ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

ĐỒ ÁN
AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN

LỚP: CQ2021/1

Giảng viên hướng dẫn:

Phạm Thị Bạch Huệ

Lương Vĩ Minh

Nhóm thực hiện: ATBMCQ-09

Học kỳ II – Năm học 2023-2024

Mục lục

Tổng quan

1. Thông tin nhóm

Mã nhóm	ATBMCQ-09	
Tên nhóm	Nhóm 09	
Số lượng	4	
MSSV	**Họ tên**	**E-mail**
21120037	Mã Thùy Anh	21120037@student.hcmus.edu.vn
21120060	Nguyễn Long Giang	21120060@student.hcmus.edu.vn
21120082	Phan Quốc Huy	21120082@student.hcmus.edu.vn
21120117	Lê Thị Hồng Phượng	21120117@student.hcmus.edu.vn

2. Phân công công việc

STT	**Công việc**	**Người thực hiện**	**Mức độ hoàn thành**
1	Cài đặt cơ sở dữ liệu	Nguyễn Long Giang Phan Quốc Huy	100%
2	Thiết kế giao diện	Mã Thùy Anh Lê Thị Hồng Phượng	100%
3	Cài đặt hàm, thủ tục	Nguyễn Long Giang Phan Quốc Huy Mã Thùy Anh Lê Thị Hồng Phượng	100%
4	Tạo role, user, priviledge	Nguyễn Long Giang Phan Quốc Huy	100%
5	Thiết lập chức năng	Nguyễn Long Giang Phan Quốc Huy	100%
6	Cấp quyền truy cập	Nguyễn Long Giang Phan Quốc Huy	100%
7	Vận dụng mô hình OLS	Nguyễn Long Giang Phan Quốc Huy Mã Thùy Anh Lê Thị Hồng Phượng	100%
8	Ghi nhật kí hệ thống	Nguyễn Long Giang Phan Quốc Huy	100%
9	Sao lưu và phục hồi dữ liệu	Mã Thùy Anh Lê Thị Hồng Phượng	100%

10	Viết báo cáo	Mã Thùy Anh Lê Thị Hồng Phượng	100%

3. Đánh giá các thành viên

MSSV	Thành viên	Mức độ hoàn thành
21120037	Mã Thùy Anh	100%
21120060	Nguyễn Long Giang	100%
21120082	Phan Quốc Huy	100%
21120117	Lê Thị Hồng Phượng	100%

I. Mô tả đồ án

1. Yêu cầu

Nội dung đồ án yêu cầu xây dựng ứng dụng Windows Form A để quản lý dữ liệu nội bộ cho khoa Công nghệ thông tin của trường đại học X. Các người dùng chính trong hệ thống là: Nhân viên cơ bản, Giảng viên, Giáo vụ, Trưởng đơn vị, trưởng khoa, Sinh viên. Các thông tin cần quản lí gồm thông tin nhân sự, thông tin sinh viên, thông tin đơn vị, học phần, kế hoạch mở môn, phân công, đăng kí môn.

Các chính sách người dùng:

Chính sách	Người dùng	Nội dung
1	Nhân viên cơ bản	- Xem dòng dữ liệu của chính mình trong quan hệ NHANSU, có thể chỉnh sửa số điện thoại của chính mình (nếu số điện thoại có thay đổi). - Xem thông tin của tất cả SINHVIEN, ĐƠNVỊ, HOCPHAN, KHMO.
2	Giảng viên	- Như một người dùng có vai trò “Nhân viên cơ bản”. - Xem dữ liệu phân công giảng dạy liên quan đến bản thân mình (PHANCONG).

		- Xem dữ liệu trên quan hệ ĐANGKY liên quan đến các lớp học phần mà giảng viên được phân công giảng dạy. - Cập nhật dữ liệu tại các trường liên quan điểm số (trong quan hệ ĐANGKY) của các sinh viên có tham gia lớp học phần mà giảng viên đó được phân công giảng dạy. Các trường liên quan điểm số bao gồm: ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK.
3	Giáo vụ	- Như một người dùng có vai trò "Nhân viên cơ bản". - Xem, Thêm mới hoặc Cập nhật dữ liệu trên các quan hệ SINHVIEN, ĐONVI, HOCPHAN, KHMO, theo yêu cầu của trưởng khoa. - Xem dữ liệu trên toàn bộ quan hệ PHANCONG. Tuy nhiên, chỉ được sửa trên các dòng dữ liệu phân công liên quan các học phần do "Văn phòng khoa" phụ trách phân công giảng dạy, thừa hành người trưởng đơn vị tương ứng là trưởng khoa. - 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, xem điều kiện có thể hiệu chỉnh đăng ký học phần được mô tả bên dưới.
4	Trưởng đơn vị	- Như một người dùng có vai trò "Giảng viên". - Thêm, Xóa, Cập nhật dữ liệu trên quan hệ PHANCONG, đối với các học phần được phụ trách chuyên môn bởi đơn vị mà mình làm trưởng,

		- Được xem dữ liệu phân công giảng dạy của các giảng viên thuộc các đơn vị mà mình làm trưởng.
5	Trưởng khoa	- Như một người dùng có vai trò "Giảng viên" - Thêm, Xóa, Cập nhật dữ liệu trên quan hệ PHANCONG đối với các học phần quản lý bởi đơn vị "Văn phòng khoa". - Được quyền Xem, Thêm, Xóa, Cập nhật trên quan hệ NHANSU. - Được quyền Xem (không giới hạn) dữ liệu trên toàn bộ lược đồ CSDL.
6	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. - Xem danh sách tất cả học phần (HOCPHAN), kế hoạch mở môn (KHMO) của chương trình đào tạo mà sinh viên đang theo học. - 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). - Sinh viên không được chỉnh sửa trên các trường liên quan đến điểm. - Sinh viên được Xem tất cả thông tin trên quan hệ ĐANGKY tại các dòng dữ liệu liên quan đến chính sinh viên.

Các yêu cầu cần thực hiện:

- Yêu cầu 1: Cấp quyền truy cập cho người dùng theo chính sách.
- Yêu cầu 2: Vận dụng mô hình điều khiển truy cập OLS để thiết lập hệ thống nhãn gồm 03 thành phần cho hệ thống phát tán thông báo.
- Yêu cầu 3: Ghi nhật kí hệ thống bằng Standard Audit và Fine-grained Audit.
- Yêu cầu 4: Sao lưu và phục hồi dữ liệu.

2. Cơ sở dữ liệu

Mô tả cơ sở dữ liệu:

NHANSU (MANV, HOTEN, PHAI, NGSINH, PHUCAP, ĐT, VAITRO, MAĐV)

Quan hệ NHANSU lưu lại dữ liệu về tất cả nhân viên trong khoa. Nhân sự trong khoa có thể phụ trách các công việc sau: nhân viên cơ bản, giảng viên, giáo vụ, ... Mỗi nhân viên có mã nhân viên (MANV), có họ tên (HOTEN), thuộc phái (PHAI), có ngày sinh (NGSINH), phụ cấp (PHUCAP), số điện thoại liên lạc (ĐT), đảm nhận một vai trò (VAITRO) và thuộc về 1 đơn vị (MAĐV).

SINHVIEN (MASV, HOTEN, PHAI, NGSINH, ĐCHI, ĐT, MACT, MANGANH, SOTCTL, ĐTBTL)

Mỗi sinh viên có mã duy nhất (MASV), họ tên (HOTEN), phái (PHAI), ngày sinh (NGSINH), địa chỉ (ĐCHI), số điện thoại (ĐT), sinh viên thuộc một chương trình đào tạo (MACT), theo học một ngành (MANGANH), số tín chỉ của chương trình đào tạo mà sinh viên đã tích lũy được (SOTCTL) và điểm trung bình tích lũy (ĐTBTL). Hệ thống hiện có khoảng 4.000 sinh viên đang học tại khoa.

ĐONVI (MAĐV, TENĐV, TRGĐV)

Mỗi đơn vị có mã đơn vị (MAĐV), tên đơn vị (TENĐV), người làm trưởng đơn vị (TRGĐV) – cũng là nhân sự của Khoa. Các đơn vị là: Văn phòng khoa, Bộ môn HTTT, Bộ môn CNPM, Bộ môn KHMT, Bộ môn CNTT, Bộ môn TGMT và Bộ môn MMT và Viễn thông. Mỗi đơn vị có một nhân sự làm trưởng (TRGĐV). Trưởng đơn vị của đơn vị Văn phòng khoa chính là nhân sự có vai trò trưởng khoa.

HOCPHAN (MAHP, TENHP, SOTC, STLT, STTH, SOSVTĐ, MAĐV)

Mỗi học phần có mã học phần (MAHP), tên học phần (TENHP), số tín chỉ (SOTC), số tiết lý thuyết (STLT), số tiết thực hành (STTH), số sinh viên tối đa tiếp nhận vào mỗi lớp học phần mỗi khi học phần được mở. Theo phân công của trưởng khoa, mỗi học phần do một đơn vị (MAĐV) phụ trách chuyên môn và do người làm trưởng đơn vị đó phân công

giảng dạy. Với các học phần do đơn vị Văn phòng khoa phụ trách phân công giảng dạy thì các nhân sự giáo vụ thừa hành trưởng khoa phân công giảng dạy.

KHMO (MAHP, HK, NAM, MACT)

Mỗi dòng trong quan hệ KHMO (kế hoạch mở môn) cho biết trong năm học NAM, học kỳ HK đối với chương trình đào tạo MACT thì có mở học phần có mã là MAHP. Các chương trình đào tạo có thể gồm: chính quy ('CQ'), chất lượng cao ('CLC'), chương trình tiên tiến ('CTTT'), Việt - Pháp ('VP'). Mỗi năm học có 3 học kỳ bắt đầu tương ứng vào ngày đầu tiên các tháng 1, 5, 9.

PHANCONG (MAGV, MAHP, HK, NAM, MACT)

Mỗi dòng trong quan hệ PHANCONG cho biết một giảng viên (MAGV, cũng là một nhân sự) được phân công giảng dạy học phần (MAHP) được mở cho chương trình đào tạo (MACT) trong học kỳ HK của năm học NAM theo Kế hoạch mở môn.

ĐANGKY (MASV, MAGV, MAHP, HK, NAM, MACT, ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK)

Mỗi dòng trong quan hệ ĐANGKY cho biết một sinh viên (MASV) đăng ký lớp học phần (đã được mở trong quan hệ KHMO và đã được phân công cho giáo viên trong quan hệ PHANCONG) được xác định bởi các thông tin gồm: mã giảng viên (MAGV), mã học phần (MAHP), mã chương trình đào tạo (MACT), học kỳ (HK), năm học (NAM). Kết quả học tập của sinh viên được ghi lại ở các cột điểm thực hành (ĐIEMTH), điểm quá trình (ĐIEMQT), điểm cuối kỳ (ĐIEMCK) và điểm tổng kết (ĐIEMTK) theo một công thức tỉ lệ cho trước.

THONGBAO (MATB, TENTB, NGAYGUI, NGUOINHAN, LINHVUC, COSO, NOIDUNG)

Mỗi thông báo có mã thông báo (MATB), tên thông báo (TENTB), ngày gửi thông báo (NGAYGUI), vai trò của người nhận (NGUOINHAN), lĩnh vực/chuyên ngành của người nhận (LINHVUC), cơ sở hiện tại người nhận đang làm việc (COSO) và nội dung thông báo (NOIDUNG). Các trường (NGUOINHAN, LINHVUC, COSO) khi có dữ liệu là NULL thì thông báo được gửi cho tất cả các vai trò/lĩnh vực/cơ sở.

II. Thực hiện các yêu cầu

1. Yêu cầu 1

Trong yêu cầu này, các chính sách kiểm soát truy cập và bảo mật dữ liệu được áp dụng bao gồm Discretionary Access Control (DAC), Role-Based Access Control (RBAC), và Virtual Private Database (VPD). Dưới đây là tổng quan về mỗi phương pháp:

a. Discretionary Access Control (DAC)

DAC là một phương pháp kiểm soát truy cập mà trong đó chủ sở hữu của tài nguyên dữ liệu có quyền quyết định ai có thể truy cập tài nguyên đó và ở mức độ nào một cách trực tiếp thông qua quyền (privilege) và vai trò (role).

Ưu điểm:

- Thân thiện với người dùng.
- Chủ sở hữu đối với tài nguyên có thể linh hoạt thu hồi, hoặc cung cấp một phần quyền hạn của mình.
- Đơn giản, dễ cài đặt.

Nhược điểm:

- Khó quản lý: quản trị viên khó có thể theo dõi được những ai có thể truy cập một tài nguyên cụ thể.
- Không đảm bảo được tính bí mật: một dữ liệu bí mật có thể được xem bởi những chủ thể đáng ra không đủ quyền xem.

Các kịch bản:

- Chính sách được áp dụng chủ yếu cho việc khởi tạo tài khoản có quyền DBA ngoài SYS, đó là N09_ADMIN. Từ đây tất cả các đối tượng trong CSDL đều được tạo ra bởi người dùng này.
- Ngoài ra một số quyền cấp cao cho việc Ghi nhật ký hệ thống cũng được gán cho người dùng Quản trị bảo mật SEC_MGR bằng phương pháp này.

b. Role-Based Access Control (RBAC)

RBAC là một phương pháp kiểm soát truy cập dựa trên vai trò, trong đó quyền truy cập được gán cho các vai trò thay vì trực tiếp cho người dùng. Người dùng sau đó được gán các vai trò, và thông qua các vai trò này, họ có quyền truy cập cần thiết.

Ưu điểm:

- Quản lý dễ dàng.
- Các thực thể không thể thay đổi nhóm/vai trò của mình, cũng không thể thay đổi quyền truy cập của các nhóm/vai trò.
- Thuận tiện cho việc tuân thủ nguyên tắc đặc quyền tối thiểu.

Nhược điểm:

- Việc cài đặt và quản lý phức tạp khi có quá nhiều nhóm/vai trò trong hệ thống.
- Các nhóm/vai trò chưa có sự phân cấp rõ ràng.

Các kịch bản:

- Phần lớn các quyền và vai trò truy cập đều được cấp thông qua phương pháp này.
- Mỗi người dùng cơ bản sau khi được khởi tạo tài khoản đều được gán 1 vai trò riêng biệt và chỉ duy nhất 1 vai trò.
- Các yêu cầu cho một người dùng có vai trò A có toàn quyền như một người dùng có vai trò B đều được cấp lại thủ công, đảm bảo 1 người dùng không được cấp quá 1 vai trò.
- Ngoài ra, việc sử dụng Trigger bổ trợ sẽ tạo nên cơ chế kết hợp mang tính bảo mật cao hơn.

c. Virtual Private Database (VPD)

VPD là một tính năng của Oracle cho phép tạo ra các chính sách bảo mật ở mức dòng hoặc cột. VPD cung cấp giải pháp bảo mật tới mức mịn trực tiếp trên các table, view, synonym. Nó gán trực tiếp các chính sách bảo mật lên các đối tượng CSDL, và các chính sách sẽ tự động được thực hiện mỗi khi có một người dùng truy nhập dữ liệu đến các đối tượng đó.

Ưu điểm:

- Khả năng truy cập cao: Người dùng có thể dễ dàng truy cập dữ liệu từ mọi nơi.
- Linh hoạt: Có thể dễ dàng sửa đổi mà không phá vỡ control flow.
- Tỷ lệ phục hồi cao: Dữ liệu có thể được lấy lại dễ dàng.
- Bảo mật động: Không cần duy trì các vai trò phức tạp.

- Không xảy ra backdoor: Chính sách bảo mật được đính kèm với dữ liệu nên không xảy ra tình trạng backdoor.

Khuyết điểm:

- Bảo mật cấp cột khó khăn.
- Cần có ID tài khoản Oracle để sử dụng dịch vụ này.
- Khó kiểm tra.

Các kịch bản:

- Đối với vai trò "Sinh Viên", việc áp dụng cơ chế VPD là bắt buộc.
- Ngoài ra, với các vai trò còn lại, phần lớn chính sách áp dụng là VPD vì tính bảo mật ở mức độ chi tiết, kiểm soát truy cập dữ liệu dựa trên từng hàng/cột, cho khả năng thiết lập truy cập tùy chỉnh trên cùng 1 bảng gốc mà không cần phải tạo View.
- Nội dung chính trong cơ chế là kiểm tra vai trò của người dùng hiện tại bằng cách xác định tiền tố trong chuỗi username của họ. Ví dụ: "Nhân Viên" sẽ có username bắt đầu bằng chuỗi "NV4", "Sinh Viên" sẽ bắt đầu bằng "SV" …
- Ngoài ra, việc sử dụng Trigger bổ trợ cho VPD sẽ tạo nên cơ chế kết hợp mang tính bảo mật cao hơn bao giờ hết.

2. Yêu cầu 2

Trong OLS, Oracle sử dụng các nhãn dữ liệu để phân lớp dữ liệu theo mức độ nhạy cảm của nó và một số tiêu chí khác. Nói cách khác, mỗi nhãn dữ liệu sẽ chứa thông tin về mức độ nhạy cảm của dữ liệu và một số tiêu chí cộng thêm mà người dùng phải đáp ứng để có thể truy xuất đến dữ liệu đó.

Nhãn dữ liệu là một thuộc tính đơn gồm ba loại thành phần:

- Level: Level biểu thị độ nhạy cảm của dữ liệu.
- Compartment: Compartment giúp phân loại dữ liệu theo lĩnh vực, chuyên ngành,… chứ không thể hiện mức độ nhạy cảm của dữ liệu.
- Group: Group giúp xác định những tổ chức, cơ quan, bộ phận nào sở hữu hoặc quản lí dữ liệu. Do vậy group có cấu trúc cây phân cấp gồm group cha và group con.

Nếu một chính sách được áp dụng cho một bảng thì mỗi hàng trong bảng đó sẽ được gán một nhãn dữ liệu để biểu diễn mức độ bảo mật của hàng dữ liệu đó. Giá trị của nhãn được lưu trong cột chứa thông tin của chính sách.

Cách thực hiện:

- Bước 1: Kiểm tra xem OLS đã được cài đặt chưa:

```
> SELECT * FROM DBA_REGISTRY WHERE COMP_ID = 'OLS';
```

Nếu ta thấy kết quả là OLS chưa được bật thì ta thực hiện tiếp haid òng lệnh ày để bật OLS:

```
> EXEC LBACSYS.CONFIGURE_OLS;
> EXEC LBACSYS.OLS_ENFORCEMENT.ENABLE_OLS;
```

- Bước 2: Kết nối với người dùng LBACSYS để cấp quyền xử lí chính sách cho người dùng ADMIN:

```
> ALTER USER LBACSYS IDENTIFIED BY LBACSYS
ACCOUNT UNLOCK;
> CONN LBACSYS/LBACSYS@//localhost:1521/PDB_N09;
> GRANT EXECUTE ON SA_COMPONENTS TO N09_ADMIN;
> GRANT EXECUTE ON SA_LABEL_ADMIN TO N09_ADMIN;
> GRANT EXECUTE ON SA_USER_ADMIN TO N09_ADMIN;
> GRANT EXECUTE ON SA_POLICY_ADMIN TO N09_ADMIN;
> GRANT EXECUTE ON SA_AUDIT_ADMIN TO N09_ADMIN;
> GRANT EXECUTE ON CHAR_TO_LABEL TO N09_ADMIN;
> GRANT EXECUTE ON SA_SYSDBA TO N09_ADMIN;
> GRANT EXECUTE ON TO_LBAC_DATA_LABEL TO N09_ADMIN;
> GRANT LBAC_DBA TO N09_ADMIN;
```

- Bước 3: Kết nối với người dùng ADMIN để tạo chính sách:

```
> CONN N09_ADMIN/123@//localhost:1521/PDB_N09;
> BEGIN
>    SA_SYSDBA.CREATE_POLICY (
>        policy_name => 'N09_POLICY_THONGBAO',
>        column_name => 'ROW_LABEL'
>    );
> END;
> GRANT N09_POLICY_THONGBAO_DBA TO N09_ADMIN;
```

- Bước 4: Tạo level, compartment, group cho chính sách:
  - Tạo level:

```
> BEGIN
>    SA_COMPONENTS.CREATE_LEVEL(
>        policy_name => 'N09_POLICY_THONGBAO',
>        long_name => 'Truong Khoa',
>        short_name => 'TKHOA',
>        level_num => 9000);
> END;
```

Ở đây, ta có mục level_num dùng để biểu thị mức độ nhạy cảm của thông tin. Giá trị của level_num càng cao thì mức độ nhạy cảm càng tăng.

- Tạo compartment:

```
> BEGIN
>    SA_COMPONENTS.CREATE_COMPARTMENT(
>        policy_name => 'N09_POLICY_THONGBAO',
>        long_name   => 'He Thong Thong Tin',
>        short_name  => 'HTTT',
>        comp_num    => 100);
> END;
```

Ở đây, ta có mục comp_num dùng để biểu thị thứ tự sắp xếp của nhãn thông tin.

- Tạo group:

```
> BEGIN
>    SA_COMPONENTS.CREATE_ CREATE_GROUP (
>        policy_name  => 'N09_POLICY_THONGBAO',
>        group_num    => 1,
>        short_name   => 'HCMUS',
>        long_name    => 'Truong DH Khoa Hoc Tu
>        Nhien VNUHCM',
>        parent_name  => NULL)
> END;
```

Ở đây, ta tạo group cha là group HCMUS. Do theo đề bài, trường có hai cơ sở là cơ sở 1 và cơ sở 2 nên ta sẽ tạo tiếp group con:

```
> BEGIN
>    SA_COMPONENTS.CREATE_ CREATE_GROUP (
>        policy_name  => 'N09_POLICY_THONGBAO',
>        group_num    => 100,
>        short_name   => 'CS1',
>        long_name    => 'Co So 1,
>        parent_name  => 'HCMUS')
> END;
```

- Bước 5: Tạo nhãn dữ liệu:

```
> CONN N09_ADMIN/123@//localhost:1521/PDB_N09;
> EXEC SA_LABEL_ADMIN.CREATE_LABEL
('N09_POLICY_THONGBAO',1,'TDONVI::CS1,CS2',TRUE);
```

Ở đây ta tạo các nhãn phù hợp với yêu cầu đề bài thông qua kết nối với người dùng ADMIN và tạo các nhãn theo thứ tự level:compartment:group.

- Bước 6: Tạo nhãn cho người dùng:

```
> CONN N09_ADMIN/123@//localhost:1521/PDB_N09;
> BEGIN
>   SA_USER_ADMIN.SET_USER_LABELS(
>   policy_name    => 'N09_POLICY_THONGBAO',
>   user_name      => 'NV001',
>   max_read_label =>
>   'TKHOA:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:HCMUS');
> END;
```

Ta lần lượt gán nhãn cho người dùng dựa theo vị trí và quyền của họ.

- Bước 7: Áp dụng nhãn cho bảng THONGBAO:

```
> CONN N09_ADMIN/123@//localhost:1521/PDB_N09;
> BEGIN
>   SA_POLICY_ADMIN.REMOVE_TABLE_POLICY (
>       policy_name    => 'N09_POLICY_THONGBAO',
>       schema_name    => 'N09_ADMIN',
>       table_name     => 'N09_THONGBAO');
> END;
> /
> CONN N09_ADMIN/123@//localhost:1521/PDB_N09;
> BEGIN
>   SA_POLICY_ADMIN.APPLY_TABLE_POLICY(
>       policy_name     => 'N09_POLICY_THONGBAO',
>       schema_name     => 'N09_ADMIN',
>       table_name      => 'N09_THONGBAO',
>       table_options   => 'NO_CONTROL');
> END;
> /
```

Ưu điểm:

- Cung cấp bảo mật trên dòng dữ liệu (row-level security).
- Kiểm soát quyền truy cập vào dòng dữ liệu dựa trên nhãn và mức bảo mật của người dùng.
- Được cài đặt sẵn trong Oracle.

Nhược điểm:

- Không bảo mật dữ liệu ở mức cột dữ liệu.
- Không giới hạn các thao tác xử lí trên dữ liệu đối với người dùng được cấp quyền.

Kịch bản test:

- Áp dụng gán nhãn vào các người dùng trong hệ thống và gán nhãn lên các dòng dữ liệu trong bảng THONGBAO để người dùng chỉ đọc được dòng thông báo dành cho mình.

3. Yêu cầu 3

Audit trong Oracle là một tính năng bảo mật cho phép ghi lại và theo dõi các hoạt động trong cơ sở dữ liệu. Việc audit giúp quản trị viên giám sát hành vi của người dùng, bảo đảm tuân thủ các chính sách bảo mật, và phát hiện các hoạt động bất thường hoặc không hợp lệ.

Ưu điểm của việc audit:

- Bằng cách theo dõi hành vi của các user, audit cho phép ràng buộc các user phải có trách nhiệm về hành động mà họ thực hiện.
- Dữ liệu audit giúp phát hiện lỗ hổng trong chính sách bảo mật.
- Đảm bảo rằng user chỉ được thực hiện những gì họ được phép.
- Ghi nhận lại sự lạm quyền hoặc dùng sai quyền, những gì đã xảy ra và có hồi đáp thích hợp.
- Không thực hiện auditing ta sẽ không thể biết khía cạnh bảo mật của hệ thống có đảm bảo hay không hay có ai đã đọc hoặc cập nhật dữ liệu một cách bất hợp pháp hay không.

Trong yêu cầu này, có 2 loại audit được sử dụng:

a. Standard Auditing

Đây là phương pháp audit truyền thống cho phép theo dõi và ghi lại các hoạt động cụ thể trong cơ sở dữ liệu như lệnh DDL, DML, quyền hệ thống và các hoạt động trên các đối tượng cụ thể như bảng, views, và thủ tục.

Theo kịch bản, việc audit được thực hiện bởi SYS, người dùng này cũng cấp các View cần thiết cho người dùng Quản trị bảo mật SEC_MGR để dễ dàng theo dõi.

Các đối tượng được audit là những đối tượng có dữ liệu quan trọng và nhạy cảm như bảng NHANSU, DANGKY…, các hàm Insert, Update, Delete trên bảng DANGKY, và các thủ tục thực hiện lệnh DML trên các bảng nêu trên.

b. Fine-Grained Auditing (FGA)

Đây là tính năng audit mạnh mẽ hơn, cho phép audit chi tiết ở mức độ hàng và cột. FGA cung cấp khả năng kiểm tra các hoạt động dựa trên các điều kiện cụ thể trước khi audit.

Các kịch bản bao gồm audit trên:

- Hành vi Cập nhật quan hệ DANGKY tại các trường liên quan đến điểm số nhưng người đó không thuộc vai trò Giảng viên.
- Hành vi của người dùng này có thể đọc trên trường PHUCAP của người khác ở quan hệ NHANSU.

4. Yêu cầu 4

a) Sao lưu và phục hồi sử dụng Flashback

Tính năng Flashback Table trong Oracle Database cho phép khôi phục dữ liệu trong bảng đến một thời điểm cụ thể trong quá khứ mà không cần phải khôi phục toàn bộ cơ sở dữ liệu. Việc sử dụng tính năng này đảm bảo sự linh hoạt và tiết kiệm thời gian cho người quản trị cơ sở dữ liệu.

Ý tưởng thực hiện: Dựa vào yêu cầu 3 ta sẽ có các bảng N09_FGA, N09_AUDIT_TRAIL nhưng chỉ gồm những hành động làm thay đổi dữ liệu. Từ đó lấy dữ liệu thời gian truyền là input của procedure khôi phục, procedure này sẽ dùng tính năng flashback để khôi phục lại thời điểm ngay trước khi hành động đó diễn ra.

Ưu điểm: Với Flashback Table, người dùng có thể phục hồi lại các phiên bản trước đó của một bảng một cách dễ dàng và nhanh chóng, giúp tiết kiệm thời gian và công sức so với việc phục hồi toàn bộ cơ sở dữ liệu từ một bản sao lưu.

Khuyết điểm: Bảng flashback chỉ lưu dữ liệu để khôi phục trong vòng mặc định là 24h, nên chỉ tiện lợi cho những thao tác mà cần khôi phục trong khoảng thời gian đã cài đặt. Nếu quá thời gian thì người dùng sẽ không khôi phục được bằng phương pháp này.

Các kịch bản bao gồm ứng dụng Flashback:

- Khôi phục bảng DANGKY là lại thời điểm ngay trước hành động chỉnh sửa diễn ra.
- Khôi phục bảng NHANSU là lại thời điểm ngay trước hành động chỉnh sửa diễn ra.
- Khôi phục bảng KHMO là lại thời điểm ngay trước hành động chỉnh sửa diễn ra.

b) Sao lưu và phục hồi sử dụng RMAN

RMAN (Recovery Manager) là công cụ sao lưu và khôi phục dữ liệu được tích hợp sẵn trong Oracle. Khi sử dụng RMAN, người dùng SYSDBA có thể sao lưu toàn bộ hoặc một phần của cơ sở dữ liệu và khôi phục toàn bộ cơ sở dữ liệu nhờ các bản sao lưu trước đó.

Các loại sao lưu dữ liệu trong RMAN:

- Full backups: Full backups chứa toàn bộ data file block đã được sử dụng.
- Incremental backups: Incremental backups, hay còn gọi là Level 0 incremental backups, là một full backup được đánh level 0.
- Cumulative incremental backups: Đây là bản backup chỉ lưu lại những thay đổi sau khi đã sao lưu dữ liệu vào một bản level 0 incremental backup gần đây nhất.
- Differential incremental backups: Đây là bản backup chỉ lưu lại những thay đổi sau lần sao lưu dữ liệu gần đây nhất.

Để tiến hành sao lưu và phục hồi dữ liệu bằng RMAN, chúng ta cần kết nối với RMAN của cơ sở dữ liệu thông qua màn hình Command Prompt dưới danh nghĩa người dùng SYSDBA rồi thực hiện các câu lệnh tùy theo mục đích muốn sao lưu hay là phục hồi.

Các câu lệnh thực hiện sao lưu dữ liệu:

- Kết nối với RMAN:

```
> RMAN TARGET SYS/PASSWORD@DATABASENAME
```

  Ở đây chúng ta sẽ thay thế password và databasename bằng mật khẩu và tên cơ sở dữ liệu mà ta muốn kết nối.
- Sao lưu cơ sở dữ liệu:

```
> BACKUP DATABASE FORMAT 'N09_%U_%T_%D';
```

  Nếu sau khi chạy dòng lệnh này mà màn hình hiện thông báo 'cannot backup database in NOARCHIVELOG mode' thì ta sẽ chạy hai dòng lệnh sau:

```
> SHUTDOWN IMMEDIATE;
> STARTUP MOUNT;
```

- Thay đổi trạng thái archivelog để có thể sao lưu:

```
> ALTER DATABASE ARCHIVELOG;
```

- Sao lưu sơ sở dữ liệu:

```
> ALTER DATABASE OPEN;
> BACKUP DATABASE FORMAT 'N09_%U_%T_%D';
> BACKUP CURRENT CPNTROLFILE FORMAT
 'N09_CONTROLFILE_%U_%T_%D';
> BACKUP SPFILE FORMAT
 'N09_SPFILE_%U_%T_%D';
```

Các câu lệnh thực hiện khôi phục dữ liệu:

- Kết nối với RMAN:
  ```
  > RMAN TARGET SYS/PASSWORD@DATABASENAME
  ```
  Ở đây chúng ta sẽ thay thế password và databasename bằng mật khẩu và tên cơ sở dữ liệu mà ta muốn kết nối.
- Tắt cơ sở dữ liệu nếu cơ sở dữ liệu đang hoạt động:
  ```
  > SHUTDOWN IMMEDIATE;
  ```
- Khôi phục cơ sở dữ liệu:
  ```
  > SET UNTIL TIME '2024-06-15:12:00:00';
  > RESTORE DATABASE;
  > RECOVER DATABSE;
  ```
  Ở câu lệnh SET UNTIL TIME, chúng ta có thể có hoặc không có dòng này vì dòng này dùng để cho RMAN biết chúng ta muốn khôi phục cơ sở dữ liệu về trước khoảng thời gian nào.
- Mở cơ sở dữ liệu:
  ```
  > ALTER DATABASE OPEN;
  ```

Ưu điểm: RMAN có hiệu suất sao lưu và khôi phục cao, sao lưu được toàn bộ cơ sở dữ liệu và đặc biệt hơn, RMAN được tích hợp sẵn vào Oracle nên chúng ta không cần cài đặt thêm. Ngoài ra, thời gian lưu trữ dữ liệu của RMAN không bị giới hạn mà sẽ tùy thuộc vào cấu hình và chính sách sao lưu của cơ sở dữ liệu.

Khuyết điểm: Do RMAN đã được tích hợp vào Oracle nên khi sử dụng, người quản trị phải nắm chắc cơ chế của Oracle để sử dụng RMAN hiệu quả.

c) Sao lưu và phục hồi sử dụng Data Pump

Một cách khác để ta có thể sao lưu và khôi phục dữ liệu là thông qua Oracle Data Pump. Để làm được vậy, ta có thể thông qua các bước sau:

Các câu lệnh thực hiện sao lưu dữ liệu:

- Kết nối với SQL*Plus thông qua màn hình Command Prompt.
- Kết nối với cơ sở dữ liệu dưới danh người dùng SYSDBA:
  ```
  > CONN/ AS SYSDBA
  ```
- Tạo đường dẫn để lưu dữ liệu sao lưu:
  ```
  > CREATE OR REPLACE DIRECTORY <directory_name>
  AS '<backup_directory_path>';
  ```
  Ở đây ta thay thế <diretory_name> bằng tên không gian lưu trữ và <backup_directory_path> bằng tên đường dẫn đến thư mục lưu trữ.

- Nếu muốn, ta có thể cấp quyền cho một người dùng nào đó để thực hiện sao lưu:

```
> GRANT read, write ON DIRECTORY
<directory_name> TO <user_name>;
```

- Ta thực hiện sao lưu dữ liệu:

```
> expdp <username>/<password>
schemas = <schema_name>
directory = <directory_name>
dumpfile = <dump_file_name>
logfile = <log_file_name>;
```

Ta thay thế <username>, <password> bằng tên đăng nhập và mật khẩu người dùng có quyền sao lưu, <schema_name> là tên của schema hiện tại, <directory_name> là tên không gian lưu trữ vừa tạo, <dump_file_name> là tên file lưu trữ ta muốn đặt và <log_file_name> là tên file log lưu lại chi tiết quá trình lưu trữ.

Các câu lệnh thực hiện khôi phục dữ liệu:

- Giả sử ta xóa một người dùng khỏi cơ sở dữ liệu thì tất cả dữ liệu về người dùng đó sẽ mất theo:

```
> DROP USER <user_name> CASCADE;
```

- Ta tiến hành khôi phục dùng câu lệnh sau:

```
> Impdp schemas = <schema_name>
directory = <directory_object_name>
dumpfile = <dump_file_name>
logfile = <log_file_name>
```

- Sau đó ta khởi động lại Talent Data Catalog.

Ưu điểm: Tốc độ xử lí nhanh và có thể cấp quyền cho các người dùng khác để thực hiện sao lưu và khôi phục, dữ liệu được lưu không chiếm nhiều dung lượng và được mã hóa để tăng cường bảo mật.

Khuyết điểm: Do các file lưu trữ được đặt tên theo người sao lưu nên khi khôi phục, ta phải sử dụng lại đúng tên file đã đặt dẫn đến ta sẽ dễ nhầm lẫn giữa các file. Vì vậy, khi sử dụng Data Pump, ta cần thống nhất một qui tắc chung để đặt tên file dễ hiểu và dễ tìm kiếm để thực hiện sao lưu và khôi phục.

III. Tài liệu tham khảo

1. Administrator's Guide, Creating a PDB from Scratch, https://docs.oracle.com/en/database/oracle/oracle-database/23/multi/creating-a-pdb-from-scratch.html
2. Administrator's Guide, Removing a PDB, https://docs.oracle.com/en/database/oracle/oracle-database/23/multi/removing-a-pdb.html
3. Administrator's Guide, Introduction to Oracle Label Security, https://docs.oracle.com/en/database/oracle/oracle-database/23/olsag/introduction-to-oracle-label-security.html
4. Administrator's Guide, Tutorial: Configuring Groups in Oracle Label Security, https://docs.oracle.com/en/database/oracle/oracle-database/19/olsag/configuring-ols-groups.html
5. Oracle Help Center, Recovery Appliance Error Message Reference, https://docs.oracle.com/cd/E55822_01/AMAGD/amagd_errors.htm
6. Oracle Corp, Oracle Label Security, https://www.oracle.com/a/tech/docs/wp-dbsec-ols.pdf
7. Administrator's Guide, Tutorial: Configuring Groups in Oracle Label Security, https://docs.oracle.com/en/database/oracle/oracle-database/21/olsag/configuring-ols-groups.html
8. Oracle Help Center, Configuring Stored Procedure Auditing, https://docs.oracle.com/cd/E20465_01/doc.50/e18695/store_proc_audit.htm
9. Trần Văn Bình, Các câu lệnh hay dùng với Oracle Auditing, https://www.tranvanbinh.vn/2022/03/cac-cau-lenh-hay-dung-voi-oracle.html
10. Oracle Help Center, Introduction to Auditing, https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/introduction-to-auditing.html
11. Nguyễn Thị Diệu, Audit database P2 - Các dạng audit chuẩn trong Oracle, https://viblo.asia/p/audit-database-p2-cac-dang-audit-chuan-trong-oracle-Do754W43lM6
12. Oracle Help Center, Configuring and Using Role Auditing, https://docs.oracle.com/cd/E20465_01/doc.50/e18695/user_role_audit.htm
13. Oracle Help Center, AUDIT (Traditional Auditing), https://docs.oracle.com/en/database/oracle/oracle-database/19/sqlrf/AUDIT-Traditional-Auditing.html

14. Oracle Help Center, Value-Based Auditing with Fine-Grained Audit Policies, https://docs.oracle.com/en/database/oracle/oracle-database/23/dbseg/value-based-auditing-fine-grained-audit-policies1.html
15. Ron Bennatan, Oracle Auditing Part 2: Mandatory and Fine-Grained Auditing, https://securityboulevard.com/2021/07/oracle-auditing-part-2-mandatory-and-fine-grained-auditing/
16. Oracle-Base, Virtual Private Databases (VPD) and Fine-Grained Access Control, https://oracle-base.com/articles/8i/virtual-private-databases
17. Oracle Help Center, Registering and Logging in to Oracle Label Security, https://docs.oracle.com/en/database/oracle/oracle-database/19/olsag/getting-started-with-oracle-label-security.html
18. Ban Cơ yếu Chính phủ, Cơ chế an toàn dựa vào nhãn và CSDL trên Oracle, https://antoanthongtin.gov.vn/giai-phap-khac/co-che-an-toan-dua-vao-nhan-va-csdl-tren-oracle-100946
19. Trần Minh Nhật, Kiểm soát truy cập an toàn, https://viblo.asia/p/kiem-soat-truy-cap-an-toan-ByEZkArq5Q0