TÀI LIỆU HƯỚNG DẪN
THỰC HÀNH THIẾT KẾ MẠNG

Bài 01: Quản lý tài khoản người dùng và nhóm cục bộ *4*

Câu 1 : Thao tác đăng nhập và đăng xuất 6

Câu 2 : Thảo tác đổi mật khẩu của tài khoản 6

Câu 3 : Thao tác xóa tài khoản 6

Câu 4 : Thao tác đổ tên tài khoản 6

Bài 02: Tạo tài khoản người dùng và nhóm trên Active Directory (sử dụng giao diện) *6*

Câu 5 : Làm quen với Active directory users and computers 7

Câu 6 : Nhập các thông tin liên quan đến tài khoản 7

Câu 7 : Truy cập hệ thống máy trạm từ tài khoản trên miền 8

Câu 8 : Thiết lập giờ truy cập vào hệ thống cho tài khoản 8

Bài 03: Tạo tài khoản người dùng và nhóm trên Active Directory sử dụng dòng lệnh (command line) *8*

Câu 9 : Tạo OU bằng tập tin .bat 9

Câu 10 : Tạo một loạt tài khoản bằng .bat 9

Nhắc lại lý thuyết *9*

Mục tiêu bài thực hành *9*

Môi trường thực hành *9*

Câu 11 : Tạo home folder cho một user 10

Câu 12 : Thực hiện kiểm tra ổ đĩa mạng ánh xạ vào home folder 12

Nhắc lại lý thuyết *15*

Mục tiêu bài thực hành *15*

Môi trường thực hành *15*

Câu 13 Tạo home folder cho một user 16

Câu 14 Thực hiện kiểm tra vấn đề bảo mật 16

Câu 15 Giải thích 16

Câu 16 Giải quyết vấn đề 16

Hướng dẫn thực hành *17*

Câu 1 17

Câu 2 17

Câu 3 18

Câu 4 19

Nhắc lại lý thuyết *22*
Mục tiêu bài thực hành *22*
Môi trường thực hành *23*
Câu 5 : Tạo user mới **23**
Câu 6 : Tạo Roaming User Profile **23**
Câu 7 : Kiểm tra ở máy trạm **25**
Nhắc lại lý thuyết *29*
Mục tiêu bài thực hành *29*
Môi trường thực hành *29*
Câu 8 : Tạo preconfigured user profile cho người dùng mới **29**
Câu 9 ..... **36**
Nhắc lại lý thuyết *38*
Mục tiêu bài thực hành *38*
Môi trường thực hành *38*
Câu 10 : Tạo mandagory user profile **39**
Câu 11 Thực hiện kiểm tra **40**
Nhắc lại lý thuyết *42*
Mục tiêu bài thực hành *43*
Môi trường thực hành *43*
Câu 12 Scripts startup và shutdown **43**
Câu 13 Scripts log on và log off **46**
Câu 14 Quyền truy cập Group Policy Editor **46**
Nhắc lại lý thuyết *46*
Mục tiêu bài thực hành *46*
Môi trường thực hành *46*
Câu 15 : Window Explorer **47**
Câu 16 : Start menu and Task bar **49**
Câu 17 : Desktop **49**
Câu 18 : System **49**
Câu 19 : Ctrl + Alt + Del options **49**
Câu 20 : System **50**
Nhắc lại lý thuyết *52*
Mục tiêu bài thực hành *53*
Môi trường thực hành *53*

Câu 21 Mật khẩu phức tạp 54
Câu 22 Chiều dài tối thiểu của mật khẩu 55
Câu 23 Chính sách khóa tài khoản 55
Nhắc lại lý thuyết 56
Mục tiêu bài thực hành 57
Môi trường thực hành 57
Câu 24 : Quyền thay đổi thời gian hệ thống 57
Câu 25 : Shutdown máy tính 58
Câu 26 : Thay đổi tên mặc định của Administrator 59
Nhắc lại lý thuyết 61
Mục tiêu bài thực hành 63
Môi trường thực hành 63
Câu 27 : Cài đặt Group Policy Management Console 63
Câu 28 : Tạo các OU, Users 63
Câu 29 :Ánh xạ ổ đĩa mạng (Mapping Network Drive manually) 64
Câu 30 :Ánh xạ ổ đĩa mạng bằng Log on script 64
Câu 31 : GPO liên kết với một OU 64
Hướng dẫn thực hành 65
Câu 32 : Cài đặt công cụ Group Policy Management Console 65
Câu 33 : Tạo các OU, Users 65
Câu 34 : Ánh xạ ổ đĩa mạng (Mapping Network Drive manually) 65
Câu 35 : Ánh xạ ổ đĩa mạng bằng Log on script 66
Câu 36 : GPO liên kết với một OU 69
Nhắc lại lý thuyết 69
Mục tiêu bài thực hành 71
Môi trường thực hành 71
Câu 37 : Thiết lập chính sách mật khẩu đơn giản 71
Câu 38 : Độ dài tối thiểu cho mật khẩu 71
Câu 39 : Thời hạn sử dụng mật khẩu 72
Câu 40 : Chính sách khóa tài khoản 72
Hướng dẫn thực hành 72
Mục tiêu bài thực hành 73
Môi trường thực hành 73
Câu 41 : Tạo các OU, Users 73

Câu 42 : Mỗi phòng ban có một hình nền riêng 74
Hướng dẫn thực hành *74*
Câu 43 : Thiết lập chính sách hình nền cho phòng Finance: 74
Mục tiêu bài thực hành *79*
Môi trường thực hành *79*
Câu 44 : Tạo các OU, Users 79
Câu 45 : Cấm chạy Internet Explorer cho một OU 80
Câu 46 : Không cho một nhóm chịu ảnh hưởng bởi chính sách 80
Hướng dẫn thực hành *80*
Câu 47 : Tạo các OU, Users 80
Câu 48 Cấm chạy Internet Explorer cho một OU 80
Câu 49 Không cho một nhóm chịu ảnh hưởng bởi chính sách 82

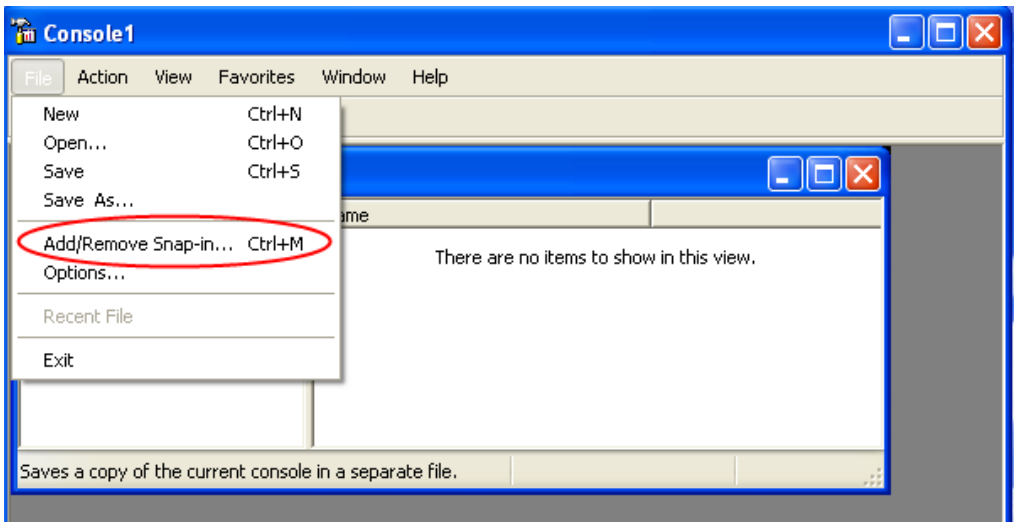
Bài 01: Quản lý tài khoản người dùng và nhóm cục bộ

Nhắc lại lý thuyết:

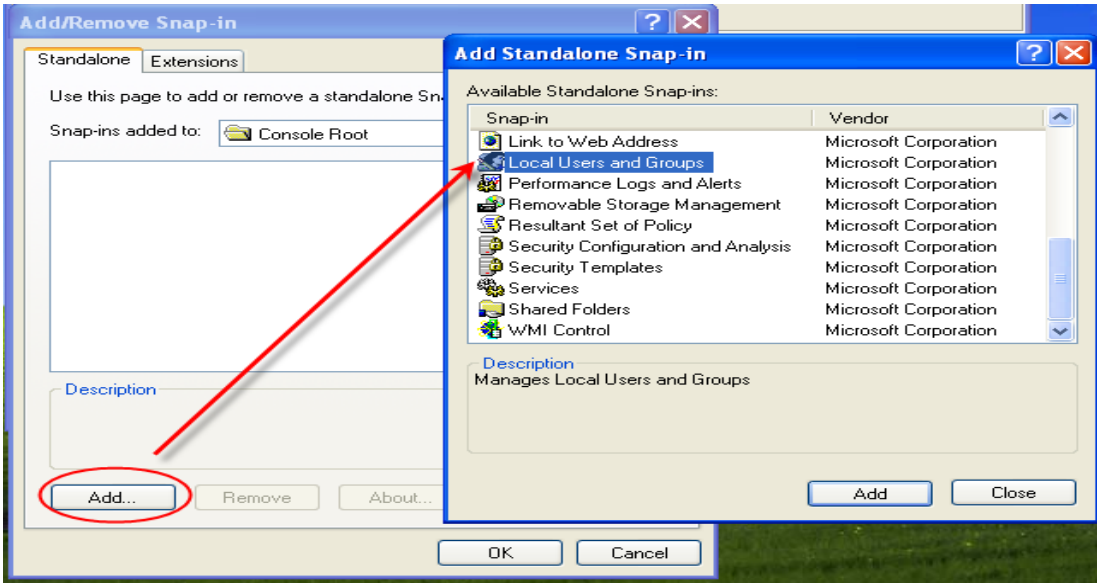
- Muốn tổ chức và quản lý người dùng cục bộ, ta dùng công cụ **Local Users and Groups**.
- Với công cụ này bạn có thể tạo, xóa, sửa các tài khoản người dùng, cũng như thay đổi mật mã.
- Có hai phương thức truy cập đến công cụ Local Users and Groups:
    - Dùng như một **MMC snap-in** (Microsoft Management Console)
    - Dùng thông qua công cụ **Computer Management**.

Hướng dẫn

- **Bước 1:** Vào Start → Run → gõ MMC
- **Bước 2:** Tại giao diện MMC, vào File → Add/Remove Snap-in



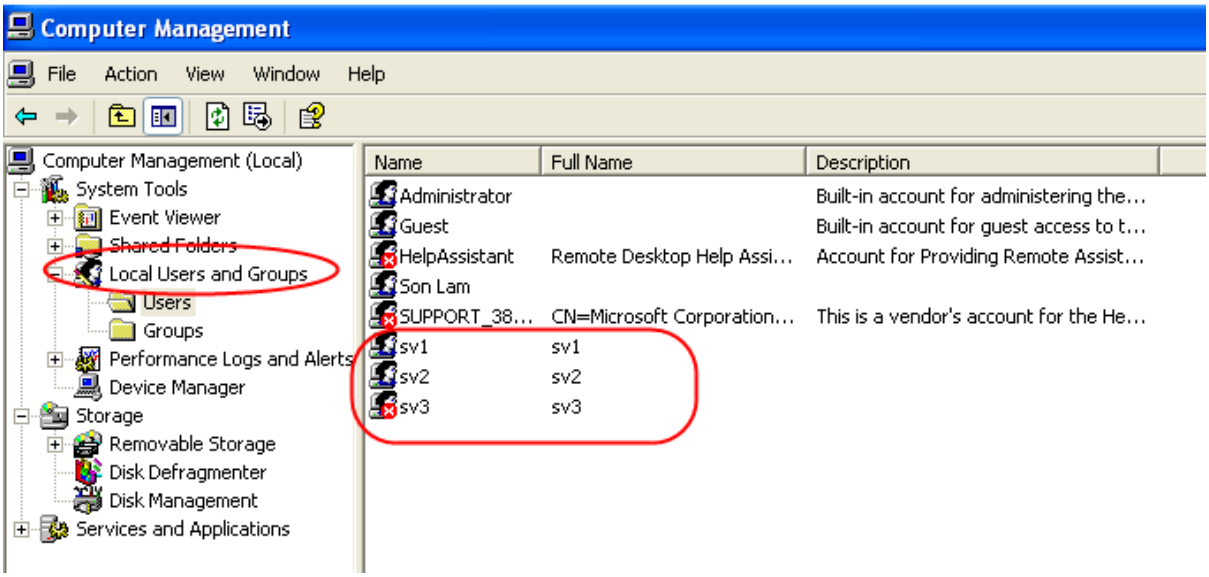
- **<u>Bước 3:</u>** Click vào nút "Add…" và tìm đến mục Local Users and Groups → click "Add"



- **<u>Bước 4:</u>** Để có thể truy cập lại vào lần sau, mà không cần phải thực hiện các thao tác trên nữa, chúng ta nên lưu lại Snap-in này:
  Vào File → Save → Đặt tên cho Snap-in.

Tạo các tài khoản nhóm và người dùng cục bộ sau:

Nhóm	Tên nhóm: **sinh vien**
Người dùng 1	Tên đăng nhập: **sv1** (thuộc nhóm "sinh vien") Mật khẩu: **123** Yêu cầu người dùng phải thay đổi mật khẩu tại lần đầu tiên đăng nhập.
Người dùng 2	Tên đăng nhập: **sv2** (thuộc nhóm "sinh vien") Mật khẩu: **123** Không cho phép người dùng thay đổi mật khẩu
Người dùng 3	Tên đăng nhập: **sv3** (thuộc nhóm "sinh vien") Mật khẩu: **123** Yêu cầu: chưa được kích hoạt tài khoản này.



Câu 1 : Thao tác đăng nhập và đăng xuất

Thực hiện các thao tác bên dưới, và ghi nhận những điều gì xảy ra:

- Thực hiện Log Off, sau đó Log On với tài khoản **sv1**.
- Thực hiện Log Off, sau đó Log On với tài khoản **sv2**.
- Thực hiện Log Off, sau đó Log On với tài khoản **sv3**.

Câu 2 : Thảo tác đổi mật khẩu của tài khoản

Thực hiện các thao tác bên dưới, và ghi nhận những điều gì xảy ra (thao tác nào không thành công?)

- Thực hiện đổi mật khẩu cho tài khoản **sv1**.
- Thực hiện đổi mật khẩu cho **sv2**.

Câu 3 : Thao tác xóa tài khoản

Thực hiện xóa tài khoản **sv1**.

Câu 4 : Thao tác đổ tên tài khoản

Thực hiện đổi tên tài khoản **sv2** thành "**sinhvien**".

Sau đó, Log Off và Log On với tên tài khoản mới này.

Lưu ý: Khi bạn đổi tên tài khoản, mã định danh bảo mật vẫn không thay đổi (**SID**: Security Identifer Definition). Điều đó có nghĩa là: mọi quyền, mọi thông tin thiết đặt cho tài khoản này vẫn như cũ.

Bài 02: Tạo tài khoản người dùng và nhóm trên Active Directory (sử dụng giao diện)

Nhắc lại lý thuyết:

- Để quản lý tài khoản người dùng và nhóm ở cấp miền, ta dùng công cụ **Active Directory Users and Computers**.

(**Lưu ý:** Khác với quản lý tài khoản người dùng và nhóm cục bộ: Local Users and Groups)

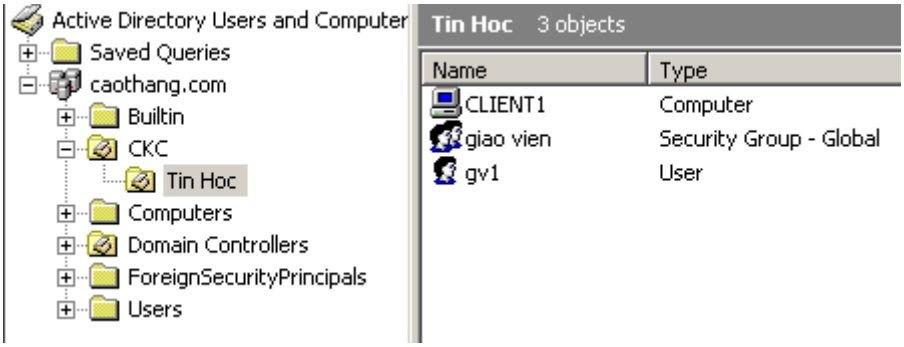
- Để truy cập vào Active Directory Users and Computers:

Start → Administrative Tools → Active Directory Users and Computers.

Câu 5 : Làm quen với Active directory users and computers

Sử dụng giao diện Active Directory Users and Computers, tạo mới:

- OU: tên là **CKC** (thuộc domain caothang.com)
- OU con: **Tin Hoc** (thuộc OU CKC)
- Group: **giao vien** (thuộc OU "**Tin Hoc**")
- User: **gv1** (password: **123abc!** và thuộc group "**giao vien**")



Câu 6 : Nhập các thông tin liên quan đến tài khoản

Nhập các thông tin sau cho gv1:

Thông tin chung (thẻ General)

- First name: Son Lam
- Last name: Vu
- Display name: Vu Son Lam
- Office (văn phòng): Bo mon Tin hoc
- Telephonenumber: 0987654321
- Email: gv1@caothang.com

Thông tin địa chỉ (thẻ Address)

- Street (Đường): Huynh Thuc Khang
- City: Ho Chi Minh
- Country: Vietnam

Thông tin về tổ chức (thẻ Organization)

- Title (chức vụ): Giang vien
- Department (phòng ban): Bo mon Tin hoc
- Company: Cao Thang

Câu 7 : Truy cập hệ thống máy trạm từ tài khoản trên miền

Truy cập vào hệ thống từ máy **Client1**, với tài khoản **gv1**.

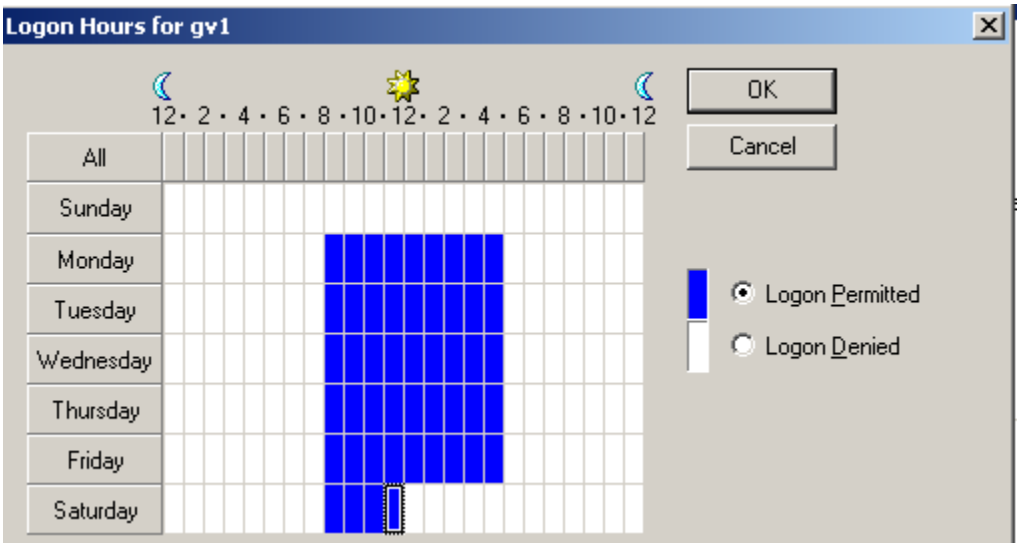
Lưu ý: Máy **Client1** đã được join vào domain **caothang.com** (từ bài tập trước). Nếu chưa join vào, hãy thực hiện join domain.

Câu 8 : Thiết lập giờ truy cập vào hệ thống cho tài khoản

Thiết đặt giờ truy cập vào hệ thống cho tài khoản gv1.

Chỉ cho truy cập vào hệ thống:

- Từ thứ 2 đến thứ 6: **8h** đến **17h**
- Thứ 7: từ **8h** đến **12h**



Vào máy DC1, chỉnh giờ hệ thống vào khoảng 10h tối.

Truy cập lại vào hệ thống từ Client1, với tài khoản gv1.

Xem thông báo lỗi là gì?

Bài 03: Tạo tài khoản người dùng và nhóm trên Active Directory sử dụng dòng lệnh (command line)

Nhắc lại lý thuyết:

- Cú pháp để tạo mới một OU:
  - Ví dụ: thêm OU "CKC" vào domain name: abc.com

    dsadd ou "ou=CKC,DC=abc,DC=com"
  - Ví dụ: thêm OU "DTTH" vào OU "CKC"

    dsadd ou "ou=DTTH,ou=CKC,DC=abc,DC=com"
- Cú pháp để tạo mới một user:
  - Ví dụ: thêm user "hung" vào OU "DTTH", có mật khẩu là "123abc!"

  dsadd user "CN=hung,ou=DTTH,ou=CKC,DC=abc,DC=com" -pwd 123abc!
- Cú pháp để thay đổi/chỉnh sửa một group:

Câu 9 : Tạo OU bằng tập tin .bat

Sử dụng dòng lệnh (tạo file .bat), tạo mới:

- OU: tên là **CKC** (thuộc domain caothang.com)
- OU con: **DTTH** (thuộc OU CKC)
- Group: **sinh vien** (thuộc OU **"DTTH"**)

Câu 10 : Tạo một loạt tài khoản bằng .bat

Sử dụng dòng lệnh (tạo tập tin .bat) để tạo hàng loạt 10 sinh viên, có username là: sv1, sv2, sv3…sv10.

Sử dụng dòng lệnh (tạo tập tin .bat) để add 10 tài khoản sinh viên ở câu trên, vào group "sinh vien".

Bài 4: Home folder

BÀI THỰC HÀNH SỐ 01

Nhắc lại lý thuyết

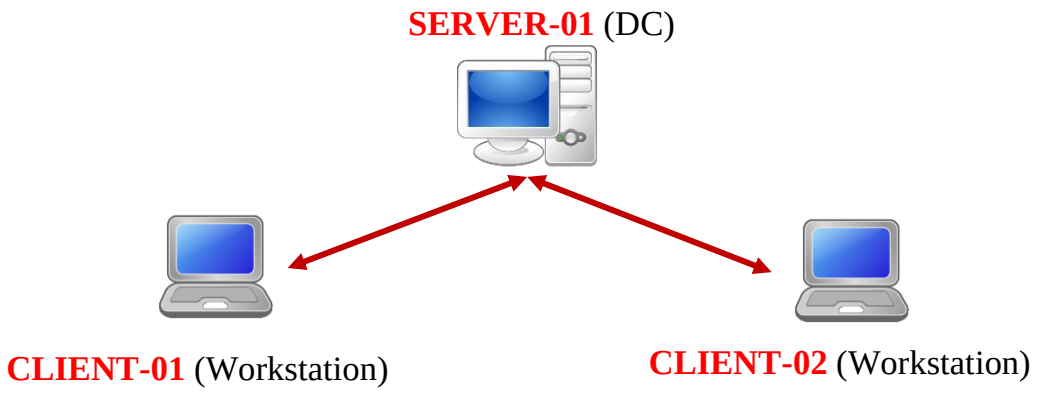
- Home folder là một thư mục trên Server, dùng để lưu trữ dữ liệu cho mỗi người dùng, vì lưu trữ trên Server, nên người dùng có thể lấy được dữ liệu của mình ở các máy trạm khác nhau.

Mục tiêu bài thực hành

- Hiểu cách tạo Home folder cho một user.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

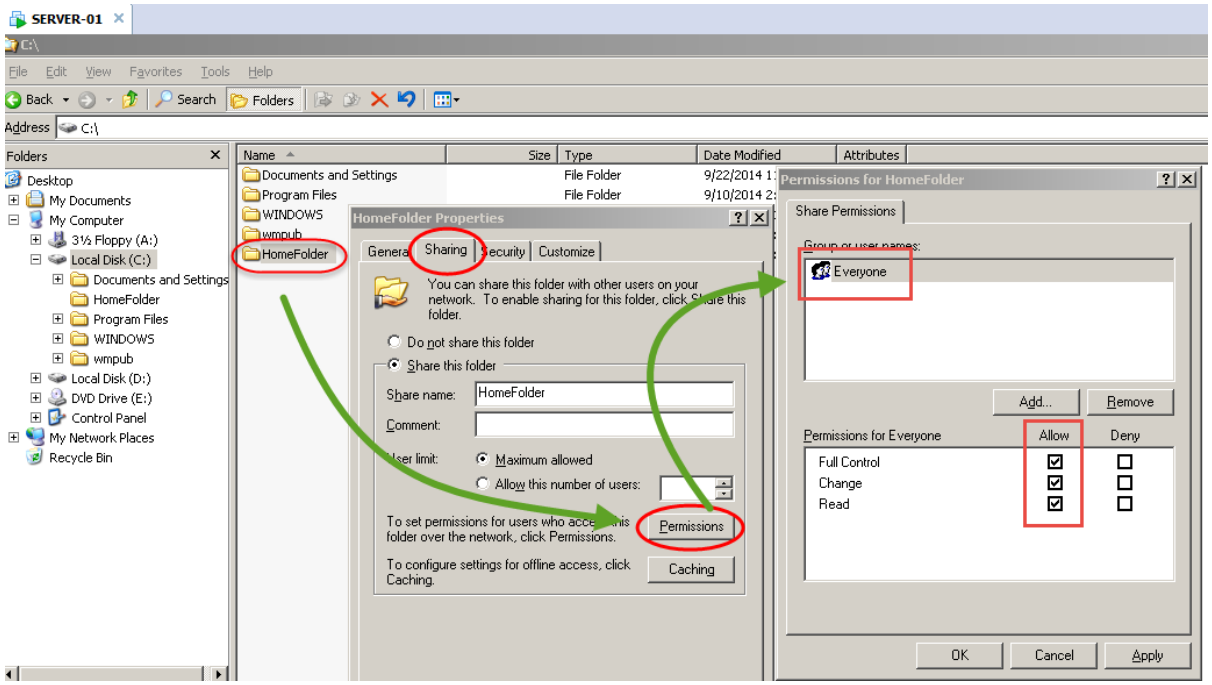
Câu 11 : Tạo home folder cho một user

- Tạo một user mới trên domain **abc.com**:
  - Tên hiển thị: **Nguyễn Văn Hải**
  - Tên đăng nhập: **hai@abc.com**
- Thực hiện tạo Home folder cho user "**hai**".
  (Mỗi user có một thư mục riêng, lưu tại **C:\HomeFolder**, chẳng hạn, user "hai" sẽ có một thư mục là **C:\HomeFolder\hai**)

Hướng dẫn

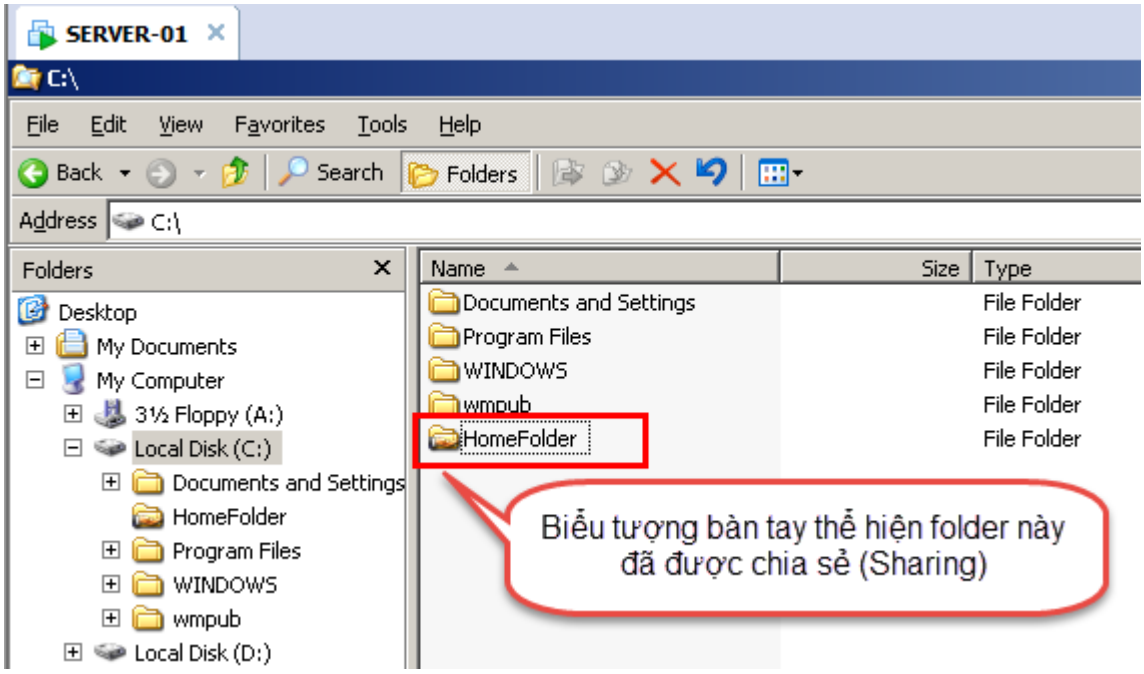
Bước 1:

- Trên máy SERVER-01, tạo một thư mục để làm Home folder cho các user.
  Ví dụ: tạo thư mục tại **C:\HomeFolder**.
- Chia sẻ thư mục này cho Everyone, với quyền Full Control:
  - Nhấp phải vào thư mục "HomeFolder", chọn "**Properties"**
  - Nhấp vào thẻ "**Sharing**"
  - Tại thẻ "**Sharing**", chọn "**Share this folder**"
  - Bấm vào nút "**Permission**" để mở hộp thoại cấu hình quyền cho user
  - Tại cửa sổ "**Permission**", chọn **Everyone**, cấp quyền "**Full Control**"



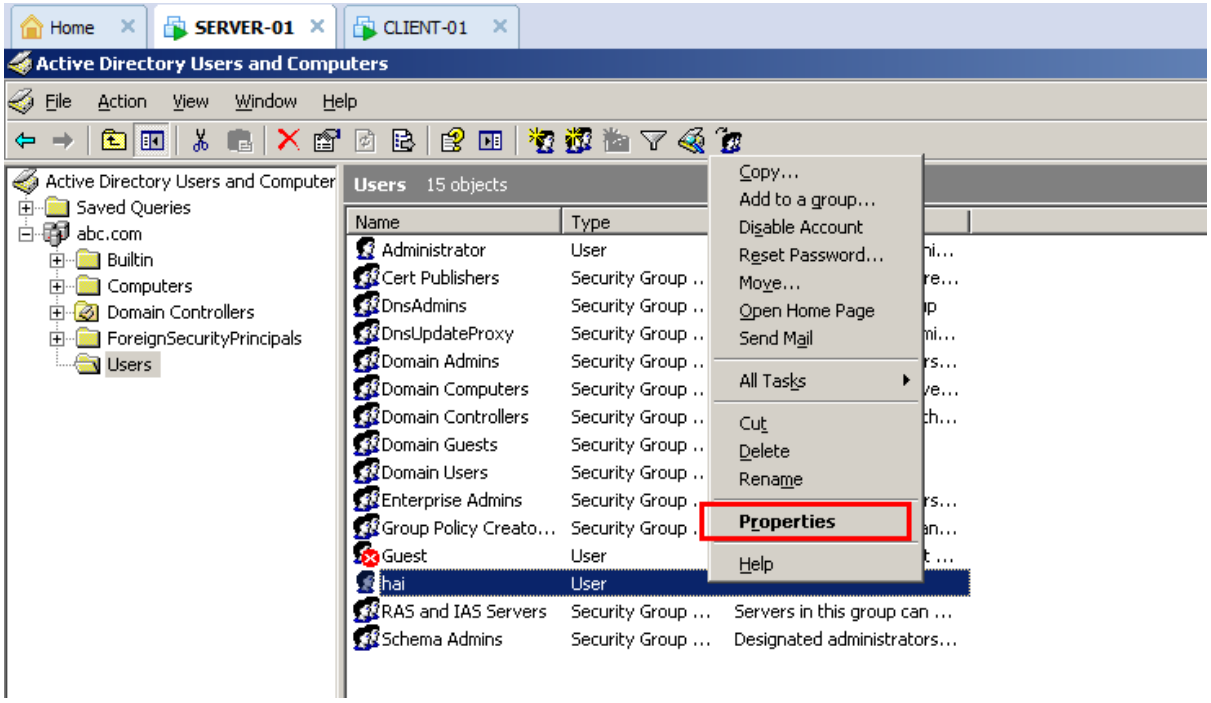
☺

Sau khi thực hiện xong, thư mục "**HomeFolder**" sẽ có biểu tượng hình bàn tay, thể hiện rằng thư mục này đã được chia sẻ.



<u>Bước 2:</u> Cấu hình đường dẫn Home folder cho user

- Vào "**AD Users and Computers**"
- Nhấp phải vào tài khoản "**hai**", chọn lệnh "**Properties**"



- Tại hộp thoại "Properties", bấm vào thẻ "Profile".
- Tại thẻ "**Profile**", ở phần "**Home folder**", chọn "**Connect**":
    - Chọn tên một ổ đĩa mạng sẽ ánh xạ vào đường dẫn Home folder. Ví dụ: chọn ổ đĩa **Z**.
    - Điền vào đường dẫn đến Home folder.
      Ví dụ: **<u>\\server-01\HomeFolder\hai</u>**

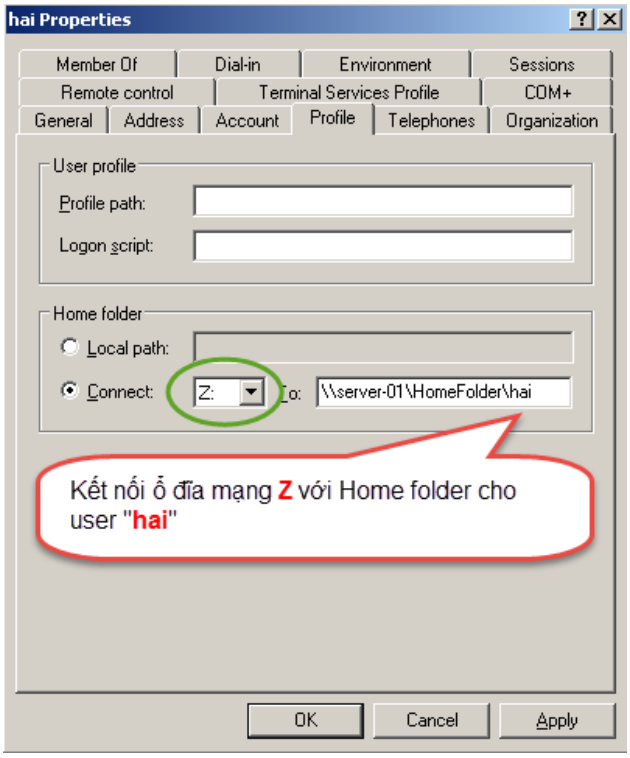
Lưu ý: Chúng ta KHÔNG gõ đường dẫn **C:\HomeFolder** mà phải gõ đường dẫn theo cách truy cập qua mạng: \\server-01\HomeFolder\, trong đó:

Server-01 chính là tên máy server (computer name).

Bạn có thể lấy tên máy tính bằng 2 cách phổ biến sau:

Cách 1: Nhấp phải vào "**My Computer**" → chọn lệnh "**Properties**" → Bấm vào thẻ "**Computer Name**"

Cách 2: Mở cmd, gõ lệnh: **hostname**



☺

Sau khi bấm "**Apply**" hoặc "**OK**", bạn sẽ thấy một thư mục "**hai**" được tạo ngay lập tức ở đường dẫn **C:\HomeFolder**

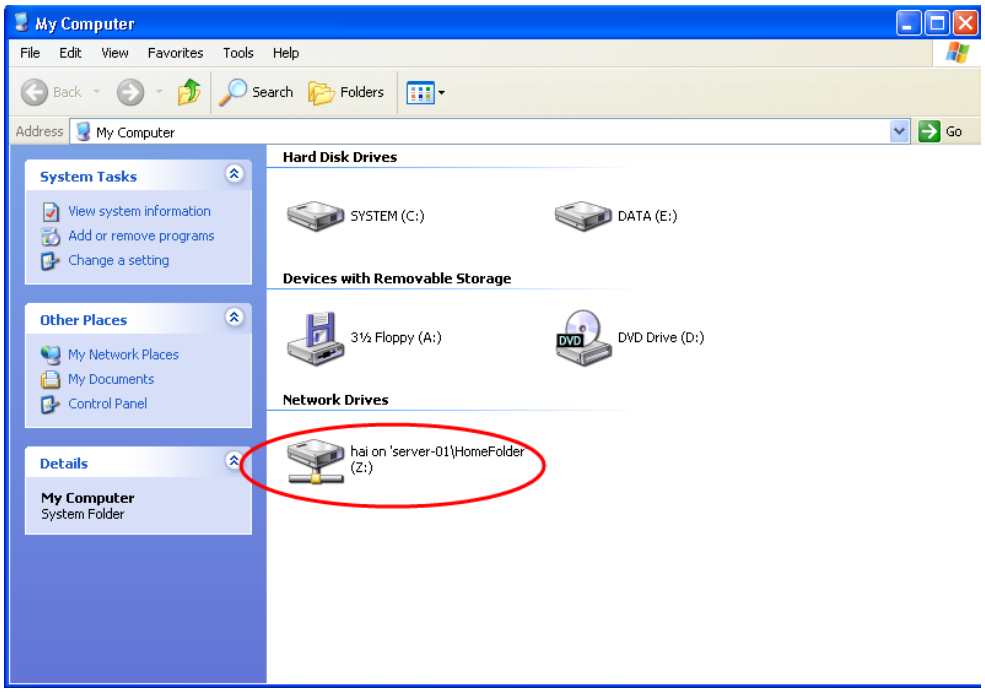
Câu 12 : Thực hiện kiểm tra ổ đĩa mạng ánh xạ vào home folder

- Tại máy trạm **CLIENT-01**, đăng nhập với tài khoản "**hai**" vừa tạo ở trên.
- Kiểm tra xem có **ổ đĩa mạng** nào ánh xạ vào Home folder không?
- Thực hiện tạo một vài files, và kiểm tra trên server, thư mục "HomeFolder" có những files này hay không?
- Tại máy trạm **CLIENT-02**, cũng đăng nhập với tài khoản "**hai**".
- Kiểm tra xem, liệu người dùng này có lấy được dữ liệu của mình trên thư mục "HomeFolder" không?

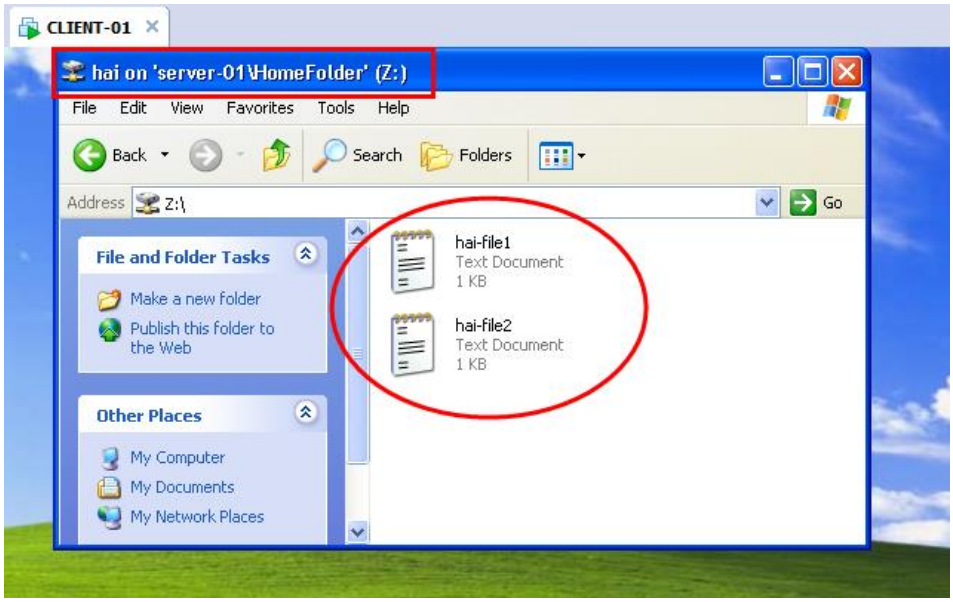
Hướng dẫn

- Tại máy trạm **CLIENT-01**, đăng nhập với tài khoản "**hai**"

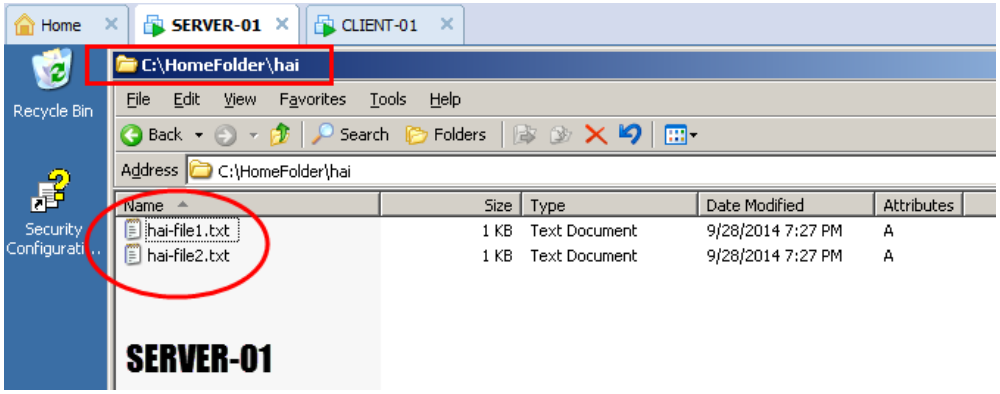
- Ổ đĩa mạng **Z** xuất hiện ở "**My Computer**"



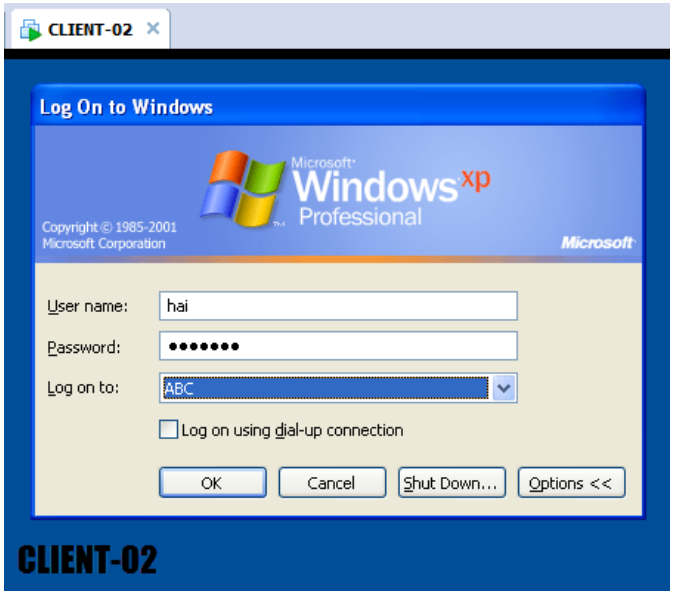
- Thực hiện tạo vài files trong ổ đĩa mạng này (tại máy trạm)



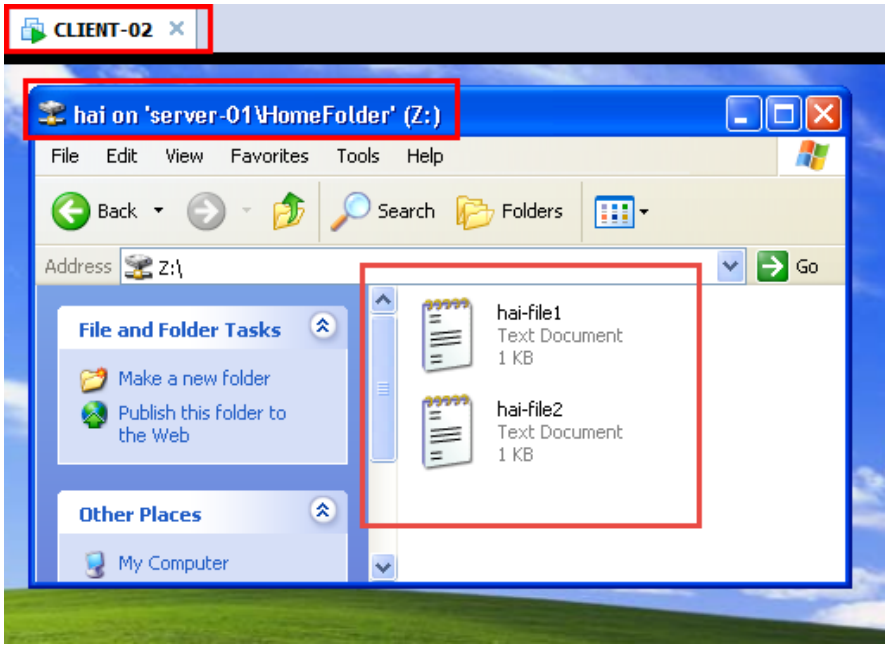
- Tại máy **SERVER-01**, kiểm tra các files:



- Tại máy CLIENT-02, đăng nhập với tài khoản "**hai**"



- Truy cập được vào HomeFolder, và xem được dữ liệu của mình



Bài 4: Home folder

BÀI THỰC HÀNH SỐ 02

Nhắc lại lý thuyết

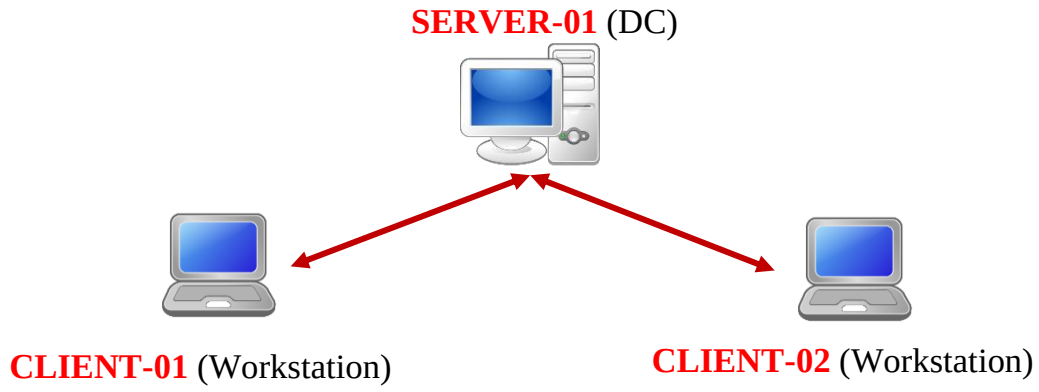
- Home folder là một thư mục trên Server, dùng để lưu trữ dữ liệu cho mỗi người dùng.
- Vì lưu trữ trên Server, nên người dùng có thể lấy được dữ liệu của mình ở nhiều máy trạm khác nhau.

Mục tiêu bài thực hành

- Hiểu về vấn đề bảo mật trong việc tạo Home folder.
- Tạo được Home folder, sao cho mỗi người dùng sẽ có một thư mục riêng, và không ai có thể xem được dữ liệu của họ (trừ admin)

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

Câu 13 Tạo home folder cho một user

- Tạo một user mới trên domain **abc.com**:
  - Tên hiển thị: **Trần Quốc Hùng**
  - Tên đăng nhập: **hung@abc.com**
- Thực hiện tạo Home folder cho user "**hung**".
  (Lưu tại thư mục **C:\HomeFolder\hung**)

Câu 14 Thực hiện kiểm tra vấn đề bảo mật

- Hùng là một người thích mày mò tìm hiểu, anh ta cố gắng truy cập vào thư mục "HomeFolder" trên Server để lấy dữ liệu của những người khác. Anh ta mở Window Explorer lên, và gõ vào thanh địa chỉ đường dẫn như sau:
  \\Server-01\HomeFolder
  Hãy cho biết, liệu Hùng có xem được dữ liệu của những người khác trên folder này không?

Câu 15 Giải thích

- Nếu Hùng có thể xem được dữ liệu của người khác, hãy giải thích vì sao lại có thể xem được?

Câu 16 Giải quyết vấn đề

- Bạn hãy đưa ra cách giải quyết vấn đề trên, để sao cho: mỗi người dùng có một thư mục riêng trên Server, và không ai có quyền xem dữ liệu của mình (trừ admin)

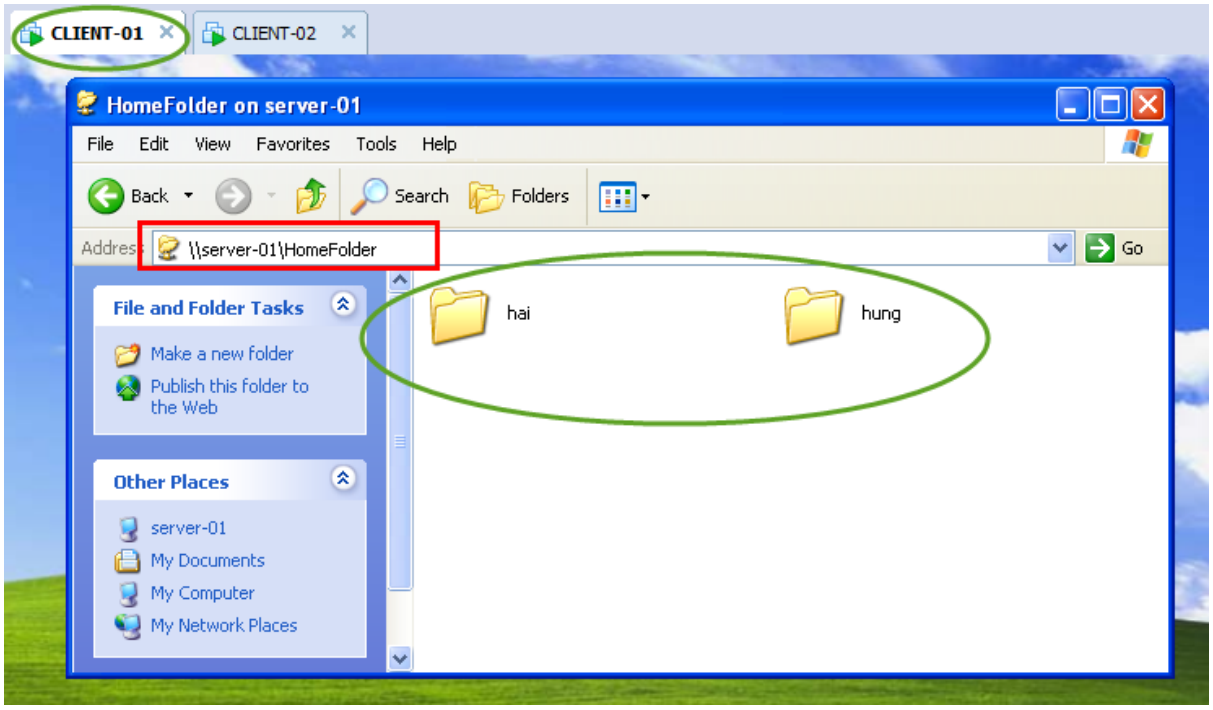
Hướng dẫn thực hành

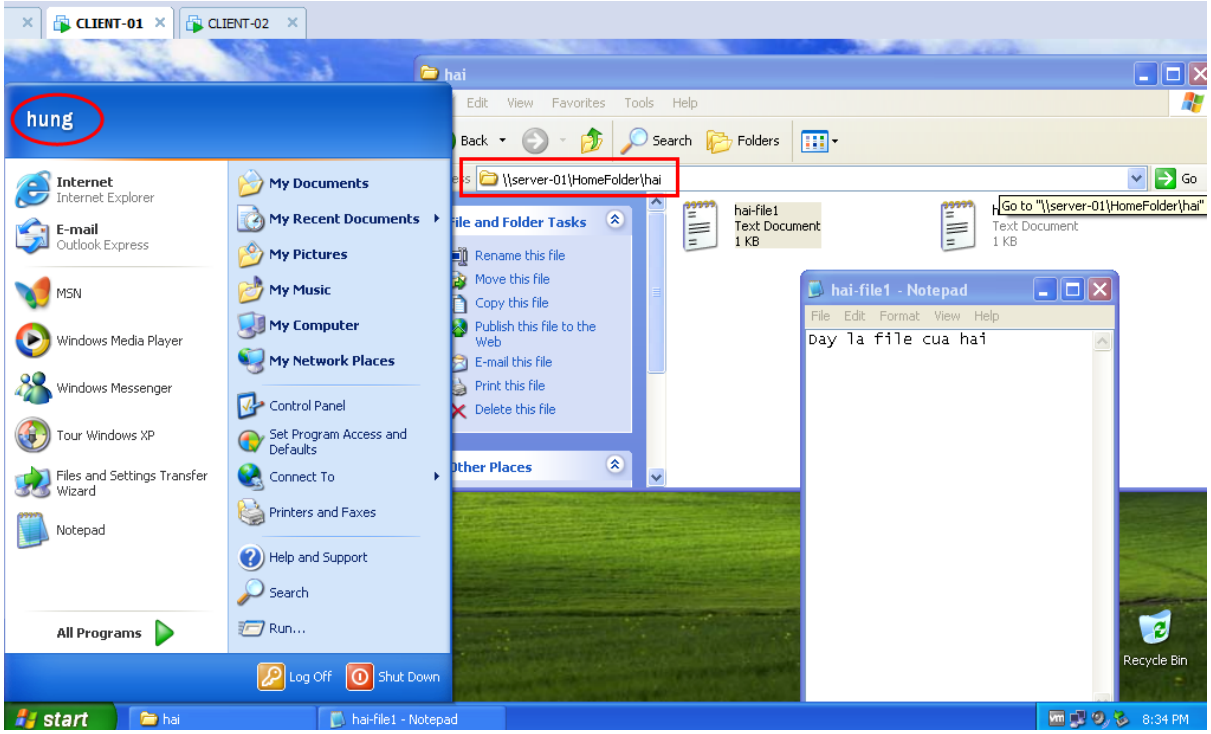
Câu 1

Câu này tương tự bài thực hành số 01, các bạn xem và làm lại.

Câu 2

- Tại máy CLIENT-01, truy cập vào với tài khoản “hung”.
- Mở Window Explorer, truy cập vào đường dẫn \\server-01\HomeFolder. Như chúng ta thấy, “hung” có thể xem được dữ liệu của người khác.





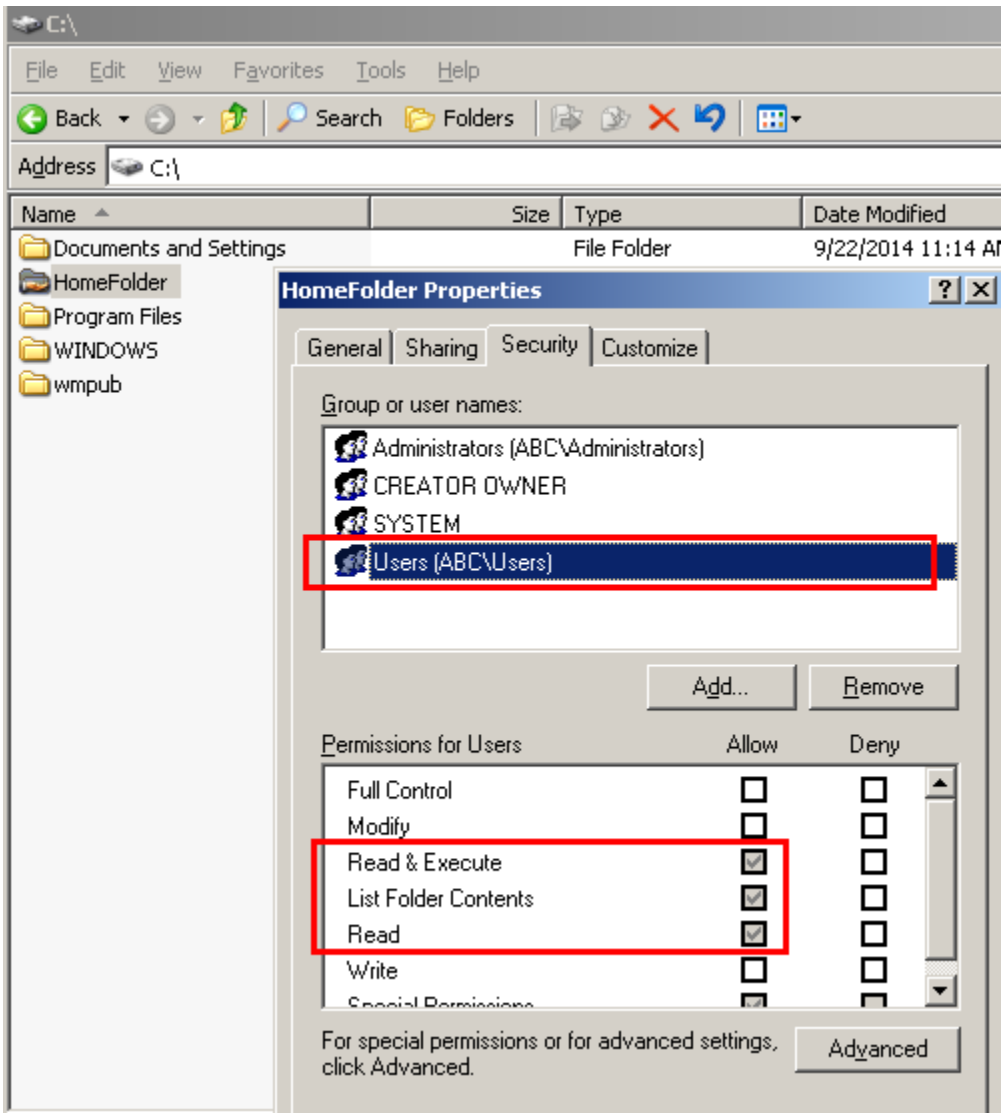
Câu 3

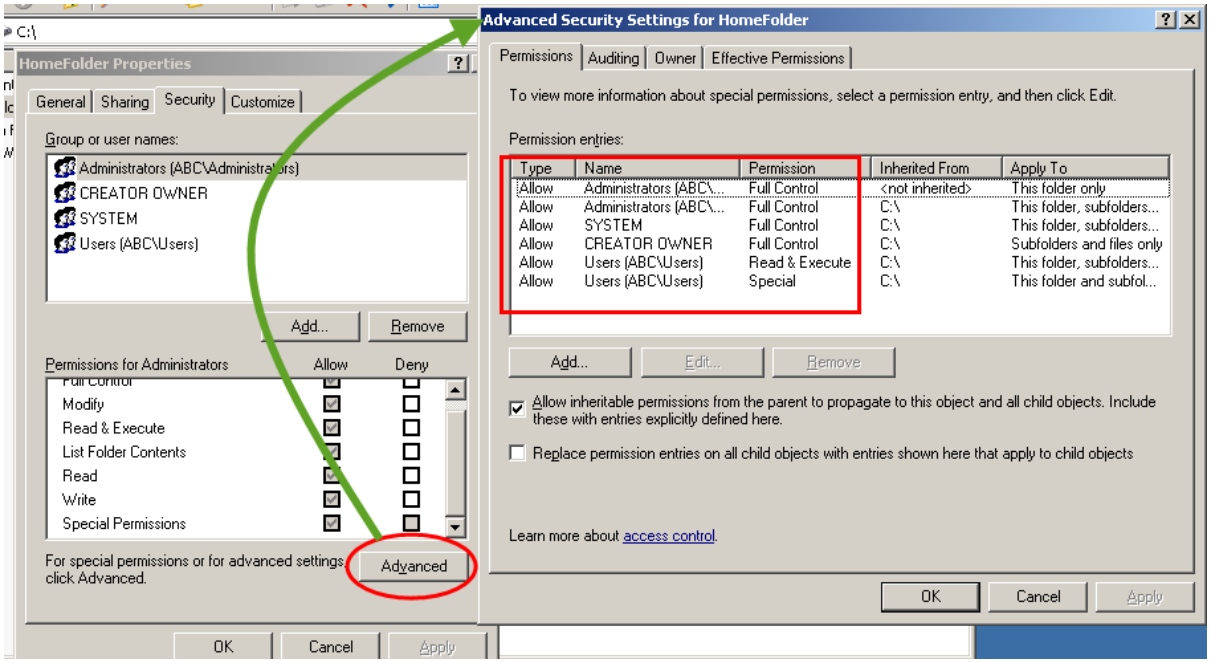
- Vì thư mục "HomeFolder" trên Server:
    - Thẻ Sharing: chia sẻ Everyone có quyền "Full Control"
    - Thẻ Security, group "Users" có quyền đọc (Read)

➔ Do đó, tổng hợp 2 phần lại, thì "Users" có quyền đọc trên thư mục "HomeFolder".

Hùng là tài khoản thuộc nhóm "Users", nên Hùng có quyền đọc dữ liệu của thư mục "HomeFolder" và các thư mục con của nó.

Lưu ý: Mọi tài khoản mới được tạo, mặc định sẽ thuộc nhóm "Users"



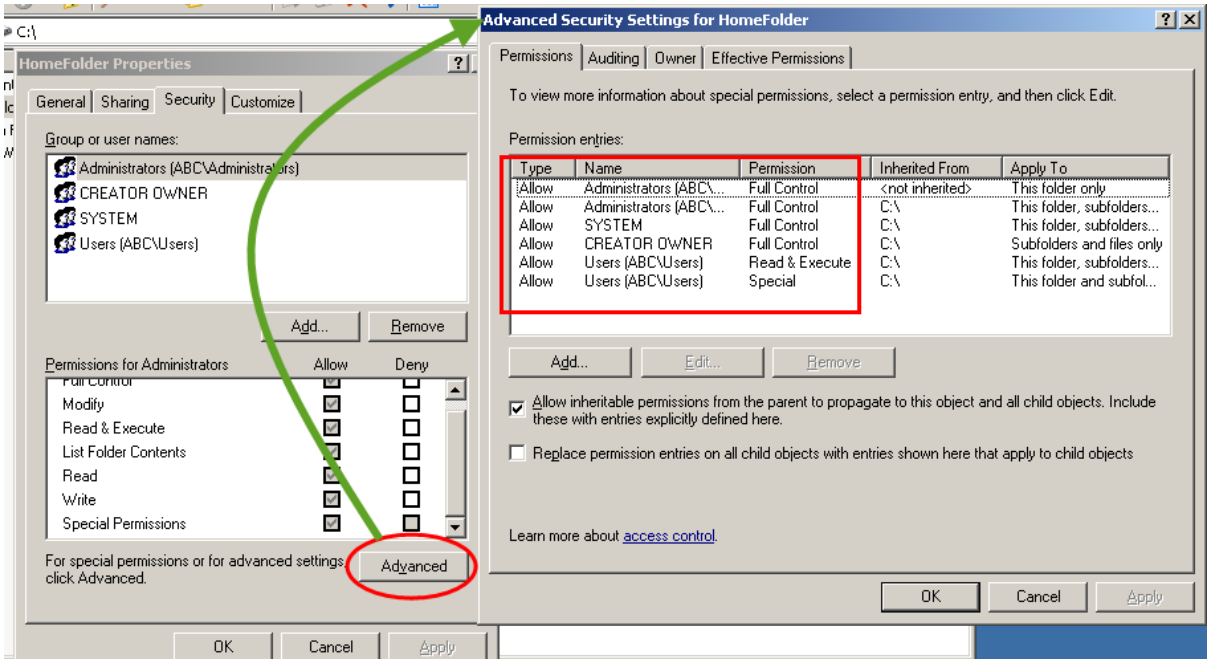


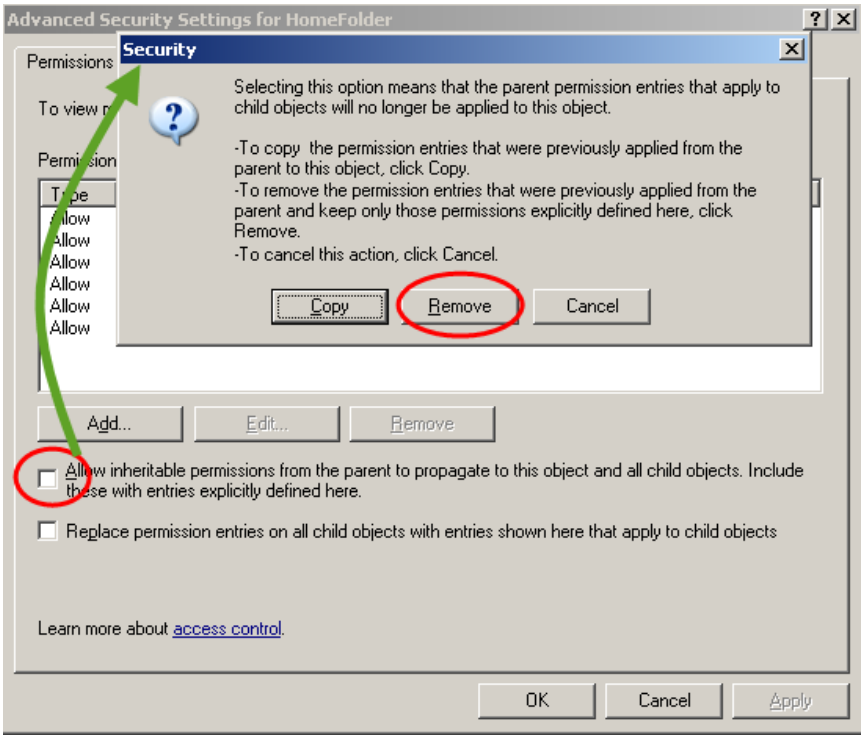
Câu 4

Ở hộp thoại "Advanced Security Settings", chúng ta nhận thấy rằng, các thiết đặt quyền cho "System", "CREATOR OWNER" và "Users" là được thừa kế từ thư mục cha của nó, là thư mục gốc C:\.

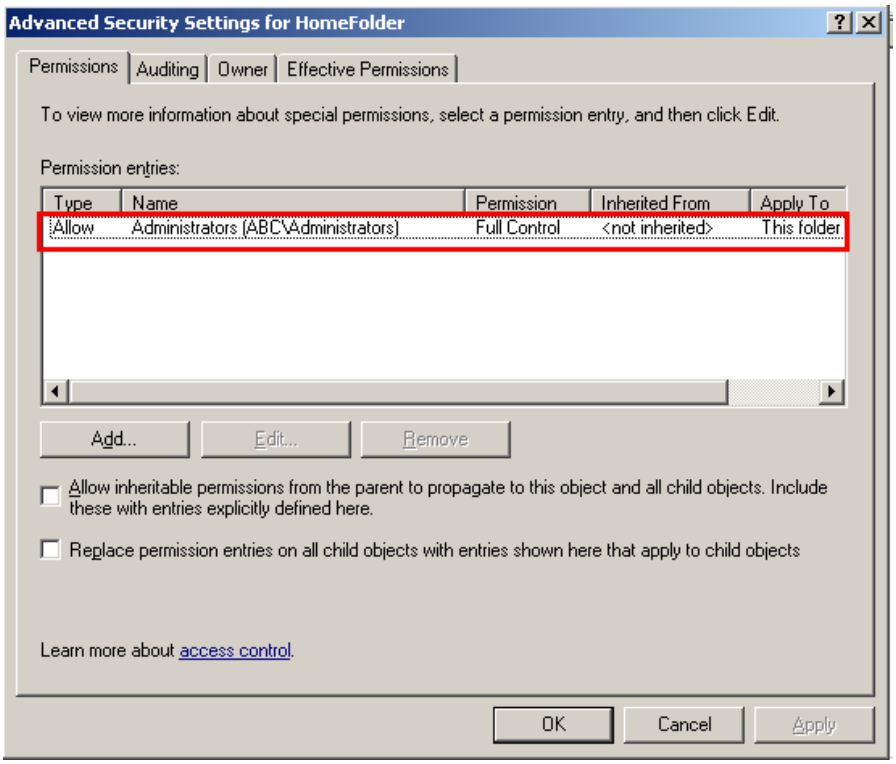
Vì vậy, chúng ta cần phải gỡ bỏ sự kế thừa này.

Để gõ bỏ sự kế thừa, chúng ta bỏ chọn ở dòng "**Allow inheritable permission from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here**".

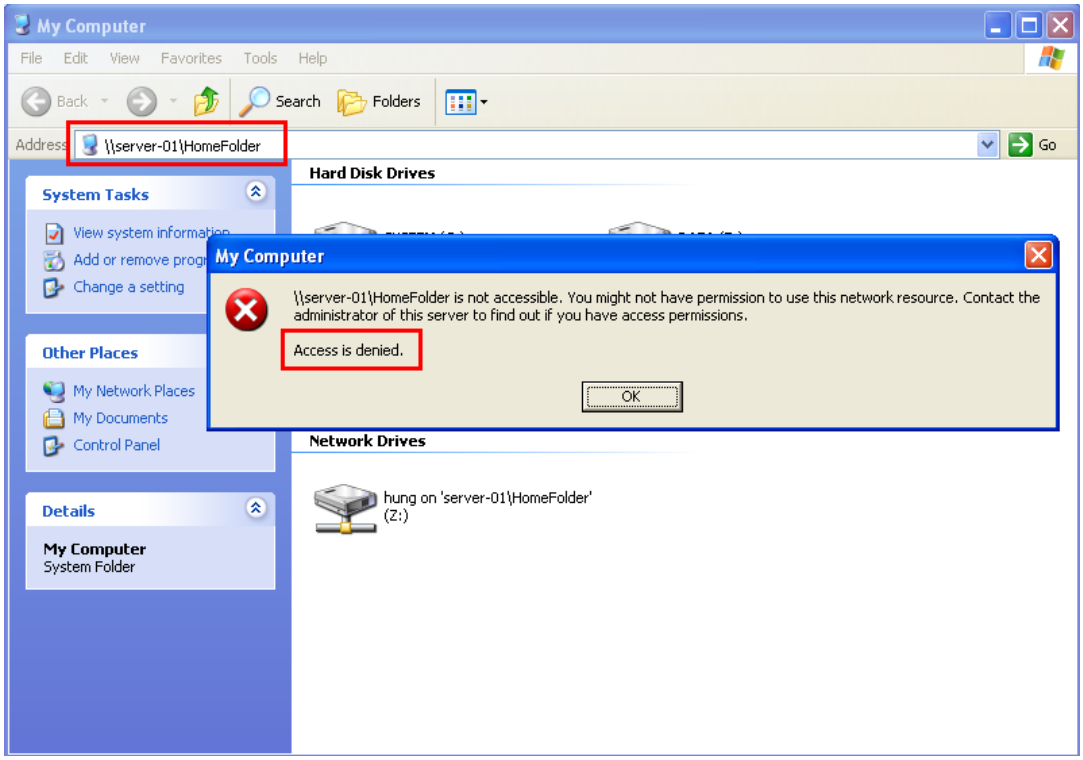


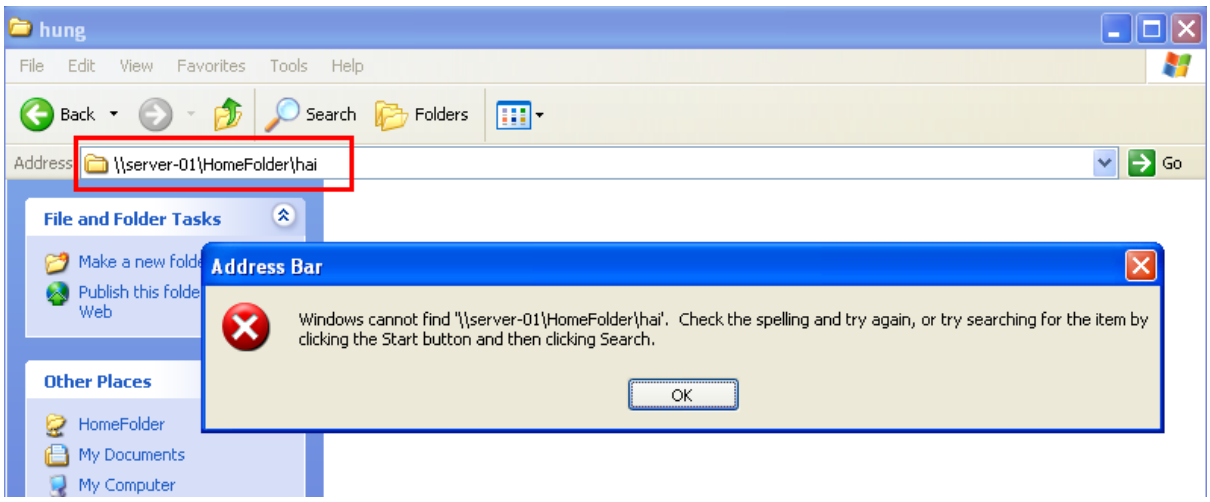


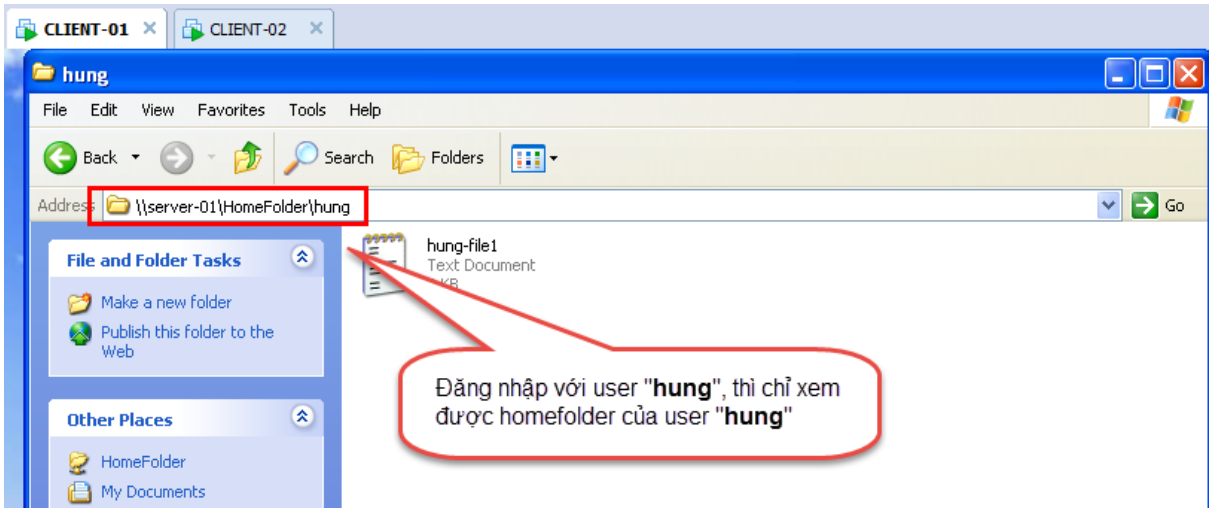
Và đây là kết quả sau khi bỏ sự thừa kế quyền, chỉ còn nhóm Administrators là có quyền “Full Control”



Thực hiện kiểm tra lại, đăng nhập với tài khoản “hung”







Bài 5: User profile

BÀI THỰC HÀNH SỐ 02

Roaming User Profile

Nhắc lại lý thuyết

- User Profile lưu trữ môi trường làm việc của mỗi người, cụ thể nó bao gồm các thiết đặt về:
    - Các shortcut ở menu Start, trên Desktop…
    - Các tài liệu lưu ở trên Desktop
    - Cấu hình Desktop như: screensaver, hình nền Desktop (wallpaper)
    - Các cấu hình cho một số chương trình như Microsoft Office Word, Excel…
    - Internet Explorer favorites and cookies
- Nếu người dùng làm việc trên nhiều máy tính khác nhau, chúng ta có thể cấu hình **Roaming User Profile** để đảm bảo rằng: môi trường làm việc của họ không bị thay đổi khi đăng nhập từ các máy tính khác nhau.
- Roaming User Profile là một loại User Profile được lưu trữ trên Server.
- Các lợi ích của Roaming User Profile:
    - Môi trường làm việc của người dùng không thay đổi, cho dù anh ta có đăng nhập vào các máy tính khác nhau.
    - User Profile được lưu trữ tập trung trên Server, giúp dễ quản lý, backup hay quét virus.
    - Nếu máy tính của người dùng gặp sự cố phải cài đặt lại, thì anh ta vẫn có được môi trường làm việc như cũ.
- Cơ chế tải và lưu User Profile:
    - Khi người dùng **Log on** vào hệ thống lần đầu tiên, User Profile tương ứng với tài khoản của họ sẽ được **download từ Server**.
    - Khi người dùng **Log off** khỏi hệ thống, User Profile sẽ được **upload lên Server**.

Lưu ý:
- Khi log off, không phải upload toàn bộ dữ liệu của User Profile, mà chỉ upload những files được thay đổi.
- Tương tự, Khi log on vào một máy mà họ đã từng làm việc trước đó, thì hệ thống chỉ download những files thay đổi (chứ không download toàn bộ User Profile)

→ Chính vì vậy, mà lần đầu tiên log on, bạn sẽ thấy màn hình khởi động lâu hơn, còn những lần log on sau, thì nhanh hơn nhiều.

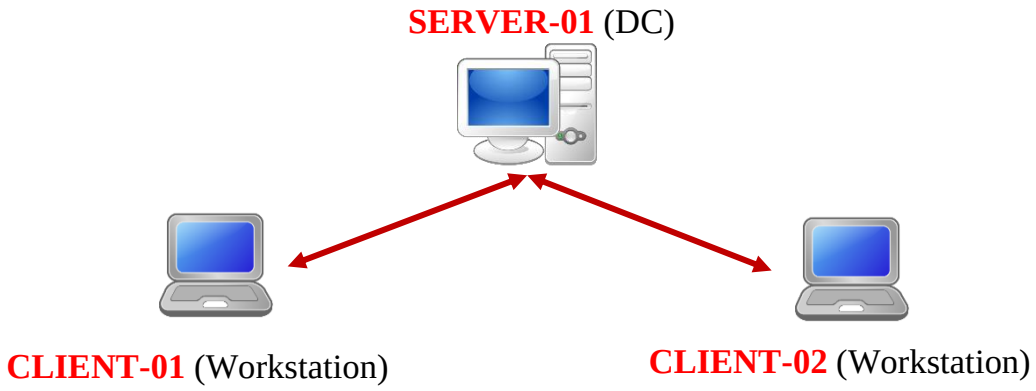
Mục tiêu bài thực hành

- Hiểu được mục đích của việc tạo Roaming User Profile.

- Biết cách tạo Roaming User Profile.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

Câu 5 : Tạo user mới

- Tạo một user mới trên domain **abc.com**:
  - Tên hiển thị: **Nguyễn Văn Hải**
  - Tên đăng nhập: **hai@abc.com**

Câu 6 : Tạo Roaming User Profile

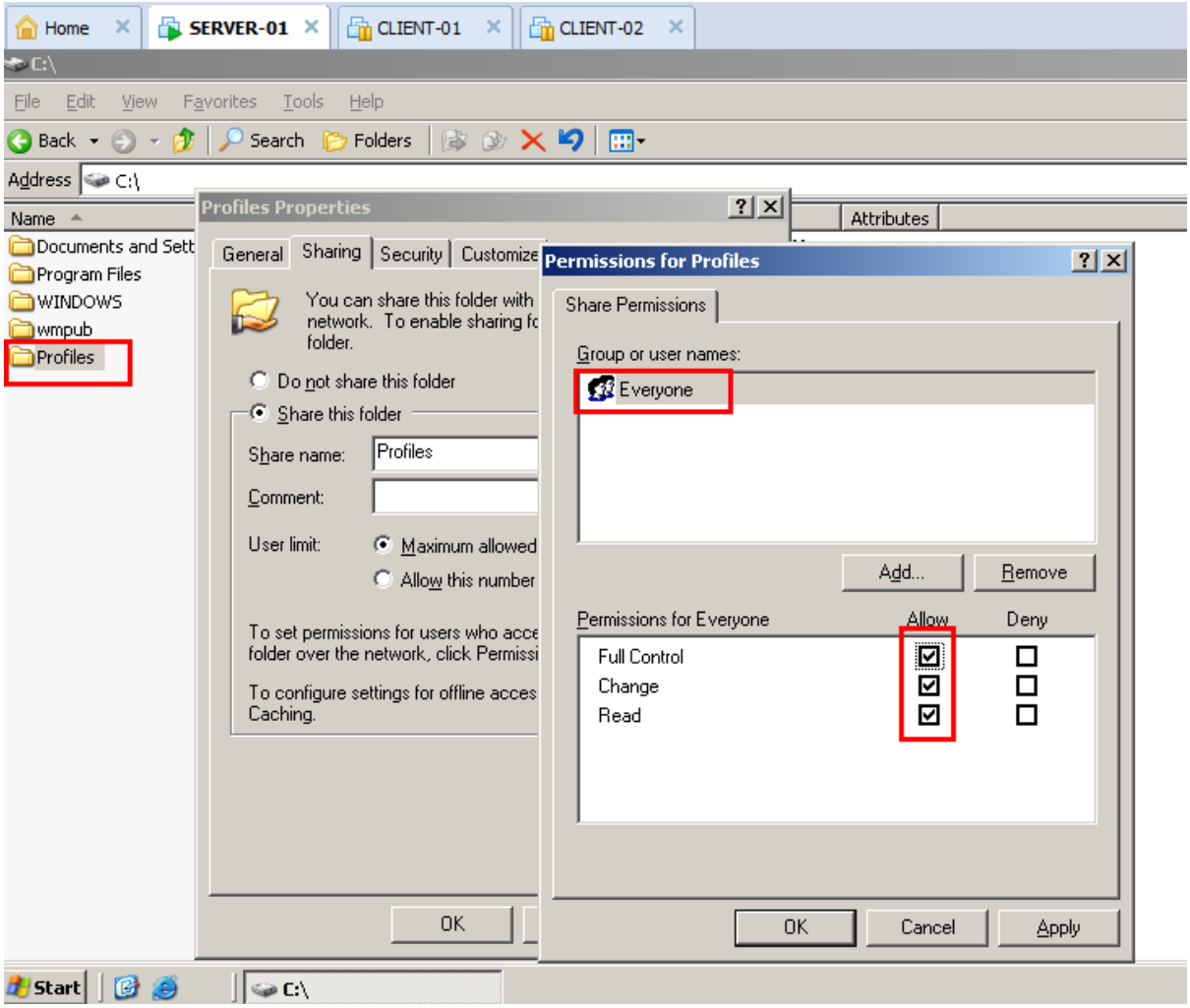
- Ở máy SERVER-01, tạo một thư mục để lưu roaming profiles, đặt tại: **C:\Profiles**.
- Tạo roaming profile cho user Hải.

Hướng dẫn

Để tạo Roaming User Profile, chúng ta thực hiện các bước sau:

Bước 1:

- Tạo một thư mục để lưu các profile. Giả sử đặt tại: C:\Profiles
- Cấu hình chia sẻ cho Everyone có quyền "Full Control"



Bước 2:

Cấu hình **Profile path** cho User Hải, bằng cách:

- Mở "AD Users and Computers"
- Nhấp phải vào User Hải, chọn lệnh "**Properties**".
- Bấm vào thẻ "**Profile**", tại phần "**User Profile**", nhập vào đường dẫn đến profile của User Hải.

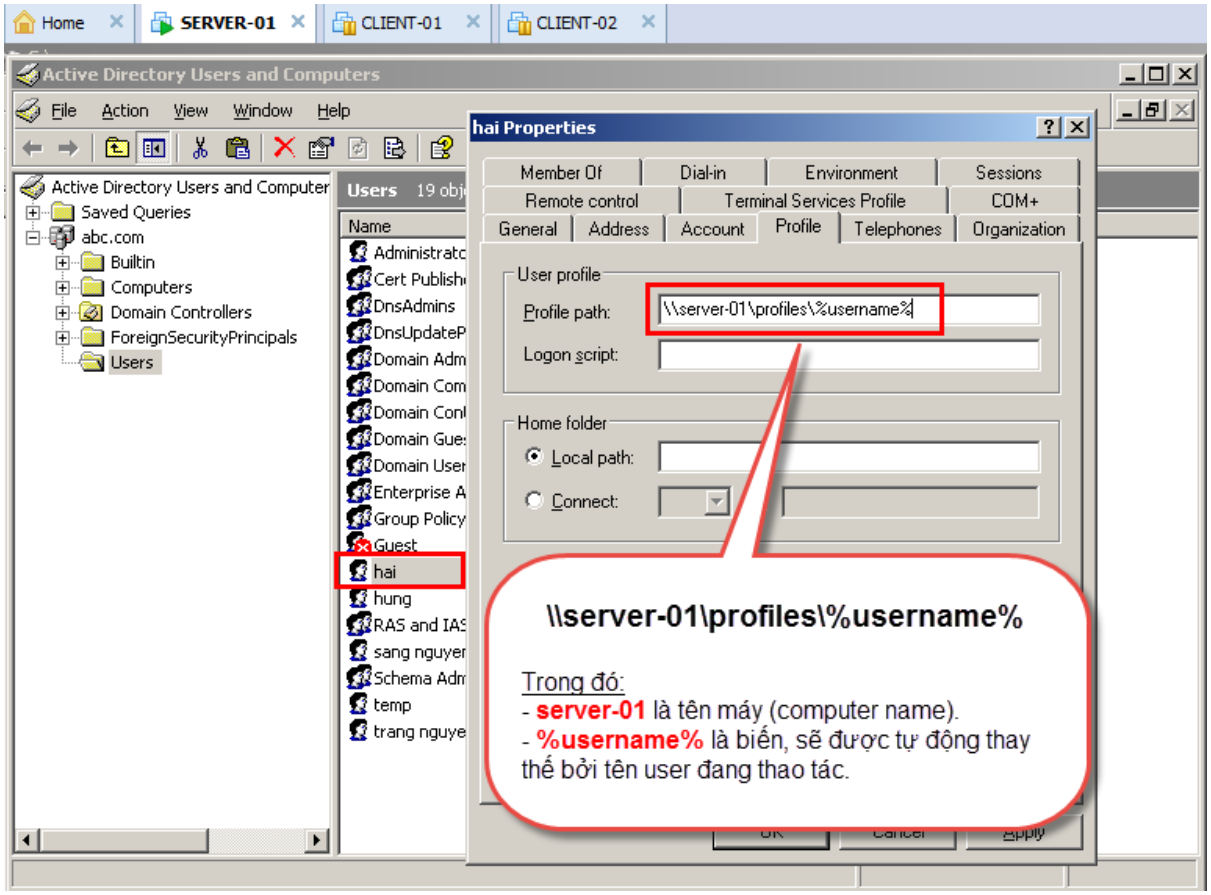
  Bạn có thể nhập vào là: \\server-01\Profiles\%username%

  Trong đó:

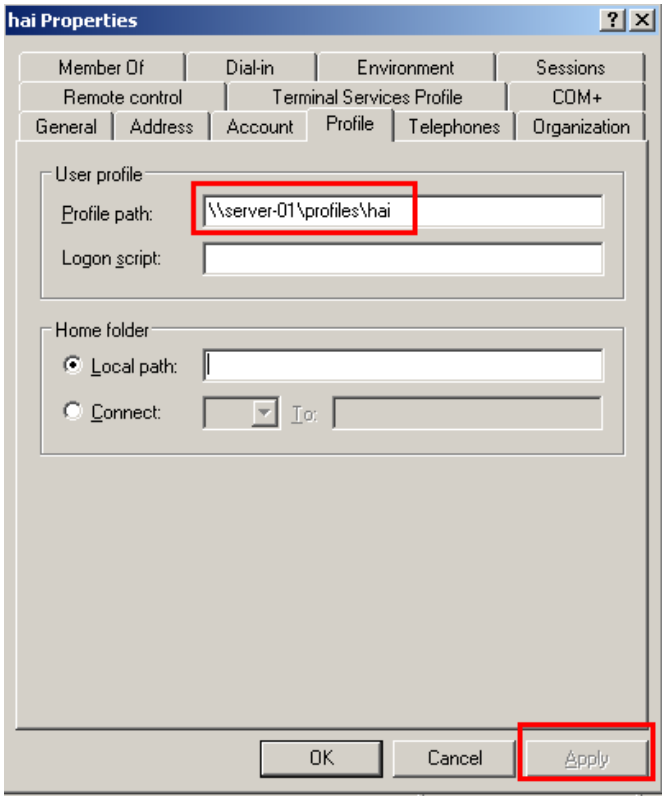
  - server-01: là tên máy server lưu profile (computer name)
  - %username%: là một biến, sẽ được tự động thay thế bởi tên User đang thao tác.

Lưu ý: Tên máy (computer name) có thể được lấy thông qua một số cách sau:

- **Cách 1:** Nhấp phải vào "**My Computer**" → chọn lệnh "**Properties**" → Bấm vào thẻ "**Computer Name**"
- **Cách 2:** Mở cmd, gõ lệnh: **hostname**



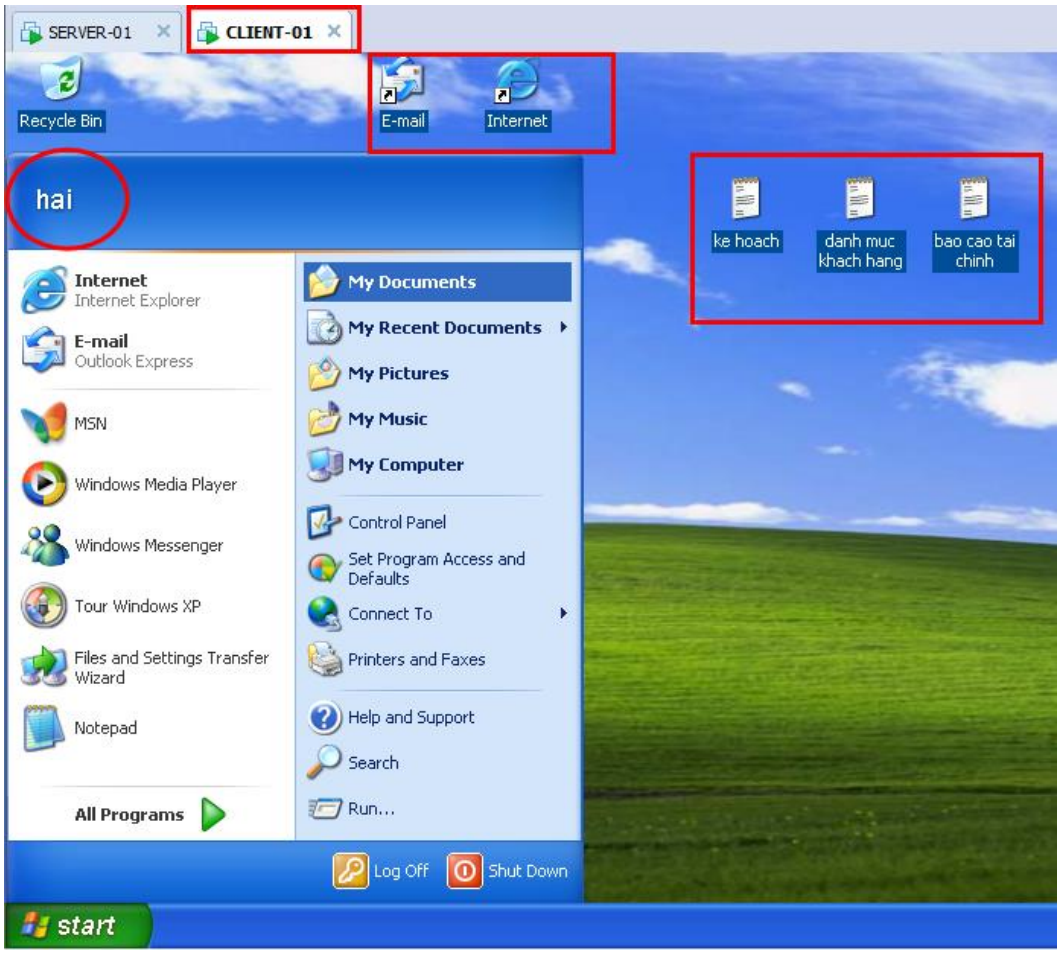
- Sau khi bấm nút "**Apply**", biến **%username%** sẽ được thay thế bởi tên user "**hai**":



Câu 7 : Kiểm tra ở máy trạm

- Tại máy **CLIENT-01**, đăng nhập với user **Hải**.

- Kiểm tra xem **loại profile** của user Hải là gì? Có thể kiểm tra ở đâu?
- Giả sử Hải là nhân viên marketing, anh ta thường sử dụng một số chương trình như **Internet Explorer**, **Outlook Express**. Anh ta tạo 2 shortcuts tương ứng trên Desktop.
- Trong quá trình làm việc, Hải cũng tạo một vài files, lưu ở màn hình Desktop (xem hình bên dưới)

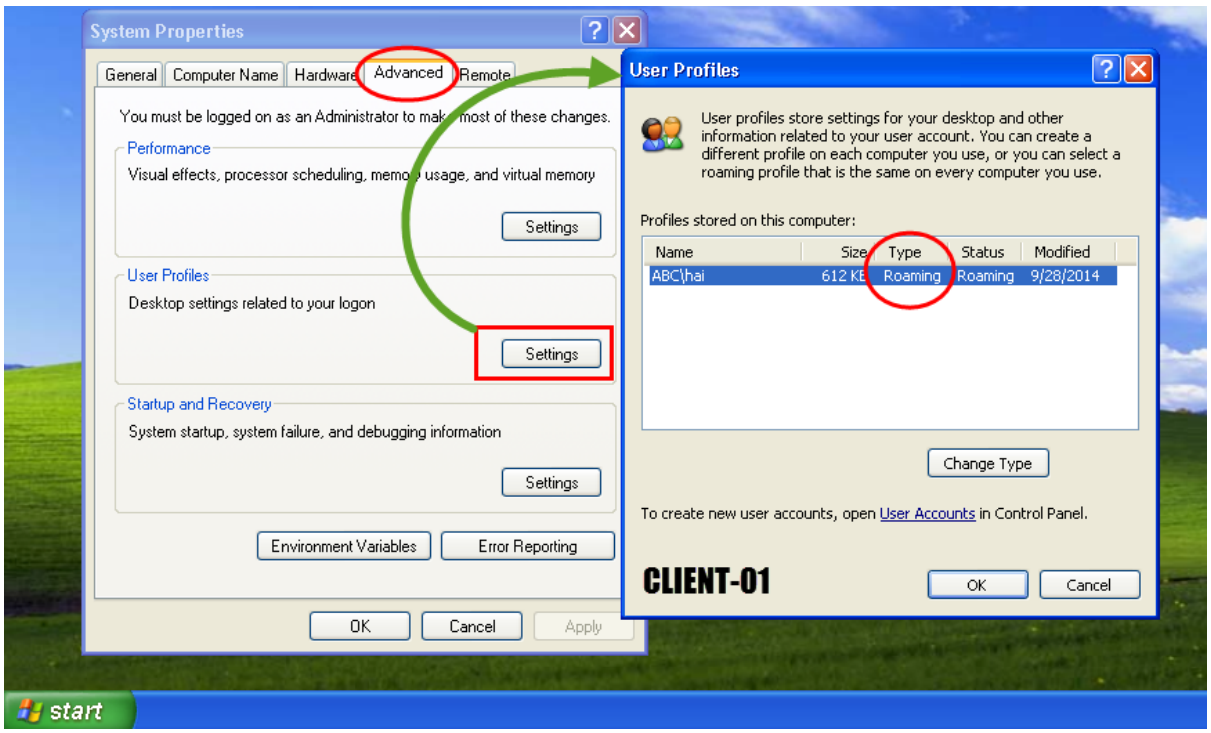


- Hãy **log off** User Hải.
- Trên máy **SERVER-01**, kiểm tra xem thư mục user profile cho Hải có được tạo không?
- Mở máy **CLIENT-02** lên, đăng nhập với User **Hải**.
- Kiểm tra xem, các shortcuts và các files trên Desktop của Hải có giống như trên máy **CLIENT-01** không?

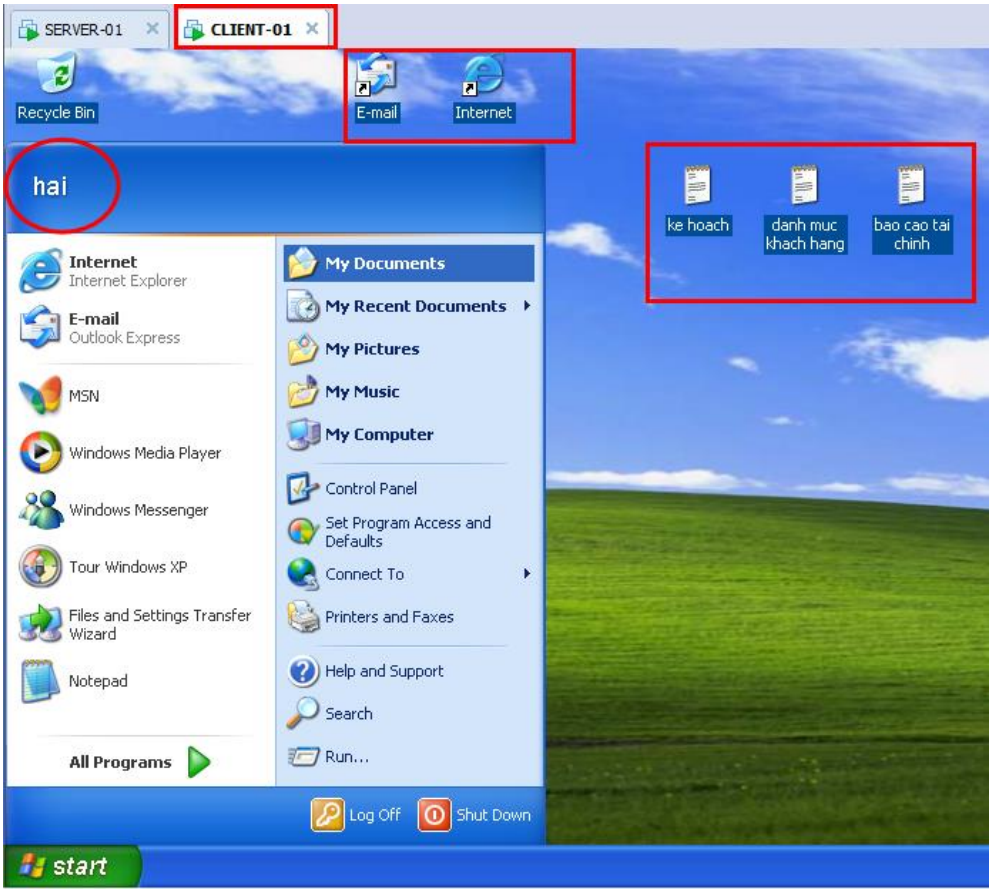
Hướng dẫn

- Tại máy **CLIENT-01**, đăng nhập với user Hải:

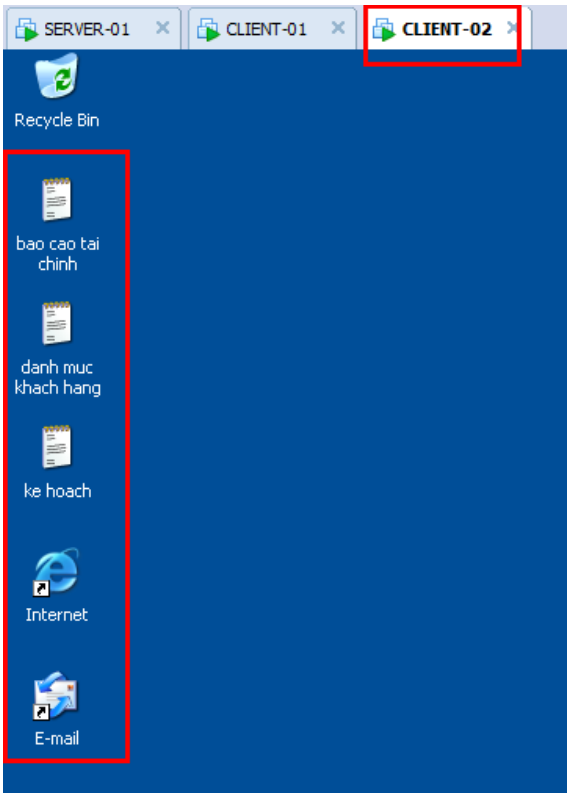
- Kiểm tra loại profile của user bằng cách:
    - Nhấp phải vào "**My Computer**" → Chọn lệnh "**Properties**"
    - Bấm vào thẻ "**Advance**"
    - Tại mục "**User Profiles**" → Bấm vào nút "**Settings**"
    - Tại hộp thoại "**User Profiles**", bạn sẽ thấy được user "**hai**" có loại profile là "**Roaming**" → Điều đó có nghĩa, profile của user này được lưu trữ trên server.



- Thực hiện tạo:
    - 2 shortcuts trên Desktop: Outlook Express và Internet Explorer.
    - Vài files trên Desktop (xem hinh bên dưới)



- Tại máy **CLIENT-02**, đăng nhập với user Hải, bạn sẽ thấy các shortcuts, files trên Desktop xuất hiện giống như trên máy **CLIENT-01**.



Bài 5: User profile

BÀI THỰC HÀNH SỐ 03

Preconfigured User Profile

Nhắc lại lý thuyết

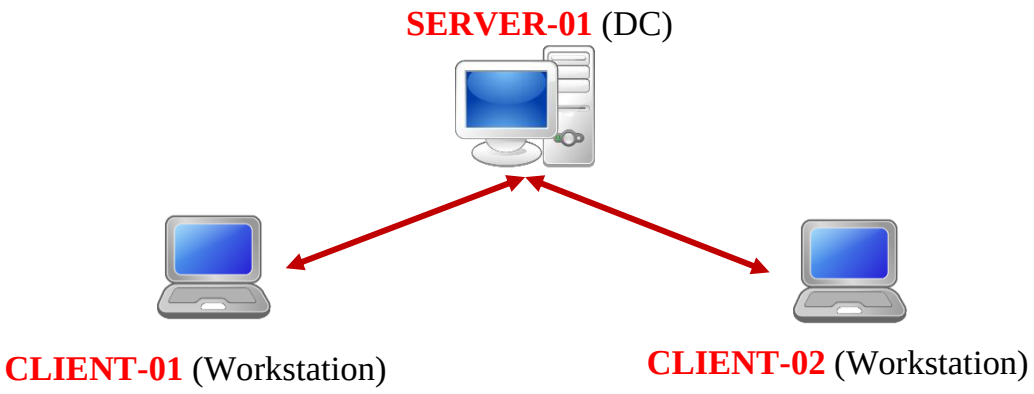
- **Preconfigured user profile** là một loại User Profile được lưu trữ tại máy SERVER, và **được người quản trị cấu hình sẵn**.
- Người sử dụng profile này vẫn có thể thay đổi profile của mình: chẳng hạn thay đổi màn hình Desktop, Start menu… (Điều này khác biệt với **Mandatory user profile**, là loại profile mà không cho phép người dùng thay đổi cấu hình profile của mình)

Mục tiêu bài thực hành

- Biết cách tạo Preconfigured user profile.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

Câu 8 : Tạo preconfigured user profile cho người dùng mới

- Thời gian sắp tới, công ty ABC có một chuyên gia từ Hà Nội vào công tác.

- Bộ phận IT cần phải tạo tài khoản cho người này, đồng thời, tạo cho anh ta một profile được cấu hình sẵn, sao cho khi anh ta log on vào hệ thống, màn hình Desktop của anh ta đã có sẵn một số shortcuts quan trọng như: **Internet Explorer**, **Outlook express**, **Windows Media Player.**
- Bạn là một IT của công ty, hãy thực hiện yêu cầu trên. Biết rằng:
    - Tên hiển thị của người dùng mới: **Mai Văn Long**
    - Tên đăng nhập: **long@abc.com**

Thực hiện kiểm tra

- Tại máy CLIENT-01, user Long đăng nhập vào, màn hình Desktop có hiện sẵn các shortcuts như đã cấu hình không?
- Trong quá trình làm việc, Long có tạo một vài files trên Desktop, sau đó log off ra.
- Tại máy CLIENT-02, Long có lấy được các files đã tạo trên Desktop trước đó không?

Hướng dẫn

Để tạo Preconfigured user profile, chúng ta thực hiện các bước sau:

Bước 1: Trên máy SERVER-01, tạo một profile mẫu.

Muốn tạo **profile mẫu**, chúng ta phải tạo một user mới, cho phép user này có quyền log on vào SERVER.

Khi user này logon vào SERVER, thì một profile cục bộ (Local user profile) tương ứng với user này sẽ được tạo ra trên máy SERVER. Profile cục bộ này chính là profile mẫu mà chúng ta cần tạo.

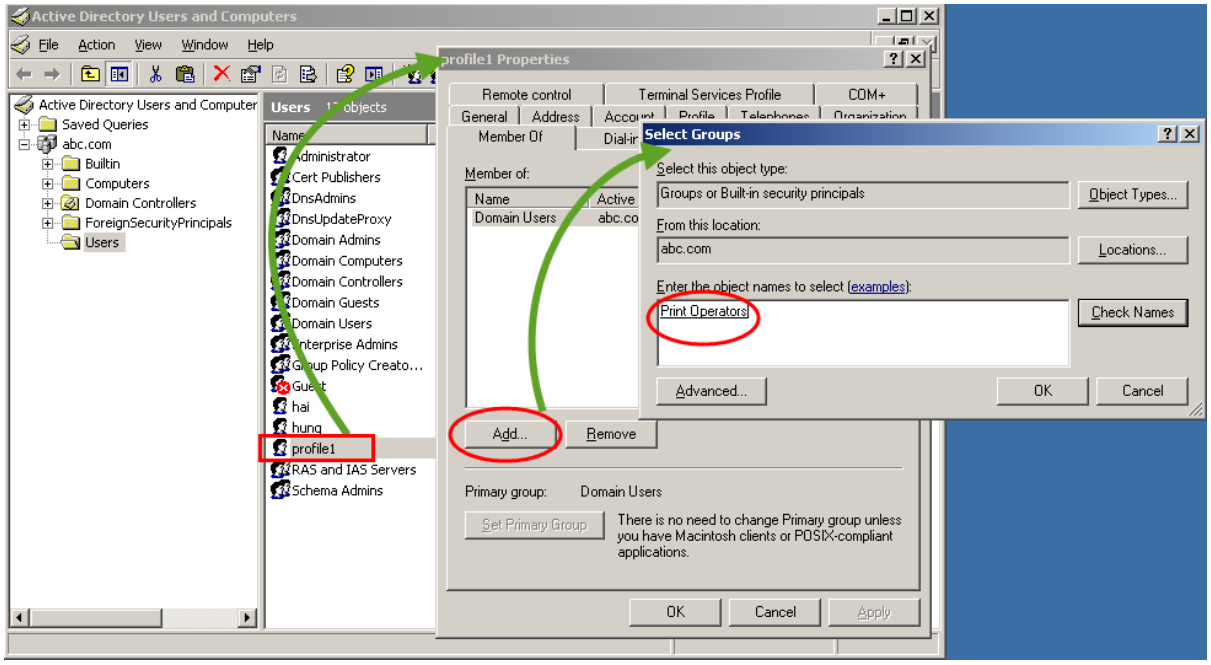
Chúng ta sẽ cấu hình thay đổi profile này như ý muốn (ví dụ: thêm shortcuts vào Desktop…)

Dưới đây là hình ảnh các bước thực hiện:

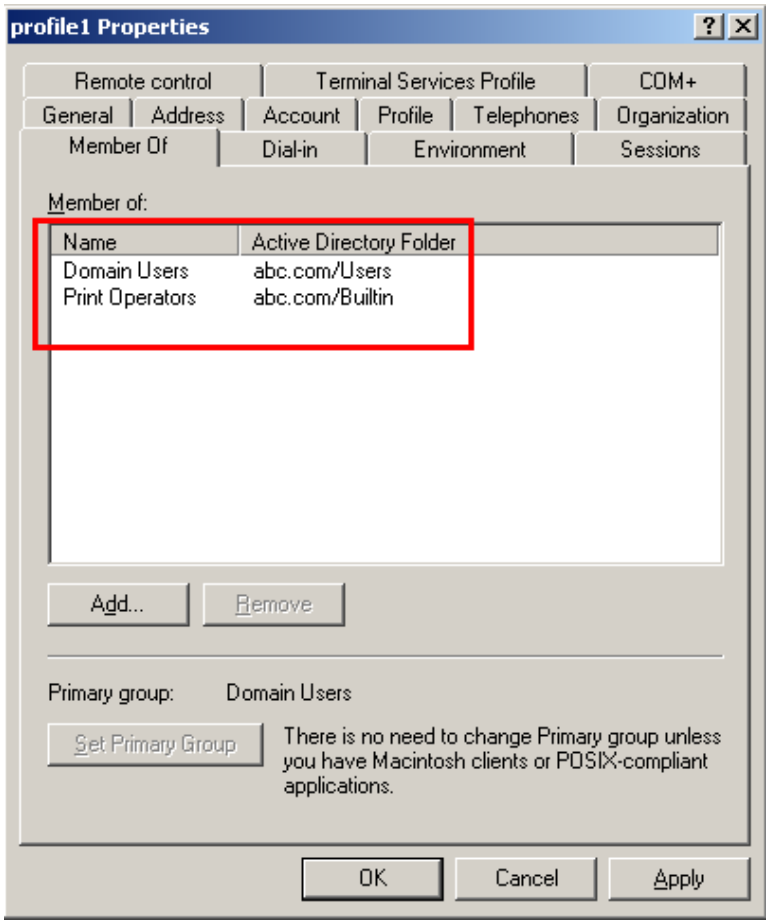
- Tạo user mới, đặt tên gì cũng được, vì user này chỉ nhằm mục đích tạo profile mẫu, chứ không dùng cho người dùng nào cả. Ví dụ ở đây là: **profile1**.

Lưu ý rằng: mặc định, một user tạo ra sẽ không có quyền đăng nhập cục bộ vào máy SERVER.
Tại máy SERVER-01, các bạn thử đăng nhập với tài khoản **profile1** (mới tạo ở trên) xem thế nào nhé! Hãy xem hệ thống báo lỗi gì?

- Có nhiều cách để gán quyền cho một user đăng nhập cục bộ. Trong đó, có một cách đơn giản và nhanh là cho user này vào nhóm "**Print Operator**" (Xem hình bên dưới)

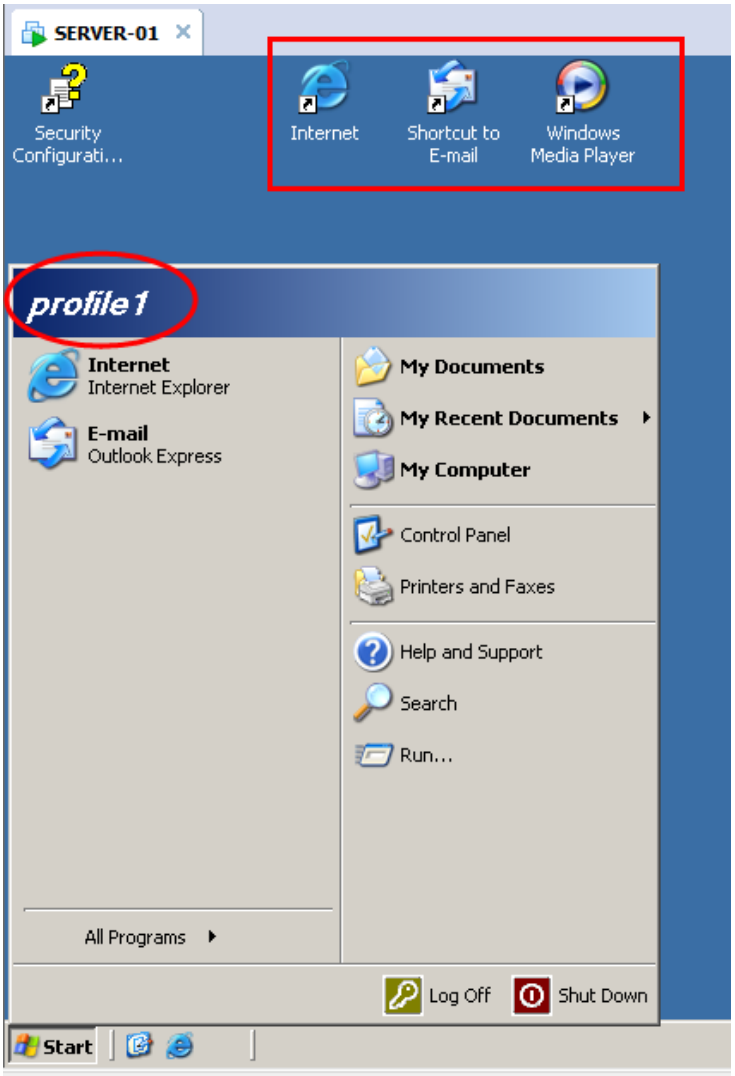


- Sau khi thêm user vào nhóm "**Print Operator**", thì thẻ "**Member Of**" của user sẽ có dạng như hình bên dưới:



- Thực hiện đăng nhập cục bộ vào máy **SERVER-01** với tài khoản **profile1**:

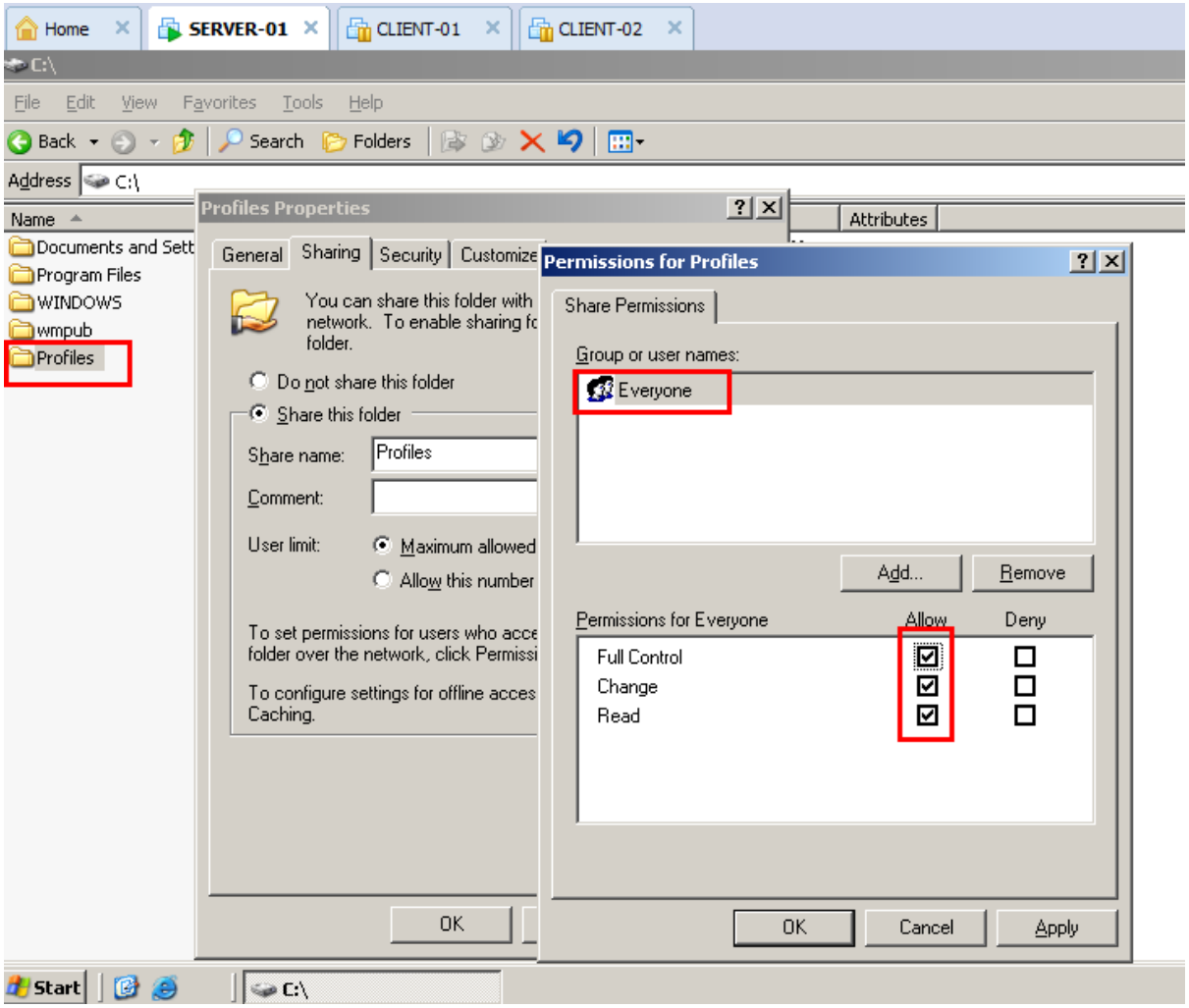
- Tạo các shortcuts theo yêu cầu: Internet Explorer, Outlook express, Windows Media Player.



Bước 2: Tạo thư mục để chứa các profiles

- Đăng nhập vào SERVER-01 với tài khoản administrator.

- Giống như phần tạo Roaming profiles, chúng ta tạo một thư mục **"C:\Profiles"** và chia sẻ cho "**Everyone"** có quyền "**Full Control"**.

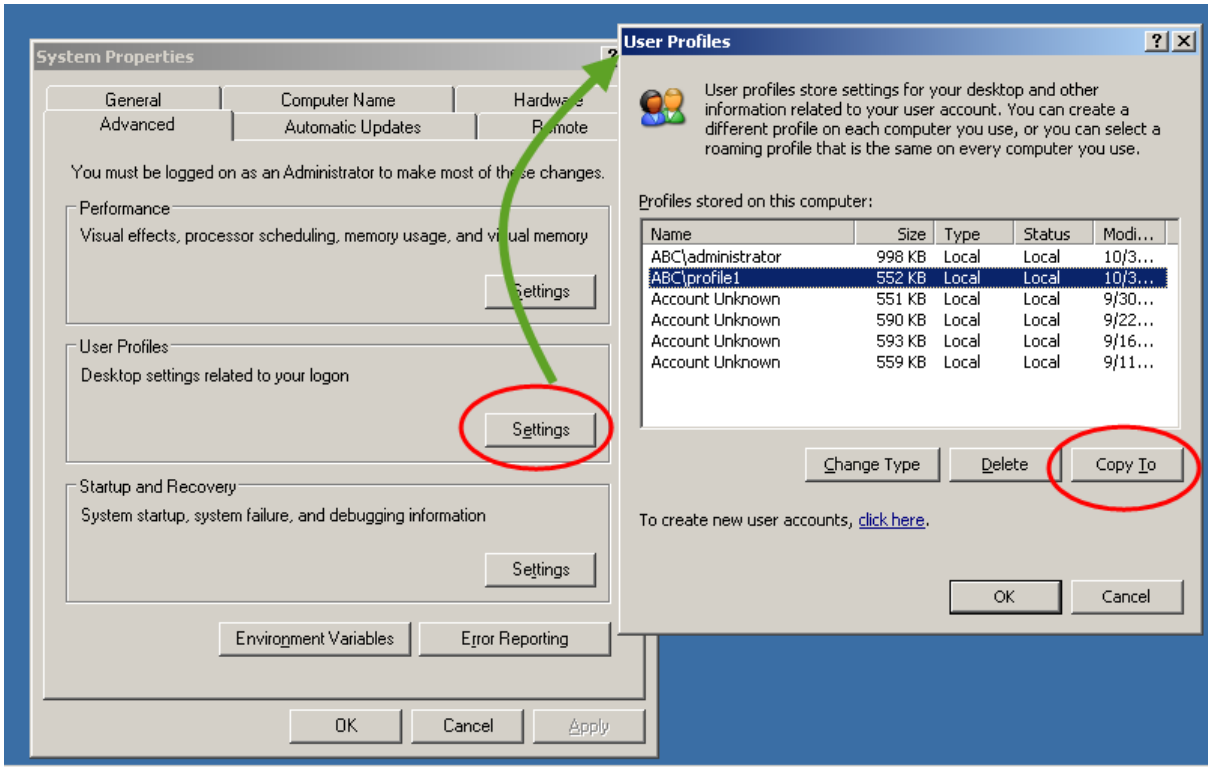


<u>Bước 3:</u> Copy Local user profile (profile mẫu đã tạo ở bước 1) vào thư mục "Profiles"

- Log off khỏi tài khoản "profile1", và log on với tài khoản "administrator".

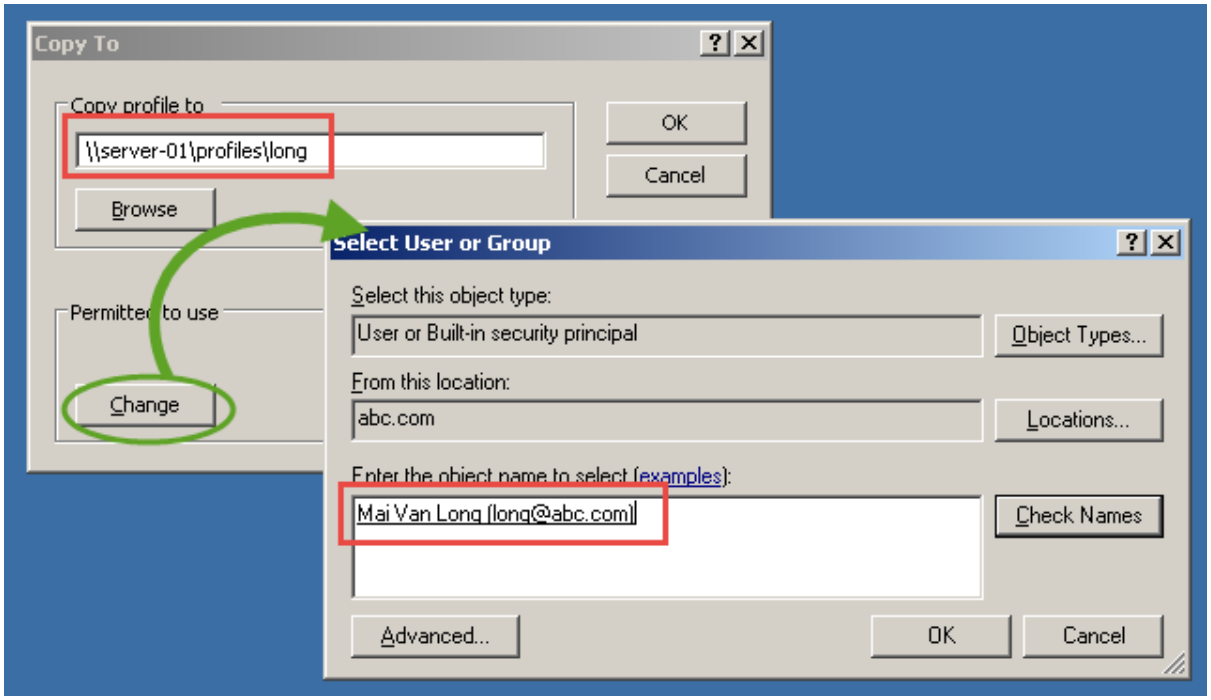
<u>Lưu ý:</u> hãy chắc rằng bạn đăng nhập vào máy SERVER với tài khoản **administrator**. Nếu không, bạn sẽ không có quyền copy profile đâu.

- Để copy một Local user profile, chúng ta nhấp phải vào "**My Computer**" → chọn lệnh "**Properties**".
- Tại thẻ "**Advanced**", ở phần "**User Profiles**", bấm vào nút "**Settings**".
- Hộp thoại "**User Profiles**" được mở ra. Tại đây, chúng ta chọn profile muốn copy, và bấm vào nút "**Copy To**".



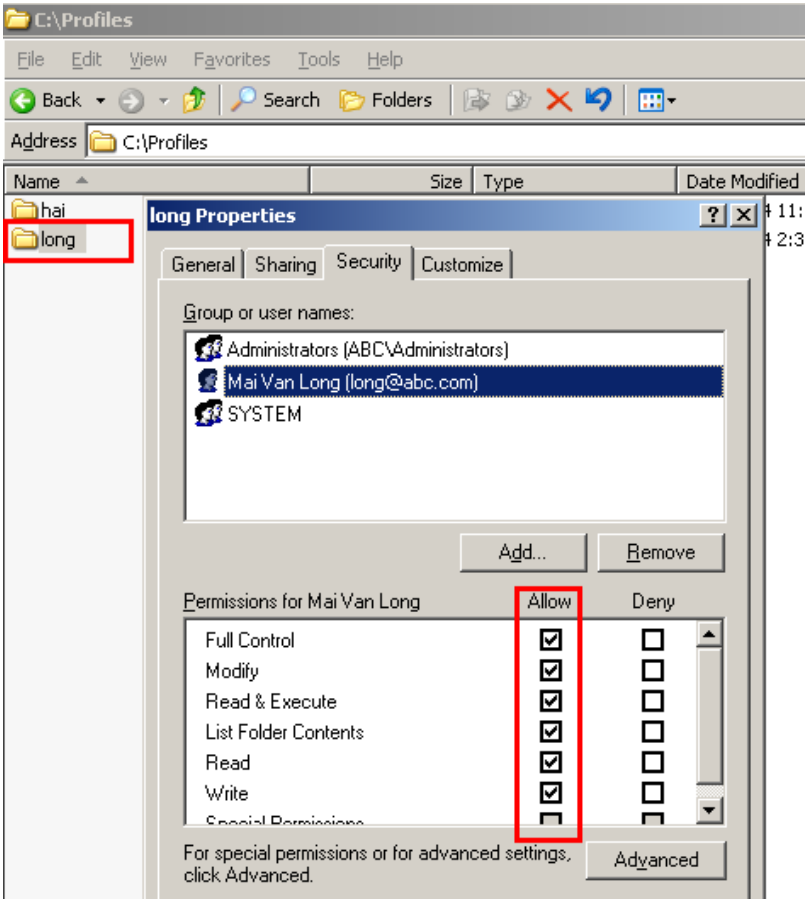
- Hộp thoại "**Copy To**" mở ra:
  - Tại mục "**Copy profile to**": gõ vào đường dẫn đến thư mục chứa profile.
  - Tại mục "**Permitted to use**": bấm vào nút "**Change**" và chọn user có quyền sử dụng profile này.

Lưu ý: Nếu bạn muốn cho cả 1 nhóm có quyền sử dụng profile này, thì add nhóm đó vào.



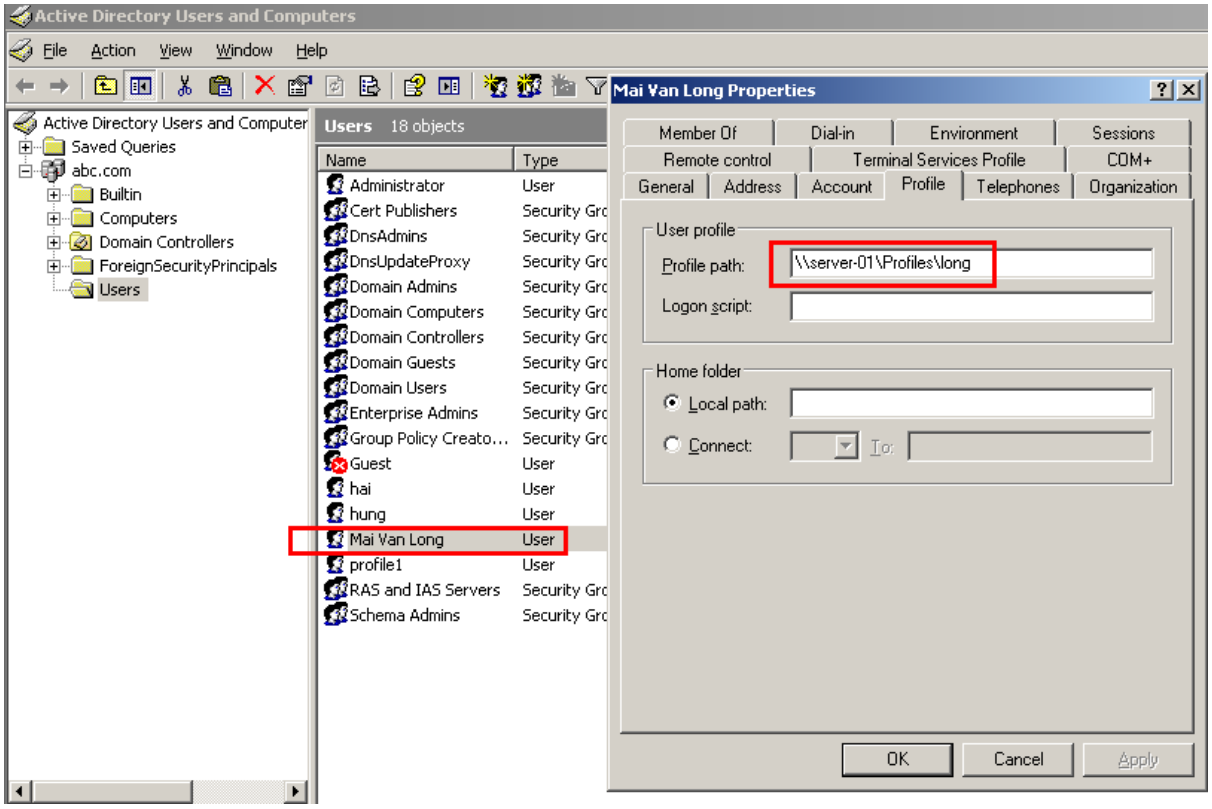
- Sau khi copy xong, bạn vào đường dẫn "**C:\Profiles**", sẽ thấy có một thư mục "**long**" được tạo mới, đây chính là thư mục được copy từ profile của tài khoản "**profile1**".

- Nhấp phải vào thư mục "**long**", chọn lệnh "**Properties**", ở thẻ "**Security**", bạn sẽ thấy user "**long**" có quyền "**Full Control**" trên thư mục này.



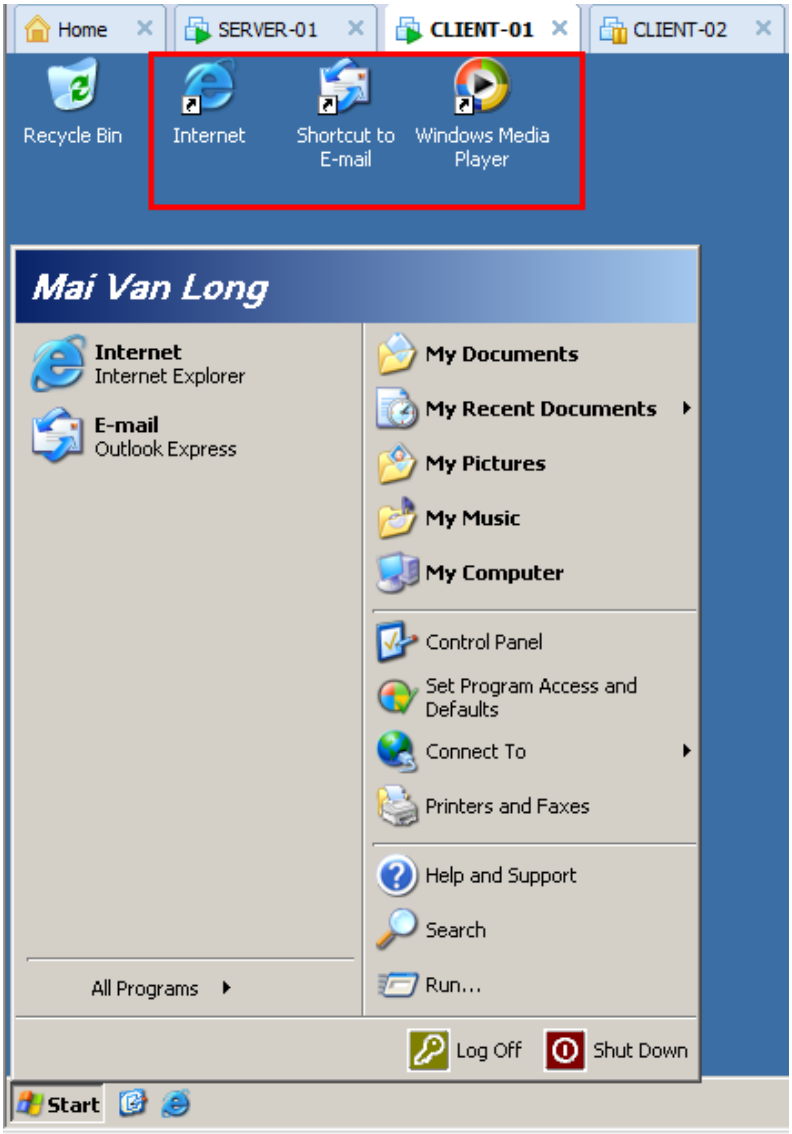
Bước 4: Cấu hình đường dẫn profile cho user

- Mở "**AD Users and Computers**", nhấp phải vào user "**long**", chọn lệnh "**Properties**".
- Tại thẻ "**Profile**", nhập vào đường dẫn đến profile ở bước trên. Ví dụ trong trường hợp này là: **\\server-01\Profiles\long**.

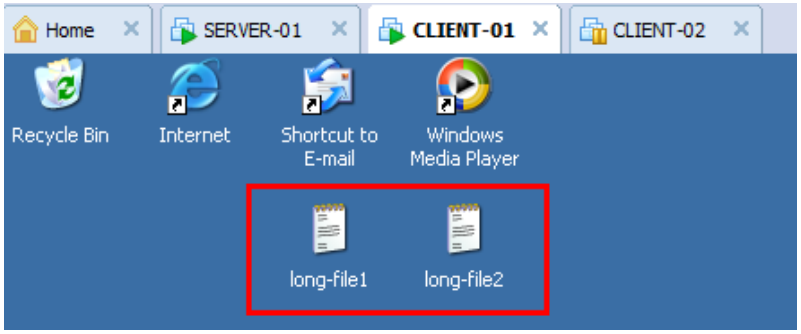


Câu 9

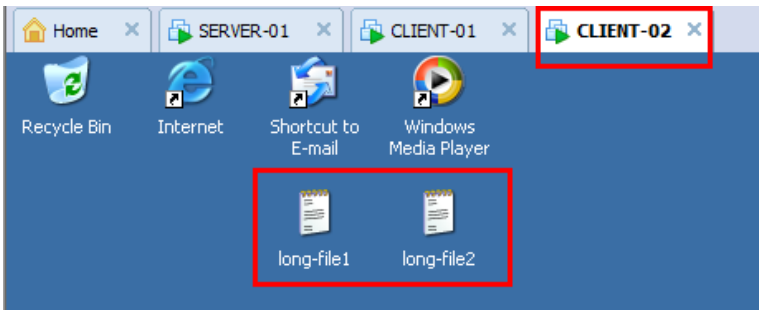
- Tại máy **CLIENT-01**, đăng nhập với tài khoản "**long**", bạn sẽ thấy trên Desktop của Long đã có sẵn các shortcuts quan trọng (như đã cấu hình ở trên)



- User "long" tạo vài files trên Desktop, sau đó log off ra khỏi máy CLIENT-01.



- Tại máy CLIENT-02, đăng nhập với tài khoản "long", sẽ thấy các files đã tạo ở máy CLIENT-01.



➔ Như vậy, preconfigured user profile cho phép người dùng thay đổi profile. Chúng ta sẽ tìm hiểu một loại profile khác, mà không cho phép người dùng

thay đổi profile, đó là "Mandatory user profile" (sẽ được thực hành trong bài tập sau)

Bài 5: User profile

BÀI THỰC HÀNH SỐ 04

Mandatory User Profile

Nhắc lại lý thuyết

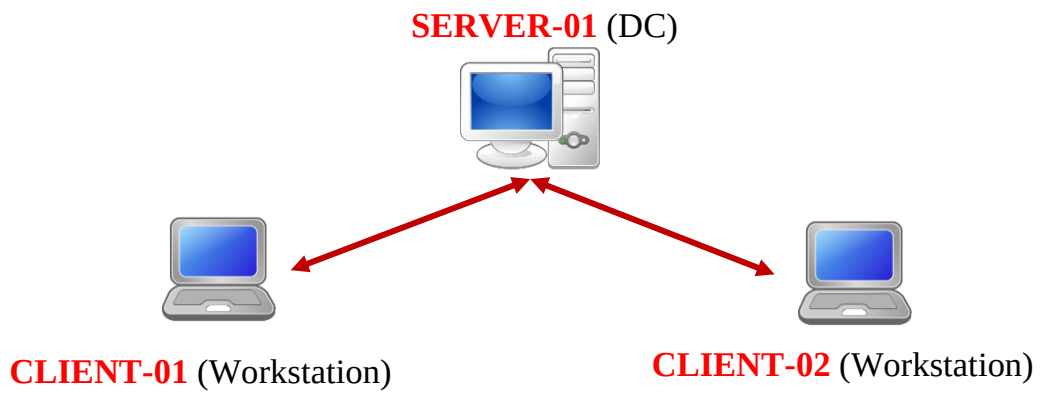
- **Mandatory user profile** là một loại User Profile được lưu trữ tại máy SERVER, và **người sử dụng không được phép thay đổi**. Hay nói cách khác, dù người sử dụng có thay đổi (chẳng hạn thêm các shortcuts ở Desktop, thay đổi Start menu…) thì ở lần đăng nhập kế tiếp, những thay đổi này sẽ không còn.
- **Mandatory user profile** thường được sử dụng trong trường hợp người quản trị mạng muốn tạo một profile chung cho các nhân viên sử dụng, và không muốn họ thay đổi những cấu hình trên profile này.
- **Từ Mandatory:** có nghĩa là **có tính chất bắt buộc** (cố định không thay đổi)

Mục tiêu bài thực hành

- Biết cách tạo Mandatory user profile.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

Câu 10 : Tạo mandagory user profile

- Tại công ty ABC, bộ phận IT không muốn nhân viên Mai Văn Long (long@abc.com) thay đổi profile của mình.
- Bạn là một IT của công ty, hãy thực hiện yêu cầu trên.

Hướng dẫn

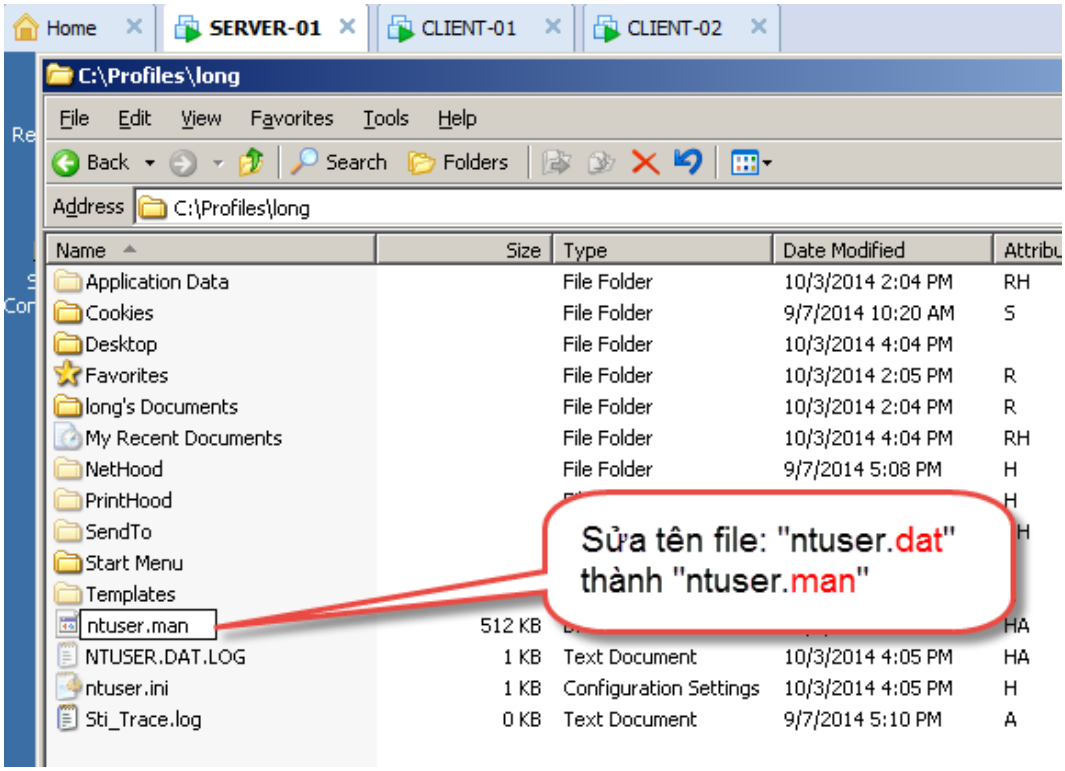
Để tạo Mandatory user profile, chúng ta thực hiện các bước sau:

Bước 1: Tạo preconfigured user profile cho tài khoản "long" (như ở bài tập trước).

Bước 2: Chuyển đuôi file NTuser.DAT thành NTuser.MAN

- **Lưu ý:**
  - Trước khi đổi đuôi file từ .DAT thành .MAN, **bạn cần log off user "long" ra**.
  - File NTuser.DAT là file ẩn (hidden file), vì vậy nếu các bạn không nhìn thấy file này trong thư mục profile, thì hãy bật chế độ xem file ẩn. (Bật chế độ xem file ẩn bằng cách: Mở Window Explorer → menu Tools → Folder Options → Qua thẻ View → Chọn "**Show hidden files and folders**").
  - Đối với **Window Server 2008**, thì file NTuser.DAT vừa có thuộc tính ẩn (hidden), vừa có thuộc tính là file hệ thống (system). Vì vậy, để có thể thấy được file NTuser.DAT, ngoài việc chọn "Show hidden files and folders", bạn phải bỏ chọn tại mục "**Hide protected operating system files**".

- Tại máy SERVER-01, vào thư mục profile của user "long", chuyển đuôi file NTuser.DAT thành NTuser.MAN.
  ➔ Vậy là profile này đã chuyển thành loại Mandatory user profile.

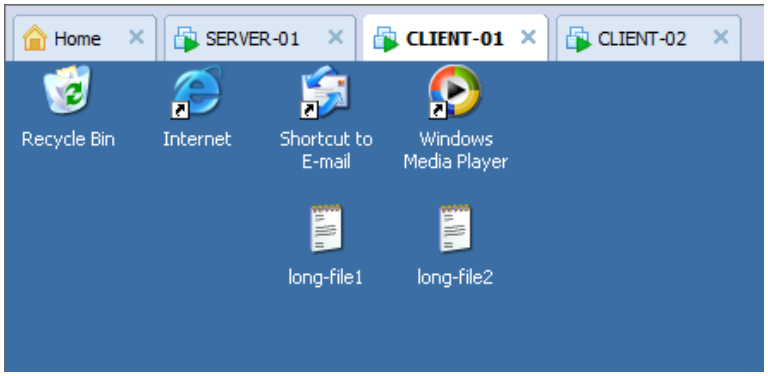


Câu 11 Thực hiện kiểm tra

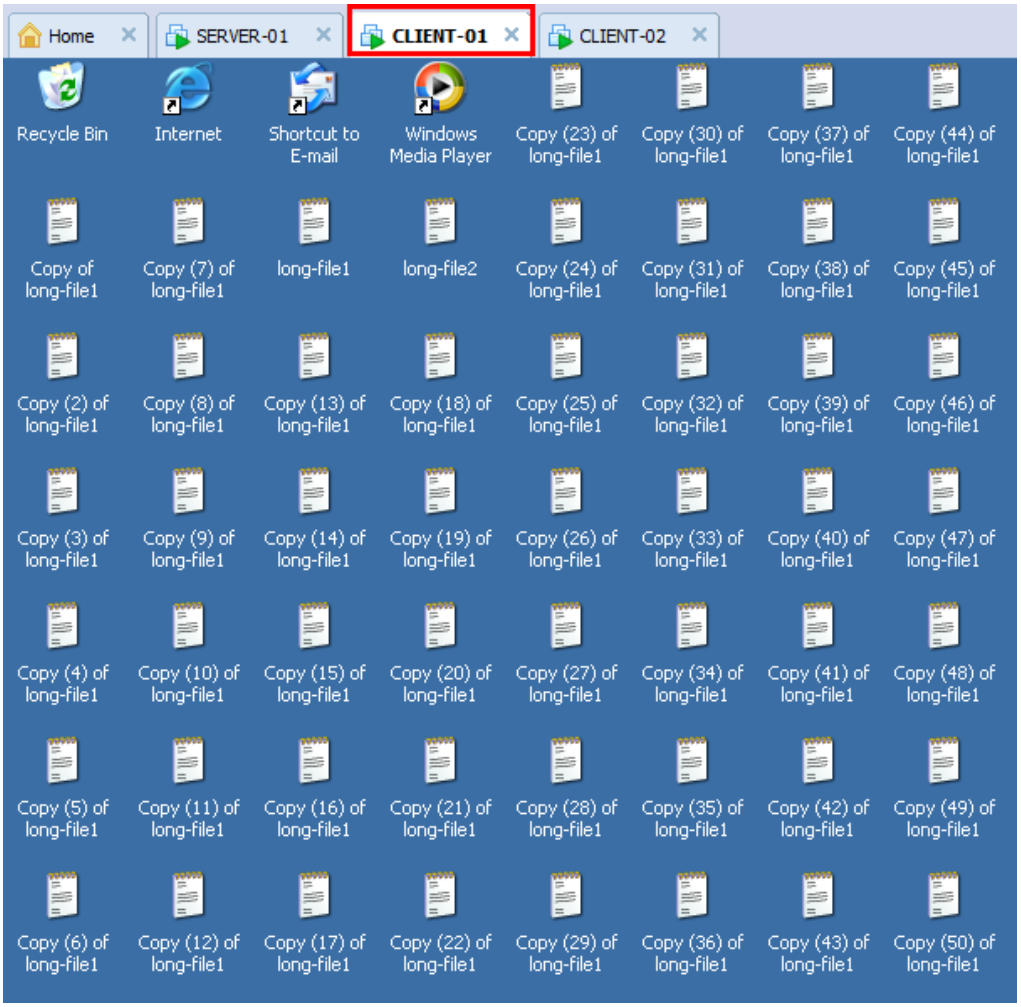
- Tại máy CLIENT-01, user Long đăng nhập vào.
- User Long thực hiện thay đổi màn hình Desktop (chẳng hạn tạo thêm 1 số files ở Desktop)
- Trong quá trình làm việc, Long có tạo một vài files trên Desktop, sau đó log off ra.
- Tại máy CLIENT-02, màn hình Desktop của Long có giống như trên máy CLIENT-01 hay không?

Hướng dẫn

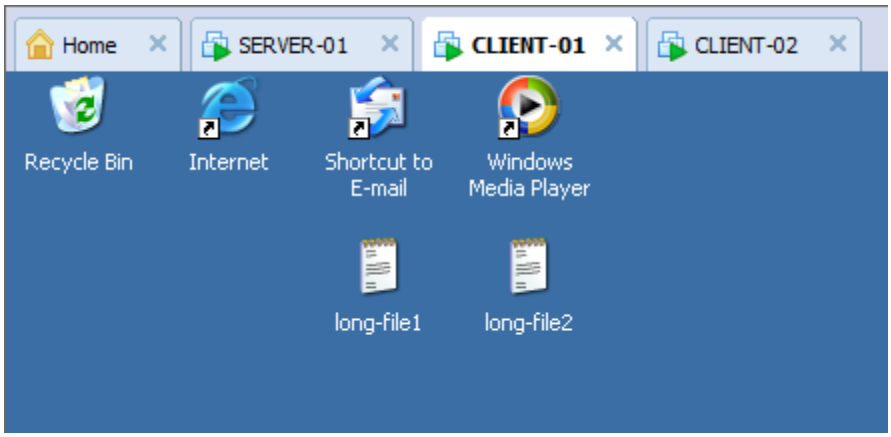
- Tại máy CLIENT-01, đăng nhập với user "long". Màn hình Desktop ban đầu như hình bên dưới:



- Thực hiện thay đổi ở Desktop (chẳng hạn tạo ra nhiều file mới)



- Log off user “long” ra khỏi máy CLIENT-01
- Tại máy CLIENT-02, đăng nhập với user “long”, bạn sẽ thấy Desktop trở lại trạng thái như ban đầu (những files mới được tạo không được lưu vào profile)



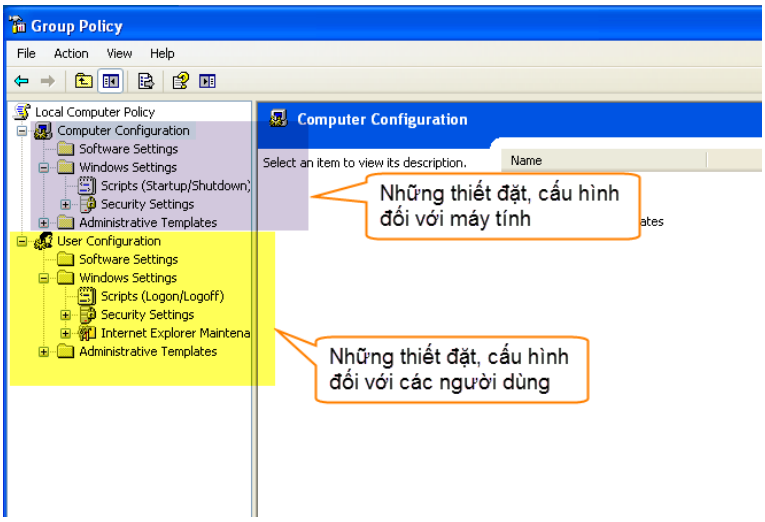
Bài 6: Local group policy

BÀI THỰC HÀNH SỐ 01

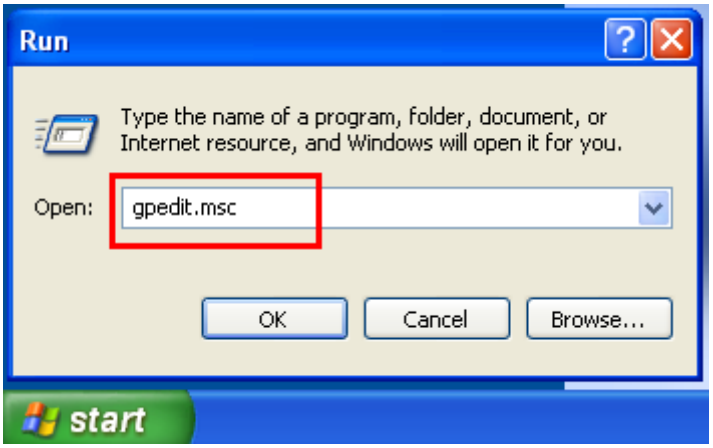
Scripts

Nhắc lại lý thuyết

- **Group Policy Object** (GPO) là những chính sách nhóm, lưu các thiết đặt chính sách với người dùng và máy tính. Chẳng hạn chính sách về mật khẩu, chính sách về khóa tài khoản, chính sách về việc sử dụng Window Explorer…



- **Local Group Policy Object** (Local GPO) là những chính sách nhóm được lưu cục bộ tại máy (không lưu trên Active Directory).
- **Group Policy Object Editor (GPO editor)** là công cụ cho phép chỉnh sửa các đối tượng chính sách (Group Policy Object)
- **Một số cách để truy cập vào GPO editor:**
  - Cách 1: tại Run → gõ lệnh: gpedit.msc



  - Cách 2: sử dụng MMC (còn nhớ cách add một snap-in vào MMC không các bạn?)

Mục tiêu bài thực hành

- Cách thiết lập các chính sách nhóm cục bộ.

Môi trường thực hành

- Máy tính: chỉ cần 1 máy tính sau :
  - Máy **CLIENT-01**cài đặt Window XP, ở chế độ Workgroup.

CLIENT-01

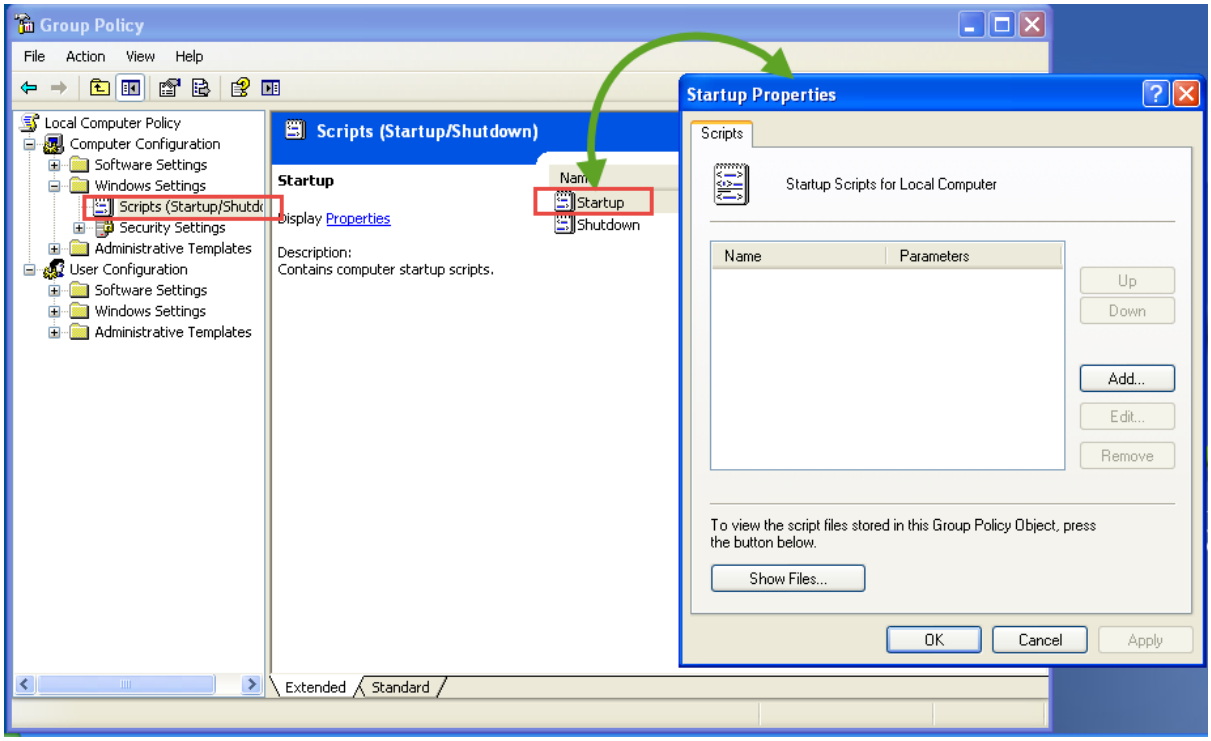
Nếu máy CLIENT-01 của bạn đã join vào domain, thì hãy rút ra khỏi domain, để chúng ta thực hành dễ dàng hơn.
Mục tiêu của bài thực hành này, là tìm hiểu về Local Group Policy, thực hiện trên 1 máy đơn (không liên quan gì tới domain cả).

Câu 12 Scripts startup và shutdown

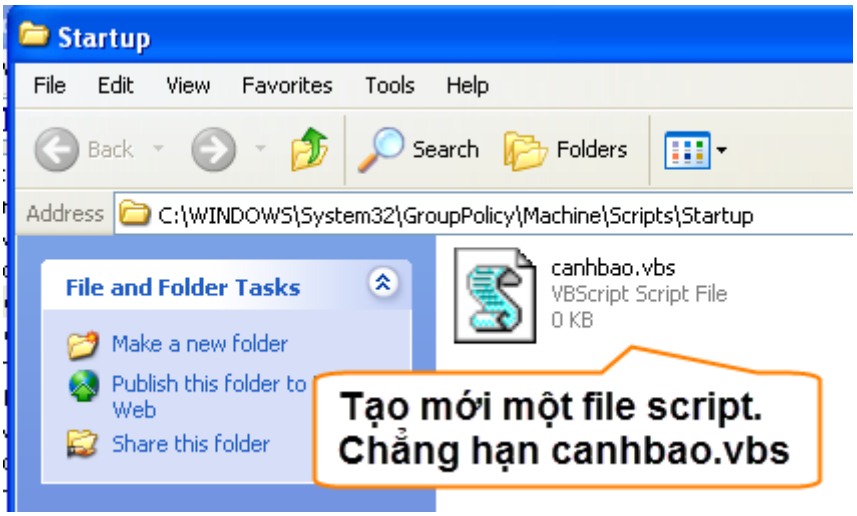
- Công ty ABC muốn nhắc nhở nhân viên mình là: "**Hãy bảo mật dữ liệu của công ty khi sử dụng máy tính**". Họ muốn **khi nhân viên mở máy lên**, thì sẽ có câu nhắc nhở như vậy.
- Đồng thời, **khi nhân viên tắt máy**, có một câu nhắc là: "**Vui lòng tắt các thiết bị điện khi ra về**".
- Bạn là IT cho công ty này, hãy thực hiện yêu cầu trên.

Script cho lúc máy khởi động (Startup)

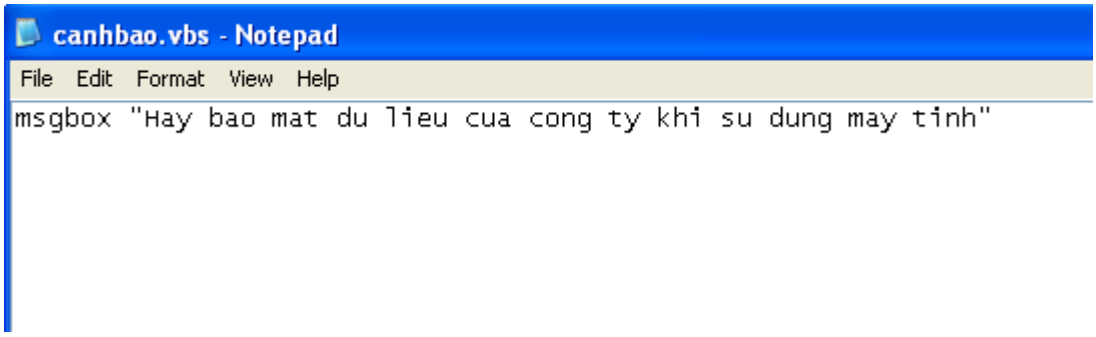
- Mở GPO editor (bằng cách nào tùy các bạn)
- Computer Configuration → Window Settings → Scripts (Startup/Shutdown)
- Nhấp đúp vào Startup



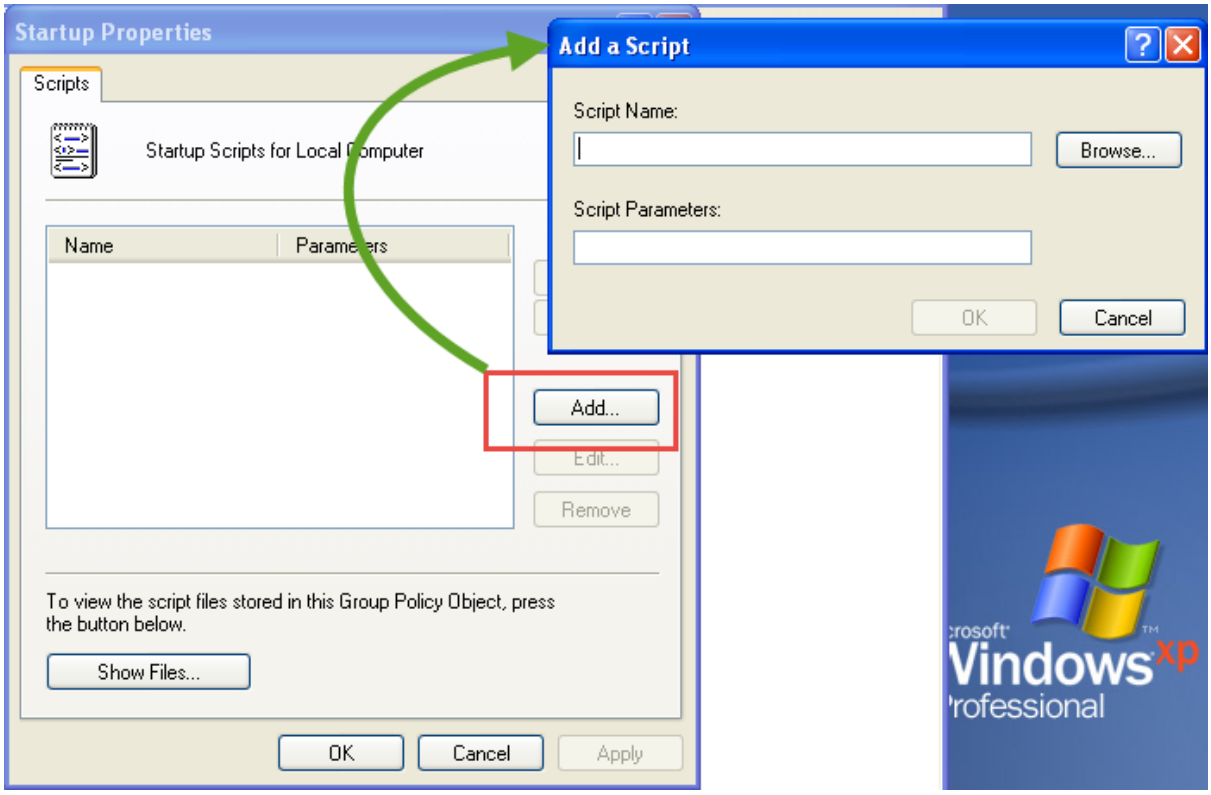
- Trên hộp thoại "Startup", bấm vào nút "Show Files…" để mở ra thư mục chứa các scripts.
- Tại thư mục này, tạo file scripts mới, giả sử đặt tên là canhbao.vbs (vbs là loại scripts dùng ngôn ngữ Visual Basic"



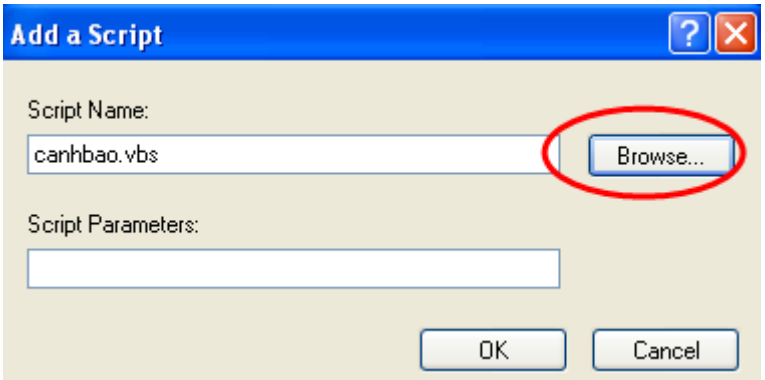
- Edit file scripts này, và ghi vào lệnh hiện thông báo như sau:
  msgbox "Hay bao mat du lieu cua cong ty khi su dung may tinh".
  Lưu ý: Trong ngôn ngữ Visual Basic, lệnh msgbox là lệnh để mở ra hộp thoại thông báo.



- Thực hiện add scripts này vào, bằng cách nhấn nút lệnh "Add"



- Bấm vào nút “Browse” để chọn file script vừa tạo ở trên (file canhbao.vbs)



Script cho lúc tắt máy (Shutdown)

- Làm tương tự như Startup.

Câu 13 Scripts log on và log off

- Hãy thực hiện yêu cầu sau:
    - Khi nhân viên log on vào hệ thống, xuất hiện hộp thoại ghi: "Chào bạn".
    - Khi nhân viên log off khỏi hệ thống, xuất hiện hộp thoại gh: "Tạm biệt".
- Đối với scripts Log on / Log off, thì sẽ gắn liền với Users.
- Chúng ta xây dựng script bằng cách vào "User Configuration → Window Settings → Scripts (Logon/Logoff)

Câu 14 Quyền truy cập Group Policy Editor

- Tạo một tài khoản user:
    - Tên đăng nhập: nv1
    - Mật khẩu: 123
- Log on với tài khoản "nv1"
- Thực hiện mở Group Policy Editor xem có được không?

Bài 6: Local group policy

BÀI THỰC HÀNH SỐ 02

Administrative Templates

Nhắc lại lý thuyết

Administrative Templates là một mục trong Group Policy. Nó có cả ở phần **Computer Configuration** và **User Configuration**.

Administrative Templates bao gồm rất nhiều các chính sách về: Window Components, Start menu and Taskbar, Desktop, Control Panel, Shared Folder, Network, System.

Mục tiêu bài thực hành

- Cách thiết lập các chính sách nhóm cục bộ.

Môi trường thực hành

- Máy tính: chỉ cần 1 máy tính sau :
    - Máy **CLIENT-01**cài đặt Window XP, ở chế độ Workgroup.

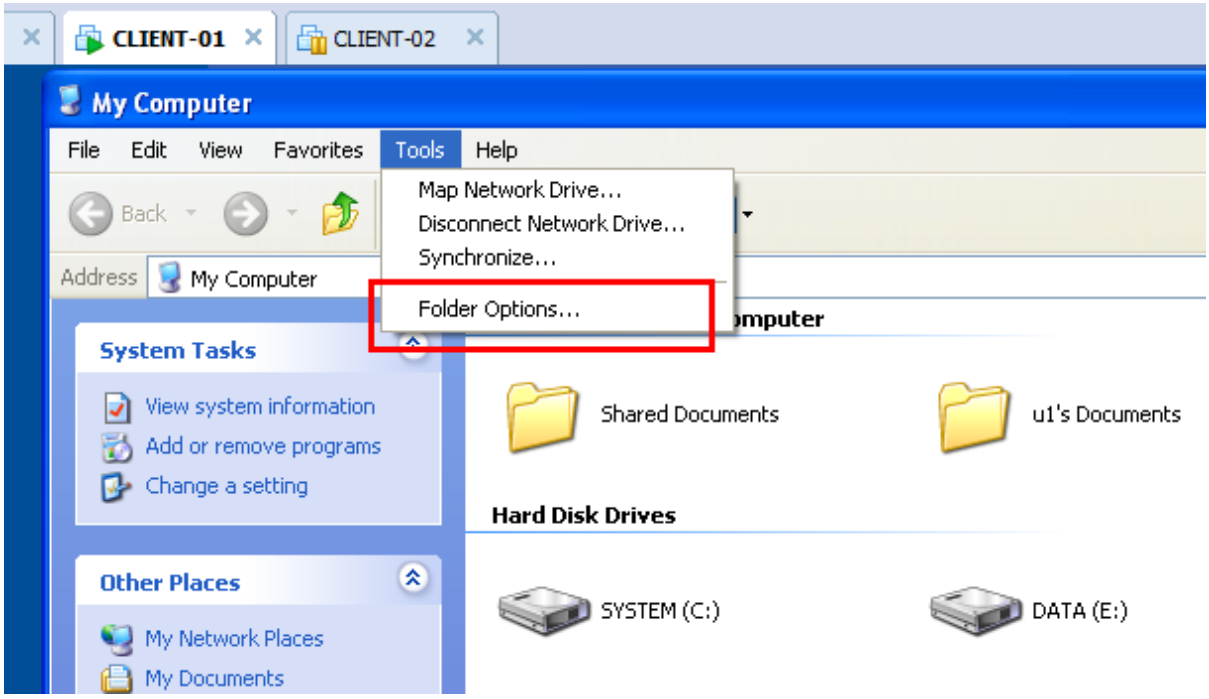
CLIENT-01

Nếu máy CLIENT-01 của bạn đã join vào domain, thì hãy rút ra khỏi domain, để chúng ta thực hành dễ dàng hơn.
Mục tiêu của bài thực hành này, là tìm hiểu về Local Group Policy, thực hiện trên 1 máy đơn (không liên quan gì tới domain cả).

Câu 15 : Window Explorer

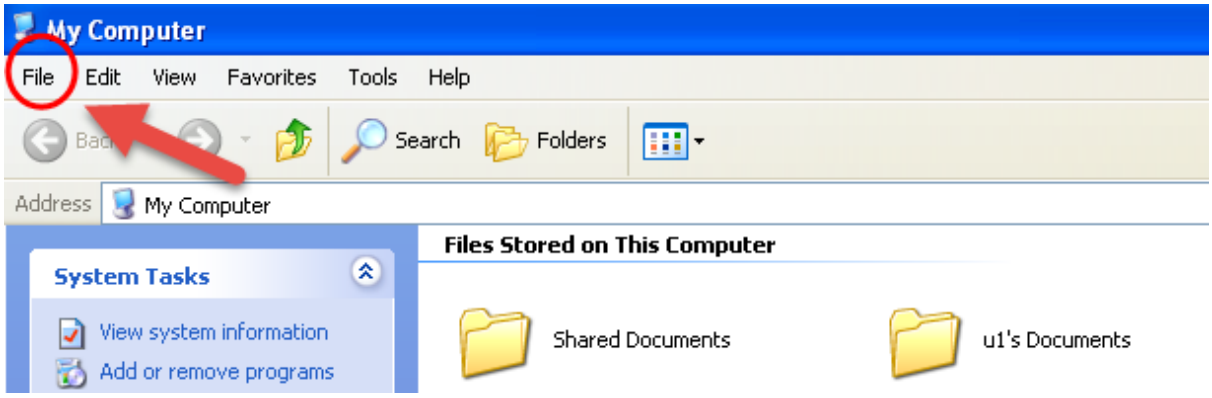
Folder Options:

- Khi máy tính bị nhiễm virus, các file virus thường ở dạng ẩn (hidden files) để che mắt chúng ta.
- Để bật chế độ xem file ẩn: tại Window Explorer → menu "Tools" → bấm vào "Folder Options" và chọn "Show hidden files and folders".
- Tuy nhiên, virus thường sẽ tắt luôn không cho chúng ta truy cập vào mục "**Folder Options**". Hãy chỉ ra cách tắt "**Folder Options**" bằng **group policy**.



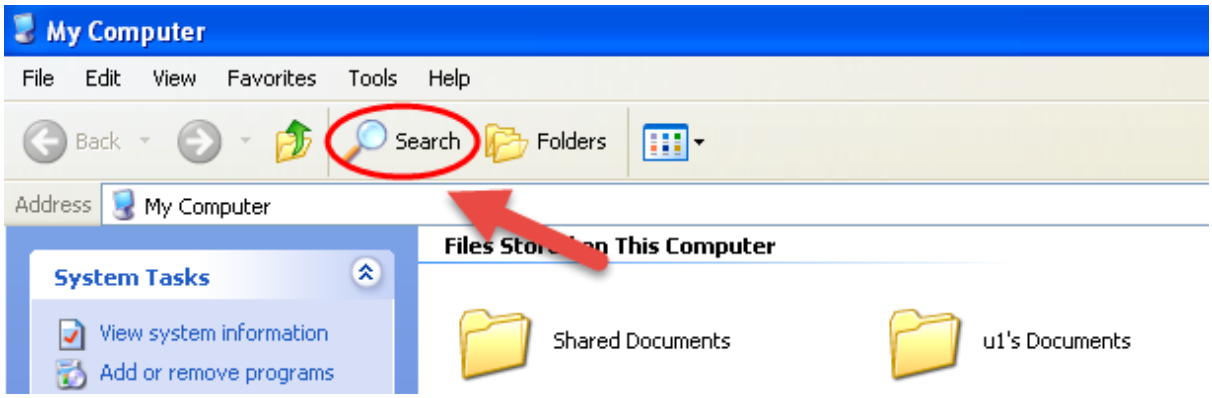
Menu File:

- Hãy ẩn menu File trên cửa sổ Window Explorer.



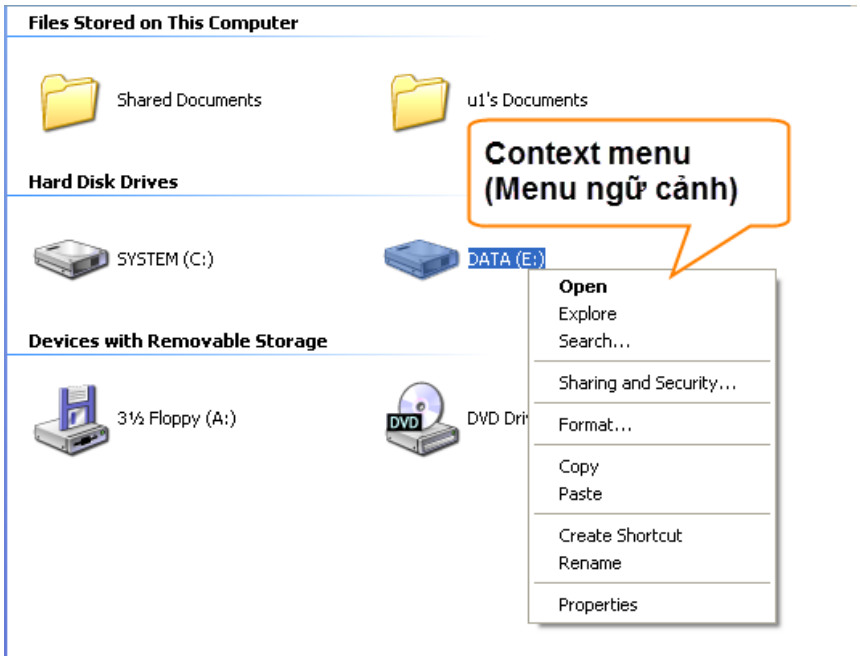
Search button:

- Hãy ẩn nút "Search" trên cửa sổ Window Explorer.



Context menu:

- Context menu (hay còn gọi là menu ngữ cảnh), là menu xuất hiện khi chúng ta nhấp chuột phải.
- Hãy ẩn context menu này.



Ẩn ổ đĩa:

- Giả sử ổ C của bạn chứa hệ điều hành, bạn không muốn mọi người thấy ổ đĩa này để giảm bớt nguy cơ mọi người xóa những file quan trọng. **Hãy thực hiện ẩn ổ đĩa C đi**.
- Sau khi ẩn xong, hãy thử truy cập vào ổ C, bằng cách gõ trực tiếp đường dẫn trên Window Explorer xem có được không?

Cấm truy cập vào ổ đĩa:

- Bây giờ, bạn hãy thực hiện **cấm truy cập** vào ổ đĩa C.
- Thử gõ trực tiếp đường dẫn đến ổ C: trên Window Explorer xem có được không?

Xóa hẳn, không đưa vào Recycle Bin:

- Hãy cấu hình để khi người dùng xóa files/folders, dữ liệu sẽ xóa hẳn, mà không đưa vào Recycle Bin.

Câu 16 : Start menu and Task bar

- Gỡ bỏ icon "**My Documents**" ra khỏi **Start menu**.
- Gỡ bỏ nút "**Run**" và không cho phép user mở hộp thoại "**Run**"
- Gỡ bỏ nút "**Log off**" ra khỏi **Start menu**.
- Gỡ bỏ nút "**Shutdown**" ra khỏi **Start menu**.
- Ẩn **Username** ở **Start menu**.

Câu 17 : Desktop

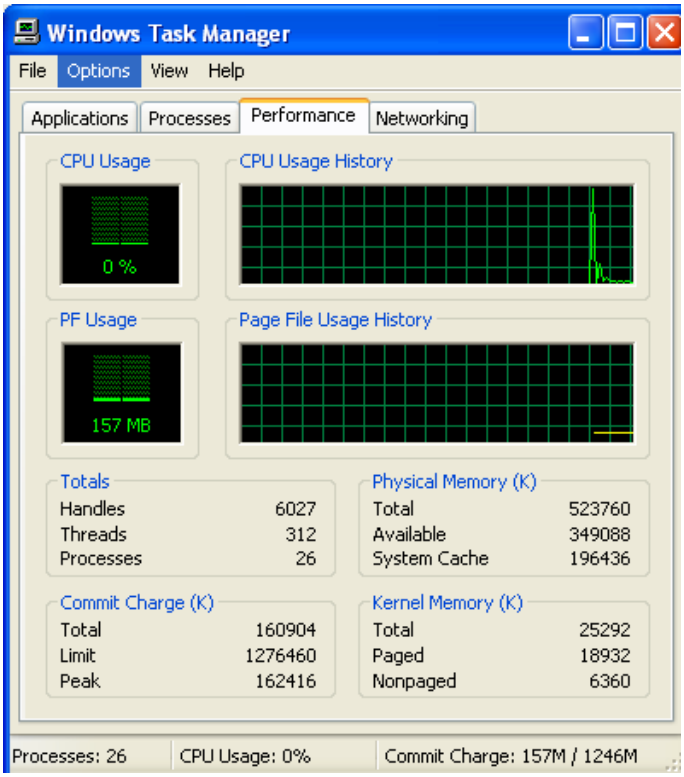
- Gỡ bỏ icon "**My Documents**", "**My Computer**", "**Recycle Bin**" ra khỏi Desktop.
- Không cho phép người dùng truy cập vào lệnh "**Properties**" khi nhấp chuột phải vào "**My Computer**".

Câu 18 : System

- Các virus thường lây nhiễm qua thiết bị lưu trữ ngoài như CD/DVD, USB… Chúng thường tự động chạy khi các thiết bị được cắm vào máy. Để giảm nguy cơ lây nhiễm, chúng ta có thể tắt chế độ "Auto play". Bạn hãy thực hiện **tắt "Auto play"**.

Câu 19 : Ctrl + Alt + Del options

- Thông qua Task Manager, người dùng có thể thực hiện những việc sau:
    - **Ở thẻ Application**: Bật hoặc tắt một chương trình ứng dụng (thường khi một chương trình bị treo, chúng ta dùng cách này để tắt cưỡng ép chương trình đó).
    - **Ở thẻ Processes**: Xem các tiến trình (process) đang chạy trên máy (thường dùng để phát hiện các tiến trình lạ, có thể nghi là virus)
    - **Ở thẻ Performance**: Xem hiệu suất làm việc của máy (CPU, RAM…)
    - **Ở thẻ Networking**: Xem các thông tin liên quan đến mạng.



- Chúng ta có thể truy cập vào Task Manager bằng một số cách như sau:
  - **Cách 1:** Nhấn tổ hợp phí **Ctrl + Alt + Del**
  - **Cách 2:** Nhấp phải chuột vào thanh Task bar, chọn lệnh Task Manager.

- Nếu các bạn ra ngoài tiệm Internet công cộng, thường chúng ta không thể truy cập được vào Task Manager (để tránh việc bật tắt các tiến trình không mong muốn,…)
- Bạn hãy thực hiện "**Ngăn không cho người dùng truy cập vào Task Manager**" bằng group policy.
  (Ghi chú: Nếu virus xâm nhập vào máy tính của chúng ta, chúng cũng sẽ cố gắng ngăn không cho phép truy cập vào Task Manager (để không phát hiện ra virus))

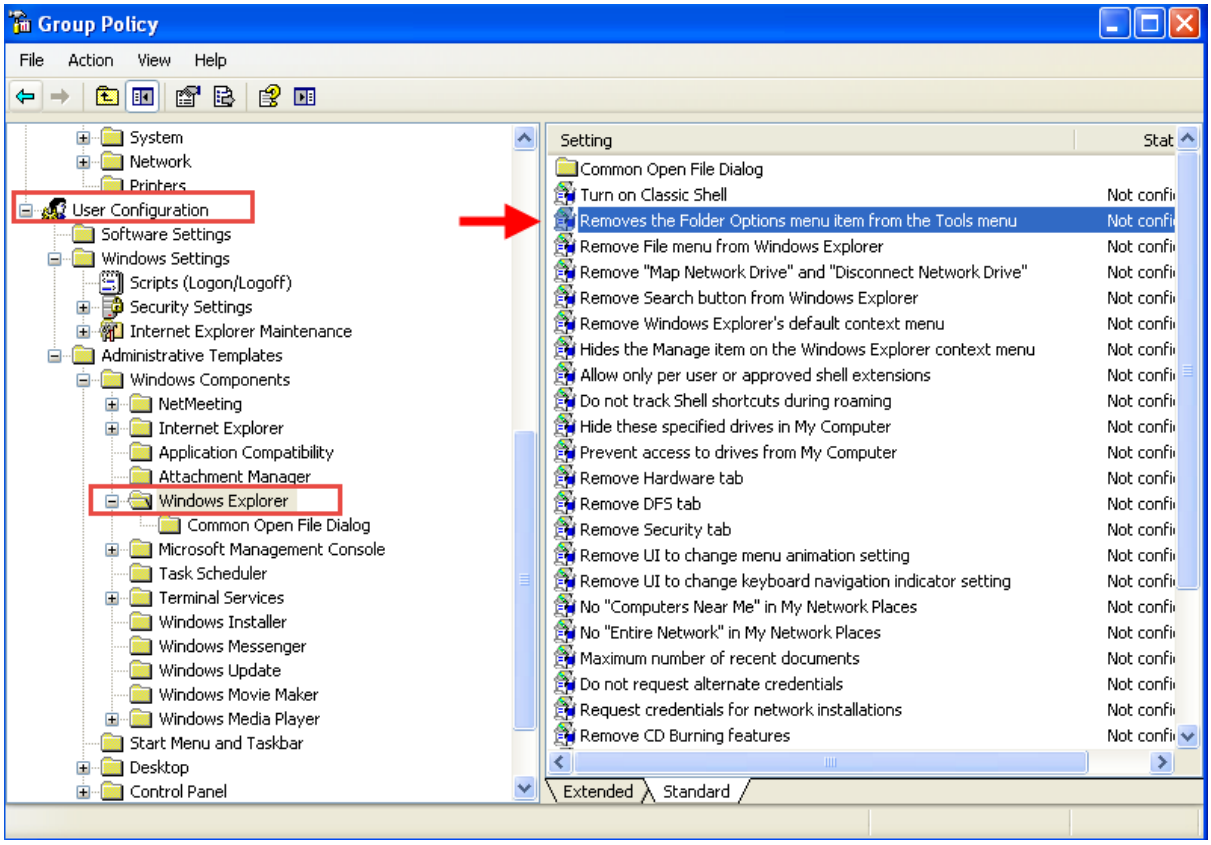
Câu 20 : System

- Trong Window, Registry là một cơ sở dữ liệu rất quan trọng. Nó lưu các thiết đặt, cấu hình về phần cứng, phần mềm và người dùng.
- Người dùng có thể truy cập vào registry bằng cách: **Run** → gõ lệnh: "**regedit**"
- Để tăng tính an toàn cho hệ thống, bạn hãy thực hiện chính sách "Không cho phép người dùng truy cập vào registry".

Hướng dẫn

Folder Options:

Tại mục "User Configuration", → "Administrative Templates" → "Window Components" → "Window Explorer" → Bấm vào mục: "**Removes the Folder Options menu item from the Tools menu**", chọn giá trị **Enable**.



Menu File:

- "**Removes the File menu from My Computer**", chọn **Enable**.

Search button:

- "**Removes Search button from Windows Explorer**", chọn **Enable**.

Context menu:

- "**Removes Windows Explorer's default context menu**", chọn **Enable**.

Ẩn ổ đĩa:

- "**Hide these specified drives in My Computer**", **chọn ẩn ổ C**.

Cấm truy cập vào ổ đĩa:

- "**Prevent access to drives in My Computer**", **chọn ẩn ổ C**

Xóa hẳn, không đưa vào Recycle Bin:

- "**Do not move deleted files to the Recycle Bin**", **chọn Enable.**

Bài 6: Local group policy

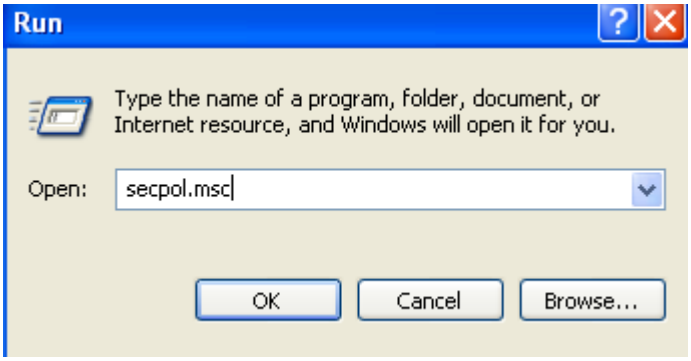
BÀI THỰC HÀNH SỐ 03

Chính sách bảo mật (Security Policies)

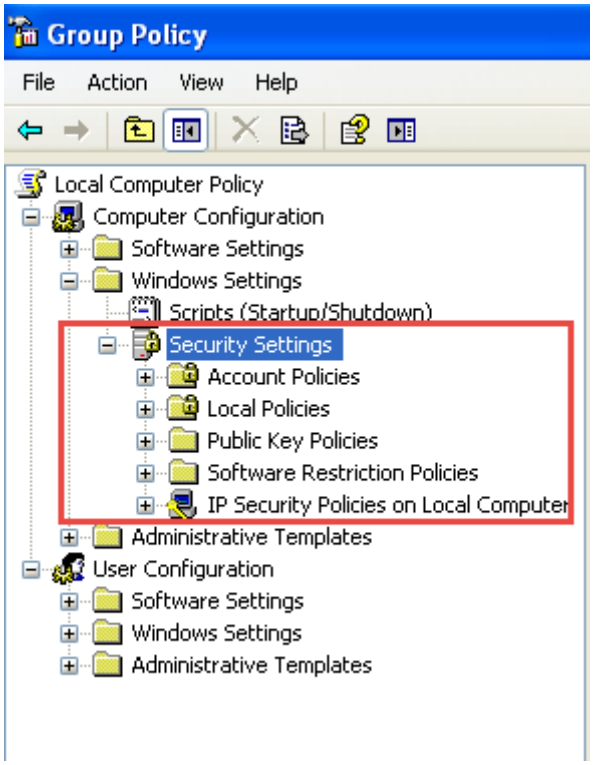
Phần A: Chính sách tài khoản (Account policies)

Nhắc lại lý thuyết

- **Chính sách bảo mật (Security Policy)** là một phần quan trọng thuộc **Group Policy.**
- Chính sách bảo mật bao gồm tất cả các chính sách để đảm bảo hệ thống của chúng ta trở nên an toàn hơn, bảo mật hơn.
- Lấy ví dụ: người dùng khi sử dụng hệ thống của chúng ta, sẽ có nguy cơ là bị đánh cắp mật khẩu. Vậy, chính sách bảo mật sẽ đưa ra một số quy định, để làm giảm nguy cơ này, chẳng hạn:
    - Quy định mật khẩu phải dài 8 ký tự.
    - Quy định mật khẩu phải có ký tự đặc biệt, có ký số, chữ hoa, thường.
- Một ví dụ khác: trước nguy cơ các hacker đánh cắp mật khẩu bằng cách dò mật khẩu (theo kiểu vét cạn chẳng hạn), để giảm nguy cơ này, chúng ta sẽ xây dựng chính sách khóa tài khoản, nếu nhập sai quá 3 lần, sẽ khóa tài khoản, và khóa trong vòng 30 phút chẳng hạn.
- **Vậy, mở Secirity Policy bằng cách nào?** Chúng ta có thể mở Security Policy bằng một số cách dưới đây:
    - **Cách 1:** Run → gõ: **secpol.msc** (secpol là viết tắt của Securit Policy)



    - **Cách 2:** Mở GPO editor (bằng cách dùng lệnh: **gpedit.msc**), và chọn tới mục "**Computer Configuration**" → "**Window Settings**" → "**Security Settings**" (xem hình bên dưới)



- **Chính sách bảo mật bao gồm các mục chính sau *(trong khuôn khổ chương trình học này, chúng ta tạm thời chỉ tìm hiểu 2 mục chính bên dưới):***
    - **Account Policies (Chính sách tài khoản):** gồm các chính sách liên quan tới tài khoản người dùng, ví dụ như:
        - **Chính sách mật khẩu** (các quy định để đảm bảo mật khẩu được an toàn hơn, chẳng hạn mật khẩu phải có độ dài tối thiểu bao nhiêu ký tự? Có yêu cầu ký tự đặc biệt không? Bao lâu thì phải thay đổi mật khẩu 1 lần?...
        - **Chính sách khóa tài khoản**: chẳng hạn nhập sai bao nhiêu lần thì khóa tài khoản, và sẽ khóa trong bao lâu?
    - **Local Policies (Chính sách cục bộ):** gồm các chính sách về quyền của người dùng, các tùy chọn bảo mật…

Mục tiêu bài thực hành

- Cách thiết lập các chính sách tài khoản.

Môi trường thực hành

- Máy tính: chỉ cần 1 máy tính sau :
    - Máy **CLIENT-01**cài đặt Window XP, ở chế độ Workgroup.

CLIENT-01

Nếu máy CLIENT-01 của bạn đã join vào domain, thì hãy rút ra khỏi domain, để chúng ta thực hành dễ dàng hơn.
Mục tiêu của bài thực hành này, là tìm hiểu về Local Group Policy, thực hiện trên 1 máy đơn (không liên quan gì tới domain cả).

Câu 21 Mật khẩu phức tạp

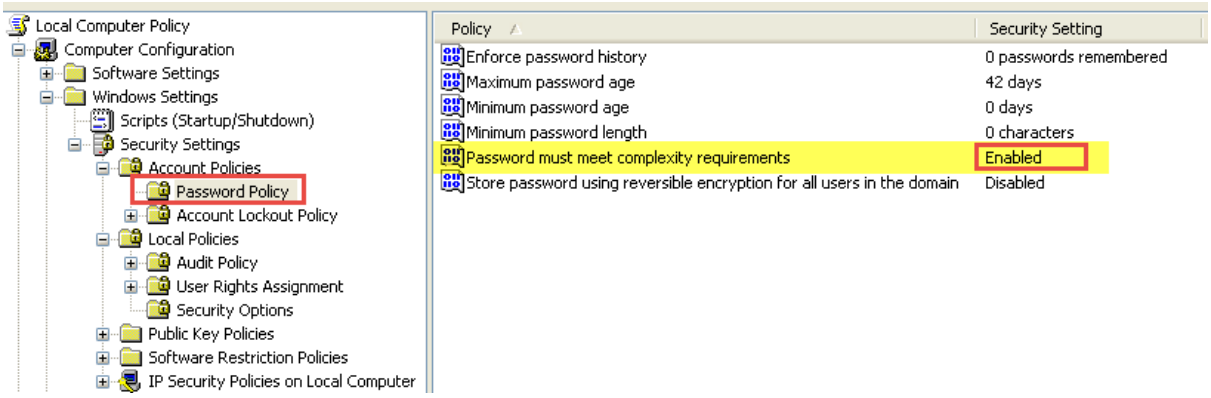
- Thiết lập chính sách để **yêu cầu password của user phải phức tạp**.
- Tiếp theo, tạo một user với mật khẩu đơn giản xem có báo lỗi gì không?
    - Tên user: **u1**
    - Password: **123** *(cố tình nhập mật khẩu đơn giản là 123)*
- Kiểm tra xem thông báo lỗi gì?
- Thực hiện tạo user trên với password phức tạp (chẳng hạn: **123abc!**)

Password phức tạp nghĩa là phải chứa các ký tự thuộc 3 trong 4 nhóm sau:

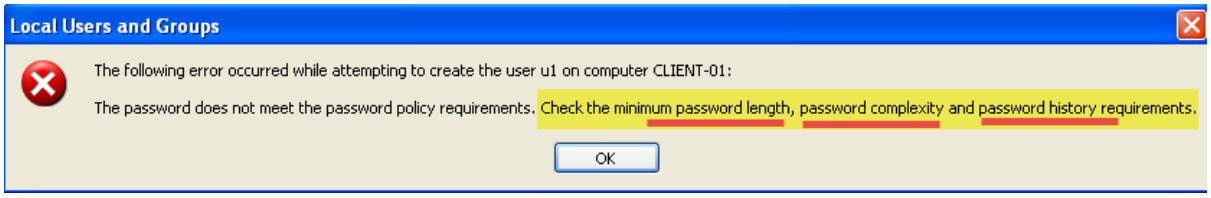
- Ký tự hoa (từ A → Z)
- Ký tự thường (từ a → z)
- Ký số (từ 0 → 9)
- Ký tự đặc biệt (ví dụ: !, $, #, %)

Ví dụ: password sau là phức tạp: 123abc!

- Mở Security Policy → Account Policies → Password Policies
- Ở thuộc tính: "Password must meet complexity requirements", chọn "Enable"



- Sau khi thiết đặt yêu cầu mật khẩu phức tạp, nếu cố tình tạo user với mật khẩu đơn giản, sẽ nhận được thông báo lỗi sau:

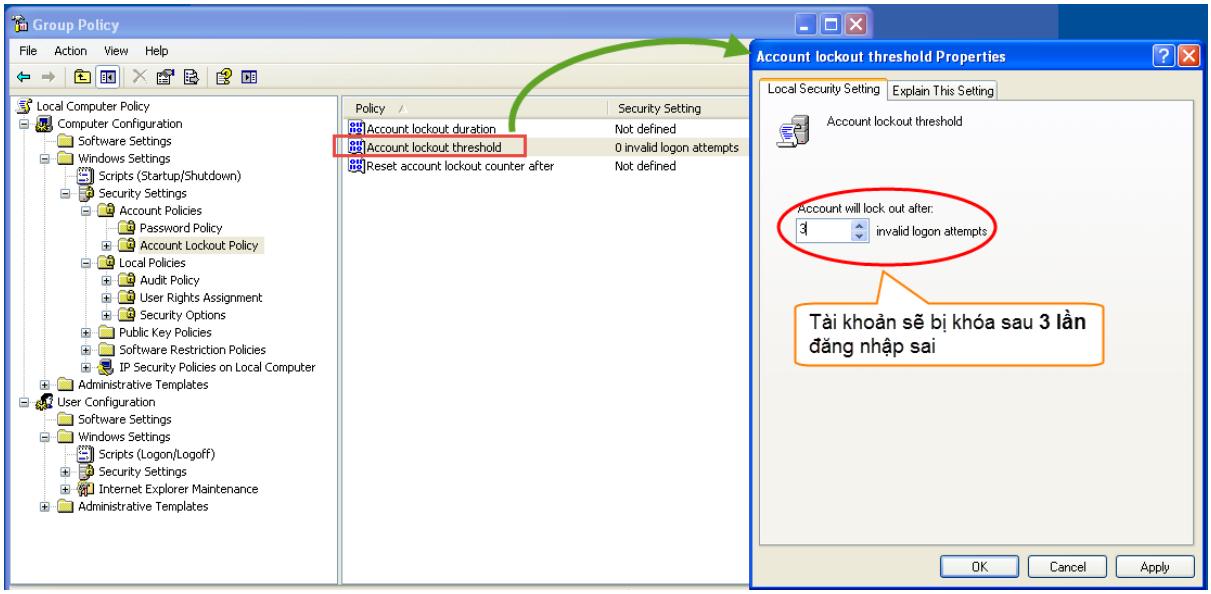


Câu 22 Chiều dài tối thiểu của mật khẩu

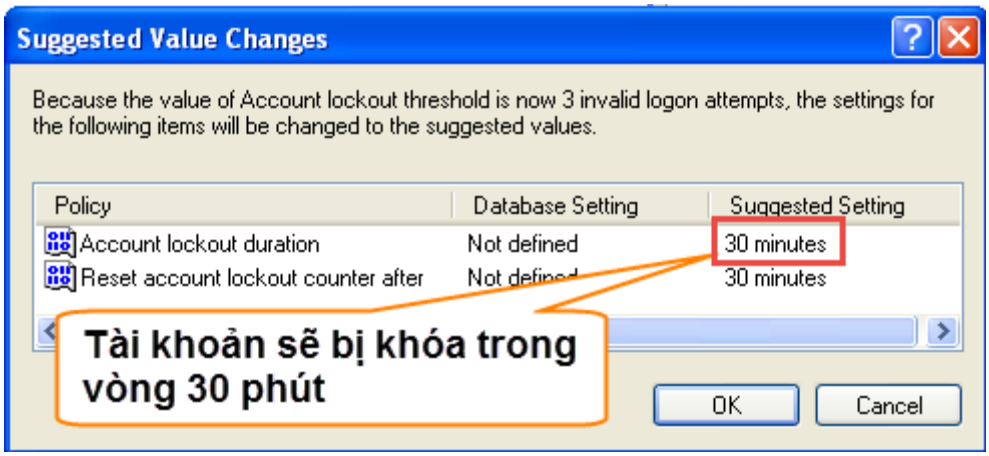
- Thiết lập 2 chính sách sau:
  - **Cho phép password đơn giản**.
  - Yêu cầu độ dài password **tối thiểu là 8 ký tự**.
- Tạo user:
  - Tên user: **u2**
  - Password: **123**
- Có lỗi gì không? Nếu có thì thông báo là gì?
- Thực hiện tạo lại user trên, với password là: **12345678**.
- Chiều dài tối thiểu của mật khẩu được quy định bởi thuộc tính: "**Minimum password length**"

Câu 23 Chính sách khóa tài khoản

- Thiết lập chính sách để:
  - Nếu người dùng đăng nhập sai mật khẩu quá 3 lần, tài khoản sẽ bị khóa
  - Thời gian khóa tài khoản: 2 phút
- Thực hiện đăng nhập vào CLIENT-01, với tài khoản u1 (đã tạo ở câu trên), nhưng cố tình nhập sai mật khẩu quá 3 lần → Hỏi có thông báo lỗi gì?
- Sau khi bị khóa tài khoản, cố tình đăng nhập tiếp có được không?
- **Đợi sau 2 phút**, đăng nhập lại xem có được không?
- Khóa tài khoản sau 3 lần đăng nhập sai (**Account lockout threshold**)



- Khi chúng ta thiết đặt giá trị cho "Account lockout threshold", thì 2 thuộc tính "Thời gian khóa tài khoản" (Account lockout duration) và "Thời gian reset bộ đếm số lần đăng nhập sai" (Reset Account lockout counter after) sẽ nhận giá trị mặc định là 30 phút. (Chúng ta có thể điều chỉnh sau nếu muốn)



Bài 6: Local group policy

BÀI THỰC HÀNH SỐ 04

Chính sách bảo mật (Security Policies)

Phần B: Chính sách cục bộ (Local Policies)

Nhắc lại lý thuyết

- **Chính sách bảo mật (Security Policy)** là một phần quan trọng thuộc **Group Policy.**
- Chính sách bảo mật bao gồm tất cả các chính sách để đảm bảo hệ thống của chúng ta trở nên an toàn hơn, bảo mật hơn.
- Trong chương trình học này, chúng ta tìm hiểu 2 phần rất quan trọng trong chính sách bảo mật:
    - Phần A: Chính sách tài khoản (Account Policies)
    - Phần B: Chính sách cục bộ (Local Policies)
- Ở bài trước, chúng ta đã thực hành với phần A, ở bài này chúng ta sẽ tìm hiểu phần B.
- **Các phần quan trong của chính sách cục bộ (Local Policies)**
    - **Audit Policy**: các chính sách để ghi nhận các sự kiện xảy ra trong hệ thống. Chẳng hạn ghi nhận lại sự kiện user đăng nhập, sự kiện tạo mới một group, một user, hay sự kiện thay đổi mật khẩu…
    - **User Rights Assigment (cấp quyền cho user)**: phần này sẽ cấp cho người dùng/nhóm có những quyền gì trên hệ thống?
    - **Security Options**: các tùy chọn bảo mật, chẳng hạn thay đổi tên đăng nhập của tài khoản "administrator".

Mục tiêu bài thực hành

- Cách thiết lập các chính sách cục bộ.

Môi trường thực hành

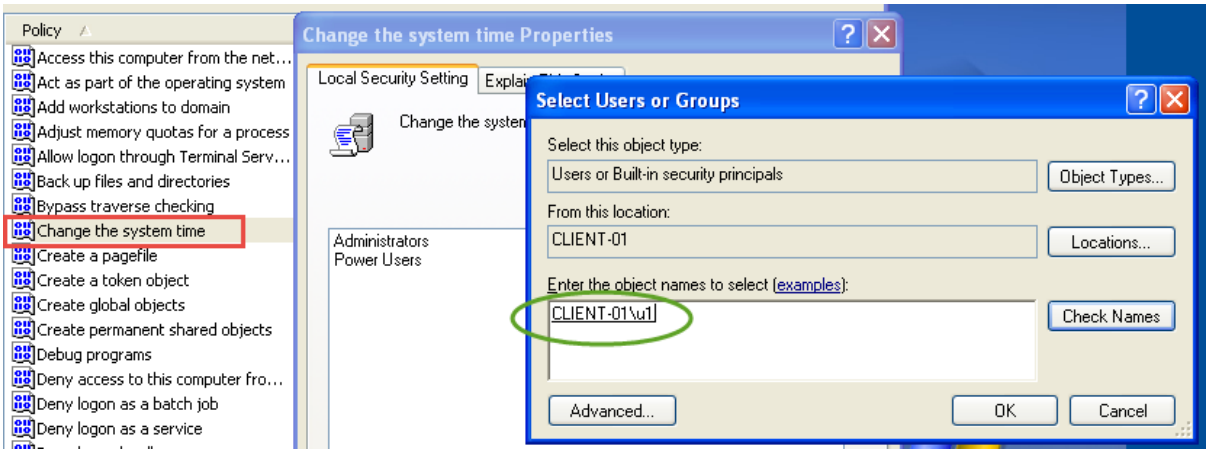
- Máy tính: chỉ cần 1 máy tính sau :
  - Máy **CLIENT-01**cài đặt Window XP, ở chế độ Workgroup.

CLIENT-01

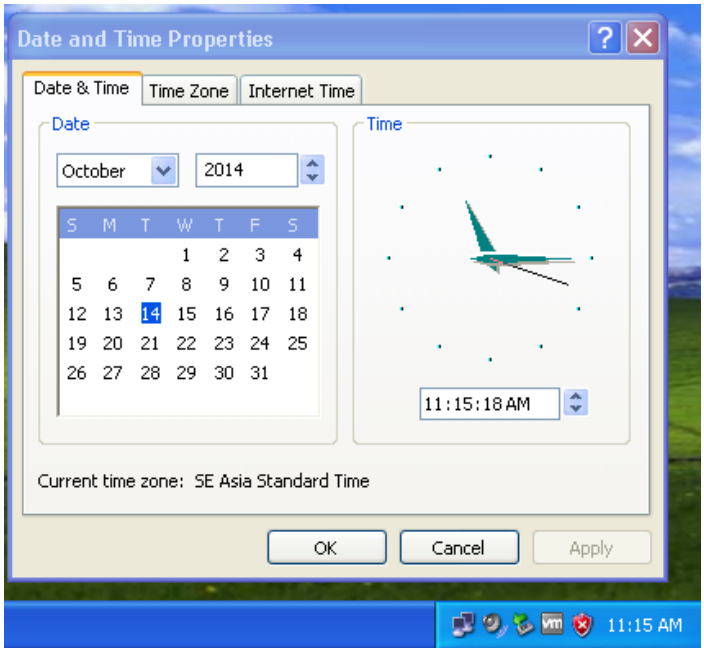
Câu 24 : Quyền thay đổi thời gian hệ thống

- Mặc định, đối với máy trạm (workstation), chỉ có những người thuộc nhóm: **Administrators** và **Power Users** mới được quyền thay đổi giờ hệ thống. Hãy thực hiện một thí nghiệm sau:
  - Tại máy CLIENT-01, đăng nhập với tài khoản u1 (tài khoản này chỉ thuộc nhóm Users)
  - Thử thay đổi giờ hệ thống xem có thông báo lỗi gì không?
- Bây giờ, hãy đăng nhập với tài khoản **administrator**, thiết lập chính sách để cho phép người dùng "**u1**" cũng được phép thay đổi thời gian hệ thống.
- Khi user "u1" thay đổi giờ hệ thống, sẽ có thông báo lỗi:
  "You do not have the proper privilege level to change the System Time."

- Để cho phép "u1" có quyền thay đổi giờ hệ thống, chúng ta thực hiện như sau:
  Mở Security Policy → Local Policies → User Rights Assigment → Tại thuộc tính "Change the System time", add user "u1" vào.
  (Lưu ý: như các bạn thấy, mặc định đã có 2 group được phép thay đổi giờ hệ thống là: Administrators và Power Users)

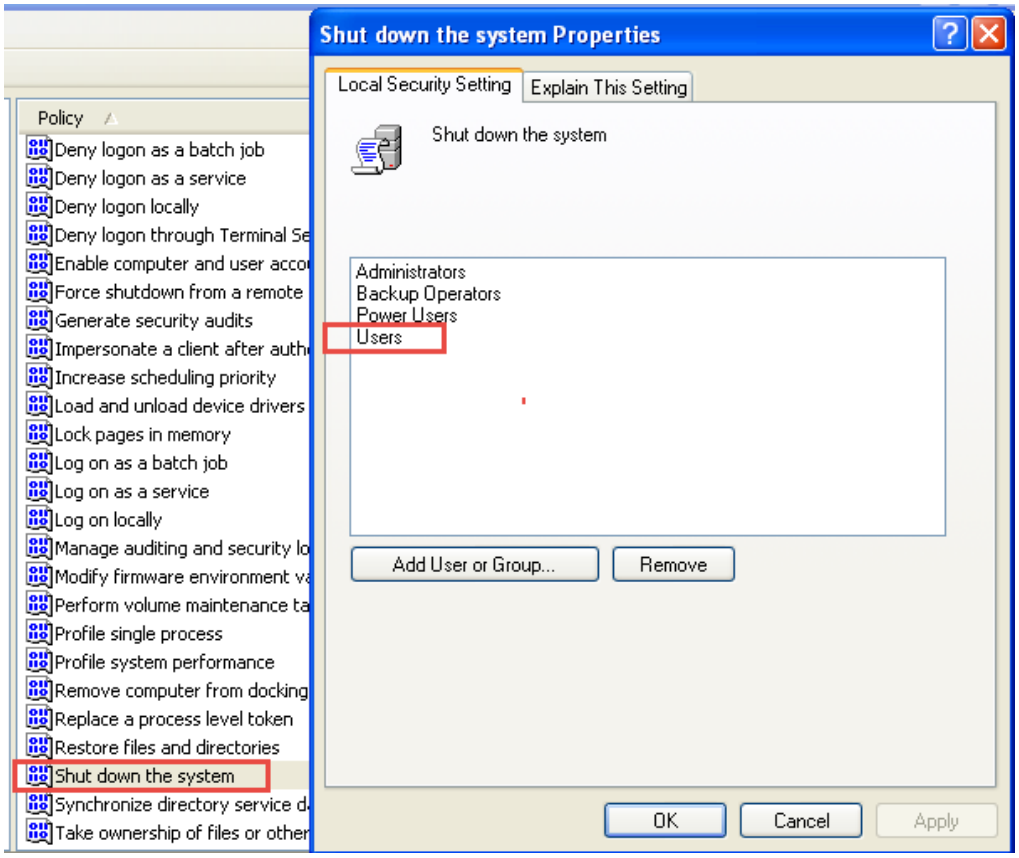


- Sau khi cấp quyền thì "u1" có thể thay đổi giờ hệ thống:



Câu 25 : Shutdown máy tính

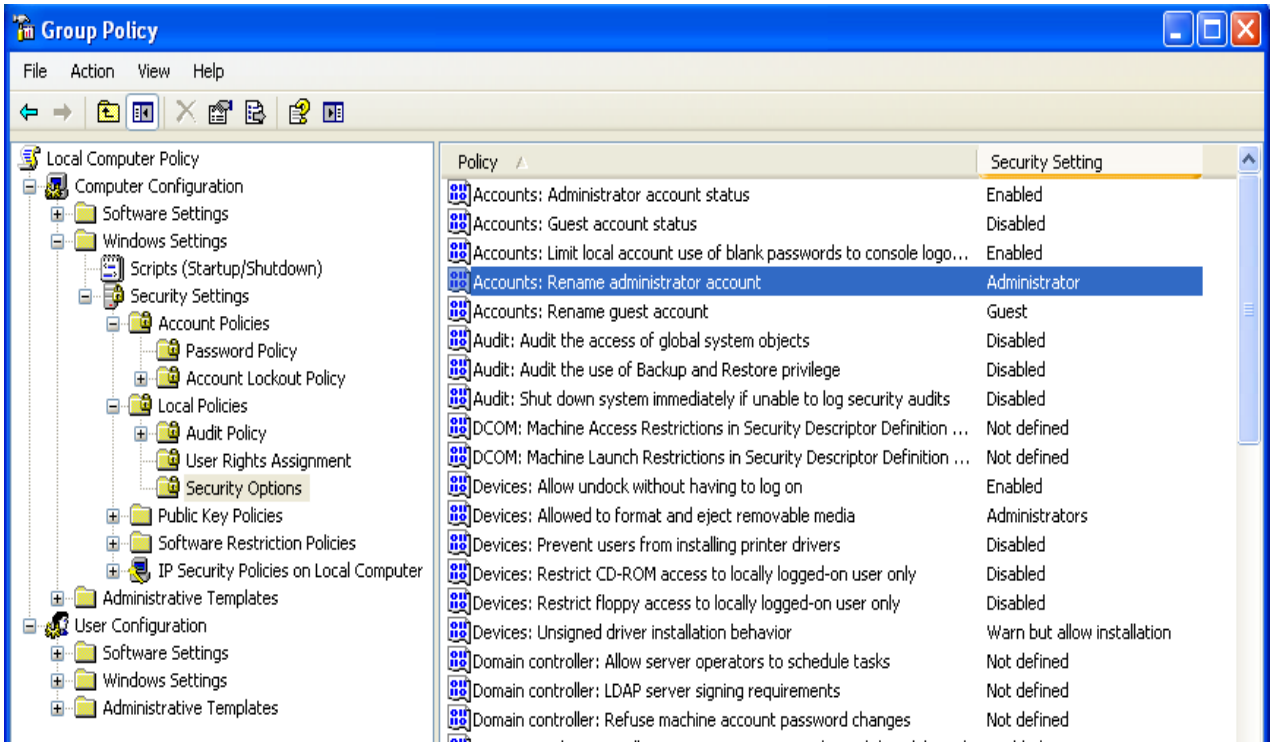
- Trên máy CLIENT-01, thiết đặt chính sách để chỉ cho phép những user trong các group sau mới có thể thực hiện shutdown máy tính:
    - Administrators
    - Backup Operators
    - Power Users
- Còn các user bình thường, không được tắt máy. (Chẳng hạn user "**u1**" đã tạo ở bài tập trước, chỉ thuộc group "**Users**" → sẽ không có quyền tắt máy.
- Để cấp quyền cho những nhóm/người dùng nào có thể shutdown máy tính, chúng ta vào mục: **User Right Assigment** → thuộc tính "**Shutdown the system**"



Câu 26 : Thay đổi tên mặc định của Administrator

- Tài khoản người quản trị mặc định thường là "administrator". Để giảm nguy cơ bị tấn công, người ta thường thay đổi tên đăng nhập mặc định này, khi đó, hacker sẽ phải đoán cả tên đăng nhập và mật khẩu.
- Bạn là người quản trị mạng, hãy thay đổi tên đăng nhập "**administrator**" thành "**admin**" bằng group policy. (Đây chỉ là ví dụ, trên thực tế, các bạn có thể đổi thành bất cứ tên gì khác cũng được)

Local Policies → Security Options → "Accounts: Rename admistrator account"


Group Policy
File Action View Help
Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Local Policies
Audit Policy
User Rights Assignment
Security Options
Public Key Policies
Software Restriction Policies
IP Security Policies on Local Computer
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Policy
Security Setting
Accounts: Administrator account status Enabled
Accounts: Guest account status Disabled
Accounts: Limit local account use of blank passwords to console logo... Enabled
Accounts: Rename administrator account Administrator
Accounts: Rename guest account Guest
Audit: Audit the access of global system objects Disabled
Audit: Audit the use of Backup and Restore privilege Disabled
Audit: Shut down system immediately if unable to log security audits Disabled
DCOM: Machine Access Restrictions in Security Descriptor Definition ... Not defined
DCOM: Machine Launch Restrictions in Security Descriptor Definition ... Not defined
Devices: Allow undock without having to log on Enabled
Devices: Allowed to format and eject removable media Administrators
Devices: Prevent users from installing printer drivers Disabled
Devices: Restrict CD-ROM access to locally logged-on user only Disabled
Devices: Restrict floppy access to locally logged-on user only Disabled
Devices: Unsigned driver installation behavior Warn but allow installation
Domain controller: Allow server operators to schedule tasks Not defined
Domain controller: LDAP server signing requirements Not defined
Domain controller: Refuse machine account password changes Not defined

Bài 7: Domain group policy

BÀI THỰC HÀNH SỐ 01

Scripts

Nhắc lại lý thuyết

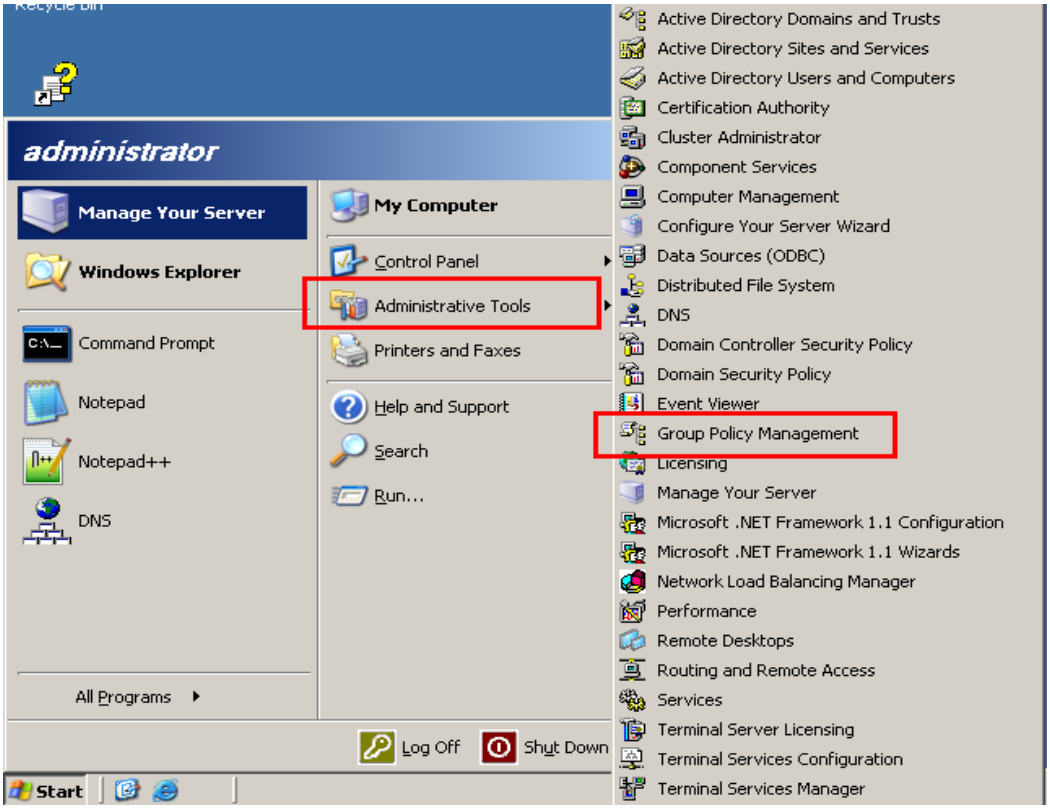
- **Group Policy Object** (GPO) là những đối tượng chính sách nhóm, lưu các thiết đặt chính sách với người dùng và máy tính. Chẳng hạn chính sách về mật khẩu, chính sách về khóa tài khoản, chính sách về việc sử dụng Window Explorer…
- Các chính sách nhóm này (GPO) có thể được **lưu tại máy cục bộ** (Local group policy) **hoặc lưu trên Active Directory**.

Dùng công cụ gì để quản lý chính sách nhóm trên Domain:

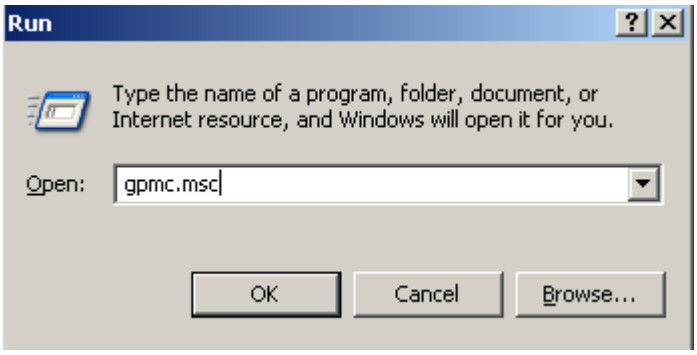
- Công cụ **Group Policy Managemenet Console (GPMC)** là một công cụ quản lý chính sách nhóm của Microsoft. Đối với máy Window Server 2008 trở lên, công cụ này đã được tích hợp sẵn. Tuy nhiên, với Window Server 2003, thì chúng ta phải download về từ trang của Microsoft và cài đặt.
- Download: http://www.microsoft.com/en-us/download/details.aspx?id=21895

Mở công cụ GPMC bằng cách nào?

- Dùng một số cách sau đây:
  Cách 1: Start → Administrative Tools → Group Policy Management

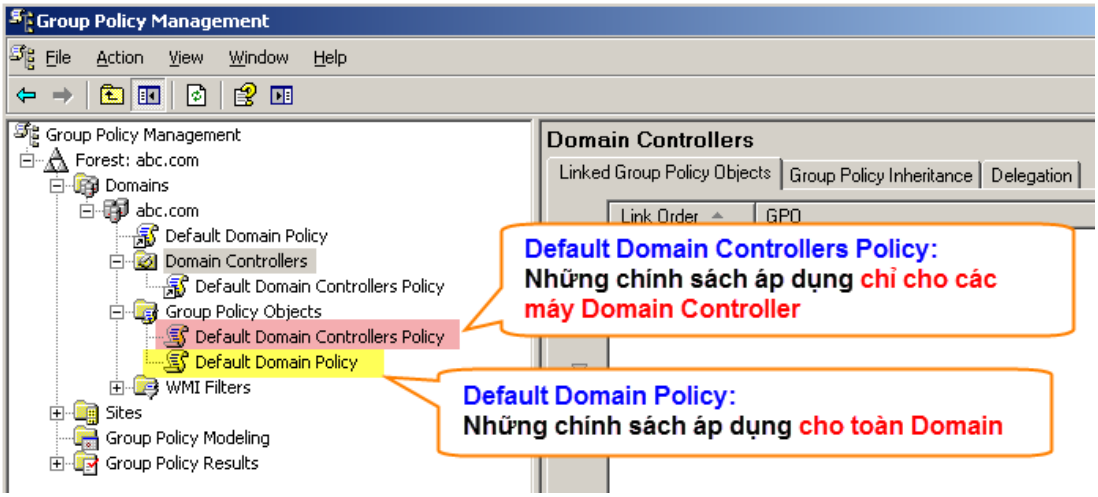


Cách 2: Run → gõ lệnh "**gpmc.msc**"



Giao diện GPMC như thế nào?

- Và đây là giao diện của GPMC:



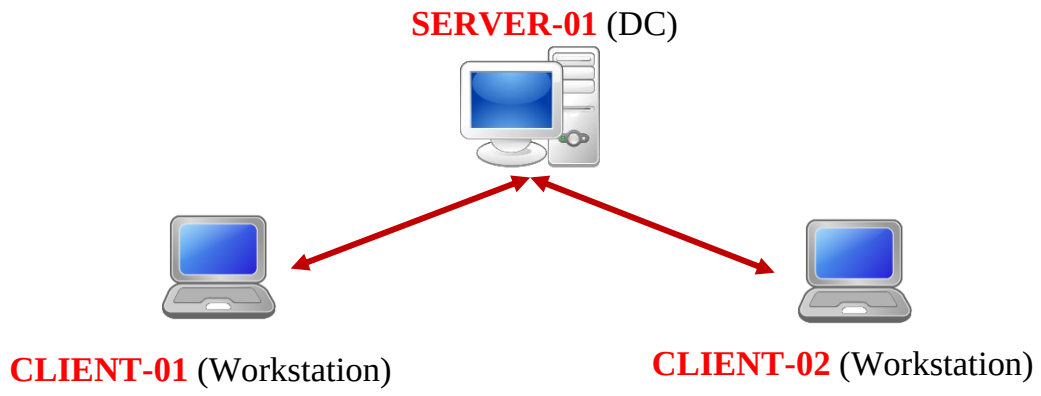
- Có 2 đối tượng chính sách nhóm mặc đinh:
    - **Default Domain Controllers Policy:** gồm những chính sách được áp dụng chỉ cho các máy Domain Controller.
    - **Default Domain Policy:** gồm những chính sách được áp dụng cho toàn domain (toàn miền).
- Ngoài 2 đối tượng chính sách nhóm mặc định, chúng ta cũng có thể tạo ra những đối tượng chính sách nhóm mới theo nhu cầu. Chẳng hạn, tạo mới một đối tượng chính sách nhóm, để cấm người dùng ở các máy trạm truy cập vào registry,…
- Chúng ta có thể xem tất cả các đối tượng chính sách nhóm (GPO) trong mục "**Group Policy Objects**" (như trên hình)

Mục tiêu bài thực hành

- Cách thiết lập chính sách nhóm liên quan tới Script.

Môi trường thực hành

- Máy tính: gồm các máy sau :
    - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
    - Máy **CLIENT-01**, **CLIENT-02,** cài đặt Window XP, đóng vai trò máy trạm.



- Tên miền : **abc.com**
- Máy CLIENT-01, CLIENT-02 đã gia nhập vào miền trên.

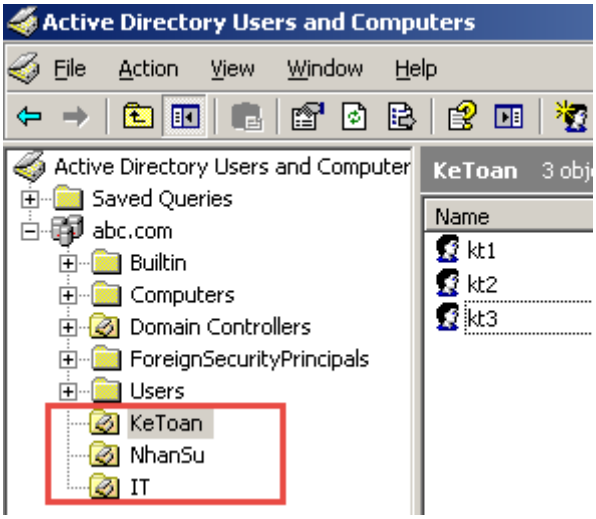
Câu 27 : Cài đặt Group Policy Management Console

- Bạn hãy tải công cụ GPMC về và cài đặt lên máy SERVER-01.

Câu 28 : Tạo các OU, Users

- Để chuẩn bị cho bài thực hành, hãy tạo các OU, Users như cấu trúc bên dưới:
- Các OU:
    - **KeToan**. Gồm 3 users: **kt1**, **kt2**, **kt3** (password: **123abc!**)
    - **NhanSu**. Gồm 3 users: **ns1**, **ns2**, **ns3** (password: **123abc!**)

- **IT**. Gồm 2 users: **it1**, **it2** (password: **123abc!**)



Câu 29 :Ánh xạ ổ đĩa mạng (Mapping Network Drive manually)

- Công ty ABC có một nhu cầu như sau: họ muốn có **một thư mục dùng chung**, chia sẻ cho toàn bộ nhân viên thuộc miền **abc.com**. Ai cũng có thể truy cập vào thư mục này để chia sẻ file cho nhau.
- Bạn là một nhân viên trong công ty này, bạn đề xuất rằng:
    - Tạo một thư mục dùng chung trên SERVER-01, giả sử lưu tại C:\Public (Chia sẻ thư mục này cho Everyone với quyền Full Control)
    - Tại máy trạm, khi nhân viên đăng nhập vào, họ mở **Window Explorer → Tools → Map Network Drive** và thực hiện ánh xạ ổ đĩa mạng vào thư mục "Public" trên Server.
- Hãy hướng dẫn cụ thể cách làm trên.

Câu 30 :Ánh xạ ổ đĩa mạng bằng Log on script

- Với cách ánh xạ ổ đĩa mạng bằng tay như trên sẽ gây nhiều phiền phức cho nhân viên. Mỗi lần họ vào một máy mới, họ phải tự tay làm lại thao tác ánh xạ ổ đĩa mạng.
- Bạn là nhân viên IT, bạn đề xuất hướng giải quyết như sau:
    - Sử dụng Log on script để mỗi khi người dùng đăng nhập vào hệ thống, sẽ có 1 script tự động chạy, thực hiện việc ánh xạ ổ đĩa mạng.
- Bạn hãy hiện thực đề xuất trên.

Câu 31 : GPO liên kết với một OU

- Công ty ABC rất hài lòng với giải pháp mới của bạn.
- Bây giờ, có một yêu cầu mới như sau: ngoài thư mục Public dùng chung cho cả công ty, phòng Kế Toán muốn có một thư mục dùng chung cho phòng của họ (giả sử đặt tên là: **PublicKeToan**), khi nhân viên thuộc phòng kế toán đăng nhập vào hệ thống, sẽ có 2 ổ đĩa mạng hiện ra:
    - **Z**: liên kết tới thư mục **Public** trên Server
    - **Y**: liên kết tới thư mục **PublicKeToan** trên Server
- Bạn hãy thực hiện yêu cầu trên.

Hướng dẫn thực hành

Câu 32 : Cài đặt công cụ Group Policy Management Console

Câu 33 : Tạo các OU, Users

- Xem lại các bài tập tạo OU, Users.

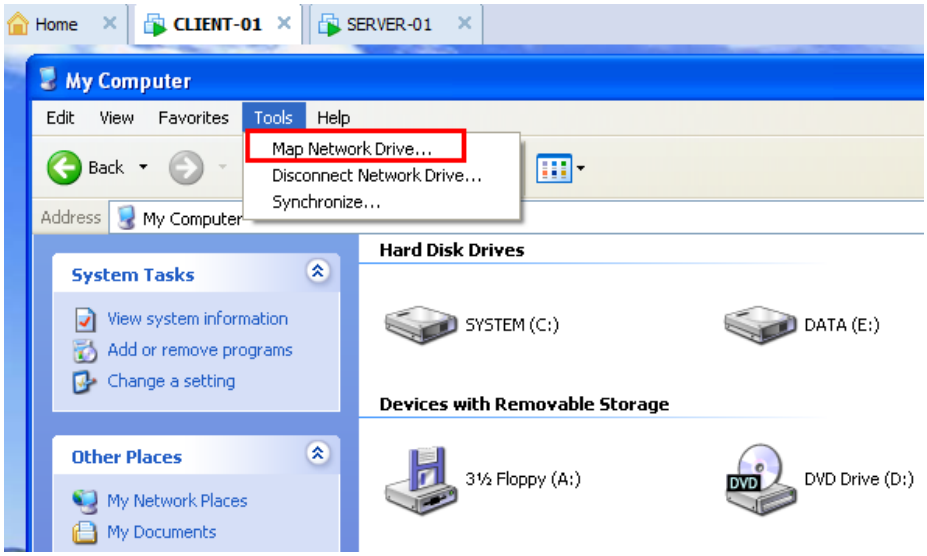
Câu 34 : Ánh xạ ổ đĩa mạng (Mapping Network Drive manually)

Bước 1:

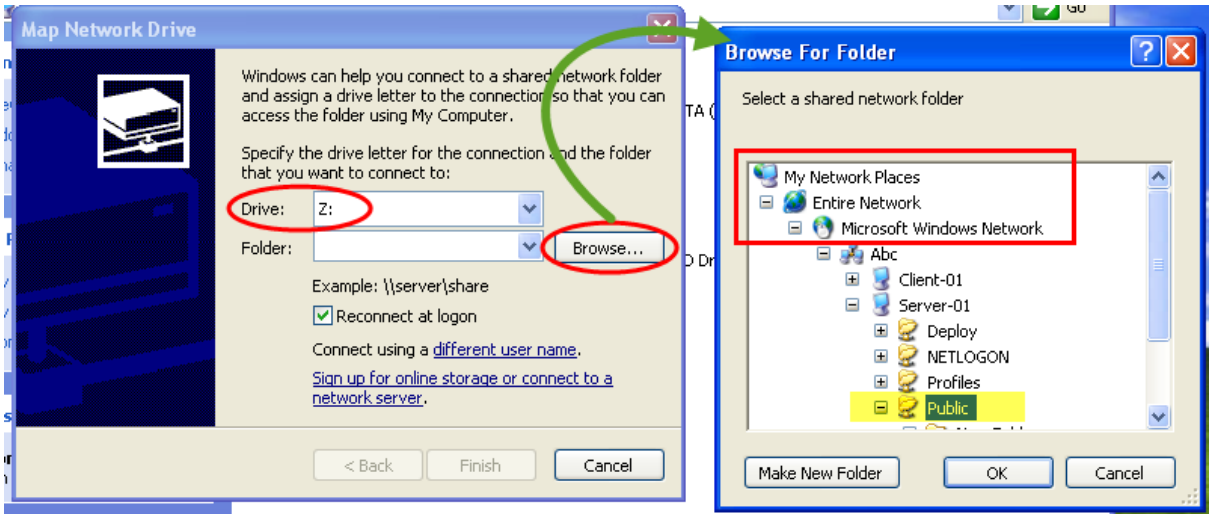
- Trên máy **SERVER-01**, tạo thư mục Public, tại **C:\Public**.
- Chia sẻ thư mục này cho **Everyone**, quyền **Full Control**.

Bước 2:

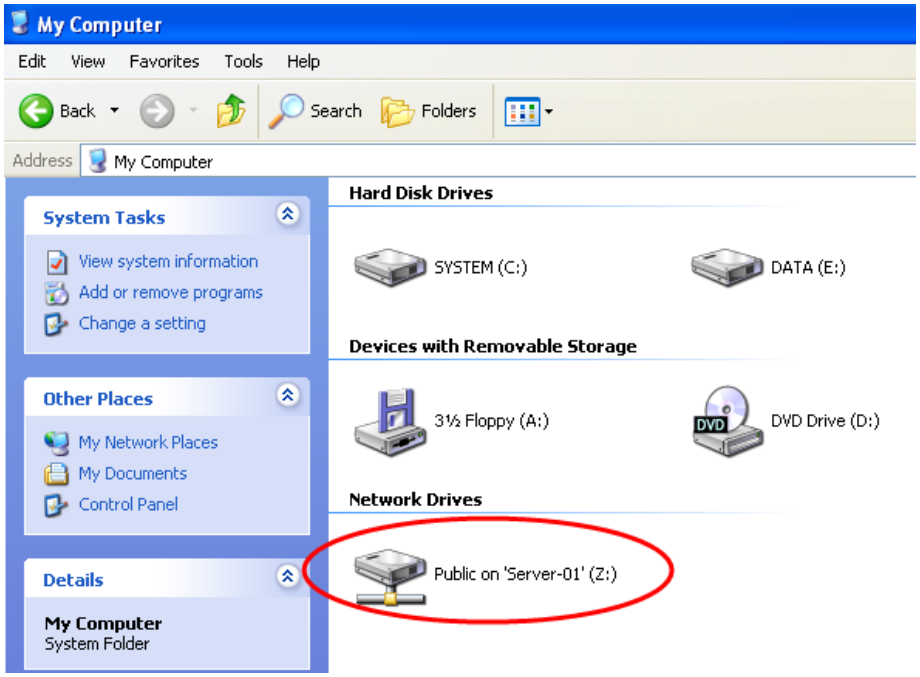
- Tại máy trạm, khi nhân viên đăng nhập vào, họ mở **Window Explorer** → **Tools** → **Map Network Drive** và thực hiện ánh xạ ổ đĩa mạng vào thư mục "**Public**" trên Server.



- Chọn thư mục Public đã được chia sẻ trên SERVER-01:



- Kết quả:

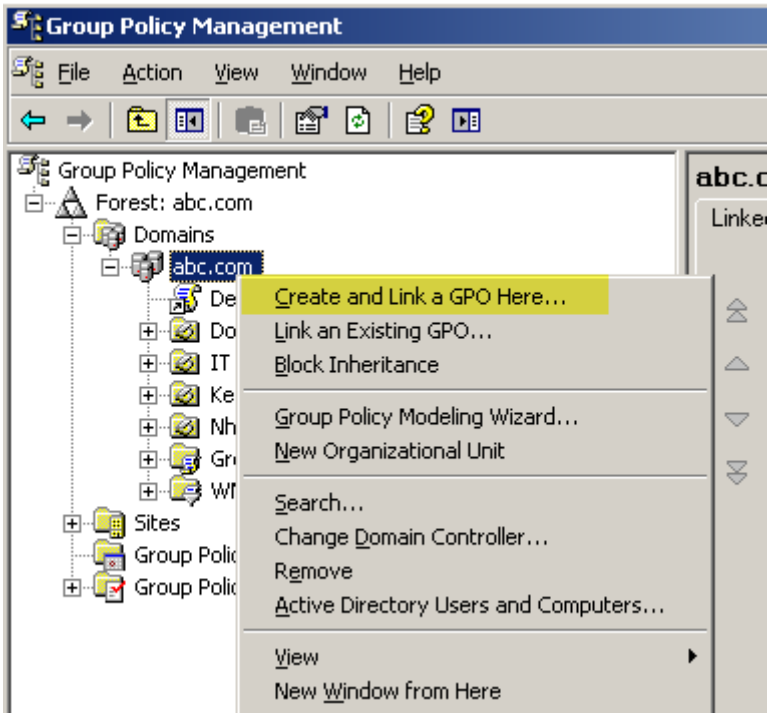


Câu 35 : Ánh xạ ổ đĩa mạng bằng Log on script

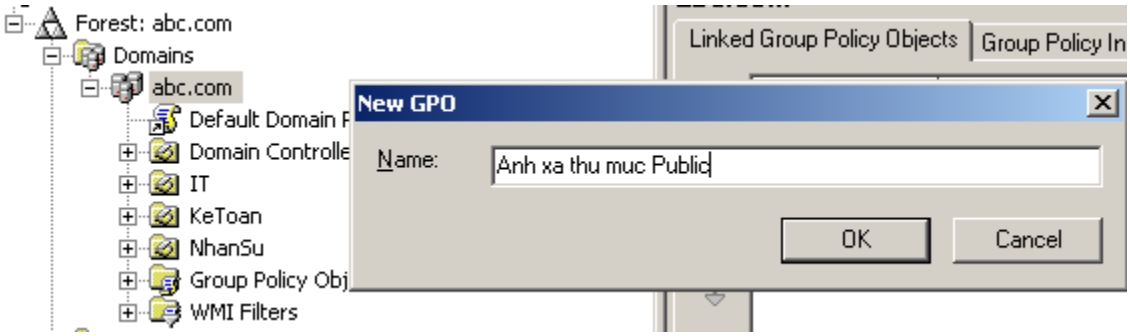
Để tạo script log on, thực hiện ánh xạ ổ đĩa mạng, chúng ta thực hiện như sau:

Bước 1: Thực hiện tạo GPO

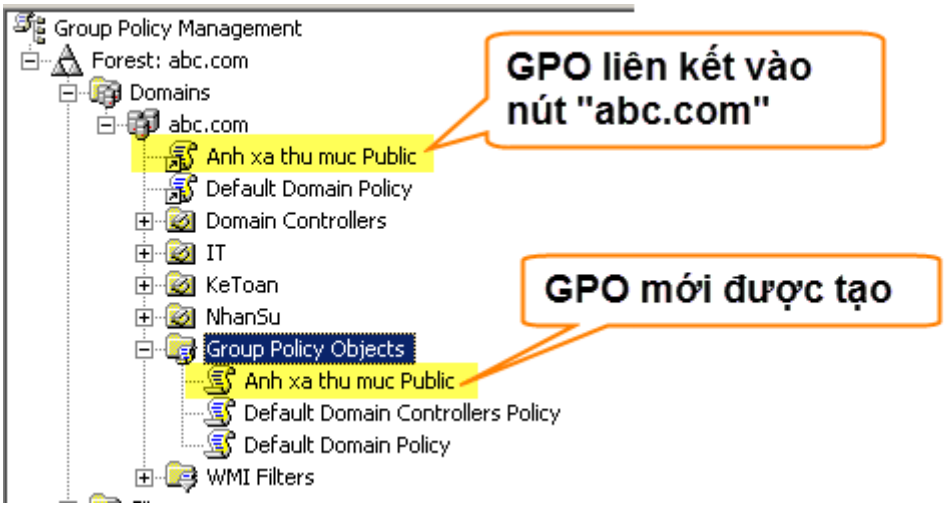
- Mở công cụ quản lý chính sách nhóm (GPMC) bằng một trong các cách đã nêu ở phần lý thuyết.
- Chúng ta sẽ tạo mới 1 đối tượng chính sách (GPO: Group Policy Object), thực hiện ánh xạ ổ đĩa. Vì chính sách này sẽ áp dụng cho toàn miền (toàn domain), nên chúng ta nhấp chuột phải vào nút "abc.com" và chọn lệnh "Create and Link a GPO here…"



- **Đặt tên cho GPO:**

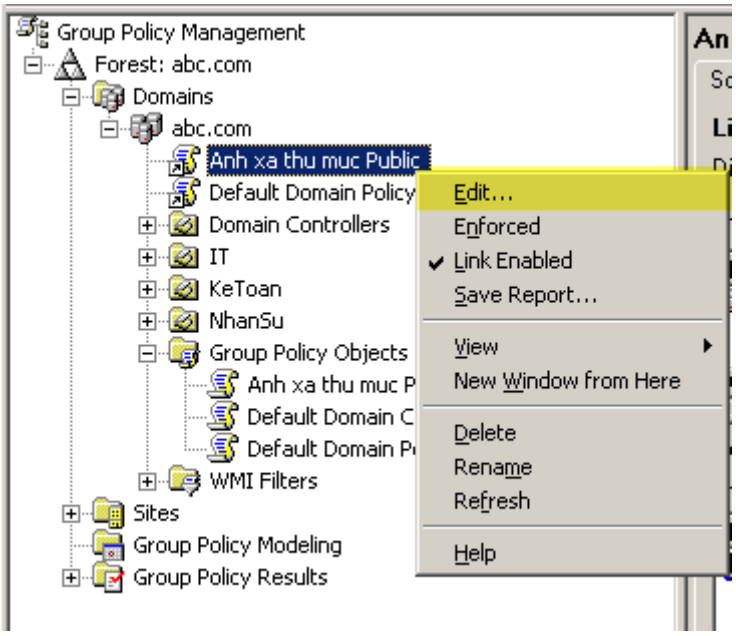


- Lệnh "**Create and Link a GPO here…**" sẽ thực hiện 2 việc:
  - Tạo mới một GPO
  - Và liên kết GPO đó vào nút "abc.com" (liên kết vào nút **abc.com** có nghĩa là GPO này sẽ được áp dụng trên toàn miền **abc.com**)



Bước 2: Thực hiện thiết lập chính sách

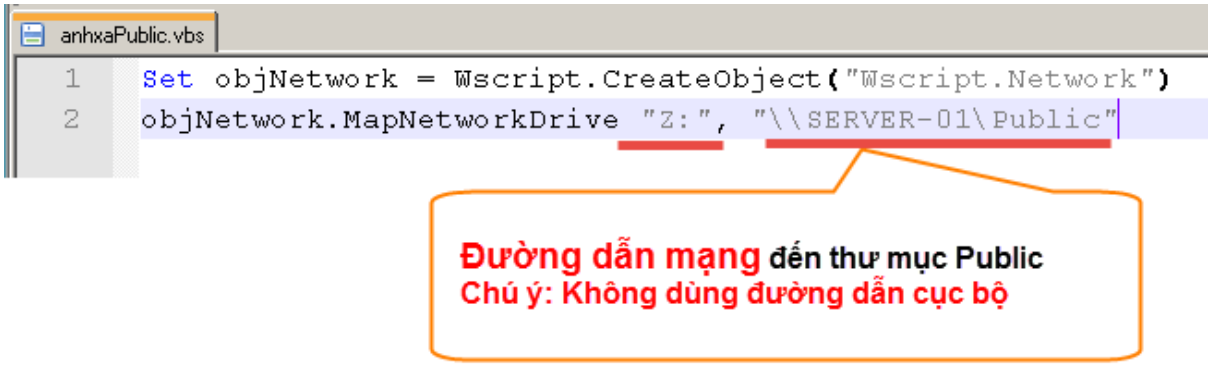
- Nhấp phải vào GPO mới tạo, chọn lệnh **Edit** để mở chương trình **Group Policy Editor**, tại đây, chúng ta có thể thiết lập các chính sách (giống như đã thực hành ở phần Local Group Policy)



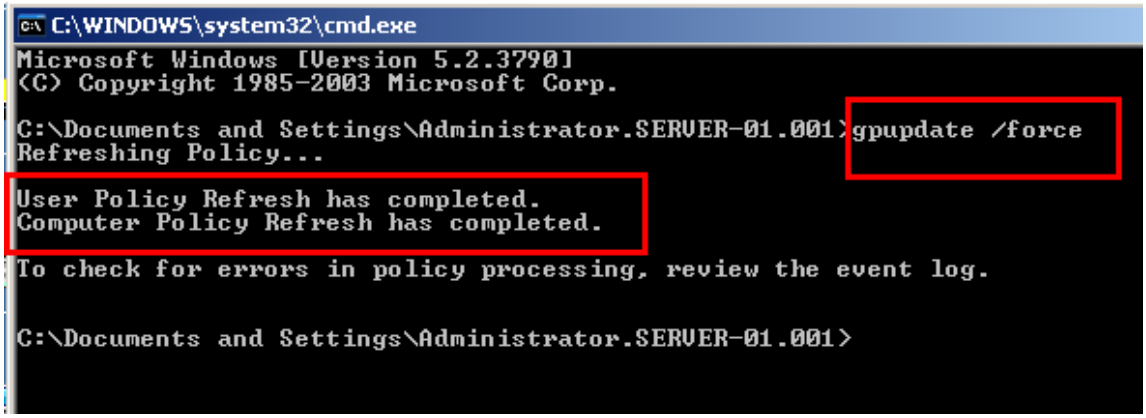
- Cửa sổ **Group Policy Object Editor** sẽ hiện ra. Tại đây, các bạn sẽ tạo Log on script (tương tự như bài tập chúng ta đã làm ở phần Local Group Policy).

- Và đây là nội dung của đoạn lệnh (script) để ổ đĩa mạng:

```
Set objNetwork = Wscript.CreateObject("Wscript.Network")
objNetwork.MapNetworkDrive "Z:", "\\SERVER-01\Public"
```



- **Nhớ thực hiện lệnh gpupdate /force để áp dụng chính sách ngay lập tức.**



Thực hiện kiểm tra:

- Tại máy CLIENT-01, thử đăng nhập với tài khoản **kt1, ns1** xem ổ đĩa mạng có được tạo ra không?
- Tài máy CLIENT-02, thử đăng nhập với tài khoản **kt1, ns1** xem ổ đĩa mạng có được tạo ra không?

Câu 36 : GPO liên kết với một OU

- Làm tương tự như câu trên, nhưng chú ý, tạo GPO tại nút OU "KeToan" (chứ không tạo tại nút "abc.com"). Điều này làm cho chính sách chỉ áp dụng cho OU "KeToan", mà không áp dụng cho toàn miền.

Bài 7: Domain group policy

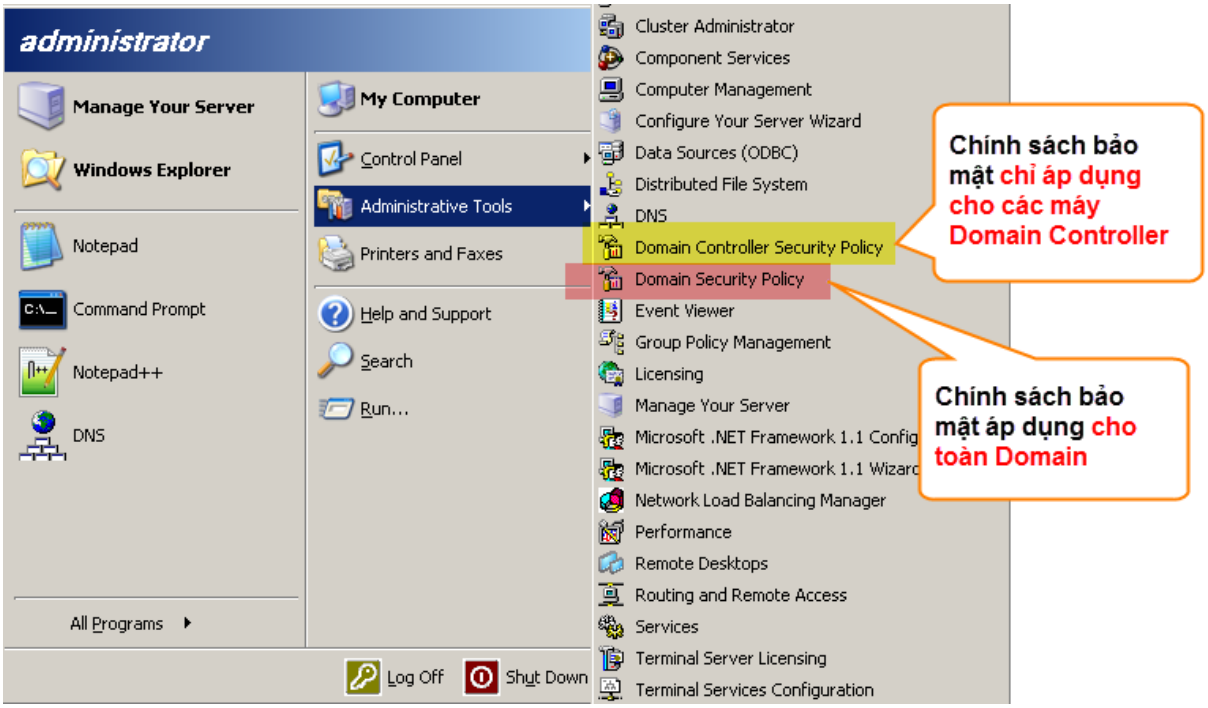
BÀI THỰC HÀNH SỐ 02

Chính sách bảo mật (Security Policies)

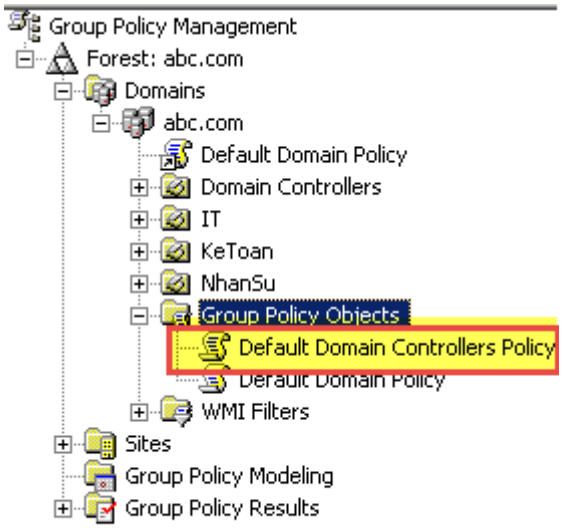
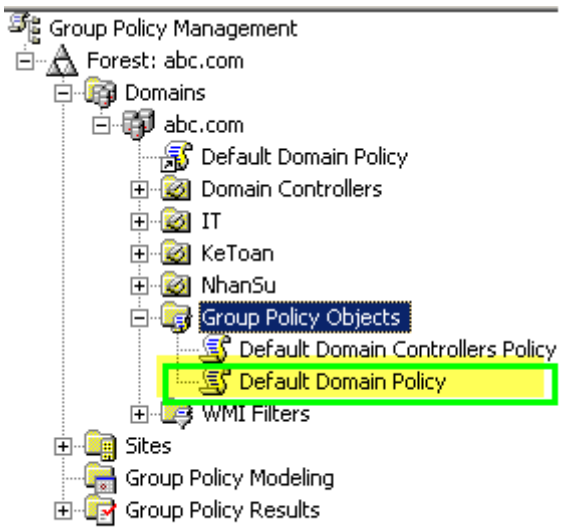
Nhắc lại lý thuyết

- **Chính sách bảo mật (Security Policy)** là một bộ phận thuộc đối tượng chính sách nhóm (Group Policy).
- Ở các máy cục bộ (máy trạm), chúng ta có thể truy cập chính sách bảo mật bằng lệnh "**secpol.msc**". Còn ở máy Domain Controller, chúng ta truy cập chính sách bảo mật bằng cách nào?

- Ở máy Domain Controller, chúng ta truy cập chính sách bảo mật bằng cách:
  - **Đối với Window Server 2003**: Vào **Administrative Tools** → chọn Domain Controller Security Policy hoặc Domain Security Policy.



Lưu ý: Ở đây, rất nhiều bạn cảm thấy nhập nhằng giữa 2 chính sách bảo mật này. Hãy xem bảng so sánh bên dưới:

Domain Controller Security Policy	Domain Security Policy
Là những chính sách bảo mật chỉ áp dụng cho máy Domain Controller.	Là những chính sách bảo mật áp dụng cho toàn Domain.
Là một bộ phận thuộc Default Domain Controllers Policy. *Bên dưới là công cụ Group Policy Management Console.*  	Là một bộ phận thuộc Default Domain Policy. *Bên dưới là công cụ Group Policy Management Console.* 

- **Đối với Window Server 2008 trở lên:** Truy cập thông qua Group Policy Management.
  - Vào Administrative Tools → Group Policy Management.
  - Mở nút "Group Policy Objects", tại đây, nếu muốn mở Security Policy cho toàn Domain, thì nhấp phải vào "Default Domain Policy", chọn lệnh **Edit**.
  - Cửa sổ Group Policy Object Editor hiện ra. Để mở Security Policy, chọn nút "Computer Configuration" → Window Settings → Security Settings.
    (Tương tự với phần Security Policy cho Domain Controllers)

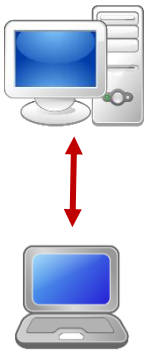
Mục tiêu bài thực hành

- Cách thiết lập chính sách nhóm liên quan tới Script.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01** cài đặt Window XP, đóng vai trò máy trạm.

SERVER-01 (DC)



CLIENT-01 (Workstation)

- Tên miền : **abc.com**
- Máy CLIENT-01 đã gia nhập vào miền trên.

Câu 37 : Thiết lập chính sách mật khẩu đơn giản

- Thiết đặt chính sách để cho phép tạo **password đơn giản** (Không cần ký tự đặc biệt)
- Tạo mới người dùng:
  - Username: **nv1**
  - Password: **1234567**

Câu 38 : Độ dài tối thiểu cho mật khẩu

- Thiết lập chính sách để yêu cầu độ dài tối thiểu của mật khẩu **là 9 ký tự**.
- Tạo mới người dùng:

- Username: **nv2**
- Password: **123456789**

Câu 39 : Thời hạn sử dụng mật khẩu

- Thiết lập chính sách để password có thời hạn sử dụng là 1 tháng. (Sau 1 tháng, password hết hiệu lực)

Câu 40 : Chính sách khóa tài khoản

- Thiết đặt chính sách để:

  - Khóa tài khoản nếu người dùng đăng nhập sai **quá 3 lần**.
  - Thời gian bị khóa là: **2 phút**.

Tại máy trạm (CLIENT-01), lần lượt thực hiện các thao tác sau đây:

1. Đăng nhập với tài khoản **nv1**, nhưng cố tình đăng nhập với password sai (quá 3 lần).
   Hãy xem thông báo lỗi là gì?
2. Sau khi xem thông báo lỗi xong, hãy đăng nhập liền với password đúng? Lần này, đăng nhập có thành công không? Có báo lỗi gì không?
3. Đợi 2 phút sau, tiếp tục đăng nhập với password đúng? Lần này đăng nhập có thành công không? Có báo lỗi gì không?

Hướng dẫn thực hành

- Bài thực hành này tương tự như bài đã được làm ở phần Local Group Policy. Chỉ có một điểm lưu ý là: Chúng ta sẽ thiết lập các chính sách này ở mục "**Domain Controllers Security Policy**" hay "**Domain Security Policy**"?
- Theo các bạn thì chúng ta sẽ chọn mục nào?
- Ở đây, chúng ta có nhu cầu thiết lập chính sách tài khoản và áp dụng xuống các máy trạm (clients), nên chắc chắn chúng ta phải chọn ở mục "**Domain Security Policy**". *(Vì "**Domain Controllers Security Policy**" chỉ áp dụng cho các máy Domain Controller)*

Bài 7: Domain group policy

BÀI THỰC HÀNH SỐ 03

Administrative Templates

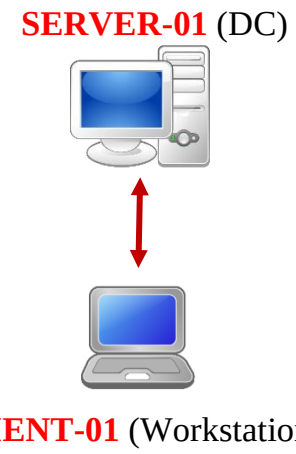
Hình nền Desktop

Mục tiêu bài thực hành

- Cách thiết lập chính sách nhóm liên quan tới Script.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01** cài đặt Window XP, đóng vai trò máy trạm.

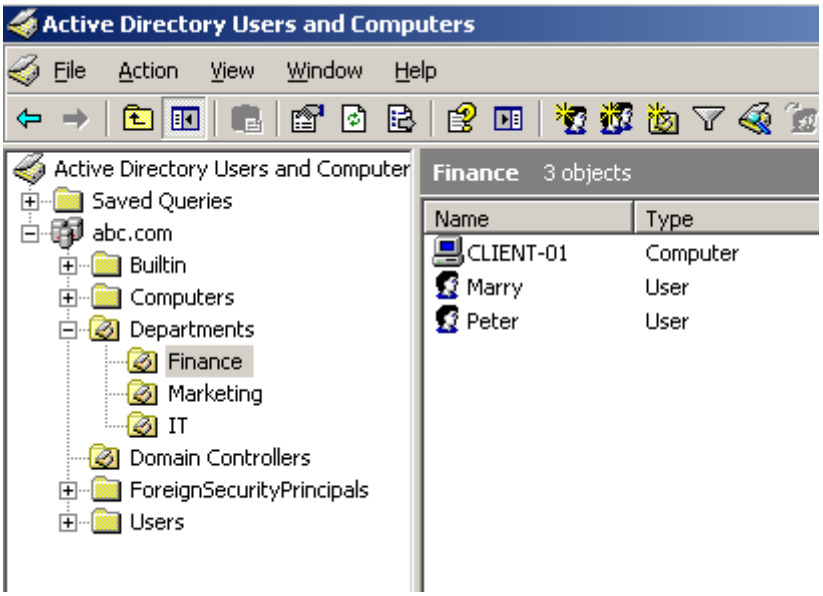


- Tên miền : **abc.com**
- Máy CLIENT-01 đã gia nhập vào miền trên.

Câu 41 : Tạo các OU, Users

Trên máy Domain Controller SERVER-01 :

- Tạo các OU: **Departments**.
- Tạo các OU con thuộc Departments (xem hình bên dưới)
  - **Finance**
  - **Marketing**
  - **IT**



Tạo các Users sau:

- Trong OU Finance:
    - Marry (password: 123)
    - Peter (password: 123)
- Trong OU Marketing:
    - John (password: 123)
- Trong OU IT:
    - Bill (password: 123)
    - Tạo nhóm: "IT group"
    - Gán user Bill là thành viên của nhóm "IT group"
- Đưa máy **CLIENT-01** vào OU **Finance** (xem hình ở trên)

Câu 42 : Mỗi phòng ban có một hình nền riêng

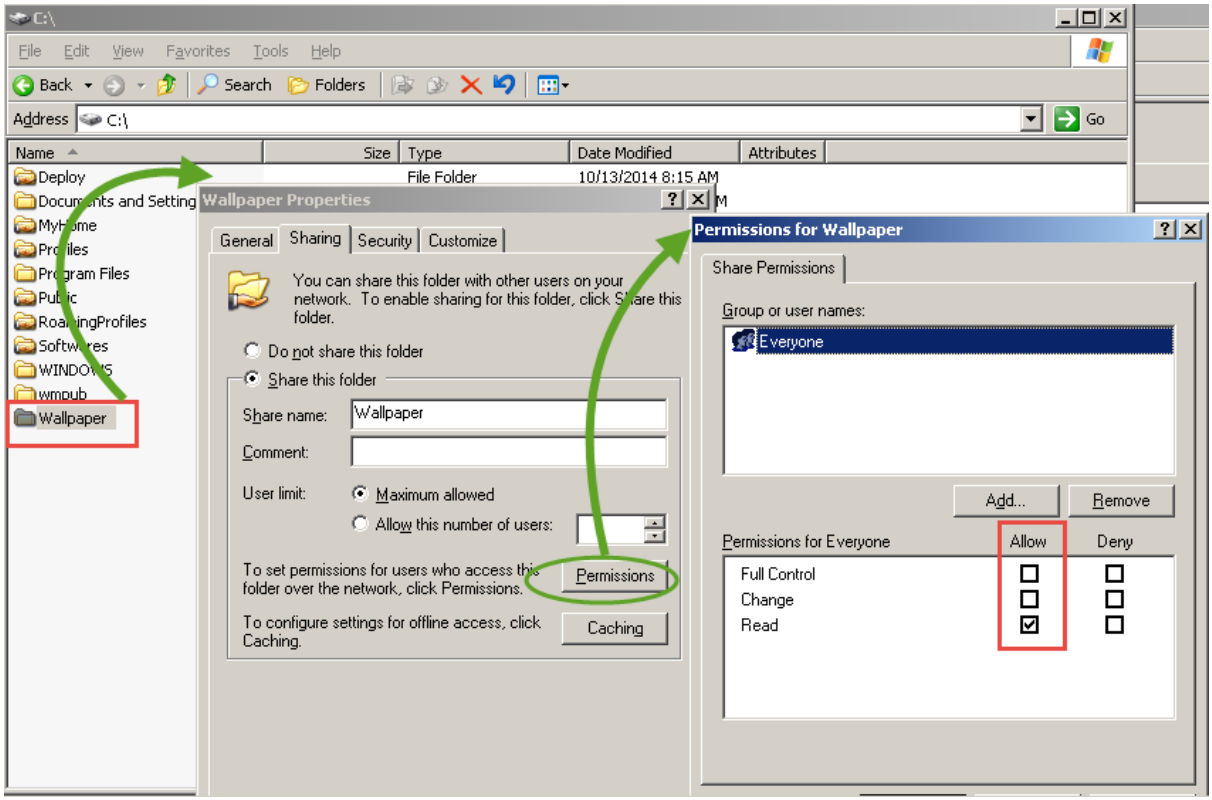
- Thiết lập chính sách để mỗi phòng ban sẽ có 1 hình nền riêng.
  Khi user thuộc phòng ban nào log on vào hệ thống, hình nền desktop của phòng ban đó hiện ra tương ứng.
- Ví dụ, User thuộc phòng tài chính (Finance) như Marry hoặc Peter log on vào hệ thống, thì sẽ có hình nền như bên dưới:

Hướng dẫn thực hành

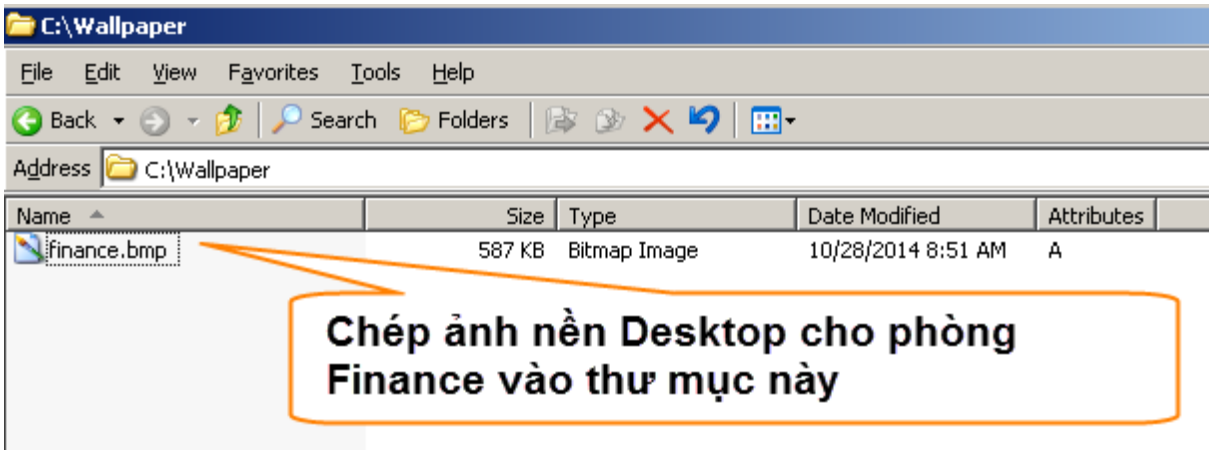
Câu 43 : Thiết lập chính sách hình nền cho phòng Finance:

Bước 1: Tạo thư mục chia sẻ hình nền

- Tạo thư mục chứa hình nền. Ví dụ tạo thư mục tại **C:\Wallpaper**. Chia sẻ cho **Everyone** (chỉ cần quyền **Read** là đủ)

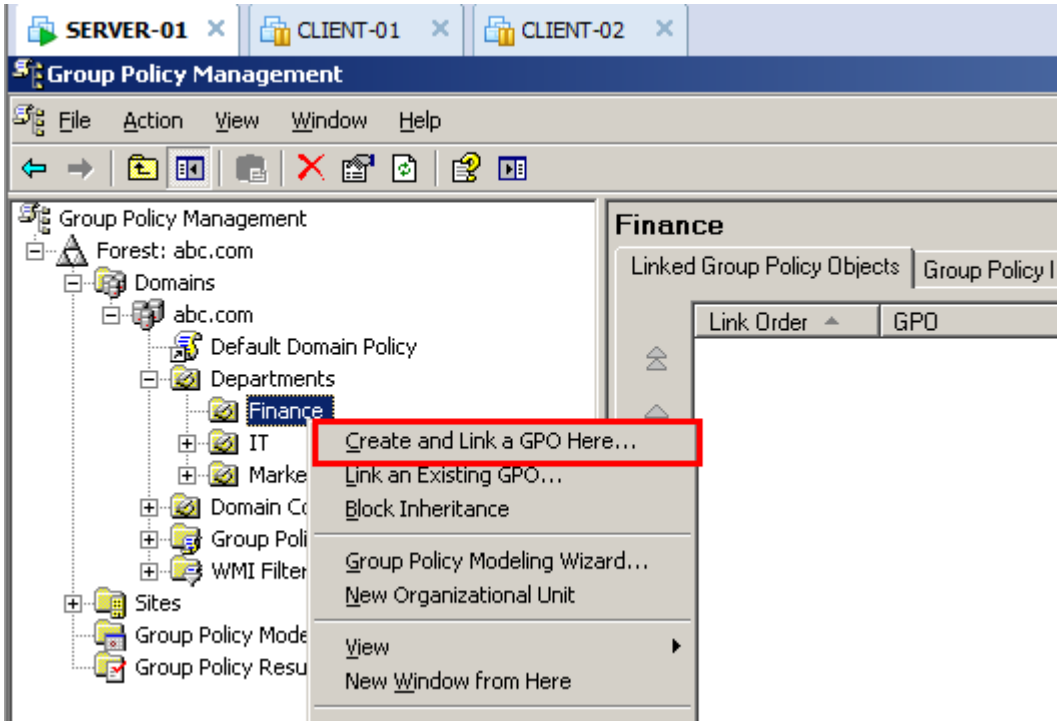


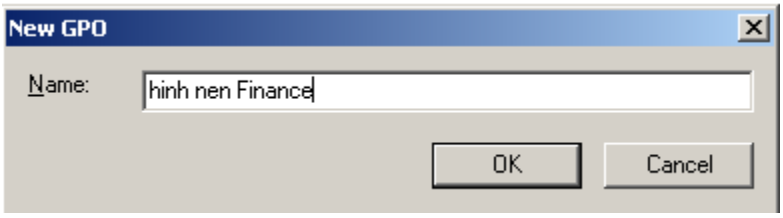
- Chép ảnh nền Desktop cho phòng Finance vào thư mục C:\Wallpaper. (Để cho nhanh, có thể tạo ảnh bằng công cụ MS Paint)



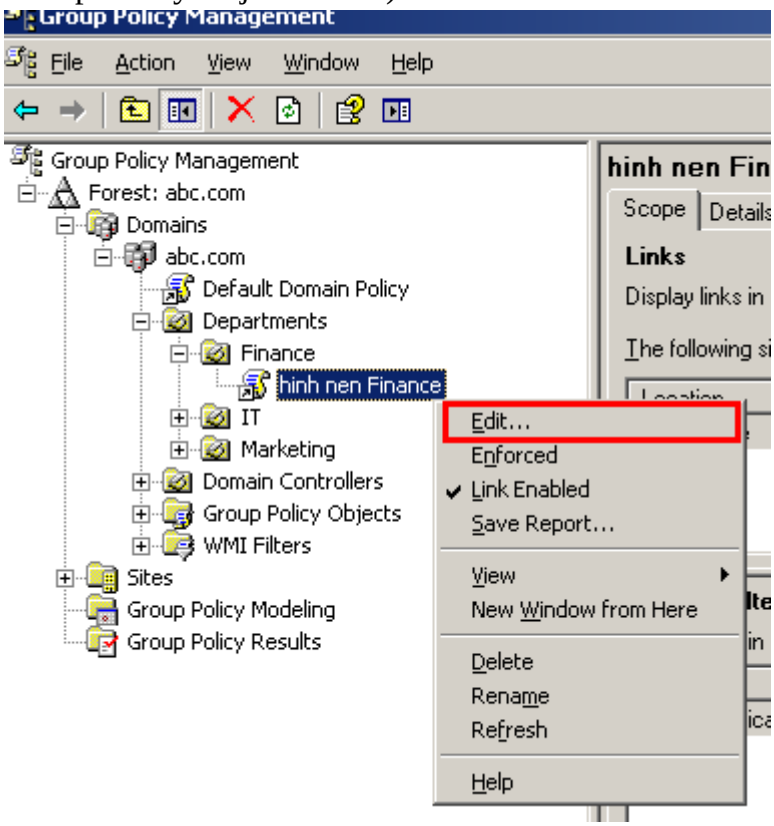
<u>Bước 2:</u> Thiết lập chính sách hình nền

- Mở GPMC, tạo một chính sách mới cho OU Finance:

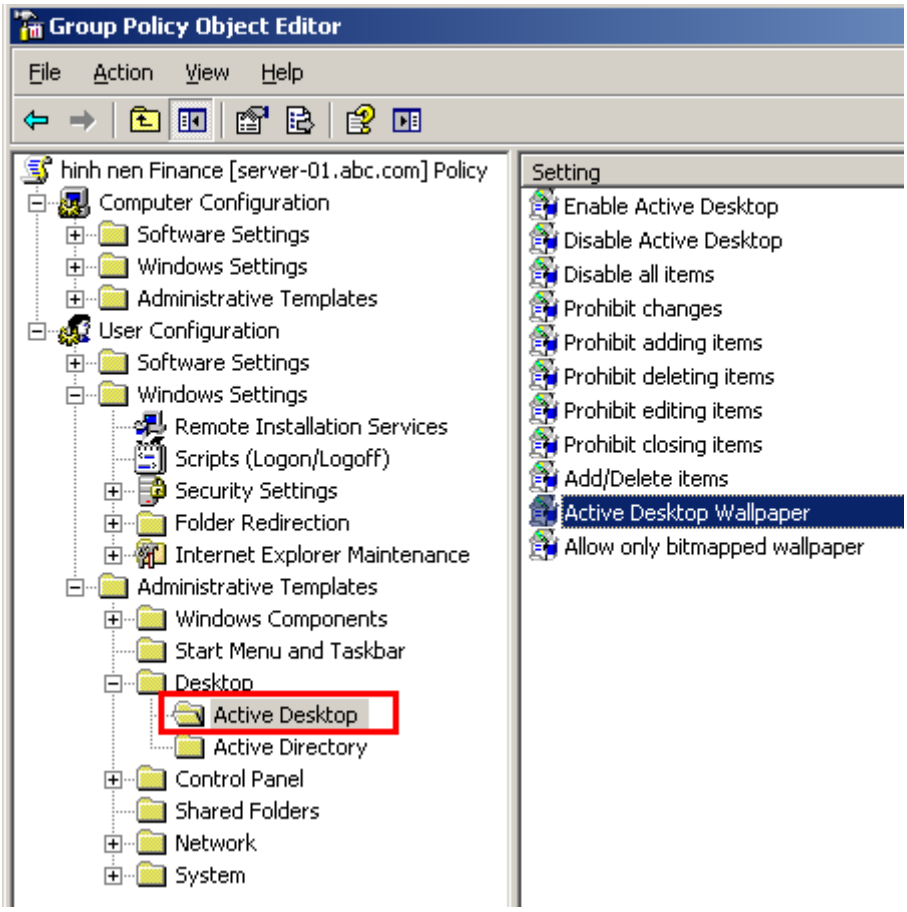




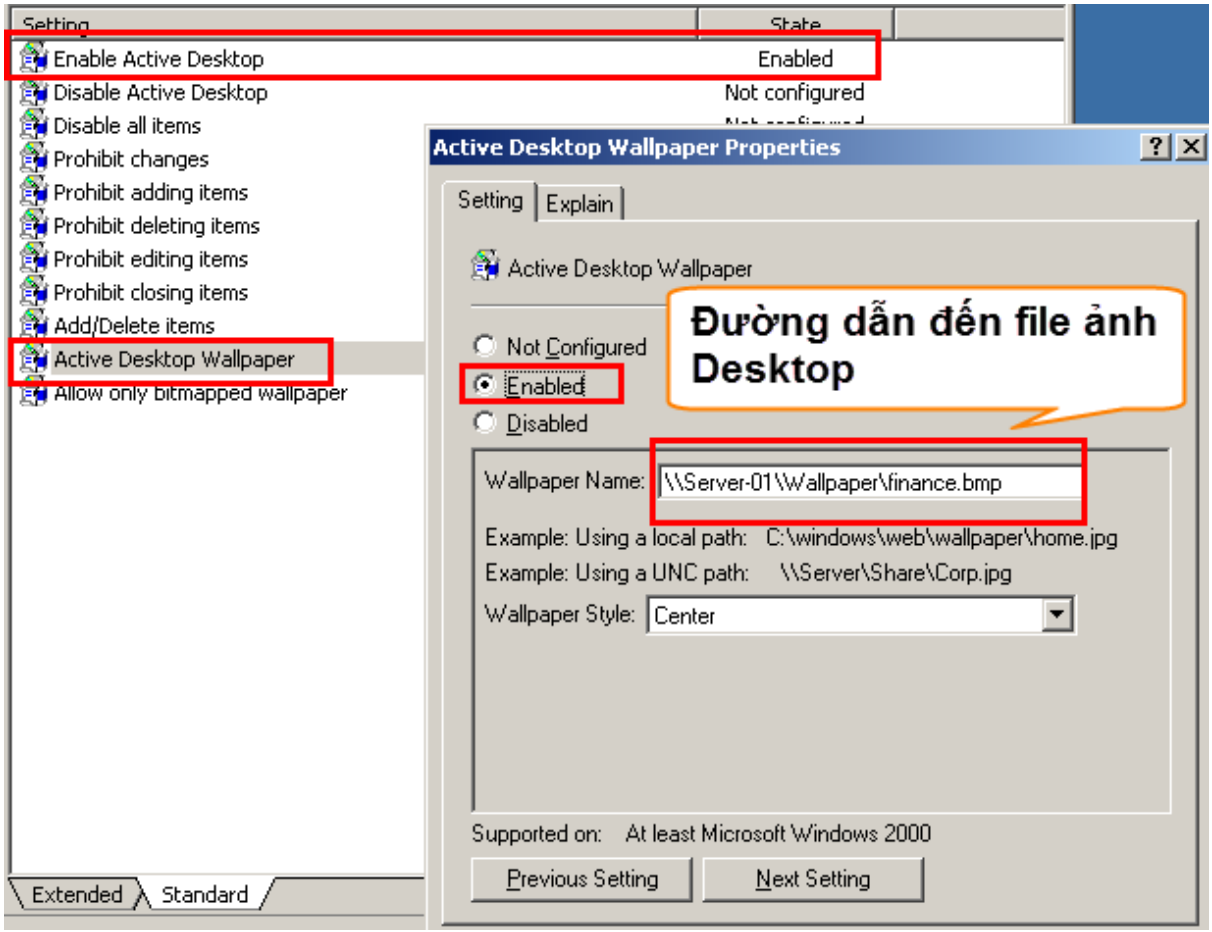
- Edit chính sách này (nhấp phải vào chính sách, chọn lệnh Edit, sẽ mở ra công cụ Group Policy Object Editor)



- Tại màn hình công cụ GPO Editor, mở đến mục “User Configuration” → “Administrative Templates” → “Desktop” → “Active Desktop”

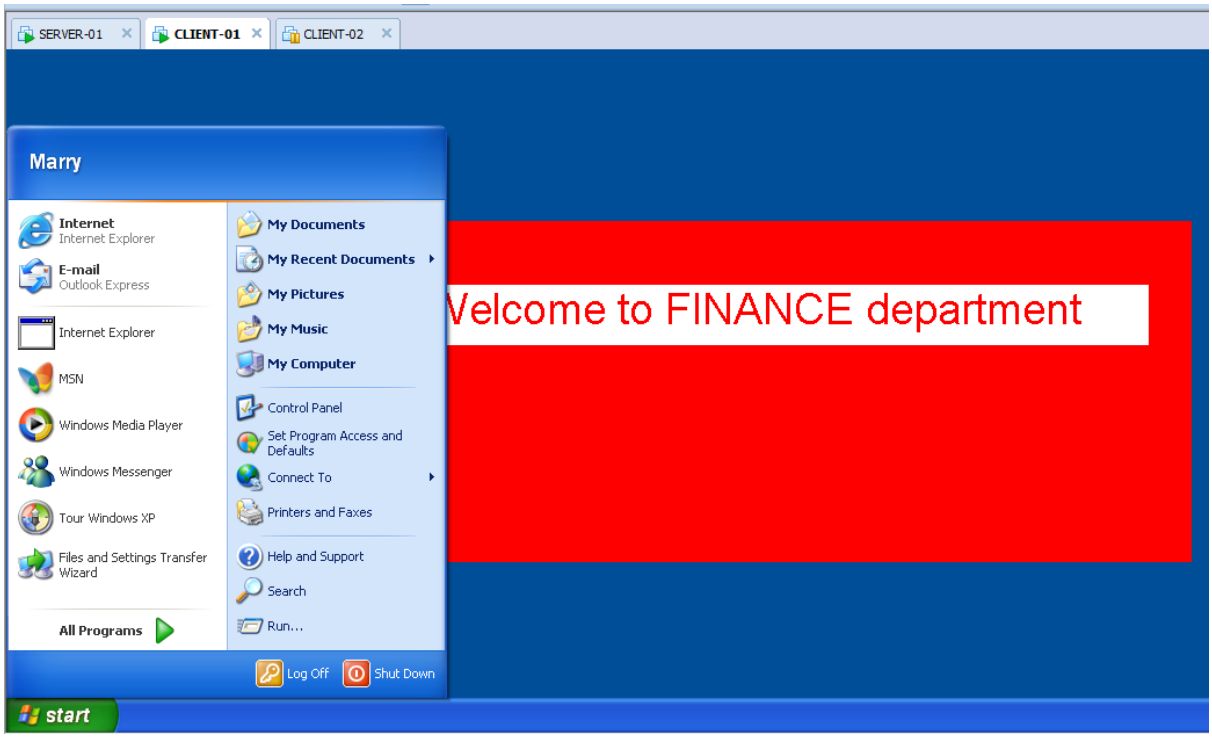


- Chỉnh 2 tham số sau:
    - Enable Active Desktop: giá trị Enable
    - Active Desktop Wallpaper: giá trị Enable, và chỉ định đường dẫn đến hình ảnh Desktop.



- **Nhớ thực hiện lệnh gpupdate /force để áp dụng chính sách ngay lập tức.**

- Kết quả (tại máy CLIENT-01, đăng nhập với tài khoản thuộc phòng Finance)



- Làm tương tự cho các phòng ban khác.

Bài 7: Domain group policy

BÀI THỰC HÀNH SỐ 04

Administrative Templates

Cấm chạy chương trình

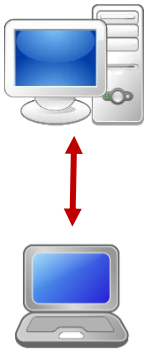
Mục tiêu bài thực hành

- Cách thiết lập chính sách nhóm liên quan tới Script.

Môi trường thực hành

- Máy tính: gồm các máy sau :
  - Máy **SERVER-01**, cài đặt Win2k3, là Domain Controller.
  - Máy **CLIENT-01** cài đặt Window XP, đóng vai trò máy trạm.

SERVER-01 (DC)



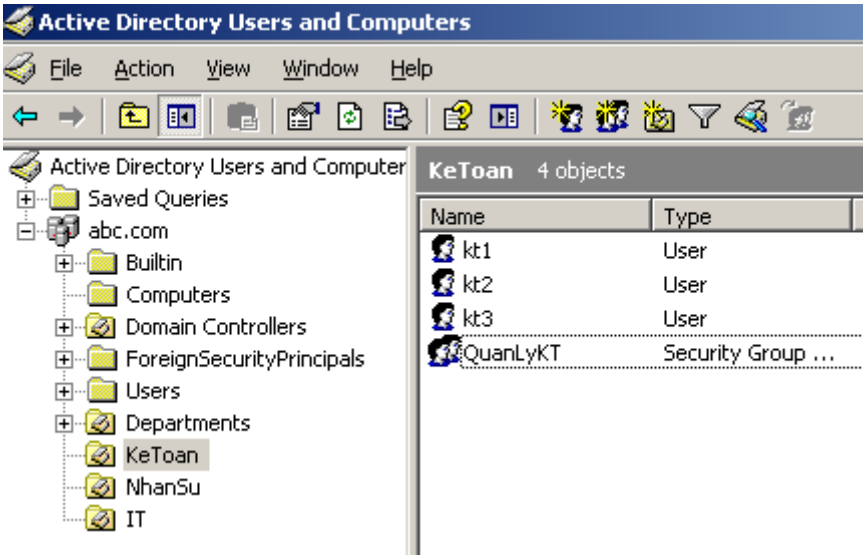
CLIENT-01 (Workstation)

- Tên miền : **abc.com**
- Máy CLIENT-01 đã gia nhập vào miền trên.

Câu 44 : Tạo các OU, Users

- Để chuẩn bị cho bài thực hành, hãy tạo các OU, Users như cấu trúc bên dưới *(Nếu các bạn đã tạo rồi, thì có thể bỏ qua câu này)*
- Các OU:
  - **KeToan**. Gồm 3 users: **kt1**, **kt2**, **kt3** (password: **123abc!**)
  - **NhanSu**. Gồm 3 users: **ns1**, **ns2**, **ns3** (password: **123abc!**)
  - **IT**. Gồm 2 users: **it1**, **it2** (password: **123abc!**)

- Trong OU **KeToan**, tạo group "**QuanLyKT**", và đưa nhân viên **kt1** vào trong group này.



Câu 45 : Cấm chạy Internet Explorer cho một OU

- Công ty ABC không muốn tất cả nhân viên phòng Kế Toán sử dụng chương trình Internet Explorer để truy cập vào internet.
- Bạn hãy thiết lập chính sách trên.

Thực hiện kiểm tra 1:

- Tại máy trạm (CLIENT-01), đăng nhập với tài khoản thuộc phòng Kế toán (chẳng hạn: kt1).
- Thử mở chương trình Internet Explorer xem có báo lỗi gì không?

Thực hiện kiểm tra 2:

- Tại máy trạm (CLIENT-01), đăng nhập với tài khoản thuộc phòng Nhân sự.
- Thử mở chương trình Internet Explorer xem có báo lỗi gì không?

Câu 46 : Không cho một nhóm chịu ảnh hưởng bởi chính sách

- Bây giờ, công ty ABC lại đưa ra yêu cầu như sau: họ **chỉ muốn cấm nhân viên** của phòng Kế Toán mở Internet Explorer, còn những người thuộc nhóm **QuanLyKT** thì được phép.
- Bạn hãy thực hiện yêu cầu trên.

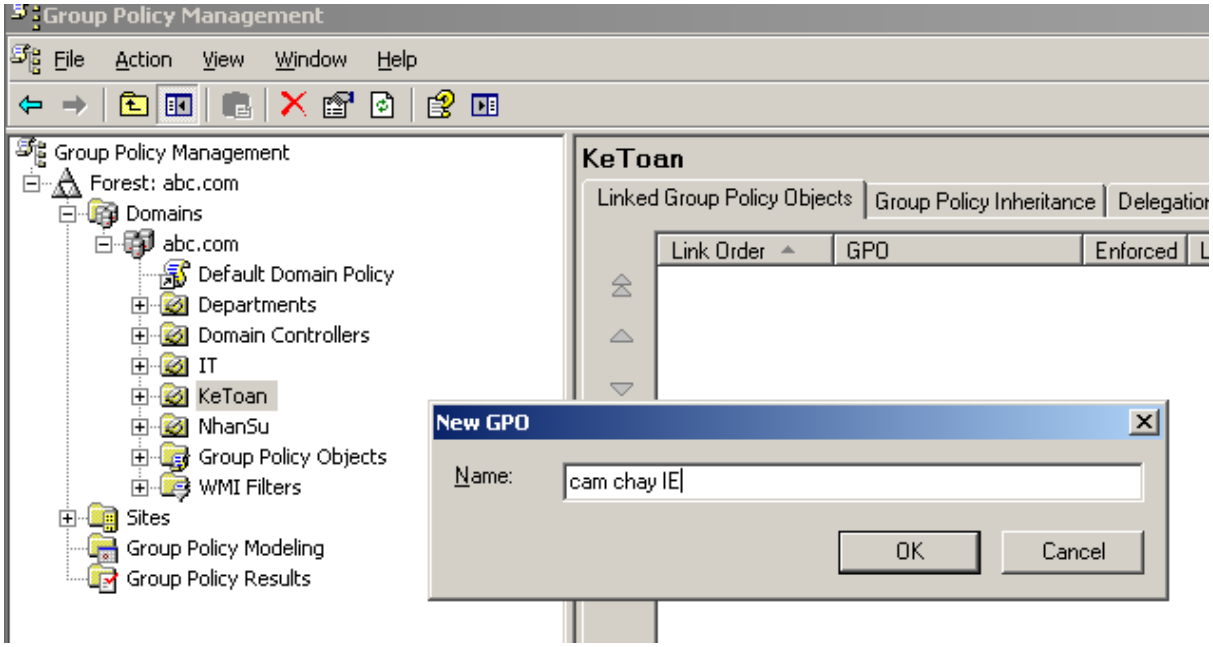
Hướng dẫn thực hành

Câu 47 : Tạo các OU, Users

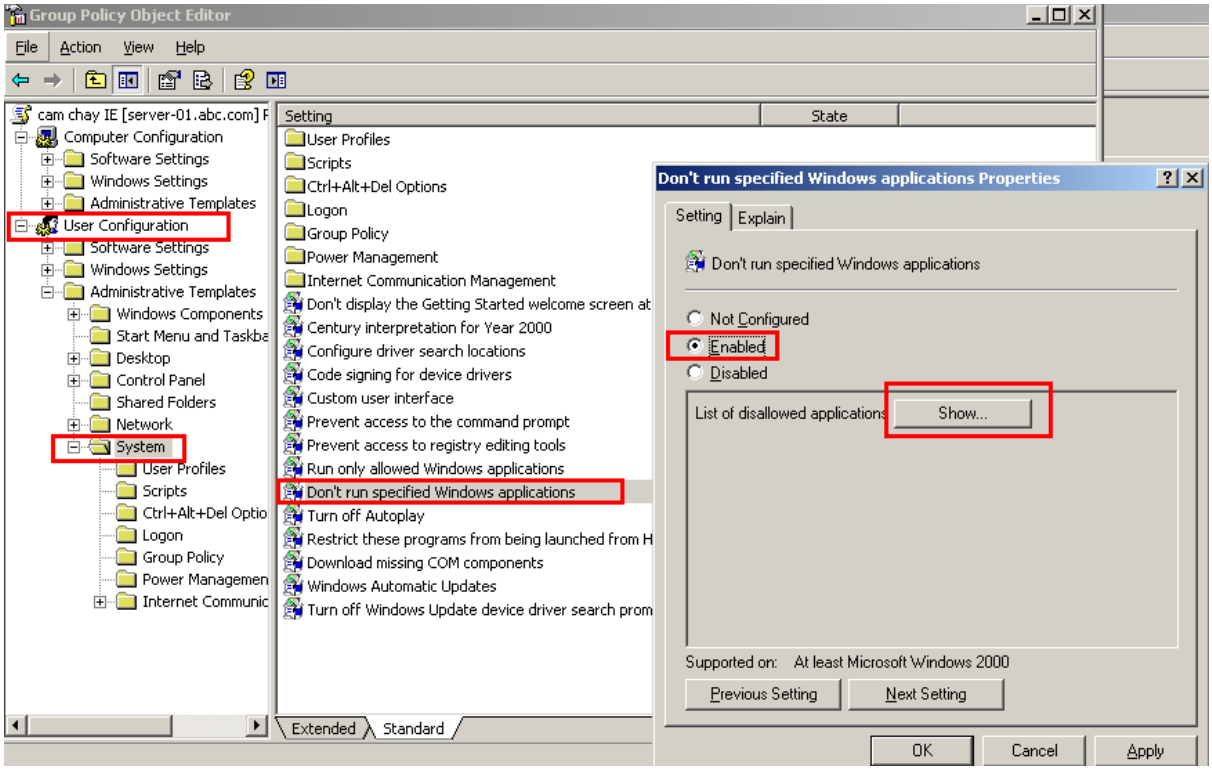
- Câu này đơn giản.

Câu 48 Cấm chạy Internet Explorer cho một OU

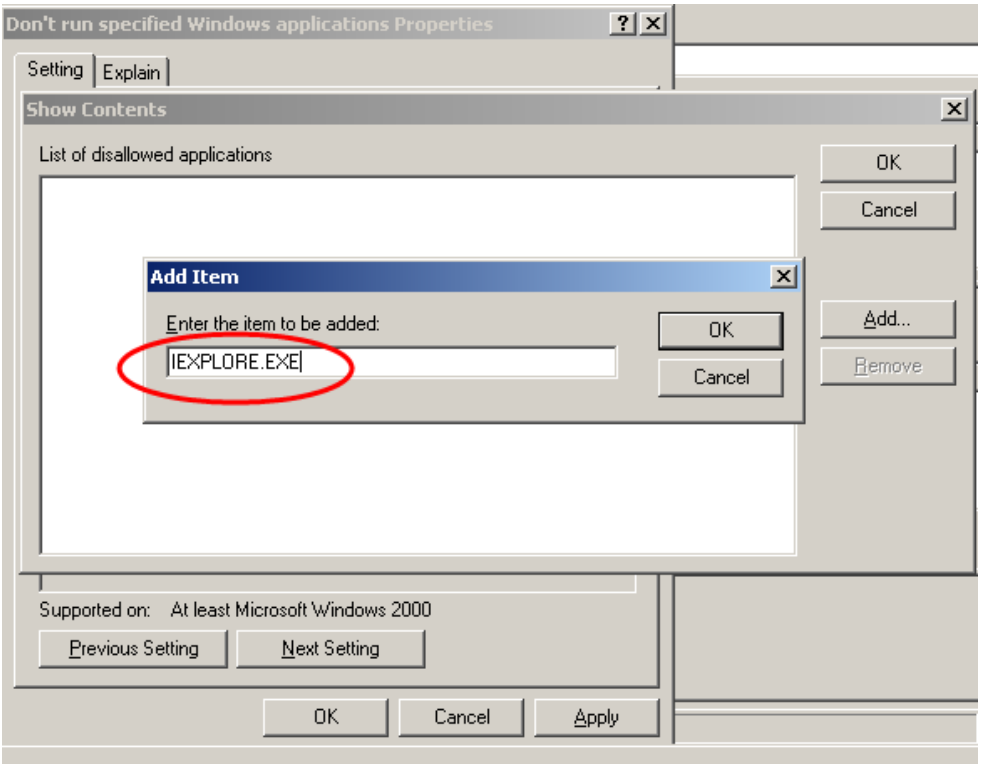
- Phần này tương tự như bài tập cấm chạy 1 chương trình ở Local Group Policy.
- Tạo chính sách cấm chạy IE cho phòng Kế Toán:



- Edit chính sách này. Vào phần "**User Configuraion**" → "**Administrative Templates**" → "**System**" → Chỉnh thiết đặt "**Don't Run specified Window applications**" với giá trị là "**Enable**".



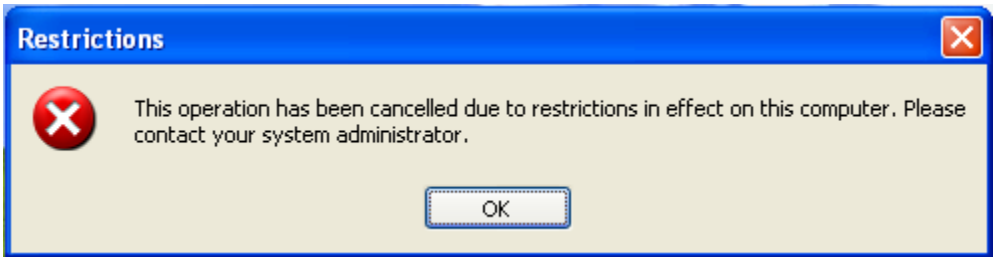
- Bấm vào nút "Show", chỉ định tên các chương trình sẽ cấm.



-

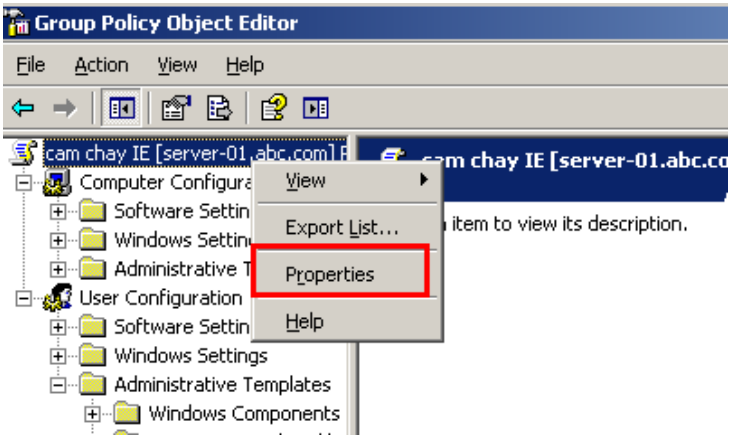
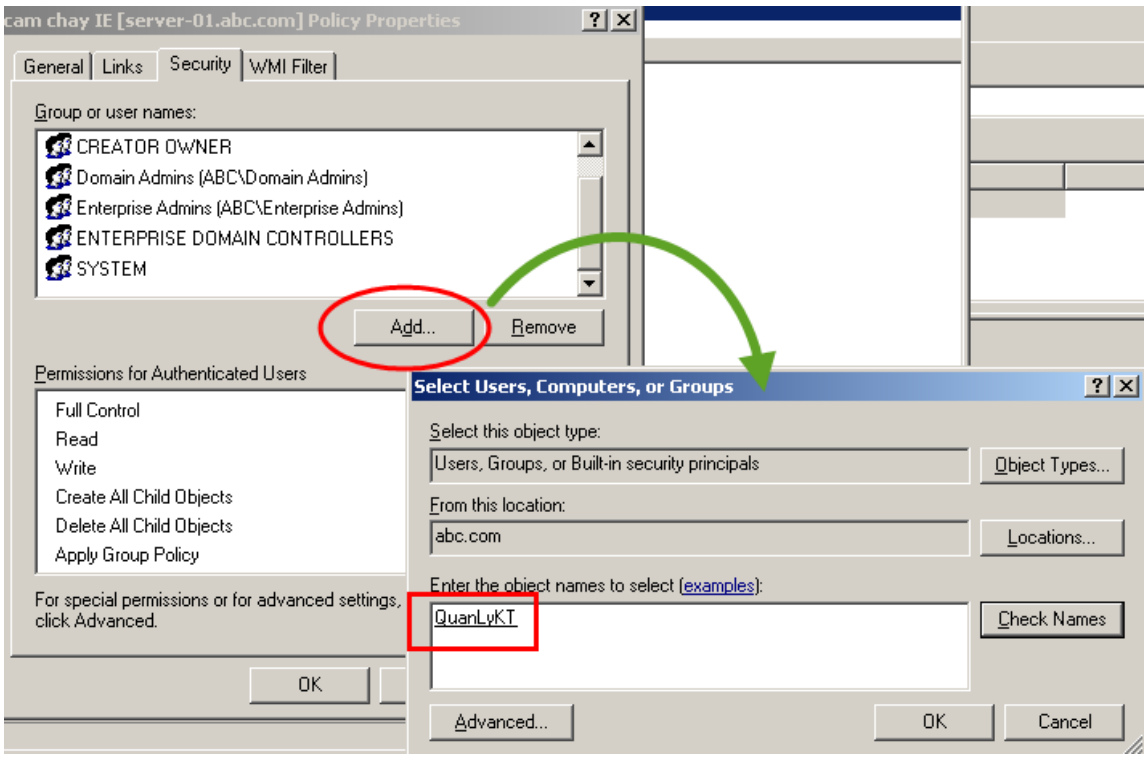
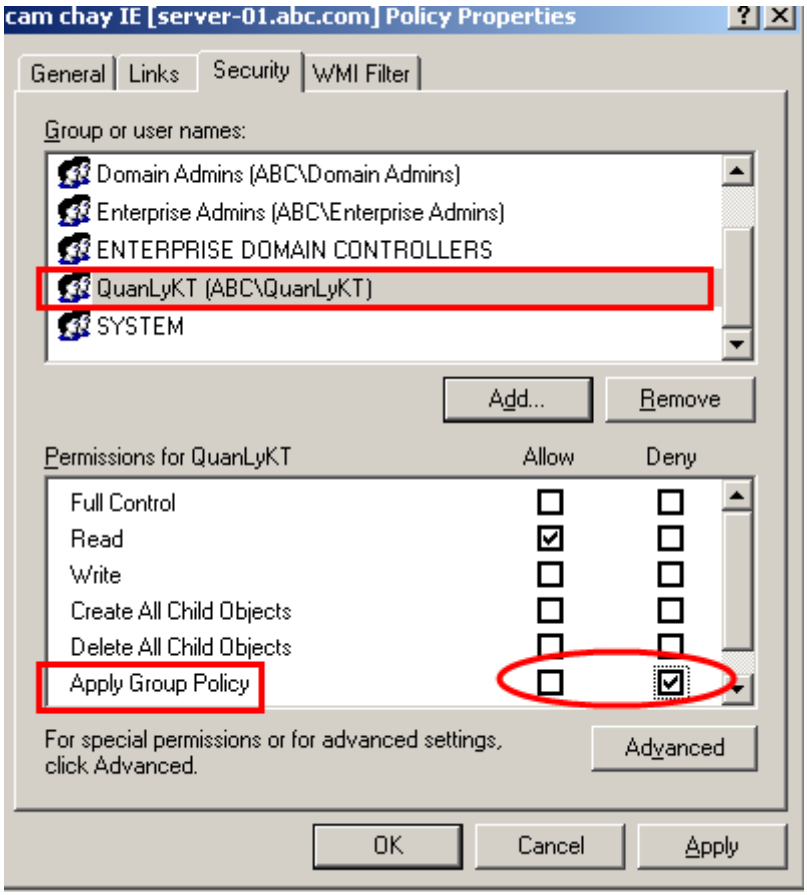
- **Nhớ thực hiện lệnh gpupdate /force để áp dụng chính sách ngay lập tức.**

- Khi nhân viên phòng Kế Toán mở Internet Explorer, sẽ hiện thông báo lỗi như sau:



Câu 49 Không cho một nhóm chịu ảnh hưởng bởi chính sách

- Ta đã tạo chính sách "**cam chay IE**" cho tất cả những người dùng thuộc OU "**KeToan**", bây giờ, ta sẽ cấu hình để cho group "**QuanLyKT**" không chịu ảnh hưởng bởi chính sách này. Có như vậy, thì những người trong nhóm "QuanLyKT" mới có thể chạy được Internet Explorer. Chúng ta sẽ thực hiện như sau:
- Nhấp phải vào GPO, chọn lệnh "Properties"



- Vào thẻ "**Security**", add thêm nhóm "**QuanLyKT**", và cấu hình để không cho nhóm này bị áp dụng bởi chính sách "**cam chay IE**". Xem hình bên dưới: