưu trữ trên một máy chủ mạng và cho phép người dùng truy cập vào hồ sơ của họ từ bất kỳ máy tính nào trong mạng. Tuy nhiên, khi người dùng đăng nhập vào một máy tính mới, hồ sơ của họ được tải xuống từ máy chủ mạng và được sử dụng để cấu hình máy tính đó theo cách mà người quản trị đã thiết lập trước đó. Khác với Roaming Profile, các thay đổi được thực hiện bởi người dùng trong phiên làm việc của họ không được lưu trữ trong hồ sơ của họ. [Mandatory Roaming Profile thường được sử dụng trong các trường hợp mà sự đồng nhất là quan trọng, chẳng hạn như trên các thiết bị kiosk hoặc trong các cài đặt giáo dục](https://learn.microsoft.com/en-us/windows/client-management/client-tools/mandatory-user-profile)

1. **Tại sao máy pcvn.vn khi remote truy cập từ xa có thể ping đến máy ảo Windows 10 sử dụng card mạng NAT (Vmware 8) ?**

Máy ảo Windows 10 sử dụng card mạng NAT (Network Address Translation) trong VMware 8. NAT cho phép máy ảo kết nối với mạng bên ngoài thông qua card mạng của máy chủ chứa máy ảo. Khi máy ảo được kết nối với mạng bên ngoài, nó có thể được ping từ xa bởi các máy tính khác trong mạng. Điều này giải thích tại sao máy pcvn.vn có thể ping đến máy ảo Windows 10 của bạn khi remote truy cập từ xa.

1. **Viết file script .bat ánh xạ ổ đĩa** [**\\ip-server\share**](file:///\\ip-server\share) **với username test password test (sinh viên có thể tìm hiểu và tự viết trên Windows 10)**
2. **Tìm hiểu dịch vụ Network Policy Server là gì ? Các chức năng cơ bản mà dịch vụ này hỗ trợ.**

Network Policy Server (NPS) là một dịch vụ trên Windows Server, cung cấp các chức năng xác thực và kiểm soát truy cập cho các máy tính và thiết bị trong mạng. [NPS hoạt động như một RADIUS (Remote Authentication Dial-In User Service) server, thực hiện xác thực, ủy quyền và tính toán tài khoản truy cập cho nhiều loại truy cập mạng, bao gồm truy cập mạng không dây, truy cập từ xa qua VPN, truy cập qua router-to-router, và truy cập qua switch 1](https://securityzone.vn/t/lab-trien-khai-nps-network-policy-server-part-1.964/)[2](https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top).

Các chức năng cơ bản mà NPS hỗ trợ bao gồm:

**Xác thực và ủy quyền truy cập**: NPS cung cấp các chức năng xác thực và ủy quyền truy cập cho các máy tính và thiết bị trong mạng. [Nó cho phép quản trị viên xác định các điều kiện để xác thực và ủy quyền truy cập, bao gồm các yêu cầu về mật khẩu, chứng chỉ số, và các thông tin khác 1](https://securityzone.vn/t/lab-trien-khai-nps-network-policy-server-part-1.964/).

**Kiểm soát truy cập**: NPS cho phép quản trị viên kiểm soát truy cập vào mạng bằng cách thiết lập các chính sách truy cập. [Các chính sách này có thể được thiết lập để kiểm soát truy cập của người dùng và thiết bị dựa trên các yêu cầu về an ninh, quyền truy cập, và các yêu cầu khác 1](https://securityzone.vn/t/lab-trien-khai-nps-network-policy-server-part-1.964/).

**Tính toán tài khoản truy cập**: NPS cung cấp tính năng tính toán tài khoản truy cập cho các máy tính và thiết bị trong mạng. [Nó cho phép quản trị viên xác định các điều kiện để tính toán tài khoản truy cập, bao gồm các yêu cầu về thời gian, số lượng truy cập, và các yêu cầu khác](https://securityzone.vn/t/lab-trien-khai-nps-network-policy-server-part-1.964/)

1. **Chiếm quyền trong thư mục Windows Server là gì? Cách thức chiếm quyền?**

Chiếm quyền trong thư mục Windows Server là một cách để đảm bảo rằng người dùng có quyền truy cập vào các tệp và thư mục mà họ không có quyền truy cập. Khi bạn chiếm quyền, bạn sẽ có quyền truy cập vào các tệp và thư mục đó và có thể thực hiện các thao tác như sao chép, di chuyển, đổi tên hoặc xóa các tệp và thư mục đó.

Để chiếm quyền trong thư mục Windows Server, bạn có thể thực hiện các bước sau:

1. Nhấp chuột phải vào thư mục hoặc tệp tin mà bạn muốn chiếm quyền và chọn Properties.
2. Chọn thẻ Security và nhấp vào Advanced.
3. Chọn Change ở phần Owner và nhập tên người dùng hoặc nhóm người dùng mà bạn muốn chiếm quyền.
4. Bật chế độ Replace owner on subcontainers and objects nếu bạn muốn chiếm quyền cho tất cả các tệp và thư mục con.
5. Nhấp vào OK để lưu các thay đổi của bạn.
6. **Làm sao để tắt kế thừa quyền Folder ? Có những chức năng tắt kế thừa nào? Giải thích từng chức năng.**

Để tắt kế thừa quyền trên một thư mục trong Windows, bạn có thể làm theo các bước sau:

1. Nhấp chuột phải vào thư mục và chọn Properties.
2. Chọn thẻ Security và nhấp vào Advanced.
3. Bấm vào Disable inheritance và chọn Convert inherited permissions into explicit permissions on this object.
4. Nhấp vào Apply và chọn OK.

Sau khi tắt kế thừa quyền, bạn có thể sử dụng các chức năng sau để quản lý quyền truy cập trên thư mục: