

## QUẢN TRỊ MẠNG

### Chương 2

#### MÔI TRƯỜNG

#### WINDOWS SERVER 2008

#### Nội dung chương 2

1. Giới thiệu Windows Server 2008
2. Quản lý user và group
3. Chính sách nhóm – Group policy
4. Giới thiệu về an toàn trên Windows 2008 Server

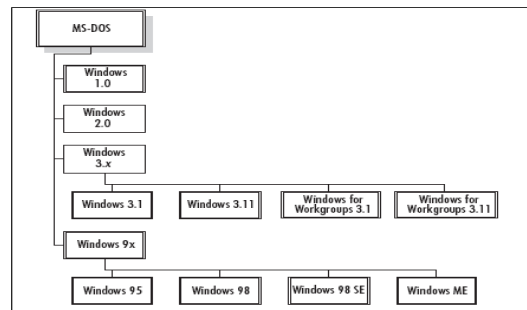
53

#### 1. Giới thiệu Windows 2008 Server

- a. Các hệ điều hành Windows
- b. Các phiên bản Windows Server 2008
- c. Các khái niệm cơ bản trên Windows Servers
- d. Cài đặt Windows Server 2008

54

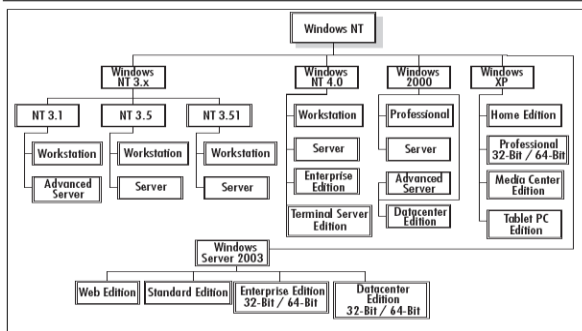
#### a. Các hệ điều hành Windows



Các hệ điều hành Windows 9x

55

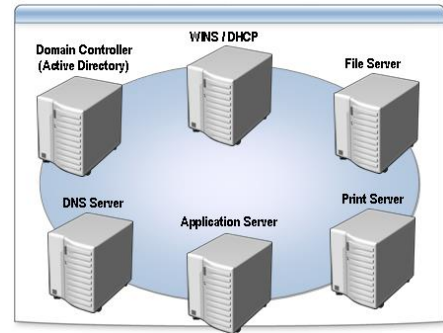
## Các hệ điều hành Windows (tt)



Các hệ điều hành Windows NT

56

## Các dạng server



57

## b. Các phiên bản Windows Server 2008

- Windows Web Server 2008
- Windows Server 2008 Standard
- Windows Server 2008 Standard without Hyper-V
- Windows Server 2008 Enterprise
- Windows Server 2008 Enterprise without Hyper-V
- Windows Server 2008 Datacenter
- Windows Server 2008 Datacenter without Hyper-V
- Windows Server 2008 for Itanium-Based Systems
- Windows HPC Server 2008

58

## Thông số của các phiên bản Windows 2008

- Windows Web Server: 4 processors, 4 GB RAM in 32-bit edition and 32GB of RAM in 64-bit edition, limited services, 32-bit or 64-bit editions, no Hyper-V role available
- Windows Server 2008 Standard: 4 processors, 4 GB RAM in 32-bit edition and 32GB of RAM in 64-bit edition, no clustering, 32-bit or 64-bit editions, Hyper-V role available
- Windows Server 2008 Enterprise: 8 processors, 64 GB RAM in 32-bit edition and 2 TB of RAM in 64-bit edition, 32-bit or 64-bit editions, Hyper-V role available
- Windows Server 2008 Datacenter: 64 processors, 64 GB RAM in 32-bit edition and 2 TB of RAM in 64-bit edition, 32-bit or 64-bit editions, Hyper-V role available

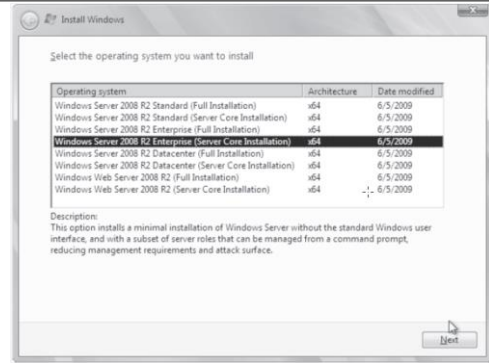
59

## Thông số của các phiên bản Windows 2008 (tt)

- Windows Server 2008 for Itanium-Based Systems: 64 processors, 2 TB RAM , 64-bit only, no Hyper-V role available
- Windows Server 2008 Standard without Hyper-V: 4 processors, 4 GB RAM in 32-bit edition and 32 GB of RAM in 64-bit edition, no clustering, 32-bit or 64-bit editions
- Windows Server 2008 Enterprise without Hyper-V: 8 processors, 64 GB RAM in 32-bit edition and 2 TB of RAM in 64-bit edition, 32-bit or 64-bit editions
- Windows Server 2008 Datacenter without Hyper-V: 64 processors, 64 GB RAM in 32-bit edition and 2 TB of RAM in 64-bit edition, 32-bit or 64-bit editions

60

## Các phiên bản Windows Server 2008 R2



61

## Dạng cài đặt Windows 2008 Server Core

Các ưu điểm:

- Giảm chi phí bảo trì
- Giảm rủi ro bị tấn công
- Giảm các thao tác quản trị
- Sử dụng ít dung lượng đĩa

Có thể quản lý:

- Địa phương hay từ xa dùng command prompt
- Từ xa dùng MMC
- Từ xa dùng Terminal Server hay Remote Shell

62

## c. Một số khái niệm trên Windows Servers

- Client-Server networking
  - Nối mạng dạng client-server
- Vai trò (role), Đặc trưng (feature)
- Domain
- Active Directory
- Log on, authentication
  - Đăng nhập, xác thực
- Các dạng bản quyền

63

## Client-Server

- Tài nguyên tập trung
  - Centralized control / sharing
- Xác thực tập trung
  - Single logon
- Quản trị tập trung
- So sánh với mạng ngang hàng (peer-to-peer / workgroup)  
→ thông tin không quản lý tập trung

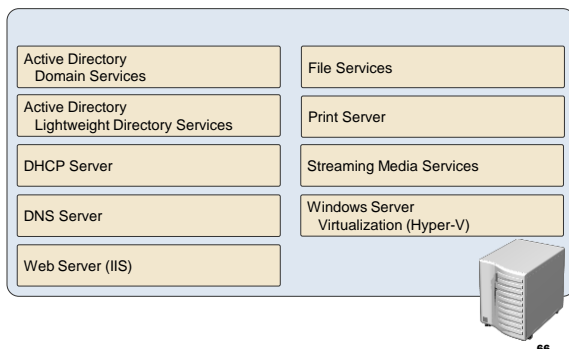
64

## Vai trò (role)

- Server role mô tả một chức năng cơ sở của server
- Mỗi role có thể bao gồm một hay nhiều role services
- Server manager là công cụ dùng để cài đặt, cấu hình, gỡ bỏ các role

65

## Ví dụ: các roles trên Server Core



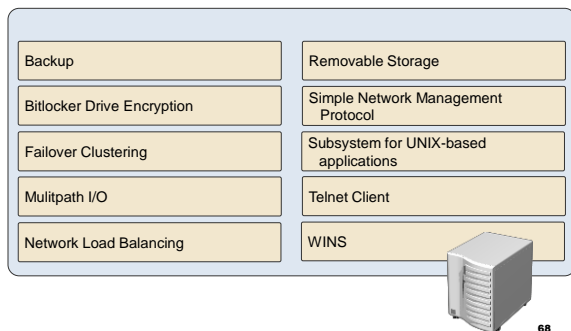
66

## Đặc trưng (feature)

- Server feature cung cấp các chức năng hỗ trợ cho server
- Người quản trị cài đặt thêm các feature không phải là chức năng cơ bản của server nhưng sẽ gia tăng chức năng các role đã cài đặt
- Server manager là công cụ dùng để cài đặt, cấu hình, quản lý các feature

67

## Các features được Server Core hỗ trợ



68

## Domain

- Domain: tập hợp các máy tính nối mạng được quản lý tập trung (trên domain controller)
- Windows 2000/2003/2008 lưu trữ dữ liệu của domain theo Active Directory

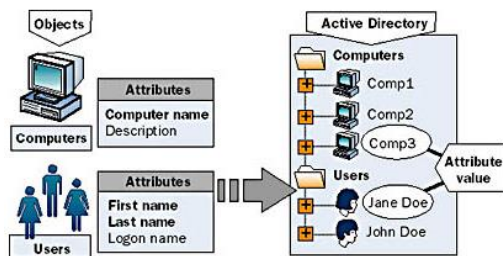
69

## Active Directory

- Active Directory là tổ chức có thứ bậc lưu trữ và quản lý thông tin về tài nguyên trên mạng Windows 2000/2003/2008
- Theo tiêu chuẩn directory service X.500
- Các tính chất:
  - Bảo mật
  - Có khả năng mở rộng
  - Dùng với DNS

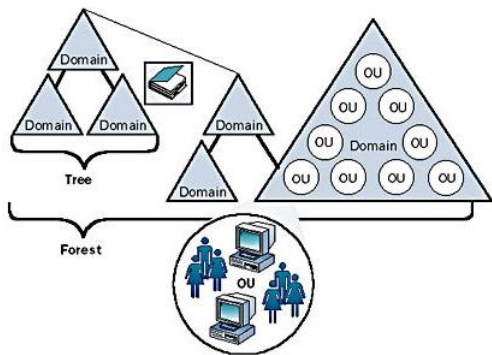
70

## Objects, Attributes trên Active Directory



71

## Cấu trúc luận lý Active Directory



72

## Cấu trúc luận lý Active Directory (tt)

- Domain: các máy tính với các tài nguyên được quản lý tập trung
- Objects: user accounts, groups, printers, ..
- Organization Unit (OU): nhóm luận lý các tài nguyên
- Tree: nhóm thứ bậc các domain
- Forest: nhóm các tree

73

## Log on, authentication

- Logon – đăng nhập
- Authentication
  - Xác thực / Chứng thực
  - Kiểm tra danh hiệu (identity)
- User/Computer cần được xác thực trước khi truy xuất tài nguyên mạng
- Các dạng đăng nhập:
  - Local logon
  - Domain logon

74

## Các dạng bản quyền

- CAL – Client Access License
  - Giấy phép cho phép máy trạm truy nhập vào máy chủ, ví dụ Windows Server 2008
- Per Server
  - Cấp phép cho server
  - Cần cho mỗi kết nối đến server
- Per Device / Per User (Per Seat)
  - Cấp phép cho user hay computer
  - Mỗi user có thể kết nối đến nhiều server
- Ví dụ

75

#### d. Cài đặt Windows Server 2008

- Chuẩn bị cài đặt
- Các dạng cài đặt

76

#### Chuẩn bị cài đặt

- Yêu cầu về phần cứng
- Tạo tài liệu hệ thống

77

#### Yêu cầu về phần cứng

- Yêu cầu phần cứng  
Hardware Requirements
- Tương thích phần cứng  
Hardware Compatibility List (HCL)

78

#### Yêu cầu về phần cứng

Component	Requirement
Processor	<ul style="list-style-type: none"><li>• Minimum: 1 Ghz</li><li>• Recommended: 2 Ghz</li><li>• Optimal: 3 Ghz or faster</li></ul>
Memory	<ul style="list-style-type: none"><li>• Minimum: 512 MB RAM</li><li>• Recommended: 1 GB RAM</li><li>• Optimal: 2 GB RAM (Full) or 1 GB RAM (Server Core) or more</li><li>• Maximum (32-bit): 4 GB (Standard) or 64 GB (Enterprise and Datacenter)</li><li>• Maximum (64-bit): 32 GB (Standard) or 2 TB (Enterprise, Datacenter, and Itanium-based systems)</li></ul>
Available Disk Space	<ul style="list-style-type: none"><li>• Minimum: 8 GB</li><li>• Recommended: 40 GB (Full); 10 GB (Core)</li><li>• Optimal: 80 GB (Full); 40 GB (Core)</li></ul>
Optical Drive	<ul style="list-style-type: none"><li>• DVD-ROM</li></ul>
Display and Peripherals	<ul style="list-style-type: none"><li>• Super VGA (800 x 600) or higher-resolution monitor</li><li>• Keyboard</li><li>• Microsoft mouse or compatible pointing device</li></ul>

## Tạo tài liệu hệ thống

- Tài liệu phần cứng
- Tài liệu mạng
- Tài liệu phần mềm

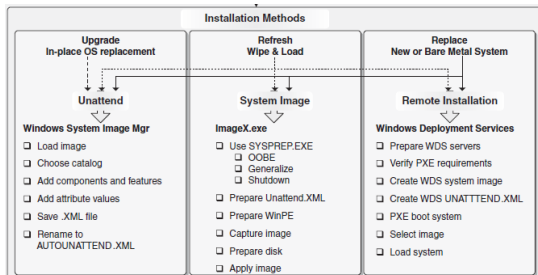
80

## Các dạng cài đặt

- Upgrades / Clean Installation
- Cài đặt từ đĩa DVD khởi động được
- Cài đặt tự động
  - Unattended – cần file unattend.xml
  - Dùng công cụ System Preparation
  - Cài qua mạng dùng Windows Deployment Services

81

## Ví dụ: áp dụng các dạng cài đặt



82

## 2. Quản lý user và group

- Các khái niệm
- Active directory
- Quản lý user
- Quản lý group

83



#### a. Các khái niệm

- User account
- Group account
- Quản lý việc truy xuất tài nguyên

84

#### User account

- Dùng để user đăng nhập vào máy hay domain
- Dùng như service account
- Công dụng:
  - Authentication – Xác thực
  - Authorization – Cấp quyền  
Được cấp quyền truy xuất tài nguyên
  - Auditing – Kiểm tra  
Theo dõi việc truy xuất tài nguyên

85

#### User account (tt)

##### Local user accounts

- Được tạo và lưu trên mỗi máy
- Dùng cho mạng ngang hàng
- Truy xuất tài nguyên địa phương

##### Domain user accounts

- Được tạo và lưu trên domain controller
- Được quản lý tập trung
- Truy xuất tài nguyên trên domain

86

#### Group account

- Gồm các user accounts
- Không đăng nhập bằng group account
- Cấp quyền truy xuất cho group account sẽ tác động trên các user là thành viên
- Tương tự user account:
  - Local groups
  - Domain groups

87

## Quản lý việc truy xuất tài nguyên

- Mục đích: truy xuất có kiểm soát
- Cấp quyền truy xuất tại tài nguyên
  - Permissions
  - Access Control List
- Cấp quyền truy xuất cho user
  - Rights
  - Security Identifier (SID)
- Xét tài nguyên files và folders
  - NTFS permissions/security
  - Shared folders

88

## NTFS permissions

- NTFS folder permissions
- NTFS file permissions
- Thiết lập NTFS file/folder permissions

89

## NTFS folder permissions

- Read
- Write
- List Folder Contents
- Read & Execute
- Modify
- Full Control

Folder permissions tác động trên các file và subfolders trong folder

90

## NTFS file permissions

- Read
- Write
- Read & Execute
- Modify
- Full Control

91

## Special permissions và standard permissions

Special Permissions		
Traverse Folder/ Execute File	Create Folders/Append Data	Read Permissions
List Folder/ Read Data	Write Attributes	Change Permissions
Read Attributes	Write Extended Attributes	Take Ownership
Read Extended Attributes	Delete Subfolders and Files	Synchronize
Create Files/Write Data	Delete	
Standard Permissions		
Read	List Folder Contents	Modify
Write	Read & Execute	Full Control

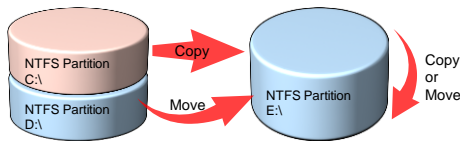
92

## Thiết lập NTFS permissions

- Nên đặt folder permissions, hạn chế sử dụng file permissions
- Nên đặt permissions cho group, hạn chế đặt cho user
- Các bước thực hiện:
  - Right-click folder/file
  - Chọn Sharing and Security
  - Chọn Security Tab
  - Đặt permissions theo yêu cầu cho user/group (deny permission ưu tiên hơn allow permissions)

93

## Sao chép (copy) và di chuyển (move)



- Copy files/folders:
  - kế thừa permissions của thư mục đích
- Move files/folders trong cùng partition:
  - giữ permissions cũ
- Move files/folders đến partition khác:
  - kế thừa permissions của thư mục đích

94

## Shared folders

- Chỉ có tác dụng khi truy xuất từ mạng
- Đặt quyền truy xuất cho folder, không đặt cho file
- Kiểm soát truy xuất cho FAT volume
- Permissions:
  - Read
  - Change
  - Full Control

95

## Shared folder (tt)

- Shared folder permissions dùng kết hợp với NTFS permissions theo nguyên tắc more restrictive  
→ dùng permissions thấp hơn

96

## Ví dụ:

Groups	Share Permissions	NTFS Permissions	Effective Permissions
Everyone	Full Control	Read	Read
Accounting	Read	Modify	Read
Accounting Managers	Change	Full Control	Modify
IT	Full Control	Modify	Modify
Administrators	Full Control	Full Control	Full Control

97

## Thiết lập shared folder

- Tạo folder
- Trong folder properties chọn Sharing
- Thiết lập các permissions theo yêu cầu
- Có thể thiết lập nhiều shared folder cho cùng một folder với các permission khác nhau

98

## Truy xuất shared folder

- Dùng UNC  
(Universal Naming Convention):
  - Ví dụ: \\S50\Home\u11
- Dùng ổ đĩa mạng (mapped drives)
- Dùng các công cụ quản lý file

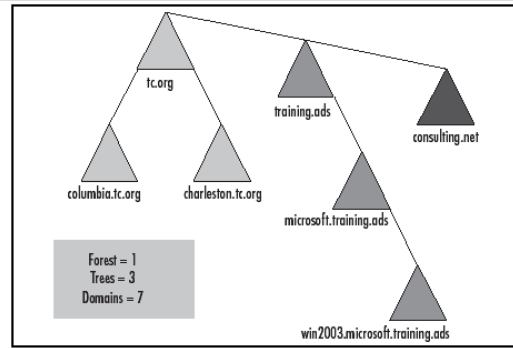
99

## b. Active directory

- Thiết lập mô hình quản trị
- Cài đặt Active Directory
- Các dịch vụ Active Directory

100

## Ví dụ: Cấu trúc Active Directory



## Các bước thiết lập mô hình quản trị

- Xác định không gian tên DNS
  - Tên domain, tên máy
- Tổ chức thứ bậc các đơn vị tổ chức
  - Theo mô hình hoạt động
  - Theo yêu cầu quản trị
- Thiết lập tổ chức vật lý
  - Thiết kế subnets, ...

102

## Thiết lập mô hình quản trị

Các mô hình:

- Forest với nhiều Domain
- Domain với nhiều Domain Controller
- Domain với 1 Domain Controller  
(single-domain)

103

## Cài đặt Active Directory

### ■ Active Directory Installation Wizard:

- Tạo Domain Controller đầu tiên
- Thêm Domain Controller
- Tạo Child Domain
- Tạo Domain Tree

### ■ Thực hiện:

- Run → dcpromo

104

## Cài đặt Active Directory (tt)

### ■ Stand-alone Server → Domain Controller (promoting)

### ■ Domain Controller → Stand-alone Server (demoting)

Chú ý: Dữ liệu Active Directory phải ở trên NTFS volume

105

## Các dịch vụ Active Directory

### ■ Công cụ:

Active Directory Users and Computers

.....

### ■ Tạo OUs:

- Theo tổ chức hoạt động
- Theo yêu cầu quản trị

### ■ Tạo các objects:

- Users, Groups,
- Computers, Printers, Shared Folders, ...

106

## c. Quản lý users

### ■ Local user accounts

### ■ Domain user accounts

107

## Local user accounts

- Công cụ:
  - Computer Management Console/
    - Local Users and Groups
- Các bước thực hiện:
  - Tạo user account
  - Thiết lập các tính chất (properties)

108

## Built-in local user accounts

- Được tạo tự động
- Các users:
  - Administrator: có toàn quyền
  - Guest: dùng cho user không thường xuyên đăng nhập vào mạng
  - ...

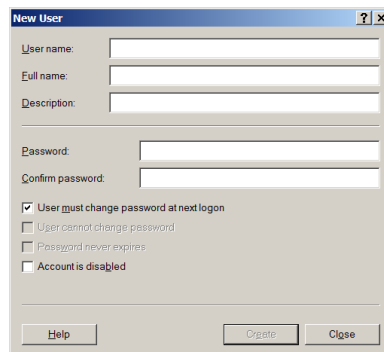
109

## Tạo local user

- Right click trên ô user (users pane)
  - chọn New user
- Đặt các thông số:
  - User name
  - Password
  - ...

110

## Tạo local user



The screenshot shows the 'New User' dialog box. It contains the following elements:

- User name:** A text input field.
- Full name:** A text input field.
- Description:** A text input field.
- Password:** A text input field.
- Confirm password:** A text input field.
- Checkboxes:**
  - ☒ User must change password at next logon
  - ☐ User cannot change password
  - ☐ Password never expires
  - ☐ Account is disabled
- Buttons:** 'Help', 'Create', and 'Close' at the bottom.

111

## Thiết lập các tính chất của local user

Các tính chất chính:

- Member of: chọn nhóm cho user làm thành viên
- User profile: các thông tin về home folder, logon script, ...

Các tính chất khác:

- Environment, Terminal Services Profile, ...

112

## Domain user accounts

■ Công cụ:

Active Directory Users and Computers

■ Các bước thực hiện:

- Tạo user account
- Thiết lập các tính chất (properties)

113

## Built-in domain user accounts

- Được tạo tự động
- Các users: (trong Users container)
  - Administrator: có toàn quyền
  - Guest: dùng cho user không thường xuyên đăng nhập vào mạng
  - ...

114

## Tạo domain user

- Right click trên ô user (users pane)  
→ chọn New → chọn User
- Đặt các thông số:
  - User name
  - Password
  - ...

115



## Thiết lập các tính chất của domain user

Các tính chất chính:

- Member of: chọn nhóm cho user làm thành viên
- User profile: các thông tin về home folder, user profile, logon script, ...

Các tính chất khác:

- Environment, Terminal Services Profile, Address, Telephones...

116

## Home Folders

- Lưu thông tin cá nhân của user
- Là thư mục mặc định của một số phần mềm
- Có thể tạo trên máy Client hay tạo tập trung tại server

Ưu điểm khi tạo trên Server:

- User có thể truy xuất từ máy Client bất kỳ
- Quản lý tập trung → dễ lưu trữ, quản lý

117

## Tạo Home Folders trên server

- Tạo và chia sẻ một thư mục lưu tất cả home folders trên server
- Gán thuộc tính (NTFS):
  - Administrators: Full control
- Gán thuộc tính (shared):
  - Domain users: Full Control
- Cung cấp đường dẫn trong Profile Tab dùng UNC name

Ví dụ: Users là share\_name

\\server\_name\Users\%username%

118

## Offline Files

- Cho phép truy cập tài nguyên trên mạng ở thời điểm mạng không hoạt động hoặc tài nguyên không khả dụng
- Cho phép chọn các tập tin hay các thư mục nào muốn khả dụng khi offline
- Tạo file nội bộ trên máy tính gọi là các offline file có thể được truy cập mọi lúc

119

## Offline Files

- Tác dụng khi user phải di chuyển ở nhiều địa điểm và nhiều mạng khác nhau
- Kết nối đến mạng khác nhau xử lý offline nội dung cho các tập tin công việc
- Chỉnh sửa các tập tin công việc và đồng bộ chúng trở lại khi có kết nối lại

120

## User Profile

- User profile tạo và duy trì tình trạng desktop (desktop settings) của từng user
- User profile có thể được lưu trên server, được dùng từ các máy client
- Có thể tạo user profile dùng cho nhiều user
- Có thể không cho phép user thay đổi tình trạng desktop

121

## Các dạng user profile

- Local profile
  - Lưu trên đĩa địa phương
  - Cho phép thay đổi
- Roaming profile
  - Lưu trên server
  - Cho phép user cập nhật các thay đổi
- Mandatory profile
  - Lưu trên server
  - Chỉ có administrator có thể thay đổi

122

## Thiết lập roaming profile

- Tạo và chia sẻ một thư mục lưu tất cả profile trên server
- Gán thuộc tính (NTFS):
  - Domain users: Modified
- Gán thuộc tính (shared):
  - Domain users: Full Control
- Cung cấp đường dẫn trong Profile Tab dùng UNC name  
Ví dụ: Profiles là share\_name  
\\server\_name\Profiles\%username%

123

#### d. Quản lý groups

- Các loại group
- Phạm vi tác dụng của group
- Tạo group
- Các nguyên tắc tạo group trên domain

124

#### Các loại group

- Distribution groups
  - Dùng phân bổ thông điệp
  - Không dùng để cấp quyền truy xuất tài nguyên
- Security group
  - Dùng để cấp quyền truy xuất tài nguyên

125

#### Phạm vi tác dụng của group

- Local groups
  - Quản lý quyền truy xuất tài nguyên địa phương
  - Sử dụng trong môi trường không có domain
- Domain local groups
  - Gồm các users/groups trong các domain
  - Có quyền truy xuất trong domain

126

#### Phạm vi tác dụng của group (tt)

- Global groups
  - Gồm các users/group trong domain
  - Có quyền truy xuất trong domain
- Universal groups
  - Gồm các users/group trong các domain
  - Có quyền truy xuất trong các domain, tree, forest

127

## Tạo group

Công cụ:

- Local groups  
Computer Management Console/  
Local Users and Groups
- Domain groups  
Active Directory Users and Computers

Các bước thực hiện:

- Đặt tên
- Chọn phạm vi (đối với domain groups)

128

## Tạo group (tt)

Thêm thành viên vào group

- Dùng Group properties
  - Chọn Tab Member
- Chọn group để làm thành viên
- Dùng User properties
  - Chọn Tab Member of

129

## Các group mặc định

- Built-in Local Group  
Administrators, Guests, Users, Power Users
- Predefined Global Group  
Domain Admins, Domain Users, ...
- Built-in Domain Local Group  
Administrators, Users, Print Operators
- Special Identity Group  
Everyone, CREATOR OWNER

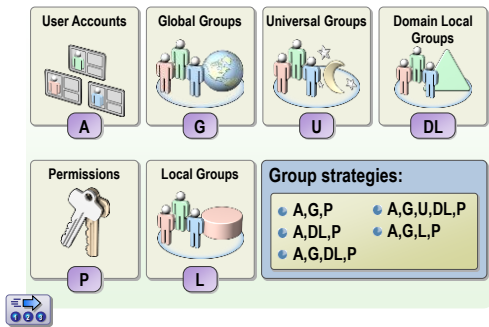
130

## Các nguyên tắc tạo group trên 1 domain

- Thêm users vào group với quyền tối thiểu
- Hạn chế thành viên administrators group
- Hạn chế cấp quyền cho Everyone, nên dùng Authenticated Users
- Tận dụng các built-in groups

131

## Một số dạng tạo group



132

## Ví dụ mô hình tổ chức NTFS volume

- Tạo các nhóm folder:  
Application, Data, Home
- Chỉ cấp các quyền truy xuất tối thiểu
- Tạo các nhóm theo yêu cầu và cấp quyền cho nhóm.  
Chỉ cấp quyền cho user khi thật cần thiết

133

## Ví dụ mô hình tổ chức NTFS volume (tt)

- Data/Application folders:  
Read & Execute đối với Users và Administrators
- Public Data folders:
  - Read&Execute và Write cho Users group
  - Full Control đối với CREATOR OWNER.

134

## 3. Chính sách nhóm – Group Policy

- Khái niệm
- Các bước thực hiện
- Ví dụ

135

#### a. Khái niệm chính sách nhóm

- Định nghĩa
- Mục đích
- Các loại chính sách nhóm
- Sự thừa kế

136

#### Định nghĩa chính sách nhóm

- Là tập hợp các thông tin cấu hình (configuration settings)
- Tác động trên một hoặc nhiều đối tượng (users, computers) trong Active Directory hoặc trên một hệ thống (local group policy)
- Chỉ áp dụng cho các hệ thống từ Windows 2000

137

#### Các thông tin cấu hình

- Chính sách nhóm cho computers
  - Desktop
  - Security
  - Startup/shutdown scripts
- Chính sách nhóm cho users
  - Desktop
  - Security
  - Logon/logoff scripts



138

#### Types of Uses for Group Policy

Administrative Templates	Registry-based Group Policy settings
Security	Settings for local, domain, and network security
Software Installation	Settings for central management of software installation
Scripts	Startup, shutdown, logon, and logoff scripts
Remote Installation Services	Settings that control the options available to users when running the Client Installation Wizard used by RIS
Internet Explorer Maintenance	Settings to administer and customize Microsoft Internet Explorer on Windows 2000-based computers
Folder Redirection	Settings for storing users' folders on a network server

### Mục đích chính sách nhóm

- Quản lý môi trường làm việc của user trong site, domain, organization unit hay trong từng hệ thống
- Đơn giản hóa một số thao tác quản trị
- Quản trị tập trung

140

### Các loại chính sách nhóm

- Các thiết lập chính sách được lưu trên GPO (Group Policy Object, đối tượng chính sách nhóm)
- Có 2 dạng GPO
  - Local GPO: lưu trên từng máy
  - Non local GPO: lưu trên Active Directory

141

### Sự thừa kế chính sách nhóm

- Thứ tự thừa kế chính sách nhóm
  - Local
  - Site
  - Domain
  - Organization Unit
- Các thiết lập có tính tích lũy (cumulative)
- Nếu có xung đột thì không thừa kế
- Có thể cấm sự thừa kế (block inheritance) hay buộc thừa kế (No override)

142

### b. Các bước thực hiện

- Công cụ
- Các GPOs mặc định
- Các bước thực hiện

143

## Công cụ

- Local Group Policy
  - Local Security Policy
- Non-local Group Policy (Domain, Organization Unit GPOs)
  - Group Policy Management

144

## Các GPOs mặc định

Local:

- Local Group Policy trên mỗi máy

Trên Active Directory:

- Default Domain Policy:
  - Liên kết với domain
  - Tác động đến tất cả user và computer trong domain
- Default Domain Controllers Policy:
  - Liên kết với Domain Controllers OU
  - Chỉ tác động trên các domain controllers

145

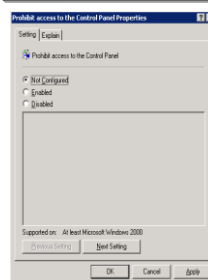
## Các bước thực hiện

- Dùng công cụ phù hợp với local, non-local GPO
- Tạo GPO
- Thiết lập các thông số
- Có thể liên kết (link) một GPO cho nhiều sites, nhiều Domains, hay nhiều Ous
- Có thể liên kết (link) nhiều GPOs cho một site, một Domain, hay một Ou

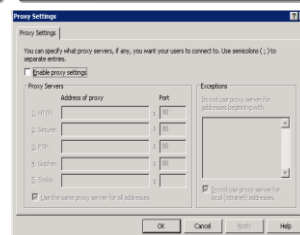
146

## Các tùy chọn thiết lập group policy

### Enable / Disable



### Multi-valued settings



147



### Ví dụ 1: cho phép domain users đăng nhập tại server

- Default Domain Controllers Policy
  - → Right Click → Edit
- Computer Configuration → Policies
- Windows Settings
- Security settings
- Local policies
- User Rights Assignment
  - Allow logon locally → thêm nhóm Domain Users

148

### Ví dụ 2: loại bỏ Run khỏi Start menu và Control Panel khỏi Settings

- Tạo GPO cho OU
  - → Right Click → Edit
- User Configuration → Policies
- Administrative Template
  - Start Menu & Task bar:
    - Remove Run menu from Start Menu: Enabled
  - Control Panel
    - Prohibit access to the Control Panel: Enabled

149

### Ví dụ 3: di chuyển folder My Documents

- Tạo GPO cho OU
  - → Right Click → Edit
- User Configuration → Policies
- Windows Settings
- Folder Redirection
  - My Documents – Properties
  - Settings:
    - Basic – Redirect everyone's folder to the same location
  - Target folder location:
    - Redirect to the user's home folder
  - Settings Tab: chọn Also apply redirection policy to Windows 2000, ...

150

### Ví dụ 4: hạn chế sử dụng phần mềm

- Tạo GPO cho OU
  - → Right Click → Edit
- User Configuration → Policies
- Windows Settings
- Security settings
  - Software Restriction Policies
    - Additional Rules
    - New Path Rule hoặc/và New Hash Rule

151

## Ví dụ 5: cài đặt phần mềm

Có 2 dạng phân phối phần mềm từ group policy

- Assigning Software – Gán phần mềm
  - Gán phần mềm cho users hay computers
  - Phần mềm được cài đặt khi đăng nhập
- Publishing Software – Công bố phần mềm
  - Công bố phần mềm cho users
  - Phần mềm được hiển thị từ hộp thoại Add or Remove Programs
  - User thực hiện cài đặt

152

## Các bước cài đặt phần mềm từ group policy

- Tạo điểm phân phối (Distribution point)
  - Tạo share folder
  - Sao chép hoặc cài đặt phần mềm
  - Dạng \*.MSI
- Tạo Group Policy Object

153

## Các bước cài đặt phần mềm từ group policy (tt)

- Gán phần mềm (Assign a Package)
  - User Configuration
  - Software Settings
  - Software Installation
  - New → Package → Assigned
  - Package được cài đặt khi client computer khởi động

154

## Các bước cài đặt phần mềm từ group policy (tt)

- Công bố phần mềm (Publish a Package)
  - User Configuration
  - Software Settings
  - Software Installation
  - New → Package → Published
  - Package được hiển thị tại:
    - Add or Remove Programs
    - Add New Programs
    - Add programs from your network
  - Package được cài đặt khi chọn Add

155

#### Các bước cài đặt phần mềm từ group policy (tt)

##### ■ Cài lại phần mềm (Redeploy a Package)

- User/Computer Configuration
- Software Settings
- Software Installation
- Chọn package
- All Tasks → Redeploy application

156

#### Các bước cài đặt phần mềm từ group policy (tt)

##### ■ Gỡ bỏ phần mềm (Remove a Package)

- User/Computer Configuration
- Software Settings
- Software Installation
- Chọn package
- All Tasks → Remove
- Chọn một trong các tùy chọn:
  - Immediate uninstall the software from users and computers
  - Allow users to continue to use the software but prevent new installation

157

#### 4. Giới thiệu về an toàn trên Windows 2008

##### ■ User rights

Quyền của user

##### ■ Permissions

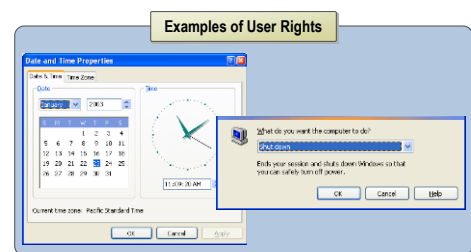
Cấp phép truy xuất tài nguyên

##### ■ Auditing

Kiểm tra

158

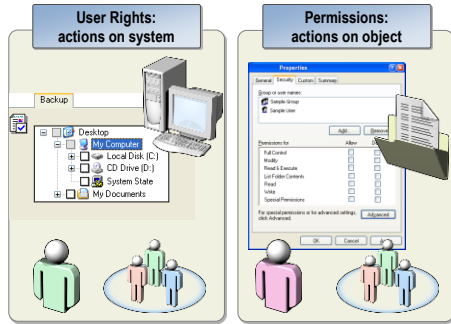
#### User rights



- User rights: quyền thực hiện các thao tác hệ thống

159

## User rights và Permissions



160

## Auditing – Kiểm tra

- Mục đích: theo dõi các hoạt động của hệ điều hành và người sử dụng
- Ghi nhận các biến cố vào nhật ký (log files)
- Người quản trị xem nhật ký từ chức năng Event Viewer

161

## Các dạng biến cố được kiểm tra


Event	Example
Account Logon	An account is authenticated by a security database
Account Management	Administrator creates, changes, or deletes a user account or group
Directory Service Access	User accesses an Active Directory object
Logon	User logs on or off a local computer
Object Access	User accesses a file, folder, or printer
Policy Change	Change is made to the user security options, user rights, or auditing policies
Privilege Use	User exercises a right, such as taking ownership of a file
Process Tracking	Application performs an action
System	User restarts or shuts down the computer

162

## Một số lệnh hệ thống

- dsquery ou domainroot  
Liệt kê các OU
- dsquery computer domainroot  
Liệt kê các computer
- dsquery group domainroot –name g0\*  
liệt kê các nhóm có tên g0\*
- dsquery user domainroot –name u\*  
Liệt kê các domain user có tên u\*

163



## Một số lệnh hệ thống (tt)

---

- `dsquery user domainroot -name u11 | dsget user -memberof -expand`

Liệt kê các group có u11 là thành viên

- `dsquery user domainroot -name u11 | dsget user -dn -hmdir -profile`

Liệt kê đường dẫn home folder, profile của user u11