WINDOWS SERVER 2012

Bài 3

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG VÀ NHÓM

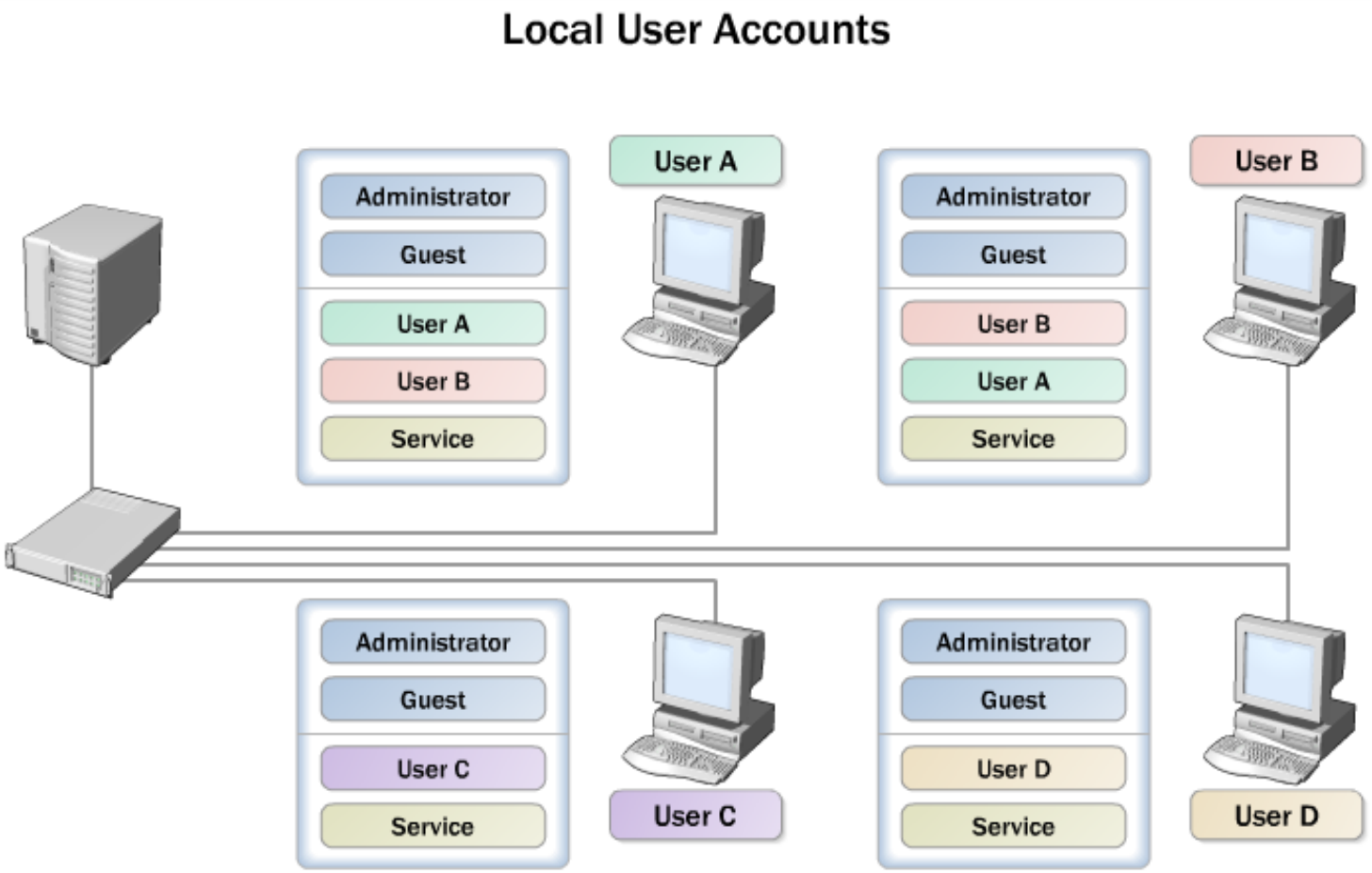
Nội dung bài học

- Tài khoản người dùng và tài khoản nhóm
- Chứng thực và kiểm soát truy cập
- Các tài khoản tạo sẵn
- Quản lý tài khoản người dùng và nhóm cục bộ
- Quản lý tài khoản người dùng vá nhóm trên Active Directory

Định nghĩa tài khoản người dùng và tài khoản nhóm

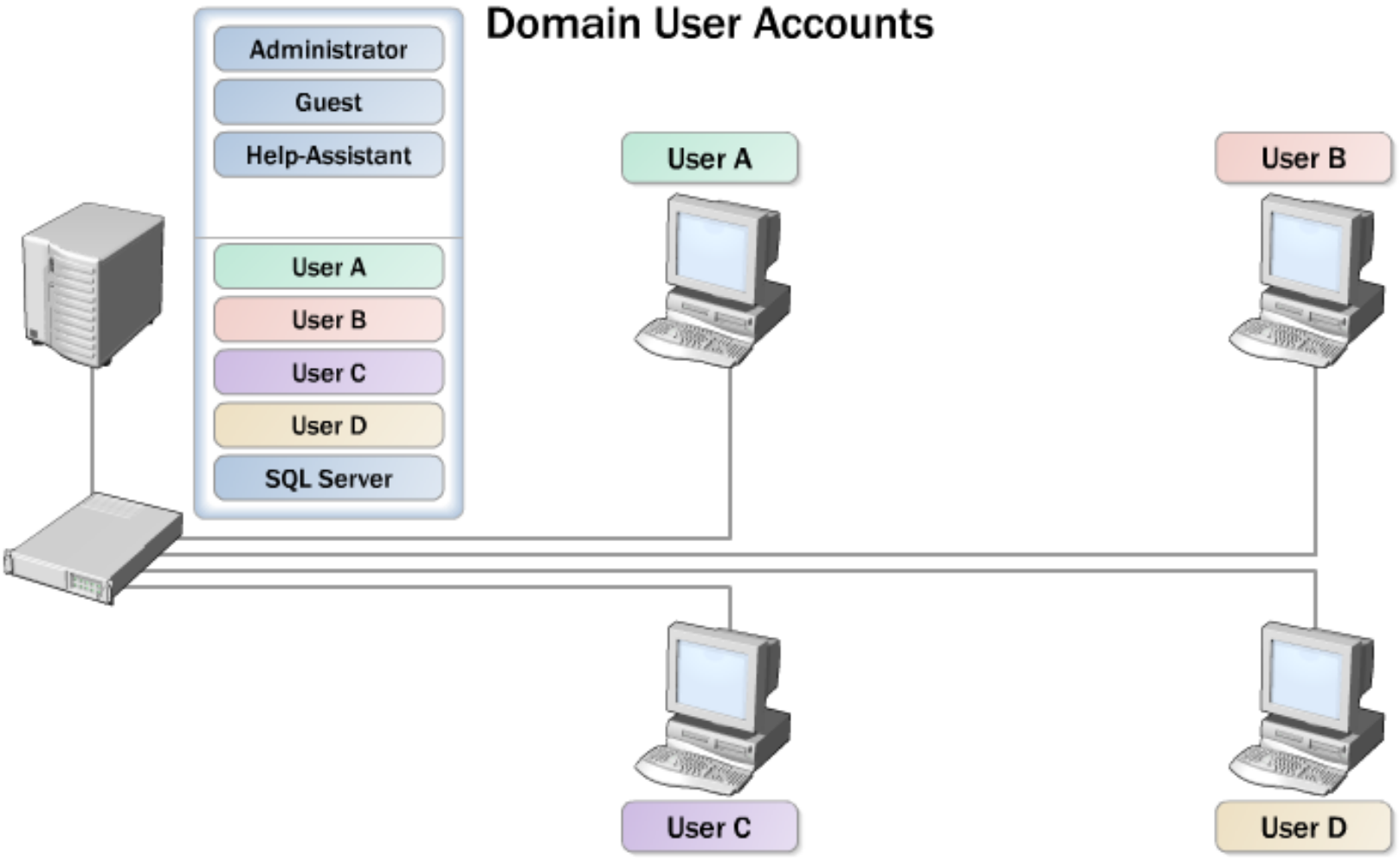
➢ Tài khoản người dùng

- **Tài khoản người dùng cục bộ**



Tài khoản người dùng (t.t)

- **Tài khoản người dùng miền**



Tài khoản người dùng (t.t)

- **Yêu cầu tài khoản người dùng**
  - **Username: dài 1-20 ký tự (từ Windows Server 2003 trở đi, username có thể dài 104 ký tự, tuy nhiên khi đăng nhập từ các máy cài hệ điều hành Windows NT 4.0 về trước thì mặc định chỉ hiểu 20 ký tự)**
  - **Username là một chuỗi duy nhất**
  - **Username không chứa các ký tự sau: " / \ [ ] : ; | = , + * ? < > "**
  - **Username có thể chứa các ký tự đặc biệt: dấu chấm câu, khoảng trắng, dấu gạch ngang, dấu gạch dưới.**

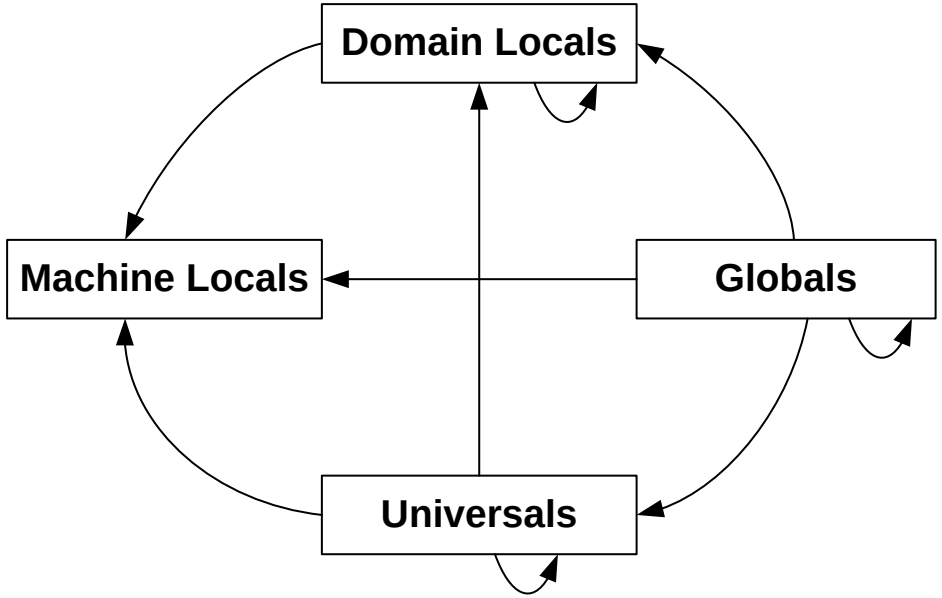
Định nghĩa tài khoản người dùng và tài khoản nhóm (t.t)

➢ Tài khoản nhóm

- **Nhóm bảo mật (Security group)**
  - Nhóm bảo mật được dùng để cấp phát các quyền hệ thống (rights) và quyền truy cập (permission).
  - Mỗi nhóm bảo mật có một SID riêng.
  - Có 4 loại nhóm bảo mật: local (nhóm cục bộ), domain local (nhóm cục bộ miền), global (nhóm toàn cục hay nhóm toàn mạng) và universal (nhóm phổ quát).
- **Nhóm phân phối (distribution group).**
  - Nhóm phân phối là nhóm phi bảo mật, không có SID và không xuất hiện trong ACL (Access Control List).

Tài khoản nhóm (t.t)

- **Qui tắt gia nhập nhóm**
  - Tất cả các nhóm Domain local, Global, Universal đều có thể đặt vào trong nhóm Machine Local.
  - Tất cả các nhóm Domain local, Global, Universal đều có thể dặt vào trong chính loại nhóm của mình.
  - Nhóm Global và Universal có thể đặt vào trong nhóm Domain local.
  - Nhóm Global có thể đặt vào trong nhóm Universal.



Chứng thực và kiểm soát truy cập

➢ Các giao thức chứng thực

- Quy trình chứng thực: đăng nhập tương tác và chứng thực mạng.
- Kerberos V5: là giao thức chuẩn Internet dùng để chứng thực người dùng và hệ thống.
- NT LAN Manager (NTLM): là giao thức chứng thực chính của Windows NT.
- Secure Socket Layer/Transport Layer Security (SSL/TLS): là cơ chế chứng thực chính được dùng khi truy cập vào máy phục vụ Web an toàn.

Chứng thực và kiểm soát truy cập (t.t)

- **Kiểm soát truy cập của đối tượng**
  - Người dùng, nhóm, máy tính, các tài nguyên mạng đều được định nghĩa dưới dang các đối tượng.
  - Kiểm soát truy cập dựa vào bộ mô tả đối tượng ACE (Access Control Entry)
  - Một ACL (Access Control List) chứa nhiều ACE, nó là danh sách tất cả người dùng và nhóm có quyền truy cập đến đối tượng.
- **Số nhận diện bảo mật SID (Security Identifier)**
  - SID có dạng chuẩn “S-1-5-21-D1-D2-D3-RID”

Các tài khoản tạo sẵn

- **Các tài khoản người dùng tạo sẵn**
  - **Administrator**
  - **Guest**
  - **ILS_Anonymous_User**
  - **IUSR_computer-name**
  - **IWAM_computer-name**
  - **Krbtgt**
  - **TSInternetUser**

Các tài khoản tạo sẵn (t.t)

- **Tài khoản nhóm Domain Local tạo sẵn**
  - Administrators
  - Account Operators
  - Domain Controllers
  - Backup Operators
  - Guests
  - Print Operator
  - Server Operators
  - Users
  - Replicator
  - Incoming Forest Trust Builders
  - Network Configuration Operators
  - Pre-Windows 2000 Compatible Access
  - Remote Desktop User
  - Performace Log Users
  - Performace Monitor Users

Các tài khoản tạo sẵn (t.t)

- **Tài khoản nhóm Global tạo sẵn**
  - **Domain Admins**
  - **Domain Users**
  - **Group Policy Creator Owners**
  - **Enterprise Admins**
  - **Schema Admins**

Các tài khoản tạo sẵn (t.t)

- **Các nhóm tạo sẵn đặc biệt**
  - Interactive
  - Network
  - Everyone
  - System
  - Creator owner
  - Authenticated users
  - Anonymous logon
  - Service
  - Dialup

Quản lý tài khoản người dùng và nhóm cục bộ

- **Công cụ quản lý tài khoản người dùng cục bộ**
  - **Dùng công cụ Local Users and Groups**
  - **Có 2 phương thức truy cập đến công cụ Local Users and Groups**
    - **Dùng như một MMC (Microsoft Management Console) snap-in.**
    - **Dùng thông qua công cụ Computer Management**
  - **Các bước chèn Local Local Users and Groups snap-in vào trong MMC. (Thực hành)**

Quản lý tài khoản người dùng và nhóm cục bộ (t.t)

- **Quản lý tài khoản người dùng cục bộ**
  - Tạo tài khoản mới
  - Xoá tài khoản
  - Khoá tài khoản
  - Đổi tên tài khoản
  - Thay đổi mật khẩu
- **Quản lý tài khoản nhóm cục bộ**
  - Tạo tài khoản nhóm
  - Xoá tài khoản nhóm
  - Thêm người dùng vào nhóm

Quản lý tài khoản người dùng và nhóm trên Active Directory

- **Công cụ quản lý tài khoản người dùng trên Active Directory**
  - Công cụ Active Directory User and Computer
  - Truy xuất công cụ Active Directory User and Computer thông qua MMC
- **Quản lý tài khoản người dùng**
  - Tạo tài khoản mới
  - Xoá tài khoản
  - Khoá tài khoản
  - Đổi tên tài khoản
  - Thay đổi mật khẩu

Quản lý tài khoản người dùng và nhóm trên Active Directory

- **Quản lý tài khoản nhóm trên Active Directory**
  - Tạo tài khoản nhóm
  - Xoá tài khoản nhóm
  - Thêm người dùng vào nhóm
  - Gia nhập nhóm vào nhóm

Quản lý tài khoản người dùng và nhóm trên Active Directory

- **Các thuộc tính của tài khoản người dùng**
  - **Tab General**
  - **Tab Address**
  - **Tab Telephones**
  - **Tab Organization**
  - **Tab Account**
  - **Tab Profile**
  - **Tab Member of**
  - **Tab Dial-in**

Quản lý tài khoản người dùng và nhóm trên Active Directory

➢ Các tùy chọn liên quan đến tài khoản người dùng

User must change password at next logon	Người dùng phải thay đổi mật khẩu lần đăng nhập kế tiếp, sau đó mục này sẽ tự động bỏ chọn
User cannot change password	Nếu được chọn thì ngăn không cho người dùng tùy ý thay đổi mật khẩu.
Password never expires	Nếu được chọn thì mật khẩu của tài khoản này không bao giờ hết hạn.
Store password using reversible encryption	Chỉ áp dụng tùy chọn này đối với người dùng đăng nhập từ các máy Apple.
Account is disabled	Nếu được chọn thì tài khoản này tạm thời bị khóa, không sử dụng được.
Smart card is required for interactive login	Tùy chọn này được dùng khi người dùng đăng nhập vào mạng thông qua một thẻ thông minh (smart card), lúc đó người dùng không nhập username và password mà chỉ cần nhập vào một số PIN.

Quản lý tài khoản người dùng và nhóm trên Active Directory

- **Các tùy chọn liên quan đến tài khoản người dùng**

Account is trusted for delegation	Chỉ áp dụng cho các tài khoản dịch vụ nào cần giành được quyền truy cập vào tài nguyên với vai trò những tài khoản người dùng khác.
Account is sensitive and cannot be delegated	Dùng tùy chọn này trên một tài khoản khách vãng lai hoặc tạm để đảm bảo rằng tài khoản đó sẽ không được đại diện bởi một tài khoản khác.
Use DES encryption types for this account.	Nếu được chọn thì hệ thống sẽ hỗ trợ Data Encryption Standard (DES) với nhiều mức độ khác nhau.
Do not require Kerberos preauthentication	Nếu được chọn hệ thống sẽ cho phép tài khoản này dùng một kiểu thực hiện giao thức Kerberos khác với kiểu của Windows Server 2003 trở lên.

Quản lý tài khoản người dùng và tài khoản nhóm

- **Quản lý tài khoản người dùng và tài khoản nhóm bằng dòng lệnh**
  - **Lệnh net user: tạo thêm, hiệu chỉnh và hiển thị thông tin của các tài khoản người dùng.**
  - **Cú pháp:**
    - **net user [username [password | *] [options]] [/domain]**
    - **net user username {password | *} /add [options] [/domain]**
    - **net user username [/delete] [/domain]**

Quản lý tài khoản người dùng và tài khoản nhóm (t.t)

- **Quản lý tài khoản người dùng và tài khoản nhóm bằng dòng lệnh (t.t)**
  - **Lệnh net group: tạo mới thêm, hiển thị hoặc hiệu chỉnh nhóm toàn cục.**
  - **Cú pháp:**
    - **net group [groupname [/comment:"text"]] [/domain]**
    - **net group groupname {/add [/comment:"text"] | /delete} [/domain]**
    - **net group groupname username[...] {/add | /delete} [/domain]**

Quản lý tài khoản người dùng và tài khoản nhóm (t.t)

- **Quản lý tài khoản người dùng và tài khoản nhóm bằng dòng lệnh (t.t)**
  - **Lệnh net localgroup: thêm, hiển thị hoặc hiệu chỉnh nhóm cục bộ.**
  - **Cú pháp:**
    - **net localgroup [groupname [/comment:"text"]] [/domain]**
    - **net localgroup groupname {/add [/comment:"text"] | /delete} [/domain]**
    - **net localgroup groupname name [...] {/add | /delete} [/domain]**

Quản lý tài khoản người dùng và tài khoản nhóm (t.t)

- **Quản lý tài khoản người dùng và tài khoản nhóm bằng dòng lệnh (t.t)**
  - **Lệnh dsadd user, dsmod user: tạo mới, chỉnh sửa tài khoản người dùng.**
  - **Các ví dụ:**
    - dsmod user "CN=Don Funk,CN=Users,DC=Microsoft, DC=Com" -pwd A1b2C3d4 -mustchpwd yes
    - dsmod user "CN=Don Funk,CN=Users,DC=Microsoft, DC=Com" "CN=Denise Smith,CN=Users,DC=Microsoft, DC=Com" -pwd A1b2C3d4 -mustchpwd yes
    - dsmod user "CN=Don Funk,CN=Users,DC=Microsoft, DC=Com" "CN=Denise Smith,CN=Users,DC=Microsoft, DC=Com" -disabled yes
    - dsmod user "CN=Don Funk,CN=Users,DC=Microsoft, DC=Com" -pwd A1b2C3d4 -mustchpwd yes

Lab 2 - Xây dựng OU

- Tạo và cấu hình tài khoản trên Domain Controller
- Tạo OU, Group, User và cấu hình ủy quyền quản trị OU

Lab 3 - LÀM VIỆC CÙNG POWERSHELL

- Tạo OU, tài khoản người dùng và nhóm thông qua PowerShell
- Sử dụng Powershell Script để tạo tài khoản người dùng với số lượng lớn

Hỏi và đáp