

# CHƯƠNG V

## QUẢN LÝ BẢO MẬT

√ Thực thi, cấu hình, quản lý và gỡ rối các chính sách trong môi trường Windows 2000.

- Thực thi, cấu hình, quản lý và gỡ rối các chính sách cục bộ trong môi trường Windows 2000.
- Thực thi, cấu hình, quản lý và gỡ rối các chính sách hệ thống trong môi trường Windows 2000.

√ Thực thi, cấu hình, quản lý và gỡ rối việc kiểm định

√ Thực thi, cấu hình, quản lý và gỡ rối các chính sách tài khoản người dùng

√ Thực thi, cấu hình, quản lý và gỡ rối sự bảo mật bằng cách sử dụng tập công cụ cấu hình sự bảo mật

Với Windows 2000 Server, bạn có thể quản lý sự bảo mật tại mức cục bộ hoặc mức miền. Tại mức miền, bạn quản lý các chính sách bảo mật miền. Và tại mức cục bộ, bạn quản lý các chính sách bảo mật cục bộ.

Việc thiết lập bảo mật được cấu hình thông qua chính sách về nhóm người dùng. Các chính sách tài khoản người dùng được sử dụng điều khiển tiến trình đăng nhập, như việc cấu hình mật khẩu và tài khoản “lockout”. Các chính sách cục bộ được sử dụng để định nghĩa các chính sách bảo mật cho chính máy tính này, như kiểm định quyền người dùng và các tùy chọn về bảo mật.

Trong WinNT 4, bạn có thể điều khiển Desktops của người dùng thông qua các chính sách hệ thống. Chức năng này cũng có trong Windows 2000 để tương thích với các phiên bản trước, nhưng nó được khuyến cáo là bạn sử dụng các chính sách nhóm người dùng thay thế chính sách hệ thống để quản lý các tùy chọn.

Công cụ “Security and Analysis Configuration” là các tiện ích mới của Windows 2000 Server, qua đó bạn có thể phân tích cấu hình bảo mật của bạn. Các tiện ích sử dụng khuôn mẫu bảo mật để so sánh cấu hình bảo mật hiện tại của bạn với cấu hình bạn yêu cầu.

Trong chương này, bạn sẽ học cách quản lý bảo mật trong môi trường Windows 2000 Server. Đầu tiên bạn sẽ cài đặt trình điều khiển MMC để quản lý việc thiết lập tính bảo mật, sau đó học cách cấu hình các chính sách về tài khoản người dùng, các chính sách cục bộ và các chính sách bảo mật. Phần cuối chương này sẽ mô tả cách để sử dụng tiện ích “Security and Analysis Configuration” để phân tích cấu hình bảo mật của bạn.

## Thiết lập quản lý bảo mật

Windows 2000 Server cho phép bạn quản lý các thiết lập về bảo mật tại mức cục bộ cho máy tính cụ thể hoặc trên mức miền lớn. Mọi chính sách bảo mật miền bạn định nghĩa đề lên các chính sách cục bộ của một máy tính.

Bạn quản lý các chính sách với chính sách nhóm người dùng cả đối tượng thích hợp:

- Để quản lý chính sách cục bộ, bạn sử dụng chính sách nhóm người dùng thông qua đối tượng Local Computer Group Policy
- Để quản lý chính sách miền, bạn sử dụng chính sách nhóm người dùng thông qua đối tượng Domain Controllers Group Policy

Để thuận tiện cho công việc quản lý chính sách của bạn, bạn có thể thêm đối tượng Local Computer Policy and Domain Controller Security vào Microsoft Management Console (MMC). Bạn cũng có thể truy cập các chính sách tài khoản người dùng và các chính sách cục bộ bằng cách chọn :

Start ► Programs ► Administrative Tools  
    ► Domain Security Policy or Local Security Policy

Bài tập 5.1, bạn sẽ thêm đối tượng Group Policy and Event Viewer trên các Server thành viên của bạn.



Tất cả các bài tập trong chương này, ngoại trừ bài 5.7, bạn phải hoàn toàn thành từ member server.

## **BÀI TẬP 5.1**

### **Tạo trình điều khiển quản lý cho các thiết lập bảo mật.**

1. Chọn Start ► Run, gõ “MMC” vào hộp hội thoại Run và bấm nút OK để mở MMC
2. Từ thực đơn chính, chọn Console ► Add/Remove Snap-in.
3. Trong hộp hội thoại Add/Remove Snap-in bấm nút Add.
4. Chọn Group Policy và bấm nút Add.
5. Đối tượng Group Policy chỉ định Local Computer là mặc định. Bấm nút Finish
6. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK.
7. Từ thực đơn chính, chọn Console ► Add/Remove Snap-in.
8. Trong hộp hội thoại Add/Remove Snap-in bấm nút Add.
9. Chọn Event Viewer và bấm nút Add.
10. Hộp hội thoại để chọn máy tính hiện ra với Local Computer được chọn mặc định. Bấm nút Finish sau đó bấm nút Close
11. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK.
12. Chọn Console ► Save As. Ghi trình điều khiển với tên Security trong thư mục Administrative Tools ( đây là vùng mặc định ) và bấm nút Save

Bạn có thể truy cập trình điều khiển bằng cách chọn:

Start ► Programs ► Administrative Tools ► Security.

## **Sử dụng các chính sách tài khoản người dùng**

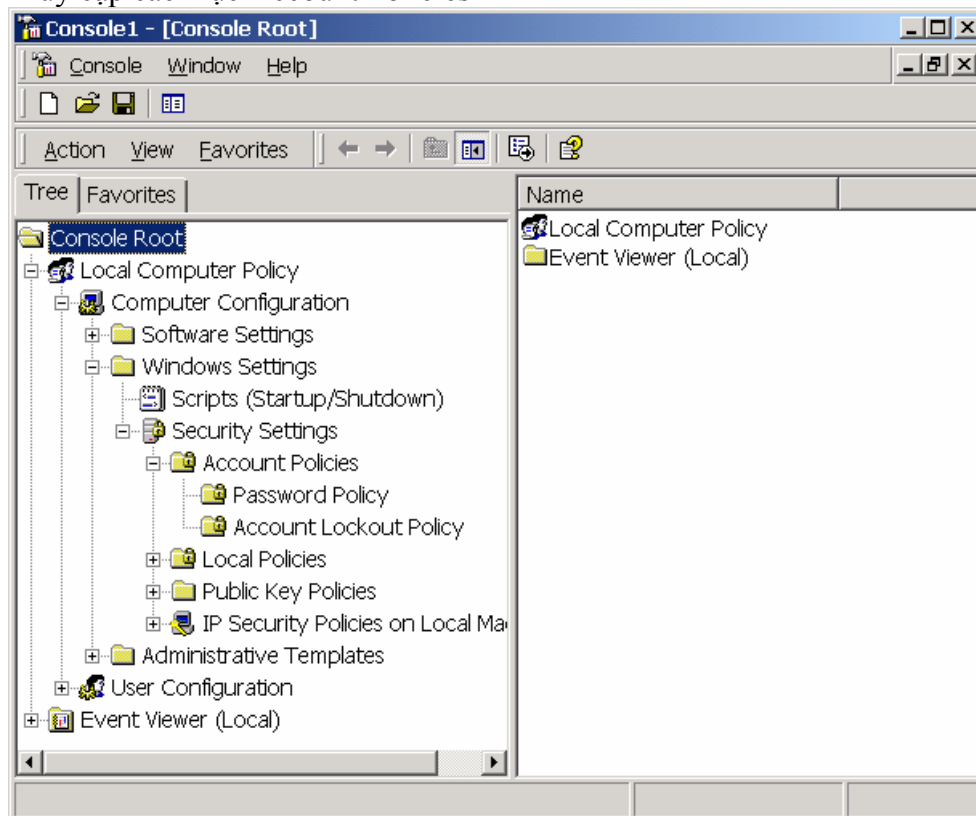
Các chính sách tài khoản người dùng được sử dụng để chỉ rõ các thuộc tính tài khoản người dùng liệt kê trong tiến trình đăng nhập. Nó cho phép bạn cấu hình việc thiết lập sự bảo mật máy tính cho mật khẩu và chỉ định tài khoản “lockout” và xác nhận Kerberos với một miền.

### **Microsoft Exam Objective**

**Thực thi, cấu hình, quản lý và gỡ rối chính sách tài khoản người dùng.**

Sau khi bạn đã nạp MMC cho Group Policy, bạn sẽ nhìn thấy một lựa chọn cho Local Computer Policy. Để truy cập các mục Account Policies, mở ra Local Computer Policy, Computer Configuration, Windows Settings, Security Settings và Account Policies. Hình 5.1 biểu diễn các mục Policies.

**HÌNH 5.1** Truy cập các mục Account Policies



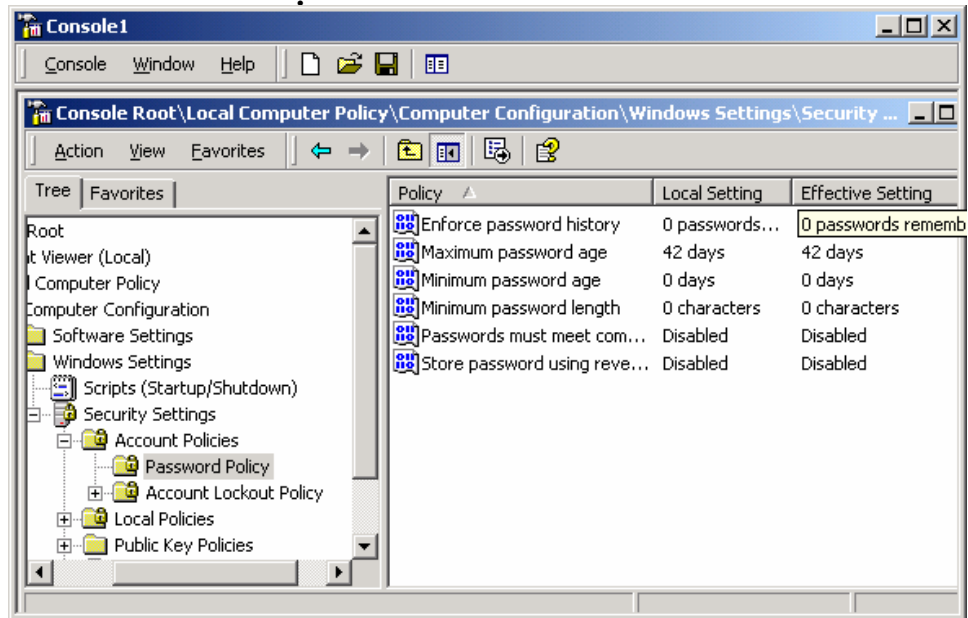
Nếu bạn đang dùng Windows 2000 member server, bạn sẽ thấy hai mục: Password Policy và Account Lockout Policy. Nếu bạn đang dùng Windows 2000 Server, máy được cấu hình là domain controller, bạn sẽ thấy ba mục: Password Policy, Account Lockout Policy và Kerberos Policy. Các chính sách tài khoản người dùng có hiệu lực cho các member server và domain controller được giải thích trong phần kế tiếp.

### **Thiết lập các chính sách mật khẩu**

Các chính sách về mật khẩu bảo đảm các yêu cầu bảo mật phải bắt buộc trên máy tính. Chú ý rằng chính sách mật khẩu được đặt trên nền tảng mỗi máy tính là rất quan trọng; nó không thể được cấu hình cho người dùng cụ thể.

Hình 5.2 thể hiện các chính sách về mật khẩu được định nghĩa trên Windows 2000 member server, nó được giải thích trong bảng 5.1. Trên Windows 2000 domain controller, tất cả các chính sách được cấu hình là “not defined”(không được định nghĩa).

**HÌNH 5.2 Các chính sách về mật khẩu**



**BẢNG 5.1 Các lựa chọn chính sách mật khẩu**

Chính sách	Giải thích	Giá trị mặc định	Giá trị tối thiểu	Giá trị tối đa
Enforce Password History	Lưu giữ lịch sử mật khẩu của người dùng	Nhớ 0 mật khẩu	Giống giá trị mặc định	Nhớ 24 mật khẩu
Maximum Password Age	Xác định số ngày tối đa người dùng có thể giữ mật khẩu hợp lệ	Giữ mật khẩu cho 42 ngày	Giữ mật khẩu cho 1 ngày	Giữ mật khẩu cho 999 ngày
Minimum Password Age	Chỉ định khoảng thời gian mật khẩu phải giữ sau khi nó bị thay đổi	0 ngày (mật khẩu có thể bị thay đổi ngay lập tức)	Giống như giá trị mặc định	999 ngày
Minimum Password Length	Chỉ định số tối thiểu các ký tự của mật khẩu phải có	0 ký tự (không yêu cầu mật khẩu)	Giống giá trị mặc định	14 ký tự
Password Must Meet Complexity Requirements	Cho phép bạn cài đặt bộ lọc mật khẩu	Vô hiệu (Disabled)	Giống giá trị mặc định	Có hiệu lực (Enable)

Store Password Using Revesible Encryption for All Users in the Domain	chỉ định mức cao hơn của việc mã hoá cho việc lưu trữ các mật khẩu của người dùng	Vô hiệu (Disabled)	Giống giá trị mặc định	Có hiệu lực (Enable)
---	---	--------------------	------------------------	----------------------

Các chính sách mật khẩu được sử dụng như sau:

- Lựa chọn Enfore Password History được sử dụng để người dùng không thể sử dụng như những mật khẩu đã được sử dụng. Người dùng buộc phải tạo re mật khẩu mới khi mà mật khẩu của họ chấm dứt hoặc bị thay đổi
- Lựa chọn Maximun Password Age được sử dụng để sau khi vượt quá số ngày tồn tại của mật khẩu, người dùng bị ép buộc phải thay đổi mật khẩu của họ
- Lựa chọn Minimum Password Age được sử dụng để ngăn cản người dùng không thay đổi mật khẩu vài lần liên tiếp nhanh chóng để mà làm thất bại mục đích của chính sách Enfore Password History
- Lựa chọn Minimum Password Length được sử dụng để bảo đảm rằng người dùng tạo ra mật khẩu tốt để chỉ ra rằng nó đáp ứng độ dài yêu cầu. Nếu lựa chọn này không được thiết lập, người dùng không được yêu cầu tạo mật khẩu.
- Lựa chọn Password Must Meet Complexity Requirements được sử dụng để ngăn cản người dùng tránh sử dụng những mục mật khẩu được tìm thấy trong từ điển của tên phổ biến
- Lựa chọn Store Password Using Revesible Encryption for All Users in the Domain được sử dụng để cung cấp một mức cao hơn cho việc giữ an toàn mật khẩu của người dùng

Trong bài tập 5.2 bạn sẽ cấu hình các chính sách mật khẩu cho máy tính của bạn. Bây giờ và những phần bài tập còn lại trong chương này cho rằng bạn đã hoàn thành bài tập 5.1 để tạo ra một trình quản lý bảo mật (Security management console) Tất cả các bài tập nên được thực hiện trên các member server

## BÀI TẬP 5.2

### Thiết lập các chính sách mật khẩu

1. Chọn Start ► Programs ► Administrative Tools ► Security và mở rộng nút Local Computer Policy
2. Mở rộng nút làm xuất hiện: Computer Configuration, Windows Settings, Security Settings, Account Policies, Password Policy.
3. Mở chính sách Enfore Password History. Trong trường Effective Policy Setting, chỉ định 5 mật khẩu được ghi nhớ. Bấm nút OK
4. Mở chính sách Maximum Password Age. Trong trường Local Policy Setting chỉ định mật khẩu kết thúc trong 60 ngày. Bấm nút OK

## Các chính sách thiết lập về đăng nhập tài khoản không hợp lệ (Account Lockout)

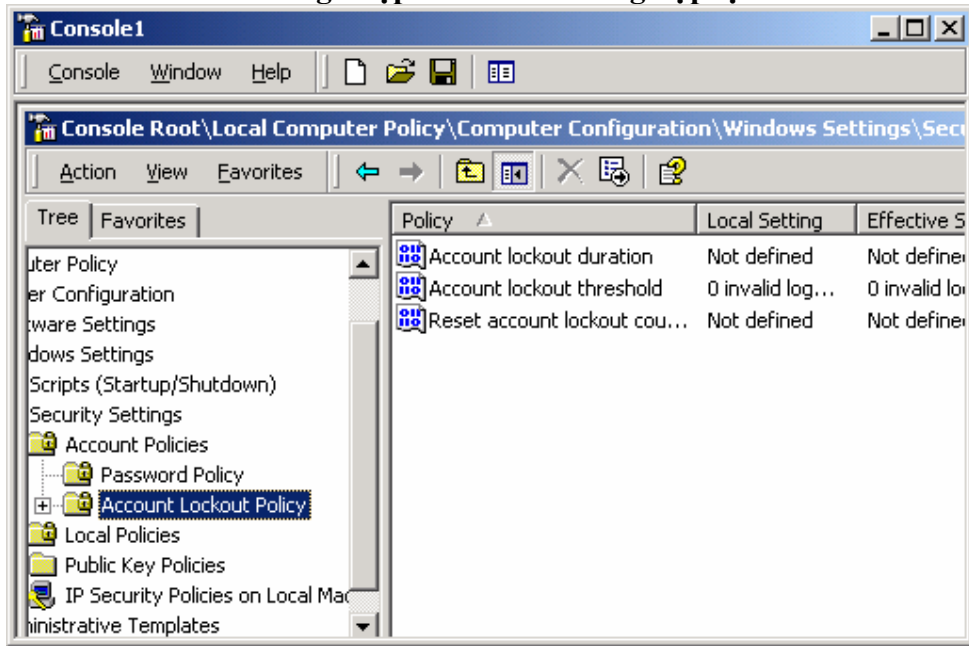
Các chính sách Account Lockout được sử dụng để chỉ định số lần thử đăng nhập không hợp lệ có thể cho phép. Bạn thiết lập các chính sách này sau  $x$  số lần thử đăng nhập không thành công trong khoảng  $y$  phút, tài khoản sẽ bị khoá trong khoảng thời gian xác định hoặc cho đến khi người quản trị mở trở lại tài khoản đó



Các chính sách về số lần cho phép đăng nhập không hợp lệ cũng giống như cách các nhà băng điều khiển ATM truy cập mã bí mật. Bạn có lượng chắc chắn các khả năng để đăng nhập thành công mã truy cập. Bằng cách đó, nếu ai đó ăn trộm thẻ của bạn, họ không thể làm được việc là thử các phỏng đoán về mã truy cập của bạn cho đến khi họ có kết quả đúng. Nhưng sau khi thử không thành công với mã truy cập của bạn, máy ATM sẽ giữ thẻ. Sau đó bạn cần yêu cầu thẻ mới từ ngân hàng.

Hình 5.3 thể hiện các chính sách về đăng nhập không hợp lệ, nó được giải thích trong bảng 5.2

**HÌNH 5.3** Các chính sách về đăng nhập tài khoản không hợp lệ



**BẢNG 5.2** Các lựa chọn về chính sách về đăng nhập tài khoản không hợp lệ

Chính sách	Giải thích	Giá trị mặc định	Giá trị tối thiểu	Giá trị tối đa	Giá trị đề nghị
Account Lockout Threshold	Chỉ rõ số lần thử truy cập không hợp lệ trước khi bị khoá	0 (Vô hiệu, tài khoản không bị khoá)	Giống giá trị mặc định	999 lần thử	5 lần thử

Account Lockout Duration	Chỉ rõ khoảng thời gian bị khoá nếu Account Lockout Threshold bị vượt quá	0; nếu Account Lockout Threshold co hiệu lực thì sẽ là 30 phút	Giờng giá trị mặc định	99,999 phút	5 phút
Reset Account Lockout Counter After	Chỉ định khoảng thời gian bộ đếm sẽ nhớ các lần thử đăng nhập không hợp lệ	0; nếu Account Lockout Threshold co hiệu lực thì sẽ là 5 phút	Giờng giá trị mặc định	99,999 phút	5 phút

Trong bài tập 5.3, bạn sẽ cấu hình các chính sách về đăng nhập tài khoản không hợp lệ và kiểm tra hiệu quả của chúng

### BÀI TẬP 5.3

#### Các chính sách thiết lập Account lockout

1. Chọn Start ► Programs ► Administrative Tools ► Security và mở nút Local Computer Policy
2. Mở rộng nút làm xuất hiện: Computer Configuration, Windows Settings, Security Settings, Account Policies, Account Lockout Policy
3. Mở chính sách Account Lockout Threshold. Trong trường Local Policy Setting, chỉ định tài khoản sẽ bị khoá sau 3 lần cố thử đăng nhập. Bấm nút Ok
4. Hộp hội thoại Suggestd Value Changes sẽ xuất hiện. Nhận giá trị mặc định cho Account lockout duration và Reset account lockout counter bằng cách bấm nút OK
5. Rời khỏi hệ thống. Thử đăng nhập với tên Emily cùng với 3 lần nhập sai password
6. Sau đó bạn sẽ thấy thông điệp lỗi tuyên bố tài khoản bị khoá, đăng nhập với tài khoản Administrator
7. Để khôi phục tài khoản của Emily, hãy mở mục Local Users and Groups trong MMC, mở nút Users, và nhấp kép chuột vào tài khoản Emily. Trong phần General của hộp hội thoại thuộc tính của Emily, bấm loại bỏ đánh dấu trong hộp chọn Account Locked Out. Sau đó bấm nút OK.

#### Thiết lập chính sách Kerberos

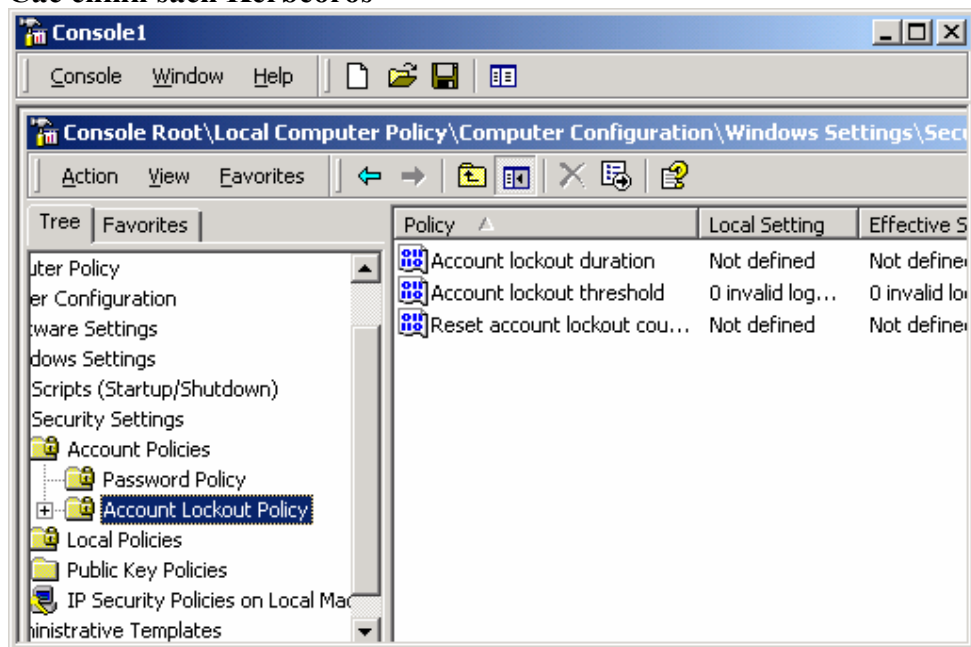
Phiên bản Kerberos 5 là giao thức bảo mật được sử dụng trong Windows 2000 Server để xác thực người dùng và các dịch vụ mạng. Nó được gọi là xác minh kép hay xác thực lẫn nhau.

Khi Windows 2000 Server được cài đặt như domain controller, nó tự động trở thành trung tâm phân phối khoá (key distribution center-KDC). KDC sẽ chịu trách nhiệm với tất cả các mật khẩu và các thông tin tài khoản người dùng trong các máy khách. Các phục vụ của Kerberos cũng được cài đặt trên mỗi máy khách và máy chủ Windows 2000.

1. Các yêu cầu kiểm định máy khách từ KDC sử dụng mật khẩu hoặc thẻ thông minh
2. KDC phát cho máy khách thẻ gọi là thẻ công nhận (ticket-granting ticket –TGT). Máy khách có thể sử dụng TGT để truy cập các dịch vụ về thẻ này (ticket-granting service –TGS). TGS cung cấp các thẻ phục vụ cho các máy khách.
3. Máy khách trình thẻ phục vụ để yêu cầu các dịch vụ mạng. Các thẻ phục vụ sẽ kiểm định lẫn nhau phục vụ từ người dùng và phục vụ đến người dùng.

Hình 5.4 Hiện thị các chính sách Kerberos và các giải thích trong bảng 5.3

**HÌNH 5.4** Các chính sách Kerberos



**BẢNG 5.3** Các lựa chọn chính sách Kerberos

Chính sách	Diễn giải	Thiết lập nội bộ mặc định	Thiết lập hiệu quả
Enforce User Logon Restrictions	Chỉ định hạn chế đăng nhập là bắt buộc	Không xác định	Cho phép
Maximum Lifetime for Service Ticket	Chỉ định tuổi tối đa cho thẻ phục vụ trước khi thay mới	Không xác định	600 phút

Maximum Lifetime for User Ticket	Chỉ định tuổi tối đa cho thẻ người dùng trước khi thay mới	Không xác định	10 giờ
Maximum Lifetime for User Renewal	Chỉ định khoảng thời gian thẻ có thể bị thay mới trước khi nó được tái sinh	Không xác định	7 ngày
Maximum Tolerance Computer Clock Synchronization	Chỉ định thời gian tối đa cho sự đồng bộ hoá giữa máy khách và KDC	Không xác định	5 phút

## Sử dụng các chính sách nội bộ

Sau khi bạn đã học hết các phần trước, các chính sách tài khoản được sử dụng điều khiển thủ tục đăng nhập. Khi bạn muốn điều khiển những thứ bạn có thể làm sau khi đăng nhập, bạn sử dụng các chính sách nội bộ. Với các chính sách nội bộ bạn có thể thi hành việc kiểm định, chỉ định quyền người dùng và đạt các tùy chọn bảo mật.

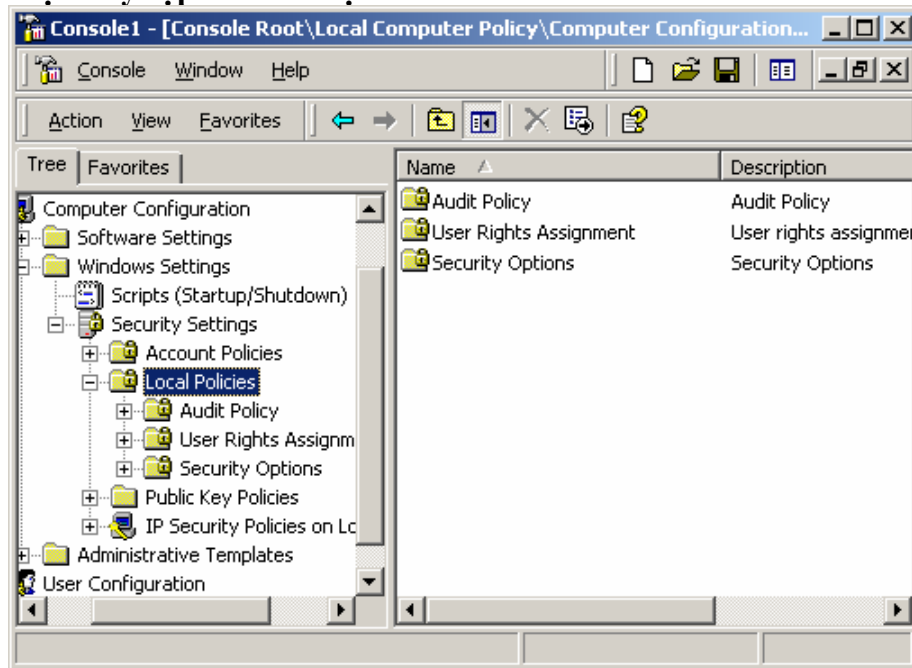
Microsoft  
Exam  
Objective

### **Thi hành, cấu hình, quản lý và gỡ rối các chính sách trong môi trường Windows 2000**

- Thi hành, cấu hình, quản lý và gỡ rối các chính sách cục bộ trong môi trường Windows 2000
- Thi hành, cấu hình, quản lý và gỡ rối các chính sách hệ thống trong môi trường Windows 2000

Để sử dụng các chính sách nội bộ, đầu tiên bạn thêm mục Local Computer Policy vào MMC (xem bài 5.1). Sau đó từ MMC lần theo đường dẫn thư mục để truy cập thư mục Local Policies: Local Computer Policy, Computer Configuration, Window Setting, Security Settings, Local Policies. Hình 5.5 hiển thị các thư mục của Local Policies

**HÌNH 5.5** Việc truy cập các thư mục của Local Policies



Có ba thư mục trong Local Policies : Audit Policy, User Rights Assignment và Security Options. Các chính sách bao trùm các phần tiếp theo

**Thiết lập chính sách kiểm định**

Microsoft **Thi hành, cấu hình , quản lý và gỡ rối việc kiểm định**

Exam  
Objective

Bạn kiểm định các sự kiện liên quan đến quản lý người dùng thông qua chính sách kiểm định. Bằng cách lưu lại vết của các sự kiện chính, bạn có thể đưa ra được tiến trình của một nhiệm vụ được chỉ định, như tạo người dùng, hoàn thành hoặc không hoàn thành trong thủ tục đăng nhập. Bạn có thể nhận ra sự xâm phạm bảo mật được phát sinh khi người dùng cố thử truy cập các nhiệm vụ quản lý hệ thống mà không có sự cho phép.

Khi bạn định nghĩa nội chính sách kiểm định bạn cần lựa chọn kiểm định việc hoàn thành hay thất bại của sự kiện được chỉ định. Sự kiện hoàn thành có nghĩa là nhiệm vụ được hoàn thành một cách hoàn hảo. Sự kiện thất bại có nghĩa là nhiệm vụ đó không hoàn thành một cách trọn vẹn.

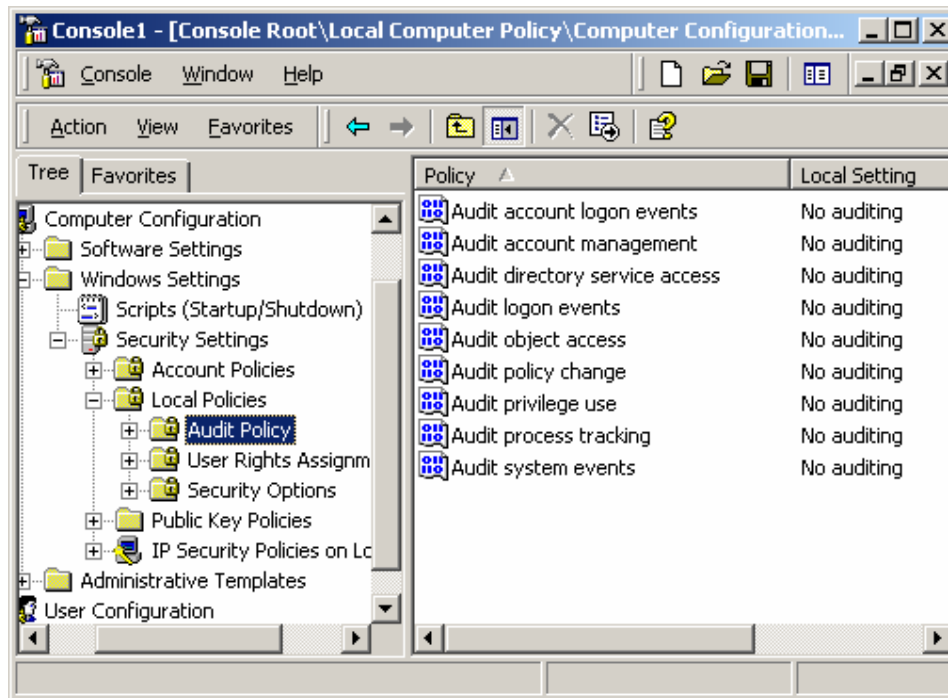
Bình thường thì việc kiểm định không hoạt động và nó phải được người dùng cấu hình. Khi việc kiểm định được cấu hình bạn sẽ thấy kết quả kiểm định thông qua tiện ích Even Viewer (Tiện ích Even Viewer được đề cập đến trong chương 15 “Thi hành các chức năng phục hồi hệ thống”

Kiểm định nhiều sự kiện quá sẽ làm giảm khả năng thực hiện của hệ thống nguyên nhân là do yêu cầu xử lý cao của nó. Việc kiểm định cũng có thể sử dụng quá mức không gian đĩa để lưu trữ nhật ký kiểm định. Bạn hãy sử dụng các tiện ích một cách hiệu quả

Hình 5.6 biểu diễn các chính sách kiểm định và diễn giải trong bảng 5.4

**HÌNH 5.6** Các chính sách kiểm định





**BẢNG 5.4 Các lựa chọn chính sách kiểm định**

Chính sách	Diễn giải
Audit Account Logon Events	Lưu lại vết khi người dùng đăng nhập, thoát khỏi hệ thống hoặc tạo ra liên kết mạng
Audit Account Management	Lưu lại vết việc tạo, xóa và quản lý tài khoản người dùng và nhóm người dùng
Audit Directory Service Access	Lưu lại vết truy cập phục vụ thư mục
Audit Logon Events	Kiểm định các sự kiện liên quan đến đăng nhập, như chạy kịch bản đăng nhập hoặc là việc truy cập hiện trạng máy tính
Audit Object Access Audit Policy Change	Kiểm định truy cập các tệp, thư mục và máy in Lưu lại vết bất kỳ sự thay đổi nào về chính sách kiểm định
Audit Privilege Use	Lưu lại vết bất kỳ sự thay đổi người có thể hoặc không thể hoặc được xem kết quả của việc kiểm định
Audit Process Tracking	Lưu lại vết các sự kiện như kích hoạt một chương trình truy cập một đối tượng và thoát khỏi một tiến trình

Audit System Events

Lưu lại vết các sự kiện hệ thống như tắt máy, khởi động lại máy giống như các sự kiện liên quan đến **Security log** trong **Event Viewer**

Trong bài tập 5.4 bạn sẽ cấu hình các chính sách kiểm định và xem kết quả

## **BÀI TẬP 5.4**

Thiết lập các chính sách kiểm định

1. Chọn Start ► Programs ► Administrative Tools ► Securyti và mở mục Local Computer Policy.
2. Mở các lần lượt các thư mục : Computer Configuration, Windows Settings, Securyti Settings, Local Policies, Audit Policy.
3. Mở chính sách Audit Account Logon Events. Trong trường Local Policy Setting, chỉ định Audit These Attempts, Chọn Success và Failure. Bấm nút OK.
4. Mở chính sách Audit Account Management. Trong trường Local Policy Setting, chỉ định Audit These Attempts, Chọn Success và Failure. Bấm nút OK.
5. Thoát khỏi hệ thống và thử truy cập với tên người dùng KevinD. Việc đăng nhập sẽ thất bại (vì không có tài khoản nào có tên là KevinD).
6. Đăng nhập lại hệ thống với tên người dùng là Administrator. Mở MMC và mở Event Viewer (xem bài tập 5.1)
7. Từ Event Viewer mở Security log. Bạn sẽ thấy các sự kiện được kiểm định được liệt kê trong bản ghi này

### **Ấn định quyền người dùng**

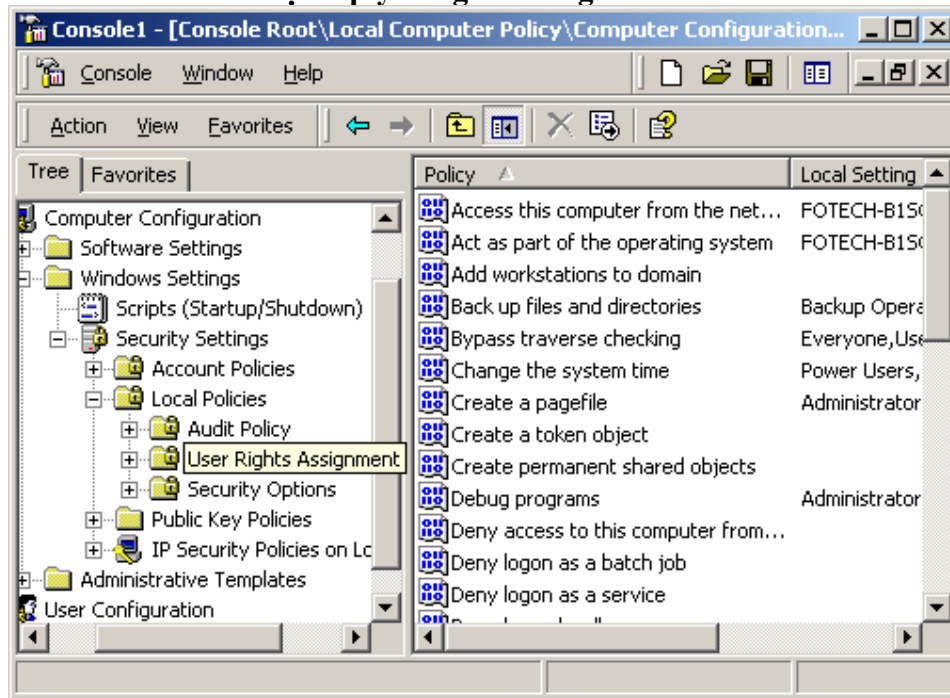
Các chính sách về quyền người dùng xác định tính hợp pháp một người dùng hoặc một nhóm người dùng trong máy tính. Quyền người dùng tham gia vào hệ thống. Nó không giống như sự cho phép, nó chỉ áp dụng cho các đối tượng được chỉ định. (Sự cho phép được đề cập đến trong chương 7, "Truy cập tệp và thư mục")

Ví dụ như một quyền người dùng chỉ được quyền Back Up Files và Directories. Nó cho phép người dùng sao lưu tệp và các thư mục dù là người dùng đó không có quyền đi qua các tệp hệ thống. Các quyền người dùng khác cũng tương tự bởi vì chúng được phân phối truy cập hệ thống chỉ định để truy cập tài nguyên.

Hình 5.7 hiện các chính sách ấn định quyền người dùng và các diễn giải trong bảng 5.5

HÌNH 5.7

Các chính sách ấn định quyền người dùng



Quyền	Diễn giải
Access This Computer from the Network	Cho phép người dùng truy cập máy tính từ mạng
Act as Part of the Operating System	Cho phép sự xác nhận mức thấp phục vụ việc xác minh với bất kỳ người dùng nào
Add Workstations to the Domain	Cho phép người dùng tạo tài khoản truy cập vào domain
Back Up File and Directories	Cho phép người dùng sao lưu tất cả các tệp và các thư mục bất kể có sự cho phép về tệp hay thư mục đó có được đặt hay không
Bypass Traverse Checking	Cho phép người dùng duyệt cây thư mục cho dù người dùng đó không được phép liệt kê các thành phần thư mục
Change the System Time	Cho phép người dùng thay đổi thời gian trong máy tính
Create a Pagefile	Cho phép người dùng thay đổi kích thước trang tệp

Create Permanent Shared Object	Cho phép một tiến trình tạo một mã thông báo nếu tiến trình sử dụng NtCreate Token API
Debug Programs	Cho phép người dùng đính kèm chương trình gỡ rối vào bất kỳ một tiến trình
Deny Access to This Computer from the Network	Cho phép bạn từ chối những người dùng chỉ định hoặc nhóm người dùng truy cập vào máy tính từ mạng
Deny Logon as a Batch File	Cho phép bạn ngăn những người dùng chỉ định hoặc nhóm người dùng đăng nhập với tệp batch (batch file)
Deny Logon as Service	Cho phép bạn ngăn những người dùng chỉ định hoặc nhóm người dùng đăng nhập với các phục vụ
Deny Logon Locally	Cho phép bạn từ chối những người dùng chỉ định hoặc nhóm người dùng truy cập vào nội bộ máy tính.
Enable Computer and User Accounts to Be Trusted by Delegation	Cho phép người dùng hoặc nhóm người dùng thiết lập Trusted by Delegation cho người dùng hoặc đối tượng máy tính
Force Shutdown from a Remote System	Cho phép hệ thống có thể tắt bởi người dùng tại vị trí từ xa trên mạng
Generate Security Audits	Cho phép người dùng, nhóm người dùng hoặc tiến trình để tạo các mục vào trong Security log
Increase Scheduling Priority	Cho phép người dùng thao tác các tiến trình được phục vụ bởi việc thực hiện các hạn ngạch xử lý
Load and Unload Device Drivers	Cho phép người dùng tự động gỡ và nạp các trình điều khiển thiết bị Plug-and-Play
Lock Page in Memory	Quyền người dùng không được sử dụng trong Windows 2000 (nó dự kiến bắt buộc dữ liệu được giữ trong bộ nhớ vật lý và không cho phép dữ liệu được phân trang vào các tệp trang

Log On as Batch Job	Cho phép một tiến trình đăng nhập hệ thống và chạy một tệp bao gồm một hoặc nhiều lệnh thao tác hệ thống
Log On as Service	Cho phép phục vụ đăng nhập hệ thống hợp lệ chạy các phục vụ được chỉ định
Log On as Locally	Cho phép người dùng đăng nhập vào máy tính nơi mà tài khoản người dùng đã được định nghĩa.
Manage Auditing and Security Log	Cho phép người dùng quản lý Security log
Modify Firmware Environment Variables	Cho phép n hoặc một tiến trình thay đổi môi trường hệ thống
Profile Single Process	Cho phép người dùng giám sát tiến trình phi hệ thống thông qua các công cụ như Performance Logs và tiện ích Alerts
Profile System Performance	Cho phép người dùng giám sát các tiến trình hệ thống thông qua các công cụ như Performance Logs và tiện ích Alerts
Remove Computer from Docking Station	Cho phép người dùng tách rời một máy tính xách tay thông qua giao diện người dùng Windows 2000
Replate a Process Level Token	Cho phép một tiến trình thay thế mã thông báo mặc định bởi mã được tạo tiến trình con với mã thông báo được chỉ định
Restore File and Directories	Cho phép người dùng khôi phục các tệp và các thư mục bất chấp sự cho phép về tệp và thư mục
Shut Down the System	Cho phép người dùng tắt máy từ tại máy hiện tại
Synchronize Directory Service Data	Cho phép người dùng đồng bộ hoá dữ liệu được kết hợp với phục vụ thư mục

Take Ownership of Files or Other Objects

Cho phép người dùng giữ quyền sở hữu các đối tượng hệ thống

Trong bài tập 5.5, bạn sẽ áp dụng chính sách ấn định các quyền người dùng nội bộ

## BÀI TẬP 5.5

Thiết lập các quyền người dùng nội bộ

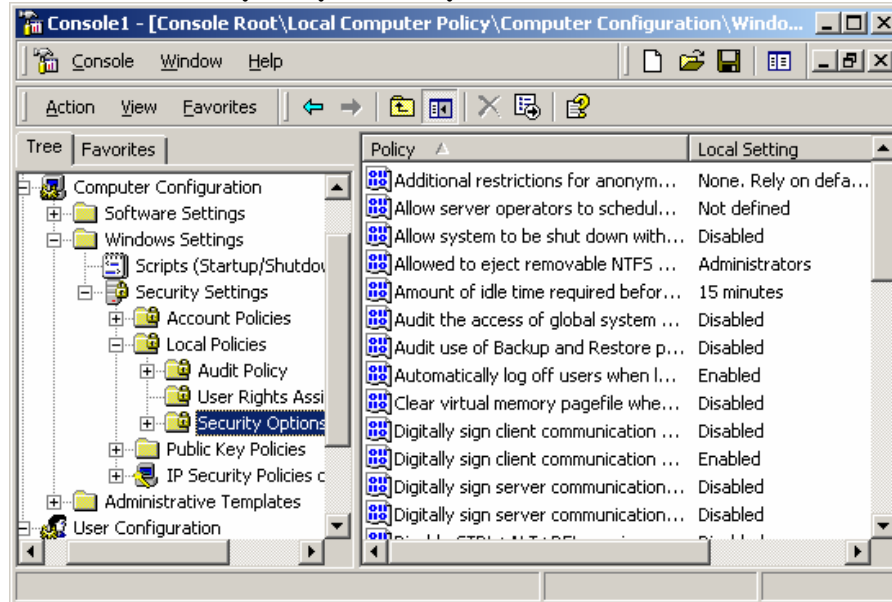
1. Chọn Start ► Program ► Administrative Tools ► Security và mở mục Local Computer Policy
2. Mở lần lượt các thư mục: Computer Configuration, Windows Settings, Security Settings, Local Policies, User Rights Assignment.
3. Mở quyền người dùng Log On as a Service. Hộp hội thoại Local Security Policy Setting xuất hiện.
4. Bấm nút Add. Hộp hội thoại Select Users or Group xuất hiện.
5. Chọn người dùng Emily. Bấm nút Add, sau đó bấm nút OK

### Định nghĩa các lựa chọn bảo mật

Các lựa chọn bảo mật được sử dụng để thiết lập sự bảo mật cho máy tính. Không giống như các chính sách về quyền người dùng được sử dụng cho 1 người hoặc 1 nhóm người dùng, các chính sách về cơ chế bảo mật chỉ áp dụng cho máy tính.

Hình 5.8 chỉ ra các chính sách lựa chọn bảo mật, các chính sách này được miêu tả ở bảng 5.6

HÌNH 5.8 Các chính sách lựa chọn bảo mật



**BẢNG 5.6 Các lựa chọn bảo mật**

Lựa chọn	Miêu tả	Giá trị mặc định
Additional Restrictions for Anonymous Users	Cho phép thêm các hạn chế cho các kết nối ẩn	Không có
Allow Server Operators to Schedule Tasks (domain controller only)	Cho phép người quản lý Server lên lịch làm việc xác định để chỉ ra thời gian chỉ định hoặc khoảng thời gian nghỉ	Không xác định
Allow System to Be Shut Down Without Having Logon	Cho phép người dùng thoát khỏi hệ thống mà không nhất thiết người đó phải đăng nhập vào hệ thống	Cho phép( nhưng sự thiết lập chính sách cục bộ bị ghi đè lên nếu nếu các thiết lập chính sách của mức domain được cài đặt Administrator
Allow to Eject Removable NTFS Media	Cho phép đóng các phương tiện NTFS có thể di chuyển được	
Amount of Time Idle Before Disconnecting Sesion	Cho phép các phiên làm việc ngừng kết nối khi chúng rời	15 phút
Audit the Access of Global System Object	Cho phép truy nhập vào đối tượng hệ thống bao trùm để kiểm định	Vô hiệu
Audit Use of All User Rights including Backup and Restore Privilege	Cho phép quyền người dùng, bao gồm các đối tượng sao lưu dữ liệu phải được kiểm định	Vô hiệu
Automatically Log Off User when Logon Time Expires	Tự động kết thúc phiên làm việc của người dùng nếu họ đã hết thời gian đăng nhập vào hệ thống	Cho phép

Clear Virtual Memory Pagefile when System Shutdown	Chỉ định rằng trang (của bộ nhớ ảo) sẽ được xoá hết khi hệ thống tắt	Vô hiệu
Digitally Sign Client Communication (always)	Chỉ định rằng Server luôn giao tiếp với client bằng tín hiệu số	Vô hiệu
Digitally Sign Client Communication (when possible)	Chỉ định rằng Server giao tiếp với client bằng tín hiệu số khi có thể	Cho phép
Digitally Sign Server Communication (always)	Đảm bảo rằng các giao tiếp của Server luôn là tín hiệu số	Vô hiệu
Digitally Sign Server Communication (when possible)	Đảm bảo rằng các giao tiếp của Server là tín hiệu số khi có thể	Vô hiệu
Disable CTRL+ALT+DEL Requirement for Logon	Cho phép vô hiệu hóa yêu cầu nhấn CTRL+ALT+DEL để đăng nhập vào hệ thống	Không xác định
Do Not Display Last User Name in Logon Screen	Không hiện tên của người dùng cuối trên màn hình đăng nhập vào hệ thống	Vô hiệu
LAN Manager Authentication Level	Chỉ định cấp độ xác nhận người quản lý mạng cục bộ.	Gửi phản hồi của nhà quản lý mạng LAN và NTLM( NT LAN Manager)
Message Text for User Attempting to Logon	Hiển thị dòng thông báo khi người dùng đang cố đăng nhập vào hệ thống	Dòng trống

Message Title for User Attempting to Logon	Hiển thị tiêu đề thông báo khi người dùng đang cố đăng nhập vào hệ thống	Dòng trống
Number of Previous Logon Attempts to Cache (in case domain controller is available)	Chỉ định số lần cố gắng đăng nhập được lưu trong bộ nhớ đệm	10
Prevent System Maintenance of Computer Account Password	Ngăn chặn sự thi hành hệ thống của các tài khoản máy tính	Vô hiệu
Prevent Users from installing print drivers	Ngăn không cho người sử dụng cài đặt các trình điều khiển máy in	Vô hiệu
Prompt User to change Password Before Expiration	Nhắc người dùng thay đổi mật khẩu trước khi mật khẩu hết hạn	14 ngày trước khi hết hạn mật khẩu
Recovery console: Allow Automatic Administrative Logon	Chỉ định rằng khi Recovery Console được nạp, đăng nhập của nhà quản trị phải là tự động, không phải tự đăng nhập nữa	Vô hiệu
Recovery console: Allow Floppy Copy and Access to All Drives and Folders	Cho phép sao chép các tệp từ tất cả các ổ đĩa và các thư mục khi Recovery Console được nạp	Vô hiệu
Rename Administrator Account	Cho phép tài khoản Administrator có thể đổi tên	Không xác định
Rename Guest Account	Cho phép tài khoản Guest có thể đổi tên	Không xác định

Restrict CD-ROM Access Locally Logged-on users only	Hạn chế những người dùng đăng nhập cục bộ truy cập vào CD-ROM	Vô hiệu
Restrict Floppy Access Locally Logged-on users only	Hạn chế những người dùng đăng nhập cục bộ truy cập vào ổ đĩa mềm	Vô hiệu
Secure Channel: Digitally Encrypt or Sign Secure Channel Data (always)	Chỉ định rằng dữ liệu kênh an toàn luôn được mã số hoá hoặc tín hiệu số hoá	Vô hiệu
Secure Channel: Digitally Encrypt Secure Channel Data (when possible)	Chỉ định rằng dữ liệu kênh an toàn được mã số hoá khi có thể	Vô hiệu
Secure Channel: Digitally Sign Secure Channel Data (when possible)	Chỉ định rằng dữ liệu kênh an toàn được tín hiệu số hoá khi có thể	Cho phép
Secure Channel: Require Strong (Windows 2000 or later) Session Key	Cung cấp một kênh đảm bảo và yêu cầu một khoá phiên làm việc tốt (trong Windows 2000 hoặc phiên bản cũ)	Vô hiệu
Send Unencrypted Passwords to Connect to Third-Party SMB Servers	Cho phép mật khẩu không được mã hoá kết nối đến Third-party SMB Server	Vô hiệu
Shut Down System immediately if Unable to Log Security Audits	Chỉ định rằng hệ thống tắt ngay lập tức nếu nó không thể ghi lại sự kiểm định bảo mật	Vô hiệu

Smart Card Removal Behavior	Thay đổi sự giao tiếp với thẻ thông minh	Không hành động
Strengthen Default Permission of Global System Object (e.g. Symbolic Links)	Làm tăng sự cho phép mặc định của đối tượng hệ thống toàn cục	Cho phép
Unsigned Driver Installation Behavior	Điều khiển sự cài đặt các thiết bị không được đánh dấu	Cảnh báo nhưng cho phép cài đặt
Unsigned Non-Driver Installation Behavior	Điều khiển sự cài đặt của các Non-Driver được đánh dấu	



Chú ý

nếu bạn thay đổi các chính sách bảo mật và chú ý rằng các thay đổi của bạn không có tác dụng, nó có thể do đã có chính sách của nhóm được áp dụng định kỳ. bạn có thể ép các chính sách của bạn được cập nhật bằng cách gõ: `secedit / refreshpolicy machine_policy` tại dấu nhắc dòng lệnh

Trong bài tập 5.6 bạn sẽ định nghĩa một số chính sách lựa chọn bảo mật và xem chúng làm việc như thế nào. Coi như bạn đã hoàn thành các bài tập ở phần trước trong chương này.

## BÀI TẬP 5.6

Định nghĩa các lựa chọn bảo mật

1. Chọn Start ► Programs ► Administrative Tools ► Security và mở mục Local Computer Policy
2. Mở các thư mục sau: Computer Configuration, Window Settings, Local Policies, Security Options.
3. Mở chính sách Message Text for Users Attempting to Log On. Trong trường Local Policy Setting gõ Wellcom to all authorized user. Bấm nút OK.
4. Mở chính sách Prompts Uer to Changes Password Before Expiration. Trong trường Local Policy Setting. Chỉ định 3 ngày. Bấm nút OK
5. Chọn Start ► Program ► Accessories ► Command Prompt. Tại dấu nhắc lệnh gõ: **secedit /refesholicy machine\_policy** và nhấn phím Enter.
6. Tại dấu nhắc lệnh gõ **exit** và nhấn phím Enter.
7. Thoát khỏi hệ thống và đăng nhập với tên người dùng **Michael** (với mật khẩu **apple** )
8. Thoát khỏi hệ thống và đăng nhập với tên người dùng Administrator

## Sử dụng các chính sách hệ thống

Thông qua các chính sách hệ thống, bạn có thể điều khiển cấu hình hệ thống máy tính và môi trường làm việc của người dùng. Họ làm việc bằng cách soạn thảo Registry tương ứng với việc thiết lập chính sách. Bạn có thể đặt các chính sách hệ thống cho những người dùng, nhóm và máy tính riêng biệt như tất cả người dùng và tất cả máy tính

### Microsoft Exam Objective

#### Thi hành, cấu hình, quản lý và gỡ rối các chính sách trong môi trường Windows 2000

- Thi hành, cấu hình, quản lý và gỡ rối các chính sách cục bộ trong môi trường Windows 2000
- Thi hành, cấu hình, quản lý và gỡ rối các chính sách hệ thống trong môi trường Windows 2000

Các chính sách hệ thống thường được liên quan tới Window NT 4. Window 2000 đề nghị bạn sử dụng Group Policy để quản lý việc thiết đặt nền màn hình của người dùng như đã giải thích phần trước. Mặc dù vậy, bạn vẫn có thể sử dụng System Policy Editor (POLEDIT) để quản lý các chính sách hệ thống trong Windows 2000. Các tệp chính sách hệ thống làm việc như sau trong dòng hệ điều hành Windows:

- Các tệp chính sách hệ thống đã tạo trong Windows 2000 hoặc Windows NT 4 sẽ làm việc với các máy khách Windows 2000 và Windows NT 4.
- Các tệp chính sách hệ thống đã tạo trong Windows 98 hoặc Windows 95 sẽ làm việc với các máy khách Windows 98 hoặc Windows 95.

Thông qua System Policy Editor, bạn có thể cấu hình các chính sách hệ thống theo các bước sau:

**Người dùng mặc định:** Chọn mặc định cho bất cứ người dùng nào đăng nhập vào từ máy tính NT (ghi vào khóa HKEY\_CURRENT\_USER của Registry)

**Người dùng:** Cho phép bạn tạo các chính sách hệ thống theo yêu cầu cho người dùng cụ thể (ghi vào khóa HKEY\_CURRENT\_USER của Registry)

**Nhóm:** Những người sử dụng giống nhau các chính sách hệ thống, nhưng cho phép bạn áp dụng các chính sách hệ thống đến các nhóm người dùng (ghi vào khóa HKEY\_CURRENT\_USER của Registry)

**Default Computer :** Chỉ định thiết lập mặc định cho bất kỳ máy tính Windows 2000 hoặc Windows NT 4 trong miền ( ghi vào khoá HKEY\_LOCAL\_MACHINE của Registry)

**Computer :** Cho phép bạn tạo các chính sách tùy ý cho một máy tính cụ thể (ghi vào khoá HKEY\_LOCAL\_MACHINE của Registry)

Mặc định rằng không chính sách hệ thống nào được sử dụng trừ khi người quản trị tạo ra chúng.

Trong phần tiếp theo, bạn sẽ học cách chọn để có thể cấu hình các



chính sách người dùng hoặc nhóm người dùng và các lựa chọn được quản lý thông qua các chính sách máy tính

Để mà quản lý các chính sách hệ thống cho các người dùng và nhóm người dùng chỉ định, máy tính cài Windows 2000 Server của bạn phải được cấu hình là **domain controller**

### Cấu hình các chính sách hệ thống người dùng và nhóm người dùng

Các chính sách đó bạn có thể áp dụng cho tất cả mọi người dùng (thông qua biểu tượng Default User), đến người dùng chỉ định hoặc đến một nhóm người dùng, nó cho phép bạn điều khiển màn hình nền và các thiết lập hệ thống. các lựa chọn chính sách hệ thống của người dùng và nhóm người dùng được diễn giải trong bảng 5.7



Các chính sách hệ thống nhắc đến WindowsNT vì chúng được thiết kế chủ yếu để điều khiển máy khách NT để tương thích với các thế hệ trước

**BẢNG 5.7** Các lựa chọn chính sách hệ thống người dùng và nhóm người dùng

Chính sách	Lựa chọn
Control Panel	Cho phép bạn chỉ định thiết lập việc hiển thị như ẩn Screen Saver và Appearance của hộp thoại Display Properties
Desktop	Cho phép bạn cấu hình hình ảnh nền và cách phối màu.
Shell	Cho phép bạn cấu hình sự hạn chế như việc ẩn Network Neighborhood và không ghi các thiết lập khi người dùng thoát
System	Cho phép bạn đặt các hạn chế như làm vô hiệu các công cụ soạn thảo Registry và chỉ cho phép chạy các ứng dụng Windows
WindowsNT Shell	Cho phép bạn cấu hình các thư mục Window NT và chỉ định hạn chế liên quan đến NT shell
WindowsNT System	Cho phép bạn chỉ định dù có phân tích được hay không tệp AUTOEXEC.BAT và dù có chạy đồng bộ hoá các kịch bản đăng nhập

Mặc định, hệ thống khoá các chính sách hệ thống domain controller xác định trong NETLOGON dùng chung tệp NTCONFIG.POL. Nếu bạn muốn các chính sách hệ thống của bạn phải có hiệu lực trong hệ thống rộng, bạn phải lưu ý và chia sẻ tệp này vì nó được chỉ định do người dùng khi chính sách hệ thống được tạo ra.

### Quy định các chính sách hệ thống phù hợp

Dựa theo các điều kiện, quy định chính sách hệ thống sẽ được sử

dùng nếu người dùng có nhiều chính sách hệ thống được định nghĩa do người dùng hoặc do các thành viên của nhóm.

- Nếu người dùng có cấu hình tùy chọn chính sách hệ thống sẽ được sử dụng và các chính sách hệ thống này trong HKEY\_CURRENT\_USER của Registry. Điều này cho phép chỉ định các chính sách người dùng để lấy thứ tự lên trên bất kỳ các chính sách hệ thống người dùng mặc định hoặc nhóm đang tồn tại. Điều này có nghĩa là các chính sách hệ thống của 1 nhóm sẽ không được sử dụng nếu tồn tại một chính sách hệ thống của một người dùng.
- Nếu người dùng là thành viên của bất kỳ nhóm nào có cấu hình các tùy chọn chính sách hệ thống và không có bất kỳ lựa chọn chính sách hệ thống cho người dùng được định nghĩa. Các chính sách hệ thống nhóm sẽ được hợp nhất vào phần HKEY\_CURRENT\_USER trong Registry bởi thứ tự ưu tiên. Nếu có nhiều chính sách nhóm được định nghĩa, nó có thể xác định quyền ưu tiên của nhóm trong các tùy chọn của System Policy Editor.
- Nếu người dùng không lựa chọn bất kỳ chính sách hệ thống người dùng hoặc chính sách hệ thống nhóm nào được áp dụng, khoá HKEY\_CURRENT\_USER sẽ được cập nhật với bất kỳ sự thay đổi nào được tạo ra bởi các chính sách hệ thống Default User.
- Nếu hiện trạng người dùng và chính sách hệ thống cùng được thể hiện có các thiết lập xung đột cho các lựa chọn giống nhau, các lựa chọn chính sách hệ thống sẽ ghi đè lên cấu hình hiện trạng người dùng trong Registry.

Ví dụ : thừa nhận rằng Lars là một thành viên của các nhóm HR và Managers. Anh ta có các chính sách hệ thống người dùng thiết lập cho Lars và chính sách hệ thống nhóm được thiết lập cho HR mà Managers. Chính sách hệ thống nhóm cho Managers cao so với của HR. Các tùy chọn chính sách hệ thống người dùng và nhóm người dùng được cấu hình được liệt kê như sau:

Tùy chọn	HR	Manager	Lars
Color Schema	Xanh lá cây 256	Hồng 256	Xanh và đen
Hide Screen Saver Tab in Control Panel	Không thiết lập	Không thiết lập	Ân
Hide Apperance Tab in Control Palnel	Không thiết lập	Không thiết lập	Ân

Shell Restriction, Hide Network Neighborhood	Không thiết lập	Ấn	Không thiết lập
Shell Restriction, Save Setting on Exit	Không thiết lập	Ấn	Không thiết lập

### **Cơ sở của các chính sách hệ thống**

Tùy chọn	Các chính sách được so sánh với Lars
Color Schema	Xanh và đen (thông qua Lars thiết lập)
Hide Screen Saver Tab in Control Panel	Ấn (thông qua Lars thiết lập)
Hide Appearance Tab in Control Panel	Ấn (thông qua Lars thiết lập)
Sell Restriction, Hide Network Neighborhood	Không thiết lập (các chính sách hệ thống người dùng không sử dụng nếu các chính sách hệ thống tông tại)
Shell Restriction, Save Setting on Exit	Không thiết lập (các chính sách hệ thống người dùng không sử dụng nếu các chính sách hệ thống tông tại)

### **Tạo các chính sách hệ thống cho người dùng hoặc nhóm người dùng .**

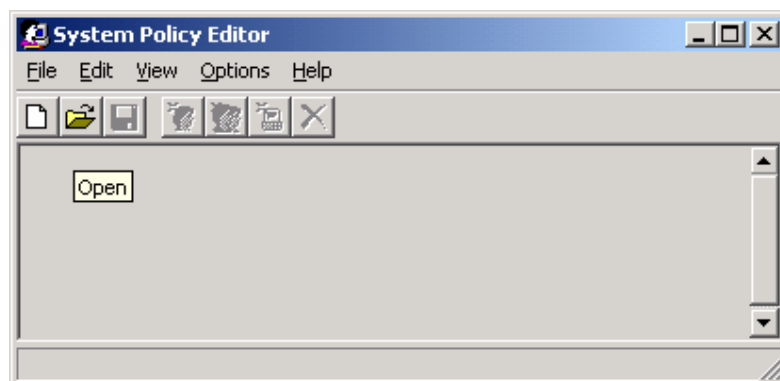


Nó rất dễ sử dụng cho soạn thảo câu hình người dùng thông qua System Policy Editor, nó là giao diện đồ họa (GUI), hơn thế nó có thể soạn thảo trên cơ sở văn bản Registry, mặc dù vậy. khi bạn sử dụng System Policy Editor. bạn đang soạn Registry của bạn, nhưng bạn cần cẩn thận. Bạn nên sao lưu Registry của bạn trước khi thay đổi

Để cấu hình các chính sách hệ thống cho người dùng hoặc nhóm người dùng, hãy thực hiện theo các bước:

1. Chọn Start ► Run, gõ POLEDIT trong hộp hội thoại Run và bấm nút OK.
2. Cửa sổ System Policy Editor mở ra như trong hình 5.9. Chọn File ► New Policy

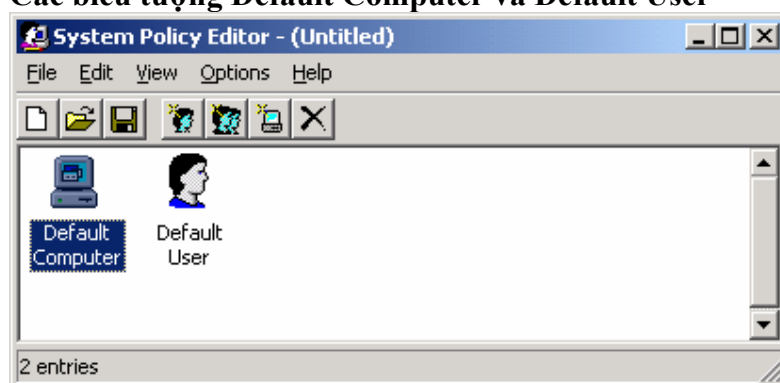
**HÌNH 5.9 System Policy Editor**



3. System Policy Editor hiển thị các biểu tượng cho Default Computer và Default User như hiển thị hình 5.10.

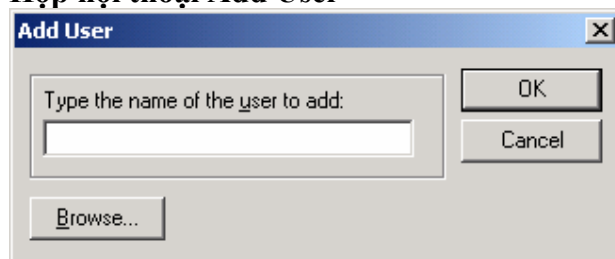
Chọn Edit ► Add User(hoặc Add Group)

**HÌNH 5.10 Các biểu tượng Default Computer và Default User**



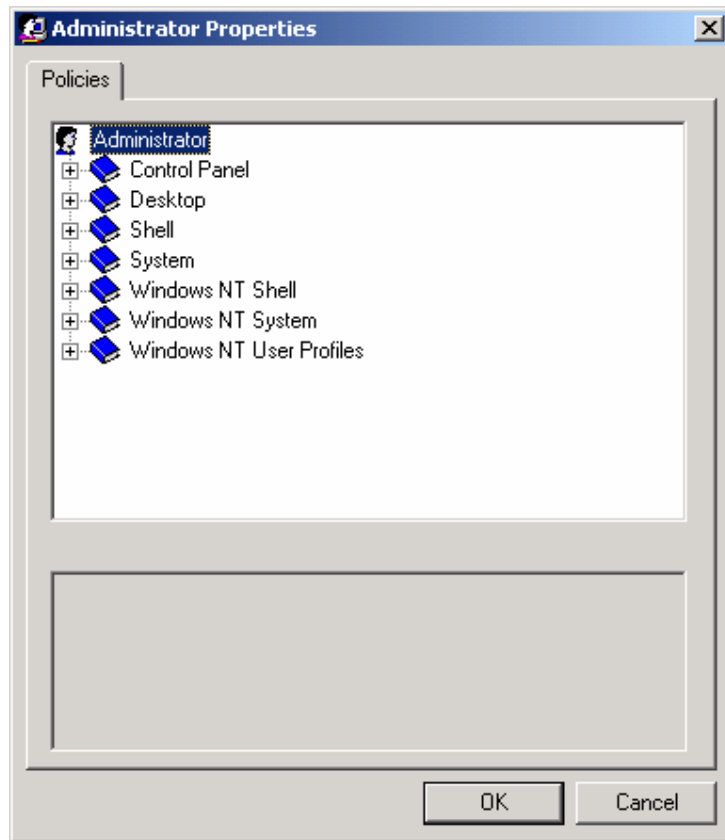
4. Hộp hội thoại Add User(hoặc Add Group) xuất hiện như trong hình 5.11. Bạn cần gõ tên của người dùng (hoặc của nhóm) hoặc bấm vào nút Browse để chọn từ danh sách các người dùng (hoặc nhóm người dùng) được liệt kê sẵn. Sau khi bạn thêm người dùng (hoặc nhóm người dùng) bấm phím OK

**HÌNH 5.11 Hộp hội thoại Add User**



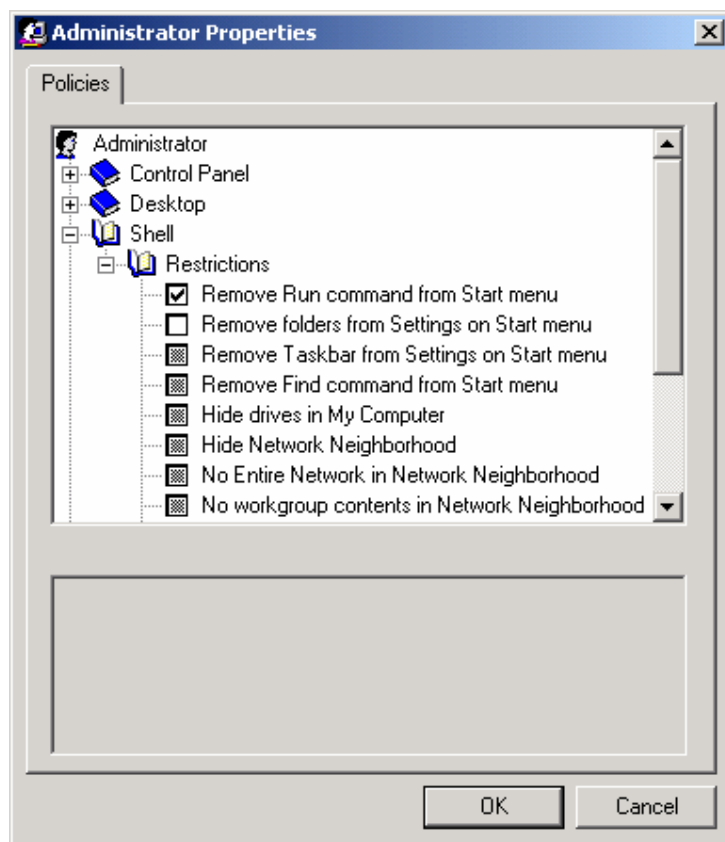
5. người dùng hoặc nhóm người dùng được bạn chọn xuất hiện trong cửa sổ System Policy Editor. Để soạn thảo hoặc hiển thị các thiết lập chính sách của người dùng (hoặc của nhóm người dùng) hãy nhấp kép vào người dùng hoặc nhóm người dùng).
6. Các chính sách sẽ được liệt kê trong phần Policies của hộp hội thoại Properties như trong hình 5.12 Bấm vào các lựa chọn mà bạn muốn cấu hình

**HÌNH 5.12 Các chính sách trong hộp hội thoại Properties của người dùng**



7. Bạn xem trong danh sách tất cả các chính sách bạn có thể định nghĩa. Hình 5.13 hiển thị một ví dụ về các chính sách Shell, Restriction. Bấm vào hộp chọn (checkbox) bạn có thể cấu hình mỗi lựa chọn như sau:
- Hộp chọn màu xám có nghĩa là không chính sách nào được áp dụng
  - Đánh dấu trong hộp chọn có nghĩa là chính sách đó được áp dụng. Coi như đó là giá trị đúng
  - Hộp chọn trống (hay trắng) có nghĩa là chính sách đó không được áp dụng. Coi như đó là giá trị sai

**HÌNH 5.13** Soạn thảo các chính sách hệ thống của người dùng



8. Lặp lại các bước 6 và 7 để cấu hình cho mỗi lựa chọn mà bạn muốn. Sau khi tất cả các lựa chọn được cấu hình Bấm nút Ok
9. Sau khi bạn kết thúc việc soạn thảo các chính sách về người dùng và nhóm người dùng, ghi lại các chính sách bằng cách chọn File ► Save

Trong bài tập 5.7 bạn sẽ cấu hình các chính sách hệ thống cho một người dùng. Trong bài này phải được thực hiện trên domain controller

#### BÀI TẬP 5.7

Tạo các chính sách hệ thống cho một người dùng

1. Sử dụng tiện ích Active Directory Users and Computer để tạo một người dùng Lars (Xem chương 4 “Quản lý người dùng và nhóm người dùng” để xem chi tiết việc tạo tài khoản người dùng)
2. Chọn Start ► Run, gõ POLEDIT trong hộp hội thoại Run và bấm nút OK
3. Trong cửa sổ System Policy Editor chọn File ► New Policy.
4. Chọn Edit ► Add User. Trong hộp hội thoại Add User bấm vào nút Browse. Chọn người dùng Lars và bấm nút Add, Sau đó bấm nút OK.
5. Nhấp kép vào người dùng Lars. Trong thành phần giao tiếp Policy chọn Shell tiếp đó là Restrictions. Đánh dấu hộp chọn Remove Run Command from Start Menu và hộp chọn Hide Drives in My Computer. Sau đó bấm nút OK
6. Chọn File ► Save trong hộp hội thoại Save As chọn

## Cấu hình các chính sách hệ thống máy tính

Bạn cũng cần quản lý thiết lập máy tính thông qua các chính sách hệ thống. Sau đây là một số các lựa chọn mà bạn có thể cấu hình:

- Thiết lập mạng được sử dụng để điều khiển cập nhật chính sách hệ thống
- Thiết lập hệ thống được sử dụng chạy các mục lúc khởi động
- Thiết lập Windows NT Network để điều khiển cách các sự chia sẻ thiết bị ẩn được tạo
- Thiết lập Windows NT Printers để điều khiển lựa chọn cấu hình máy in
- Thiết lập Windows NT Remove Access để điều khiển lựa chọn truy cập từ xa
- Thiết lập Windows NT Shell để điều khiển các mục đối tượng được khách hàng chia sẻ như các mục trong Desktop và trong thực đơn Start
- Thiết lập Windows NT System được sử dụng cấu hình đăng nhập và thiết lập tệp hệ thống
- Thiết lập Windows NT User Profiles được sử dụng cấu hình các thiết lập hiện trạng người dùng

## Sử dụng công cụ Security Configuration and Analysis

Windows 2000 Server bao gồm một tiện ích được gọi là Security Configuration and Analysis, bạn có thể sử dụng để phân tích nhằm hỗ trợ việc cấu hình các thiết lập bảo mật nội bộ trong máy tính.

Tiện ích này làm việc bằng cách so sánh cấu hình bảo mật hiện thời của bạn với cấu hình mẫu trong các thiết lập đề nghị của bạn

Microsoft **Thực thi, cấu hình, quản lý và gỡ rối vấn đề bảo mật bằng cách**  
Exam **sử dụng tập công cụ cấu hình bảo mật (Security Configuration**  
Objective **Tool Set)**

Tiến trình phân tích bảo mật gồm các bước sau:

1. Sử dụng tiện ích Security Configuration and Analysis, chỉ định cơ sở dữ liệu làm việc sẽ được sử dụng suốt thời gian phân tích bảo mật
2. Mở mẫu về bảo mật mà bạn sử dụng làm nền tảng để bạn cấu hình sự bảo mật tương tự như mẫu này
3. Thực hiện phân tích vấn đề bảo mật. Nó sẽ so sánh lại cấu hình của bạn với mẫu mà bạn đã chỉ định trong bước 2
4. Xem lại kết quả của việc phân tích
5. Quyết định bất cứ sự khác nhau nào được chỉ ra thông qua kết quả phân tích.

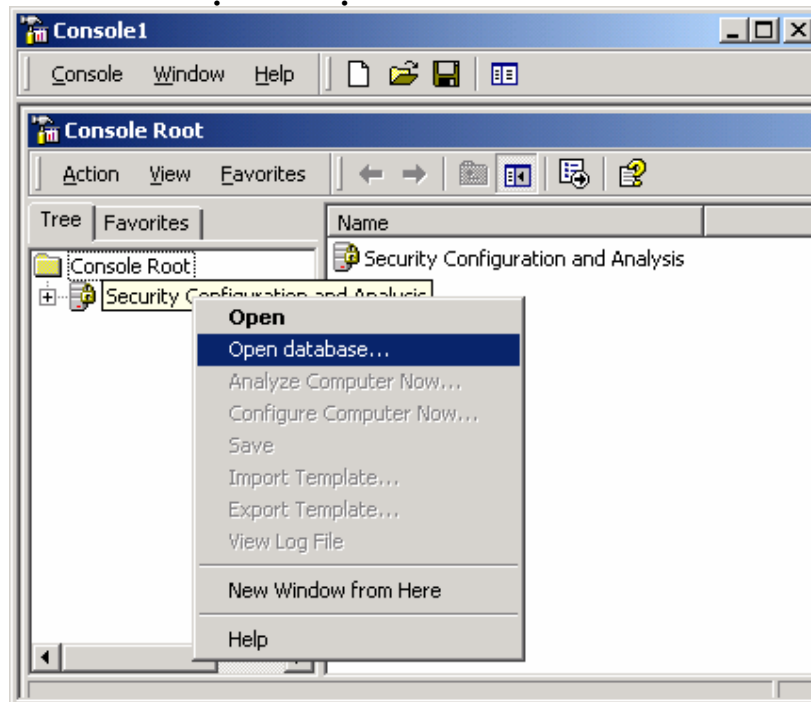
Tiện ích Security Configuration and Analysis có trong MMC. Sau khi bạn thêm tiện ích này vào trong MMC, bạn có thể chạy tiến trình phân tích bảo mật, nó được diễn giải trong phần tiếp theo

## Chỉ định cơ sở dữ liệu bảo mật

Cơ sở dữ liệu bảo mật được sử dụng để lưu trữ kết quả phân tích bảo mật của bạn. Để chỉ định cơ sở dữ liệu bảo mật hãy thực hiện theo các bước sau:

1. Trong MMC bấm chuột phải vào Security Configuration and Analysis và chọn Open Database từ menu như trong hình 5.14

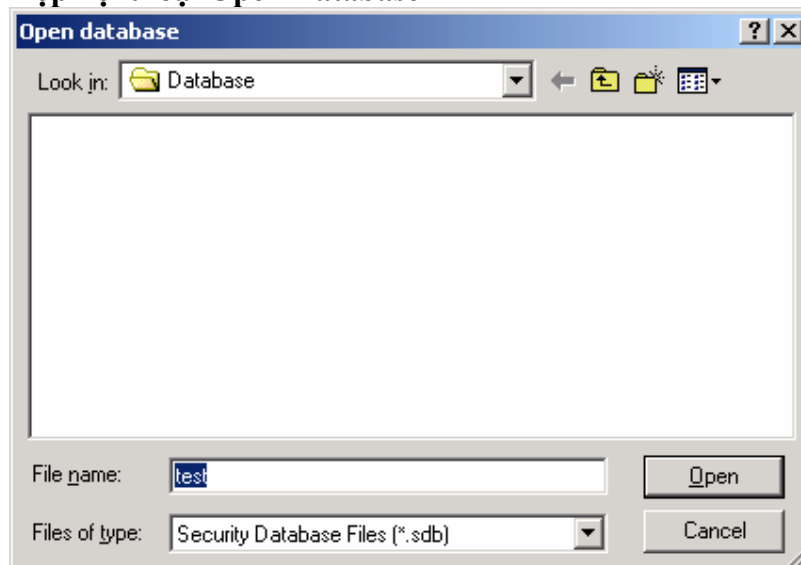
**HÌNH 5.14** Mở cơ sở dữ liệu bảo mật



Hộp hội thoại Open Database sẽ xuất hiện như trong hình 5.15.

Trong ô Filename gõ tên tệp cơ sở dữ liệu bạn sẽ tạo. Mặc định phần mở rộng của tệp là .sdb (cho cơ sở dữ liệu bảo mật). Bấm nút OK

**HÌNH 5.15** Hộp hội thoại Open Database



2. Hộp hội thoại Import Template mở ra, chọn mẫu mà bạn

muốn sử dụng. Bạn có thể chọn các mẫu định nghĩa sẵn thông qua hộp hội thoại này. Trong phần tiếp theo, bạn sẽ học cách tạo ra và sử dụng các tệp mẫu tùy biến. Bạn chọn và bấm nút OK.

## Nhập Security Template (mẫu bảo mật)

Bước tiếp theo trong tiến trình phân tích bảo mật là nhập một mẫu về bảo mật. Mẫu này được sử dụng như công cụ so sánh. Tiện ích Security Configuration and Analysis so sánh thiết lập bảo mật của các thiết lập trong bản mẫu với các thiết lập hiện thời của bạn. Bạn không đặt bảo mật thông qua các mẫu. Đúng hơn là mẫu bảo mật chỉ là nơi mà bạn tổ chức tất cả các thuộc tính bảo mật của bạn trên vị trí đơn lẻ.



Với nhà quản trị, bạn có thể định nghĩa một bản mẫu về bảo mật trên máy đơn lẻ và chuyển chúng cho tất cả các máy chỉ thông qua mạng

### Tạo bản mẫu bảo mật

Bạn tạo bản mẫu bảo mật thông qua Security Templates trong MMC. Bạn có thể cấu hình nó với các mục như trong bảng 5.8

**BẢNG 5.8 Các lựa chọn cấu hình mẫu bảo mật**

Mục của mẫu bảo mật	Diễn giải
Account Policies	Chỉ định cấu hình phải được sử dụng cho các chính sách mật khẩu, các chính sách kiểm soát tài khoản thử đăng nhập và các chính sách Kerberos
Local Policies	Chỉ định cấu hình phải được sử dụng cho các chính sách kiểm định, các chính sách quyền người dùng và các lựa chọn bảo mật
Event Log	Cho phép bạn đặt thiết lập cấu hình áp dụng cho các tệp nhật ký của Event Viewer.
Restricted Groups	Cho phép bạn quản trị các thành viên của nhóm nội bộ
Registry	Chỉ định bảo mật cho các khoá Registry nội bộ
File System	Chỉ định bảo mật cho các tệp hệ thống nội bộ
System Services	Đặt cơ chế bảo mật cho các phục vụ hệ thống mô hình khởi động mà các phục vụ của hệ thống nội bộ sẽ được sử dụng

Sau khi bạn thêm Security vào MMC, bạn có thể mở 1 mẫu bảo mật đơn giản và thay đổi chúng như sau:

1. trong MMC bung nút Security Templates và mở thư mục cho

\Windir\Security\Templates.

2. Nhấp kép chuột vào bản mẫu mà bạn muốn soạn thảo bao gồm **basicv** (basic server) và **basicdc** (basic domain controller)
3. Tạo mọi sự thay đổi mà bạn muốn từ bản mẫu đơn giản này. Cúng thường chỉ là các chỉ định mà bạn muốn hệ thống được cấu hình.

Sau đó bạn ghi bản mẫu được lựa chọn, bấm chuột phải làm xuất hiện thực đơn và chọn tùy chọn Save As từ thực đơn này. Chỉ định vị trí và tên tệp cho bản mẫu mới này. Mặc định nó sẽ được ghi với phần mở rộng là .inf trong thư mục

\Windir\Security\Templates

### **Mở Security Template (mẫu bảo mật)**

Sau khi bạn cấu hình bản mẫu, bạn có thể nhập nó để sử dụng cùng tiện ích Security Configuration and Analysis. Để nhập mẫu bảo mật trong MMC, bấm chuột phải vào tiện ích Security Configuration and Analysis và chọn Import Template. Sau đó chọn tệp mà bạn muốn mở và bấm nút Open

### **Thực hiện phân tích bảo mật**

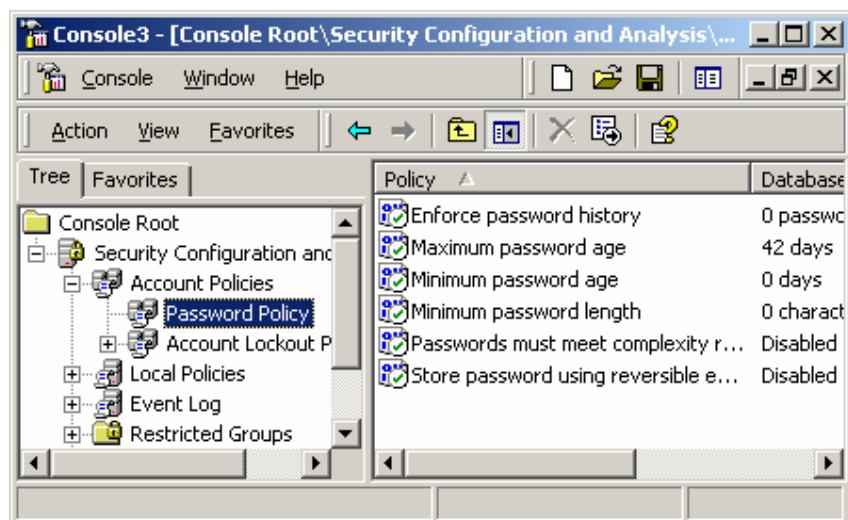
Bước tiếp theo là thực hiện phân tích bảo mật. Để thực hiện việc phân tích này, bấm chuột phải vào tiện ích Security Configuration and Analysis và chọn Analyze Computer Now. Bạn sẽ thấy hộp thoại Perform Analysis xuất hiện cho phép bạn chỉ định vị trí và tên tệp cho đường dẫn tệp lưu trữ các lỗi sẽ được phát sinh trong suốt quá trình phân tích. Sau khi các thông tin đã được cấu hình, bấm nút OK

Khi việc phân tích hoàn thành, bạn sẽ quay trở lại cửa sổ MMC chính. Từ đây bạn có thể xem kết quả của quá trình phân tích bảo mật

### **Hiển thị kết quả phân tích bảo mật và xác định những sự sai khác.**

Kết quả của việc phân tích bảo mật được lưu trữ trong Security Configuration and Analysis, dưới đối mục bảo mật được cấu hình (xem bảng 5.8) Ví dụ để xem kết quả của các chính sách mật khẩu, nhấp kép chuột vào Security Configuration and Analysis, nhấp kép chuột vào Account Policies và nhấp kép chuột vào Password Policy. Hình 5.16 hiển thị ví dụ của kết quả của sự phân tích bảo mật cho các chính sách mật khẩu

### **HÌNH 5.16 Hiển thị kết quả của sự phân tích bảo mật**



Các chính sách đã được phân tích sẽ có các dấu X hoặc √ tại mỗi chính sách như hiển thị trong hình 5.16. Dấu X có biểu thị chính sách mẫu và chính sách hiện thời là không tương ứng. Dấu √ có biểu thị chính sách mẫu và chính sách hiện thời là tương ứng. Nếu có bất kỳ sự trái ngược nào đã được biểu diễn, bạn phải sử dụng Group Policy để giải quyết sự tranh chấp ấy.

## BÀI TẬP 5.8

Sử dụng Security Configuration and Analysis

Ở bài tập này bạn sẽ thêm Security Configuration and Analysis vào MMC, chỉ định ra một cơ sở dữ liệu bảo mật, tạo một mẫu bảo mật, nhập mẫu bảo mật, thực hiện phân tích và xem xét kết quả.

Thêm tiện ích Security Configuration and Analysis

1. Chọn Start ► Programs ► Administrative Tools ► Security
2. Chọn Console ► Add/Remove Snap-in
3. Trong hộp hội thoại Add/Remove Snap-in bấm chuột vào nút Add. Chọn Security Configuration and Analysis rồi bấm vào nút Add. Rồi bấm vào nút Close
4. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK

Chỉ định cơ sở dữ liệu bảo mật

1. Trong MMC bấm chuột phải vào Security Configuration and Analysis, chọn Open Database
2. Trong hộp hội thoại Open Database gõ sampledb trong hộp nhập tên tệp. Sau đó bấm Open
3. Trong hộp hội thoại Import Template chọn mẫu baicsv và bấm nút Open

Tạo mẫu bảo mật

1. Trong MMC chọn Chọn Console ► Add/Remove Snap-in
2. Trong hộp hội thoại Add/Remove Snap-in bấm chuột vào nút Add. Chọn Security Template rồi bấm vào nút Add. Rồi bấm vào nút Close
3. Trong hộp hội thoại Add/Remove Snap-in bấm nút OK

4. Mở mục Security Template sau đó mở thư mục Window NT\Security\Templates
5. Nhấp đúp vào tệp basicsv
6. Chọn Account Policies, sau đó là Password Policy
7. Soạn thảo các chính sách mật khẩu theo các bước sau:
  - Đặt tùy chọn Enforce Password History là nhớ 10 mật khẩu.
  - Thiết lập tùy chọn Passwords Must Meet Complexity Requirements là cho phép
  - Đặt tuổi thọ tối đa là 30 ngày
8. Chọn tệp basicsv và bấm vào lựa chọn Save As
9. Trong hộp hội thoại Save As gõ tên tệp servertest vào thư mục mặc định. Bấm nút Save

#### Nhập mẫu bảo mật

1. Chọn Security Configuration and Analysis, bấm chuột phải và chọn Import Template
2. Trong hộp hội thoại Import Template chọn tệp servertest và bấm nút Open

#### Thực hiện và Xem xét kết quả phân tích bảo mật

1. Chọn Security Configuration and Analysis bấm chuột phải và chọn Analyze Computer Now
2. Trong hộp hội thoại Perform Analysis chấp nhận đường dẫn mặc định cho tệp ghi lại lỗi và bấm nút OK
3. Khi quay trở lại cửa sổ chính MMC nhấp đúp vào Security Configuration and Analysis.
4. Nhấp đúp vào Account Policies và nhấp đúp vào Password Policy. Bạn sẽ thấy kết quả của sự phân tích cho mỗi chính sách được chỉ định bởi dấu X và √ cạnh mỗi chính sách

## Tổng kết

Trong chương này bạn đã học được về các đặc tính của Windows 2000 Server. Nó bao phủ các chủ đề:

- Thiết lập bảo mật, nó có thể được áp dụng cho mức nội bộ hoặc mức miền. Việc quản lý các chính sách bảo mật nội bộ, sử dụng Group Policy với đối tượng Local Computer Group Policy. Để quản lý các chính sách bảo mật miền sử dụng Group Policy với đối tượng Domain Controller Group Policy.
- Các chính sách tài khoản điều khiển tiến trình đăng nhập. Có 3 loại chính sách tài khoản là mật khẩu, chính sách kiểm soát sự vi phạm đăng nhập và chính sách Kerberos.
- Các chính sách nội bộ điều khiển những cái mà bạn có thể làm với máy tính nội bộ. Có 3 loại chính sách gồm: kiểm định, ấn định quyền người dùng, và các chính sách lựa chọn bảo mật
- Các chính sách hệ thống được sử dụng định nghĩa môi trường Desktop của người dùng. Trong Window 2000 các chính sách hệ thống này được giữ lại nhằm tương thích với máy khách Window 9x và WindowsNT
- Tiện ích Security and Analysis Configuration được sử dụng phân tích cấu hình bảo mật của bạn. bạn thực hiện tiện ích này để so sánh thiết lập bảo mật tồn tại với cấu hình mẫu để bạn thiết lập sự sai khác