Đại học Khoa học Tự nhiên – ĐHQG TP.HCM

----------□□----------

Môn học: An toàn và bảo mật dữ liệu trong hệ thống thông tin

ĐỒ ÁN MÔN HỌC

HỆ QUẢN TRỊ CƠ SỞ DỮ LIỆU ORACLE

BÁO CÁO

Lớp: 21HTTT

Giảng viên phụ trách:

Cô Phạm Thị Bạch Huệ

Thầy Lương Vĩ Minh

Cô Tiết Gia Hồng

Thông tin sinh viên:

21127456 – Võ Cao Trí

21127608 – Trần Trung Hiếu

21127668 – Đinh Quang Phong

Thông tin thành viên:

STT	**Mã số sinh viên**	**Họ tên**
1	21127456	Võ Cao Trí
2	21127608	Trần Trung Hiếu
3	21127668	Đinh Quang Phong

MỤC LỤC

I. Danh sách chức năng hoàn thành:

STT	Chức năng		Mức độ hoàn thành
1	Yêu cầu 1: Cấp quyền truy cập	Cài đặt cấu trúc cơ sở dữ liệu	100%
2		CS#1: Người dùng có VAITRO là 'Nhân viên cơ bản'	100%
3		CS#2: Người dùng có VAITRO là Giảng viên'	100%
4		CS#3: Người dùng có VAITRO là 'Giáo vụ'	80% Giáo vụ đã thực hiện thêm xóa được trên DANGKY nhưng không phải là thông qua yêu cầu của sinh viên (trên ứng dụng) mà có quyền trực tiếp trên DANGKY
5		CS#4: Người dùng có VAITRO là 'Trưởng đơn vị'	100%
6		CS#5: Người dùng có VAITRO là 'Trưởng khoa'	100%
7		CS#6: Người dùng có VAITRO là 'Sinh viên'	100%
8	Yêu cầu 2: Vận dụng mô hình điều khiển truy cập OLS	Gán nhãn cho người dùng là Trưởng khoa có thể đọc được toàn bộ thông báo	100%
9		Gán nhãn cho các Trưởng bộ môn phụ trách Cơ sở 2 có thể đọc được toàn bộ thông báo. dành cho trưởng bộ môn không phân biệt vị trí địa lý.	100%
10		Gán nhãn cho 01 Giáo vụ có thể đọc toàn bộ thông báo dành cho giáo vụ	100%

11		Nhãn của dòng thông báo t1 để t1 được phát tán (đọc) bởi tất cả Trưởng đơn vị.	100%
12		Nhãn của dòng thông báo t2 để phát tán t2 đến Sinh viên thuộc ngành HTTT học ở Cơ sở 1.	100%
13		Nhãn của dòng thông báo t3 để phát tán t3 đến Trưởng bộ môn KHMT ở Cơ sở 1.	100%
14		Nhãn của dòng thông báo t4 để phát tán t4 đến Trưởng bộ môn KHMT ở Cơ sở 1 và Cơ sở 2.	100%
15		Nhãn cho giảng viên viên bộ môn HTTT ở Cơ sở 2 có thể xem toàn bộ thông báo cho giảng viên HTTT tại 2 cơ sở	100%
16		Nhãn cho sinh viên HTTT ở Cơ sở 2 có thể xem toàn bộ thông báo cho sinh viên.	100%
17		Nhãn cho giảng viên viên bộ môn HTTT ở Cơ sở 2 có thể xem toàn bộ thông báo cho giảng viên tại 2 cơ sở	100%
18		Cài đặt cấu trúc cơ sở dữ liệu cho OLS	100%
19		Thực hiện ghi nhật ký hệ thống dùng Standard audit	100%
20		Thực hiện ghi nhật ký hệ thống dùng Fine-grained Audit	100%
21		Đọc dữ liệu nhật ký	100%
22	Yêu cầu 4: Sao lưu và phục hồi dữ liệu		80%

II. Phân công công việc và đánh giá:

STT	Công việc	Người phụ trách	Mức độ hoàn thành
1	Cài đặt cấu trúc cơ sở dữ liệu ở Yêu cầu 1 và của OLS	Trí, Phong, Hiếu	100%
2	CS#1, CS#3	Trí, Phong	100%
3	CS#2, CS#4	Hiếu, Phong	100%
4	CS#5, CS#6	Hiếu, Trí	100%
5	Cài đặt label cho OLS	Hiếu, Phong	100%
6	Gán label cho user	Hiếu, Trí	100%
7	Ghi nhật ký hệ thống Standard Audit	Hiếu, Phong	100%
8	Ghi nhật ký hệ thống Fine-grained Audit	Hiếu, Trí	100%
9	Sao lưu và phục hồi dữ liệu	Trí, Phong	80%
10	Thiết kế giao diện	Trí, Hiếu	100%
11	Cài đặt chức năng trên hệ thống	Phong, Hiếu, Trí	100%
12	Viết báo cáo	Phong, Trí, Hiếu	100%

III. Nội dung báo cáo

1. Access control

1.1. RBAC

- Tạo các role:
  - RL_NVCB: cho người dùng có vai trò là nhân viên cơ bản.
  - RL_GIAOVU: cho người dùng có vai trò là giáo vụ.
  - RL_GIANGVIEN: cho người dùng có vai trò là giảng viên.
  - RL_TDV: cho người dùng có vai trò là trưởng đơn vị.
  - RL_TK: cho người dùng có vai trò là trưởng khoa.
  - RL_SV: cho người dùng có vai trò là sinh viên.
- Tạo các user là nhân viên và sinh viên:
  - Tạo user sinh viên với username là MASV
  - Tạo user nhân viên với username là MANV
- Cấp role cho user:
  - Với sinh viên gán vai trò là RL_SV

    - Với nhân viên: dựa vào VAITRO của nhân viên để gán role tương ứng bao gồm: RL_NVCB, RL_GIAOVU, RL_GIANGVIEN, RL_TDV, RL_TK.
- Cấp quyền cho role:
    - Cấp các quyền trong các table và view để thỏa mãn các chính sách đề yêu cầu với từng vai trò người dùng tương ứng.

1.2. View:

- Tạo các view để ép thõa các chính sách của các loại người dùng:
    - VIEW_THONGTIN_NVCB: là view dùng để người dùng là nhân viên để có thể coi toàn bộ thông tin cá nhân của bản thân mình.
    - VIEW_THONGTIN_NVCB: cấp quyền update trên thuộc tính DT để nhân viên có thể chỉnh sửa số điện thoại của mình.
    - VIEW_GV_PC: là view dùng để người dùng có vai trò là ‘Giảng viên’, ‘Trưởng khoa’, ‘Trưởng đơn vị’ có thể coi được các PHANCONG liên quan đến chính mình giảng dạy.
    - VIEW_GV_DK: là view dùng để người dùng có vai trò là ‘Giảng viên’, ‘Trưởng khoa’, ‘Trưởng đơn vị’ có thể coi được các DANGKY liên quan đến chính mình giảng dạy.
    - VIEW_TDV_PC: là view dùng để người dùng có vai trò là ‘Trưởng đơn vị’ có thể coi được các PHANCONG có các học phần được phụ trách chuyên môn bởi mình làm trưởng.
    - VIEW_TDV_PC_GV: là view dùng để người dùng có vai trò là ‘Trưởng đơn vị’ có thể coi được các PHANCONG của các giáo viên thuộc đơn vị bởi mình làm trưởng.
    - VIEW_TK_PC: là view dùng để người dùng có vai trò là ‘Trưởng khoa’ có thể coi được các PHANCONG của các học phần được quản lý bởi văn phòng khoa.
- Lợi ích của việc dùng View trong Access control
    - Đảm bảo yêu cầu truy cập của từng loại người dùng với từng đối tượng cụ thể.
    - Giới hạn quyền truy cập của từng người cụ thể - hiển thị nội dung cho từng người dùng hoặc cho từng role cụ thể.
    - Giúp giảm thiểu sự phụ thuộc vào cấu trúc dữ liệu bảng
    - View giúp tăng khả năng tái sử dụng và sự linh hoạt cho các chức năng bằng cách tạo ra view và chỉ cần gọi từng view cho từng chức năng, nhu cầu cụ thể.
    - View giúp bảo vệ cấu trúc của cơ sở dữ liệu - người dùng chỉ có thể xem được các thuộc tính mà view cung cấp mà không biết đến cấu trúc cơ sở dữ liệu bên dưới.
    - View có thể được tối ưu hóa để cải thiện hiệu suất truy vấn, đặc biệt là cho các truy vấn phức tạp hoặc thường xuyên được sử dụng.
    - View có thể được thiết kế để ẩn chi tiết dữ liệu phức tạp, chỉ hiển thị thông tin cần thiết cho người dùng cụ thể.

- Kiểm soát nội dung truy cập của người dùng:
    - Thông qua mệnh đề where của view để kiểm soát những người dùng nào có thể truy cập dữ liệu thích hợp
    - Thông qua mệnh đề select để có thể lựa chọn những field nào được hiển thị cho người dùng

1.3. VPD:

- Tác dụng của VPD:
    - Giúp kiểm soát truy cập ở mức dòng.
    - Kiểm soát truy cập dựa trên các ngữ cảnh cụ thể và lọc dữ liệu động để hiển thị các dòng dữ liệu phù hợp với từng loại người dùng cụ thể dựa vào vị từ của hàm trả về và chính sách cài đặt.
    - Hạn chế truy cập một cách trái phép của người dùng không có quyền và hạn chế truy cập dữ liệu nhạy cảm giúp nâng cao bảo mật dữ liệu và giúp quản lý người dùng truy cập dữ liệu dễ dàng hơn so với RBAC và DAC.
    - Áp dụng chính sách bảo mật phức tạp: VPD cho phép áp dụng các chính sách bảo mật phức tạp dựa trên nhiều yếu tố, chẳng hạn như vai trò người dùng, vị trí, thời gian và dữ liệu cụ thể.
- Cách sử dụng VPD:
    - Tạo vị từ: vị từ trả về của hàm sử được ghép vào mệnh đề where của người dùng cụ thể.
    - Tạo Policy có hàm trả về vị từ trên các quan hệ cụ thể với các loại truy cập cụ thể
    - Khi người dùng truy cập vào quan hệ (với loại truy cập có áp dụng Policy) đó thì Policy sẽ chạy và tự động thêm vị từ của hàm trả về vào sau mệnh đề where để chọn các dữ liệu hiển thị phù hợp với người dùng đó.
- Các chức năng trong đề bài sử dụng VPD:
    - Dùng cho chức năng của người dùng có vai trò là ‘Giáo vụ’: Xóa hoặc Thêm mới dữ liệu trên quan hệ ĐANGKY theo yêu cầu của sinh viên trong khoảng thời gian còn cho hiệu chỉnh đăng ký.
        - Chức năng cài đặt: Người dùng có VAITRO là ‘Giáo vụ’ được quyền thêm xóa trực tiếp trên bảng DANGKY thỏa
          Cài đặt function để tính ngày bắt đầu học kỳ. Dựa vào đó hàm trả về các MAHP còn trong thời hạn đăng ký hay hủy đăng ký.
    - Dùng cho chức năng của người dùng là vai trò là ‘Sinh viên’:
        - Trên quan hệ SINHVIEN, sinh viên chỉ được xem thông tin của chính mình, được Chỉnh sửa thông tin địa chỉ (ĐCHI) và số điện thoại liên lạc (ĐT) của chính sinh viên.
            - Tạo hàm có vị từ trả về username của connection bằng với MASV của chính mình và áp dụng Policy có hàm trên với quyền select trên bảng SINHVIEN

        - Xem danh sách tất cả học phần (HOCPHAN), kế hoạch mở môn (KHMO) của chương trình đào tạo mà sinh viên đang theo học.
            - Tạo hàm có vị từ trả về các MAHP của CT mà sinh viên đang theo học và trả về vị từ các MAHP đó để áp dụng vào Policy với quyền select trên bảng KHMO và HOCPHAN.
        - Thêm, Xóa các dòng dữ liệu đăng ký học phần (ĐANGKY) liên quan đến chính sinh viên đó trong học kỳ của năm học hiện tại (nếu thời điểm hiệu chỉnh đăng ký còn hợp lệ).
            - Cài đặt một function để xem ngày hiện tại đang là học kỳ nào và năm nào và dùng hàm đó trong Function của Policy update và delete trên DANGKY để sinh viên chỉ có thể thêm hoặc xóa học phần trên DANGKY trong vòng 15 ngày kể từ ngày bắt đầu học kỳ. Đặc biệt khi thêm DANGKY mới sinh viên không thể thêm trưởng điếm

1.4. OLS:

- Cách cài đặt OLS:
    - Tạo Level là các bậc của Use gồm: Trưởng khoa > Trưởng đơn vị > Giảng viên > Giáo vụ > Nhân viên > Sinh viên.
    - Tạo các compartment gồm các bộ môn: HTTT, CNPM, KHMT, CNTT, TGMT, MMT.
    - Tạo các group là các cơ sở: CS1, CS2.
    - Tạo policy cho cột label của bảng THONGBAO để kiểm soát truy cập người dùng và gán nhãn cho từng dòng của bảng
    - Tạo các label cho các thông báo
    - Gán các label cho các user
    - Sử dụng mô hình No read up - No write down của OLS
- Tác dụng của OLS trong Access control:
    - Cài đặt quyền truy cập dữ liệu một cách chặt chẽ, hạn chế và ngăn chặn truy cập dữ liệu nhạy cảm không được phép nếu không có quyền
    - Kiểm soát truy cập dữ liệu ở mức hàng giúp kiểm soát truy cập chặt chẽ
    - Tạo các chính sách để có thể quản lý yêu cầu truy cập phức tạp
    - Tăng cường bảo mật dữ liệu: OLS giúp bạn bảo vệ dữ liệu nhạy cảm khỏi truy cập trái phép bằng cách cô lập dữ liệu khỏi những người dùng không có quyền truy cập nếu không có nhãn phù hợp.

2. Audit

- Lợi ích của Audit
    - Giám sát Bảo mật:
        - Giúp phát hiện các hoạt động đáng ngờ, nỗ lực truy cập trái phép hoặc các vi phạm dữ liệu tiềm ẩn.
        - Cung cấp các bản ghi về hành động của người dùng, cho phép điều tra và có thể xác định các mối đe dọa bảo mật.
    - Khắc phục sự cố và Phân tích:

        - Hỗ trợ điều tra các sự cố hoặc lỗi cơ sở dữ liệu bằng cách cung cấp bản ghi lịch sử về các sự kiện mà người dùng đã thay đổi dữ liệu.
    - Kiểm soát Truy cập Dữ liệu:
        - Kiểm toán chi tiết (FGA) cho phép giám sát có mục tiêu việc truy cập và sửa đổi dữ liệu nhạy cảm.
        - Giúp đảm bảo rằng chỉ những người dùng được ủy quyền mới có thể truy cập và sửa đổi thông tin quan trọng.
- So sánh Fine-grained Audit và Standard Audit:

	Fine-grained Audit	Standard Audit
Phạm vi giám sát	Giám sát ở mức chi tiết từng cột, từng loại hành động cụ thể	Giám sát ở mức rộng hơn như bảng, view, function
Sự linh hoạt	Thực hiện ghi khi đúng điều kiện của Audit_condition	Chỉ có thể xác định hành động thành công hay không thành công trên đối tượng chứ không thể xác định điều kiện cụ thể
Tính bảo mật	Có tính bảo mật cao hơn vì mức độ giám sát chi tiết ở mức cột với những điều kiện của dữ liệu cụ thể giúp bảo đảm an toàn cho dữ liệu nhạy cảm	Giám sát ở mức hệ thống giúp kiểm soát người dùng vào/ra hệ thống, có thể bị sót việc ghi Audit trên những hành động trên một số dữ liệu nhạy cảm

2.1. Standard Audit

- Cách cài đặt:
    - Xác định đối tượng (bảng, view, stored procedure, function) nào cần được audit
    - Xác định loại hành động trên đối tượng phù hợp (CRUD).
    - Xác định tính chất của hoạt động (thành công hay không thành công) để ghi audit
- Có thể kiểm soát được những hành động của người dùng trên những bảng, view không phù hợp dù thành công hay không thành công để có thể phát hiện ra lỗi bảo mật và có thể cập nhật kịp thời.

2.2. Fine-grained Audit

- Cách cài đặt:
    - Người dùng xem PHUCAP không phải là của mình
        - Cài đặt Policy cho FGA (Fine-grained Audit) và điều kiện để Policy thực hiện ghi Audit được ghi trong ‘Audit_Condition’ là ‘Sys_context(‘’userenv’’, ‘’session_user’’)!=MANV’ để kiểm

tra có phải chính Nhân viên đã xem PHUCAP của mình trên bảng NHANSU không.

- Người dùng không phải là vai trò ‘Giảng viên’ cập nhật điểm của sinh viên trên quan hệ DANGKY
  - Tạo một Function cho Policy để kiểm tra vai trò hiện tại của người dùng có phải là Giảng viên không
  - Function sẽ được gọi trong Audit_condition để kiểm tra điều kiện sẽ ghi Audit

3. Backup và Recovery

3.1. Các phương pháp thực hiện sao lưu và phục hồi dữ liệu

3.1.1. Recovery Manager (RMAN)

- Ưu điểm:
  - RMAN là công cụ chính thức của Oracle cho sao lưu và phục hồi, tích hợp tốt với các tính năng của hệ thống quản lý cơ sở dữ liệu.
  - RMAN có thể thực hiện sao lưu cơ sở dữ liệu trong khi cơ sở dữ liệu đang mở mà không làm gián đoạn hoạt động.
  - Cung cấp khả năng thực hiện sao Incremental backups, giúp giảm thời gian và tài nguyên cần thiết cho sao lưu.
  - Có khả năng phát hiện và báo cáo về các khối dữ liệu bị hỏng trong quá trình sao lưu.
  - RMAN có thể được cấu hình để tự động thực hiện các sao lưu theo lịch trình được xác định trước.
  - Hỗ trợ sao lưu ở cấp block và phục hồi ở cấp block, giúp tối ưu hóa việc sử dụng tài nguyên.
  - Cung cấp khả năng thực hiện sao lưu và phục hồi trên toàn bộ cơ sở dữ liệu hoặc các phần cụ thể.
- Khuyết điểm:
  - Việc cấu hình và sử dụng RMAN hiệu quả đòi hỏi kiến thức chuyên sâu về Oracle Database.
  - Catalogs backups performed: Yêu cầu quản lý một catalog để lưu trữ thông tin về các sao lưu, điều này có thể tăng phức tạp và tài nguyên hệ thống.

3.1.2. Cold Backup

- Ưu điểm:
  - Đảm bảo tính nhất quán của dữ liệu tại thời điểm sao lưu bằng cách tắt cơ sở dữ liệu.
  - Dữ liệu được sao lưu trong trạng thái tĩnh, việc phục hồi từ sao lưu cold backup thường đơn giản và nhanh chóng.
- Khuyết điểm:
  - Cần dừng cơ sở dữ liệu trong quá trình sao lưu, có thể gây ra sự gián đoạn cho dịch vụ.
  - Thời gian sao lưu tương đối chậm.

3.1.3. Hot Backup

- Ưu điểm:
  - Có thể thực hiện sao lưu trong khi cơ sở dữ liệu đang hoạt động mà không làm gián đoạn hoạt động.
- Khuyết điểm:
  - Yêu cầu sử dụng các công nghệ như archive log để đảm bảo tính nhất quán và độ tin cậy của dữ liệu.

3.1.4. Data pump export and Import utilities

- Ưu điểm:
  - Cho phép sao lưu và phục hồi dữ liệu ở mức logic, giúp dễ dàng trong việc di chuyển dữ liệu giữa các database khác nhau.
- Khuyết điểm:
  - Không hỗ trợ sao lưu và phục hồi ở mức block như RMAN.
  - Thời gian sao lưu và phục hồi có thể lâu đối với các database lớn.

3.1.5. Tổng kết

- Tùy thuộc vào yêu cầu cụ thể của dự án và nguồn lực có sẵn, mỗi phương pháp sẽ có ưu và nhược điểm riêng. Việc lựa chọn phương pháp phù hợp sẽ đảm bảo tính an toàn và hiệu quả cho việc sao lưu và phục hồi dữ liệu.

3.2. Unified Auditing

- Enable unified auditing: ren orauniaud.dll.dlb orauniaud.dll.
- Để kích hoạt Unified Audit cho RMAN, chúng tôi sử dụng PL/SQL để thiết lập các thuộc tính liên quan trong DBMS_AUDIT_MGMT package:

```
BEGIN
    DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_PROPERTY(
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_WRITE_MODE,
    DBMS_AUDIT_MGMT.AUDIT_TRAIL_IMMEDIATE_WRITE);
END;
/
```

- Kích hoạt Unified Audit cho RMAN trên hệ thống. Mọi hoạt động liên quan đến RMAN sẽ được ghi lại trong bảng Unified Audit Trail, cung cấp thông tin quan trọng cho quản trị và phân tích sau này.

3.3. Flash recovery area

- alter system set db_recovery_file_dest_size = 10g scope = both;
- alter system set db_recovery_file_dest = '' scope = both;
- Cấu hình dung lượng và vị trí lưu cho FRA.

3.4. Backup chủ động

- Gọi file backup.bat hay thực hiện thông qua command line.
- File backup.bat chứa các thông số cấu hình và gọi thực thi file backup.rman

```
@echo off
echo Automatic Backup Oracle
cd /d "D:\backup"
SET ORACLE_HOME=D:\21c\dbhomeXE
SET ORACLE_SID=XE
echo ----------------------------------------------------
echo ORACLE_HOME : %ORACLE_HOME%
echo ORACLE_SID  : %ORACLE_SID%
echo ----------------------------------------------------
%ORACLE_HOME%\BIN\RMAN TARGET / @backup.rman log=backup.log
```

- Thực hiện backup full database và archivelog

```
run {
backup database plus archivelog;
}
```

3.5. Backup tự động

- Thực hiện lập lịch gọi file backup.bat

3.6. Recovery(trường hợp mất file dữ liệu)

- Thực hiện bằng command line.
- Tắt cơ sở dữ liệu và khởi động ở chế độ nomount;
- Chọn control file từ thư mục auto backup trong FRA và thực hiện restore control file từ đường dẫn file backup trên
- Thay đổi database thành chế độ mount.
- Thực hiện restore database, recover database.
- Mở database ở chế độ resetlogs.