

QUẢN TRỊ CHÍNH SÁCH NHÓM

Nội dung

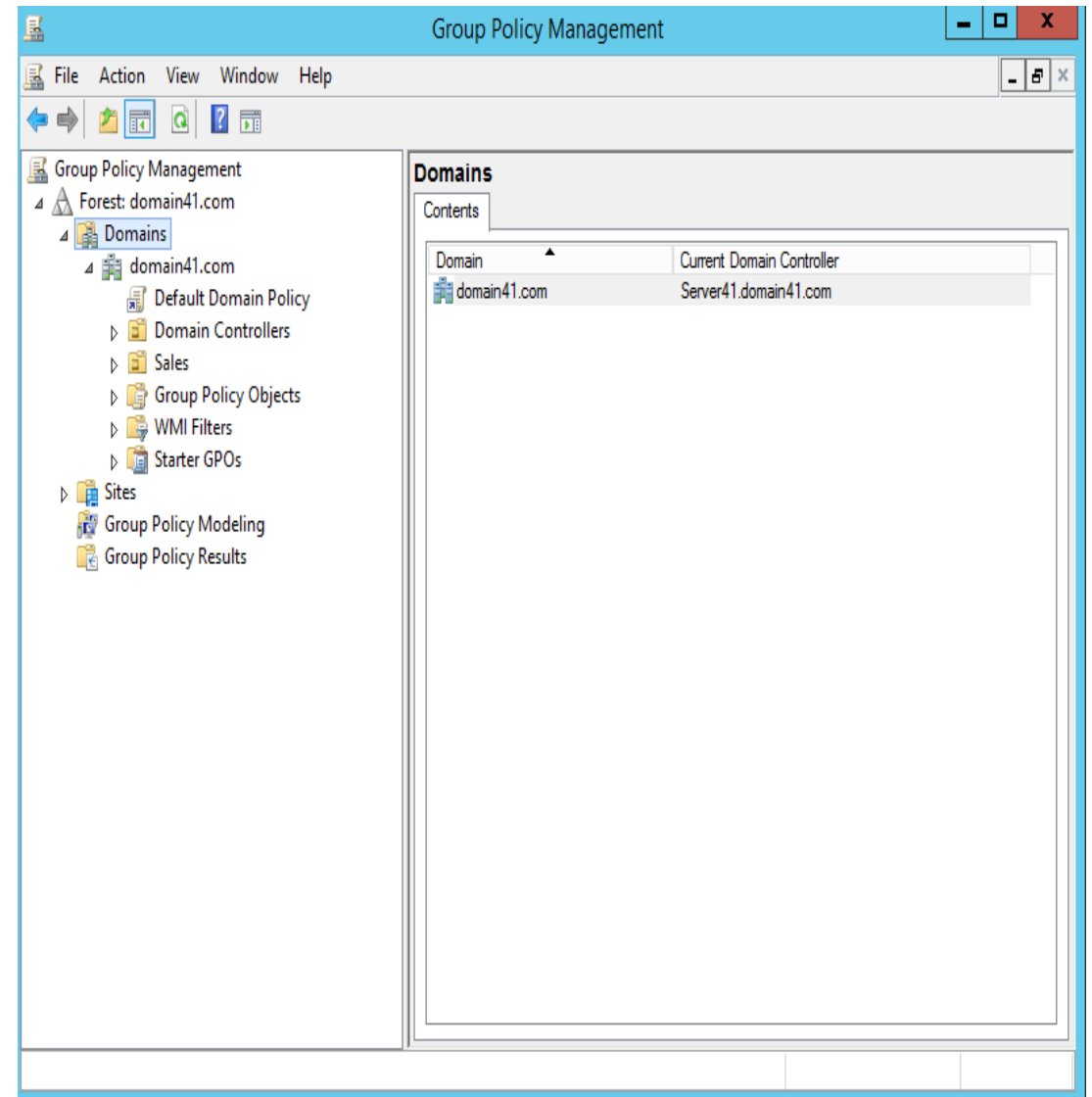
- ❖ Chính sách nhóm là gì?
- ❖ Các thiết lập chính sách nhóm
- ❖ Trình tự xử lý chính sách nhóm
- ❖ Thừa kế chính sách nhóm
- ❖ Backup và Restore GPO

Khái niệm Group Policy (GP) và Group Policy Object (GPO)

❖ GP là những thiết đặt về cấu hình của người dùng và máy tính như:

- ☐ Software Settings
- ☐ Scripts
- ☐ Security Settings
- ☐ Administrative
- ☐ Templates
- ☐ Folder Redirection

❖ GPO là một nhóm các GP được thiết đặt cho computers, sites, domain hay OUs



Chính sách nhóm là gì?

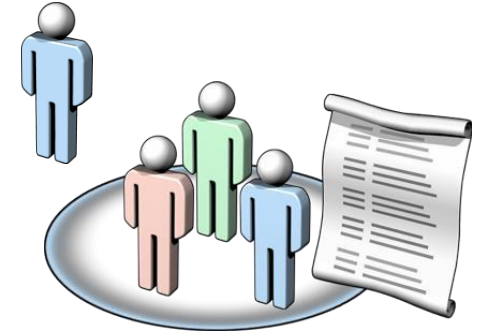
- ❖ Chính sách nhóm cho phép quản trị mạng thực hiện việc quản lý tự động đến các nhóm người dùng và máy tính
- ❖ Sử dụng chính sách nhóm để:
 - ☐ Áp dụng các cấu hình chuẩn
 - ☐ Triển khai phần mềm
 - ☐ Thực thi các thiết lập bảo mật
 - ☐ Thực thi một môi trường làm việc phù hợp

Chính sách nhóm cục bộ (Local Group Policy) luôn có hiệu lực cho các thiết lập người dùng cục bộ - miền và máy tính cục bộ

Các thiết lập chính sách nhóm

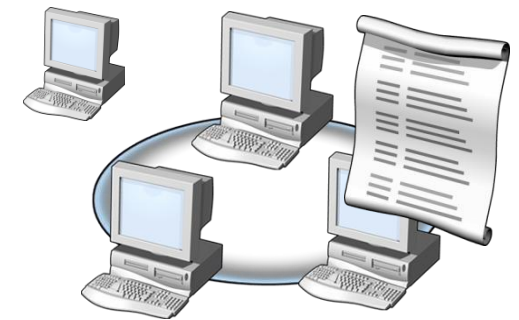
Các thiết lập chính sách
nhóm điều khiển
người dùng:

- Software
- Windows
- Security
- Desktop



Các thiết lập chính sách
nhóm điều khiển
máy tính:

- Software
- Windows
- Security
- Operating systems



Các thiết lập chính sách nhóm

- ❖ Có hai loại thiết lập chính sách nhóm:
 - ❑ Thiết lập cho cấu hình máy tính:
Computer Configuration Settings -> được áp dụng trong quá trình khởi động máy tính
 - ❑ Thiết lập cho cấu hình người dùng:
User Configuration Settings -> được áp dụng sau khi người dùng đăng nhập
- ❖ Các thiết lập cấu hình máy tính và người dùng gồm:
 - ❑ Thiết lập phần mềm: Software settings
 - ❑ Thiết lập Windows: Windows settings
 - ❑ Các khuôn mẫu quản trị: Administrative Templates.

Các loại GPO

- ❖ Máy tính Win2012 có một GPO cục bộ (local GPO) và/hoặc một hoặc nhiều GPO không cục bộ (nonlocal Active Directory-based GPOs).
- ❖ Local GPO:
 - ☐ Lưu trên máy tính, kể cả khi là thành viên của AD DS
 - ☐ Có thể bị ghi đè bởi nonlocal GPO.
- ❖ Nonlocal GPO
 - ☐ Được liên kết tới Sites, Domain, OUs.
 - ☐ Được lưu trên Domain Controller.
- ❖ 02 Nonlocal GPO mặc định trên domain
 - ☐ Default Domain Policy
 - ☐ Default Domain Controllers Policy

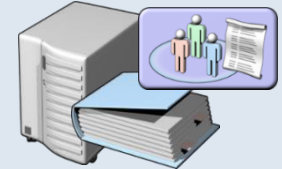
Các thành phần chính sách nhóm

Group Policy Object



- Chứa các thiết lập chính sách nhóm
- Lưu nội dung ở hai địa điểm

Group Policy Container



- Lưu trong AD DS
- Cung cấp thông tin phiên bản

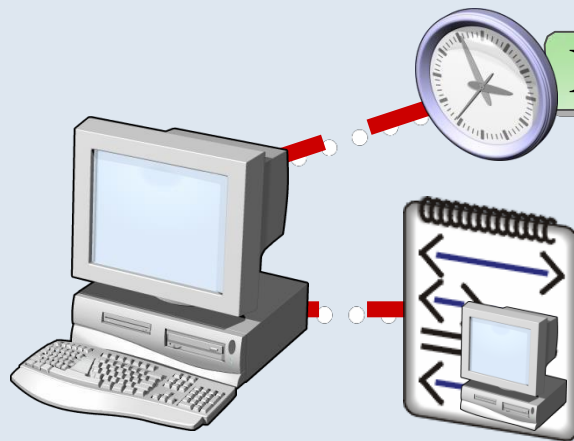
Group Policy Template



- Lưu trong thư mục chia sẻ SYSVOL
- Cung cấp các thiết lập chính sách nhóm
- Hỗ trợ cả mẫu ADM và ADMX

Áp dụng chính sách nhóm

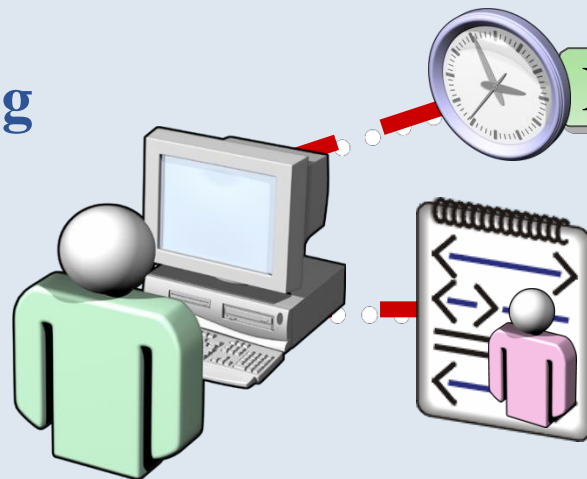
Máy tính khởi động



Refresh interval: Mỗi 90 phút

- Áp dụng các thiết lập máy tính
- Thực thi mã khởi động

Người dùng đăng nhập



Refresh interval : Mỗi 90 phút

- Áp dụng các thiết lập người dùng
- Thực thi mã đăng nhập

Tập tin ADM và ADMX là gì?

❖ Tập tin ADM là:

- ☐ Sao chép vào mỗi GPO trong SYSVOL
- ☐ Tùy chỉnh rất khó khăn

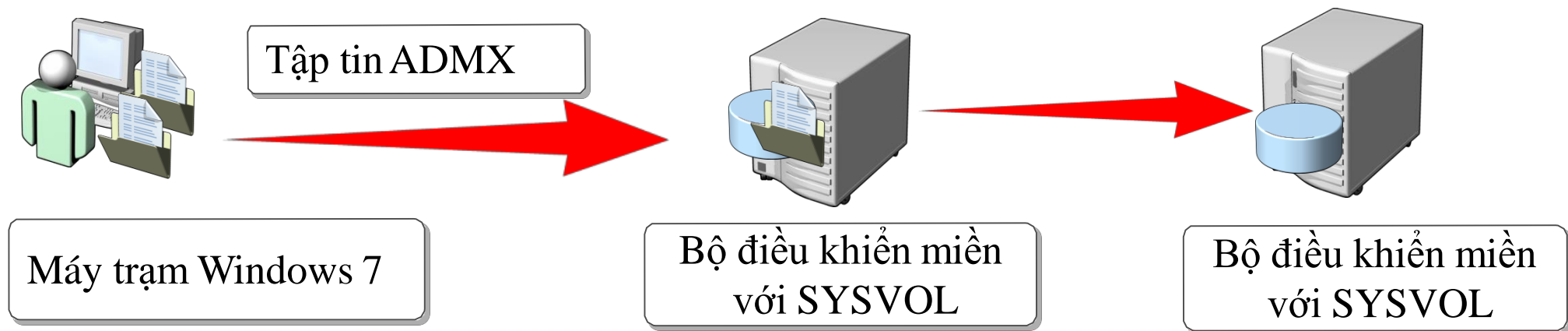
❖ Tập tin ADMX là:

- ☐ Ngôn ngữ trung tính
- ☐ Không được lưu trữ trong các GPO
- ☐ Mở rộng thông qua XML

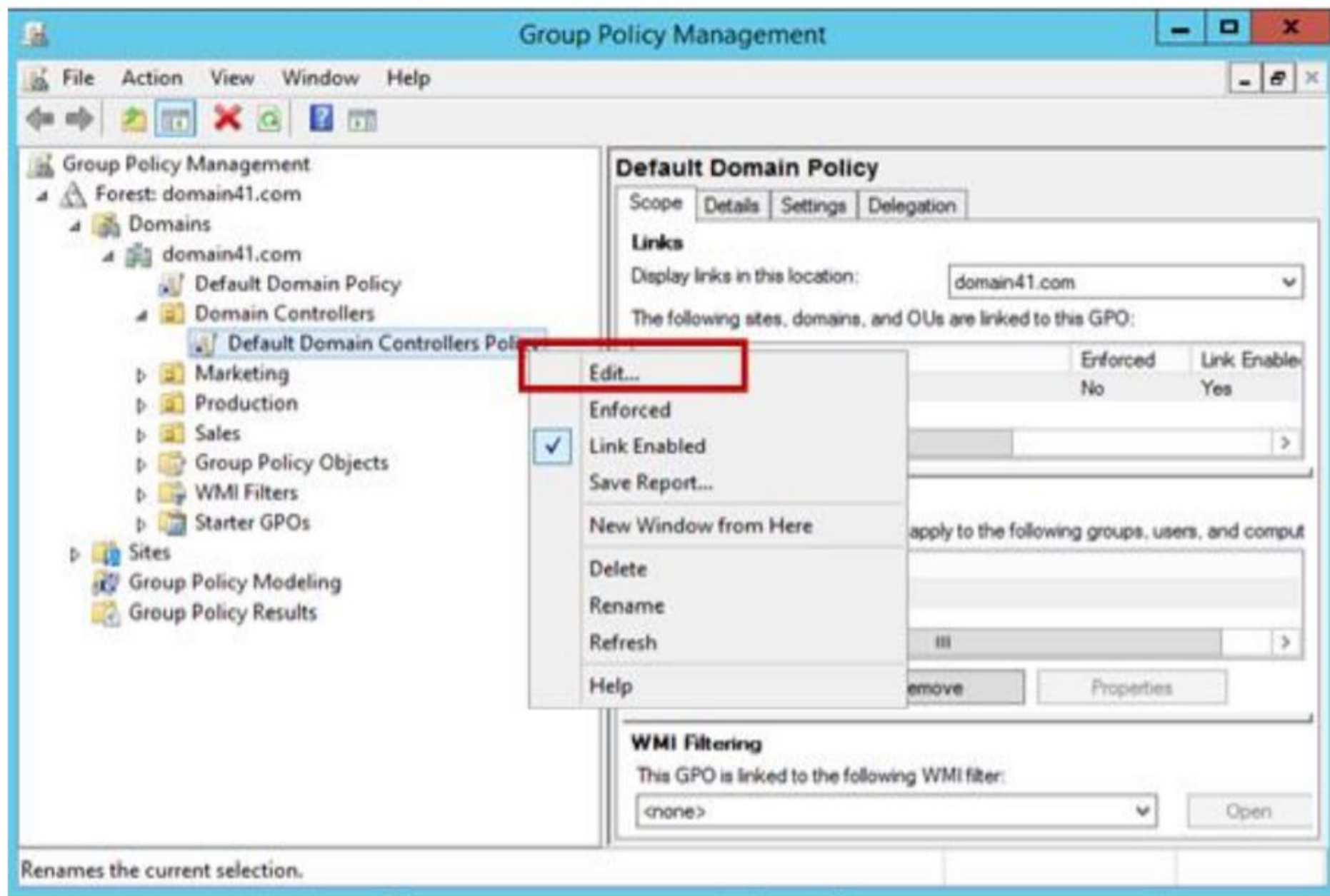
Trung tâm lưu trữ là gì?

❖ Trung tâm lưu trữ:

- ☐ Là một kho lưu trữ trung tâm cho các tập tin ADMX và ADML
- ☐ Được lưu trong SYSVOL
- ☐ Phải được tạo thủ công
- ☐ Được phát hiện tự động bởi Windows Vista trở về sau

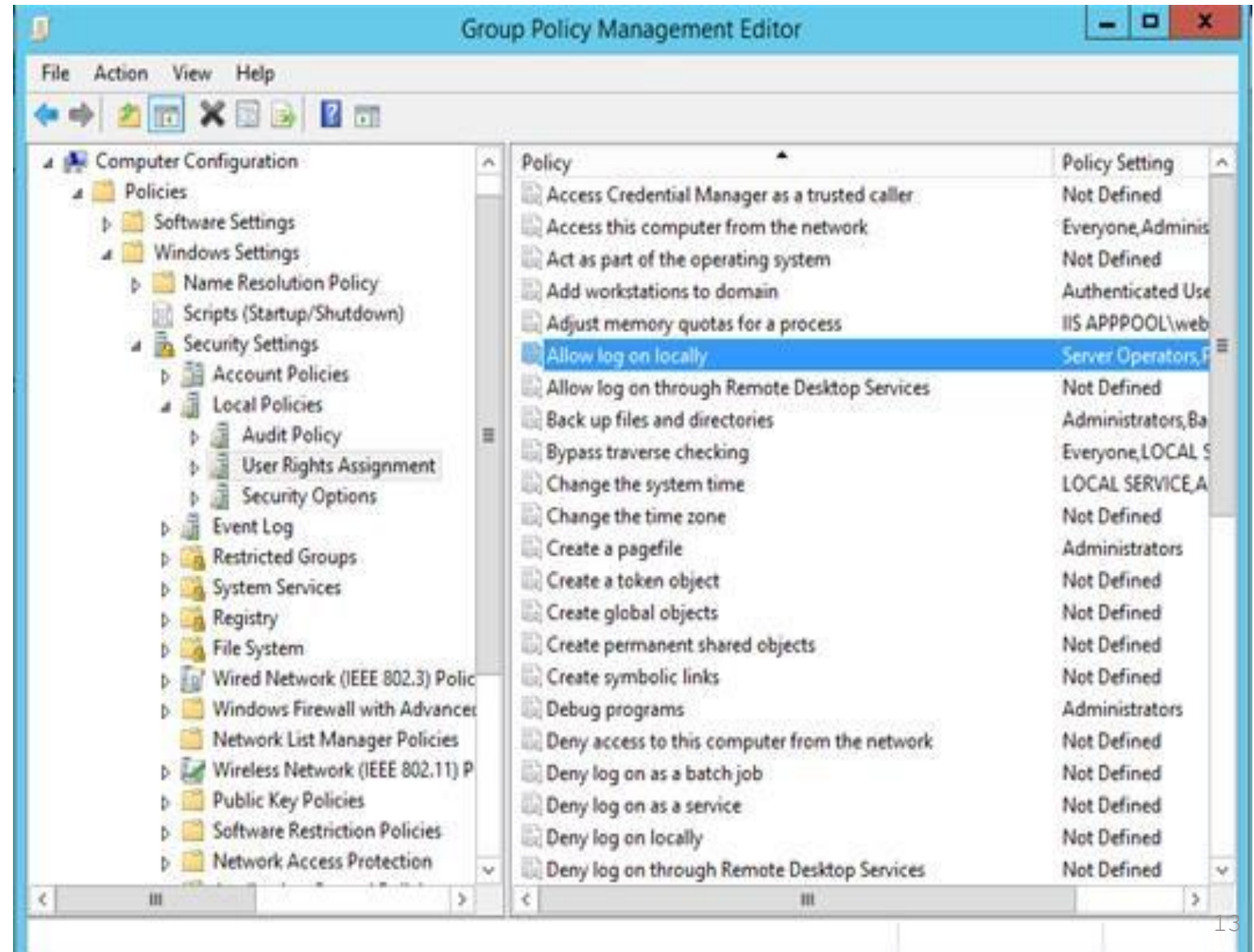


Điều chỉnh Policy



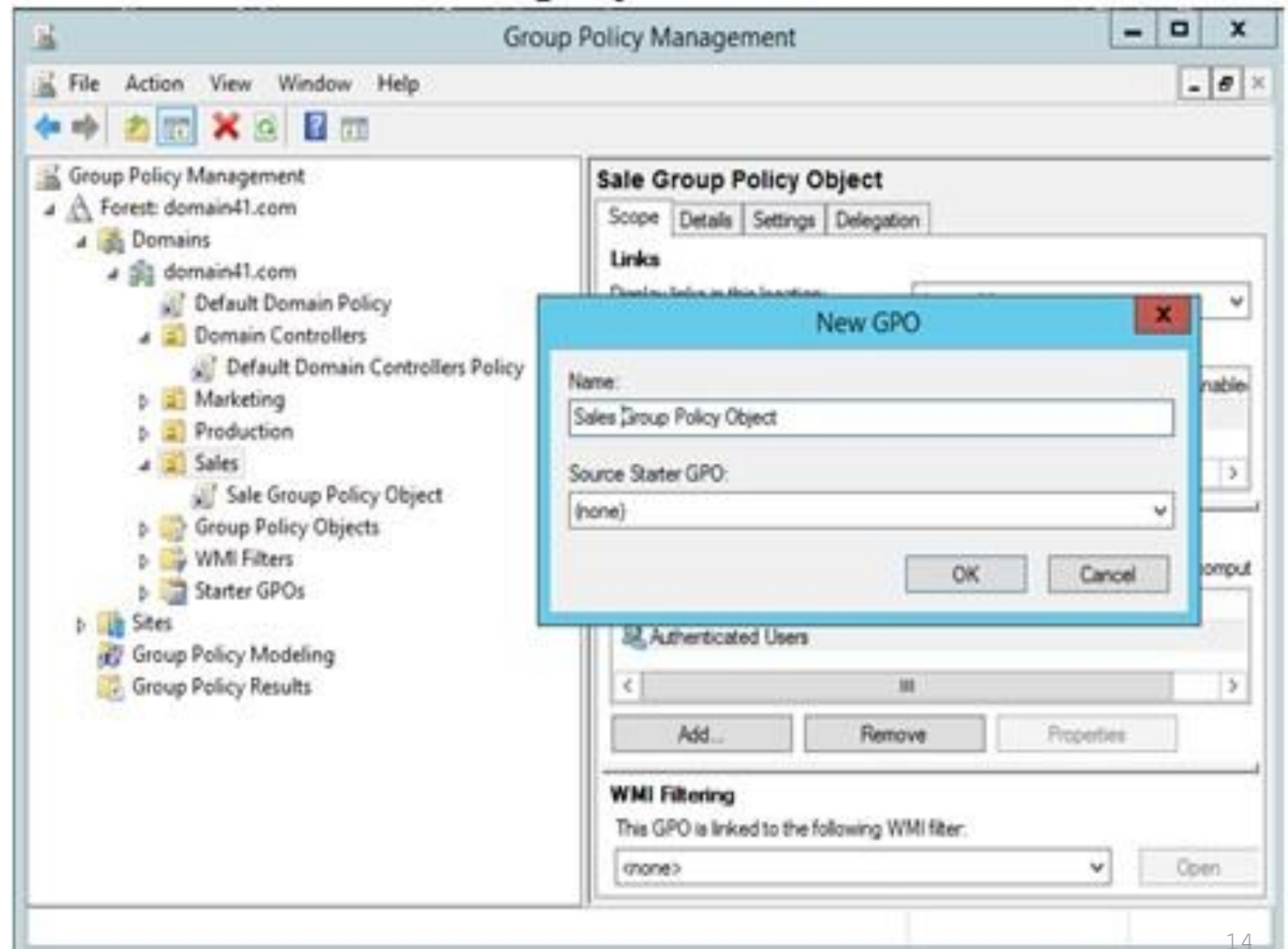
Cho phép Group Users logon trên máy Domain Controller

Vào Computer Configuration \ Policies \ Windows Settings \ Security Settings \ Local Policies \ User Rights Assignment \ Double click vào Allow log on locally.



Tạo một chính sách nhóm (Group Policy) cho OU

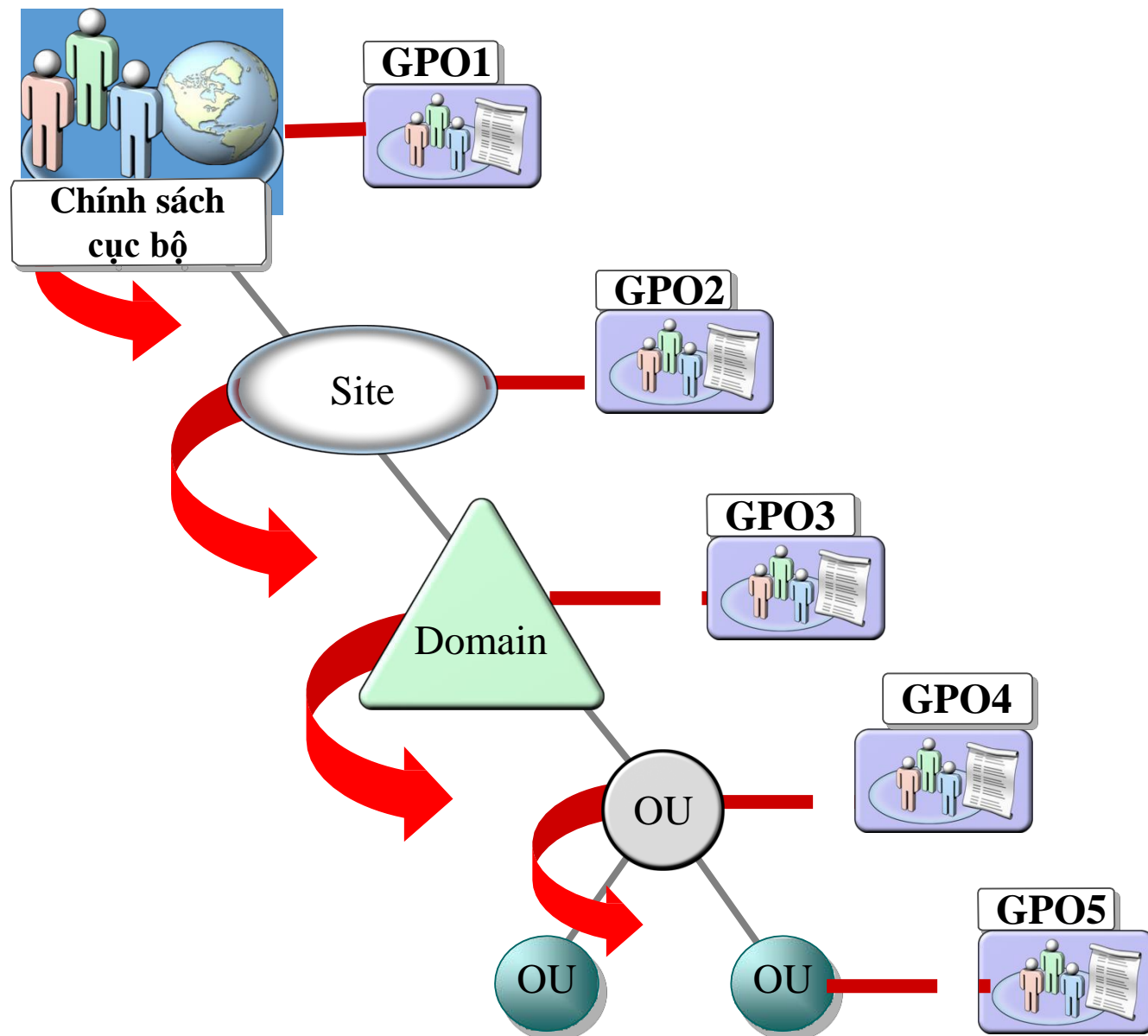
- Vào Server Manager \ Tools \ Group Policy Management.
- Click phải lên mục cần tạo \ Chọn Create a GPO in this domain. Nhập tên Sales Group Policy Object
- Click phải lên Group Policy Object \ Chọn Edit.



Trình tự xử lý chính sách nhóm GPO

- ❖ Các GPO được xử lý theo thứ tự sau:
 - ☐ Local GPO
 - ☐ Sites GPO
 - ☐ Domains GPO
 - ☐ Organizational Unit GPO
- ❖ Local GPO được xử lý trước tiên và cuối cùng là các OU GPO
- ❖ Mặc định các GPO được xử lý sau được ghi đè lên các GPO được xử lý trước.

Trình tự xử lý chính sách nhóm



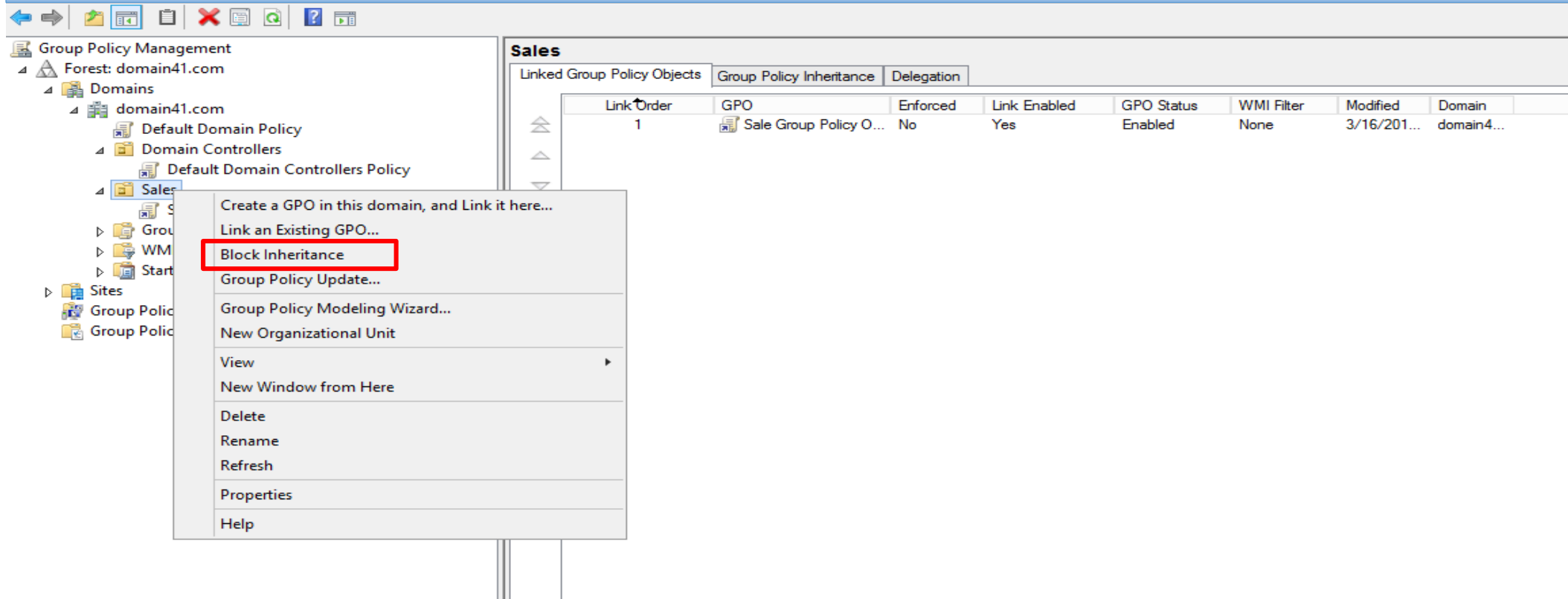
Thừa kế chính sách nhóm

- ❖ Mặc định các bộ chứa con thừa kế chính sách nhóm từ bộ
 - chứa cha
- ❖ Nếu các thiết lập chính sách của OU cha không được cấu hình thì chúng không được thừa kế bởi OU con
- ❖ Các thiết lập chính sách bị vô hiệu hóa được thừa kế ở dạng
 - bị vô hiệu hóa
- ❖ Nếu các thiết lập chính sách của cha không tương ứng với chính sách của con thì những chính sách được cấu hình cho con thì các thiết lập được cấu hình ở con sẽ được áp dụng

Các ngoại lệ

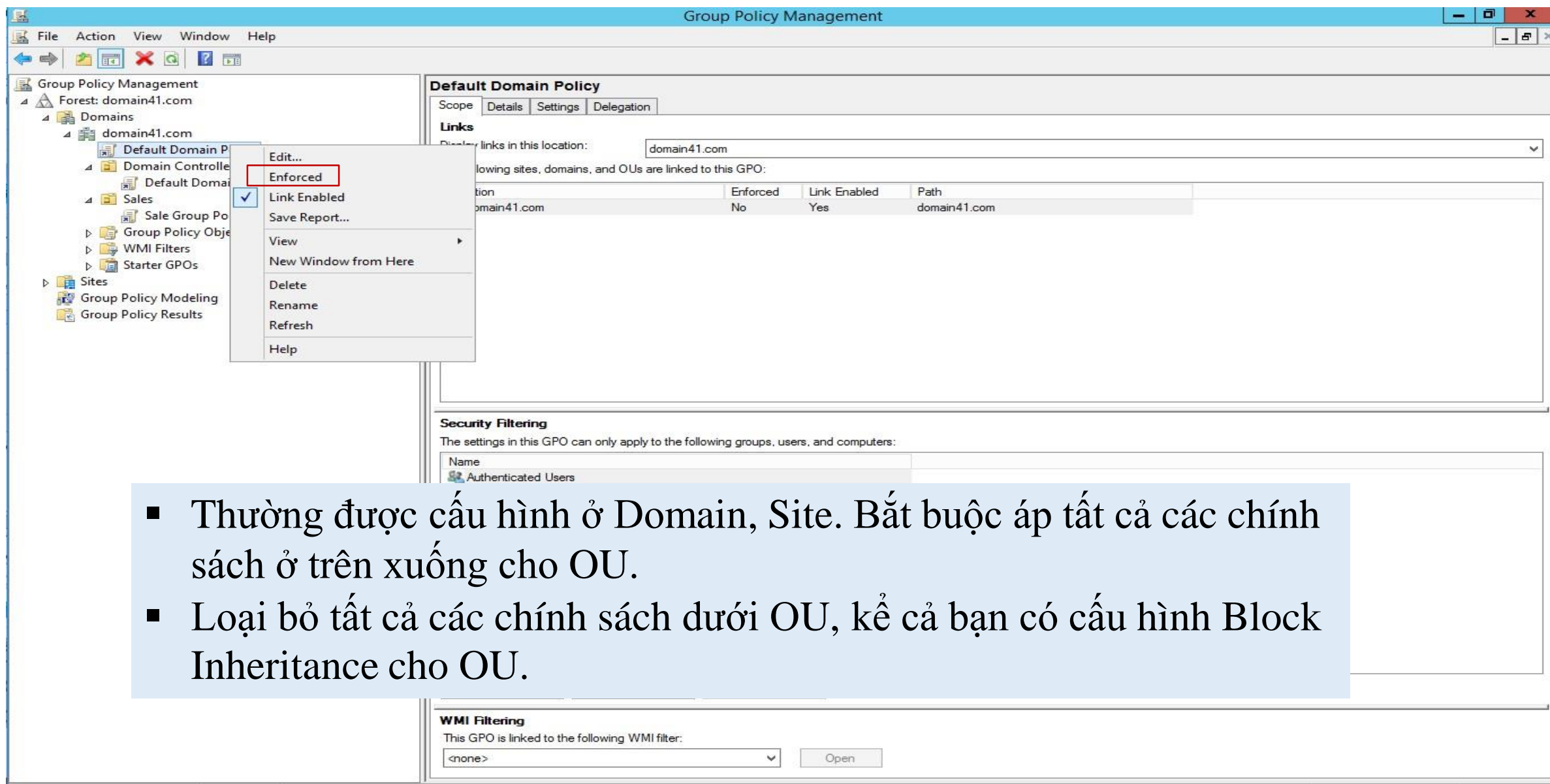
- ❖ Các máy tính và người dùng không tham gia vào miền (cục bộ) chỉ bị chỉ phối bởi GPO cục bộ.
- ❖ Không ghi đè – No Override: đảm bảo rằng các thiết lập chính sách của GPO này không bị đè bởi các GPO áp dụng sau đó
- ❖ Ngăn chặn kế thừa chính sách – block Policy Inheritance: không thừa hưởng các thiết lập chính sách của các GPO cha
- ❖ Việc ngăn chặn các thừa kế chính sách sẽ bị vô hiệu nếu thiết lập No Override được cấu hình trên GPO cha
- ❖ Thiết lập Loopback – loopback Setting: thiết lập này làm thay đổi thứ tự áp dụng các GPO cho người dùng

Block Inheritance



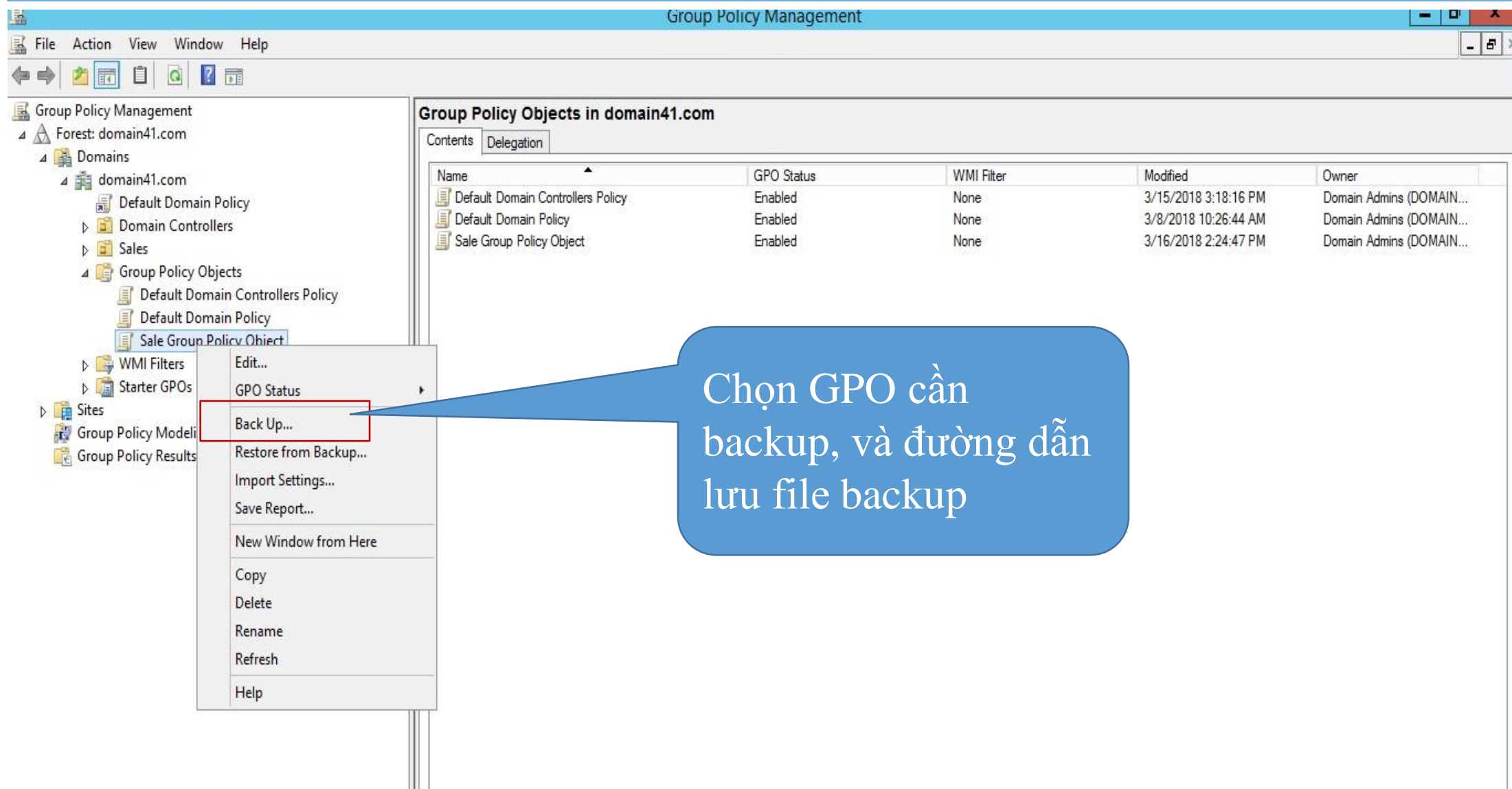
Block Inheritance : thường cấu hình ở OU, cho phép bỏ qua tất cả những chính sách của cấp trên như Site, Domain. Chỉ áp dụng các chính sách trong OU đó.

Enforced



- Thường được cấu hình ở Domain, Site. Bắt buộc áp tất cả các chính sách ở trên xuống cho OU.
- Loại bỏ tất cả các chính sách dưới OU, kể cả bạn có cấu hình Block Inheritance cho OU.

Backup GPO



Restore GPO:

