QUẢN TRỊ HỆ THỐNG VỚI GROUP POLICY TRONG WINDOWS XP – PHẦN I

Trong Windows XP có một công cụ khá hay, đó là Group Policy (GP). Nhiều người sử dụng Windows đã lâu nhưng chưa hề biết có công cụ này vì không tìm thấy nó trong Control Panel, Administrative Tools hay System Tools. GP là một trong các th&agr

Khởi động chương trình: Có 2 cách khởi động chương trình. Cách 1: Vào menu Start > Run, rồi nhập lệnh mmc để khởi động Microsoft Management Console. Sau đó vào trình đơn File, chọn Open. Trong cửa sổ Open, nhấn nút Browse rồi tìm đến thư mục System32. Bạn sẽ thấy nhiều tập tin xuất hiện có phần mở rộng là *.msc. Các tập tin dạng này là những thành phần được tạo bởi Microsoft Management Console. Nếu để ý, bạn sẽ thấy một số công cụ quen thuộc như: Event Viewer (eventvwr.msc), Services (services.msc) (hai công cụ này nằm trong Adminstation Tools)... và còn nhiều nữa. Trong phạm vi của bài viết này, bạn cần chọn gpedit.msc để mở Group Policy.

Cách 2: Nếu bạn làm việc thường xuyên với GP thì cách này sẽ nhanh hơn. Vào menu Start > chọn Run và nhập vào gpedit.msc rồi nhấn OK để khởi động chương trình. Khi chương trình đã khởi động, bạn sẽ thấy cửa sổ giao diện như hình bên dưới:

Chương trình được phân theo dạng cây và rất dễ dùng. Nếu sử dụng các phần mềm như Security Administrator, TuneUp Utilities,... bạn sẽ thấy hầu hết các tùy chọn cấu hình hệ thống đều nằm trong GP. Và bạn hoàn toàn có thể sử dụng GP mà Windows cung cấp sẵn để quản trị hệ thống, không cần phải cài thêm các phần mềm trên. * Cách sử dụng chung: tìm tới các nhánh, Chọn Not configured nếu không định cấu hình cho tính năng đó, Enable để kick hoạt tính năng, Disable để vô hiệu hóa tính năng. * Computer Configuration: Các thay đổi trong phần này sẽ áp dụng cho toàn bộ người dùng trên máy. Trong nhánh này chứa nhiều nhánh con như: + Windows Settings: bạn sẽ cấu hình về việc sử dụng tài khoản, password tài khoản, quản lý việc khởi động và đăng nhập hệ thống... + Administrative Templates: - Windows Components: bạn sẽ cấu hình các thành phần cài đặt trong Windows như: Internet Explorer, NetMeeting... - System: cấu hình về hệ thống. Cần lưu ý là trước khi cấu hình cho bất kỳ thành phần nào, bạn cũng cần phải tìm hiểu thật kỹ về nó. Bạn có thể chọn thành phần rồi nhấp chuột phải để chọn Help.

Còn một cách khác là không chọn Help mà chọn Properties. Khi cửa sổ Properties xuất hiện, chuyển sang thẻ Explain để được giải thích chi tiết về thành phần này.

Mặc định thì tình trạng ban đầu của các thành phần này là "Not configured". Để thay đổi tình trạng cho thành phần nào đó, bạn chọn thẻ Setting trong cửa sổ Properties, sẽ có 3 tùy chọn cho bạn chọn lựa là: Enable (có hiệu lực), Disable (vô hiệu lực) và Not configure (không cấu hình). * User Configuration: giúp bạn cấu hình cho tài khoản đang sử dụng. Các thành phần có khác đôi chút nhưng việc sử dụng và cấu hình cũng tương tự như trên. Phần I: Computer Configuration: Windows Setting: Tại đây bạn có thể tinh chỉnh, áp dụng các chính sách về vấn đề sử dụng tài khoản, password tài khoản, quản lý việc khởi động và đăng nhập hệ thống... + Scripts (Startup/Shutdown): Bạn có thể chỉ định cho windows sẽ chạy một đoạn mã nào đó khi Windows

Startup hoặc Shutdown. + Security settings: Các thiết lập bảo mật cho hệ thống, các thiết lập này được áp dụng cho toàn bộ hệ thống chứ không riêng người sử dụng nào.

Name
Tóm tắt tính năng

Account Policies
Các chính sách áp dụng cho taî khoản cửa ngươi dùng.

Local Policies
Kiểm định như~ ng chính sách, như~ ng tuỳ chọn quyên lợi va`chính sách an toàn cho ngươi dung tại chỗ.

Public Key Policies
Các chính sách khóa dùng chung

Sau đây chúng ta sẽ~ lần lượt đi vaò tìm hiểu chi tiết tưng phần nho cửa no. 1. Account Policies: Thiết lập các chính sách cho tài khoản a> Password Policies: Bao gồm các chính sách liên quan đến mật khẩu tài khoản cửa ngươi sư dụng tài khoản trên máy. Enforce password history: Với những người sử dụng có không có thói quen ghi nhớ nhiều mật khẩu, khi buộc phải thay đổi mật khẩu thì họ vẫn dùng chính mật khẩu cũ để thay cho mật khẩu mới, điều này là một kẽ hở lớn lên quan trực tiếp đến việc lộ mật khẩu. Thiết lập này bắt buộc một mật khẩu mới không được giống bất kỳ một số mật khẩu nào đó do ta quyết định. Có giá trị từ 0 đến 24 mật khẩu. Maximum password age: Thơi gian tôi đa mật khẩu coǹ hiệu lực, sau thời gian này hệ thống sẽ yêu cầu ta thay đổi mật khẩu. Việc thây đổi mật khẩu định kỳ nhằm nâng cao độ an toàn cho tài khoản, vì một kẻ xấu có thể theo dõi những thói quen của bạn, từ đó có thể tìm ra mật khẩu một cách dễ dàng. Số giá trị từ 1 đến 999 ngày. Giá trị mặc định là 42. Minimum password age: Xác định thơi gian tôi thiểu trước khi có thể thay đổi mật khẩu. Hết thời gian này bạn mới có thể thay đổi mật khẩu của tài khoản, hoặc bạn có thể thay đổi ngay lập tức bằng cách thiết lập giá trị là 0. Giá trị từ 0 đến 999 ngày. Bạn cần thiết lập "Minimum password age" lớn hơn không nếu bạn muốn chính sách "Enforce password history" có hiệu quả, vì người sử dụng có thể thiết lập lại mật khẩu nhiều lần theo chu kỳ để họ có thể sử dụng lại mật khẩu cũ. Minimum password length: Độ daî nho tối thiểu cuả mật khẩu taî khoản. (Tính băng số ký tự nhập vaò). Độ dài của mật khẩu có giá trị từ 1 đến 14 ký tự. Thiết lập giá trị là không nếu bạn không sử dụng mật khẩu. Giá trị mặc định là 0. Password must meet complexity requirements: Quyết định độ phức tạp của mật khẩu. Nếu tính năng này có hiệu lực. Mật khẩu của tài khoàn ít nhất phải đạt những yêu cầu sau: - Không chứa tất cả hoặc một phần tên tài khoản người dùng - Độ dài nhỏ nhất là 6 ký tự - Chứa từ 3 hoặc 4

loại ký tự sau: Các chữ cái thường (a -> Z), các chữ cái hoa (A -> Z), Các chữ số (0 -> 9) và các ký tự đặc biệt. Độ phức tạp của mật khẩu được coi là bắt buộc khi tạo mới hoặc thay đổi mật khẩu. đinh : Disable. Store password using reversible encryption for all users in the domain: Lưu trữ mật khẩu sư dụng mã hoá ngược cho tất cả các ngươi sư dụng domain. Tính năngcung cấp sự hỗ trợ cho các ứng dụng sử dụng giao thức,nó yêu cầu sự am hiểu về mật khẩu của người sử dụng. Việc lưu trữ mật khẩu sử dụng phương pháp mã hóa ngươc thực chất giống như việc lưu trữ các văn bản mã hóa của thông tin bảo vệ mật khẩu. Mặc đinh : Disable. b> Acount lockout Policy: * Account lockout duration: Xác định số phút còn sau khi tài khoản được khóa trước khi việc mở khóa đươc thực hiện. Có giá trị từ 0 đến 99.999 phút. Có thể thiết lập giá trị 0 nếu không muốn việc tự động Unlock. Mặc định không có hiệu lực vì chính sách này chỉ có khi chính sách "Account lockout threshold" được thiết lập. * Account lockout threshold: Xác định số lần cố gắng đăng nhập nhưng không thành công. Trong trường hợp này Acount sẽ bị khóa. Việc mở khóa chỉ có thể thực hiện bởi người quản trị hoặc phải đợi đến khi thời hạn khóa hêt hiệu lực. Có thể thiết lập giá trị cho số lần đăng nhập sai từ 1 đến 999. Trong trường hợp thiết lập giá trị 0, account sẽ không bị khóa. * Reset account lockout counter after: Thiết lập lại số lần cố gắng đăng nhập về 0 sau một khoảng thời gian quy định. Thiết lập này chỉ có hiệu lực khi "Account lockout threshold" được thiết lập. 2. Local Policies: Các chính sách cục bộ: User rights Assignment: Ấn định quyên cho ngươi sư dụng. Quyền của người sử dụng ở đây bao gồm các quyền truy cập, quyền backup dữ liệu, thay đổi thời gian của hệ thống… Trong phân nay, để cấu hình cho một mục nao đo bạn co thể nhay đup chuột lên mục đo va nhấn nut Add user or group để trao quyên cho user hoặc Group nao bạn muốn. * Access this computer from the network: Với những kẻ tò mò, tọc mạch thì tại sao chúng ta lại phải cho phép chúng truy cập vào máy tính của mình. Với thiết lập này bạn có thể tuy ý thêm, bớt quyền truy cập vào máy cho bất cứ tài khoản hoặc nhóm nào. * Act as part of the operating system: Chính sách này chỉ định tài khoản nào sẽ được phép hoạt động như một phần của hệ thống. Mặc định, tài khoản Aministrator có quyền cao nhất, có thể thay đổi bất kỳ thiết lập nào của hệ thống, được xác nhận như bất kỳ một người dùng nào, vì thế có thể sử dụng tài nguyên hệ thống như bất kỳ người dùng nào. Chỉ có những dịch vụ chứng thực ở mức thấp mới yêu cầu đặc quyền này. * Add workstations to domain: Thếm một tài khoản hoặc nhóm vào miền. Chính sách này chỉ hoạt động trên hệ thống sử dụng Domain Controller. Khi được thêm vào miền, tài khoàn này sẽ có thêm các quyền hoạt động trên dịch vụ thư mục (Active Directory), có thể truy cập tài nguyên mạng như một thành viên trên Domain. * Adjust memory quotas for a process: Chỉ định những ai được phép điều chỉnh chỉ tiêu bộ nhớ dành cho một quá trình xử lý. Chính sách này tuy có làm tăng hiệu suất của hệ thống nhưng nó có thể bị lạm dụng để phục vụ cho những mục đích xấu như tấn công từ chôi dịch vụ DoS (Dinal of Sevices). * Allow logon through Terminal Services: Terminal Services là một dịch vụ cho phép chúng ta đăng nhập từ xa đến máy tính. Chính sách này sẽ quyết định giúp chúng ta những ai được phép sử dụng dịch vụ Terminal để đăng nhập vào hệ thống. * Back up files and directories: Tương tự như các chính sách trên, ở đây sẽ cấp phép cho những ai sẽ có quyền backup dữ liệu. * Change the system time: Cho phép ngươi sư dụng nao co quyền thay đôi thơi gian cua hệ thống. * Create global objects: Cấp quyền cho những ai có thể tạo ra các đối tượng dùng chung * Force shutdown from a remote system: Cho phép những ai có quyền tắt máy qua hệ thống điều khiển từ xa. * Shut down the system: Cho phép ai có quyền Shutdown máy. Và còn rất nhiều chính sách khác nữa đang chờ bạn khám phá. Nguyễn Quang Duy – IITM Email: quangduy2500@gmail.com