TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH


# BÁO CÁO ĐỒ ÁN

**Môn: An toàn và bảo mật dữ liệu trong Hệ thống thông tin**

**Lớp: 21HTTT2**

**Nhóm: ATBM-B-08**

---

**GVHD:**

**TS. Phạm Thị Bạch Huệ**

**ThS. Lương Vĩ Minh**

**ThS. Tiết Gia Hồng**

# MỤC LỤC

## I. Danh sách thành viên trong nhóm và phân công

| MSSV | Họ và tên | Công việc | Đánh giá |
|---|---|---|---|
| 21127719 | Nguyễn Minh Tuấn | - CS#<br>- Giao diện ứng dụng | 100% |
| 21127591 | Nguyễn Hiển Đạt | - CS#<br>- OLS | 100% |
| 20127055 | Lê Minh Nhân | - CS#<br>- Audit | 100% |

## II. Các chức năng đã hoàn thành

**PHÂN HỆ 1 – HỆ THỐNG WINDOWS FORM DÀNH CHO NGƯỜI QUẢN TRỊ**

| STT | Nội dung | Hoàn thành |
|---|---|---|
| 1.1<br>1.2<br>1.6 | Xem danh sách tài khoản user.<br>Xem thông tin quyền của (user/role) trên các đối tượng DL. | **100%** |
| 1.3 | Tạo mới, xoá, sửa (user/role). | **100%** |
| 1.4 | Cấp quyền (user, role, role2user, with grant, mức cột). | **100%** |
| 1.5 | Thu hồi quyền user/role. | **100%** |

## PHÂN HỆ 2 – THỰC HIỆN CHÍNH SÁCH BẢO MẬT TRÊN HỆ THỐNG

| STT | Nội dung | %hoàn thành |
|---|---|---|
| **YC1** | **Giải pháp cấp quyền truy cấp cho 6 chính sách CS#i:** | |
| | CS#1 | 100% |
| | CS#2 | 100% |
| | CS#3 | 100% |
| | CS#4 | 100% |
| | CS#5 | 100% |
| | **CS#6** | 100% |
| **YC2** | **Cơ chế phát tán thông báo** | |
| | Số lượng chức năng đã hoàn tất: 8/8 | 100% |
| **YC3** | **Ghi nhật ký hệ thống** | |
| 3.1 | Kích hoạt / tắt việc ghi nhật ký. | 100% |
| 3.2 | Standard Audit (table/view/SP/Func). | 100% |
| 3.3 | Fine-grained Audit (Dangky.diem, Nhansu.phucap). | 100% |
| 3.4 | Xem dữ liệu nhật ký. | 100% |
| **YC4** | **Sao lưu & Phục hồi dữ liệu** | |
| | Báo cáo tìm hiểu giải pháp sao lưu & phục hồi, đánh giá, kết luận. | 100% |
| | Hiện thực trên ứng dụng. | |

# III. Các cơ chế bảo mật đã làm trong đồ án

***Các cơ chế bảo mật và mức độ đã làm trong đồ án. [DAC+RBAC]***

Ứng dụng RBAC để phân loại nhóm người dùng có những chức năng giống nhau trong hệ thống, rồi sử dụng DAC để phân quyền tương ứng cho từng role. Việc ứng dụng role này giúp cho hệ thống kiểm soát các truy cập của những người dùng tốt hơn và dễ quản lý hơn.

Ngoài ra một số user đặc biệt cũng sẽ được cấp quyền riêng mà không cần sử dụng role (OLS admin)

***Các cơ chế bảo mật và mức độ đã làm trong đồ án. [VPD]***

Ứng dụng VPD để che đi các cột nhạy cảm (Địa chỉ, điện thoại, điểm) trong hệ thống. Trong hệ thống sẽ có một số role có thể xem được những thông tin khác, bao gồm cả địa chỉ, điện thoại và điểm. Do đó VPD được sử dụng để che giấu đi những thuộc tính đó và chỉ cho duy nhất trường địa chỉ, điện thoại, điểm của người xem được hiển thị. (Tất cả các VPD đã cài đặt đều được áp dụng trên view, vì việc áp trực tiếp lên table sẽ có nhiều vấn đề khó khăn cho việc xử lý các nhóm người dùng khác)

***Các cơ chế bảo mật và mức độ đã làm trong đồ án. [OLS]***

Cài đặt thành công OLS và ứng dụng OLS để phát tán các thông báo tương ứng đến các người dùng nhất định. Dựa vào cơ chế gán nhãn, gán nhãn cho user và gán nhãn cho dữ liệu mà những thông báo sẽ được đảm bảo gửi đến những đối tượng nhất định, những đối tượng không thỏa mãn sẽ không thể thấy được các thông báo.

***Các cơ chế bảo mật và mức độ đã làm trong đồ án. [Standard Audit]***

Dùng standard audit ở các table NHANSU, SINHVIEN, HOCPHAN, PHANCONG, DANGKY, KHMO

***Các cơ chế bảo mật và mức độ đã làm trong đồ án. [Fine-Grained Audit]***

Dùng ở cả 2 tình huống: DANGKY.DIEM và NHANSU.PHUCAP

***Các chính sách bảo mật đã ép thỏa dùng DAC + RBAC***

Sử dụng role để quản lý nhóm người dùng, tạo các role theo vai trò của user trong hệ thống. Cấp các quyền tương ứng cho từng role.

***Các chính sách bảo mật đã ép thỏa dùng VPD***

Cài đặt VPD trên các view mà cho phép người dùng xem các thông tin của người dùng khác ví dụ như Sinh viên. Cụ thể trên 2 view là , VPD này có nhiệm vụ là che giấu đi những dòng dữ liệu nhạy cảm liên quan đến địa chỉ, điện thoại, điểm của người khác, cho nên hàm điều kiện của VPD trong cả 2 trường hợp đều là "MASV = SYS_CONTEXT('USERENV', 'SESSION_USER')". Để dòng dữ liệu

nào thỏa mãn điều kiện, tức là dòng dữ liệu thuộc về người đó thì trường địa chỉ và điện thoại mới được hiện ra, ngược lại tất cả sẽ bị ẩn đi.

***Các chính sách audit đã cài đặt***

**Câu 1:** Tạo chính sách tên 'audit_nhansu' với thuộc tính audit_condition của chính sách là khi VAITRO của người thực hiện truy vấn khác với vai trò là GIẢNG VIÊN để theo dõi các hoạt động cập nhật trên thuộc tính của quan hệ DANGKY, sau đó kích hoạt chính sách trên và hệ thống sẽ lưu vết lại các hành vi vi phạm chính sách trên

**Câu 2**: Tạo chính sách tên 'audit_nhansu' với thuộc tính audit_condition của chính sách là khi mã nhân viên của người thực hiện truy vấn khác với mã nhân viên của dòng cần truy vấn trên các thuộc tính trong quan hệ NHANSU, sau đó kích hoạt chính sách trên và hệ thống sẽ tiến hành lưu vết lại các hành vi vi phạm chính sách trên

***Tìm hiểu giải pháp sao lưu và phục hồi***

1. **Backup**

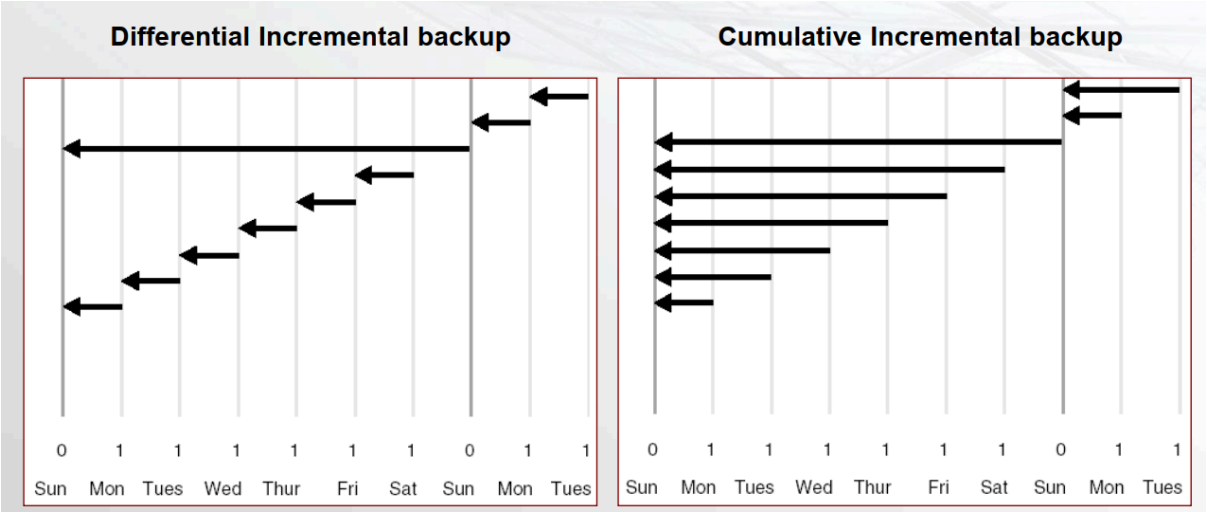
- Backup là một bản sao lưu của cơ sở dữ liệu.

- Full backup:

+ Theo mặc định, RMAN tạo một full backup. Một full backup của một data file bao gồm mọi block được phân bổ trong tệp đang được sao lưu.
+ Full backup không thể là một phần của chiến lược incremental backup.

- Incremental backup:

+ RMAN có thể tạo các incremental backup nhiều cấp độ. Mỗi cấp độ tăng dần được biểu thị bằng một giá trị 0 hoặc 1.
+ Incremental backup chỉ sao lưu những block thay đổi giữa những lần backup.
+ Một incremental backup level 0, sao lưu mọi block trong data file, được sử dụng như điểm bắt đầu cho chiến lược incremental backup.
+ Một incremental backup level 1, chỉ sao lưu những block thay đổi từ incremental backup level 0 hoặc 1 trước đó.
+ Incremental backup có thể thuộc 1 trong 2 loại sau:
    - Differential incremental backup: sao lưu tất cả các block được thay đổi sau Incremental backup level 0 hoặc 1 gần nhất.
    - Cumulative incremental backup: sao lưu tất cả các block được thay đổi sau Incremental bạckup level 0 gần nhất.
    - Cumulative incremental backup được ưu tiên hơn là Differential incremental backup khi thời gian phục hồi ngắn quan trọng hơn dung lượng ổ đĩa vì phải có ít bản sao lưu tăng tiên hơn áp dụng trong quá trình phục hồi




+ Lợi ích khi sử dụng incremental backup:
  - Giảm thời gian sao lưu định kỳ.
  - Giảm áp lực băng thông khi gửi backup qua internet.
  - Giảm dung lượng của backup, tránh hư hỏng file, rò rỉ dữ liệu qua internet.

**2. Recovery**

- Complete recovery: Khi thực hiện Complete Recovery thì cơ sở dữ liệu sẽ được khôi phục đến thời điểm mới nhất, bao gồm tất cả các transaction đã hoàn thành và các dữ liệu đã được chỉnh sửa cho đến thời gian hiện tại. Về bản chất, khi thực hiện Complete Recovery, chúng ta khôi phục cơ sở dữ liệu đến thời điểm gần hiện tại nhất.

- Incomplete recovery: Khác với Complete recovery, Incomplete recovery khôi phục database về một thời điểm cụ thể trong quá khứ. Incomplete recovery còn được gọi là Point in Time Recovery (PITR). Sử dụng incomplete recovery khi:

+ Media failure ( trường hợp khi các tập tin dữ liệu của database bị lỗi và không thể khởi động lại Oracle Instance) phá hủy một phần hoặc tất cả các online redo logs.

+ Lỗi người dùng gây mất dữ liệu, ví dụ một người dùng vô tình xóa một bảng.

+ Không thể thực hiện Complete recovery vì thiếu các archived redo logs.

- Ta có thể lựa chọn giữa hai cách cơ bản để khôi phục các tệp vật lý:

+ RMAN (Recovery Manager): Công cụ quản lý khôi phục được cung cấp bởi Oracle để tự động hóa và quản lý các nhiệm vụ sao lưu và khôi phục.

+ Sao lưu và khôi phục do người dùng quản lý (User-managed Backup and Recovery):

Phương pháp sao lưu và khôi phục dữ liệu mà người quản trị phải tự thực hiện thủ công thay vì

dùng RMAN như công cụ sao lưu và phục hồi chính.

- Phương pháp đầu tiên, sử dụng RMAN, được khuyến nghị:

+ Oracle Recovery Manager (RMAN) cung cấp một nền tảng toàn diện để sao lưu và khôi phục cơ sở dữ liệu Oracle một cách hiệu quả.

+ RMAN tối ưu hóa hiệu suất và tiết kiệm không gian trong quá trình sao lưu với việc đa dạng hóa file và nén bộ sao lưu.

| | Complete recovery | Incomplete recovery |
|---|---|---|
| Ưu điểm | - Phục hồi toàn bộ dữ liệu một cách chính xác, bao gồm tất cả hoạt động giao dịch như Insert, Update, Delete.<br><br>- Đảm bảo tính toàn vẹn và độ chính xác cao của dữ liệu sau khi phục hồi. | - Tiết kiệm không gian lưu trữ do không cần lưu trữ toàn bộ thông tin giao dịch.<br><br>- Quá trình phục hồi nhanh hơn do không cần phục hồi toàn bộ dữ liệu. |
| Nhược điểm | - Đòi hỏi việc lưu trữ toàn bộ thông tin giao dịch, điều này có thể tốn nhiều thời gian và không gian lưu trữ. | - Không thể phục hồi toàn bộ dữ liệu nếu cần.<br><br>- Có thể mất một số dữ liệu gần đây nếu không có bản sao lưu đầy đủ. |