**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

**=======🕮=======**

Logo

Description automatically generated

**CUỐN ĐỒ ÁN**

**MÔN: AN TOÀN BẢO MẬT VÀ BẢO MẬT DỮ LIỆU TRONG HTTT**

**Nhóm : ATBMCQ-13**

**Lớp : 19\_1**

**TP. Hồ Chí Minh – 2022**

**THÔNG TIN THÀNH VIÊN**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ tên** | **Email cá nhân** |
| 1 | 19120644 | Lê Đức Tâm | ldtam.110201@gmail.com |
| 2 | 19120622 | Nguyễn Minh Phụng | nmphung08@gmail.com |
| 3 | 19120617 | Mạch Vi Phong | machviphong21042001@gmail.com |
| 4 | 19120641 | Nguyễn Đức Phát Tài | taiinguyen217@gmail.com |

**PHÂN CÔNG CÔNG VIỆC**

**Phân hệ 1:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ tên** | **Nhiệm vụ** | **Hoàn thành** | **Đánh giá** |
| 1 | 19120644 | Lê Đức Tâm | -Thiết kế App | 100% | 10/10 |
| 2 | 19120622 | Nguyễn Minh Phụng | -Quay video demo  -SQL script  -Thiết kế giao diện App (UI) | 100% | 9/10 |
| 3 | 19120617 | Mạch Vi Phong | -Viết báo cáo  -SQL script  -Thiết kế giao diện App (UI) | 100% | 9/10 |
| 4 | 19120641 | Nguyễn Đức Phát Tài | -Gán quyền cho roles user  -SQL script | 100% | 9/10 |

**Phân hệ 2:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **STT** | **MSSV** | **Họ tên** | **Nhiệm vụ** | **Hoàn thành** | **Đánh giá** | **Nhận xét** |
| 1 | 19120644 | Lê Đức Tâm | -Thiết kế App  -Quay clip demo  -TC1 | 100% | 9/10 | -Hoàn thành tốt công việc được giao. |
| 2 | 19120622 | Nguyễn Minh Phụng | -Tổng hợp báo cáo(hỗ trợ)  -Thiết kế dữ liệu mẫu  -Hoàn thành 7 tiêu chí | 100% | 10/10 | -Nhiệt tình  -Hoàn thành tốt công việc được giao.  -Hỗ trợ các bạn trong nhóm. |
| 3 | 19120617 | Mạch Vi Phong | -Tổng hợp báo cáo  -Thiết kế dữ liệu mẫu  -Mã hóa | 100% | 9/10 | -Hoàn thành tốt công việc được giao.  -Tinh thần trách nhiệm. |
| 4 | 19120641 | Nguyễn Đức Phát Tài | -Audit  -TC2  -TC6 | 100% | 9/10 | - Hoàn thành tốt công việc được giao.  -Hòa đồng. |

Mục lục

[Phân hệ 1 6](#_Toc107350714)

[A. Yêu cầu đồ án 6](#_Toc107350715)

[B. Hình ảnh minh họa: 6](#_Toc107350716)

[1. Xem danh sách user: 6](#_Toc107350717)

[2. Thông tin về quyền (privilenges) của user/role trên các đối tượng: 7](#_Toc107350718)

[User: 7](#_Toc107350719)

[Role: 8](#_Toc107350720)

[3. Hiệu chỉnh (thêm, xóa, sửa) user/role: 9](#_Toc107350721)

[User: 9](#_Toc107350722)

[Role: 12](#_Toc107350723)

[4. Cấp quyền: 15](#_Toc107350724)

[Quyền select/update (trên mức cột): 15](#_Toc107350725)

[Quyền insert/delete: 16](#_Toc107350726)

[5. Cho phép thu hồi quyền từ user/role: 16](#_Toc107350727)

[User: 16](#_Toc107350728)

[Role: 18](#_Toc107350729)

[6. Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền: 19](#_Toc107350730)

[7. Cho phép chỉnh sửa quyền trên user/role: 20](#_Toc107350731)

[User: 20](#_Toc107350732)

[Role: 21](#_Toc107350733)

[C. Link video demo: 22](#_Toc107350734)

[Phân hệ 2 23](#_Toc107350735)

[1. Lý thuyết áp dụng 23](#_Toc107350736)

[a. VPD – RLS 23](#_Toc107350737)

[b. OLS 24](#_Toc107350738)

[c. Mã hóa dữ liệu 26](#_Toc107350739)

[d. Auditting 28](#_Toc107350740)

[Standard Audit 28](#_Toc107350741)

[Fine gain Audit 31](#_Toc107350742)

[Các chính sách đã tạo 33](#_Toc107350743)

[Table/View lưu record 34](#_Toc107350744)

[2. Các tiêu chí 36](#_Toc107350745)

# Phân hệ 1

# Yêu cầu đồ án

**PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU**

Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện

công việc sau:

- Xem danh sách người dùng trong hệ thống.

- Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.

- Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.

- Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role,

cấp role cho user. Quá trình cấp quyền có tùy chọn là có cho phép người được

cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH

GRANT OPTION hay không). Quyền, select, update thì cho phép phân quyền

tinh đến mức cột; quyền insert, delete thì không.

- Cho phép thu hồi quyền từ người dùng/ role.

- Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.

- Cho phép chỉnh sửa quyền của user/ role.

# Hình ảnh minh họa:

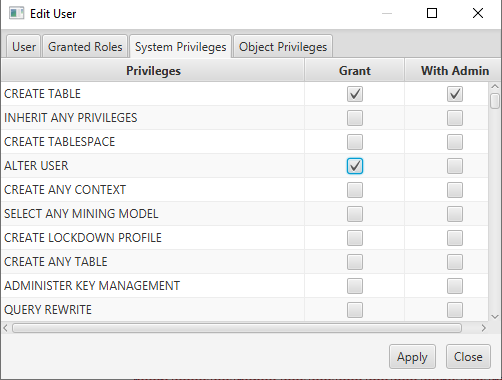
## Xem danh sách user:

Graphical user interface, application

Description automatically generated

## Thông tin về quyền (privilenges) của user/role trên các đối tượng:

### User:



Table

Description automatically generated

### Role:

Table

Description automatically generated

Graphical user interface, table

Description automatically generated

## Hiệu chỉnh (thêm, xóa, sửa) user/role:

### User:

Graphical user interface, application

Description automatically generated

Add User TAI:Graphical user interface

Description automatically generated

Graphical user interface, application

Description automatically generated

Edit User TAI:

Table

Description automatically generated with medium confidence

Delete User TAI:

Graphical user interface, application

Description automatically generated

### Role:

Add Role SINHVIEN:

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Edit role SINHVIEN:

Table

Description automatically generated

Delete Role SINHVIEN: Graphical user interface, text, application

Description automatically generated

## Cấp quyền:

### Quyền select/update (trên mức cột):

Graphical user interface, application

Description automatically generated

### Quyền insert/delete:

Table

Description automatically generated

## Cho phép thu hồi quyền từ user/role:

### User:

Cấp quyền Create table cho NAMEK

Graphical user interface, application

Description automatically generated

Sau khi thu hồi quyềnGraphical user interface, application

Description automatically generated

### Role:

Cấp role THUTHU cho user NAMEK

Graphical user interface

Description automatically generated with low confidence

Cấp quyền CREATE TABLE cho role THUTHU:

Graphical user interface

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application

Description automatically generated

## Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền:

Graphical user interface, application

Description automatically generated

### Cho phép chỉnh sửa quyền trên user/role:

### User:

Cấp quyền, thu hồi quyền bằng tick

Table

Description automatically generated

Thu hồi quyền:

Table

Description automatically generated

### Role:

Cấp quyền, thu hồi quyền bằng tick

Graphical user interface, application, table

Description automatically generated

Thu hồi quyền:

Table

Description automatically generated

# Phân hệ 2

# Lý thuyết áp dụng

## VPD – RLS

RLS (Row-level Security) là cơ chế bảo mật thuộc phạm vi VPD (Virtual Private Database). Được ứng dụng để bảo mật dữ liệu trên mức độ dòng (Row-level).

Cơ chế hoạt động: Bằng chính sách bảo mật được quy định từ trước, RLS giúp quản lý truy xuất dữ liệu bằng việc nối thêm hoặc tạo mới chuỗi WHERE để tương ứng với phân quyền của các đối tượng, người dùng trên dữ liệu.

Các bước thực hiện:

* Tạo hàm trả về chuỗi để ứng với vị trí WHERE, có cú pháp:

CREATE OR REPLACE FUNCTION function\_name (  
 v\_schema IN VARCHAR2,   
 v\_objname IN VARCHAR2)  
  
RETURN VARCHAR2(size);  
  
BEGIN

-- CODE HERE  
 RETURN VARCHAR2;

EXCEPTION

WHEN OTHERS THEN RETURN VARCHAR2;  
END;

Như đã đề cập, sẽ cần xây dựng 1 hàm để hỗ trợ chính sách trả về chuỗi nối WHERE. Hầu hết các trường hợp, hàm sẽ thực hiện kiểm chứng USER hiện tại đang truy vấn để trả về tương ứng theo đúng USER đấy. Sẽ thực hiện ở phần đánh dấu CODE HERE, còn EXCEPTION xử lý các lỗi ngoài mong muốn của hệ thống (chẳng hạn như gặp dữ liệu null thì ngoài tầm kiểm soát của hàm)

* Áp dụng chính sách lên bảng, view cụ thể là đối tượng dữ liệu cần được quản lý cùng với các tham số đầu vào thích hợp

DBMS\_RLS.ADD\_POLICY (   
 object\_schema IN VARCHAR2 DEFAULT NULL,  
 object\_name IN VARCHAR2,  
 policy\_name IN VARCHAR2,  
 function\_schema IN VARCHAR2 DEFAULT NULL,  
 policy\_function IN VARCHAR2,  
 statement\_types IN VARCHAR2 DEFAULT NULL,  
 update\_check IN BOOLEAN DEFAULT FALSE,  
 enable IN BOOLEAN DEFAULT TRUE,  
 static\_policy IN BOOLEAN DEFAULT FALSE,  
 policy\_type IN BINARY\_INTEGER DEFAULT NULL,  
 long\_predicate IN BOOLEAN DEFAULT FALSE,  
 sec\_relevant\_cols IN VARCHAR2 DEFAULT NULL,  
 sec\_relevant\_cols\_opt IN BINARY\_INTEGER DEFAULT NULL,  
 namespace IN VARCHAR2 DEFAULT NULL,  
 attribute IN VARCHAR2 DEFAULT NULL);

Tuỳ vào yêu cầu của tham số mà ta nhập dữ liệu phù hợp để thiết lập chính sách bảo mật. Các tham số quan trọng bao gồm: object\_schema: schema chứa bảng hoặc view áp dụng chính sách, object\_name: tên bảng hoặc view, policy\_name: tên để phân biệt các chính sách với nhau, function\_schema: schema chứa hàm, policy\_function: tên hàm hỗ trợ chính sách.

Các tham số còn lại sẽ phụ thuộc vào nhu cầu đặc biệt của chính sách, khi cần sẽ được đề cập ở các tiêu chí.

## OLS

OLS (Oracle Label Security) là cơ chế bảo mật dựa trên nhãn. Đại khái sẽ cần xây dựng lên một chính sách quy định các nhãn phân cấp nhất định, sau đó các nhãn sẽ được gán với dữ liệu lẫn người dùng. Cơ chế hỗ trợ bảo mật dữ liệu: chỉ có những người dùng có độ tin cậy nhất định mới có thể truy cập đến dữ liệu có độ nhạy cảm cao. Nói đơn giản, người dùng chỉ có thể truy cập đến dữ liệu khi nhãn của họ phù hợp hoặc đáp ứng được yêu cầu của nhãn được gán trên dữ liệu.

Nhãn OLS thì bao gồm các thành phần:

* LEVEL: Mức độ nhạy cảm của dữ liệu
* COMPARTMENT: Bộ phận dữ liệu được phân bổ vào
* GROUP: Khu vực, vị trí dữ liệu được phân bố vào

Trật tự của nhãn: LEVEL1,LEVEL2,…:COMPARTMENT1,COMPARTMENT2,…:GROUP1,GROUP2,…

Các bước thực hiện:

* Tạo chính sách (quyền thực thi được gán mặc định cho người dùng LBACSYS)

SA\_SYSDBA.CREATE\_POLICY (  
 policy\_name IN VARCHAR2,  
 column\_name IN VARCHAR2 DEFAULT NULL,  
 default\_options IN VARCHAR2 DEFAULT NULL);

Sau khi tạo chính sách, thủ tục mặc định tạo ra role POLICY\_NAME\_DBA (thay thế tên policy cho POLICY\_NAME) để dành cho người dùng có vai trò quản lý chính sách này

* Định nghĩa các thành phần của nhãn
* Thành phần LEVEL:

SA\_COMPONENTS.CREATE\_LEVEL (  
 policy\_name IN VARCHAR2,  
 level\_num IN NUMBER(38),  
 short\_name IN VARCHAR2,  
 long\_name IN VARCHAR2);

Thành phần LEVEL có mức độ nhạy cảm càng cao khi level\_num càng cao (0 – 9999)

* Thành phần COMPARTMENT

SA\_COMPONENTS.CREATE\_COMPARTMENT (  
 policy\_name IN VARCHAR2,  
 comp\_num IN NUMBER(38),  
 short\_name IN VARCHAR2,  
 long\_name IN VARCHAR2);

Vị trí của COMPARTMENT trong trật tự nhãn phụ thuộc vào comp\_num, comp\_num thấp đứng trước comp\_cum cao

* Thành phần GROUP

SA\_COMPONENTS.CREATE\_GROUP (  
 policy\_name IN VARCHAR2,  
 group\_num IN NUMBER(38),  
 short\_name IN VARCHAR2,  
 long\_name IN VARCHAR2,  
 parent\_name IN VARCHAR2 DEFAULT NULL);

Vị trí của GROUP trong trật tự nhãn phụ thuốc vào group\_num, group\_num thấp đứng trước group\_num cao

Group có cấu trước cây phân cấp, tức sẽ có Group cha và Group con, quy định bằng tham số parent\_name (điền vào Group cha của Group đang tạo). Một Group có thể thuộc 1 Group cha và có nhiều Group con, dữ liệu thuộc Group con sẽ thuộc luôn Group cha

* Tạo các nhãn cần thiết để gán cho dữ liệu

SA\_LABEL\_ADMIN.CREATE\_LABEL (  
 policy\_name IN VARCHAR2,  
 label\_tag IN BINARY\_INTEGER,  
 label\_value IN VARCHAR2,  
 data\_label IN BOOLEAN DEFAULT TRUE);

Cần thiết tạo một số nhãn nhất định để gán cho dữ liệu. Chuyển thể nhãn dạng chuỗi sang mã số để thuận tiện cho việc đối chiếu.

* Áp dụng chính sách

SA\_POLICY\_ADMIN.APPLY\_TABLE\_POLICY (  
 policy\_name IN VARCHAR2,  
 schema\_name IN VARCHAR2,  
 table\_name IN VARCHAR2,  
 table\_options IN VARCHAR2 DEFAULT NULL,  
 label\_function IN VARCHAR2 DEFAULT NULL,  
 predicate IN VARCHAR2 DEFAULT NULL);

Áp dụng chính sách lên đối tượng (bảng hoặc view) sẽ tạo thêm cột để lưu lại giá trị nhãn của dữ liệu

* Gán nhãn cho dữ liệu

FUNCTION CHAR\_TO\_LABEL (  
 policy\_name IN VARCHAR2,  
 label\_string IN VARCHAR2)  
RETURN NUMBER;

Sử dụng hàm chuyển đổi để lấy nhãn kết hợp câu lệnh UPDATE lên đối tượng để gán các nhãn phù hợp cho dòng dữ liệu

* Gãn nhãn cho người dùng

SA\_USER\_ADMIN.SET\_USER\_LABELS (  
 policy\_name IN VARCHAR2,  
 user\_name IN VARCHAR2,  
 max\_read\_label IN VARCHAR2,  
 max\_write\_label IN VARCHARet2 DEFAULT NULL,  
 min\_write\_label IN VARCHAR2 DEFAULT NULL,  
 def\_label IN VARCHAR2 DEFAULT NULL,  
 row\_label IN VARCHAR2 DEFAULT NULL);

Cuối cùng, ta cần gán nhãn cho người dùng, phụ thuộc vào vai trò mà người dùng nắm giữ

## Mã hóa dữ liệu

* Mã hóa (encrypt): là quá trình chuyển đổi dữ liệu từ dạng đọc hiểu (plaintext – bản rõ) sang dạng dữ liệu không thể đọc hiểu được (ciphertext – bản mã).
* Giải mã (decrypt): là quá trình chuyển đổi dữ liệu từ dạng mã trở về dạng dữ liệu mà chúng t có thể đọc hiểu dễ dàng.

Các lý thuyết đã sử dụng trong bài:

* Gói mã hóa **DBMS\_CRYPTO**: sẽ cung cấp một giao diện để người dùng có thể mã hóa hoặc giải mã dữ liệu cần được lưu trữ. DBMS\_CRYPTO cũng hỗ trợ một số thuật toán mã hóa tiêu chuẩn như DES, 3DES, AES, RC4, 3DES\_2KEY.
* Kiểu dữ liệu thô (dạng nhị phân): **RAW**

Lưu ý: Đối với dữ liệu VARCHAR2, trước khi thực thi chương trình mã hóa, phải chuyển sang tập ký tự **AL32UTF8**, sau đó chuyển sang dạng dữ liệu thô RAW. Khi đó ta mới có thể dùng gói **DBMS\_CRYPTO** để mã hóa dữ liệu.

* Thuật toán thêm các ký tự: **PAD\_PKCS5** sẽ thêm một lượng số bằng với lượng byte còn thiếu của khối cuối cùng. Trường hợp khối cuối cùng vừa đủ thì vẫn thêm số lượng số bằng với số byte của một khối nữa vào sau.
* Chế độ chuỗi mật mã khối**: CHAIN\_CBC** (Cipher Block Chainin) là khối Plaintext kế tiếp được XOR với khối ciphertext trước đó trước khi nó được mã hóa. Vector khởi tạo (IV) được xem như khối plaintext đầu tiên.
* Chuẩn mã hóa: **ENCRYPT\_AES256** là chuẩn mã hóa khối đối xứng, có kích thước khối là 256 bit.
* Các dữ liệu hỗ trợ mã hóa: **PLS\_INTEGER** – xác định loại thuật toán mã hóa (dùng với các kiểu dữ liệu BLOB, CLOB, và RAW).

Hàm mã hóa **encrypt\_aes**:

Graphical user interface, text, application

Description automatically generated

Hoạt động: hàm nhận 2 tham số là dat ( dữ liệu sẽ được mã với kiểu **varchar2**), id\_user ( nội dung mật khẩu (key) với kiểu **varchar2**).

* aes\_key với kểu dữ liệu **RAW**(32): tại đây sẽ dùng hàm **rpad** để dán thêm chuỗi “ph2” vào dữ liệu cho khóa đến khi đủ 32 byte (nếu khóa có độ dài chưa đủ 32 byte), lúc này dữ liệu đang ở kiểu dữ liệu **varchar2**, sau đó dùng hàm **CAST\_TO\_RAW** để chuyển dữ liệu qua dạng **RAW**.
* **Encryption\_type:** bao gồm thuật toán mã hóa + phương pháp chuyển đổi khối mã hóa và kiểu đệm thêm.
* **Src**: dữ liệu dạng **RAW**, chuyển dữ liệu từ chuỗi **varchar2** sang dữ liệu **RAW**.
* **Typ**: thuật toán mã hóa.
* **Key**: khóa mã hóa.

Sau khi chạy xong hàm thì sẽ trả về kiểu dữ liệu **RAW** đã được mã hóa.

Hàm mã hóa **decrypt\_aes**:

Graphical user interface, text, application

Description automatically generated

Về cơ bản thì hàm tương tự **encrypt\_aes** nhưng dữ liệu đầu vào dữ liệu cần được mã hóa là dữ liệu **RAW**

Và sau dùng chúng ta thực hiện bước chuyển dữ liệu từ dạng **RAW** sang **varchar2** để thuận tiện trong việc đọc dữ liệu.

## Auditting

### Standard Audit

*Standard Audit (Kiểm soát chuẩn)* là cơ sở kiểm soát toàn diện và đầy đủ nhất trong cơ sở dữ liệu Oracle. Nó cho phép kiểm soát các loại hành động, đối tượng, đặc quyền (Privilege), user truy cập,… trong Cơ sở dữ liệu.

Có 2 giai đoạn liên quan đến sử dụng Standard Audit.

* Kích hoạt cơ chế kiểm soát (Audit).
* Xác định các chuyên mục (category) cần kiểm soát, tức là xác định các hành động nào sẽ được ghi lại dấu vết.

#### Kích hoạt cơ chế kiểm soát :

*Cơ chế kiểm soát (Audit trail)* : là một table/view dữ liệu hoặc 1 tập tin trên hệ điều hành.Chỉ có kiểm soát viên(DBA) có đặc quyền mới có thể kích hoạt (privilege) .

Có 4 cách để thiết lập cách thức lưu trữ "cơ chế kiểm soát".

|  |  |
| --- | --- |
| name\_audit\_trail | Giải thích |
| DB | Dấu vết được lưu trữ trong bảng AUD$, chỉ chứa lệnh (statement) không phải văn bản đầy đủ. |
| DB,EXTENDED | Dấu vết được lưu trữ trong bảng AUD$, văn bản đầy đủ (Giá trị các biến (variable) đối với mỗi bản ghi..) |
| XML | Dấu vết được lưu trữ trên tập tin của hệ điều hành, theo định dạng XML, nội dung giống tham số DB. |
| XML,EXTENDED | Dấu vết được lưu trữ trên tập tin của hệ điều hành, theo định dạng XML, nội dung giống tham số DB,EXTENDED. |

ALTER SYSTEM SET audit\_trail=**<name\_audit\_trail>** SCOPE=SPFILE : kích hoạt cơ chế kiểm soát



show parameter audit\_trail  : kiểm tra cơ chế audit trail hiện tại

Text

Description automatically generated with medium confidence

show parameter audit\_file\_dest  : kiểm tra đường dẫn tới file audit (XML)

Shape

Description automatically generated

#### Xác định các chuyên mục

Diagram

Description automatically generated

#### Audit trên quyền table/view

Audit **insert/select/update/delete** on [schema].[object] by user

Audit **all** on [schema].[object] by user

Text

Description automatically generated

#### Audit trên quyền hệ thống

Audit **create/drop/delete** any **table/proceduce/trigger** by user

Audit **all** on any **table/proceduce/trigger/privileges** by user

Graphical user interface, text, application

Description automatically generated

Text, letter

Description automatically generated

#### Audit trên các đối tượng,người dùng

By User : kiểm soát trên người dụng



#### Audit trên đặc quyền

Có 2 lựa chọn khi thiết lập chế độ kiểm soát (Audit):

* BY ACCESS: kiểm soát mỗi lần có các hành động, có nghĩa là các hành động giống nhau sẽ được ghi lại.



* BY SESSION: Khi đăng nhập vào Oracle một session sẽ được tạo ra và khi phiên làm việc kết thúc. Oracle sẽ ghi lại các hành động của người dùng nhưng không trùng lặp.



Các hành động lưu dưới dạng bitmap : mỗi dấu “-” thể hiện một hành động

S: viết tắt là thành công

F: viết tắt không thành công

B: viết tắt vừa có lệnh thành công vừa có lênh không thành công



|  |  |
| --- | --- |
| **Position** | **Action** |
| 1 | Alter |
| 2 | Audit |
| 3 | Comment |
| 4 | Delete |
| 5 | Grant |
| 6 | Index |
| 7 | Insert |
| 8 | Local |
| 9 | Rename |
| 10 | Select |
| 11 | Update |
| 12 | Reference |
| 13 | Execute |

#### Audit Session

*AUDIT SESSION* cho phép kiểm soát việc tạo các session. Một bản ghi kiểm soát được tạo đối với mỗi kết nối đến instance, nó bản ghi vào audit trail tại thời điểm kết nối và cập nhật bản ghi tại thời điểm ngắt kết nối.



#### Audit not existt

Ghi lại đoạn lệnh lỗi xảy ra khi đối tượng không tồn tại:



#### Audit network

Kiểm soát mạng để ghi lại các lỗi



#### Noaudit

Bỏ đi các lệnh audit trước đó bằng cách thay **audit** bằng **noaudit** để bỏ

Có thể xem các lệnh đã audit bằng các bảng :

* DBA\_STMT\_AUDIT\_OPTS: cho biết các câu lệnh đang được kiểm soát

Table

Description automatically generated

* DBA\_PRIV\_AUDIT\_OPTS : cho biết các đặc quyền (privilege) đang được kiểm soát

Table

Description automatically generated

* DBA\_OBJ\_AUDIT\_OPTS : cho biết các đối tượng đang được kiểm soát

A screenshot of a computer

Description automatically generated with low confidence

Vd :



### Fine gain Audit

Fine-grained auditing (FGA) có thể thỏa mãn những nhu cầu mà standard audit không thể:

* Tối thiểu những giám sát không cần thiết
* Chỉ ra những truy cập gây hại
* Có thể đặt ra nhiều điều kiện giám sát chi tiết hơn
* không cần phải thiết lập thông số cho AUDIT\_TRAIL để kích hoạt chức năng
* Tạo ra các chính sách FGA rồi áp dụng chúng trên các hoạt động hay các đối tượng muốn giám sát.
* Cơ chế này trong cơ sở dữ liệu ngăn chặn người dùng khỏi việc cố gắng tìm cách truy vấn vòng để không bị giám sát.

#### Chính sách trong FGA

Chính sách FGA có thể theo dõi việc truy xuất dữ liệu dựa trên nội dung của dữ liệu.

Sử dụng chính sách,có thể chỉ rõ cột nào và điều kiện khi nào cần phải ghi lại việc truy xuất đó.

Có thể cung cấp thêm tên hàm muốn thực thi khi một sự kiện giám sát xảy ra. Hàm đó có thể nhắc nhở hoặc báo động cho người quản trị hay xử lí lỗi và các bất thường.

#### DBMS\_FGA

#### Thủ tục ADD\_POLICY

DBMS\_FGA.ADD\_POLICY(

object\_schema VARCHAR2,

object\_name VARCHAR2,

policy\_name VARCHAR2,

audit\_condition VARCHAR2,

audit\_column VARCHAR2,

handler\_schema VARCHAR2,

handler\_module VARCHAR2,

enable BOOLEAN,

statement\_types VARCHAR2,

audit\_trail BINARY\_INTEGER IN DEFAULT,

audit\_column\_opts BINARY\_INTEGER IN DEFAULT);

Giải thích tham số:

|  |  |  |
| --- | --- | --- |
| Tên | Nội dung | Mặc định |
| object\_schema | Tên của schema chứa đối tượng bị giám sát | Null |
| object\_name | Tên của object bị giám sát. |  |
| policy\_name | Tên của chính sách |  |
| audit\_condition | Điều kiện để hàm đó được giám sát. | Null |
| audit\_column | Những cột liên quan sẽ được kiểm tra mỗi khi truy cập. | Null |
| handler\_schema | Schema chứa hàm xử lí sự kiên. | Null |
| handler\_module | Tên hàm xử lí sự kiện. | Null |
| enable | True là kích hoạt và ngược lại | True |
| statement\_types | INSERT, UPDATE, DELETE, SELECT | select |
| audit\_trail | Nơi ghi lại các bản ghi giám sát | DB,extend |
| audit\_column\_opts | Câu lệnh bị giám sát khi câu truy vấn tham khảo tới một trong những cột được chỉ ra trong tham số audit\_column hay phải tham khảo tới tất cả các cột được chỉ ra trong đó | ANY\_COLUMNS |

#### Thủ tục DISABLE\_POLICY

Cú pháp : DBMS\_FGA.DISABLE\_POLICY(

object\_schema VARCHAR2,

object\_name VARCHAR2,

policy\_name VARCHAR2 );

#### Thủ tục ENABLE\_POLICY

Cú pháp DBMS\_FGA.ENABLE\_POLICY(

object\_schema VARCHAR2,

object\_name VARCHAR2,

policy\_name VARCHAR2,

enable BOOLEAN);

#### Thủ tục DROP\_POLICY

Cú pháp DBMS\_FGA.DROP\_POLICY(

object\_schema VARCHAR2,

object\_name VARCHAR2,

policy\_name VARCHAR2 );

### Các chính sách đã tạo

#### 1/Chính sách theo dõi để bảo vệ dữ liệu nhân viên : kiểm tra xem nếu bất kỳ ai xem thông tin nhạy cảm của nhân viên

* bán dữ liệu nhân viên
* cướp nhân sự,
* hối lộ các thanh tra,cấp cao
* …

Text

Description automatically generated

#### 2/Chính sách kiểm tra chuẩn đoán của bác sĩ: kiểm tra xem các bác sĩ khi thay đổi chuẩn đoán cho bệnh nhân

* Các bác sĩ chuẩn đoán sai, muốn bỏ trách nhiệm bằng cách xoá đi các thông tin đã chuẩn đoán.
* Người nào đó muốn sử dụng thông tin chuẩn đoán nhầm đe doạ mạng sống người bệnh

Graphical user interface, text

Description automatically generated

#### 3/Chính sách theo dõi bảo vệ bệnh nhân : kiểm tra xem nếu bất kỳ ai thay đổi thông tin trong BENHNHAN

* Sử dụng thông tin dị ứng, tiền sử bệnh đe doạ đến tính mạng, an toàn, cuộc sống của bệnh nhân

Text

Description automatically generated

#### 4/Chính sách theo dõi dịch vụ đã khám : kiểm tra xem ai đã thay đổi thông tin HSBA\_DV

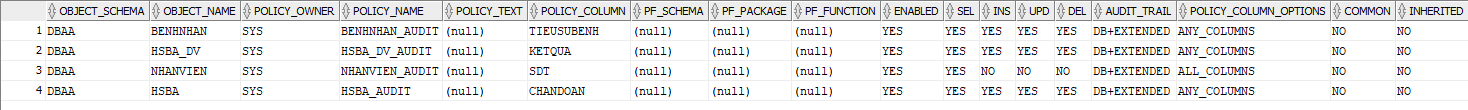
* Tráo đổi thông tin kết quả bệnh nhân nhằm gây ra những sự cố,cố ý đánh giá sai sót của bác sĩ gây ra sự tiêu cực cho bệnh nhân

Text

Description automatically generated

### Table/View lưu record

dba\_audit\_policies : các chính sách audit



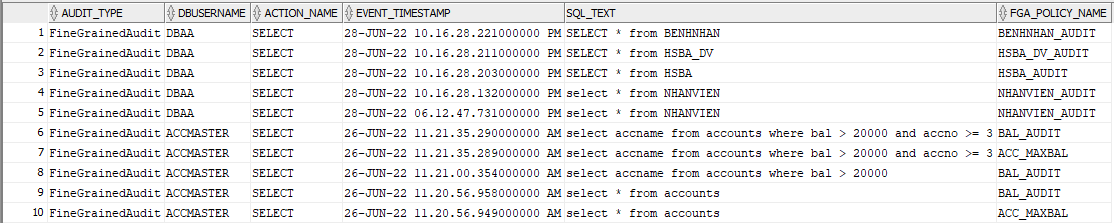
dba\_audit\_policy\_columns : chính sách audit trên cột

Table

Description automatically generated

unified\_audit\_trail: các record của standart và FGA

Graphical user interface

Description automatically generated with medium confidence

dba\_stmt\_audit\_opts: -- các quyền trên hệ thống

Table

Description automatically generated

dba\_priv\_audit\_opts: -- các quyền hệ thống

Table

Description automatically generated

dba\_obj\_audit\_opts :-- các quyền trên object

A screenshot of a computer

Description automatically generated with low confidence

# Các tiêu chí

* Tiêu chí 1:

Text

Description automatically generated

Các nhân viên hoặc bệnh nhân khi thêm dữ liệu sẽ được trigger tạo người dùng sử dụng mã số làm tài khoản với mật khẩu mặc định bằng 1

A screenshot of a computer

Description automatically generated with low confidence

Thử thêm dữ liệu vào bảng NHANVIEN

A screenshot of a computer

Description automatically generated

Trigger sẽ được kích hoạt mỗi khi bảng NHANVIEN nhận thấy dữ liệu mới và tạo ra số lượng người dùng cho nhân viên đã thêm trước đó

* Tiêu chí 2:

Text

Description automatically generated

Áp dụng mô hình phân quyền RBAC, tạo role THANHTRA kèm với các quyền đã được quy định và gán role cho các người dùng nhân viên có vai trò là Thanh tra

* Tiêu chí 3:

Graphical user interface, text

Description automatically generated

Áp dụng mô hình phân quyền DAC, các người dùng nhân viên có vai trò Cơ sở y tế sẽ được phân quyền thao tác trên các view đã được tạo trước đó dựa trên yêu cầu của tiêu chí: chỉ được thao tác với dữ liệu thuộc cùng cơ sở với nhân viên (bảng HSBA và bảng HSBA\_DV)

Để thuận tiện cho việc quản lý thì các view khi tạo có trật tự chung MASO\_TENBANG (nếu người dùng NV1 có phân quyền nhất định trên bảng HSBA thì view được tạo là NV1\_HSBA)

Text

Description automatically generated

NV8 là tài khoản của nhân viên có vai trò tương ứng có thể truy vấn trên các view đã tạo

Graphical user interface, text, application

Description automatically generated

Thiết lập trigger để ngăn chặn người dùng truy cập trái khung giờ đã quy định

Text

Description automatically generated

Mọi truy cập ngoài khung giờ cho phép đều bị từ chối

* Tiêu chí 4:

Text

Description automatically generated

Tương tự như tiêu chí 3, các view được tạo giữa trên quyền truy cập dữ liệu của các nhân viên là Bác sĩ, sau đó gán các quyền thích hợp cho người dùng Bác sĩ

Để thuận tiện cho việc quản lý thì các view khi tạo có trật tự chung MASO\_TENBANG (nếu người dùng NV1 có phân quyền nhất định trên bảng HSBA thì view được tạo là NV1\_HSBA)

Text

Description automatically generated

NV2 là người dùng có vai trò Bác sĩ, có thể truy cập đến các dữ liệu trong phân quyền của mình thông qua view đã tạo trước đó

* Tiêu chí 5:

Text

Description automatically generated

 Các view được tạo ra tùy vào khả năng truy cập dữ liệu của nhân viên nghiên cứu. Sau đó gán các quyền được yêu cầu lên view cho người dùng nhân viên.

Để thuận tiện cho việc quản lý thì các view khi tạo có trật tự chung MASO\_TENBANG (nếu người dùng NV1 có phân quyền nhất định trên bảng HSBA thì view được tạo là NV1\_HSBA)

Text

Description automatically generated

NV5 là người dùng có vai trò Nghiên cứu, có thể truy cập đến các dữ liệu trong phân quyền của mình thông qua view đã tạo trước đó

* Tiêu chí 6:

Áp dụng cơ chế bảo mật RLS – VPD để hỗ trợ quản lý truy cập dữ liệu. Lần lượt thực hiện các bước xây dựng các hàm: xem xét người dùng, tùy trường hợp mà trả về chuỗi nối WHERE, áp dụng các hàm vừa tạo vào các chính sách sao cho thỏa yêu cầu tiêu chí

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated with medium confidence

Hàm hỗ trợ chính sách giới hạn người dùng (bệnh nhân, nhân viên) chỉ được truy cập đến thông tin cá nhân của bản thân

Graphical user interface, text, application

Description automatically generated

Hàm hỗ trợ chính sách ngăn chặn người dùng thay đổi thông tin của cột quy định (đã mã hóa)

Text

Description automatically generated with low confidenceGraphical user interface, text, application

Description automatically generated

Áp dụng cách chính sách sách lên các đối tượng. Khi đối tượng truy cập đến đối tượng, chính sách sẽ xem xét áp dụng các hàm đã xây dựng để đưa ra chuỗi nối WHERE nhất định.

Text

Description automatically generated

Lấy NV2 làm ví dụ minh họa, là người dùng nhân viên. Khi truy vấn từ bảng nhân viên thì sẽ thấy mỗi thông tin cá nhân của bản thân. Các thao tác chỉnh sửa dữ liệu đã mã sẽ bị ngăn chặn.

* Tiêu chí 7:

Áp dụng cơ chế bảo mật OLS (Oracle Label Security) để hỗ trợ quản lý các thao tác truy cập dữ liệu. Đảm bảo chỉ có những người dùng có mức độ tin cậy nhất định mới có thể truy cập đến dữ liệu nhạy cảm.

Ở đây áp dụng OLS để gán nhãn cho dữ liệu trong bảng thông báo, hỗ trợ phân bố thông báo đến các người có quyền nhất định trong hệ thống.

Text, letter

Description automatically generated

Thực hiện tạo chính sách được mặc định phân quyền cho tài khoản LBACSYS (cần phải mở khóa trước khi sử dụng)

Text

Description automatically generated

Sau khi tạo chính sách, quy định từng thành phần của nhãn, đầu tiên sẽ là mức độ nhạy cảm (LEVEL)

Có 2 mức độ: PUBLIC – P: công khai; SENSITIVE – S: Nhạy cảm, riêng tư, phù hợp để gắn với các thông tin quan trọng

Graphical user interface, text, application

Description automatically generated

Tiếp đến là thành phần bộ phận, cục công việc (COMPARTMENT). Như quy định thì các cơ sở đều được chia ra làm 3 tuyến: Điều trị ngoại trú, Điều trị nội trú, Điều trị chuyên sâu

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Thành phần cuối cùng là khu vực (nhóm – GROUP). Như quy định thì các cơ sở sẽ phân bố ở những vị trí: Sở y tế tức khu vực tổng thể thành phố, Trung tâm, Cận trung tâm, Ngoại thành

Text

Description automatically generated Text

Description automatically generated

Xem xét tính nhạy cảm của dữ liệu lập ra các nhãn dữ liệu cần thiết để tạo lập, mục đích nhằm chuyển nhãn dạng chuỗi sang dạng số để thuận tiện cho việc đối chiếu

Graphical user interface, text

Description automatically generated

Áp dụng chính sách lên bảng cần quản lý để chế độ không kiểm soát nhằm tạo thêm cột nhãn, sau đó ta cập nhật các nhãn của dữ liệu trong bảng

Text, letter

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Sau khi đã cập nhật các nhãn cho dữ liệu thì ta hủy rồi tái áp dụng chính sách để chính sách bắt đầu thực thi

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text

Description automatically generated

Sau khi gán nhãn dữ liệu, việc cuối cùng là gắn các nhãn thích hợp cho người dùng

Các người dùng cụ thể cùng các nhãn:

* GIAMDOC (FULL): là giám đốc sở có quyền truy cập mọi thông báo trong bảng
* GIAMDOC\_TT (S::TT): là giám đốc khu vực Trung tâm, thấy được thông báo quan trọng gửi riêng đến trung tâm
* GIAMDOC\_CTT (S::CTT): là giám đốc khu vực Cận trung tâm, thấy được thông báo quan trọng gửi riêng đến cận trung tâm
* GIAMDOC\_CS\_NT (S:CS:NT): là giám đốc khu vực Ngoại thành tuyến Chuyên sâu, thấy được thông báo quan trọng gửi riêng đến ngoại thành, tuyến chuyên sâu
* NV2 (P): là nhân viên có vai trò bác sĩ, được giả sử thấy được các thông báo công khai

Text

Description automatically generated

Giám đốc sở có toàn quyền nên thấy hết các thông báo

Text

Description automatically generated

Giám đốc khu vực Trung tâm do có thể thấy được dữ liệu mức độ SENSITIVE nên có thể thấy được dữ liệu ở mức độ thấp hơn (dữ liệu mức PUBLIC)

Graphical user interface, text

Description automatically generated

Giám đốc khu vực Cận trung tâm có quyền truy cập đến thông báo được gửi riêng đến khu vực mình mà các giám đốc khu vực khác không thấy được

Text

Description automatically generated

Giám đốc khu vực Ngoại thành tuyến Chuyên sâu có thể truy cập đến thông báo gửi riêng đến tuyến của mình mà các người dùng không thể truy cập được nếu không thuộc cùng tuyến quy định

Graphical user interface

Description automatically generated

Các bác sĩ (cụ thể người dùng NV2) theo nhãn được gắn cho bản thân thì chỉ truy cập đến dữ liệu có mức độ công khai (PUBLIC)

# Tài liệu tham khỏa:

OLS

<https://tieuluan.info/bi-thc-hnh-oracle-label-security-1-tm-tt-ni-dung.html> <https://tieuluan.info/lab-10-bo-mt-h-thng-thng-tin.html>

VPD - RLS

<https://tieuluan.info/bo-mt-h-thng-thng-tin-v8.html> <https://tieuluan.info/bo-mt-h-thng-thng-tin-v11.html> <https://tieuluan.info/bo-mt-h-thng-thng-tin-v11.html#Column_Sensitive_VPD_L%C3%BD_thuy%E1%BA%BFt>

Standard audit :

<https://openplanning.net/11309/oracle-standard-database-auditing#:~:text=Standard%20Audit%20(Ki%E1%BB%83m%20so%C3%A1t%20chu%E1%BA%A9n,)%2C%20user%20truy%20c%E1%BA%ADp>..

Fine gained audit :

<https://cuuduongthancong.com/dlf/503252/an-toan-va-bao-mat-he-thong-thong-tin//lab-13_fine-grained-auditing.pdf>

Mã hóa:

<https://www.tranvanbinh.vn/2021/06/goi-ma-hoa-dbmscrypto-trong-oracle.html>

<https://docs.oracle.com/database/121/ARPLS/d_crypto.htm#ARPLS65675>

# Link video demo:

Phân hệ 1:

Link youtube: <https://youtu.be/TxdYQSeol7I>

Link Drive : <https://drive.google.com/file/d/12cNw5HRM3ug3qr_-tNSVFyRVJDeVfa-Q/view?usp=sharing>

Phân hệ 2:

Link youtube: <https://youtu.be/ZB2EpzvBYBI>