# Lab 6: Hệ điều hành và kiểm soát truy cập

## Mục tiêu

Mục tiêu của bài này là làm quen với các tính năng kiểm soát truy cập có sẵn trong các hệ thống dựa trên Microsoft Windows.

## Bối cảnh

Kiểm soát truy cập (Access control) đề cập đến khả năng của người dùng truy cập vào một đối tượng cụ thể và có thể sửa đổi nó. Trong ngữ cảnh của hệ điều hành, kiểm soát truy cập đề cập đến khả năng của một người sử dụng để đọc, viết hoặc thực thi một tập tin hoặc thư mục nhất định. Trong bài này, chúng ta sẽ nghiên cứu khung (framework) điều khiển truy cập cho các nền tảng dựa trên Microsoft Windows.

## Tài nguyên yêu cầu

Một PC hoặc máy ảo với Microsoft Windows 2000/XP/Vista hay tương tự.

## Kiểm soát truy cập

### Bài 1: Thêm user vào hệ thống

1. Log in vào tài khoản của Admin.

2. Vào Start -> Control Panel -> User Accounts and Family Safety -> Add or remove user accounts

3. Nhấn vào “Create a new account” để tạo user mới. Nhập username là tên mình, viết thường, không dấu, không cách (ví dụ: *nguyenvana*). Chọn “Standard User” cho account type.

4. Nhấn “Create Account…”

### Bài 2: Tìm hiểu tác dụng của các thuộc tính *Read-Only* và *Hidden* của một file

1. Log in vào tài khoản của Admin.

2. Mở ứng dụng *Notepad* để tạo một file văn bản (Start->All Programs -> Accessories -> Notepad)

3. Gõ nội dung tùy ý vào văn bản và lưu ở thư mục *C:\doctemp* với tên theo mẫu *file1\_nguyenvana.txt*

4. Mở thư mục *C:\doctemp* và mở *Properties* của file mới tại.

5. Trong mục Attributes, đánh dấu thuộc tính **Read-Only** và nhấn *OK*

6. Mở lại file này và thêm vào vài nội dung mới rồi thử lưu.

a. Điều gì xảy ra? Giải thích tại sao.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Log off khỏi tài khoản Adminvà log on vào *nguyenvana*.

8. Mở thư mục *C:\doctemp* và mở *Properties* của file *file1\_nguyenvana.txt*.

9. Đánh dấu thuộc tính **Hidden.** Nhấn OK. Đóng cửa sổ và mở thư mục *C:\doctemp lại.*

a. Bây giờ bạn có thấy file không? Không thấy được file

b. Nếu bạn không thấy file, hãy thử tìm cách khác để hiện file ẩn.

### Bước 1: Mở File Explorer (Windows Explorer).

### Bước 2: Trong File Explorer, chọn thẻ "View" (Xem) ở góc trên bên phải.

### Bước 3: Trong nhóm "Show/hide" (Hiện/ẩn), kiểm tra ô "Hidden items" (Mục ẩn).

### Khi bạn thực hiện bước trên, File Explorer sẽ hiển thị các file và thư mục đã được đánh dấu là ẩn trong thư mục C:\doctemp hoặc bất kỳ thư mục nào bạn đang xem. Bạn có thể thấy file1\_nguyenvana.txt được hiển thị lại trong thư mục.

### Bài 3: Cấp quyền tường minh cho các user khác nhau đối với một file cho trước

1. Log in vào tài khoản của Admin.

*2.* Dùng *Notepad* để tạo một văn bản .txt và lưu vào thư mục *C:/doctemp* với tên là *file2\_nguyenvana.txt* as the filename.

3. Mở thư mục *C:\doctemp* và mở *Properties* của file vừa tạo.

4. Chọn tab *Security*. Nhấn nút *Edit…*

*5.* Nhấn nút *Add...* và thêm user *nguyenvana vào file bằng cách đánh nguyenvana* vào text box. Nhấn nút *Check Names* button. Nếu không có báo lỗi, thì nhấn OK. Nhấp tiếp OK cho tới khi trở về *Properties* window và *Security* tab được kích hoạt.

6. Chọn user mình mới thêm bằng cách nhấn vào username của nó. Quyền mặc định (default

permissions) cho user này là gì? Trong khi vẫn xem các option của tab *Security* cho file này, hãy xem các quyền được chỉ định cho nhóm *Users*. Các quyền mặc định cho nhóm này có khác với quyền của người dùng bạn đã thêm để có quyền truy cập vào file không?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

7. Xem các quyền nâng cao để truy cập vào file này cho user *nguyenvana*. Trước hết, mở tab *Security* trong cửa sổ *Properties* của file này, chọn user đó, nhấn nút *Advanced*, chọn lại user đó trong cửa sổ mới và nhấn *Edit,* lại nhấn nút *Edit*

8. Bạn thấy gì? Nó khác với các quyền trong tab *security* cha như thế nào? Có mối liên hệ nào không?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Bài 4: Hiểu cơ chế kiểm soát truy cập của MS Windows

1. Log in vào tài khoản của Admin.

2. Tạo thêm người dùng trong hệ thống. Tên người dùng sẽ là *nguyenvana1*

(Tham khảo Bài 1).

3. Mở thư mục *C:\doctemp* và tạo 1 thư mục tên là *foldernguyenvana*

4. Chọn thư mục vừa tạo và mở *Properties* của nó.

5. Chọn tab *Security* và nhấn vào *Edit..*

6. Nhấn nút *Add...* và thêm user *nguyenvana1*. Nhớ nhấn *Check Names* trước khi nhấn OK.

7. Chọn user *nguyenvana1* trong cửa sổ *Permissions*. Quyền gì hiện được gán cho user này?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Đánh dấu quyền *List folder contents* vào cột *Deny*. Nhấn OK và chấp nhận các thay đổi.

9. Logoff tài khoản Admin và log in vào *nguyenvana*

10. Mở *Notepad* và tạo một file văn bản (Start->All Programs -> Accessories -> Notepad)

11. Thêm nội dung và lưu nó vào thư mục *C:\doctemp\foldernguyenvana* với tên là *file3\_nguyenvana.txt*

12. Mở thư mục *C:\doctemp\foldernguyenvana* và kiểm tra xem mình có thể mở file vừa tạo không.

13. Logoff khỏi tài khoản *nguyenvana* và log in vào *nguyenvana1*

14. Mở thư mục *C:\doctemp\foldernguyenvana*. Điều gì sẽ xảy ra khi bạn truy cập vào thư mục và tại sao?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Auditing trong Windows

Họ sản phẩm Windows OS từ Windows 2000 trở đi cung cấp các chức năng audit bao gồm:

- audit collection

- audit review

- audit log overflow protection

- audit log restricted access protection

Theo mặc định, khi cài đặt, chỉ nhật ký ứng dụng (application logs) và nhật ký lỗi (error logs) được thu thập và lưu trữ bởi chức năng Audit. Quản trị viên máy chủ phải bật security auditing trên máy.

### Bài 5: Audit Log Review

Quản trị viên có thể xem tất cả các security log records bằng cách sử dụng event viewer administrator tool và phân biệt các security logs của ứng dụng và system logs. Mục tiêu của bài này là xem các security log records với các đặc quyền quản trị (administrative privileges).

1. Log in vào tài khoản của Admin.

2. Mở event viewer. (Start->Control Panel->System and Maintenance ->Administrative tools -> View event logs)

3. Khi ở trong Event Viewer, chọn category *Windows Logs* (phía trái cửa sổ)

4. Xem các entries của security logs, application logs và system logs.

5. Log off khỏi tài khoản Admin và log on vào *nguyenvana*

6. Lặp lại bước 2 tới 4

**Câu hỏi**

1. Bạn có thể xem security logs khi là người dùng thường không? Người dùng thường có nên được xem security logs không? Tại sao?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

2. Sự khác biệt giữa security logs và system logs là gì?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Bài 6: Object Access Auditing

Windows cho phép kiểm tra *truy cập đối tượng*, do đó cho phép audit truy cập thành công cũng như không thành công. Để bật kiểm tra truy cập đối tượng, hãy làm như sau:

1. Log in vào tài khoản của Admin.

2. Mở event Microsoft Management Console. (Start->Control Panel ->System and Maintenance ->Administrative tools -> Local Security Policy)

*3.* Chọn *Local Policies* rồi chọn *Audit Policy*

4. Vào properties của *Audit Object Access*

5. Chọn cả “Success” và “Failure” trong cửa sổ properties

6. Nhấn OK để lưu thay đổi.

**Câu hỏi**

Tại sao các chính sách audit mặc định là disable?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### Bài 7: Audit Collection

Bây giờ kiểm tra truy cập đối tượng đã được kích hoạt trên hệ thống. Bạn có thể xác định đối tượng nào cần được kiểm tra. Mục tiêu của bài tập này là kiểm tra các hoạt động tạo và xóa thành công trên một tập hợp các tập tin và thư mục cho tất cả người dùng đã được xác thực trên máy.

1. Log in vào tài khoản của Admin

2. Mở thư mục *C:\doctemp* và tạo thư mục mới tên *folder2\_nguyenvana*

3. Chọn thư mục vừa tạo và mở *Properties* của nó.

4. Chọn tab *Security* và nhấn *Advanced*

5. Chọn tab *Auditing* và nhấn *Continue*.

6. Nhất nút *Add..* và thêm user *nguyenvana1*. Nhớ nhấn *Check Names* trước khi nhấn OK.

7. Bạn sẽ thấy danh sách các sự kiện có thể kiểm tra được khi người dùng truy cập thư mục bạn đang làm việc. Bạn sẽ quan tâm đến sự kiện nào?

Giải thích lý do của mình cho ít nhất 3 sự kiện. Vui lòng xem xét rằng các sự kiện audit tạo ra rất nhiều thông tin có xu hướng tạo ra các log files lớn mà quản trị viên phải xem xét sau này, vì vậy hãy cố gắng lựa chọn cụ thể các sự kiện để audit.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

8. Trong phần này chọn *List folder/Read Data* và *Create files/write data* ở cột Successful. Nhấn OK để lưu.

9. Thoát tài khoản Admin và log in vào user *nguyenvana1*.

10. Dùng *Notepad* tạo một văn bản .txt rồi lưu nó ở thư mục *C:\doctemp\folder2\_nguyenvana* với tên *file5\_nguyenvana.txt*

11. Mở thư mục *C:\doctemp\folder2\_nguyenvana* và kiểm xem mình có vào được file vừa tạo không

12. Log off *nguyenvana1* và log in vào Admin.

13. Mở event viewer. (Start->Control Panel->System and Maintenance ->Administrative tools -> View event logs)

14. Trong Event Viewer, chọn mục *Windows Logs* (bên trái) và chọn mục *Security*

15. We will search the Security log for the audit entries related to the *group<gr#>B* user. To do this, in the *Actions* panel of the window (right side of the window) select the *Find*… command and write *group<gr#>B* in the find box.

16. Xem các entries tong security log không thuộc về Logoff hay Log on attempts. Cụ thể là xem các mục thuộc về File System access và các mục đăng ký trong Access Request Information a Read Data hay ListDirectory event.

Bạn có thể phải đi qua qua một số log entries cho đến khi bạn tìm thấy những entries đáp ứng tiêu chí này. ID sự kiện đã đăng ký cho các entries này là gì?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

17. Để hoàn thành phần này của bài tập, hãy thực hiện các bước được nêu trong Bài 6 nhưng **disable** object access auditing

## Khôi phục hệ thống

Log in vào tại khoản Admin và xóa các tài khoản đã tại trong bài này.

## Tham khảo

James B D Joshi, IS-2150/TEL2810: Information Security and Privacy, School of Computing and Information, University of Pittsburgh