Windows Server 2022 – Active Directory & DHCP Failover Lab

Thiết kế và Quản trị hệ thống doanh nghiệp quy mô vừa

Vị trí định hướng: Network Engineer / System Admin (Fresher)
Thời gian thực hiện: 2025
Người thực hiện: Chu Trọng Việt

1.Giới thiệu chung về Dự Án

1.1. Mục tiêu của dự án

- Dự án Triển khai môi trường Windows Server 2022 mô phỏng hệ thống doanh nghiệp nhỏ và vừa được cấu hình ảo hóa bằng phần mềm VMWare Workstation 17, tập trung vào các tính năng cơ bản:

- Active Directory Domain Services (ADDS)
- Dynamic Host Configuration Protocol (DHCP)
- Tạo các Organize Unit (OU) /User /Group
- Cấu hình các Home folder /Share /NTFS
- Tạo các Group Policy (GPO) quản lí người dùng và máy tính

Ngoài ra, để đề phòng hệ thống có thể có các sự cố, cần có sự dự phòng trong hệ thống bằng các có thêm 1 Windows Server dự phòng cung cấp khả năng:

- DHCP Failover
- NIC Teaming

1.2 Phạm vi dự án

- Môi trường lab nội bộ (on-premises)
- Không sử dụng cloud
- Không dùng script tự động
- Tập trung triển khai thủ công để hiểu bản chất dịch vụ

2.Kiến trúc hệ thống mạng

2.1. Thành phần hệ thống mạng

Thành phần	Vai trò
DC01	Domain Controller chính (GUI)
DC02	Domain Controller dự phòng (Server Core)
Workstation	Các máy trạm trong hệ thống domain

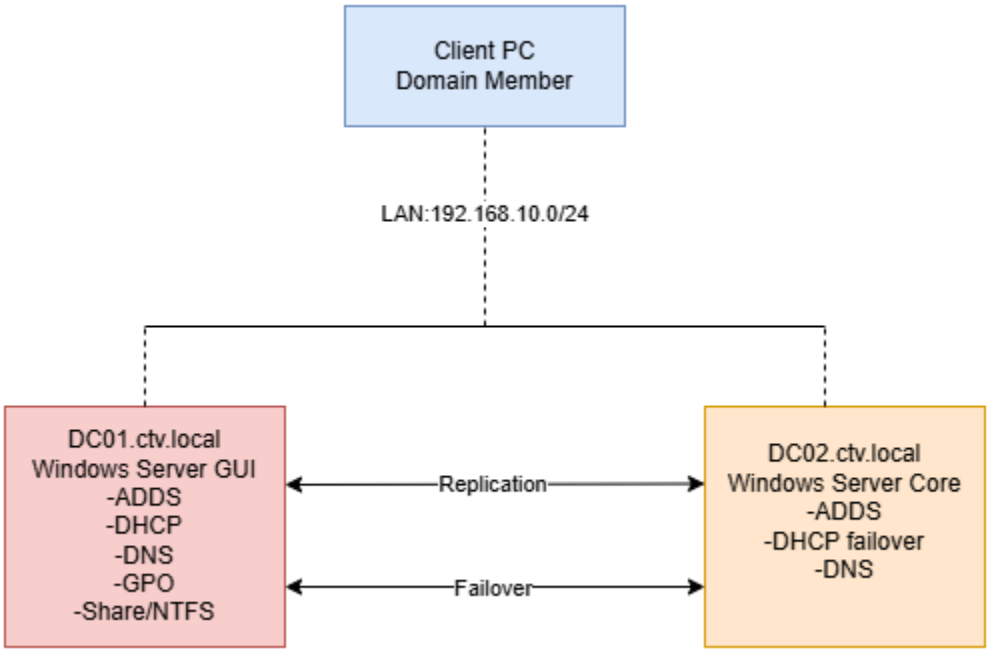
Thành phần hệ thống mạng gồm 3 phần chính:

+ DC01: là Domain Controller (DC) chính chạy bằng Windows Server 2022 phiên bản Datacenter GUI.Vì là DC chính nên DC01 có đầy đủ các chức năng ADDS, DHCP, GPO, các OU/user/group và các thư mục chứa các file Home Folder…

+ DC02: là Domain Controller dự phòng chạy bằng Windows Server 2022 phiên bản Datacenter Core (không có giao diện đồ họa), giúp tiết kiệm tài nguyên hệ thống và tính bảo mật tốt. DC02 được join vào Domain và chạy DHCP failover – cấp IP dự phòng trường hợp DC01 xảy ra sự cố

+ Workstation: các máy trạm được cấp địa chỉ IP tương ứng, các Computer đại điện cho các User trong các phòng ban: IT, KeToan, KinhDoanh được cấu hình tham gia vào domain và áp các quy định về phòng ban

2.2. Sơ đồ hệ thống mạng



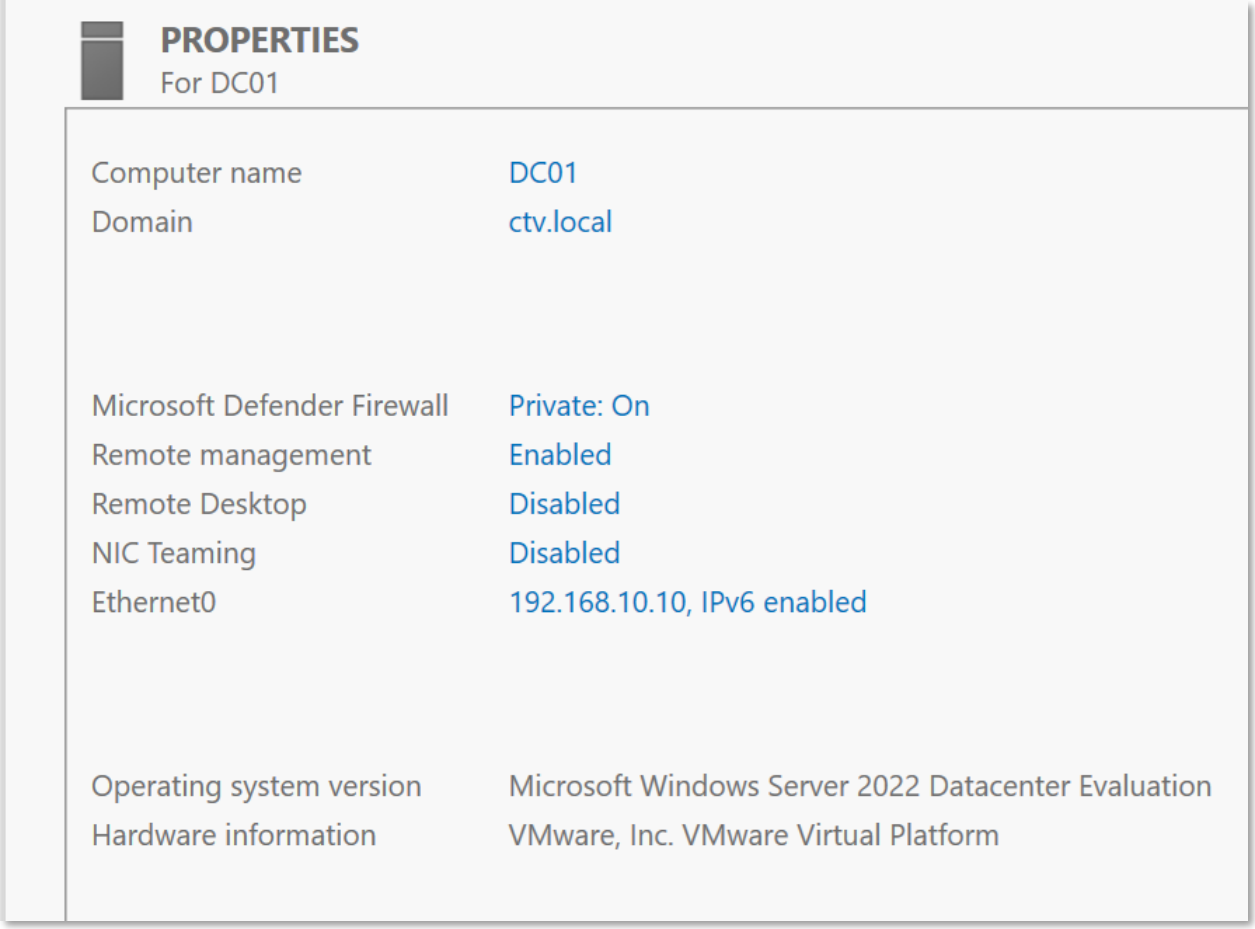
- DC01 và DC02 đồng bộ AD và DNS
- DHCP được cấu hình failover để tránh gián đoạn cấp IP
- DC02 đóng vai trò dự phòng & sẵn sàng mở rộng

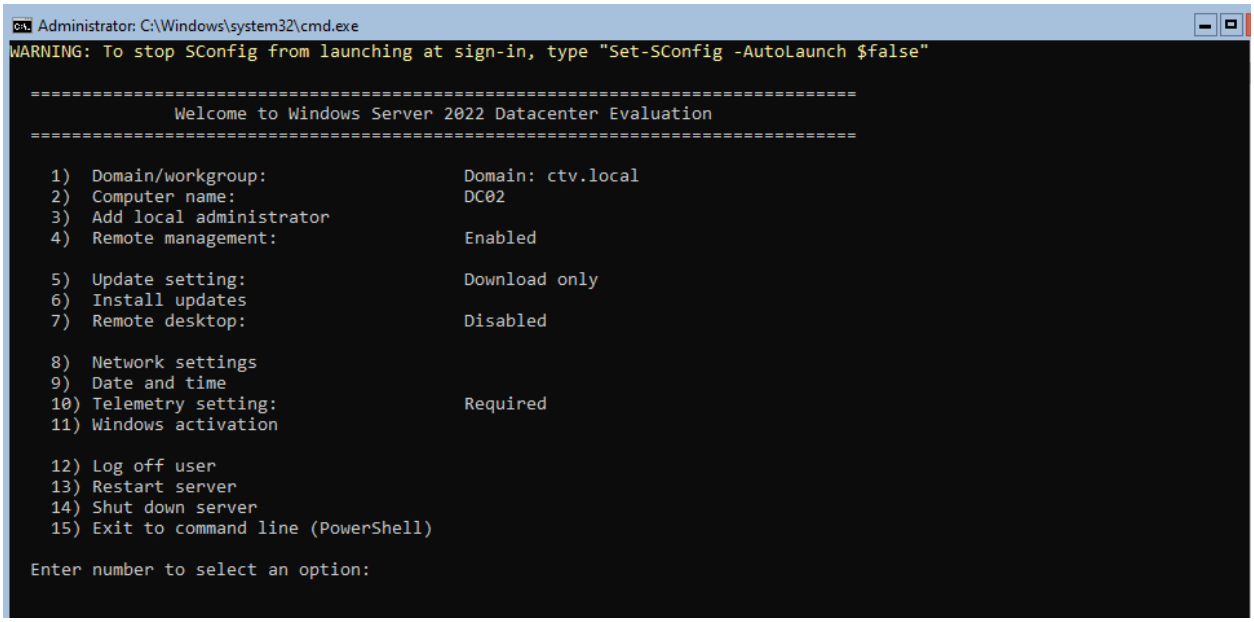
3.Các thành phần được triển khai

3.1. Active Directory Domain Services (AD DS)

- AD DS là dịch vụ quản lý tập trung trong Windows Server:

- Quản lý user, computer, group
- Áp dụng chính sách (GPO) cho toàn hệ thống
- Kiểm soát bảo mật và quyền truy cập





Trong bài lab này, ta có:

+ Domain name: ctv.local

+ 2 Domain Controller:

- DC01: GUI
- DC02: Server Core

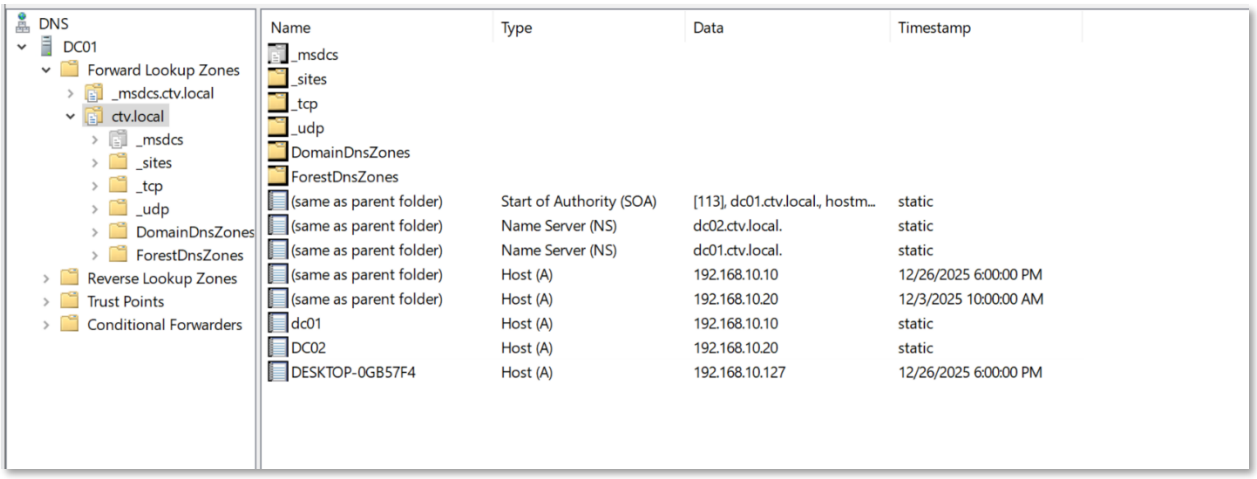
Triển khai 2 DC mục đích là để đảm bảo đăng nhập domain khi 1 DC gặp sự cố, tránh làm ngừng hoạt động công việc của doanh nghiệp

3.2. DNS

DNS là dịch vụ phân giải tên miền chuyển tên miền thành địa chỉ IP

Vai trò của DNS:

- Phân giải tên cho domain
- Hỗ trợ đăng nhập AD
- Hỗ trợ dịch vụ DHCP

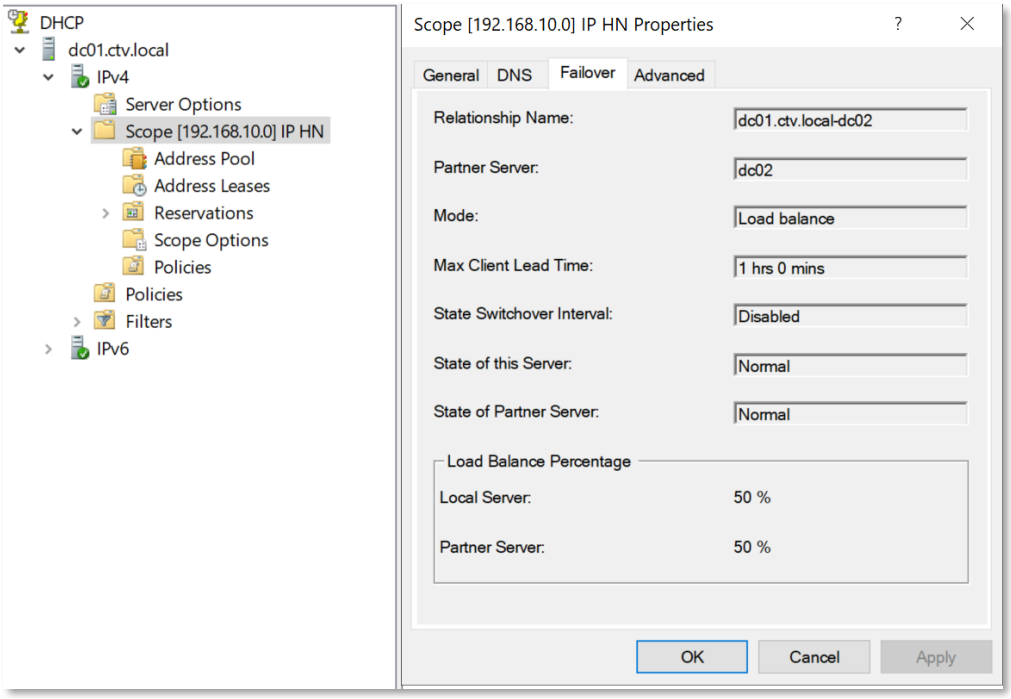


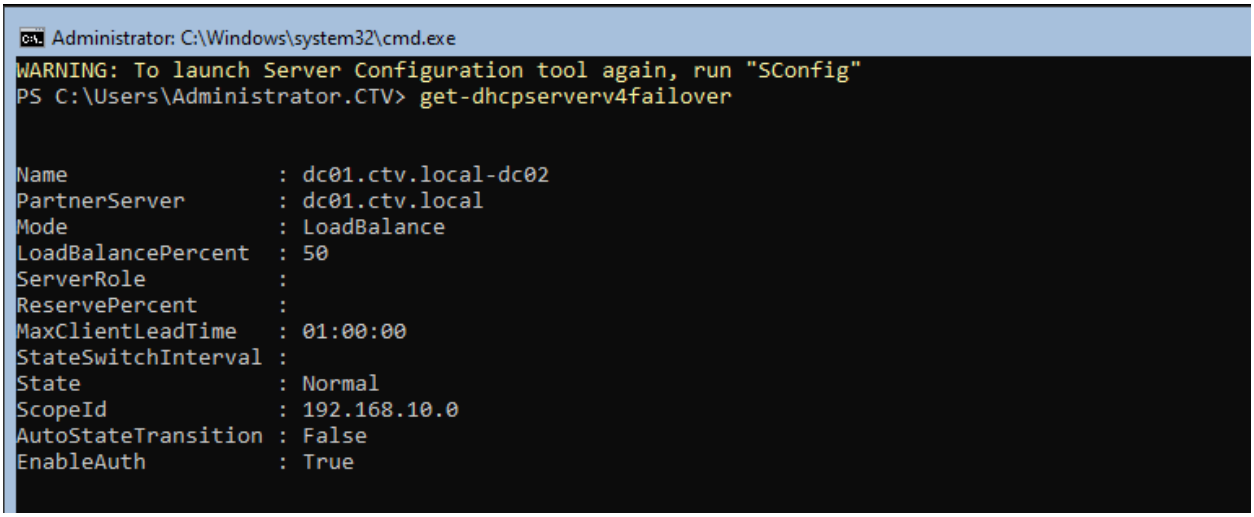
DNS được cài trên cả DC01 và DC02 được tích hợp Active Directory (AD)

3.3. DHCP & DHCP Failover

- DHCP là một tính năng tự động cấp phát IP và cấu hình mạng cho máy client.DHCP sẽ cấp IP, Subnet Mask, Default Gateway, DNS

- DHCP Failover là một giải pháp dự phòng DHCP trường hợp máy cấp DHCP chính bị trục trặc vấn đề để khi một server lỗi thì còn server còn lại vẫn cấp phát được IP tạm thời giúp đỡ quá trình làm việc không bị gián đoạn





- Scope: 192.168.10.50 – 192.168.10.200
- DHCP Failover Mode: Load Balance
- DC01: Active
- DC02: Load Balance

Mục tiêu bài lab:

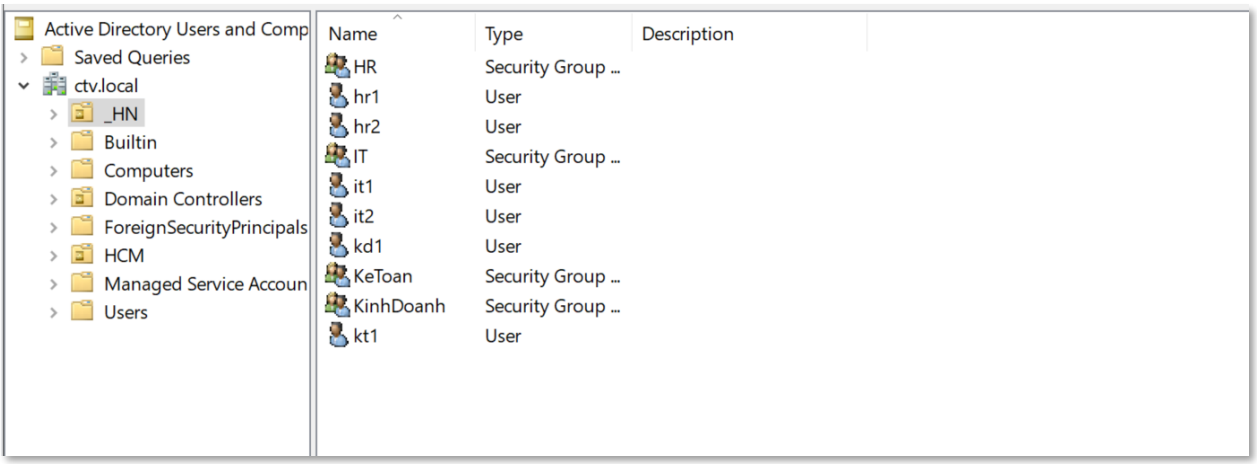
- Client vẫn nhận IP khi DC01 ngừng hoạt động
- Đảm bảo dịch vụ mạng liên tục

3.4. Quản lí người dùng

Tạo các Organizational Unit (OU) cho các chi nhánh HN và HCM với các group IT, HR, KinhDoanh, Ketoan với các user tương ứng mỗi phòng ban

- OU là thư mục logic để tổ chức và quản lý user, computer, group trong AD, dùng để gom đối tượng theo phòng ban, chi nhánh , chức năng, áp dụng các GPO và phân quyền

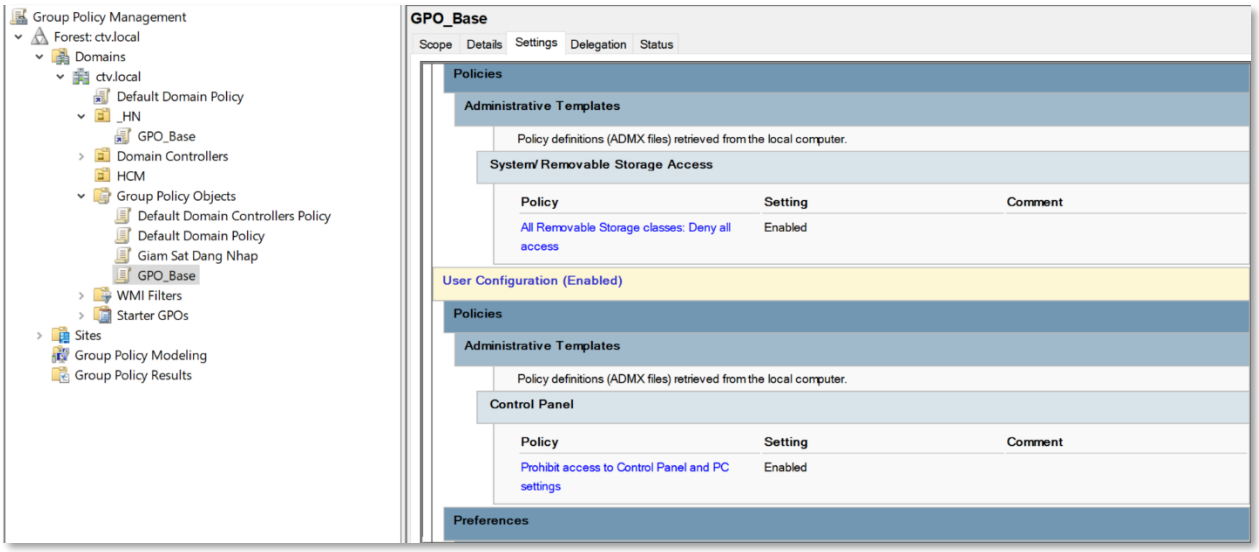
truy cập



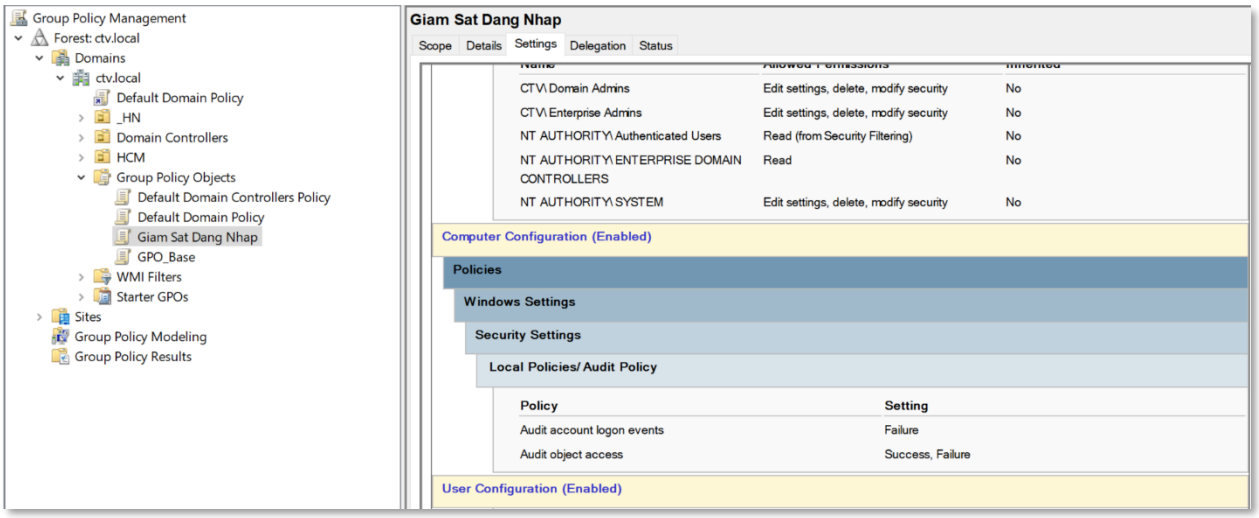
3.5. Group Policy Object (GPO)

- GPO là tập hợp các chính sách (rules) để cấu hình và kiểm soát User và Computer trong domain, quy định kiểm soát môi trường làm việc của user và máy tính, user có thể làm gì và không làm gì?

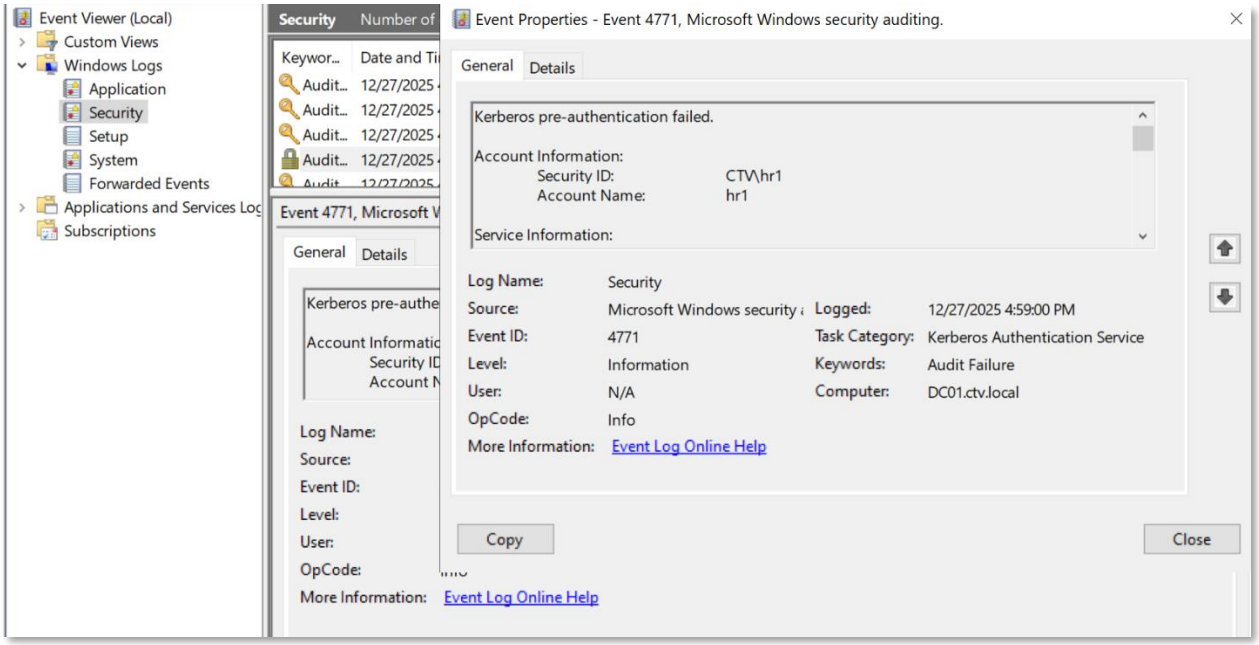
- Ưu điểm thay vì cấu hình cho từng máy, từng user, với GPO chúng ta có thể cấu hình một lần trên server và áp cho hàng loạt user máy tính trong domain



+ Trong bài Lab ngoài các Policy mặc định thì còn có thêm GPO_Base với các quy định về chặn các thiết lạ kết nối vào máy tính như USB, ổ cứng…và các computer được chỉ định sẽ bị chặn truy cập vào Control Panel và PC setting.Điều này giúp cho máy tính được bảo mật khỏi các cuộc tấn công



- GPO_Giam_Sat_Dang_Nhap giúp hệ thống chi chép lại các hoạt động bảo mật khi 1 user cố gắng đăng nhập trên một máy tính và một tài khoản truy cập vào 1 folder dữ liệu thông qua Event Viewer

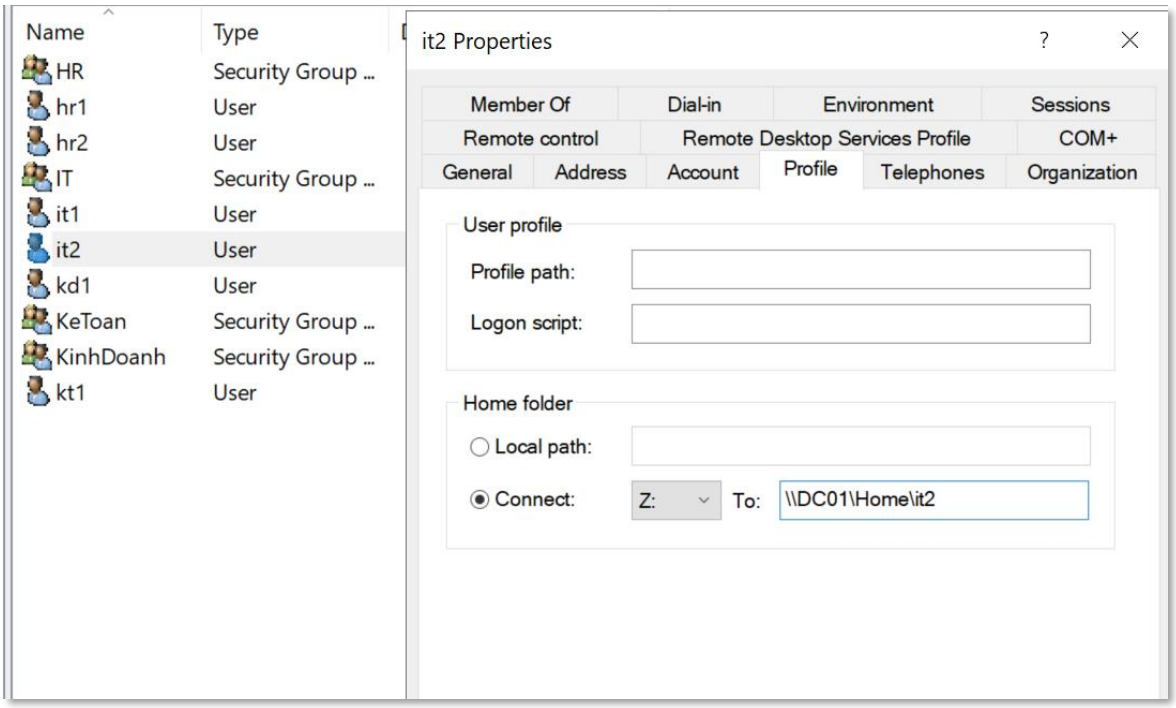


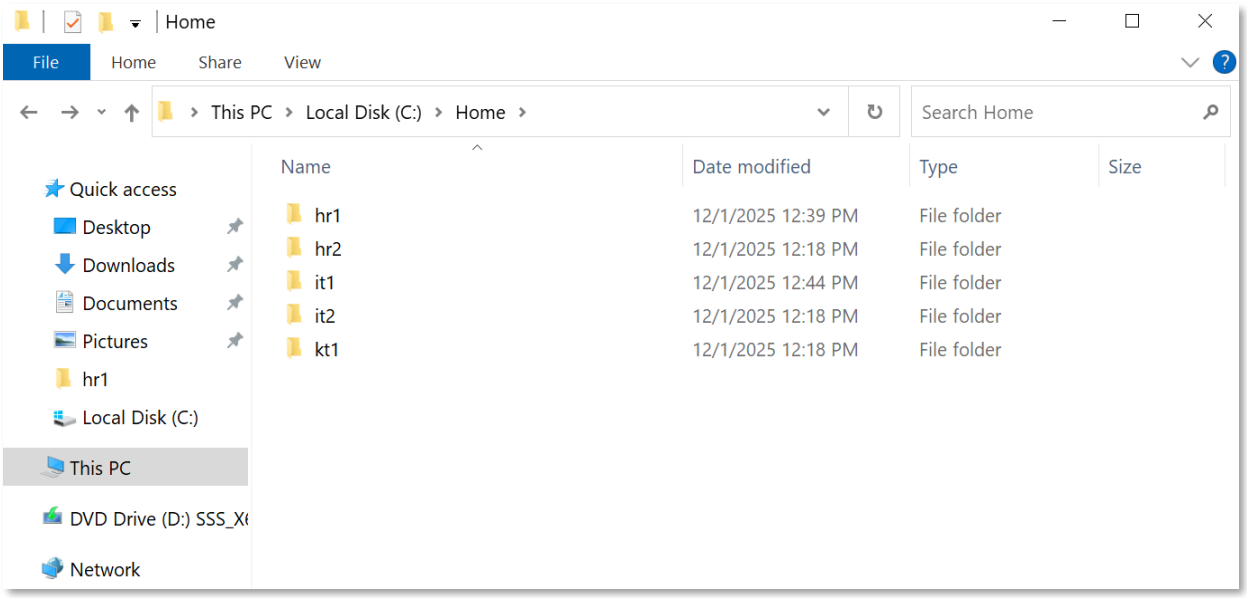
3.6. Home folder

- Home folder là thư mục cá nhân riêng của mỗi user trên server và mỗi user có một thư mục riêng, user khác không thể xem được.Mục đích dùng để lưu tài liệu cá nhân và sao lưu dữ liệu

- Khi cấu hình có thể map thành ổ tùy ý ví dụ: A…Z và chạy câu lệnh:

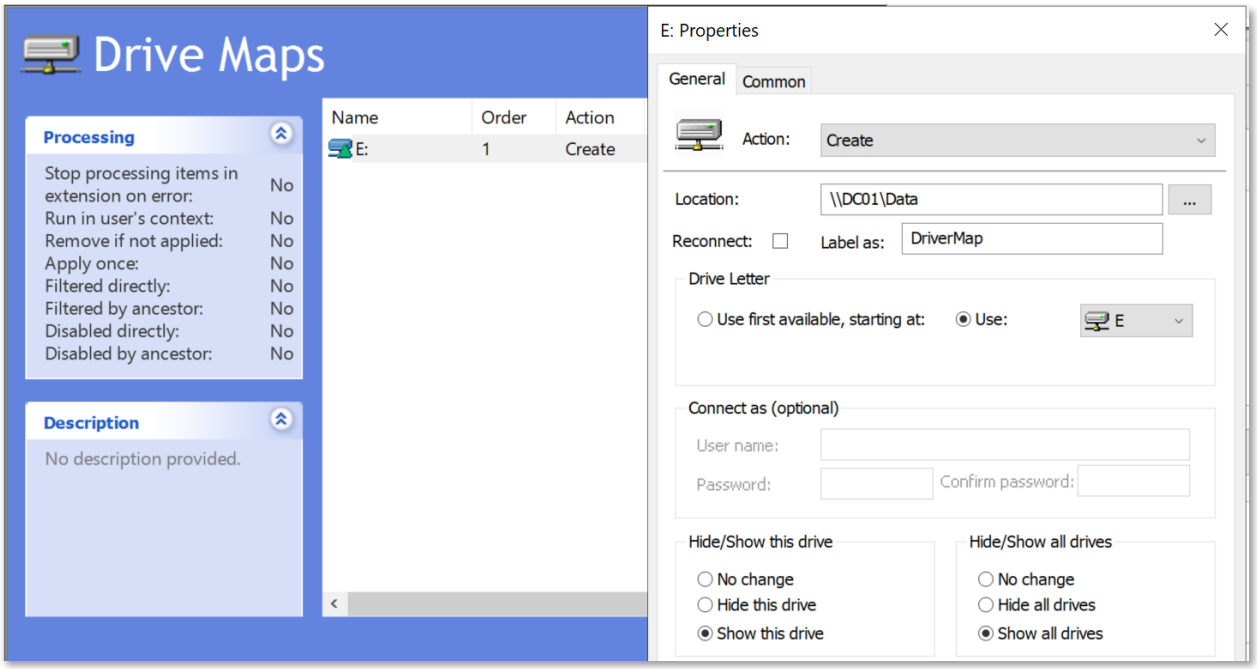
\\DC01\Home\%username%

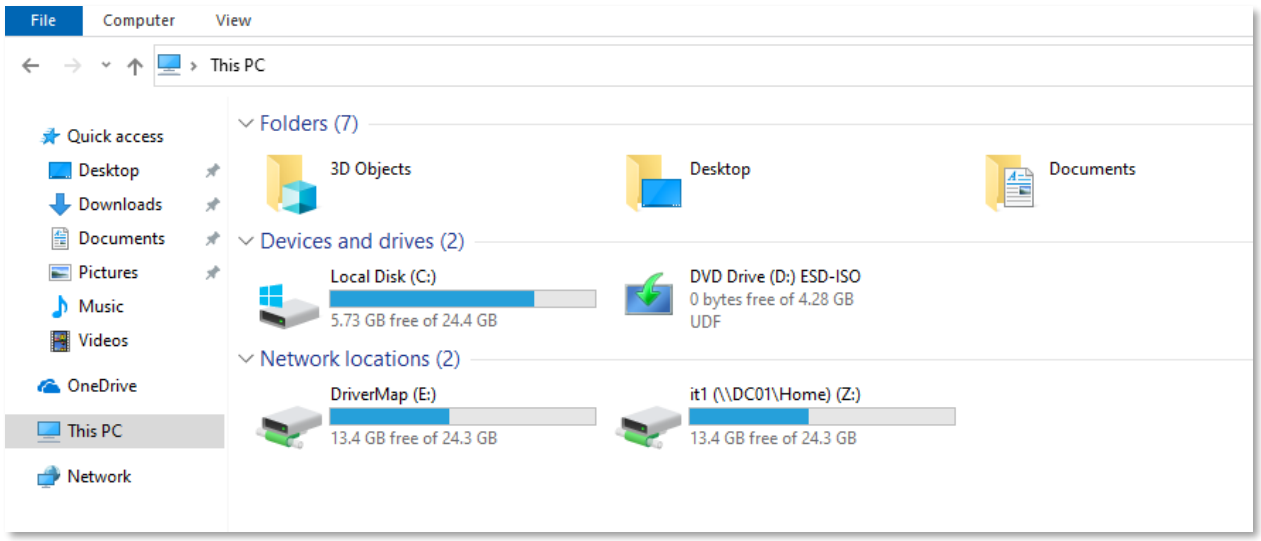




- Map Driver là một tính năng không thể thiếu trong hệ thống mạng doanh nghiệp, giúp gán thư mục mạng thành ổ đĩa như ổ cứng

- Sử dụng Group Policy để Map Drive theo OU và Group, giúp user truy cập dữ liệu đúng quyền, dễ quản lý dữ liệu tập trung và đảm bảo an toàn vì dữ liệu ổ đĩa nằm trên server





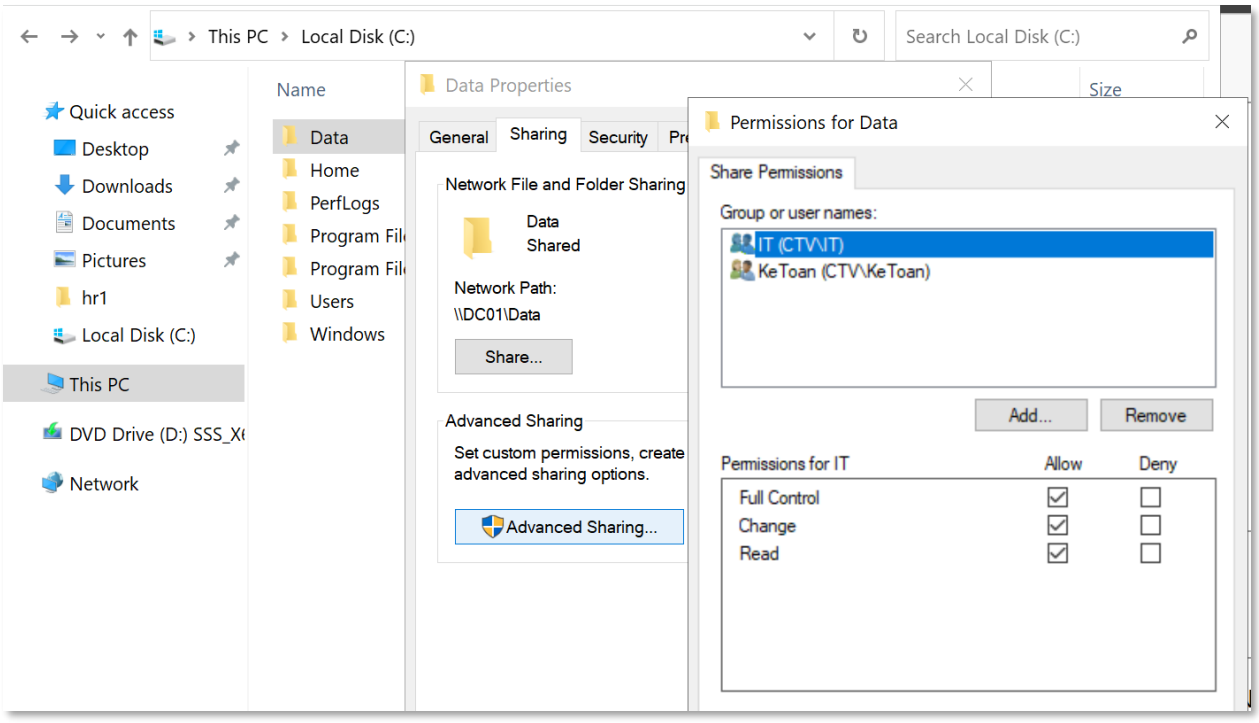
3.7. Share và NTFS

- Share Permission là cơ chế phân quyền truy cập thư mục qua mạng trên Windows Server, được cấu hình tại mức chia sẻ (Sharing) của thư mục.
Share Permission chỉ có hiệu lực khi người dùng truy cập thư mục thông qua đường dẫn mạng (UNC path) như \\Server\Share

Các mức quyền cơ bản của Share Permission gồm:

- Read
- Change
- Full Control

Share Permission thường được dùng để kiểm soát quyền truy cập tổng quát và kết hợp với NTFS Permission để đảm bảo an toàn dữ liệu



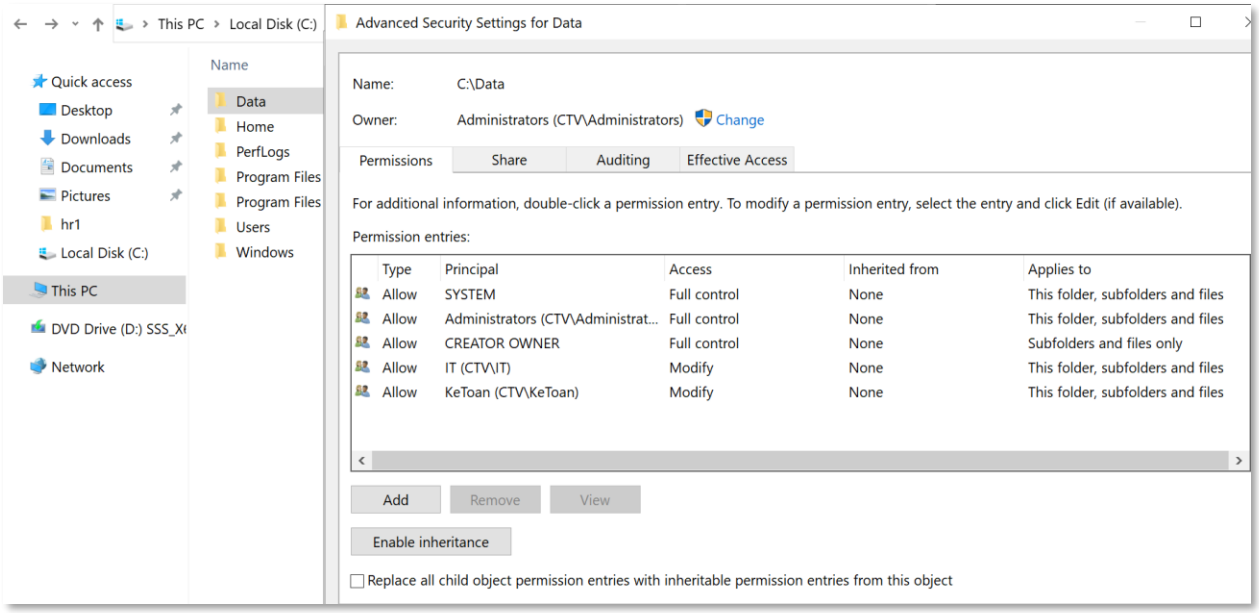
Trong bài lab này, thư mục Data chỉ được chia sẻ với 2 phòng ban là IT và KeToan với quyền mở rộng Full Controll

- NTFS Permission là cơ chế phân quyền truy cập file và thư mục trên hệ thống tập tin NTFS của Windows, áp dụng cho cả truy cập cục bộ (local) và qua mạng (network). NTFS Permission cho phép kiểm soát chi tiết các thao tác như đọc, ghi, chỉnh sửa, xóa dữ liệu

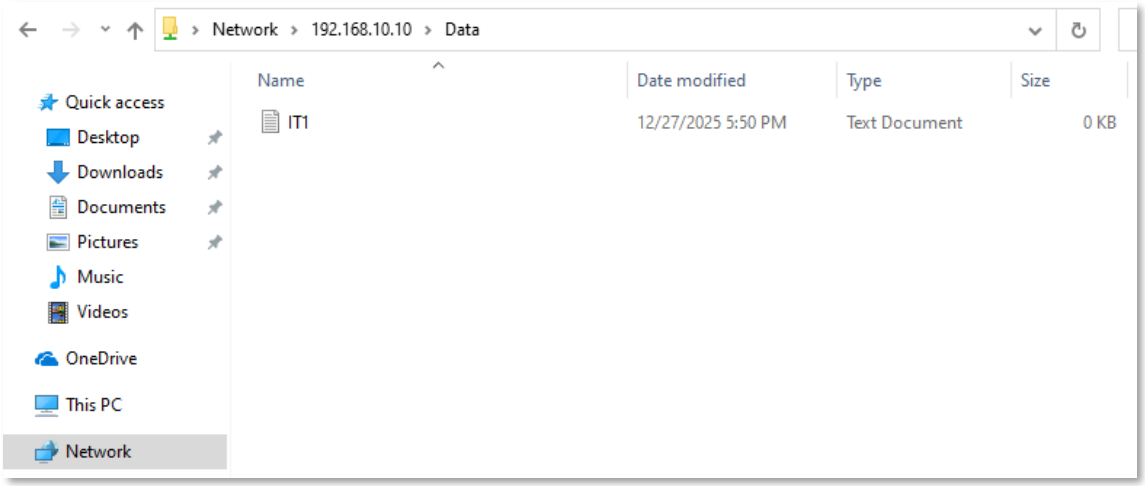
Các quyền phổ biến của NTFS Permission bao gồm:

- Read
- Write
- Modify
- Full Control

NTFS Permission là cơ chế phân quyền chính trong môi trường Windows Server do tính chi tiết và bảo mật cao



Trong phần security advanced, các phòng ban IT và KeToan chỉ có quyền modify. Vì vậy, quyền chung áp dụng cho thư mục Data này là Modify vì theo nguyên tắc hệ thống sẽ lấy quyền thấp hơn giữa Share và NTFS.Bên cạnh đó, các user có toàn quyền Full Control sẽ là Admin, Owner và System



4.Kiểm thử

4.1 Kiểm tra Active Directory & DNS

- Domain Controller trên cả 2 máy server đều đã hoạt động ổn định, các máy client đã join vào domain ctv.local thành công

```
PS C:\Users\Administrator> netdom query dc
>>
List of domain controllers with accounts in the domain:

DC01
DC02
The command completed successfully.
```

- Tuy nhiên, khi kiểm tra DNS thì xảy ra một lỗi "(8524) The DSA operation is unable to proceed because of a DNS lookup failure", nguyên nhân là bởi Domain Controller không phân giải được DNS của máy DC còn lại, nên một số phiên replication thất bại, do cấu hình sai địa chỉ Preferred DNS và Alternate DNS.Vì vậy, cách khắc phục chỉ cần cấu hình lại địa chỉ DNS của các máy DC thì quá trình phân giải tên và replication Active Directory hoạt động ổn định

```
PS C:\Users\Administrator> repadmin /replsummary
>>
Replication Summary Start Time: 2025-12-30 12:12:27

Beginning data collection for replication summary, this may take awhile:
  .....


Source DSA          largest delta    fails/total %%   error
 DC01                       11m:53s    0 /   5    0
 DC02                02d.19h:24m:34s    1 /   5   20  (8524) The DSA operation is unable to proceed because of a DNS lookup failure.


Destination DSA     largest delta    fails/total %%   error
 DC01                02d.19h:24m:34s    1 /   5   20  (8524) The DSA operation is unable to proceed because of a DNS lookup failure.
 DC02                       11m:53s    0 /   5    0
```

```
C:\Users\Administrator>repadmin /replsummary
Replication Summary Start Time: 2025-12-30 12:41:23

Beginning data collection for replication summary, this may take awhile:
  .....


Source DSA          largest delta    fails/total %%   error
 DC01                       40m:49s    3 /   5   60  (1908) Could not find the domain controller for this domain.
 DC02                          :41s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 DC01                          :41s    0 /   5    0
 DC02                       40m:49s    3 /   5   60  (1908) Could not find the domain controller for this domain.
```

- Tiếp theo là một lỗi "(1908) Could not find the domain controller for this domain", máy DC01 không tìm được DC02 qua DNS, tình huống này sau khi được tìm hiểu nguyên nhân ban đầu có thể do topology Active Directory chưa được tự động thiết lập, vì vậy để khắc phục thì cần chạy lệnh ép hệ thống xây dựng và đồng bộ lại replication topology qua câu lệnh : "repadmin /kcc", "repadmin /syncall /AdeP"

```
C:\Users\Administrator>repadmin /replsummary
Replication Summary Start Time: 2025-12-30 13:23:57

Beginning data collection for replication summary, this may take awhile:
  .....


Source DSA          largest delta    fails/total %%   error
 DC01                       :20s    0 /   5    0
 DC02                    26m:26s    0 /   5    0


Destination DSA     largest delta    fails/total %%   error
 DC01                    26m:26s    0 /   5    0
 DC02                       :20s    0 /   5    0
```

4.2. Kiểm tra DHCP Failover

- Thực hiện shutdown (Power Off) DC01 (DHCP Primary)

- Kiểm tra khả năng cấp phát IP từ DC02 (Load Balance)

```
thernet adapter Ethernet0:

  Connection-specific DNS Suffix  . : ctv.local
  Link-local IPv6 Address . . . . . : fe80::80fa:731c:cdd2:f14f%7
  IPv4 Address. . . . . . . . . . . : 192.168.10.127
  Subnet Mask . . . . . . . . . . . : 255.255.255.0
  Default Gateway . . . . . . . . . : 192.168.10.1
```

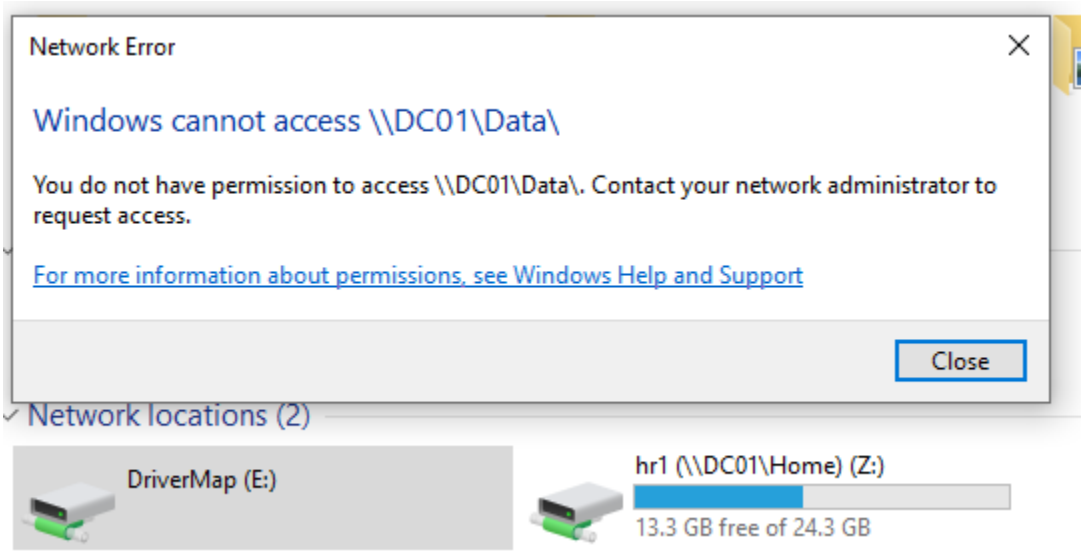
```
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : ctv.local
   Link-local IPv6 Address . . . . . : fe80::80fa:731c:cdd2:f14f%7
   IPv4 Address. . . . . . . . . . . : 192.168.10.128
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

Kết quả sau khi kiểm tra:

- Client vẫn nhận được địa chỉ IP hợp lệ
- Không xảy ra gián đoạn kết nối mạng
- DHCP Failover hoạt động đúng theo mô hình đã cấu hình

4.3. Kiểm tra phân quyền & Home Folder

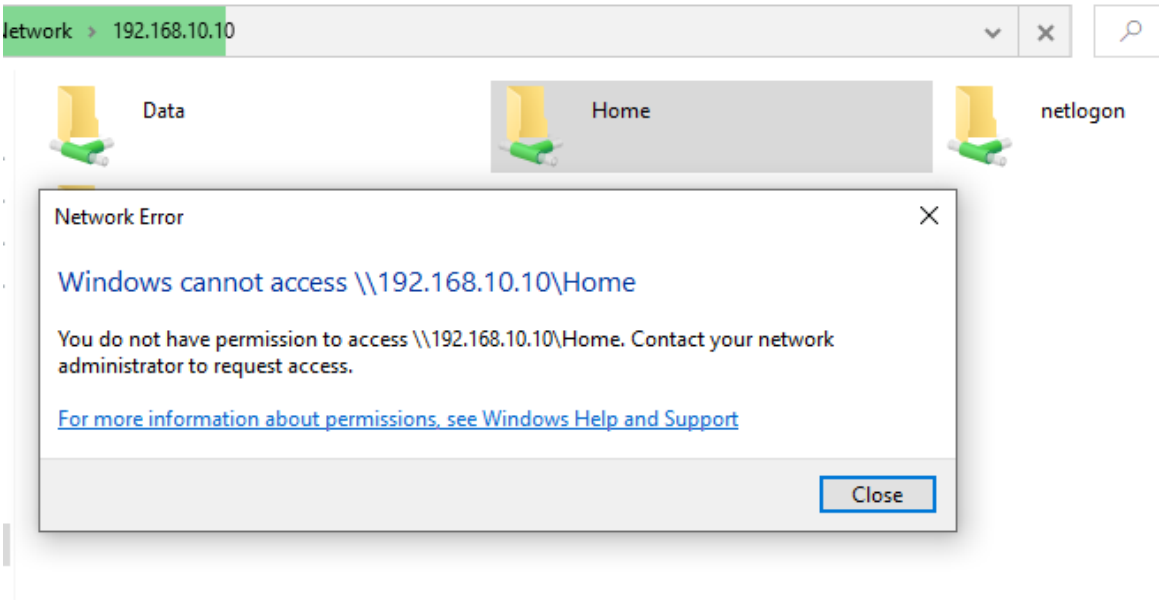
- Kiểm tra quyền truy cập thư mục theo từng group phòng ban: HR không thể truy cập được Folder Data của hệ thống



- Kiểm tra Home Folder:

+ User chỉ truy cập được thư mục cá nhân

+ Không truy cập được Home Folder của user khác



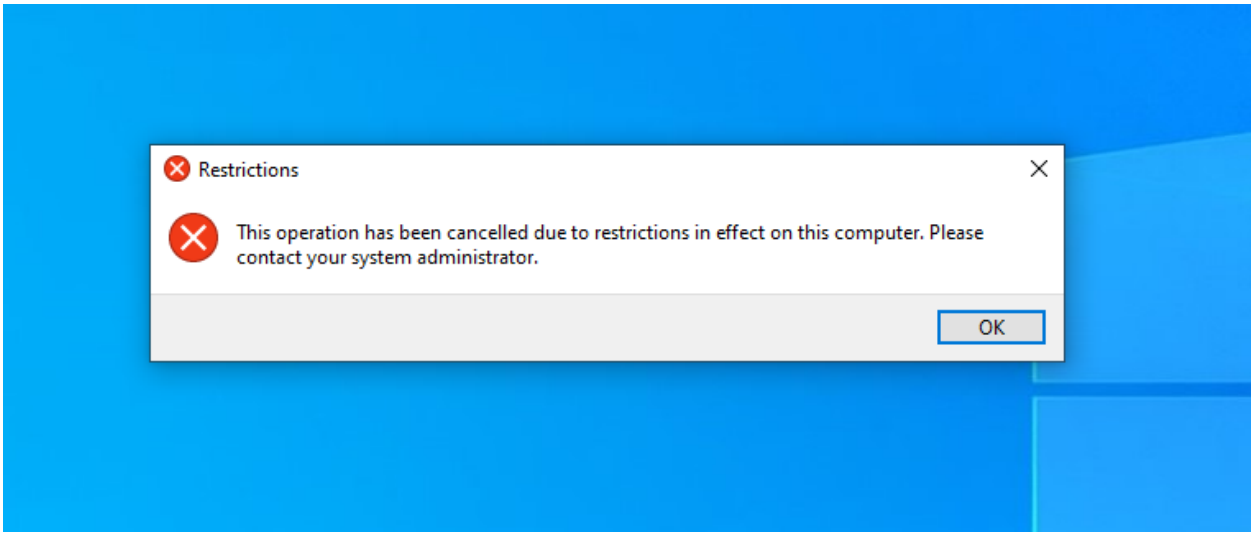
+ Mỗi user đã có một Home riêng, vì vậy khi truy cập qua ổ đĩa mạng thì quyền truy cập sẽ bị chặn lại

Tổng kết:

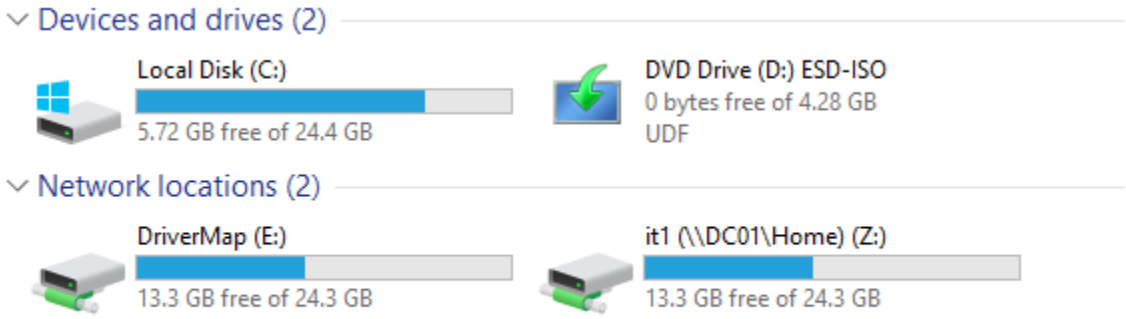
- Phân quyền được áp dụng chính xác theo group
- Home Folder hoạt động đúng yêu cầu bảo mật

4.4. GPO

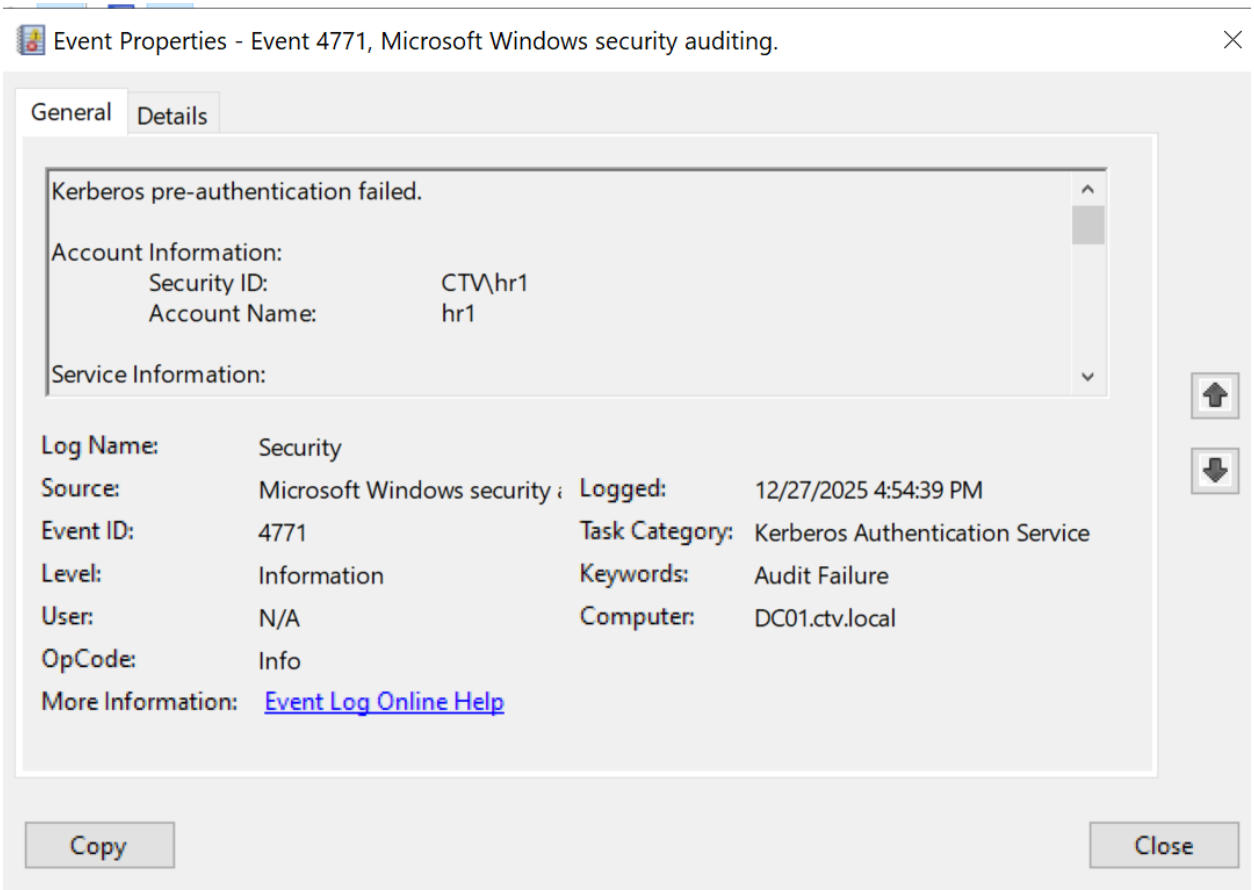
- Kiểm tra quyền truy cấp Control Panel trên máy PC: các máy PC được cấu hình không được phép truy cập Control Panel



- Kiểm tra Map Driver: các máy PC được map ổ đĩa mạng chia sẻ nhằm thuận tiện chia sẻ dữ liệu từ server



- Audit Policy:Giám sát đăng nhập và kiểm tra truy cập dữ liệu



Kết quả:

+ Các máy PC đã bị chặn Control Panel

+ Các máy trong phòng ban group đều có ổ đĩa mạng Map Driver

+ Hệ thống giám sát đăng nhập Audit Logon phát hiện và ghi nhận các trường hợp đăng nhập sai mật khẩu

5. Hạn chế của hệ thống mạng

Hạn chế hiện tại của hệ thống:

- Hệ thống mới triển khai trong môi trường lab ảo hóa (VMware), chưa áp dụng trên hạ tầng mạng thực tế
- Chưa triển khai các dịch vụ nâng cao như:

  + DFS (Distributed File System) để đồng bộ dữ liệu

  + WSUS để quản lý cập nhật tập trung

  + Certificate Services (CA) cho xác thực và bảo mật hệ thống

- Chưa tích hợp với Cloud (Azure AD / Azure Hybrid)
- Chưa triển khai Backup & Disaster Recovery cho Domain Controller

- Số lượng user, OU, GPO còn ở mức mô phỏng cho doanh nghiệp nhỏ
- Chưa có hệ thống monitoring (theo dõi log, hiệu năng, cảnh báo)

6. Hướng phát triển và nâng cấp trong tương lai

- Trong tương lai, hệ thống sẽ cần phải nâng cấp để phù hợp với yêu cầu mới của doanh nghiệp và công nghệ hiện đại ngày càng mở rộng:

+ DFS + DFS Replication cho file server

+ WSUS để quản lý cập nhật Windows tập trung

+ Xây dựng Domain Controller dự phòng nâng cao kết hợp Backup AD và Restore và Disaster Recovery

+ Tích hợp Azure AD Hybrid Đồng bộ user on-premise lên cloud

+ Áp dụng Security nâng cao: báo cáo chi tiết, mã hóa

+ Triển khai Monitoring & Logging: Event Viewer tập trung, theo dõi DNS,DHCP, AD health

+ Mở rộng mô hình cho doanh nghiệp vừa và lớn