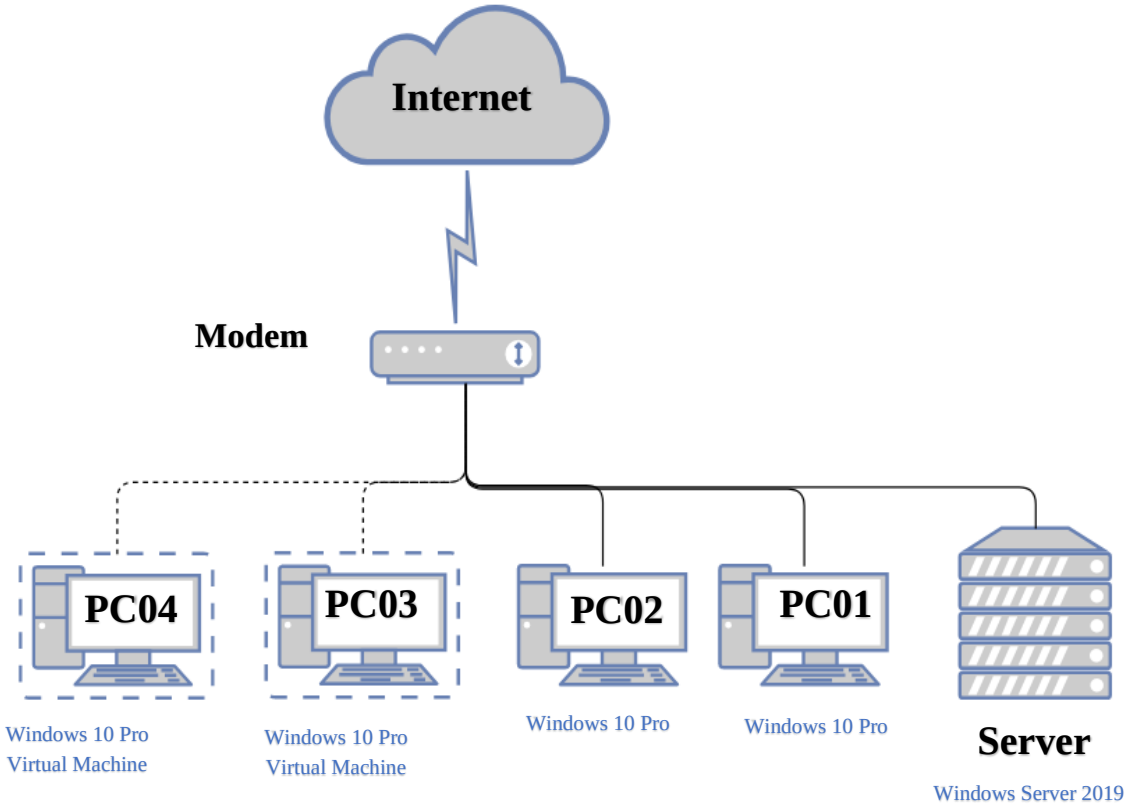
BÀI THỰC HÀNH 2: MÔ HÌNH MẠNG VỪA VÀ NHỎ

1. **Mục tiêu:**

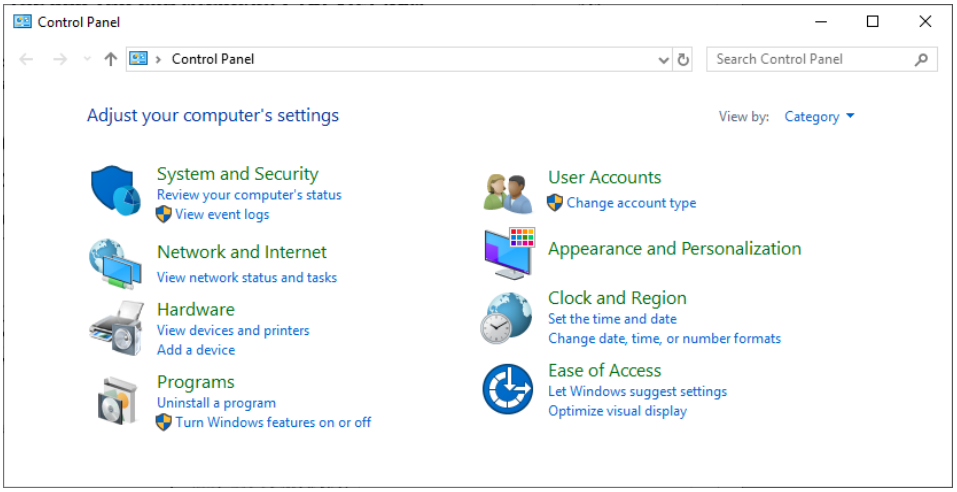
- Tùy chỉnh Local User, Local Group
- Tùy chỉnh Local Group Policy và Local Security Policy
- Phân quyền NTFS

Nội dung thực hành

Mô hình bài Lab:

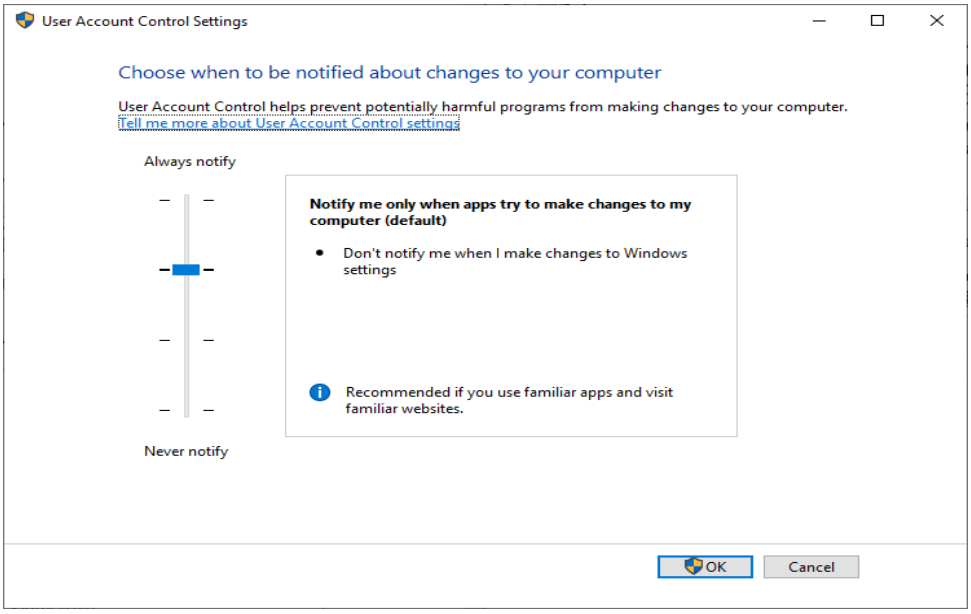


1. Tắt UAC (User Account Control) trên Windows Server 2019



Sinh viên mở Control Panel sau đó mở phần User Accounts, chọn tiếp phần User Account trong màn hình điều khiển. Tiếp đó, sinh viên chọn vào **"Change User Account Control Settings"**

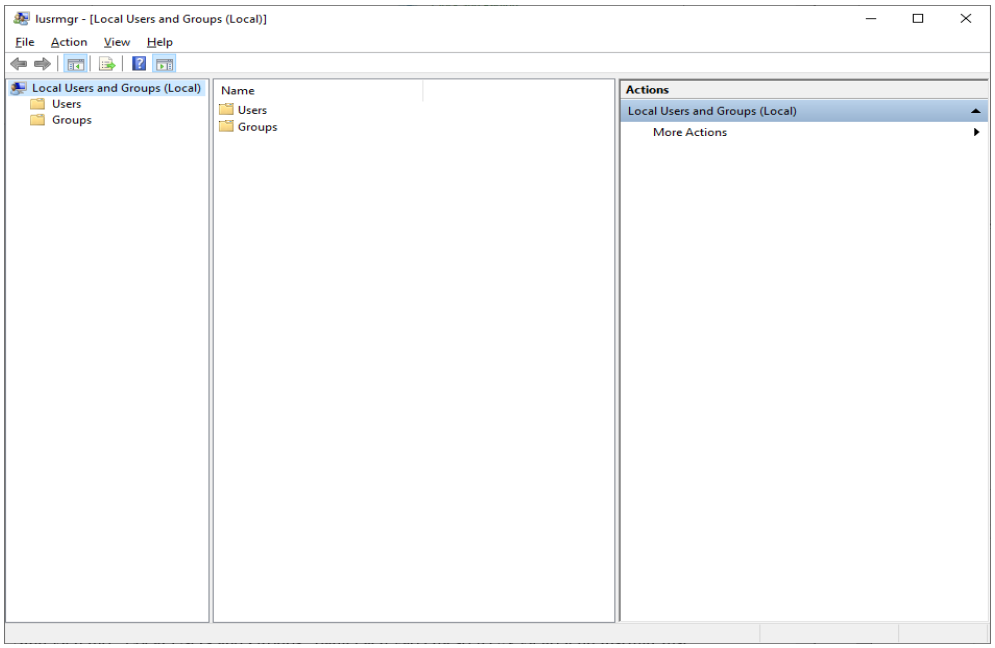
Sinh viên kéo xuống phần thấp nhất và nhấn nút OK.



2. Tạo Local User Account

Sinh viên mở "Local Users and Groups" bằng cách vào cửa sổ RUN và gõ lệnh lusrmgr.msc

Click phải vào mục User → chọn New User để tạo người dùng mới.

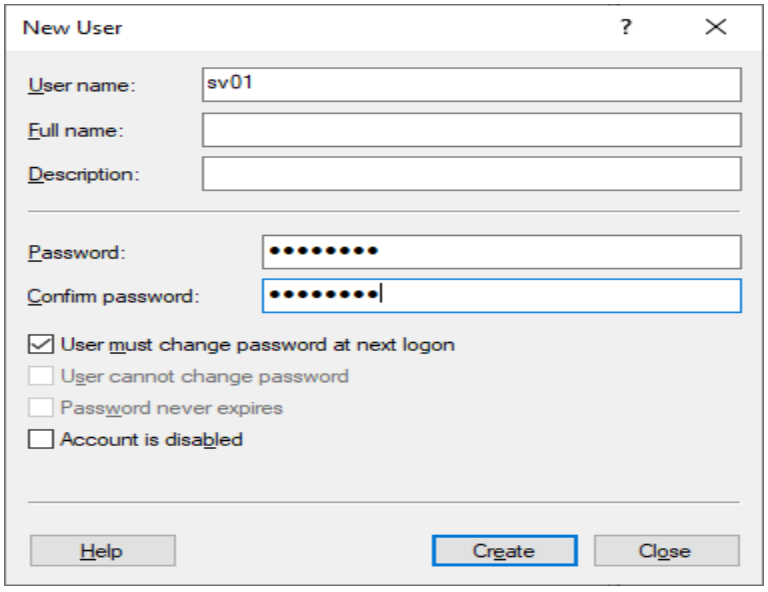


Sinh viên điền các thông tin sau:

Username: sv01

Password và Confirm password: P@ssw0rd

Sau đó nhấn nút Create



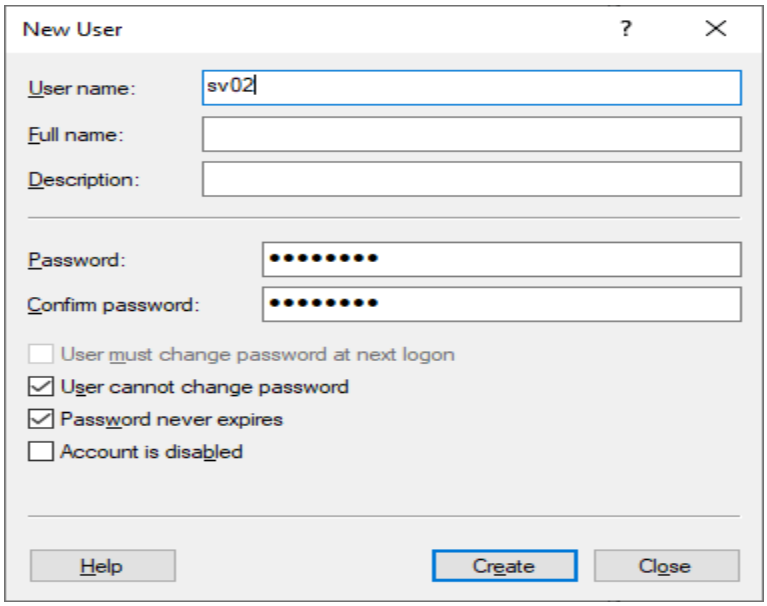
Tương tự phần trên, sinh viên tạo tài khoản người dùng như sau:

Username: sv02

Password và Confirm password: P@ssw0rd

Bỏ check tùy chọn "User must change password at next logon" và chọn 2 tùy chọn như hình dưới.

Sau đó nhấn nút Create



Sau khi tạo, sinh viên tiến hành logout tài khoản và login bằng từng tài khoản sv01 và sv02 và nêu sự khác nhau viết vào báo cáo bài lab cuối buổi.

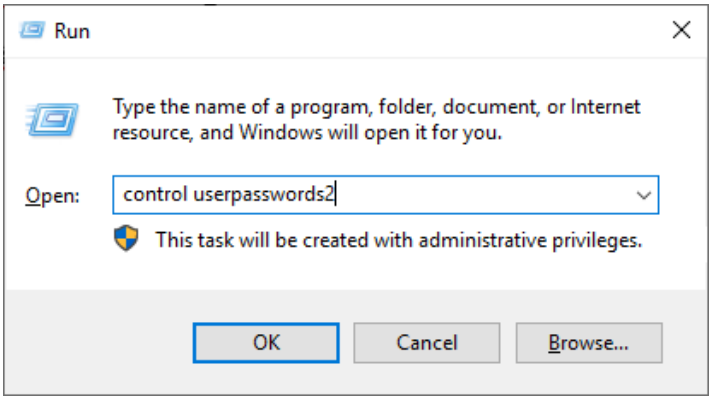
Tiếp theo, đăng nhập bằng tài khoản sv01, truy xuất vào Folder C:\Users\sv01, thư mục này chứa tất cả profile của tài khoản sv01. Hãy chụp hình Profile của tài khoản sv01 để viết báo cáo.

Tiếp theo sinh viên dùng tài khoản sv01 truy xuất vào Folder C:\Users\Administrator và nêu nhận xét.

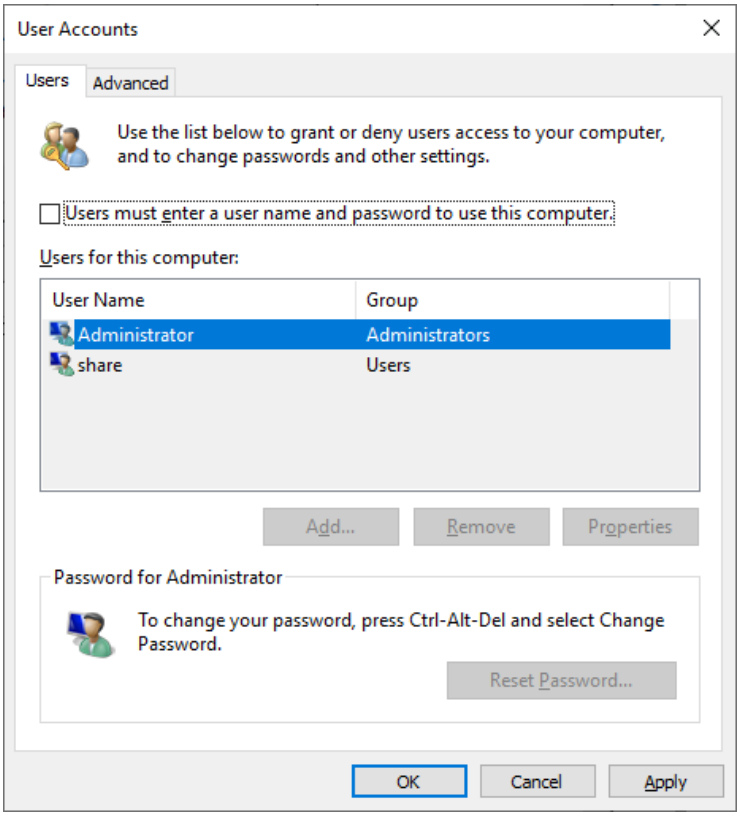
3. Cấu hình Log on tự động bằng account định sẵn.

Logon tự động là cách thức cấu hình hệ điều hành tự động sử dụng tài khoản định sẵn đăng nhập vào hệ điều hành khi khởi động.

Để thiết lập mở hộp thoại RUN gõ control userpasswords2



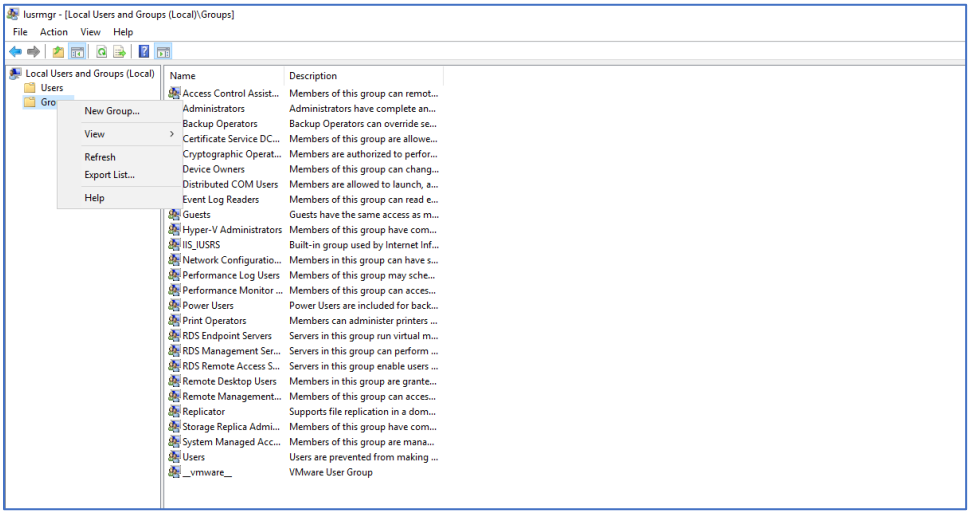
Bỏ check ở ô "Users must enter a user name and password to use this computer" → OK.



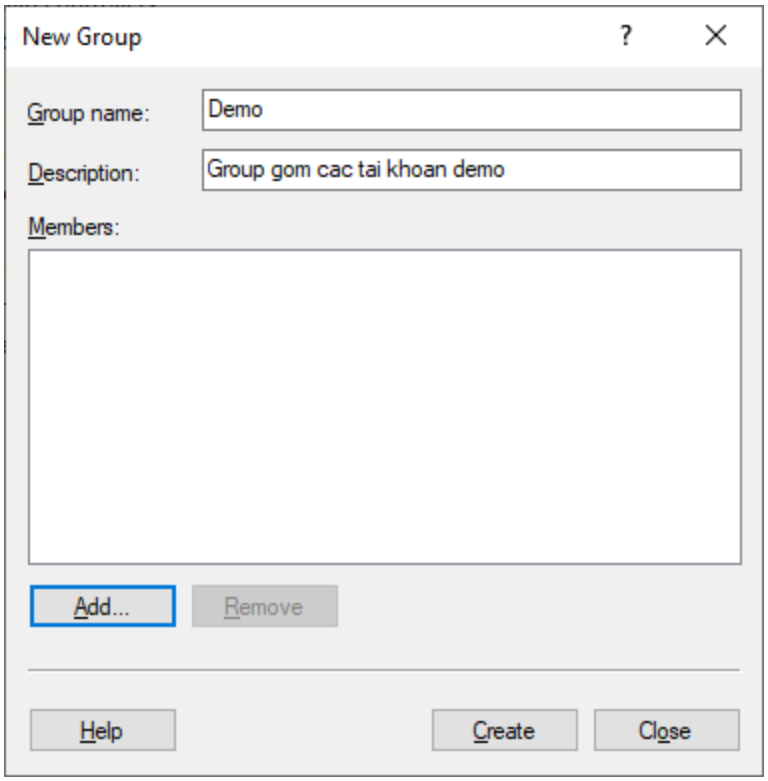
Chọn tài khoản mà muốn sử dụng để đăng nhập tự động, khi chọn phải nhập mật khẩu để lưu. Sau đó sinh viên thực hiện khởi động lại máy ảo để kiểm tra tính năng.

4. Tạo Local Group Account

Chọn mục Group trong Local Users and Groups và click phải chọn New Group



Sinh viên tạo group với tên Demo để thử nghiệm tính năng, sau đó thêm các user sv01, sv02 và Administrator vào group này.



Sinh viên tìm hiểu vài trò và tính năng của các group sau đây và viết vào báo cáo thực hành:

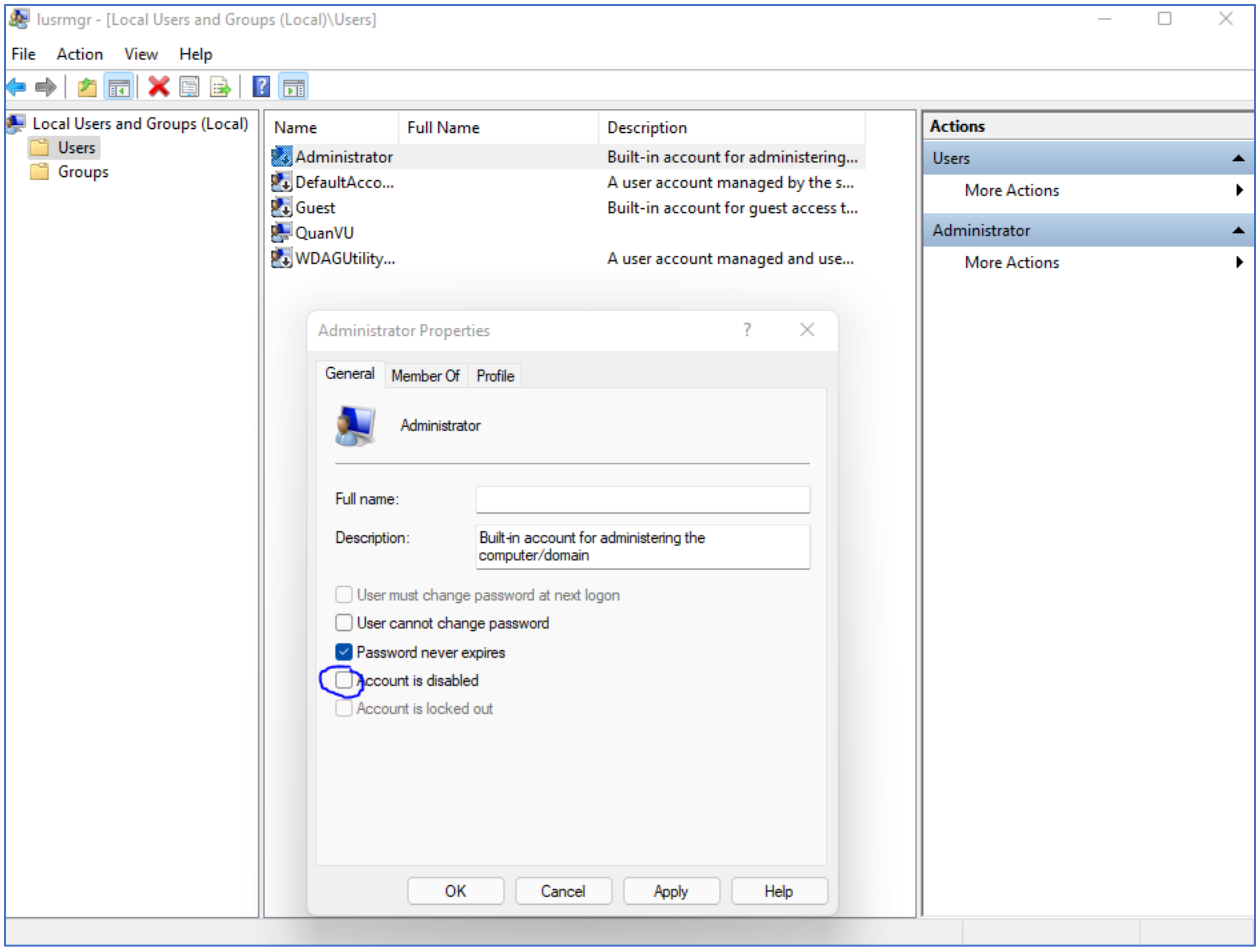
- Remote Desktop Users
- Users
- Administrators
- IIS_IUSRS

Để chuyển đổi tài khoản, sinh viên có thể sử dụng tổ hợp phím Ctrl + Alt + Delete với các tính năng sau:

- Lock: Khóa máy tính
- Switch User: Chuyển đổi môi trường làm việc của user khác mà không tắt phiên hiện tại.
- Sign out: Chuyển đổi môi trường làm việc của user khác và tắt phiên hiện tại.
- Task Manager: xem thông số hiệu năng của máy tính.

5. Hiệu chỉnh trên các Windows cho Client (Windows 10 Pro, ProN …)

Đối với Windows 10 sinh viên tiến hành bật tài khoản Administrator trong Local Users and Groups. Mặc định tài khoản Administrator trên các hệ Windows không phải phiên bản dành cho Server, tài khoản Administrator sẽ được tắt mặc định vì lý do bảo mật. Sinh viên bật tài khoản bằng cách vào cửa sổ RUN gõ lệnh lusrmgr.msc, chọn tài khoản Administrator, bỏ chọn Account is disabled → OK.



Các tùy chọn khác:

Password never expires: mật khẩu của người dùng không bao giờ hết hạn.

Account is diabled: Tắt hiệu lực của tài khoản, hay nói cách khác vô hiệu hóa Account.

Account is locked out: Account sẽ bị khóa tạm thời.

Sinh viên cấu hình tài khoản Administrator logon tự động với hướng dẫn nêu ở mục 3.

6. Local Policy

Local Policy bao gồm các chính sách trên máy cục bộ, các chính sách này tác động trực tiếp đến tính năng của hệ điều hành ví dụ như tắt/bật các dịch vụ, tác vụ, hay triển khai phần mềm…

Trong local policy gồm có Computer Configuration và User Configuration:

- Computer Configuration: Chứa cài đặt máy tính cho tất cả người dùng đăng nhập.
- User Configuration: Chứa cài đặt áp dụng cho tài khoản người dùng.

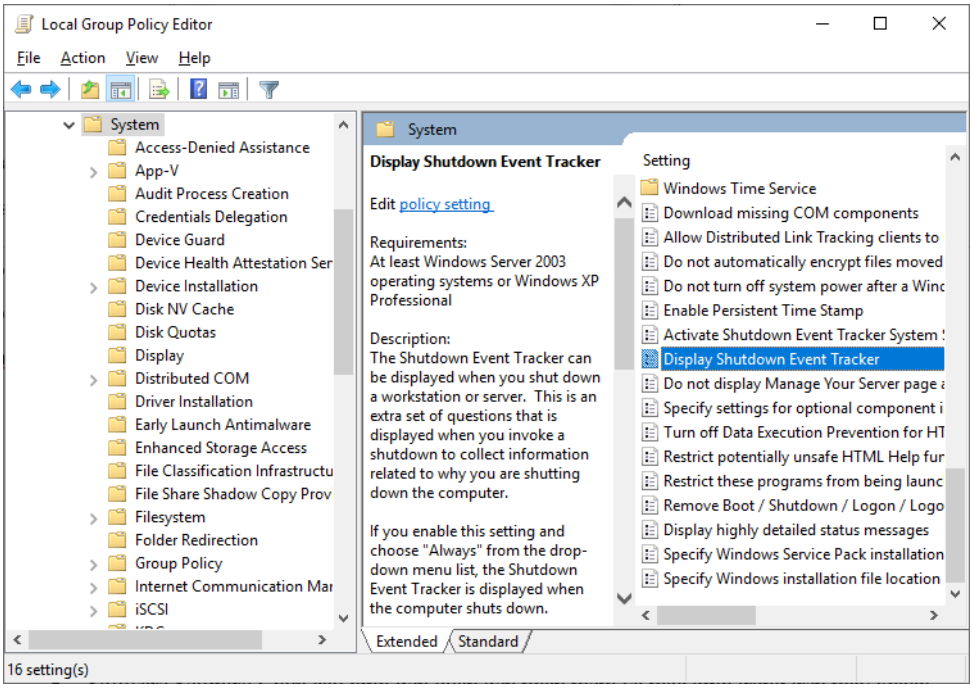
Trong mỗi một thư mục này có một số thư mục khác cung cấp một số cài đặt có sẵn:

- Software Settings: Chứa cấu hình liên quan đến phần mềm và mặc định trống trên máy khách Windows.

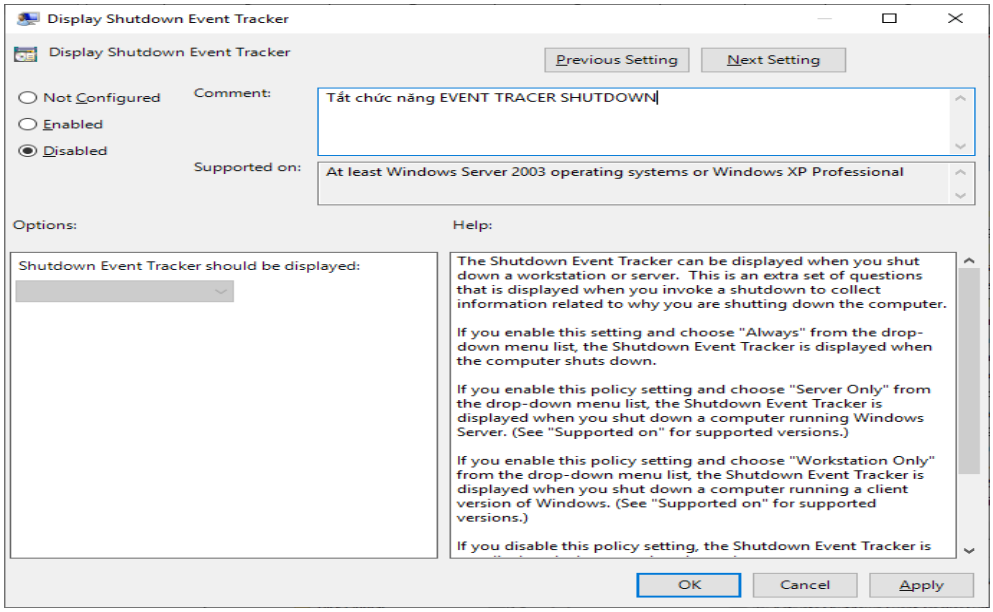
- Windows Settings: Chứa các cài đặt bảo mật và script cho đăng nhập/đăng xuất, khởi động/tắt máy.
- Administrative Templates: Thư mục này chứa các cấu hình dựa trên registry để tinh chỉnh máy tính hoặc tài khoản người dùng một cách nhanh chóng.

Sinh viên mở cửa sổ RUN gõ gpedit.msc để có thể mở Local Computer Policy

Vào mục Computer Configuration chọn Administrative Templates → System. Ở hộp thoại bên phải click đôi vào Display Shutdown Event Tracker.



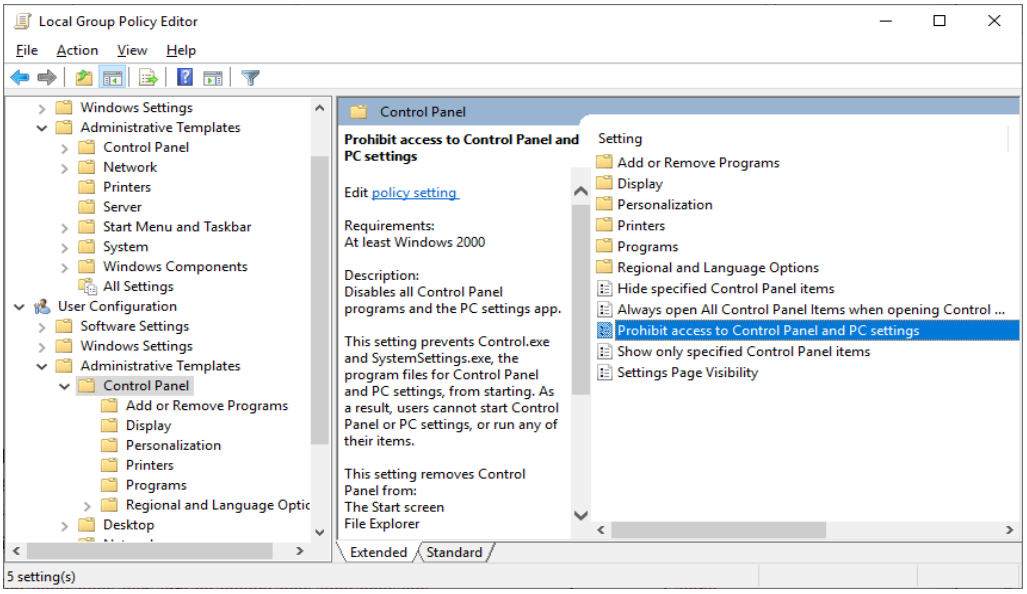
Chọn Disable trong hộp thoại và chọn OK.



Policy này cho phép tắt phần hộp thoại tracker khi nhấn shutdown trên server, sinh viên tiến hành tắt máy thử nghiệm sẽ không thấy hộp thoại xuất hiện. Lưu ý: nếu vẫn thấy có nghĩa là policy chưa áp dụng, sinh viên thực hiện lệnh gpupdate /force trong cmd để cập nhật chính sách.

Hiệu chỉnh Policy User Configuration

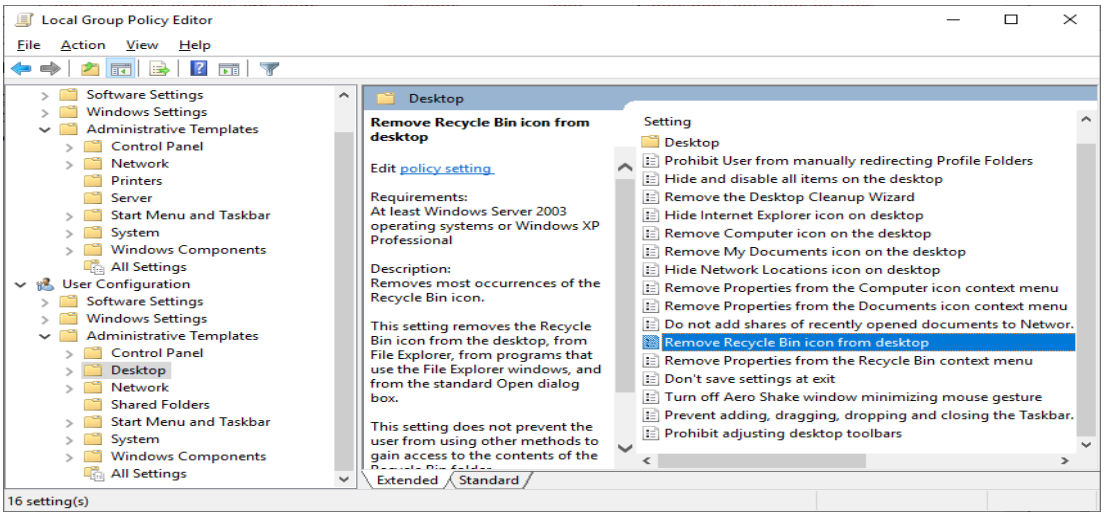
Cũng bằng cách truy cập đã hướng dẫn, sinh viên mở Local User Computer Policy chọn User Configuration → Administrative Templates → Control Panel. Ở khung bên phải nhấn đúp vào Prohibit access to Control Panel and PC Settings.



Sinh viên mở Enable sau đó chọn OK.

Sinh viên mở Control Panel sẽ xuất hiện thông báo lỗi chặn truy cập.

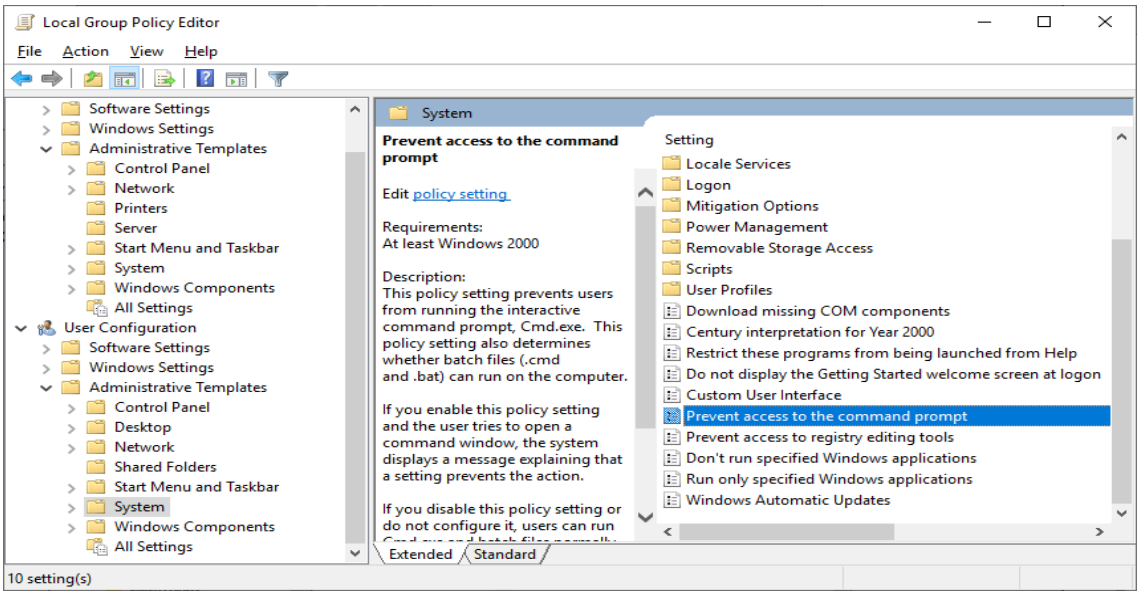
Tiếp tục, sinh viên quay lại Local Group Policy sau đó mở theo đường dẫn sau User Configuration → Administrative Templates → Desktop. Ở khung bên phải, nhấn đúp vào Remove Recycle Bin icon from Desktop → Enabled.



Vào CMD gõ gpupdate /force để cập nhật policy.

Kiểm tra bằng cách Log off và log on lại máy sẽ không còn biểu tượng Recycle Bin trên Desktop.

Tiếp tục, truy cập vào Administrative Templates → System. Chọn Prevent access to the command prompt → chọn Enabled.



Cũng cách thức tương tự như các bước trên, sinh viên sau khi tùy chỉnh thì CMD sẽ không sử dụng được.

Sinh viên tìm cách dùng Policy chặn Registry trên máy tính để viết báo cáo.

7. Hiệu chỉnh Local Security Policy

Password Policy

Logon bằng tài khoản Administrator → Tạo user với mật khẩu là số 1 sẽ xuất hiện lỗi không thể tạo được do không thỏa yêu cầu về độ phức tạp của Password.

- Mở Server Manager vào menu Tools chọn Local Security Policy hoặc gõ lệnh secpol.msc trong RUN.
- Mở Account Policy → Password Policy → Quan sát khung bên phải.
- Enforce password history; Số password hệ thống lưu trữ (thường dùng là 24)
- Maximum password age: Thời gian sử dung tối đa của 1 password (thường dùng là 42)
- Minimum password age: Thời gian sử dụng tối thiểu của 1 password (thường dùng là 1)
- Minimum password length: Độ dài tối thiệu của một password (thường dùng là 7)
- Password must meet complexity requirements: Password yêu cầu phải thiết lập phức tạp (thường dùng Enabled)

Sinh viên chỉnh password policy như sau:

- Password must meet complexity requirements → Chọn Disabled
- Các password policy còn lại chỉnh giá trị về 0 → OK
- Gõ gpupdate /force trong CMD.

Tiến hành kiểm tra: tạo account sv03 với password là số 1 → kết quả thành công.

Account Lockout Policy

- Mở Local Security Policy chọn đường dẫn Account Policies → Account Lockout Policy.
- Quan sát các policy bên phải:
- Account lockout duration: Thời gian account bị khóa.
- Account lockout threshold: Số lần nhập sai password trước khi account bị khóa.
- Reset account lockout counter after: thời gian chuyển bộ đếm về giá trị 0.

Điều chỉnh thông số các policy:

- Account lockout threshold: 3
- Account lockout duration: 5
- Reset ccount lockout counter after 5

Kiểm tra: Đăng nhập password sai 3 lần → không thể đăng nhập tiếp. Chờ sau 5 phút → có thể đăng nhập lại.

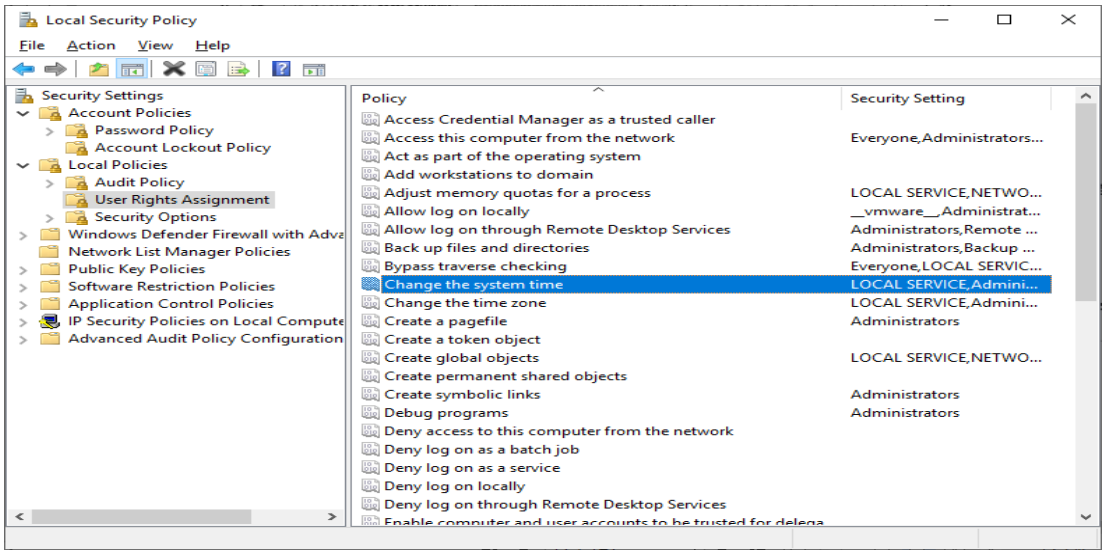
User Rights Assignment

Yêu cầu:

- Logon bằng quyền sv01 → shutdown máy tính → không được
- Thay đổi ngày giờ hệ thống → không được.

Hường dẫn:

- Logon tài khoản Administrator → mở Local Security Policy → Local Lolicies → User Rights Assignment → Cột bên trái : Quan sát thấy 2 policy.
- Change the system time: Cho phép user/group có quyền thay đổi ngày giờ hệ thống.
- Shutdown the system: Cho phép user/group có quyền tắt máy.



Điều chỉnh thông số policy

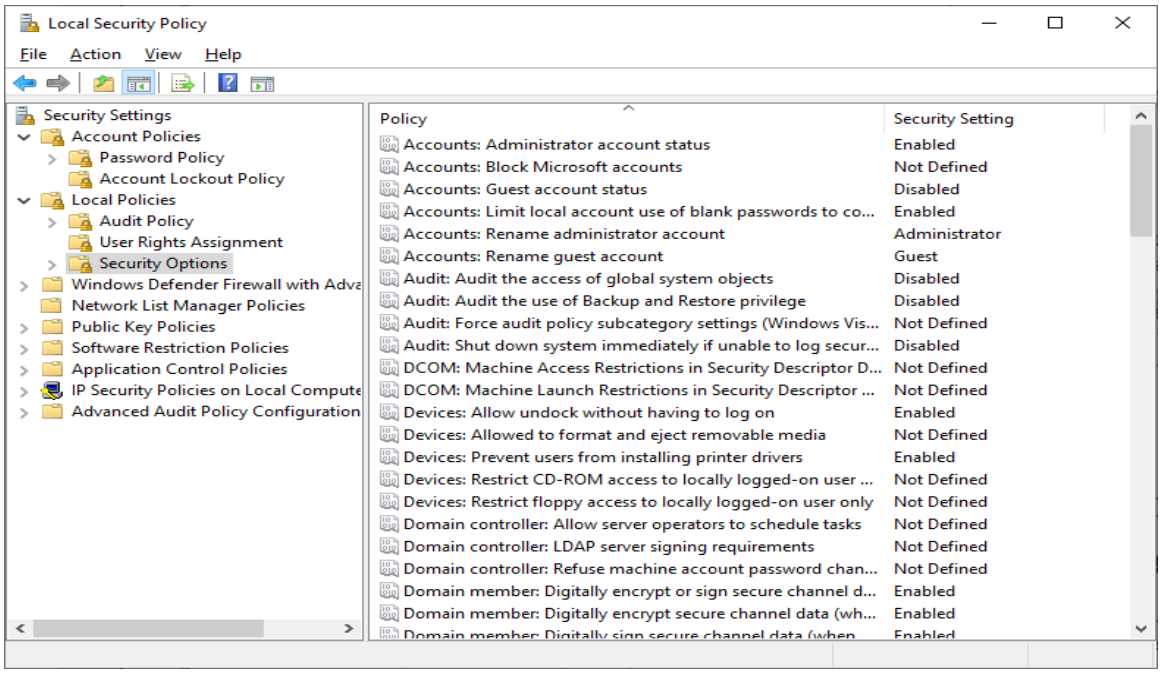
- Change the system time: Đưa group Users vào
- Shutdown the system: Đưa group Users vào

➔ Điều chỉnh xong user sẽ có quyền chỉnh thời gian và tắt hệ thống.

Network Access

Trường hợp 1: Classic

Mở local security policy → Local policy → Security Options → click đúp vào Network Access: chọn Sharing and security model for local account. (Mặc định Windows Server chạy Classic)



a. Classic 2 máy cùng password (thực hiện trên cả 2 máy)

- Đổi password administrator là abc

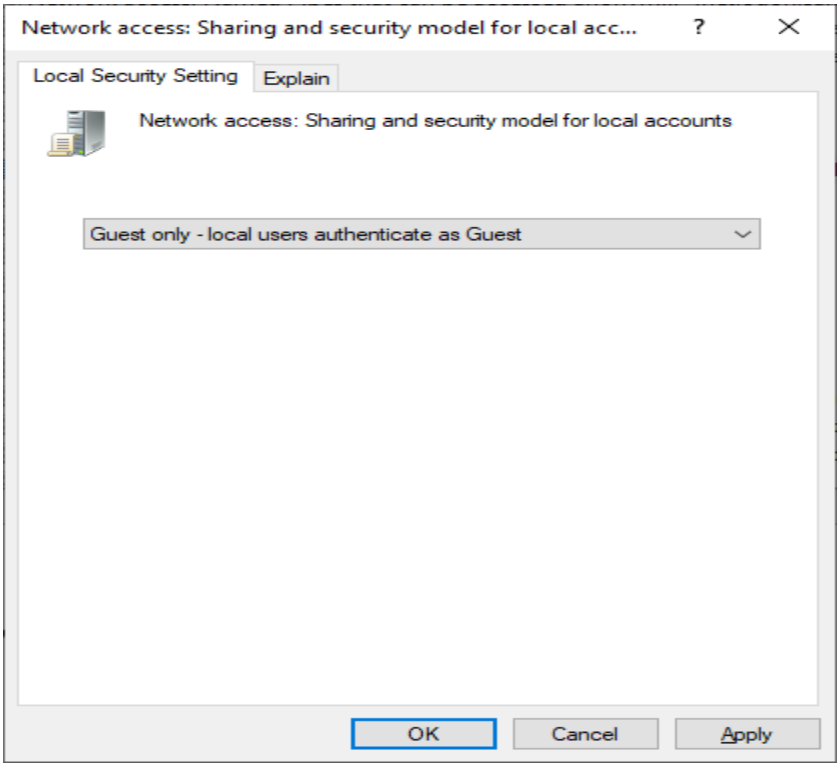
- Thực hiện truy cập bằng URL từ máy PC01 qua máy PC02 và ngược lại
- Tại máy PC01 gõ Windows + R gõ \\PC02 → truy cập thành công mà không bị hỏi username password.
  Ghi chú: Khi truy cập vào PC02 nếu account dùng logon trên máy PC01 trùng username và password với 1 account trên máy PC02 thì khi network access không bị hỏi username và password.

b. Classic 2 máy khác password (thực hiện trên cả 2 máy)
Đổi password administrator trên máy PC01 thành 123 và password administrator trên máy PC02 thành 456 → log on vào PC01 bằng account administrator.
Thực hiện truy cập bằng URL từ máy PC01 sang máy PC02 và ngược lại.
Tại PC01: nhấn Windows + R gõ \\pc02 → hiện thông báo username và password → khai báo username và password sẽ truy cập thành công vào PC02. Và ngược lại.

Trường hợp 2: Guest only (Thực hiện trên cả 2 máy)

Máy PC02: Enable user Guest.

Mở Local Security Policy → Local Policy → Security Options → click đúp vào Network Access : Sharing and Security Model for Local Account → Guest Only – local users authenticate as Guest.



PC01 truy cập vào PC02: không hỏi username, password. Mặc định chứng thực bằng account Guest.

PC02: Disable account Guest. PC01 truy cập vào PC02 sẽ bị hỏi Username và password, tuy nhiên dù nhập account Administrator cũng không thể truy cập được vì chỉ có thể truy cập bằng account Guest (Đã bị Disabled)

PHÂN QUYỀN NTFS

Mục tiêu:

Phân quyền thư mục bằng Standard Permision

Phân quyền thư mục bằng Special Permission

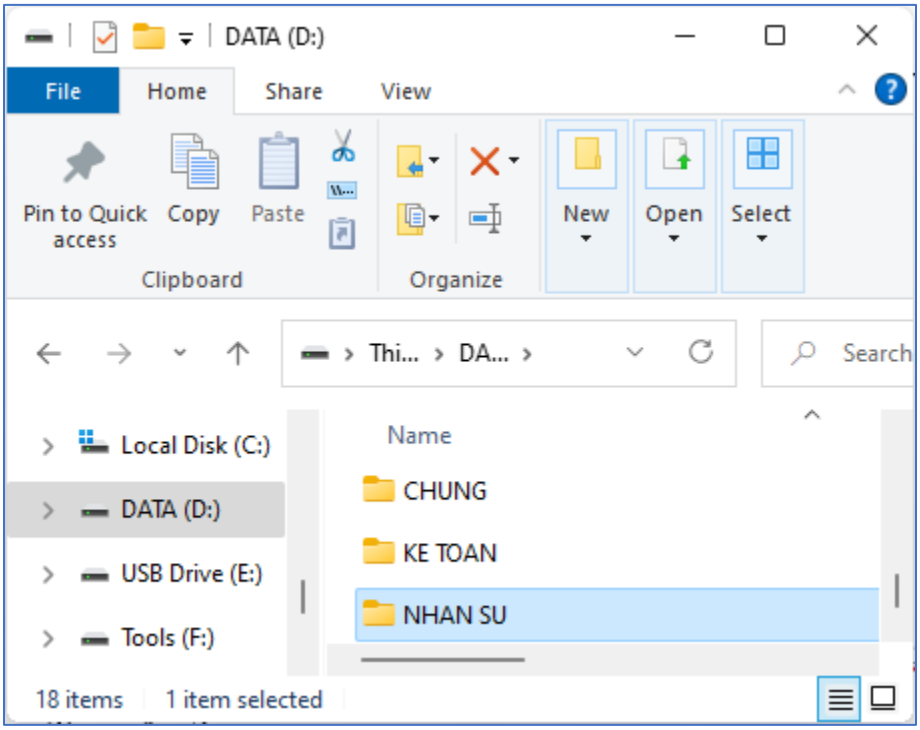
Take OwnerShip

Xét quyền khi di chuyển dữ liệu

Sinh viên chuẩn bị:

Sinh viên sử dụng 1 Windows Server 2019 để thực hiện:

Tạo cây thư mục:



Tạo 2 group: KeToan, NhanSu

Tạo 2 user: KT1, KT2, thêm 2 user này vào Group KeToan

Tạo 2 user: NS1, NS2, thêm 2 user này vào Group NhanSu

Thực hiện:

Phân quyền thư mục bằng Standard Permisson

Phân quyền cho các group như sau:

Trên thư mục Data: Group Ketoan va Nhansu có quyền Read

Trên thư mục Chung: Group Ketoan va Nhansu có quyền Full

Trên thư mục Ketoan:

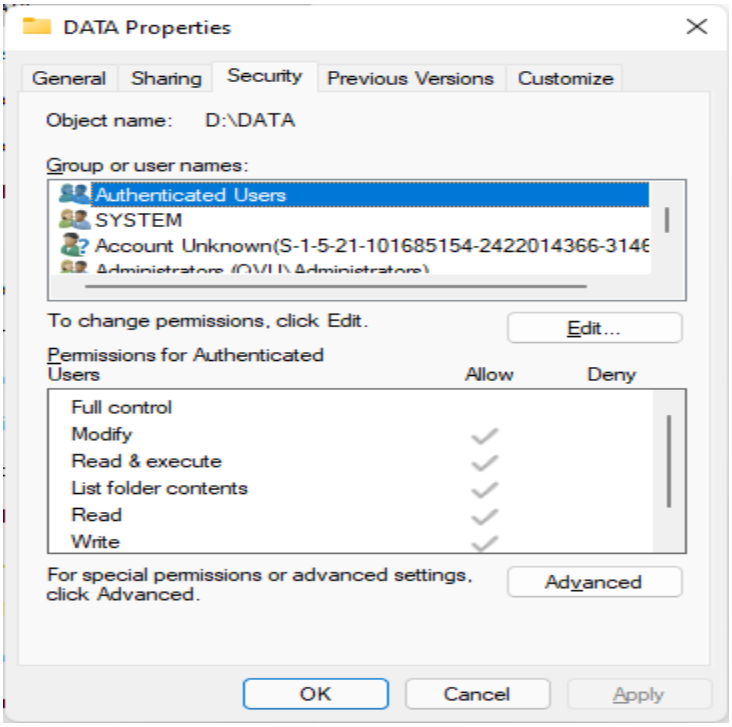
*Group Ketoan có quyền **Full**. Group Nhansu **không có quyền***

Trên thư mục Nhansu:

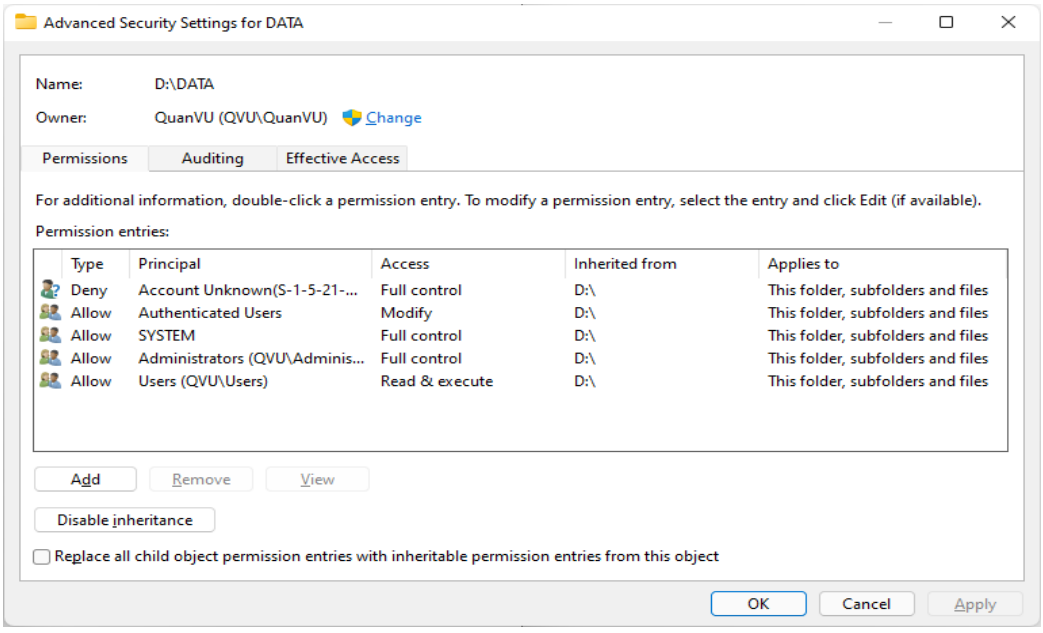
*Group Nhansu có quyền **Full**. Group Ketoan **không có quyền***

Phân quyền thư mục DATA:

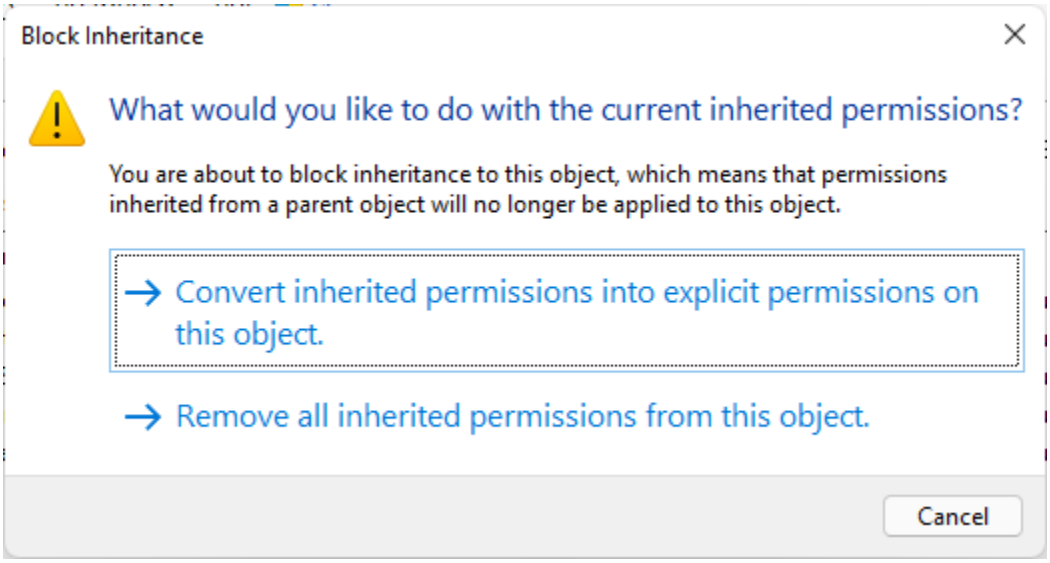
Click phải lên thư mục DATA chọn properties sau đó chuyển qua tab Security chọn Advanced



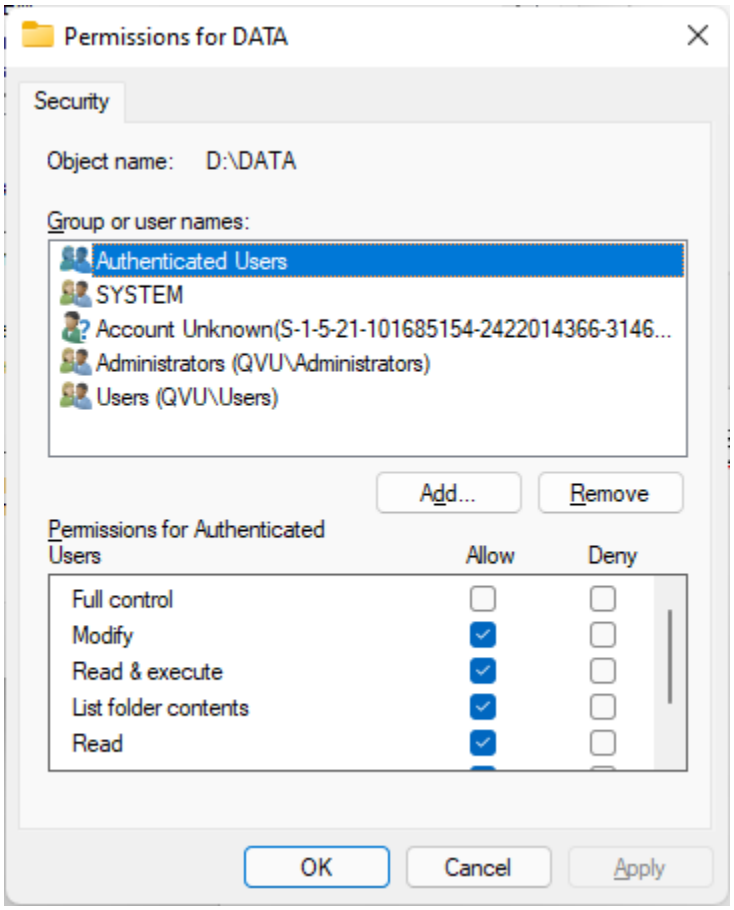
Trong tab permission → chọn Disable Inheritance.



Trong cửa sổ Block Inherited, chọn Convert permissions into explicit permissions on this object → OK.



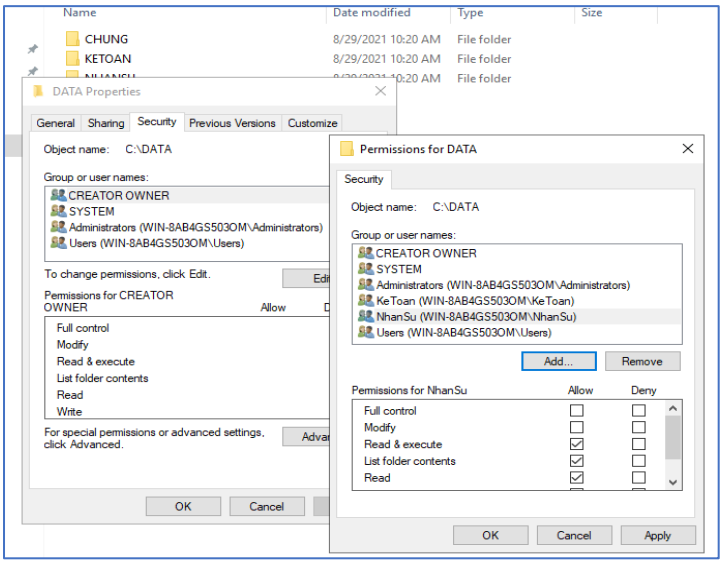
Quay lại cửa sổ Data Properties → Chọn Edit.



Cửa sổ Permissions for Data hiện ra → Nhấn nút Add.

Nhập vào ketoan, nhansu → chọn Check Name xong nhấn OK.

Quan sát hai group Ketoan và Nhansu có 3 quyền Allow đó là: Read & execute, List folder contents, Read.

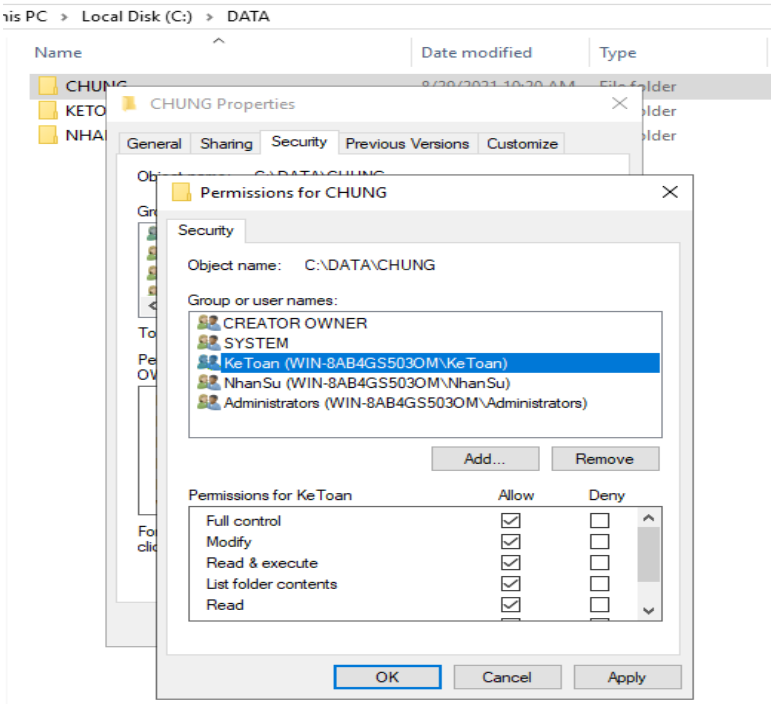


Chọn group Users → Remove → OK.

Thực hiện kiểm tra quyền: logon từng user kt01 và ns01 → mở thư mục C:\Data sẽ truy cập thành công. Tuy nhiên không thể tạo folder tại thư mục Data.

Phân quyền thư mục chung:

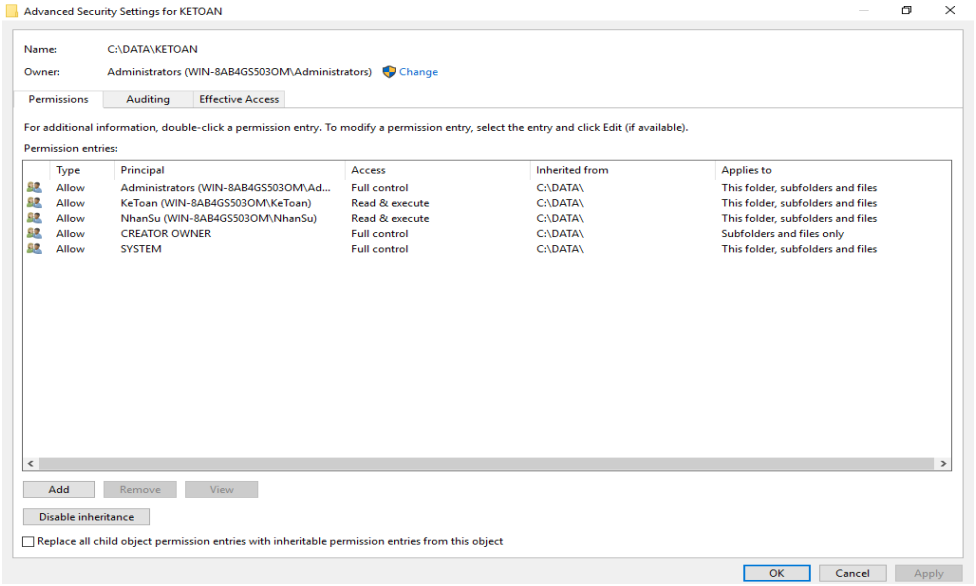
Đăng nhập (logon) tài khoản Administrator chọn Folder Chung, click phải vào folder này chọn Properties, chọn tab Security, chọn Edit → lần lượt chọn group Ketoan va Nhansu → Cấp cho quyền Allow Full Control → OK.



Kiểm tra quyền: lần lượt đăng nhập (logon) tài khoản kt01 và ns02 truy cập vào Folder Chung, sau đó tạo thử file hoặc folder đều thành công.

Phân quyền cho thư mục Kế Toán (KETOAN):

Click phải vào Folder Ke Toan, chọn properties → Tab Security → Advanced → Disable inheritance.

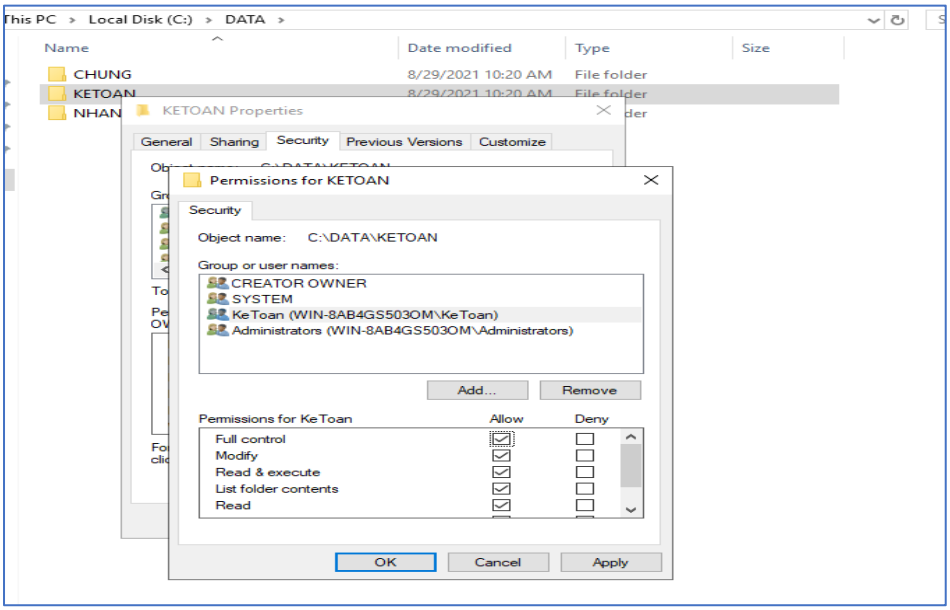


Trong cửa sổ Block Inherited, chọn Convert permissions into explicit permissions on this object → OK.

Cửa sổ KETOAN Properties chọn Edit.

Chọn Group Nhan Su → Remove.

Chọn Group Ke Toan → Allow Full Control.



Kiểm tra: lần lượt logon user kt01 và ns02 vào thư mục kế toán (KETOAN) → user kt01 tạo Folder thành công; user ns02 không thể truy cập vào folder KETOAN.

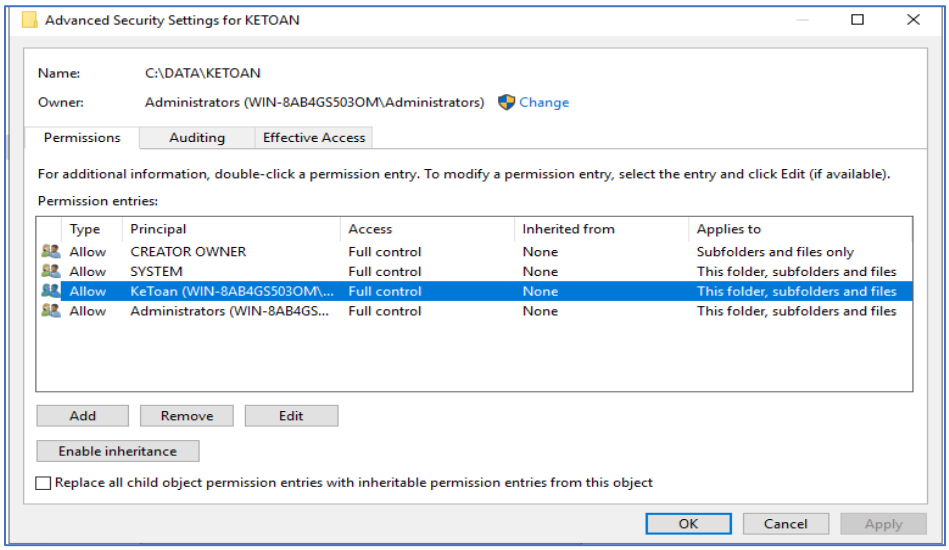
Phân quyền cho thư mục Nhân Sự (NHANSU): (*Sinh viên làm tương tự như phân quyền thư mục kế toán ở trên).*

Phân quyền thư mục bằng Special Permission:

Phân quyền theo yêu cầu: File do user nào tạo ra user đó mới xóa được.

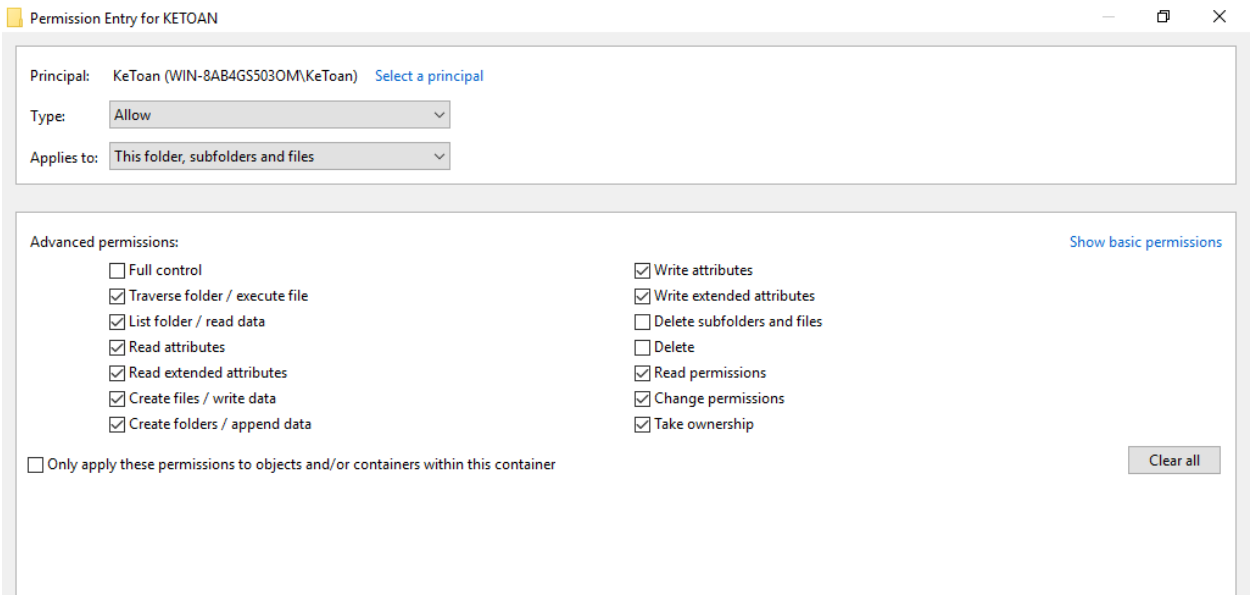
Click phải lên thư mục KETOAN → Properties → Tab security → nhấn vào nút Advanced

Trong tab Permission chọn group Ketoan → chọn Edit.



Trong cửa sổ permission Entry For KETOAN, nhấn vào liên kết Show Advanced Permissions

Ở mục Allow tắt dấu chọn ở ô Delete subfolder and files và Delete.



Kiểm tra quyền: lần lượt logon user KT01 và KT02 tạo file txt tương ứng

User KT01 tạo kt01.txt

User KT02 tạo kt02.txt

Logon bằng KT01 vào xóa kt02.txt → không thành công.

Logon bằng KT02 vào xóa kt01.txt → không thành công.

Take Ownership

- Logon KT01, truy cập vào Folder KeToan → tạo folder KT1File.
- Phân quyền thư mục KT1File → Chọn Properties → Tab Security → Advanced → Diabled Inheritence
- Quay lại chọn Tab Security → chọn Edit → Remove tất cả các Object ngoại trừ KT01 (Full control) → OK.
- Logon user Administrator, truy cập vào folder KT1File bị báo lỗi không thể truy cập được → Click phải vào folder KT1File chọn Properties → Tab Security → chọn Advanced → Mục Owner chọn Change.
- Nhập Administrator xong chọn Check Name → OK.
- Đánh dấu Replace Owner on subcontainers and object → yes → OK.
- Kiểm tra bằng cách click phải vào folder KT1File thấy Administrator đã có quyền Full Control.

Xét quyền di chuyển data trên cùng partition.

Copy:

Trong ổ C tạo folder tên là A

Click phải vào C:\Data chọn copy → mở thư mục A → click phải chọn Paste.

Kiểm tra quyền của thư mục : C:\A\Data → các quyền đã bị thay đổi.

Move:

Trong ổ C tạo folder tên là B

Click phải lên C:\Data chọn cut → mở thư mục B → Click phải chọn paste.

Kiểm tra quyền thư mục C:\B\Data → các quyền không bị thay đổi.

Nhận xét:

- Khi di chuyển dữ liệu trong cùng partition quyền của dữ liệu không thay đổi
- Khi copy dữ liệu vào nơi khác cùng paritition thì quyền của data vừa copy bị thay đổi phụ thuộc vào nơi đến

BÀI TẬP PHÂN QUYỀN NTFS THƯ MỤC

Câu 1: Tạo cây thư mục như sau

Data CTY

PHONG IT

TẠO CÁC FOLDER CON ADMIN, IT01, IT02, IT03

PHONG HC

TẠO CÁC FOLDER CON HC01…. HC10

HC_CHUNG

PHONG NS

TẠO CÁC FOLDER CON NS01…. NS10

NS_CHUNG

PHONG KD

TẠO CÁC FOLDER CON KD01…. KD10

KD_CHUNG

PHONG TC

TẠO CÁC FOLDER CON TC01…. TC10

TC_CHUNG

PHONG TN

TẠO CÁC FOLDER CON TN01…. TN10

TN_CHUNG

QUAN LY

GIAMDOC

PHOGIAMDOC

Phân quyền theo yêu cầu:

a) Mỗi phòng tạo 10 nhân viên theo chữ cái phía sau của phòng và đánh số từ 01 đên 10, riêng phòng QUAN LY tạo GiamDoc và PhoGiamDoc.
b) Mỗi phòng tạo một tài khoản trưởng phòng. Ví dụ trưởng phòng Phong HC là tphc và mật khẩu là P@55w0rd. Tương tự cho các phòng khác.
c) Mật khẩu cho nhân viên từng phòng sẽ khác nhau theo yêu cầu sau:

   Phong HC: Mật khẩu là hc01 cho user hc01; Phòng NS: Mật khẩu là ns01 cho user ns01 và tương tự cho các phòng khác yêu cầu tạo bằng Excel và chụp lại kết quả.

   Thư mục CHUNG của mỗi phòng thì các nhân viên trong phòng đều có quyền Read, Trưởng phòng có toàn quyền.

d) Trưởng phòng TC có quyền Write các phòng NS, KD, TN và Full Control cho phòng TC.
e) Trưởng phòng KD có quyền Read các Folder NS01…NS10 và thư mục NS_CHUNG có quyền Write.
f) Trưởng phòng TN có quyền Read thư mục KD_CHUNG.

g) Nhân viên phòng HC có quyền xem (Read/Write) vào thư mục Chung của các phòng phòng NS, KD, TN và IT.
h) Nhân viên phòng kế toán có quyền (Read/Write) vào tất cả thư mục CHUNG của tất cả các phòng trừ phòng QUANLY
i) Phòng QUANLY có toàn quyền trên tất cả các thư mục của công ty.

Câu 2: Thiết lập ánh xạ thư mục Data CTY thành ổ đĩa M: trên Windows 10. (Thiết lập bằng 2 cách dùng dòng lệnh và dùng Map Network Drive)

Câu 3: Tìm hiểu lệnh phân quyền "**icacls**". Và lệnh Copy.

Bài tập thiết lập Local Group Policy

1. Cấm Task Manager.
2. Cấm Registry
3. Cấm CMD
4. Cấm Control Panel
5. Cấm người dùng cài đặt phần mềm với Policy Windows Installer → Prohibit User Install