QUẢN TRỊ ACTIVE DIRECTORY: OU VÀ USER

Tổng quan

1. Quản lý đơn vị tổ chức
2. Quản lý tài khoản người dùng
3. Tạo tài khoản máy tính
4. Tự động quản lý đối tượng AD DS

1. Quản lý đơn vị tổ chức

- Đơn vị tổ chức (OU) là gì?
- Các thành phần chứa trong OU
- Cấp bậc OU là gì?
- Các thao tác quản trị OU
- Sử dụng công cụ dòng lệnh
- Demo tạo OUs

Đơn vị tổ chức (OU) là gì?

- Một đơn vị tổ chức (OU):
  - Là một đối tượng thư mục động trong miền
  - Là phạm vi nhỏ nhất, đơn vị mà bạn có thể ấn định cài đặt chính sách nhóm hoặc uỷ quyền quản trị
  - Có thể chứa người dùng, máy tính, nhóm, máy in, và các OU khác
- OUs được dùng để:
  - Tạo địa giới hành chính trong miền bằng cách ủy quyền
  - Triển khai mô hình quản lý phi tập trung
  - Áp đặt chính sách nhóm (GPO)

Các thành phần chứa trong OU

- Tài khoản người dùng, nhóm, các OU khác
- Các ứng dụng
- Máy tính, Máy in,..
- Các thiết bị ngoại vi
- Thư mục chia sẻ

Các lợi ích của OU

- Được thực hiện trong OU
  - Ủy quyền các tác vụ quản trị
  - Quản trị chính sách nhóm
  - Che giấu đối tượng
- Các thao tác quản trị OU
  - Tạo, xóa, ẩn, di chuyển OU
  - Di chuyển đối tượng trong OU

Sử dụng công cụ dòng lệnh

Thêm một OU

dsadd ou OrganizationalUnitDN -desc Description -d Domain -u UserName -p Password

Sử dụng công cụ dòng lệnh

Sửa đổi mô tả các thuộc tính của OU

dsmod ou OrganizationalUnitDN -desc Description -d Domain -u UserName -p Password

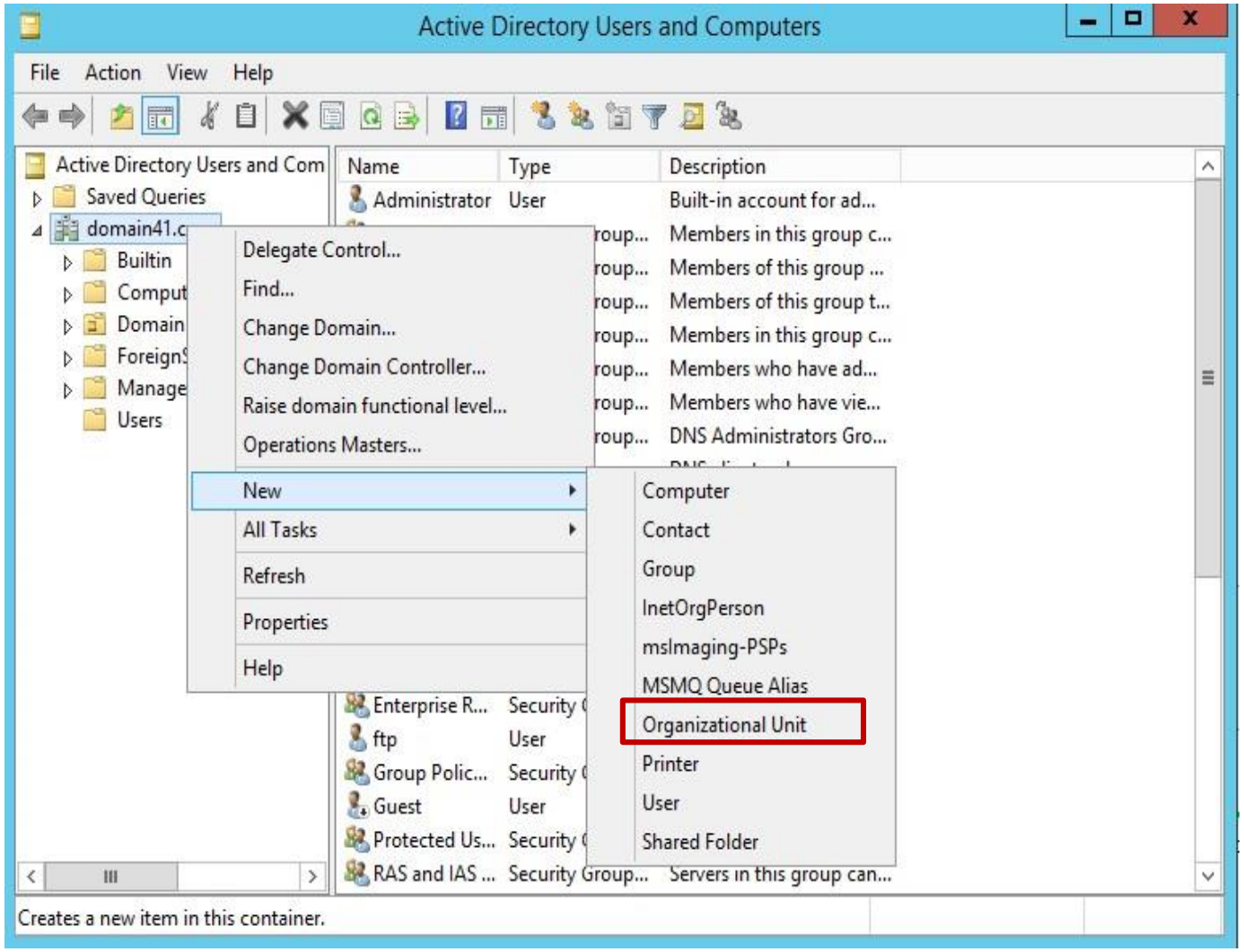
Sử dụng công cụ dòng lệnh

Xóa một OU

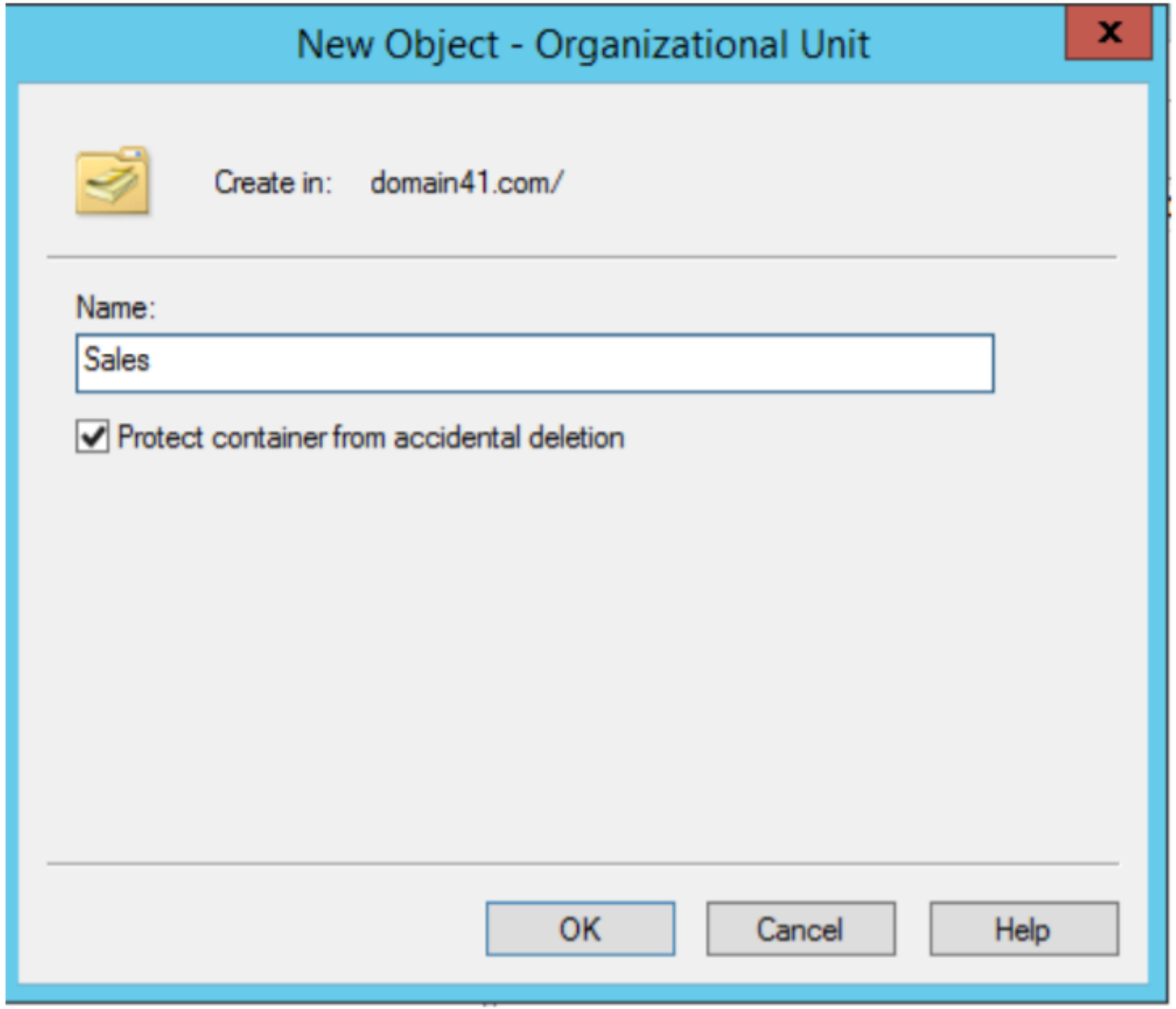
dsrm ou OrganizationalUnitDN -desc Description -d Domain -u UserName -p Password

Tạo OUs

- Vào Server Manager, chọn Active Directory User and Computer
- Click phải lên miền cần tạo OU, chọn new, OU

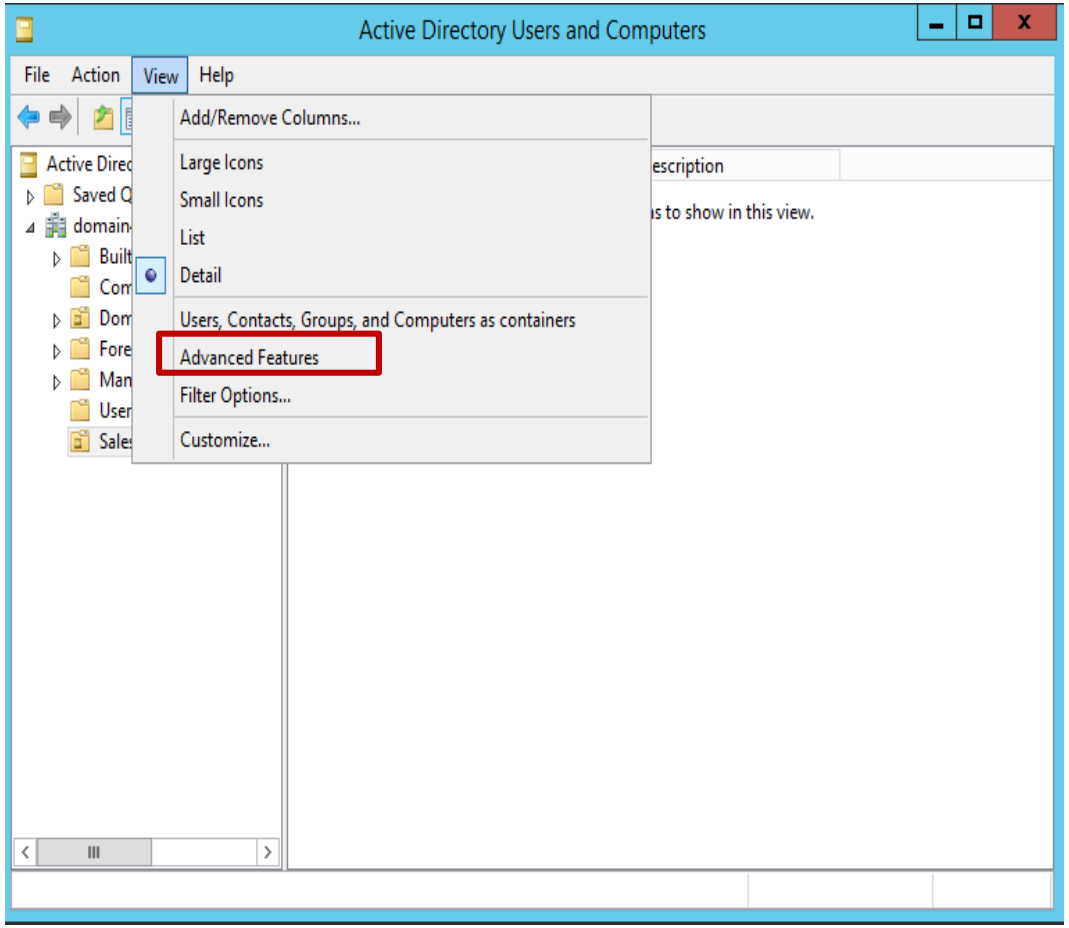


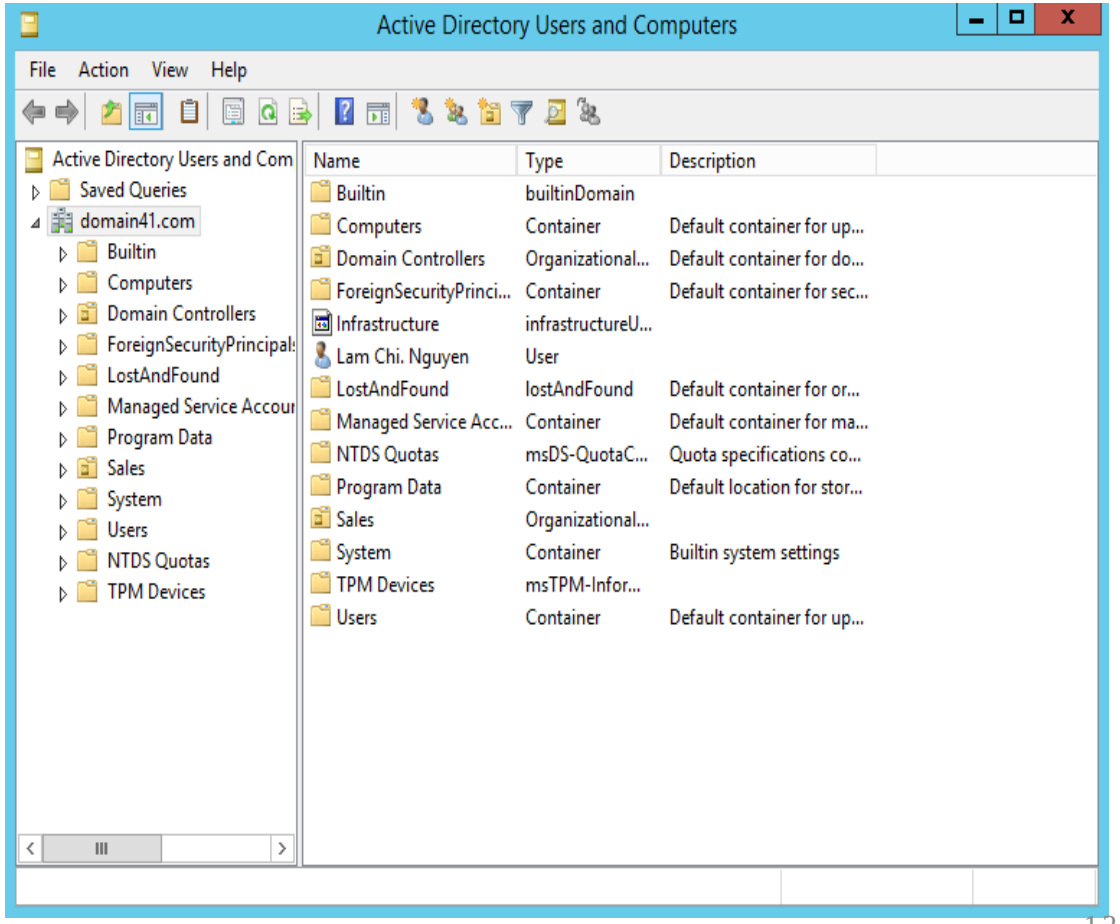
Thêm OU Sales



Xóa OU

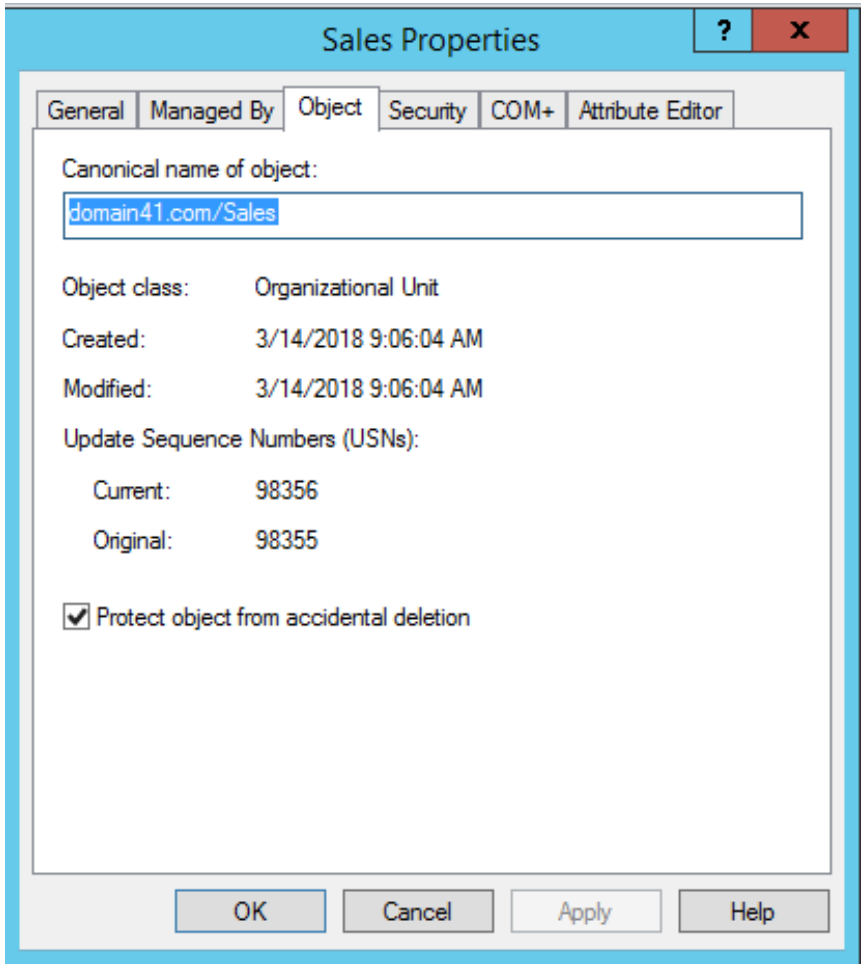
- Trong cửa sổ **Active Directory Users and Computers** > chọn **View** > chọn **Advanced Features**





Xóa OU

1. Click Phải chuột vào **OU cần xóa ->** chọn **Properties**
2. Trong **cửa sổ Properties của OU,** chọn tab **Object** > tick bỏ **Protect object from accidental deletion -> chon OK**
3. Lúc này ta có thể delete OU như bình thường



QUẢN TRỊ NGƯỜI DÙNG VÀ MÁY TÍNH

2. Quản trị tài khoản người dùng

- Tài khoản người dùng là gì?
- Lập kế hoạch quản trị tài khoản người dùng
- Tên (định danh) tài khoản người dùng miền
- Mật khẩu tài khoản người dùng
- Thiết lập thuộc tính cho tài khoản
- Công cụ cấu hình các tài khoản người dùng
- Tài khoản người dùng mẫu là gì?
- User profile là gì?
- Demo: Quản trị tài khoản người dùng

Tài khoản người dùng là gì?

- Một tài khoản người dùng là một đối tượng cho phép xác thực và truy cập vào tài nguyên cục bộ và mạng
- Một tài khoản người dùng có thể lưu:
  - Trong AD DS (Tài khoản AD DS)
    - ✓Tài khoản AD DS cho phép đăng nhập vào miền và cung cấp quyền truy cập vào tài nguyên mạng chia sẻ
  - Trên một máy cục bộ (tài khoản cục bộ)
    - ✓Tài khoản cục bộ cho phép đăng nhập vào một máy tính và truy cập vào tài nguyên cục bộ

Tạo một tài khoản người dùng cũng tạo ra một ID bảo mật (SID)

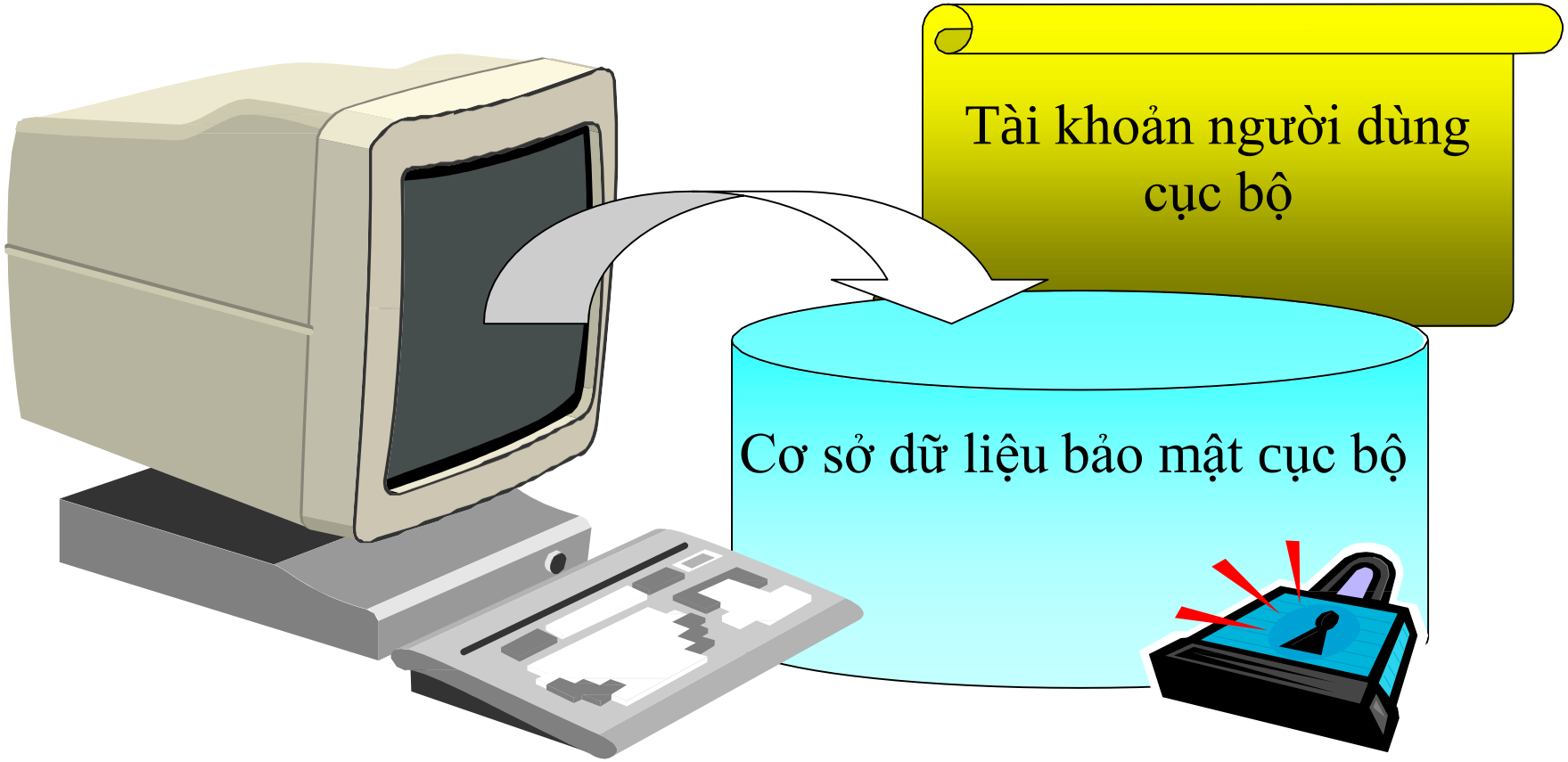
Tài khoản người dùng

- tài khoản người dùng cho phép người dùng đăng nhập vào miền và truy cập tài nguyên mạng.
- Một người dùng được cấp một tài khoản duy nhất.
- Một tài khoản người dùng là một đối tượng chứa tất cả dữ liệu cần thiết để định nghĩa người dùng trong miền.
- Đối tượng người dùng bao gồm các dữ liệu sau:
  - Username (định danh)
  - Password (mật khẩu)
  - Groups (nhóm mà người dùng là thành viên)
  - Rights (quyền hệ thống)
  - Permissions (cấp phép/quyền truy cập)

Tài khoản người dùng cục bộ

- Tài khoản người dùng cục bộ được tạo cho người dùng được phép truy cập có giới hạn đến máy tính tạo ra nó.
- Tài khoản này được tạo ra trong cơ sở dữ liệu bảo mật của máy tính cục bộ.
- Cơ sở dữ liệu này được gọi là **cơ sở dữ liệu bảo mật cục bộ**.
- Tài khoản người dùng được tạo bởi **Computer Management Console**

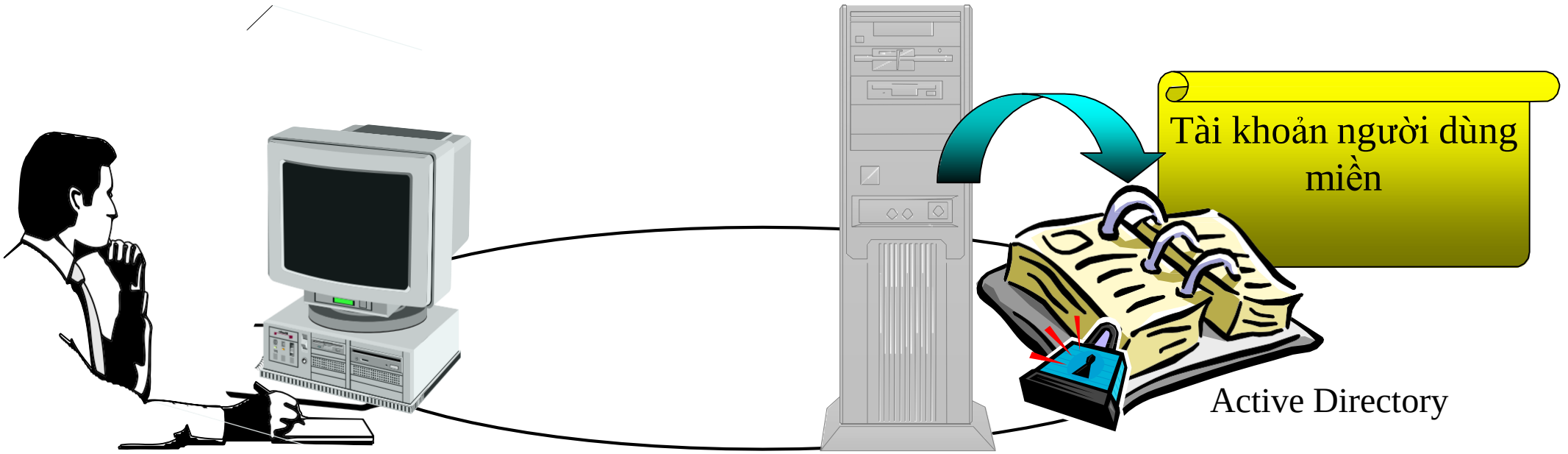
Tài khoản người dùng cục bộ



Tài khoản người dùng miền

- Cho phép người dùng đăng nhập đến miền và truy cập tài nguyên mạng bất kỳ nơi nào trên mạng.
- Bạn phải cung cấp **Username** và **Password** hợp lệ để đăng nhập thành công.
- Được tạo ra trong một bộ chứa hoặc một OU trong bản sao của cơ sở dữ liệu Active Directory trên bộ điều khiển miền.

Tài khoản người dùng miền



Lập kế hoạch tạo tài khoản người dùng

- Lập kế hoạch giúp việc tạo và tổ chức thông tin tài khoản người dùng hiệu quả
- Gồm 4 yếu tố
  - Tên tài khoản
  - Mật khẩu
  - Thẻ thông minh
  - Thuộc tính tài khoản

Tên tài khoản người dùng

- Một quy ước đặt tên giúp dễ nhớ tên đăng nhập và dễ định vị tên trong danh sách
- Các vấn đề cần lưu ý khi đặt tên:
  - Tên đăng nhập là duy nhất
  - Có tối đa 20 ký tự
  - Tránh dùng những ký tự không hợp lệ: " / \ [ ] : ; / =, + * ? < >
  - Tính tương thích E-mail
  - Tên đăng nhập không phân biệt kiểu chữ
  - Xác định loại nhân viên
  - Tên nhân viên trùng nhau

Mật khẩu tài khoản người dùng

- Ngăn chặn truy cập trái phép, phải thiết lập mật khẩu cho tài khoản
- Các vấn đề cần lưu ý khi đặt mật khẩu:
  - Tài khoản người quản trị phải có mật khẩu.
  - Hoặc người quản trị hoặc người dùng phải quản lý mật khẩu. Tốt nhất, người dùng nên quản lý mật khẩu của mình.
  - Nên tránh những mật khẩu mà người khác dễ đoán ra.
  - Không nên đặt mật khẩu quá ngắn (ít nhất 8 ký tự)
  - Nên kết hợp các ký tự chữ và số để tạo mật khẩu.
  - Chắc chắn rằng mật khẩu thay đổi không trùng với những mật khẩu trước đây và không chứa đựng tên người dùng.
  - Tốt nhất nên có ít nhất một ký tự đặc biệt trong mật khẩu.
  - Đừng bao giờ dùng một từ rất chung hay tên như là mật khẩu.

Tùy chọn mật khẩu tài khoản người dùng

- Mật khẩu người dùng là một khía cạnh quan trọng của an ninh mạng và có thể có các tùy chọn cấu hình cho:
  - Lịch sử mật khẩu (Password history)
  - Chiều dài (Length)
  - Phức tạp (Complexity)
- Mặc định, trong Windows Server ® 2012 mật khẩu miền phải đáp ứng ba trong số bốn yêu cầu phức tạp sau đây:
  - Chữ hoa (Uppercase)
  - Chữ thường (Lowercase)
  - Ký tự đặc biệt (Special characters)
  - Số (Numbers)

Thẻ thông minh

- Là một thiết bị giống như thẻ tín dụng, dùng PIN để chứng thực và truy cập hệ thống
- Một số thông tin có thể được lưu:
  - Thông tin cá nhân: tên, địa chỉ, thông tin tài khoản
  - Chứng nhận (Certificates)
  - Khoá chung (Public Keys)
  - Khoá riêng (Private Keys)
  - Mật khẩu (Password)

Thẻ thông minh

- Những yêu cầu để dùng Smart card:
  - Thiết bị đọc Smart card
  - Kết nối Smart card với một máy tính
  - Bộ phận đăng ký (người dùng có chứng nhận bộ phận đăng ký)
  - Quyền chứng nhận của đơn vị/ bộ phận đăng ký thứ 3

Thẻ thông minh

- Những vấn đề quan trọng cần xem xét:
  - Có bao nhiêu người dùng cần chứng thực?
  - Phát hành thẻ như thế nào?
  - Người dùng phải cung cấp những thông tin cá nhân nào?
  - Những người dùng cơ bản nào sẽ phải được điều tra?
  - Quá trình để báo cáo sự mất mát thẻ
  - Phát hành những thẻ tạm thời

Thiết lập thuộc tính cho tài khoản

- Các thuộc tính cho tài khoản người dùng bao gồm:
  - **Cập nhật nhóm thành viên**: cung cấp các thành viên nhóm người dùng và quyền truy cập
  - **Đặt lại mật khẩu người dùng**: thay đổi chứng thực bảo mật được sử dụng để truy cập máy tính miền
  - **Thiết lập hạn sử dụng**: là ngày hết hạn người sử dụng có thể truy cập miền
  - **Thiết lập giờ đăng nhập**: đặt giờ trong đó người dùng có thể đăng nhập vào miền
  - **Chỉ định profiles và thiết lập home folders**: Chỉ định profiles và home folders để điều chỉnh truy cập vào tài nguyên

Công cụ cấu hình các tài khoản người dùng

❖ Bạn sử dụng các công cụ khác nhau để tạo và quản lý các tài khoản người dùng cục bộ và miền:

Tài khoản	Công cụ
Tài khoản cục bộ	Windows XP, Windows Vista® và Windows 7: User Accounts
Tài khoản miền	• Windows Server 2003/2012: Active Directory Users and Computers • Command-line utilities: dsadd, Windows PowerShell™, CSVDE, LDIFDE

Tài khoản người dùng mẫu là gì?

- Là tài khoản với các thuộc tính chung đã được cấu hình sẵn
- Tận dụng các đặc điểm tương tự nhau giữa các tài khoản
- Sử dụng tài khoản người dùng mẫu để:
  - Tạo nhiều tài khoản người dùng cho các nhóm khác nhau trong tổ chức của bạn
  - Bản sao các tài khoản người dùng nhiều nhất như các tài khoản mới bạn muốn tạo
  - Sửa đổi các thuộc tính: tên, địa chỉ e-mail, đăng nhập tên, vv

User profile

- User profile là một thiết lập các thư mục và dữ liệu.
- Nó lưu trữ môi trường desktop hiện tại, các thiết lập ứng dụng và dữ liệu cá nhân của người dùng.
- User profile cung cấp một môi trường desktop nhất quán đến các người dùng.
- Các thiết lập desktop cho môi trường làm việc của người dùng trên máy tính cục bộ tự động được tạo và duy trì bởi các user profile.
- Khi người dùng đăng nhập vào máy tính lần đầu tiên, một user profile được tạo ra.

Các kiểu của User Profile

- **Mandatory User Profile:** một user profile bắt buộc một **roaming profile**
- **Local User Profile:** được tạo ra và lưu giữ trên đĩa cứng cục bộ của máy tính
- **Roaming User Profile:** quản trị hệ thống tạo ra một user profile di động, và lưu giữ trên một server
- **Temporary User Profile:** profile này sẽ bị xóa khi người dùng kết thúc session

Lưu trữ các User Profile

- Local user profile: được lưu trữ trong thư mục:
  - **C:\Users\user_logon_name**
- Roaming user profile: được đặt trong một thư mục dùng chung trên server.
- Thư mục My Documents được thiết lập tự động bởi Windows 2012.
- Nó là vị trí mặc định để lưu trữ dữ liệu người dùng cho các ứng dụng Microsoft

Local user Profile

- Local user profile: được tạo bởi Windows 2012 khi người dùng đăng nhập vào máy tính lần đầu tiên.
- Khi người dùng đăng nhập vào một máy trạm chạy Windows 2012, người dùng nhận được:
  - Các thiết lập desktop
  - Các kết nối riêng biệt

Roaming User Profiles

- Roaming user profiles có thể thiết lập để hỗ trợ người dùng làm việc trên nhiều máy tính.
- Khi họ đăng nhập vào một máy tính trong mạng, roaming user profile được sao chép bởi Win2012 từ một server mạng đến máy tính trạm đó.
- Các thiết lập roaming user profile sẽ được áp dụng lên máy tính đó.
- Win2012 sao chép tất cả tài liệu đến máy tính cục bộ khi người dùng đăng nhập lần đầu tiên.
- Một roaming user profile chuẩn có thể được tạo cho nhóm của người dùng bằng cách cấu hình môi trường desktop như yêu cầu.
- Profile chuẩn sẽ được sao chép đến vị trí đặt roaming user profile của người dùng.

Mandatory User Profile

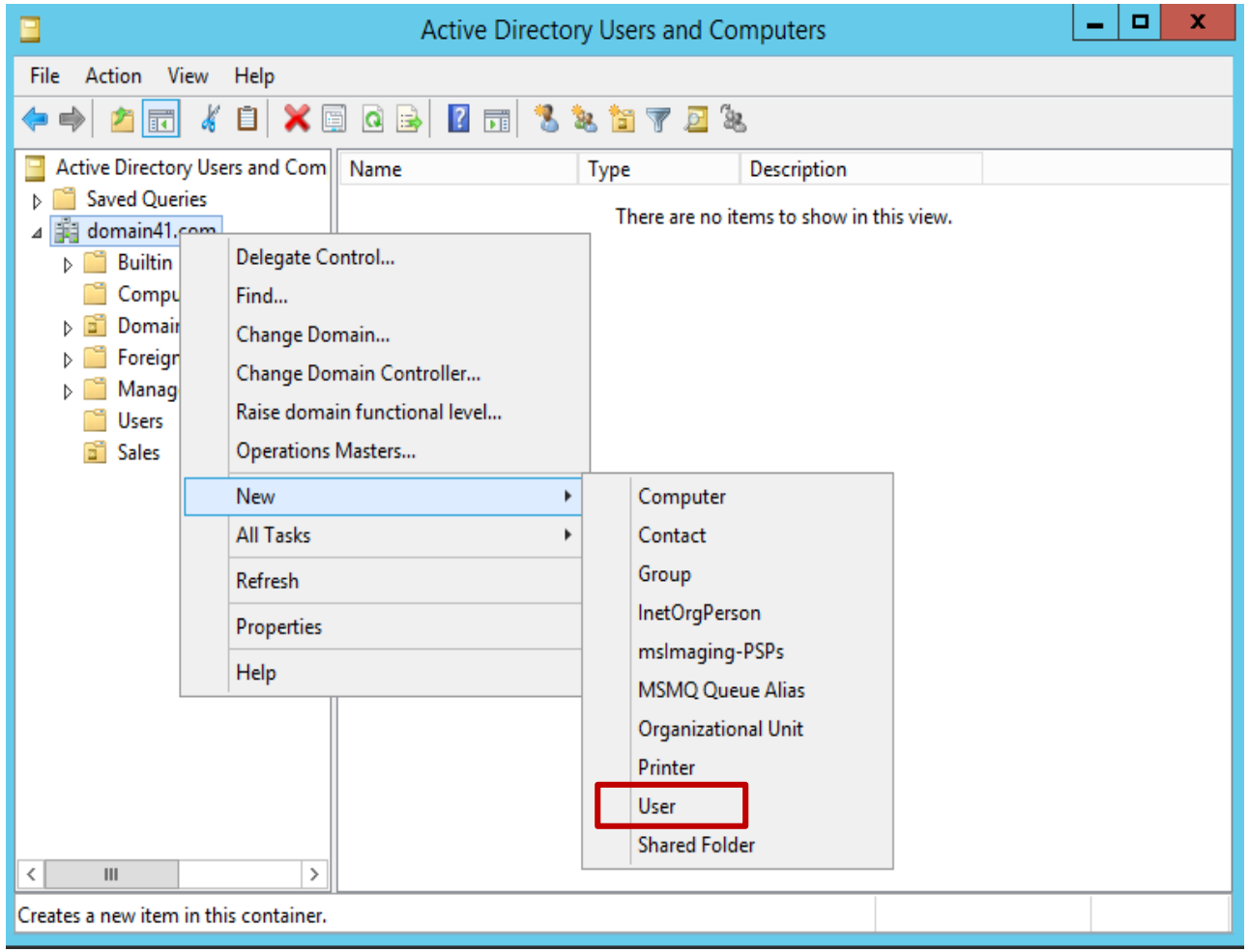
- Một mandatory user profile là một roaming user profile chỉ đọc.
- Người dùng có thể sửa đổi các thiết lập desktop khi họ đăng nhập, nhưng các thay đổi này không được lưu lại khi họ log off.
- Khi người dùng đăng nhập lần tiếp theo, profile cũng giống hệt như
  - profile đó và cho đến những lần đăng nhập sau
- Một mandatory profile có thể được gán đồng thời cho nhiều người dùng có cùng sở thích cho các thiết lập desktop.

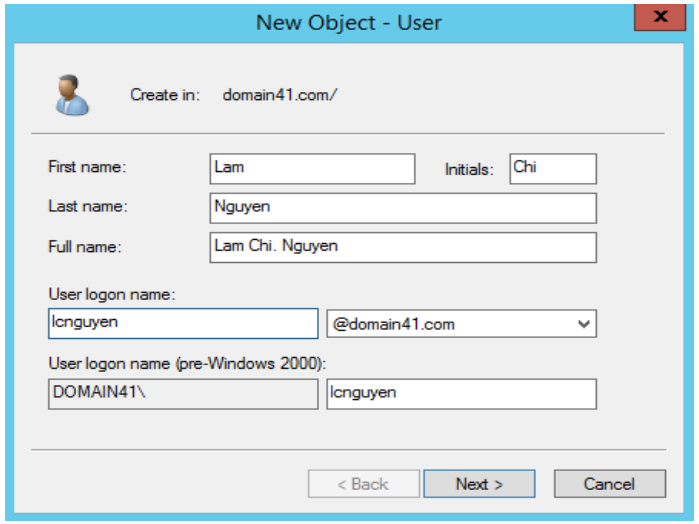
Home Directories

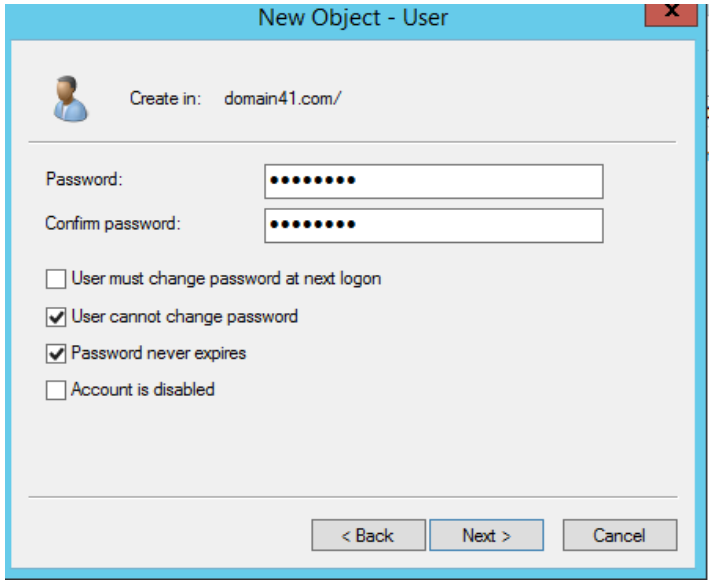
- Vị trí mặc định cho người dùng lưu trữ các tài liệu cá nhân của họ là thư mục **My Documents**.
- **Home directory** của người dùng là cung cấp thêm một vị trí nữa bởi Windows 2012 cho mục đích lưu trữ.
- Một home directory có thể lưu trữ trên máy trạm hoặc trong một thư mục dùng chung trên một file server.
- Home directories của tất cả người dùng có thể đặt vào vị trí trung tâm trên một server mạng.

Tạo người dùng

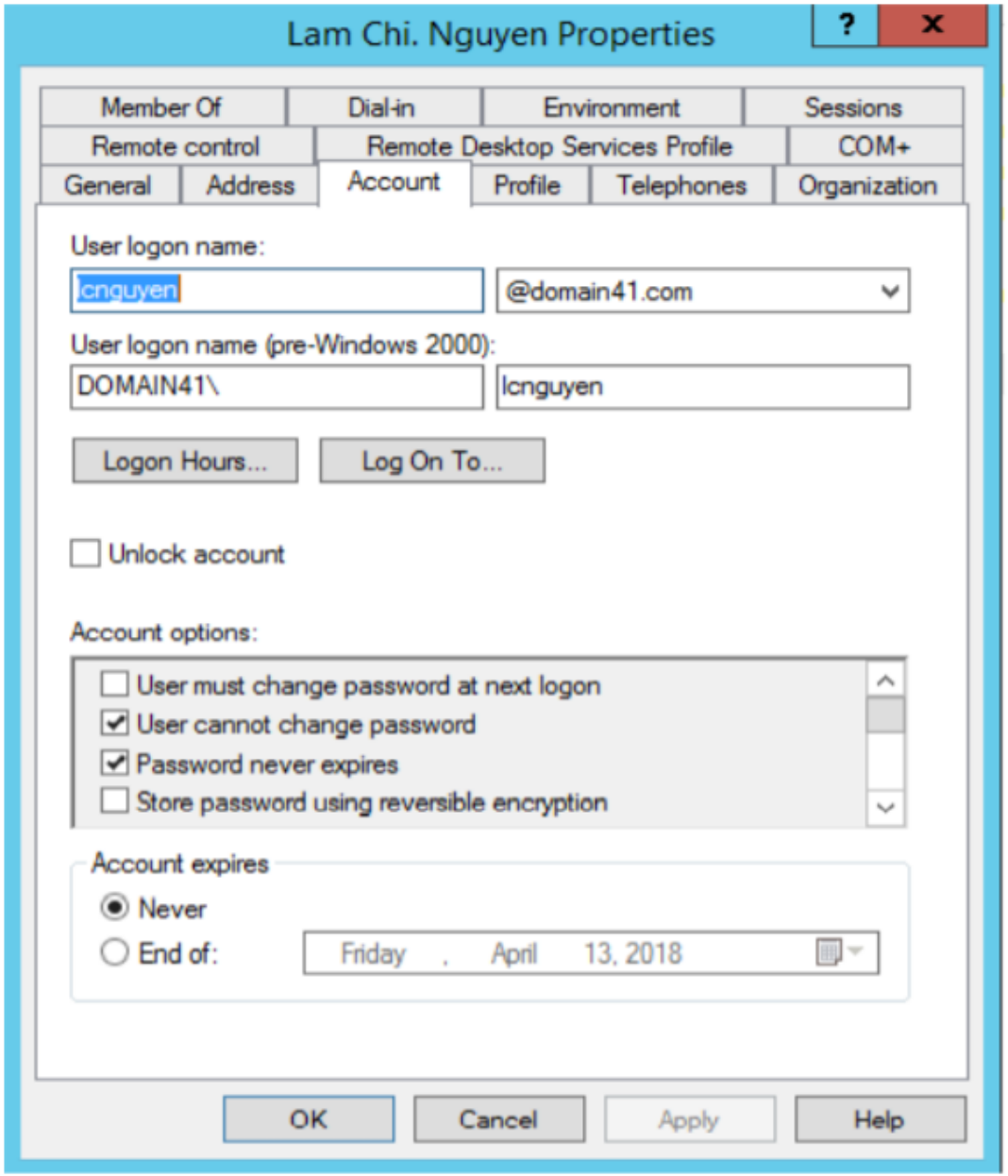
- Từ Active Directory Users and computer, click phải lên domain, chọn new và user

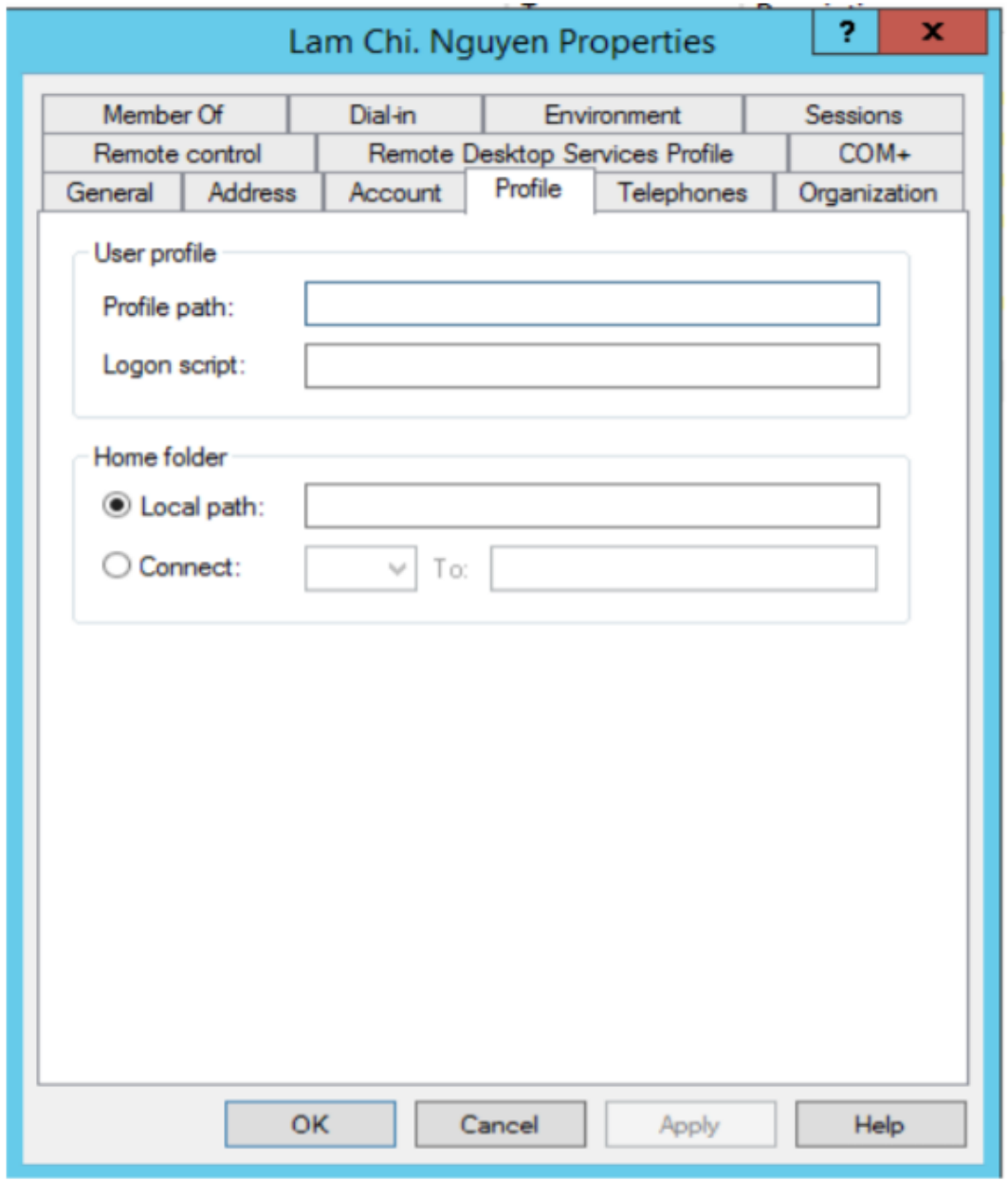




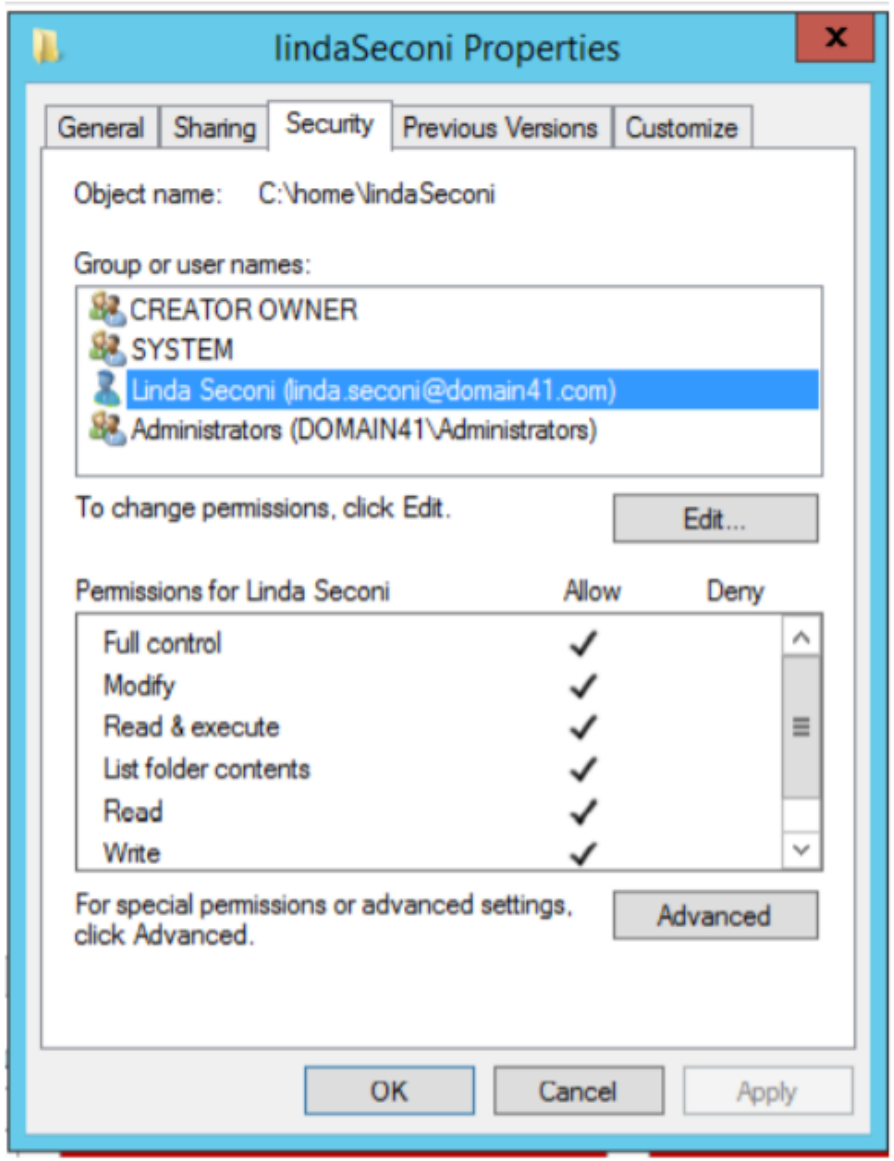


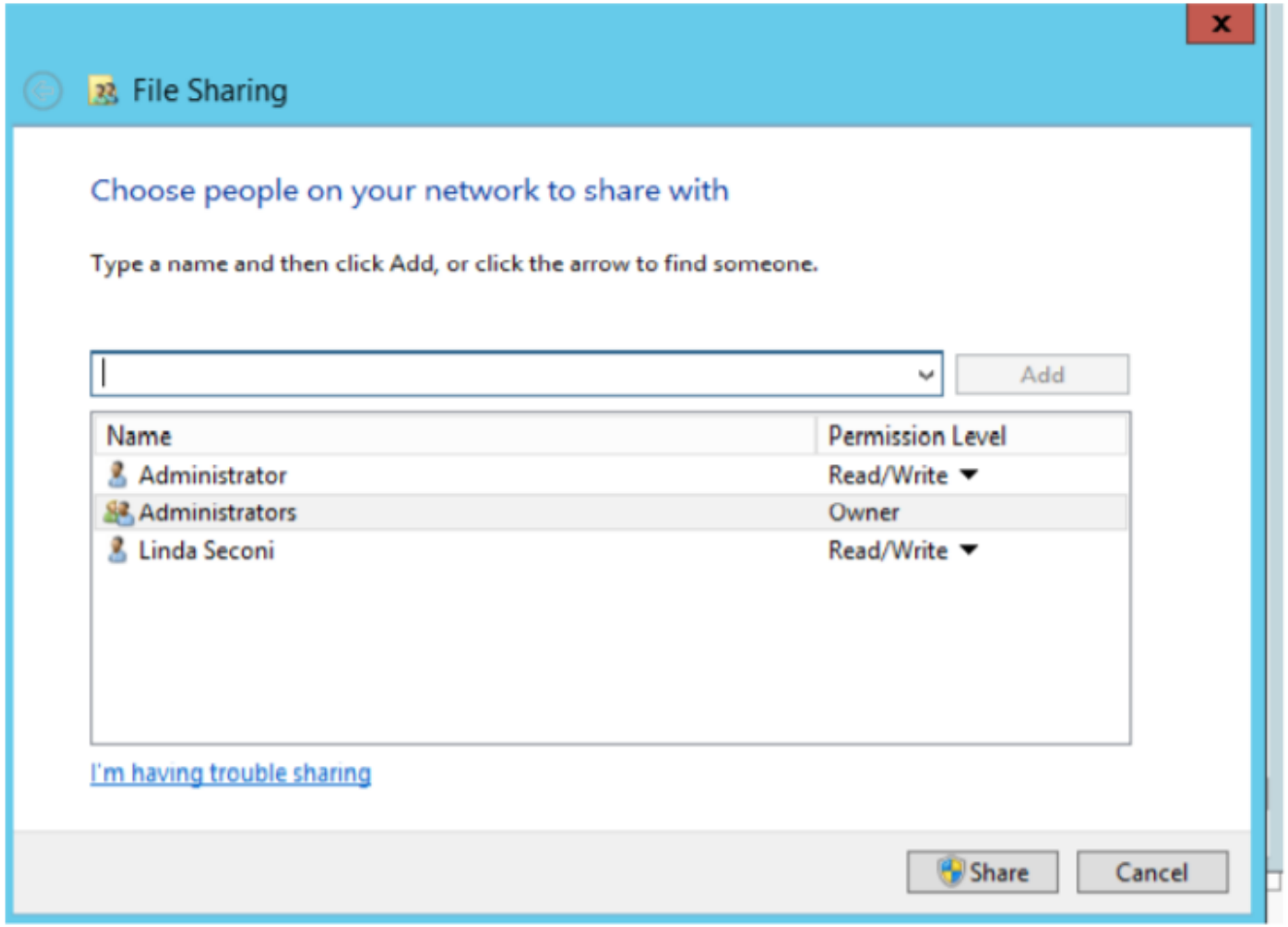
Thuộc tính của tài khoản người dùng



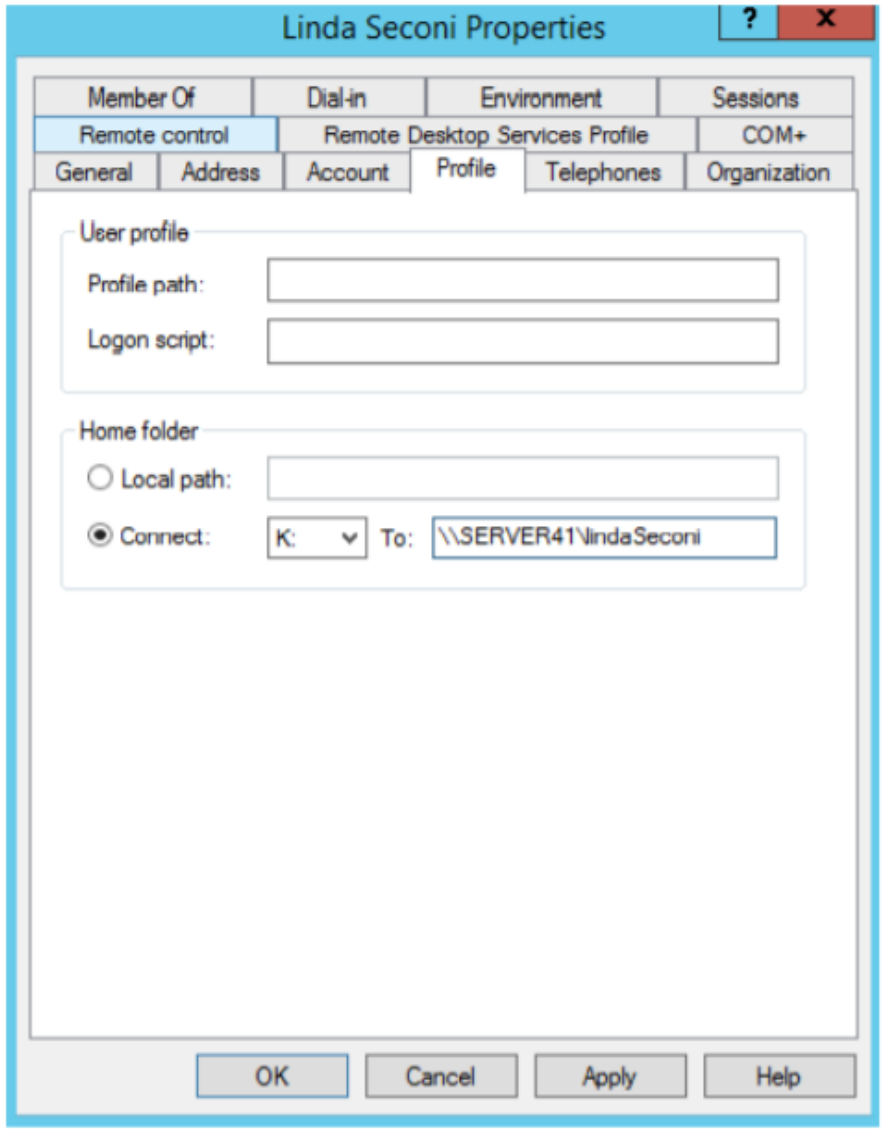


Tạo thư mục C:\hone\lindaSeconi

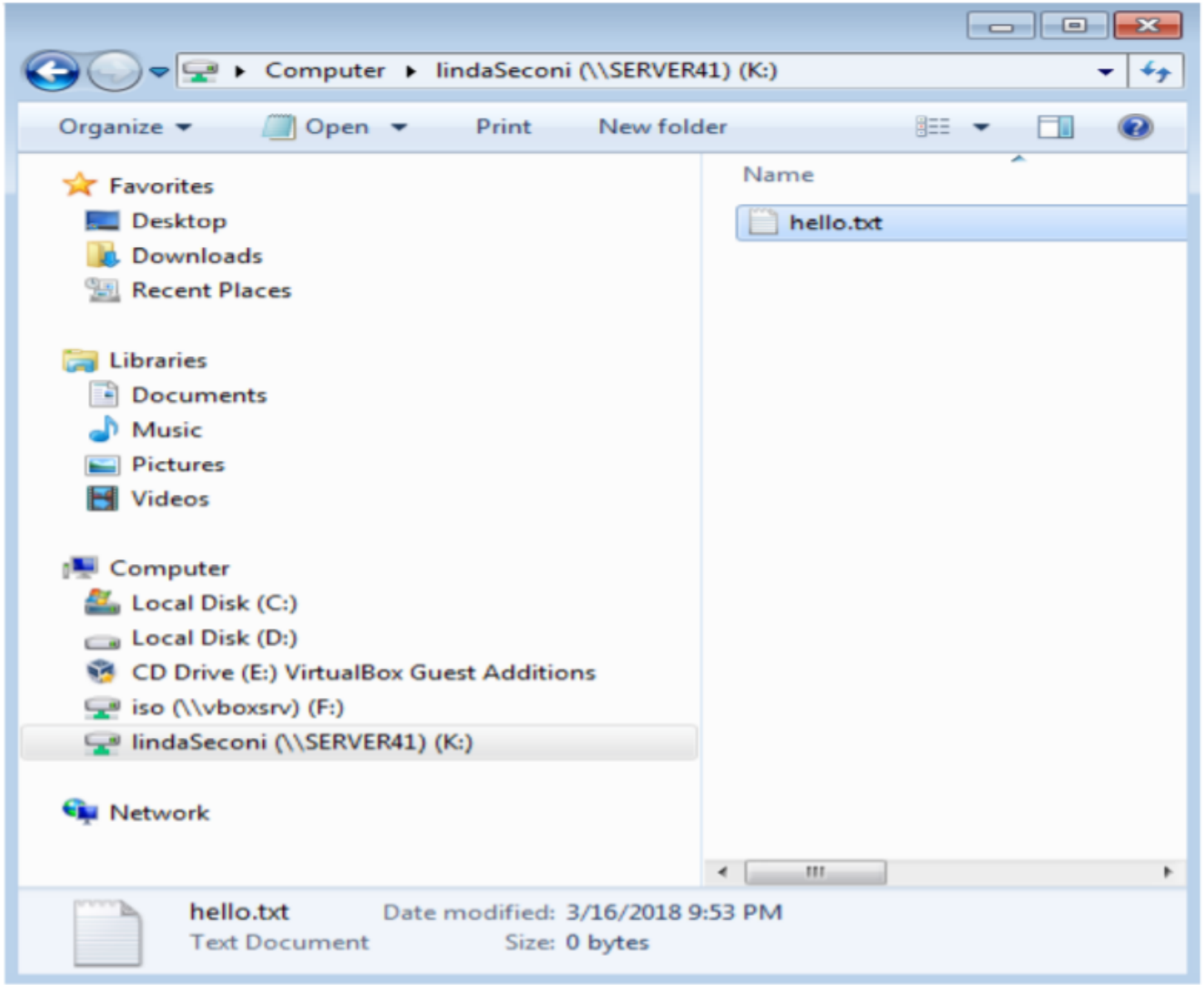




Win2012: đặt Home cho người dùng



Win7: Sử dụng tài khoản linda đăng nhập vào miền



3: Tạo tài khoản máy tính

- Tài khoản máy tính là gì?
- Các tùy chọn khi tạo tài khoản máy tính
- Quản lý tài khoản máy tính

Tài khoản máy tính là gì?

- Một tài khoản máy tính là một đối tượng trong
- AD DS xác định một máy tính kết nối vào miền.

Tài khoản máy tính:

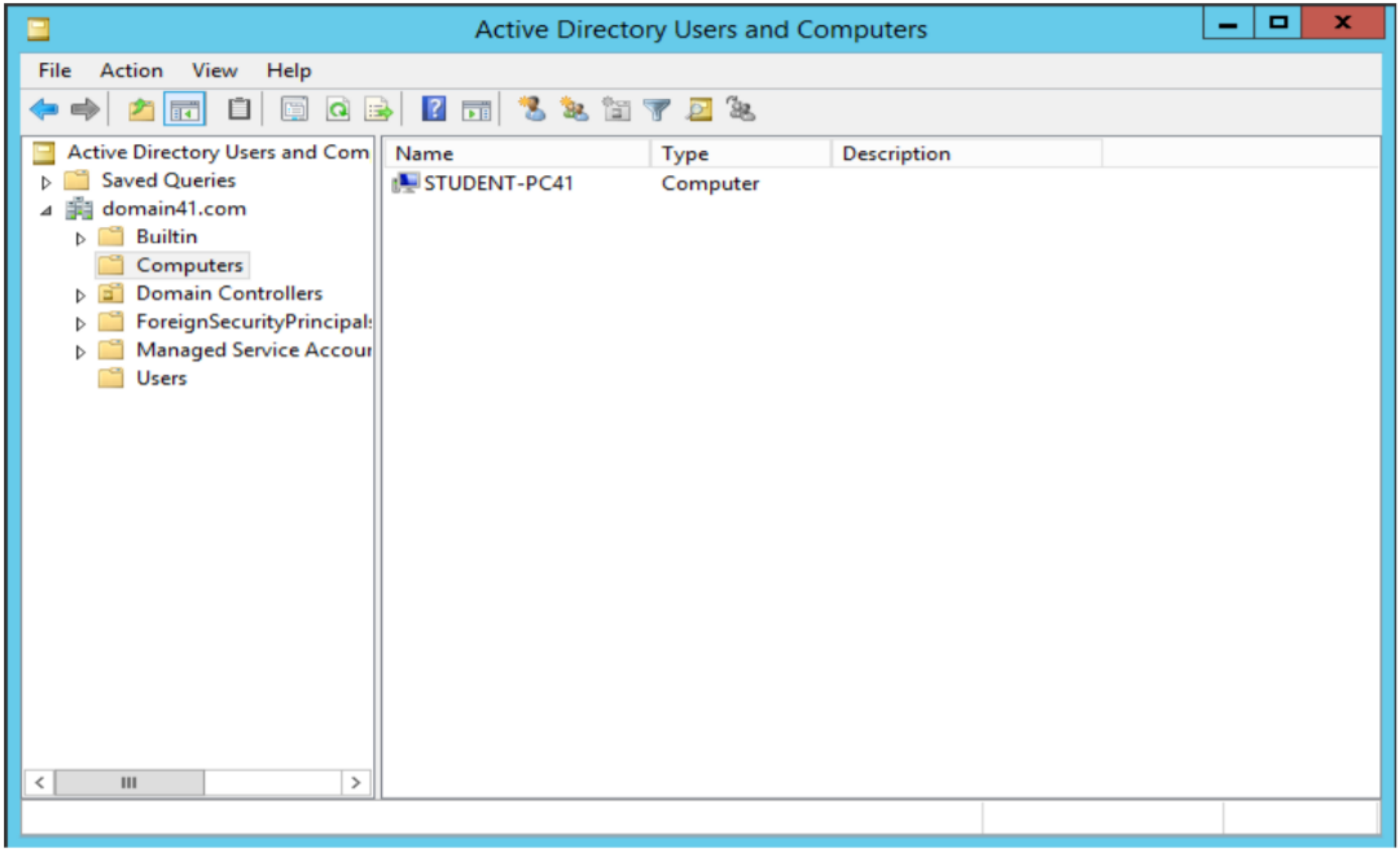
- Được yêu cầu để thẩm định và kiểm soát (trước quá trình chứng thực người dùng).
- Kích hoạt tính năng quản lý máy tính bằng cách sử dụng các chính sách nhóm

Lưu ý: nếu có tài khoản người dùng, nhưng nếu sử dụng máy tính chưa có tài khoản thì người dùng cũng không thể đăng nhập hệ thống

Các tùy chọn khi tạo tài khoản máy tính

Kịch bản	Quy trình
Thêm máy tính cá nhân vào một miền (join máy tính vào miền)	▪ Thêm máy tính vào miền thông qua computer system properties ▪ Tài khoản sẽ được tạo theo mặc định trong bộ chứa Computers
Tạo nhiều tài khoản máy tính trong việc chuẩn bị để tự động hoá một hệ điều hành và triển khai phần mềm	1. Tạo một OU cho từng bộ phận 2. Tạo các tài khoản máy tính mới 3. Thêm máy tính vào miền

Tài khoản máy tính khi được thêm vào Miền



Quản lý tài khoản máy tính

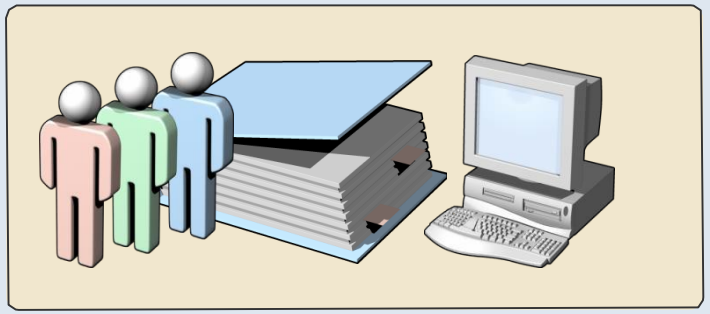
- **Quản lý máy tính hoạt động bao gồm:**
  - Thêm tài khoản máy tính: cung cấp tên máy tính và xác định các tùy chọn quản lý
  - Vô hiệu tài khoản máy tính: duy trì tài khoản, nhưng ngăn cản đăng nhập vào từ tài khoản
  - Đặt lại tài khoản máy tính: thiết lập lại các kết hợp bảo mật giữa miền và máy tính khách hàng (cần tái gia nhập)
  - Xóa tài khoản máy tính: loại bỏ máy tính từ tất cả các dịch vụ miền
  - Cấu hình chính sách nhóm: quản lý các phần mềm hay môi trường máy tính để bàn

4: Tự động quản lý đối tượng AD DS

- Các công cụ để quản lý đối tượng AD DS tự động
- Cấu hình đối tượng AD DS sử dụng công cụ dòng lệnh
- Quản lý đối tượng sử dụng với LDIFDE
- Quản lý đối tượng sử dụng với CSVDE
- Windows PowerShell là gì?

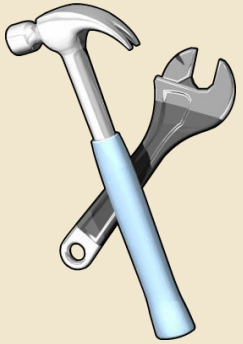
Các công cụ để quản lý đối tượng AD DS tự động

Active Directory Users and Computers

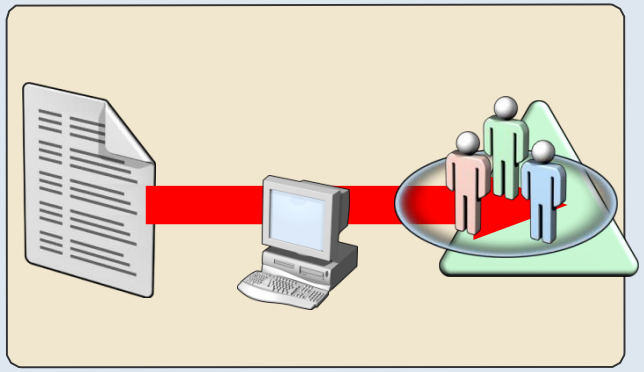


Directory Service Tools

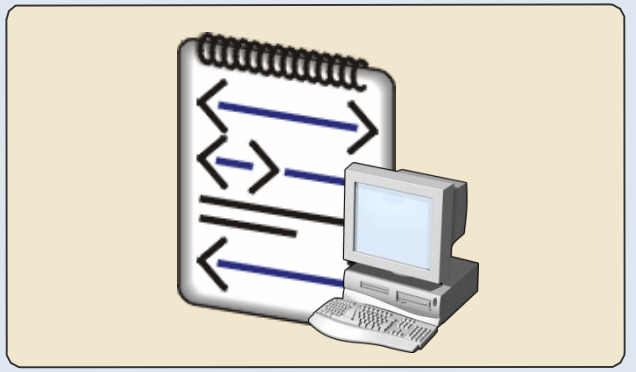
- Dsadd
- Dsmod
- Dsrm



Csvde and Ldifde Tools



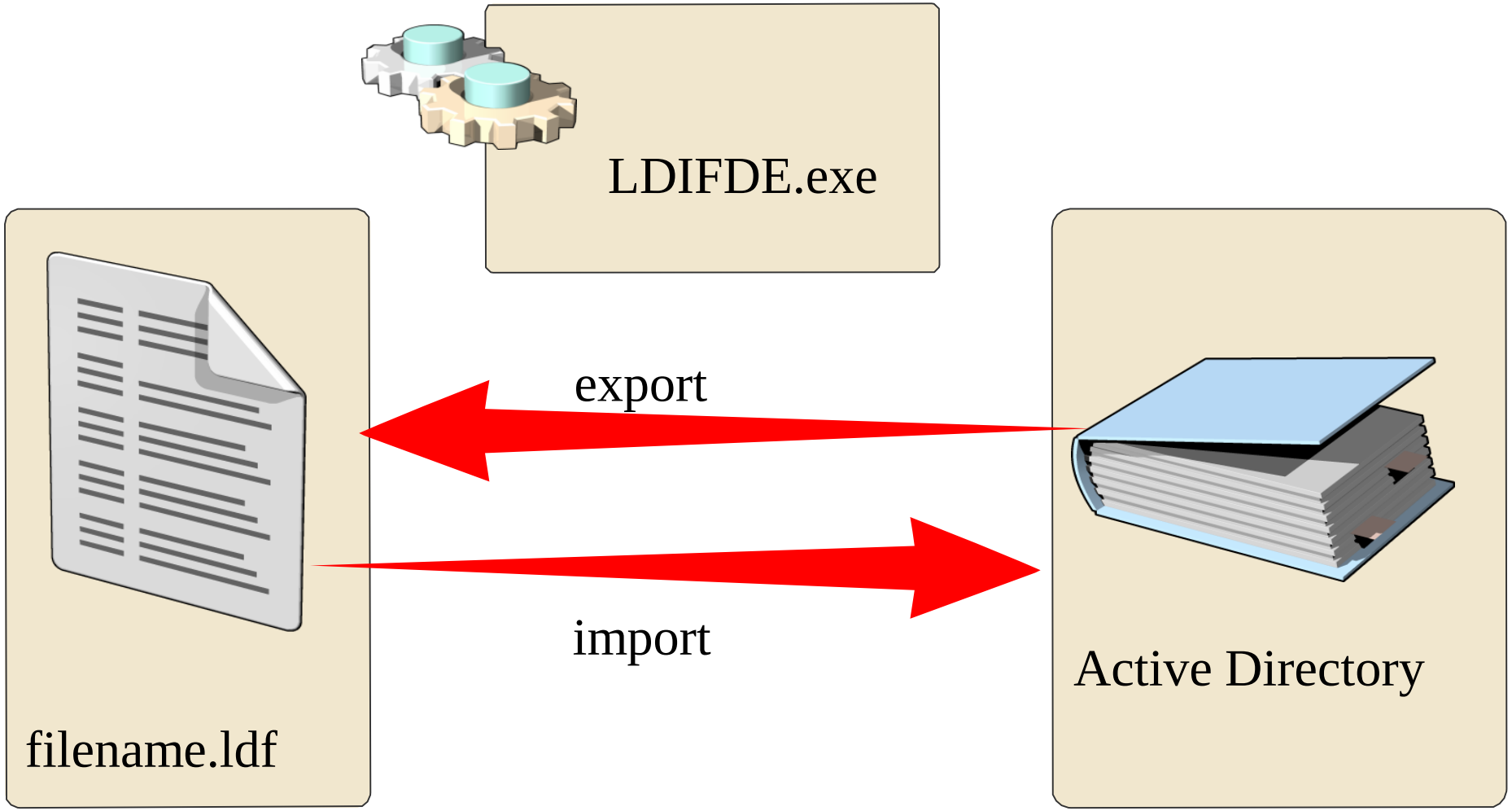
Windows PowerShell



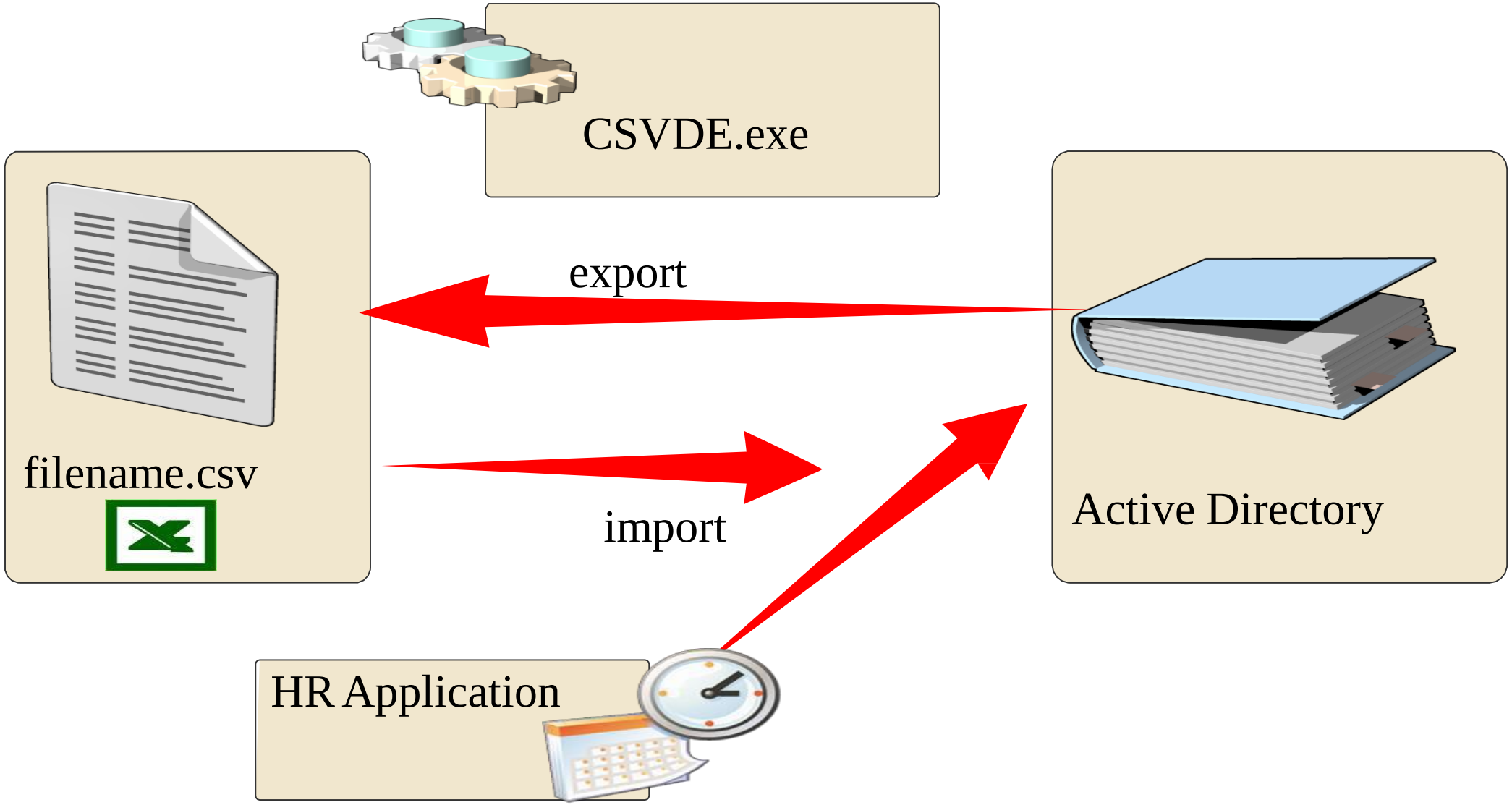
Cấu hình đối tượng AD DS sử dụng công cụ dòng lệnh

- **Công cụ dòng lệnh:**
  - Dsadd – Thêm một đối tượng đến AD DS
  - Dsmod - Sửa đổi đối tượng trong AD DS
  - Dsrm - Hủy bỏ đối tượng từ AD DS
  - Dsget - Xác định vị trí đối tượng trong AD DS
  - net user - Thêm hoặc sửa đổi tài khoản người dùng
  - Net group - Thêm hoặc thay đổi nhóm truy cập
  - Net computer - Thêm hoặc loại bỏ đối tượng máy tính từ AD DS

Quản lý đối tượng sử dụng với LDIFDE



Quản lý đối tượng sử dụng với CSVDE



Windows PowerShell là gì?

Windows PowerShell là một kịch bản và công nghệ dòng lệnh mà mà bạn có thể sử dụng để quản lý AD DS và các thành phần khác của Windows

Tính năng của Windows PowerShell bao gồm:

- Powerful single line cmdlets
- Aliases
- Variables

- Pipelining
- Scripting support
- Access to all cmd.exe commands