Lab: Cấu hình chính sách tài khoản domain

Mục tiêu

Sau khi hoàn thành bài lab này, học viên sẽ có thể:

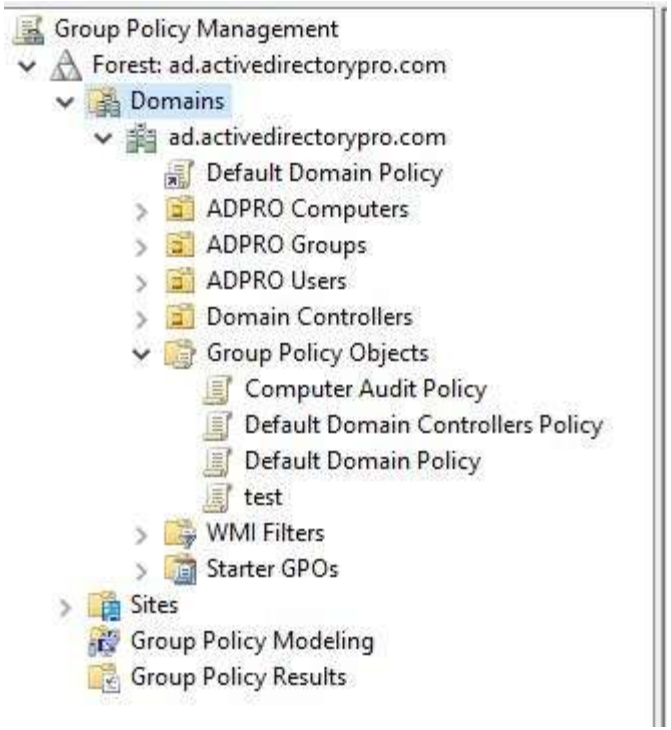
- Hiểu và cấu hình chính sách mật khẩu dựa trên domain
- Thiết lập chính sách khóa tài khoản để bảo vệ hệ thống
- Áp dụng các best practices cho bảo mật tài khoản trong môi trường Active Directory

Yêu cầu hệ thống

- Windows Server với vai trò Domain Controller
- Tài khoản Domain Administrator
- Máy client đã join domain để test
- Group Policy Management Console (GPMC)

Phần 1: Cấu hình chính sách mật khẩu domain

Bước 1: Truy cập Group Policy Management

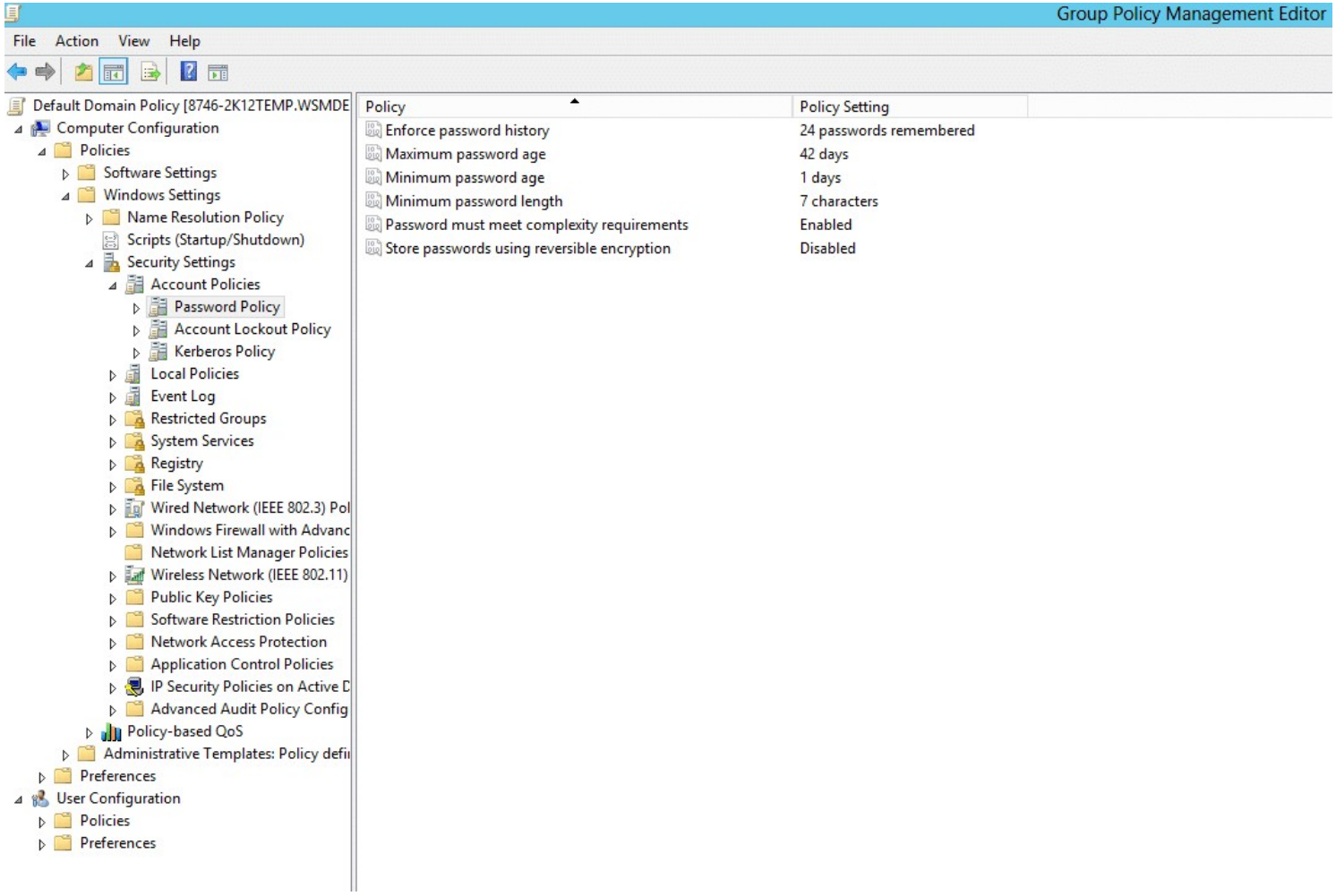


1. Mở **Server Manager**
2. Chọn **Tools** → **Group Policy Management**

3. Mở rộng cây thư mục: **Forest** → **Domains** → **[Tên domain của bạn]**
4. Right-click vào **Default Domain Policy** → **Edit**

Bước 2: Điều hướng đến Password Policy

1. Trong Group Policy Management Editor, điều hướng đến:
2. Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy


Group Policy Management Editor
File Action View Help
Default Domain Policy [8746-2K12TEMP.WSMDE
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Password Policy
Account Lockout Policy
Kerberos Policy
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Pol
Windows Firewall with Advanc
Network List Manager Policies
Wireless Network (IEEE 802.11)
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active D
Advanced Audit Policy Config
Policy-based QoS
Administrative Templates: Policy defi
Preferences
User Configuration
Policies
Preferences
Policy
Policy Setting
Enforce password history
24 passwords remembered
Maximum password age
42 days
Minimum password age
1 days
Minimum password length
7 characters
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled

Bước 3: Cấu hình các thiết lập mật khẩu

Cấu hình các policy sau:

Policy	Giá trị đề xuất	Mô tả
Enforce password history	12 passwords remembered	Ngăn người dùng tái sử dụng mật khẩu cũ
Maximum password age	90 days	Thời gian tối đa trước khi phải đổi mật khẩu
Minimum password age	1 day	Thời gian tối thiểu trước khi có thể đổi mật khẩu
Minimum password length	8 characters	Độ dài tối thiểu của mật khẩu
Password must meet complexity requirements	Enabled	Yêu cầu mật khẩu phức tạp
Store passwords using reversible encryption	Disabled	Không lưu mật khẩu dạng có thể giải mã

Bước 4: Cấu hình chi tiết

1. Double-click vào **"Enforce password history"**
    - Check **"Define this policy setting"**
    - Nhập **12** vào ô passwords remembered
    - Click **OK**
2. Double-click vào **"Maximum password age"**
    - Check **"Define this policy setting"**
    - Nhập **90** days
    - Click **OK**
3. Double-click vào **"Minimum password age"**
    - Check **"Define this policy setting"**
    - Nhập **1** day
    - Click **OK**
4. Double-click vào **"Minimum password length"**
    - Check **"Define this policy setting"**

- Nhập **8** characters
- Click **OK**

5. Double-click vào **"Password must meet complexity requirements"**
   - Select **"Enabled"**
   - Click **OK**
6. Double-click vào **"Store passwords using reversible encryption"**
   - Select **"Disabled"**
   - Click **OK**

Phần 2: Cấu hình chính sách khóa tài khoản

Bước 1: Truy cập Account Lockout Policy

1. Trong cùng Group Policy Management Editor, điều hướng đến:
2. Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Account Lockout Policy

Bước 2: Cấu hình các thiết lập khóa tài khoản

Cấu hình các policy sau:

Policy	Giá trị đề xuất	Mô tả
Account lockout duration	30 minutes	Thời gian khóa tài khoản
Account lockout threshold	5 invalid logon attempts	Số lần đăng nhập sai trước khi khóa
Reset account lockout counter after	30 minutes	Thời gian reset bộ đếm

Bước 3: Thiết lập chi tiết

1. Double-click vào **"Account lockout threshold"**
    - Check **"Define this policy setting"**
    - Nhập **5** invalid logon attempts
    - Click **OK**
    - Hệ thống sẽ tự động đề xuất giá trị cho 2 policy còn lại
2. Chấp nhận các giá trị được đề xuất hoặc tùy chỉnh:
    - **Account lockout duration**: 30 minutes
    - **Reset account lockout counter after**: 30 minutes

Phần 3: Áp dụng và kiểm tra chính sách

Bước 1: Áp dụng chính sách

1. Đóng Group Policy Management Editor
2. Mở Command Prompt với quyền Administrator
3. Chạy lệnh để force update policy:
4. gpupdate /force

Bước 2: Kiểm tra trên Domain Controller

gpresult /h gpresult.html

Mở file HTML để xem các policy đã được áp dụng.

Bước 3: Test chính sách mật khẩu

1. Tạo user mới:
2. net user testuser Password123 /add /domain
3. Thử đổi mật khẩu không đạt yêu cầu:
4. net user testuser 123 /domain
    - Kết quả: Lỗi do không đáp ứng độ phức tạp

5. Đổi mật khẩu hợp lệ:
6. net user testuser NewPass123! /domain

Bước 4: Test chính sách khóa tài khoản

1. Từ máy client, thử đăng nhập sai mật khẩu 5 lần liên tiếp
2. Quan sát tài khoản bị khóa
3. Kiểm tra Event Viewer trên DC:
    - Windows Logs → Security
    - Tìm Event ID 4740 (Account lockout)

Phần 4: Giám sát và báo cáo

Kiểm tra chính sách hiện tại

```
# Kiểm tra password policy
Get-ADDefaultDomainPasswordPolicy

# Kiểm tra fine-grained password policy (nếu có)
Get-ADFineGrainedPasswordPolicy -Filter *
```

Tạo báo cáo tài khoản bị khóa

Tìm tất cả tài khoản bị khóa

Search-ADAccount -LockedOut | Select Name, LockedOut, LastLogonDate

Mở khóa tài khoản

Unlock-ADAccount -Identity "username"

Phần 5: Cấu hình nâng cao (Tùy chọn)

Fine-Grained Password Policies

Nếu cần áp dụng chính sách khác nhau cho các nhóm user:

1. Mở **Active Directory Administrative Center**
2. Điều hướng đến **System** → **Password Settings Container**
3. Tạo **New** → **Password Settings**
4. Cấu hình các thiết lập riêng biệt
5. Áp dụng cho specific groups hoặc users

Group Policy Preferences

Cấu hình thêm các registry settings để tăng cường bảo mật:

- Disable LM hash storage
- Enable strong session key requirement
- Configure additional audit policies

Câu hỏi thực hành

1. **Câu hỏi 1**: Tại sao nên set minimum password age là 1 day thay vì 0?
2. **Câu hỏi 2**: Nếu một user bị khóa tài khoản, có những cách nào để unlock?
3. **Câu hỏi 3**: Làm thế nào để áp dụng chính sách mật khẩu khác nhau cho các nhóm user khác nhau?
4. **Câu hỏi 4**: Password complexity requirements bao gồm những yêu cầu nào?

Troubleshooting thường gặp

Lỗi 1: Group Policy không áp dụng

Giải pháp:

- Kiểm tra DNS resolution
- Chạy gpupdate /force

- Restart máy client nếu cần

Lỗi 2: User không thể đổi mật khẩu

Nguyên nhân có thể:

- Chưa đến minimum password age
- Mật khẩu mới trùng với history
- Không đạt complexity requirements

Lỗi 3: Tài khoản bị khóa liên tục

Kiểm tra:

- Scheduled tasks chạy với credentials cũ
- Services sử dụng tài khoản domain
- Mapped drives với saved credentials

Kết luận

Bài lab này đã hướng dẫn cách cấu hình các chính sách bảo mật cơ bản cho tài khoản domain. Việc thiết lập đúng các policy này là nền tảng quan trọng cho việc bảo vệ môi trường Active Directory khỏi các cuộc tấn công brute force và đảm bảo tính bảo mật của hệ thống.