Trường Đại học Khoa Học Tự Nhiên ĐHQG TP HCM

Khoa Công Nghệ Thông Tin

----------🙠🕮🙢----------



**AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG**

**HỆ THỐNG THÔNG TIN**

**Đồ án: Môn học**

**GV: Phạm Thị Bạch Huệ**

**Lương Vĩ Minh**

**Thành viên:**

1. Phạm Minh Khoa
2. Trần Hữu Hoàng
3. Huỳnh Ngọc Hòa

**Tên nhóm: 7**

**Liên lạc:**

SĐT:0336069400

Mục Lục

[A. Mô tả đồ án 3](#_Toc68478892)

[1. PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU 3](#_Toc68478893)

[2. PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN 4](#_Toc68478894)

[3. Yêu cầu: 5](#_Toc68478895)

[4. MỘT SỐ QUY ĐỊNH: 6](#_Toc68478896)

[B. Phân công công việc 6](#_Toc68478897)

[C. Nội dung 7](#_Toc68478898)

[D. Đánh giá 7](#_Toc68478899)

[E. Tham khảo 7](#_Toc68478900)

# Mô tả 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.
* Sinh viên hãy thực hiện chức năng ghi nhật ký hệ thống (chỉ yêu cầu thực hiện mức HQT CSDL Oracle):
* Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống.
* Admin được chỉ định ghi nhật ký của những hành động thực hiện bởi những
* user nào trên những đối tượng cụ thể. Các hành động đó là: đăng nhập, thay đổi thông tin user account, select, insert, update, delete, execute.; các đối tượng là table, view, stored procedure, function. Admin cũng được quyền chọn ghi nhật ký hành động được thực hiện thành công hay không thành công.
* Kiểm tra dữ liệu nhật ký hệ thống. Sinh viên nên đề ra một số kịch bản theo dõi hệ thống để phân tích dữ liệu nhật ký.

## PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN

Một bệnh viện quy mô vừa có những vai trò sau: bộ phận quản lý, bộ phận tiếp tân và điều phối bệnh, bác sĩ điều trị, phòng tài vụ, phòng bán thuốc và bộ phận kế toán.Bệnh nhân đến bệnh viện sẽ gặp bộ phận tiếp tân và điều phối bệnh để khai bệnh ban đầu gồm tên, năm sinh, địa chỉ liên lạc, số điện thoại, triệu chứng bệnh. Nếu bệnh nhân trước đó đã khám bệnh thì đọc mã khám bệnh thì thông tin bệnh nhân đã có và không cần phải nhập lại. Sau khi hoàn tất giai đoạn tiếp bệnh, nhân viên tiếp tân chỉ định phòng khám và bác sĩ khám. Tại phòng tài vụ, nhân viên phòng tài vụ nhìn thấy thông tin khám bệnh của bệnh nhân mới sẽ thu tiền khám của bệnh nhân và hướng dẫn bệnh nhân đến gặp bác sĩ. Sau khi xem bệnh, bác sĩ chỉ định và ghi nhận vào CSDL liên quan đến bệnh nhân đó là phải dùng thuốc gì, hoặc phải tiếp tục làm những thủ tục xét nghiệm hoặc chẩn đoán hình ảnh nào. Nhân viên phòng tài vụ căn cứ vào đó thu tiền trước khi bệnh nhân được xét nghiệm hoặc chụp hình theo yêu cầu của bác sĩ. Bộ phận tiếp tân và điều phối bệnh dựa vào dữ liệu của hệ thống ghi lại yêu cầu của bác sĩ sẽ ghi lại trên CSDL thông tin điều phối bệnh vào các phòng liên quan và hướng dẫn bệnh nhân vào phòng nào gặp bác sĩ nào. Sau khi hoàn tất các yêu cầu, bệnh nhân mang kết quả về cho bác sĩ khám bệnh ban đầu đọc kết quả và đề nghị dùng thuốc theo toa bác sĩ kê. Nhân viên phòng thuốc căn cứ vào đó bán thuốc cho bệnh nhân. Chính sách bảo mật trong ứng dụng trên được mô tả như sau:

* Thành viên của bộ phận quản lý được chia ra làm 3 nhóm: nhóm quản lý tài

nguyên và nhân sự (phòng ban, bác sĩ, nhân viên, chấm công), nhóm quản lý tài vụ (đơn giá các loại dịch vụ khám bệnh, đơn giá thuốc), và nhóm quản lý chuyên môn. Nhóm quản lý tài nguyên nhân sự chỉ được thêm, xóa, sửa các thông tin trong cách danh mục như: phòng ban, bác sĩ, nhân viên trong từng phòng ban, bác sĩ nào trực phòng nào vào thời gian nào, …và được xem tất cả các thông tin khác kể cả thông tin nhân viên kế toán tạo ra nhưng không được quyền sửa. Nhóm quản lý tài vụ chỉ được nhập mới chỉnh sửa các thông tin liên quan, những thông tin khác được quyền xem tất cả nhưng không được phép sửa. Nhóm quản lý chuyên môn được xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ để theo dõi về chuyên môn của bệnh viện và có chiến lược trong tương lai mà không được chỉnh sửa bất cứ thông tin nào.

* Bộ phận tiếp tân và điều phối bệnh được quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân, được điều phối bệnh nhưng không thể xem các thông tin liên quan đến số tiền cho từng thủ tục khám, xét nghiệm hoặc chụp hình hoặc thông tin thuốc điều trị bệnh cho bệnh nhân.
* Nhân viên phòng tài vụ chỉ nhìn thấy các thủ tục mà bác sĩ yêu cầu bệnh nhân phải làm khi điều trị bệnh, thông tin mà bộ phận điều phối bệnh đã điều phối và tính tiền. Nhân viên phòng tài vụ chỉ được cập nhật số tiền phải trả cho từng chi tiết khám trị bệnh của bệnh nhân mà không được chỉnh sửa bất cứ thông tin gì.
* Bác sĩ: chỉ có thể thêm hoặc sửa thông tin liên quan đến việc điều trị bệnh và các loại thuốc phải dùng, liều dùng cho bệnh nhân mà bác sĩ chịu trách nhiệm điều trị. Bác sĩ không được xem hoặc chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác điều trị hoặc những thông tin khác trong hệ thống.
* Nhân viên bộ phận bán thuốc: chỉ có thể nhìn thấy toa thuốc mà bác sĩ kê cho từng bệnh nhân để tính tiền thuốc cho bệnh nhân mà không thể xem được bệnh nhân bệnh gì hay bất cứ thông tin gì khác.
* Nhân viên kế toán: tính lương cho các bác sĩ và các nhân viên khác dựa vào

lương cơ bản, phụ cấp, số ngày công. Nhân viên kế toán không nhìn thấy bất cứ thông tin gì trong hệ thống liên quan đến quá trình điều trị bệnh cho bệnh nhân của những bộ phận liên quan.

## Yêu cầu:

1. Sinh viên tự thiết kế mô hình dữ liệu và tạo dữ liệu thử cho ứng dụng trên.

Hãy dùng các cơ chế bảo mật đã học của Oracle để hiện thực các cơ chế ảo mật đề ra.

1. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế mã hóa trong ứng dụng trên,

và dùng thư viện hỗ trợ mã dữ liệu của Oracle. Cho biết mục đích, đối

tượng cần bảo vệ dữ liệu bằng phương pháp mã hóa, phương pháp quản

lý khóa.

1. Sinh viên hãy đề ra bối cảnh sử dụng cơ chế OLS của Oracle. Nhãn gồm

đầy đủ 3 thành phần: level, compartment và group. Hãy gán nhãn cho dữ

liệu, người dùng và minh họa chính sách bảo mật đã cài đặt.

1. Nếu sinh viên cài đặt thêm các chính sách bảo mật có ứng dụng thực tế

trong ứng dụng đã cho sẽ được xem xét điểm.

## MỘT SỐ QUY ĐỊNH:

1. Các nhóm đều làm cả hai phân hệ, cùng ứng dụng.

2. Chấm đồ án vào ngày thi theo lịch thi chung của Trường.

3. Cuốn đồ án: trình bày lý thuyết ngắn gọn, dễ hiểu, ghi rõ tài liệu tham khảo,

không dịch lại tài liệu, chủ yếu là phần tóm lược những gì tìm hiểu được, nhận xét, đánh giá, thuyết minh các kết quả đạt được. Nhóm trưởng làm bảng phân công công việc và đánh giá hai thành viên trong nhóm (đóng chung trong cuốn đồ án). Ghi rõ nhóm đã cài đặt những chính sách bảo mật cụ thể nào, kịch bản gì. Nhóm cố gắng cài đặt tất cả các cơ chế bảo mật đã học.

4. Nộp file: ngoài bản in nộp vào ngày chấm đồ án, sinh viên phải nộp file trên Moodle, gồm file word báo cáo (file cuốn đồ án), source code. Tên file là mã sinh viên của các thành viên trong nhóm, cách nhau bởi dấu ‘\_’.

5. Chia công việc sao cho tất cả các thành viên của nhóm đều phải thực hiện được yêu cầu của đồ án. Sinh viên có thể được yêu cầu phải thực hiện tại chỗ yêu cầu cài đặt một số chính sách bảo mật.

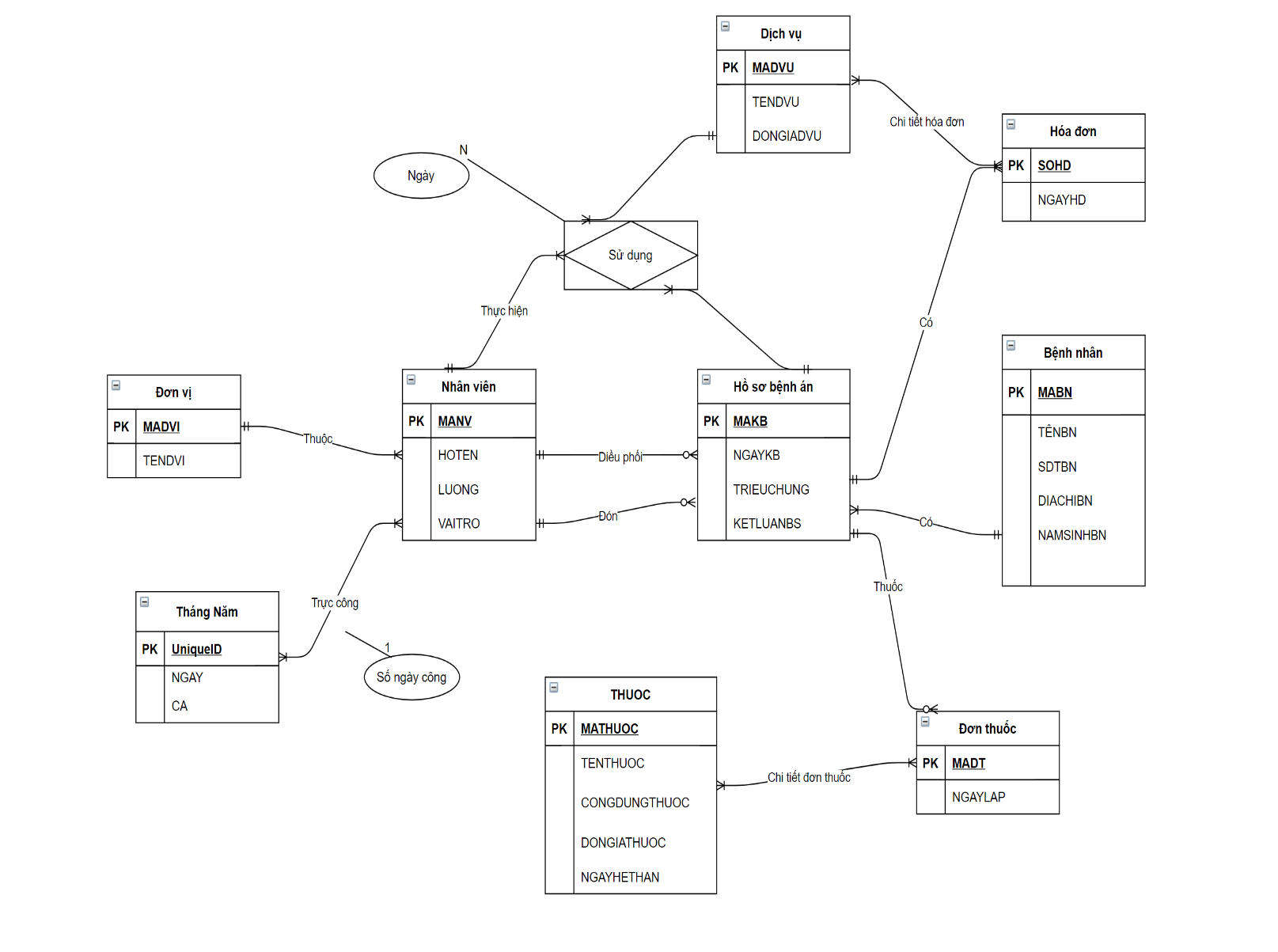
6. Bài giống nhau: tất cả đều 0 điểm.

# Phân công công việc

|  |  |  |  |
| --- | --- | --- | --- |
|  | Phạm Minh Khoa | Trần Hữu Hoàng | Huỳnh Ngọc Hòa |
| Phân hệ 1 | - Thiết kế ERD  - Viết báo cáo | - Thiết kế ERD | - Thiết kế ERD |
|  |  |  |  |
|  |  |  |  |

# Nội dung

## Thiết kế cơ sở dữ liệu



* DONVI(MADVI, TENDVI)
* cTHANGNAM(NGAY, CA)
* CTTRUCCONG(NGAY, CA, MANV, SONGAYTRUC)
* NHANVIEN(MANV, MADVI, TENNV, VAITRO,LUONG)
* HOADON(MAHD, MAKB, NGAYHD)
* CTHOADON(MADV, MAHD)
* DICHVU(MADVU, TENDV, DGIADVU)
* SUDUNG (MANV, MADV, MAKB, NGAYSUDUNG)
* HOSOKB(MAKB, MABN, MANV\_DON, MANV\_DIEUPHOI, NGAYKB, TRIEUCHUNG, KETLUANBS)
* BENHNHAN(MABN, TENBN, SDT, DIACHIBN, NAMSINHBN)
* DONTHUOC(MADT, MAKB, NGAYLAP)
* CTDONTHUOC(MATHUOC, MADT)
* THUOC(MATHUOC,TENTHUOC,CONGDUNGTHUOC,NGAYHETHAN,DONGIATHUOC)

## Phân hệ 1: Dành cho người quản trị cơ sở dữ liệu

* Proc xem người dùng có trong hệ thống:

create or replace procedure showAllUser

is

stmt varchar(1000);

begin

stmt := 'select username from dba\_users';

execute immediate(stmt);

end;

* Proc in ra quyền của user hoặc role trên đối tượng dữ liệu

create or replace procedure showPrivilegeOfUserOrRole

(granteename varchar2,obj varchar2)

is

grantee\_name varchar2(50) := granteename;

v\_obj varchar2(50) := obj;

stmt varchar2(1000);

begin

stmt := 'select \* from ' || v\_obj || ' where granteename = ' || grantee\_name;

end;

* Proc thêm, xóa, sửa hoặc cập nhập quyền của user hoặc role:

create or replace procedure CDUUserOrRole(objectname varchar2,pass varchar2 := null,CDU varchar2,obj varchar2)

is

object\_name varchar2(20) := objectname;

pwd varchar2(20) := pass;

c\_d\_u varchar2(20) := CDU;

v\_obj varchar2(20) := obj;

stmt varchar2(1000);

begin

if v\_obj != 'user' or v\_obj != 'role'

then

dbms\_output.put\_line('object must be role or user');

rollback;

end if;

if c\_d\_u = 'create'

then

stmt := 'create ' || v\_obj || ' ' || object\_name || ' identified by ' || pwd ;

elsif c\_d\_u = 'delete'

then

stmt := 'drop ' || v\_obj || ' ' || object\_name;

elsif c\_d\_u = 'update'

then

stmt := 'alter ' || v\_obj || ' ' || object\_name || ' identified by ' || pwd;

else

dbms\_output.put\_line('CDU must be create or delete or update');

rollback;

end if;

execute immediate(stmt);

end;

* Proc thu hồi quyền của user hoặc role:

create or replace procedure revokePriv(objectname varchar2, priv varchar2,obj varchar2 := null)

is

object\_name varchar2(20) := objectname;

v\_priv varchar2(20) := priv;

v\_obj varchar2(20) := obj;

stmt varchar2(1000);

begin

if v\_obj != null

then

stmt := 'revoke ' || v\_priv || ' on ' || obj || ' from ' || object\_name;

else

stmt := 'revoke ' || v\_priv || ' from ' || object\_name;

end if;

execute immediate(stmt);

end;

* Proc cấp quyền cho user hoặc role:

create or replace procedure grantPriv(objectname varchar2, priv varchar2,obj varchar2 := null,WRO char := '0',cot varchar2 := null)

is

object\_name varchar2(50) := objectname;

v\_priv varchar2(50) := priv;

v\_obj varchar2(50) := obj;

v\_wro char(1) := WRO;

v\_col varchar2(50) := cot;

stmt varchar2(1000);

begin

if (v\_priv = 'select' or v\_priv = 'update') and v\_col != null

then

if v\_obj != null

then

if v\_wro = '1'

then

stmt := 'grant ' || v\_priv || '(' || v\_col || ') on ' || obj || ' to ' || object\_name || ' with grant option';

else

stmt := 'grant ' || v\_priv || '(' || v\_col || ') on ' || obj || ' to ' || object\_name;

end if;

else

if v\_wro = '1'

then

stmt := 'grant ' || v\_priv || '(' || v\_col || ') to ' || object\_name || ' with grant option';

else

stmt := 'grant ' || v\_priv || '(' || v\_col || ') to ' || object\_name;

end if;

end if;

else

if v\_obj != null

then

if v\_wro = '1'

then

stmt := 'grant ' || v\_priv || ' on ' || obj || ' to ' || object\_name || ' with grant option';

else

stmt := 'grant ' || v\_priv || ' on ' || obj || ' to ' || object\_name;

end if;

else

if v\_wro = '1'

then

stmt := 'grant ' || v\_priv || ' to ' || object\_name || ' with grant option';

else

stmt := 'grant ' || v\_priv || ' to ' || object\_name;

end if;

end if;

end if;

execute immediate(stmt);

end;

* Proc chỉnh sửa quyền của user hoặc role:

create or replace procedure alterUserOrRole(objectname varchar2,obj varchar2,priv varchar2)

is

object\_name varchar2(100) := objectname;

v\_obj varchar2(100) := obj;

v\_priv varchar2(100) := priv;

stmt varchar2(1000);

begin

stmt := 'alter ' || v\_obj || ' ' || object\_name || ' ' || v\_priv;

execute immediate(stmt);

end;

### Các chính sách và phân quyền

## Phân hệ 2: Quản lý thông tin của một bệnh viện

### Lược đồ cơ sở dữ liệu

### Các chính sách bảo mật

#### DAC và RBAC

#### VPD

#### MAC (OLS)

#### Mã Hóa

* + - 1. Những chính sách

1. Đảm bảo tính bảo mật về lịch sử bệnh của bệnh nhân tránh trường hợp bị đánh cắp làm rò rỉ ảnh hưởng tới bệnh nhân. Cần mã hóa dữ liệu của bệnh nhân rồi lưu vào cơ sở dữ liệu. (VD: kẻ đánh cắp sẽ lấy thông tin này để đưa ra tòa án khi có tranh chấp).
2. Mã hóa tiền lương của nhân viên rồi lưu vào cơ sở dữ liệu.
   * + 1. Cài đặt

* Cài đặt chính sách (1)
* Dùng bộ thuật toán DES\_CBC\_PKCS5

#### Audit cơ bản và FGA

* + - 1. Những chính sách

1. Theo dõi việc login, logout của các user.(1)[[1]](#footnote-1)

Việc theo dõi này giúp ta giám giám sát hoạt động của nhân viên (làm đúng giờ, số giờ hoạt động trên hệ thống, tính toán đánh giá độ chăm chỉ làm việc.)

1. Giám sát hoạt động của bộ phận tiếp tân và điều phối bệnh: xóa, sửa thông tin bệnh nhân và hồ sơ bệnh nhân. (1)
2. Giám sát nhân viên phòng tài vụ cập nhật tiền về việc sử dụng các dịch vụ và hóa đơn tính tiền của bệnh nhân.(2)[[2]](#footnote-2)
3. Giám sát bác sĩ thêm, sửa những thông tin liên quan đến việc trị bệnh, các loại thuốc mà bác sĩ đã kê cho bệnh nhân. (2)
4. Giám sát nhân viên kế toán tính lương.
   * + 1. Cài đặt

Đầu tiên user cài đặt chính sách audit phải có quyền audit system (giám sát câu lệnh) và audit any (giám sát đối tượng). Bạn dùng 2 user sys và sysoper để giám sát.

Nếu bạn giám sát trong CDB thì đó là giám sát common user, còn PDB là giám sát local user.

Dưới đây đều thực hiện trên user SYS.

1. Cài đặt 1 chính sách standard audit

* Để thực hiện standard audit bạn cần phải mở SQLPLUS lên đăng nhập với user sys.
* Thay đổi tham số AUDIT\_TRAIL, mình chọn DB, EXTENDED để có thêm SQL TEXT và SQL BIND
* SHUTDOWN và STARTUP lại DATABASE sau khi thay đổi tham số.

Sau đây là những câu lệnh sau khi đăng nhập bằng user SYS vào SQLPLUS, thực hiện theo thứ tự:

* ALTER SYSTEM SET audit\_trail=db, EXTENDED SCOPE=SPFILE;
* SHUTDOWN IMMIDEATE
* STARTUP
* Thực hiện giám sát chính sách (2): Giám sát hoạt động của bộ phận tiếp tân và điều phối bệnh: xóa, sửa thông tin bệnh nhân và hồ sơ bệnh nhân. Các câu lệnh:
* AUDIT delete, update ON bv\_schema.benhnhan;
* Xem kết quả audit trong table sys.aud$ hoặc view dba\_common\_audit\_trail.
* SELECT audit\_type, db\_user, os\_user, object\_schema, object\_name, statement\_type,sql\_text, extended\_timestamp as "luc may gio"

FROM dba\_common\_audit\_trail

WHERE statement\_type = 'UPDATE' OR statement\_type = 'DELETE';

1. Cài đặt 1 chính sách FGA

* Không cần thiết lập tham số AUSIT\_TRAIL như standard audit.
* Chỉ cần dùng gói DBMS\_FGA và dùng thủ tục ADD\_POLICY để add các chính sách mà bạn cần audit.
* Add tối đa 256 chính sách trên 1 bảng hoặc view.
* Chọn chính sách (3) “Giám sát nhân viên phòng tài vụ cập nhật tiền về việc sử dụng các dịch vụ và hóa đơn tính tiền của bệnh nhân” để thực hiện vì nó yêu cầu giám sát trên cột. Cú pháp:
* begin

dbms\_fga.add\_policy

(

object\_schema => 'BV\_SCHEMA',

object\_name => 'HOADON',

policy\_name => 'chiphikhambenh\_audit',

audit\_column => 'TONGTIEN',

statement\_types => 'UPDATE, DELETE'

);

end;

# Đánh giá

# Tham khảo

1. File .pdf hướng dẫn đồ án của giảng viên.
2. Tham khảo Ternary relationship: <https://core.ac.uk/download/pdf/81570774.pdf>
3. Chính sách bảo mật OSL và VPD: <http://antoanthongtin.gov.vn/giai-phap-khac/co-che-an-toan-dua-vao-nhan-va-csdl-tren-oracle-100946>
4. Video cài đặt VPD: <https://www.youtube.com/watch?v=L8pYGkji-_g&t=14s&ab_channel=ToanTruongToanTruong>
5. link audit: <https://docs.oracle.com/cd/E11882_01/network.112/e36292/auditing.htm#DBSEG30002>
6. link cú pháp câu lệnh audit: <https://docs.oracle.com/cd/E11882_01/server.112/e41084/statements_4007.htm#SQLRF01107>
7. Mã hóa trên đường truyền (Mã trên C# rồi chuyển qua cho oracle): <https://stackoverflow.com/questions/14500914/oracles-dbms-crypto-des-cbc-pkcs-equivalent-in-c-sharp>. DES: [DESCryptoServiceProvider](http://msdn.microsoft.com/en-us/library/system.security.cryptography.descryptoserviceprovider.aspx) Dùng hàm này và chọn 2 thuộc tính còn lại (padding-PKCS5 and mode-CBC) trong hàm.
8. Mã hóa giữa oracle và C#: <https://community.oracle.com/tech/developers/discussion/2552665/aes128-encryption-compatible-with-oracle-and-c>
9. Hướng dẫn encrypt và decrypt: <https://codingsight.com/oracle-database-security-encryption-and-decryption/>

1. standart audit [↑](#footnote-ref-1)
2. FGA-Fine Grain Audit [↑](#footnote-ref-2)