QUẢN TRỊ ACTIVE DIRECTORY: NHÓM NGƯỜI DÙNG (GROUP)

Tổng quan

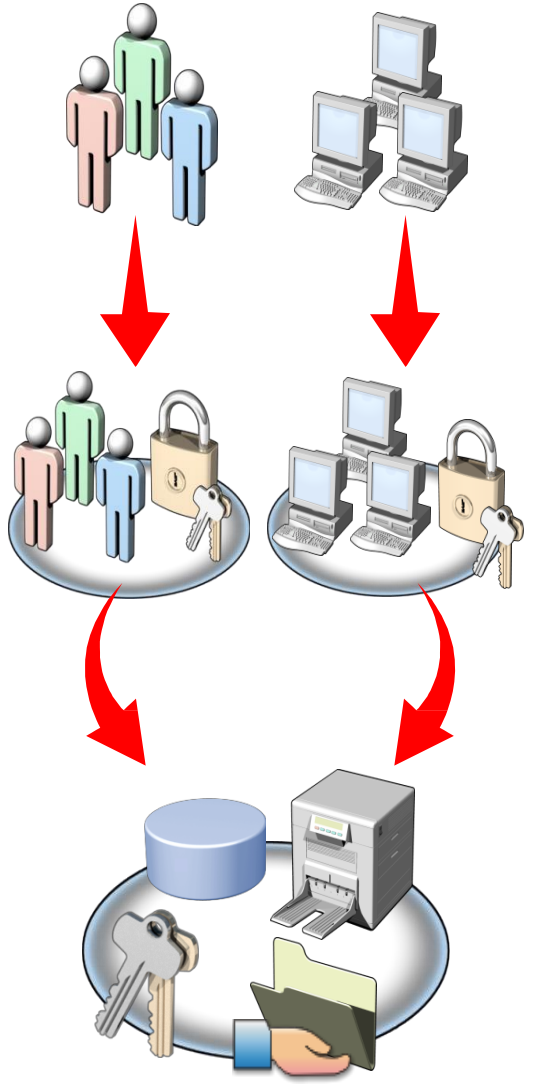
1. Giới thiệu về nhóm
2. Phạm vi nhóm
3. Kế hoạch tạo nhóm
4. Quản lý nhóm
5. Bốn kiểu nhóm mặc định

Giới thiệu về nhóm

- Các loại tài khoản
- Nhóm là gì?
- AD DS mức miền chức năng
- OU và nhóm

Các loại tài khoản

- Tài khoản người dùng
  - Cho phép người dùng đăng nhập
  - Cung cấp truy xuất tài nguyên
- Tài khoản máy tính
  - Cho phép chứng thực và ghi vết máy tính truy cập tới tài nguyên
- Tài khoản nhóm
  - Giúp đơn giản hóa việc quản trị



Nhóm là gì?

- Nhóm là tập hợp các tài khoản người dùng và tài khoản máy tính
- Nhóm được sử dụng cấp quyền sử dụng tài nguyên cho nhiều người dùng cùng lúc thay vì gán cho từng tài khoản người dùng riêng lẻ
- Một người dùng có thể thuộc nhiều hơn một nhóm.
- Một nhóm có thể là thành viên của một nhóm khác.
- Máy tính, contacts, và các nhóm khác cũng có thể được thêm vào nhóm.

Các kiểu của nhóm

- Nhóm bảo mật (Security groups)
  - Được dùng để gán quyền truy cập tài nguyên
- Nhóm phân phối (Distribution groups)
  - Không được dùng để gán quyền truy cập và phân quyền
  - Được các ứng dụng sử dụng để phân phối thông điệp tới nhiều người dùng (ví dụ: Microsoft Exchange)

OUs và Group

OUs	Nhóm
Bạn có thể áp dụng các thiết lập chính sách nhóm đến một OU	Bạn không thể áp dụng các thiết lập chính sách nhóm trực tiếp vào một nhóm
Một người dùng chỉ có thể thuộc về một OU tại một thời điểm	Một người dùng có thể thuộc về nhiều nhóm cùng một lúc
Bạn không thể sử dụng một OU để cấp hoặc từ chối quyền truy cập bảo mật đến các tài nguyên	Nhóm được sử dụng để cấp hoặc từ chối quyền truy cập bảo mật đến các tài nguyên
Bạn không thể sử dụng một OU để phân phối e-mail	Bạn có thể sử dụng các nhóm để phân phối e-mail

Phạm vi nhóm

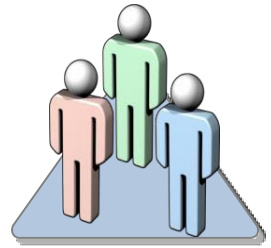
- Các loại phạm vi nhóm
- Nhóm toàn cầu (Global Groups) là gì?
- Nhóm chung (Universal Groups) là gì?
- Nhóm cục bộ miền (Domain Local Groups) là gì?
- Nhóm cục bộ (Local Groups) là gì?

Các loại phạm vi nhóm

Nhóm cục bộ miền
Domain Local Group

Phạm vi

Nhóm toàn cục
Global Group



Nhóm chung
Universal Group

Nhóm cục bộ miền (Domain Local Group) là gì?

- Các thành viên:
  - Tài khoản người dùng / tài khoản máy tính từ bất kỳ miền trong rừng hoặc bất kỳ miền tin cậy
  - Nhóm toàn cục từ bất kỳ miền trong rừng hoặc bất kỳ miền tin cậy
  - Nhóm chung từ bất kỳ miền trong rừng hoặc miền tin cậy
  - Nhóm cục bộ miền khác trong cùng một miền
- Sử dụng: để cấp quyền sử dụng các tài nguyên nằm trên chính miền đó
- Có thể được chuyển thành: nhóm chung (nếu không tồn tại nhóm cục bộ miền khác là thành viên)

Nhóm toàn cầu (Global Group) là gì?

- Các thành viên:
  - Tài khoản người dùng và máy tính của cùng một miền
  - Nhóm toàn cầu trong cùng một miền
- Quyền truy cập:
  - Thường được lồng vào nhóm cục bộ miền để cấp quyền truy cập tài nguyên trong mọi miền trong rừng.
  - Được nhân bản đến các domain controller trong cùng miền
- Cách sử dụng: để nhóm các người dùng có cùng yêu cầu truy cập tài nguyên mạng tương tự như nhau
- Có thể được chuyển thành: nhóm chung (Universal) (nếu nó không phải là thành viên của bất kỳ nhóm toàn cầu nào khác)

Nhóm chung (Universal Group) là gì?

- Các thành viên:
  - Tài khoản người dùng và máy tính từ bất kỳ miền trong rừng
  - Nhóm toàn cầu và nhóm chung từ bất kỳ miền trong rừng
- Quyền truy cập:
  - Có thể được gán quyền truy cập vào bất kỳ miền nào trong rừng hoặc bất kỳ miền tin tưởng khác
- Cách sử dụng: được lồng vào nhóm **cục bộ miền** để cấp quyền đến tài nguyên mọi miền trong rừng
- Có thể được chuyển thành:
  - Nhóm cục bộ miền (Domain local)
  - Nhóm toàn cầu (nếu nó không có nhóm chung khác tồn tại như là một thành viên)

Phạm vi nhóm

Global group

Members come only from local domain.
Members can access resources in any domain.

Domain local group

Members can come from any domain.
Members access resources only in local domain.

Universal group

Members can come from any domain.
Members can access resources in any domain.

Nhóm cục bộ (Local Groups)?

- Các thành viên:
  - Tài khoản người dùng cục bộ
  - Tài khoản người dùng miền
  - Nhóm miền
- Quyền truy cập:
  - Nhóm cục bộ chỉ được gán quyền truy cập đến tài nguyên trên máy tính cục bộ đó

Nhóm cục bộ không thể được tạo ra trên bộ điều khiển miền

Kế hoạch tạo nhóm

- Nhóm **toàn cục** có các người dùng có cùng trách nhiệm, công việc
- Tạo nhóm **cục bộ miền** cho các tài nguyên dùng chung
- Các nhóm **toàn cục** cần truy cập đến tài nguyên có thể là thành viên của nhóm **cục bộ miền**
- Thiết lập quyền truy cập tài nguyên cho nhóm cục bộ miền
- Những hạn chế khác trong kế hoạch tạo nhóm:
  - Có các nhóm toàn cục với các tài khoản người dùng và thiết lập quyền cho các nhóm toàn cục
  - Có các nhóm cục bộ miền với các tài khoản người dùng và thiết lập quyền cho các nhóm cục bộ miền

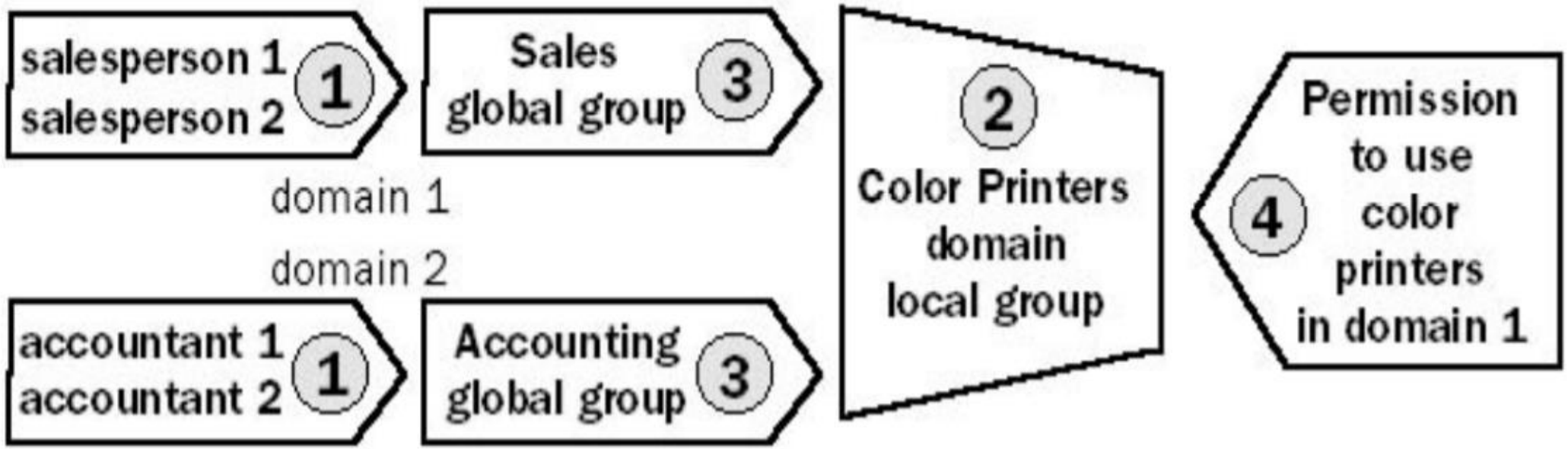
Nhóm lồng nhau là gì?

- Lồng nhau là cho một nhóm là thành viên của một nhóm khác
- Lợi ích của việc sử dụng một chiến lược lồng nhau trong việc quản lý nhóm AD DS:
  - Lồng nhau giúp lưu lượng mạng giữa các miền giảm và việc quản trị trong cây miền được đơn giản hơn
  - Nhóm lồng nhau giúp việc quản lý đơn giản hơn

Kế hoạch tạo nhóm

Loại nhóm	Có thể được xếp lồng trong nhóm Local	Có thể được xếp lồng trong nhóm Domain Local	Có thể được xếp lồng trong nhóm Global	Có thể được xếp lồng trong nhóm Universal
Local	Không	Không	Không	Không
Domain Local	Có	Có (nếu cùng miền)	Không	Không
Global	Có	Có	Có (nếu cùng miền)	Có
Universal	Có	Có	Không	Có

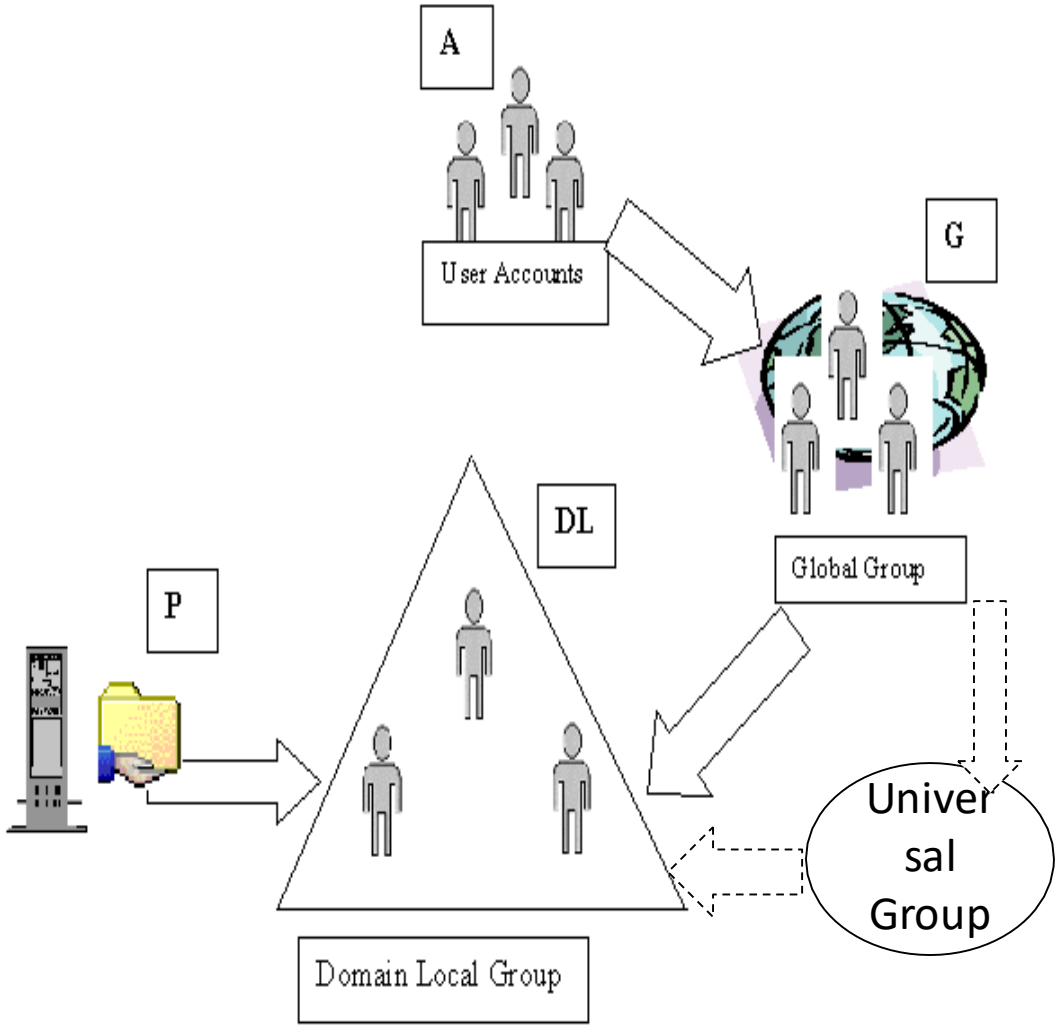
Kế hoạch tạo nhóm



1. Assign users with common job responsibilities to global groups.
2. Create a domain local group for resources to be shared.
3. Add global groups who need access to the resources to the domain local group.
4. Assign resource permissions to the domain local group.

Chiến lược tạo nhóm

1. Tạo tài khoản người dùng
2. Cho tài khoản người dùng là thành viên của nhóm toàn cục
3. Lồng nhóm toàn cục vào nhóm phổ quát
4. Lồng nhóm phổ quát vào nhóm miền cục bộ
5. Thực hiện cấp quyền cho nhóm miền cục bộ



Quản lý nhóm

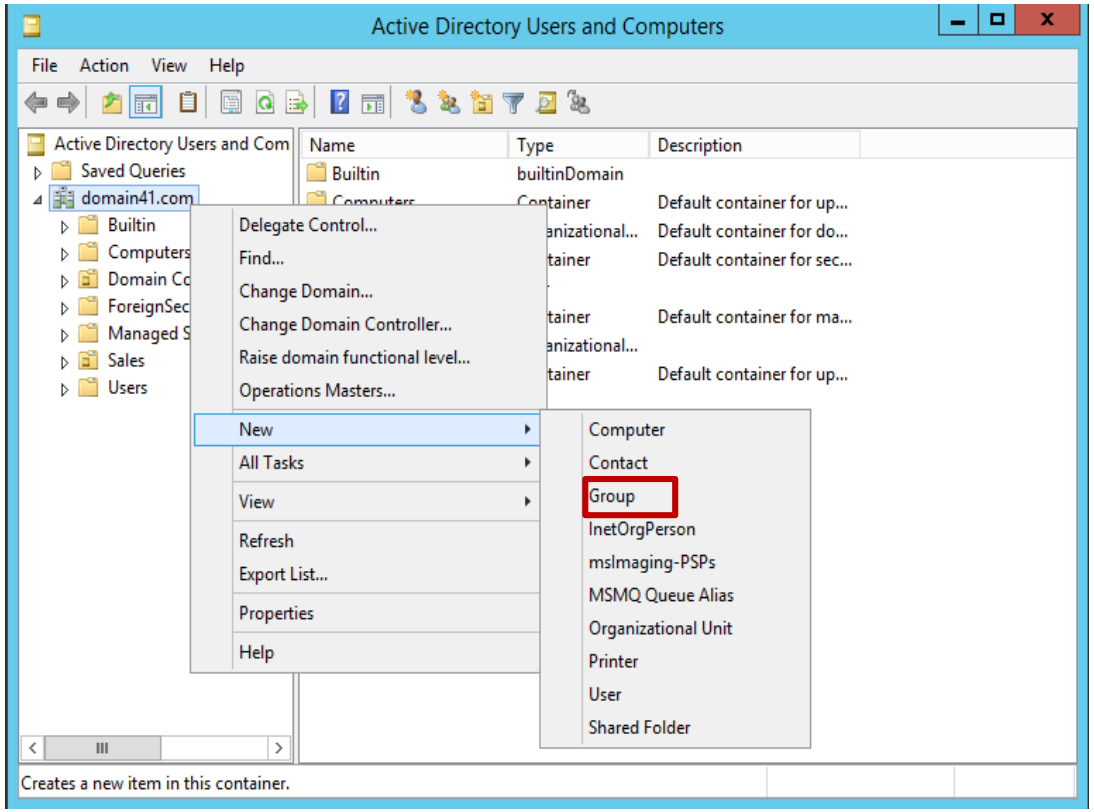
- Xem xét việc đặt tên nhóm
- Tạo và xóa nhóm
- Xác định các thành viên của nhóm
- Thay đổi kiểu nhóm
- Thay đổi phạm vi nhóm

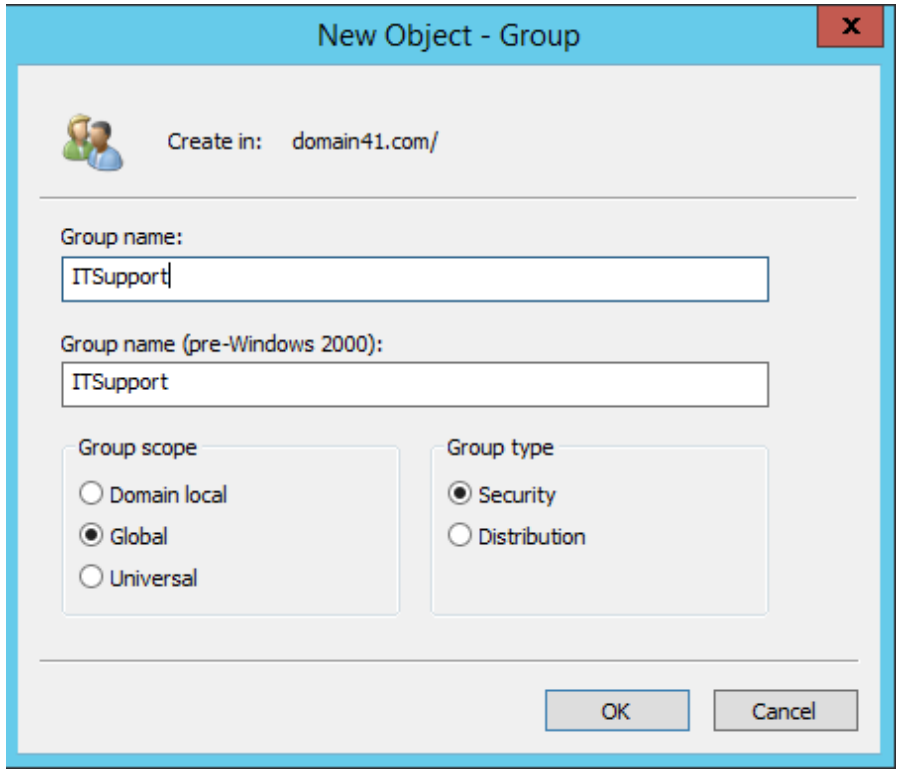
Xem xét việc đặt tên nhóm

Sử dụng cách đặt tên ngắn gọn	▪ Tránh các tên dài phức tạp ▪ Sử dụng tên chung
Sử dụng tên phòng ban	▪ Sales ▪ Marketing ▪ Executives (Nhân viên điều hành)
Sử dụng các tên địa lý	Nhóm người dùng theo các địa điểm: ▪ Quốc gia (Countries) ▪ Vùng ▪ Thành phố (Cities)
Sử dụng tên dự án cụ thể	Nếu các nhóm được tạo ra cho dự án, sử dụng tên dự án để mô tả

Tạo và xóa nhóm

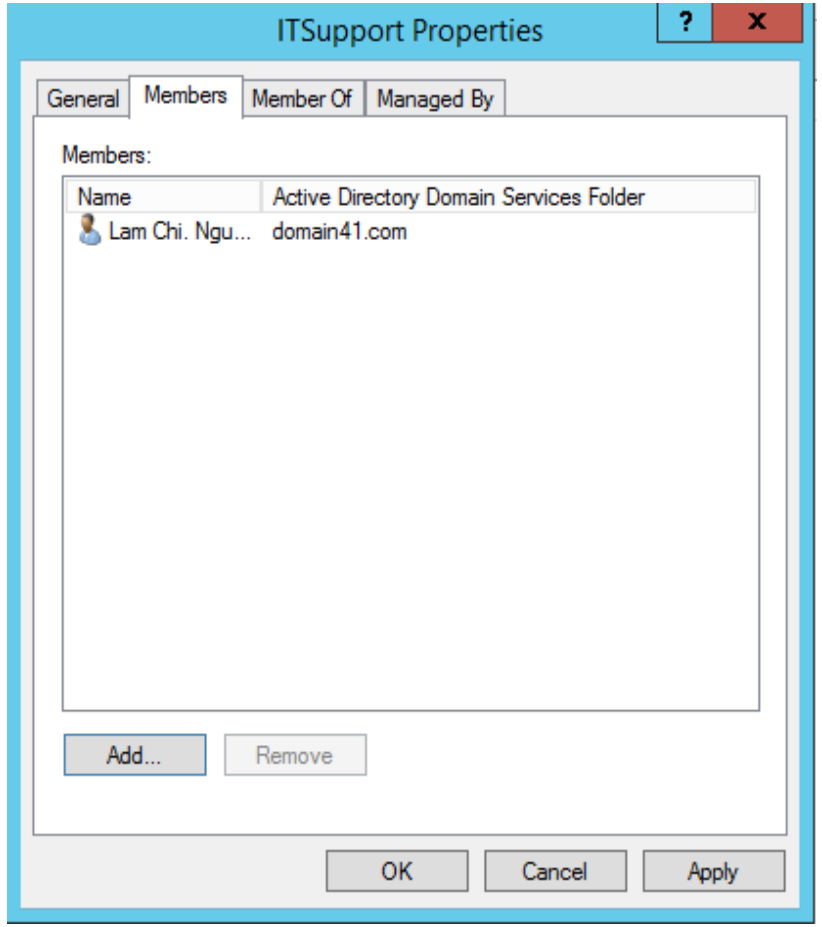
- Bạn có thể sử dụng Active Directory Users and Computers console để tạo và xóa nhóm.
- Bạn phải tạo nhóm trong bộ chứa users, bộ chứa khác, hoặc một OU đó là tạo sự rõ ràng cho nhóm.





Xác định các thành viên của nhóm

- Members tab: các thành viên của một nhóm được liệt kê trong tab Members:
  - Tài khoản người dùng
  - Nhóm lồng nhau
- Members Of tab
  - Tab Members Of là danh sách các nhóm mà hiện tại nhóm là thành viên



Thay đổi kiểu nhóm

- Kiểu nhóm có thể được thay đổi bằng các nhóm chức năng thay đổi.
- Click chuột phải lên nhóm và chọn **Properties**.
- Bạn có thể thay đổi kiểu trên tab **General**

Thay đổi phạm vi nhóm

- **Nhóm toàn cục** có thể được thay đổi thành nhóm **universal** chỉ khi nhóm toàn cục đó không nằm trong nhóm toàn cục khác.
- Nhóm **cục bộ miền** có thể được thay đổi thành nhóm **universal** chỉ khi nhóm cục bộ miền đó không có nhóm cục bộ miền khác là thành viên.

Bốn kiểu nhóm mặc định

- Nhóm được định nghĩa trước - Predefined
- Nhóm cục bộ miền dựng sẵn - Built-in domain local
- Nhóm cục bộ dựng sẵn - Built-in local
- Nhóm định danh đặc biệt -Special identity.

Các nhóm toàn cục được định nghĩa trước

- Có phạm vi toàn cục, những thành viên này được thêm vào tự động
- **Domain Admins:** được thêm tự động vào nhóm cục bộ miền được định nghĩa sẵn là Administrators bởi WS2012.
- **Domain Users:** được thêm tự động vào nhóm cục bộ miền là nhóm **Users**, tài khoản người dùng được tạo ra trong miền là thành viên mặc định của nhóm này
- **Domain Guests:** được thêm tự động vào nhóm cục bộ miền là nhóm Guests, tài khoản guest là thành viên mặc định của
- **Enterprise Admins:** thành viên của nhóm có thể điều khiển quản trị toàn mạng hệ thống mạng, Administrator là tài khoản mặc định của nhóm này

Các nhóm cục bộ miền dựng sẵn

- Được dùng để gán quyền cho chúng để thực hiện nhiệm vụ trên
- những bộ điều khiển miền

Các nhóm phổ biến

- **Account Operators**: cho phép để tạo ra, xóa, và sửa đổi tài khoản người dùng và nhóm
- **Administrators**: cho phép thực hiện tất cả những nhiệm vụ quản trị trên miền này, và trên tất cả các bộ điều khiển miền khác
- **Backup Operators**:cho phép để thực hiện việc sao lưu và khôi phục tất cả các bộ điều khiển miền với sự trợ giúp của tiện ích Windows Backup
- **Guests**: chỉ để thực hiện một số quyền mà họ được gán quyền

Các nhóm cục bộ miền dựng sẵn

- **Print Operators:** thiết lập và quản lý các máy in mạng trên những bộ điều khiển miền
- **Replicator:** thực hiện các chức năng tạo nhân bản thư mục
- **Server Operators:** các thành viên của nhóm được cho phép để chia sẻ những tài nguyên trên đĩa, sao lưu và khôi phục các tập tin trên bộ điều khiển miền.
- **Users:** các thành viên chỉ có thể thực hiện những nhiệm vụ riêng biệt được xác định trước, và chúng được cho truy cập tới tài nguyên mà ta có gán quyền

Các nhóm cục bộ dựng sẵn

- Hiện diện trên tất cả server độc lập (standalone), các server thành viên và các máy tính cài Windows 2012
- Các nhóm dựng sẵn thông dụng:
  - **Administrators:** cho phép thực hiện tất cả các nhiệm vụ quản trị trên máy tính
  - **Backup Operators**: cho phép để sử dụng tiện ích Windows Backup nhằm sao lưu và khôi phục máy tính
  - **Guests:** chỉ để thực hiện đúng quyền mà nó được cấp
  - **Power Users**: cho phép để tạo ra và sửa đổi tài khoản người dùng cục bộ trên máy tính và thực hiện chia sẻ tài nguyên
  - **Replicator**: thực hiện những chức năng nhân bản thư mục
  - **Users**: chỉ có thể thực hiện những nhiệm vụ riêng biệt được xác định trước, và chúng được cho truy cập tới tài nguyên mà chúng ta có gán quyền

Nhóm định danh đặc biệt

- Nhóm này không chứa thành viên cụ thể mà có thể thay đổi, nhóm này đại diện cho những người dùng khác nhau tại những thời điểm khác nhau, dựa vào cách một người dùng truy cập tài nguyên
- Các nhóm thông dụng:
  - Anonymous Logon: bất kỳ tài khoản người dùng nào không được xác thực bởi Windows 2012 đều là một thành viên của nhóm này
  - Authenticated Users: tất cả các người dùng với một tài khoản người dùng hợp lệ trên máy tính hay trong Active Directory là những thành viên của nhóm này
  - Creator Owner: tài khoản người dùng được tạo ra hay lấy quyền sở hữu của một tài nguyên là một thành viên của nhóm này
  - Dialup: bất kỳ người dùng nào mà hiện thời có một kết nối quay số là một thành viên của nhóm này
  - Everyone: tất cả những người dùng có thể truy cập máy tính đều là thành viên của nhóm này

Nhóm Administrators

- Microsoft đề nghị người quản trị không được gán đến nhóm Administrators.
- Khi bạn chạy Windows 2012 bằng **administrator** hoặc là một thành viên của nhóm quản trị, mạng sẽ dể bị Trojan tấn công và mất an toàn.
- Đăng nhập với đặt quyền quản trị sẽ bao hàm các rủi ro to lớn.
- Bạn chỉ nên gán mình vào nhóm **Users hoặc Power Users.**
- Để thực hiện các thao tác quản trị, đăng nhập bằng **administrator**, thực hiện các thao tác cần thiết và log off máy tính.

Danh sách các nhóm