**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC GIA TP HCM**

Nhóm thực hiện: Nhóm 9

GV phụ trách: Phạm Thị Bạch Huệ, Lương Vĩ Minh

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

HỌC KỲ II – NĂM HỌC 2019-2020

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

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |  |
| --- | --- | --- | --- |
| **Mã nhóm:** | NHÓM 9 | |  |
| **Số lượng:** | 5 thành viên | |  |
| **MSSV** | **Họ tên** | **Email** | **Chú thích** |
| 1712889 | Lê Thị Thanh Tuyền | 1712889@student.hcmus.edu.vn |  |
| 1712890 | Nguyễn Thị Thanh Tuyền | 1712890@student.hcmus.edu.vn |  |
| 1712895 | Trần Thị Diễm Uyên | 1712895@student.hcmus.edu.vn |  |
| 1712896 | Phạm Thị Cẩm Vân | 1712896@student.hcmus.edu.vn |  |
| 1712926 | Lương Tường Vy | 1712926@student.hcmus.edu.vn | Nhóm trưởng |

**Bảng phân công & đánh giá hoàn thành công việc**

|  |  |  |  |
| --- | --- | --- | --- |
| **Người thực hiện** | **Công việc thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| 1712889\_ Lê Thị Thanh Tuyền | Tạo cơ sở dữ liệu Bệnh viện  Hỗ trợ thêm dữ liệu  Thiết kế giao diện cho Phân hệ 2: giao diện cho Bác Sĩ, Nhân viên bán thuốc, Log in | 80% | 8/10 |
| 1712890\_ Nguyễn Thị Thanh Tuyền | Giao diện phân quyền, lấy lại quyền của một User/Role Script phân quyền, thu hồi quyền, kiểm tra quyền của chủ thể vừa được cấp | 70% | 7/10 |
| 1712895\_ Trần Thị Diễm Uyên | Phân tích, phân loại và cài đặt các chính sách cho nhóm người dùng: Nhóm quản lý tài nguyên và nhân sự, bộ phận tiếp tân và điều phối bệnh, nhân viên phòng tài vụ, Nhóm quản lý tài vụ, Trưởng phòng ban  Thêm dữ liệu cho cơ sở dữ liệu,  Cài đặt 1 cơ chế RBAC, 1 cơ chế DAC, 1 cơ chế VPD, 1 cơ chế mã hóa | 80% | 8/10 |
| 1712896\_ Phạm Thị Cẩm Vân | Xem danh sách các đối tượng hiện có trên CSDL (user, role, table, view, ....)  Thêm mới đối tượng (user, role, ...)  Xem quyền của một chủ thể, thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.  Cho phép chỉnh sửa quyền của user/ role.  Kịch bản audit ghi nhật ký hệ thống  Trình bày báo cáo phần đã thực hiện | 100% | 10/10 |
| 1712926\_ Lương Tường Vy | Phân tích, phân loại các chính sách cho nhóm người dùng: Nhóm quản lý chuyên môn, Bác sĩ, Nhân viên bộ phận bán thuốc, Nhân viên kế toán, Giám đốc bệnh viện  Thêm dữ liệu cho cơ sở dữ liệu  Cài đặt 1 cơ chế RBAC, 1 cơ chế DAC, 1 cơ chế OLS, 1 cơ chế VPD  Tổng hợp báo cáo | 80% | 8/10 |

Mục Lục

[**A.** **Yêu cầu của Đồ án** 4](#_Toc49750372)

[**B.** **Kết quả** 4](#_Toc49750373)

[I. PHÂN HỆ 1 4](#_Toc49750374)

[1. Ứng dụng quản trị hệ thống 4](#_Toc49750375)

[2. Kiểm tra dữ liệu nhật ký hệ thống 14](#_Toc49750376)

[II. PHÂN HỆ 2 18](#_Toc49750377)

[1. Lược đồ cơ sở dữ liệu 18](#_Toc49750378)

[2. Các chính sách, phân tích, phân loại 18](#_Toc49750379)

[3. Các chính sách đã cài đặt được 20](#_Toc49750380)

[4. Giao diện 22](#_Toc49750381)

[III. TÀI LIỆU THAM KHẢO 27](#_Toc49750382)

# **Yêu cầu của Đồ án**

<https://drive.google.com/drive/u/0/folders/1qaHro1EDXGS9-Ou562iIGymhxXHWVqBL>

# **Kết quả**

## PHÂN HỆ 1

### Ứng dụng quản trị hệ thống

Một số system object cần dùng trong việc quản trị người dùng trong hệ thống:

DBA\_TABLES: Hiển thị các tables có trong csdl

DBA\_USERS: Hiển thị những users có trong csdl

DBA\_ROLES: Hiển thị những role có trong csdl

DAB\_VIEWS: Hiển thị những view có trong csdl

DBA\_TAB\_PRIVS: Hiển thị các user và quyền trên các bảng của họ

DBA\_ROLE\_PRIVS: Hiển thị thông tin của user và role của chúng

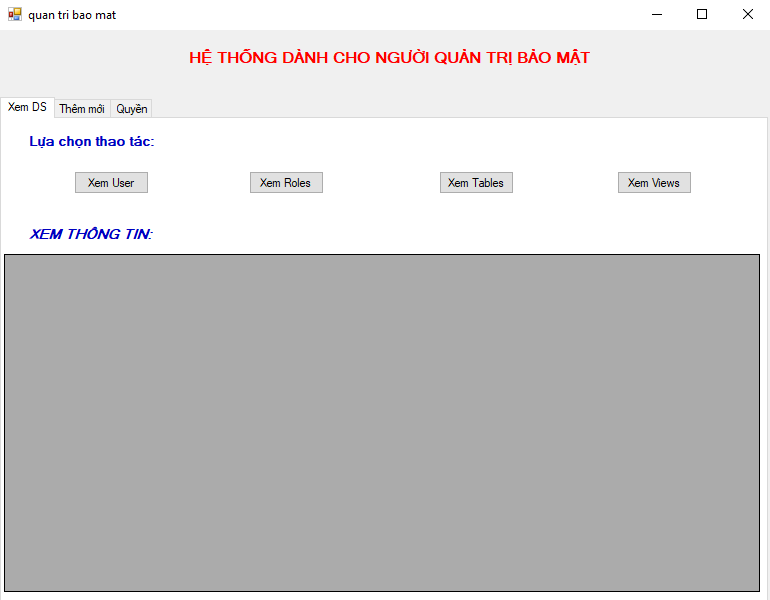
DBA\_COL\_PRIVS: thông tin gán quyền hệ thống mức cột

Thực hiện các thao tác trên giao diện và kiểm tra kết quả:

Đăng nhập vào User đã được cấp các quyền trên:

Giao diện HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ BẢO MẬT

Tab Xem DS: Xem danh sách các đối tượng hiện có trên hệ thống



Tab Thêm mới: Tạo Role, User

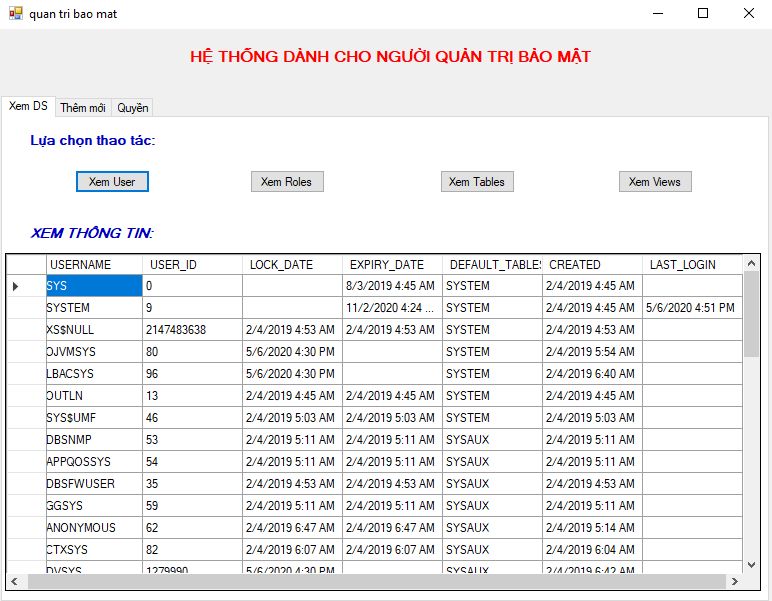


Tab Quyền: Xem các quyền của các đối tượng, user

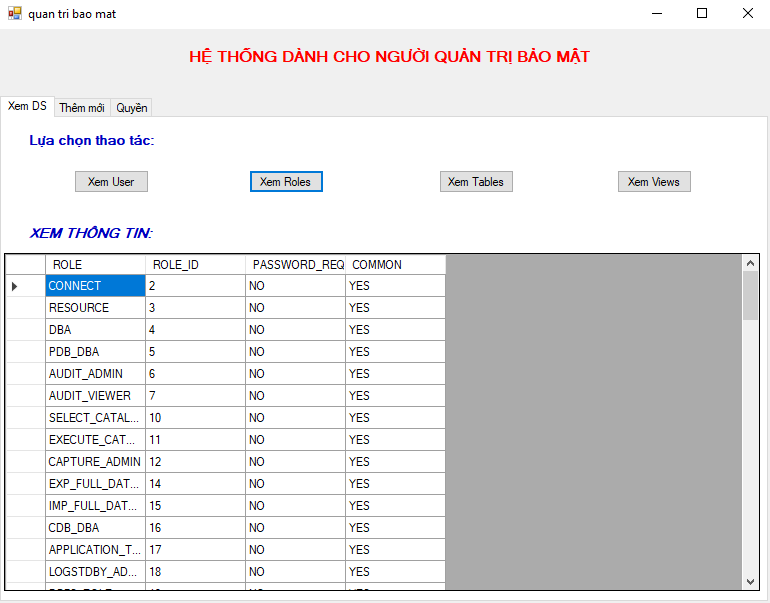
Mở tab Xem DS Để xem danh sách các đối tượng hiện có trên CSDL:

Lựa chọn đối tượng dữ liệu cần xem và kiểm tra kết quả:

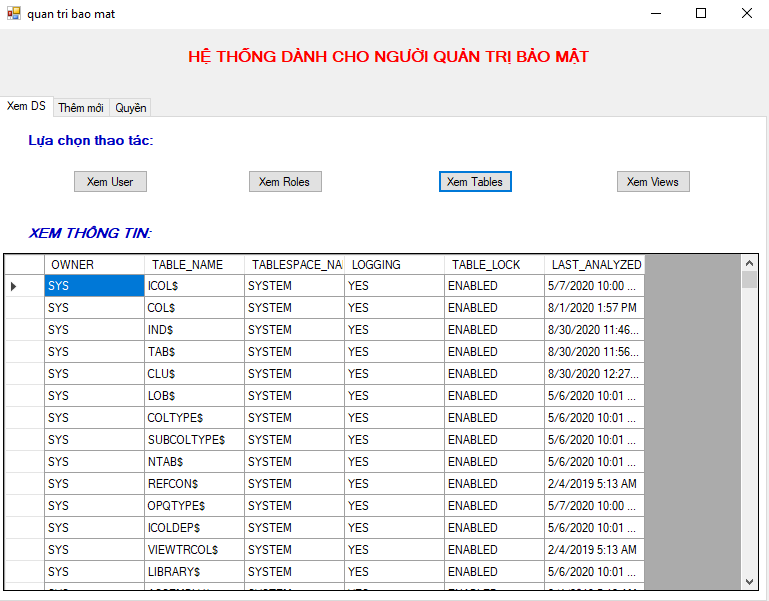
Xem USer



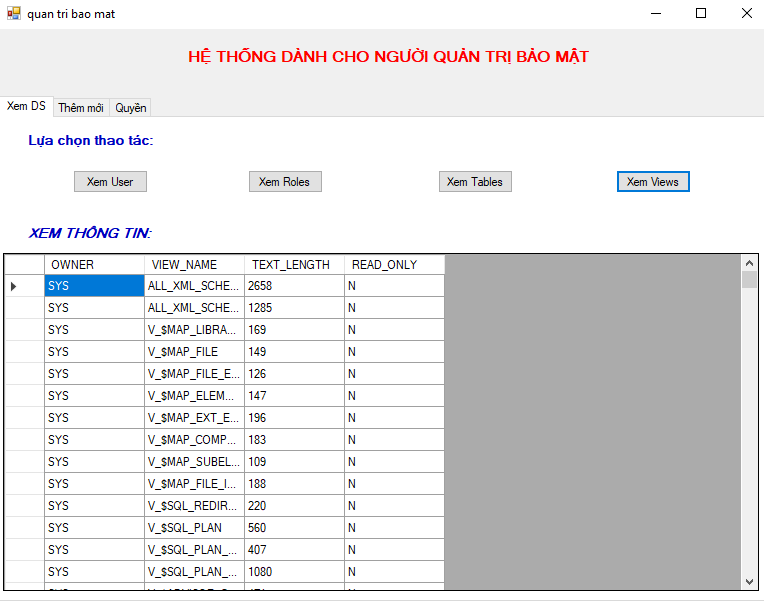
Xem Roles:



Xem Tables:

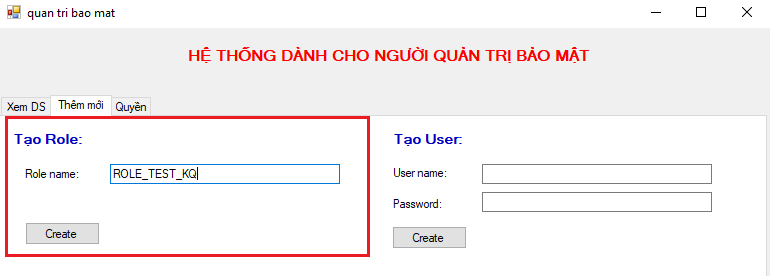


Xem Views:

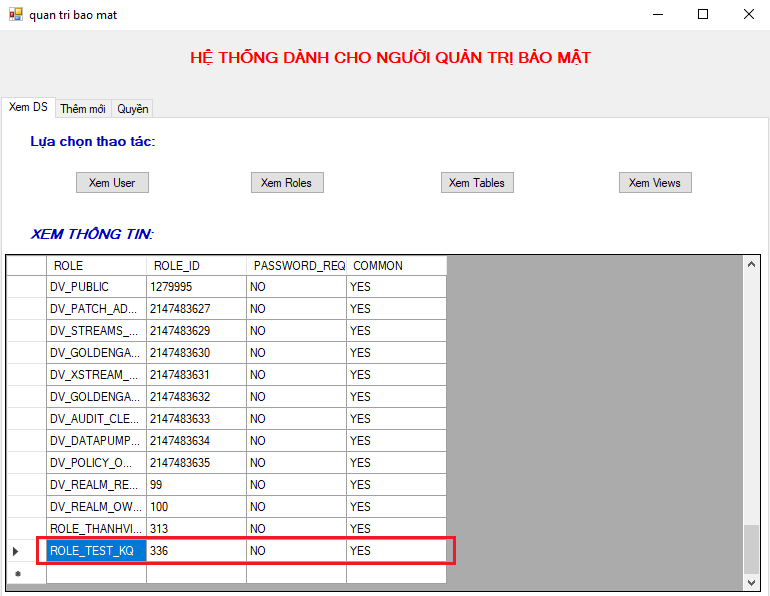


Mở tab Thêm mới để tạo một ROLE hoặc một USER:

Nhập tên Role cần tạo và chọn Create:



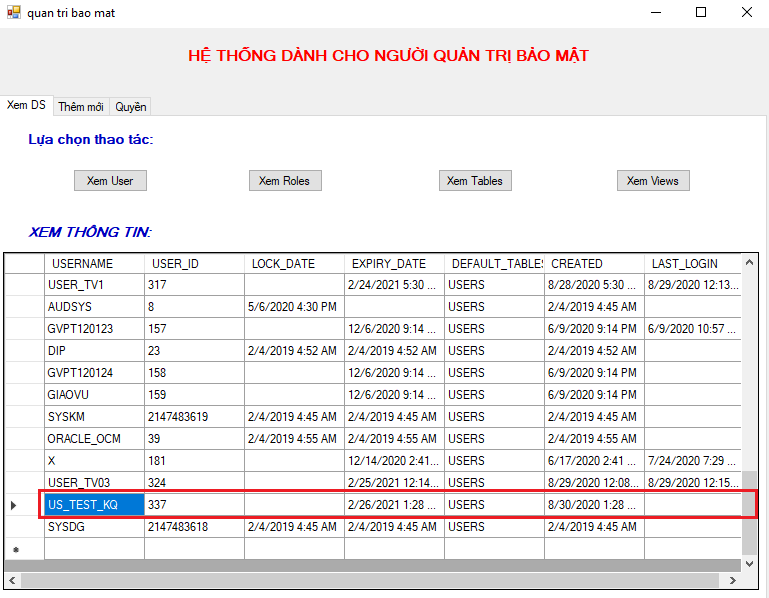
Kiểm tra kết quả: Role ROLE\_TEST\_KQ đã được tạo thành công



Nhập tên một User và mật khẩu:

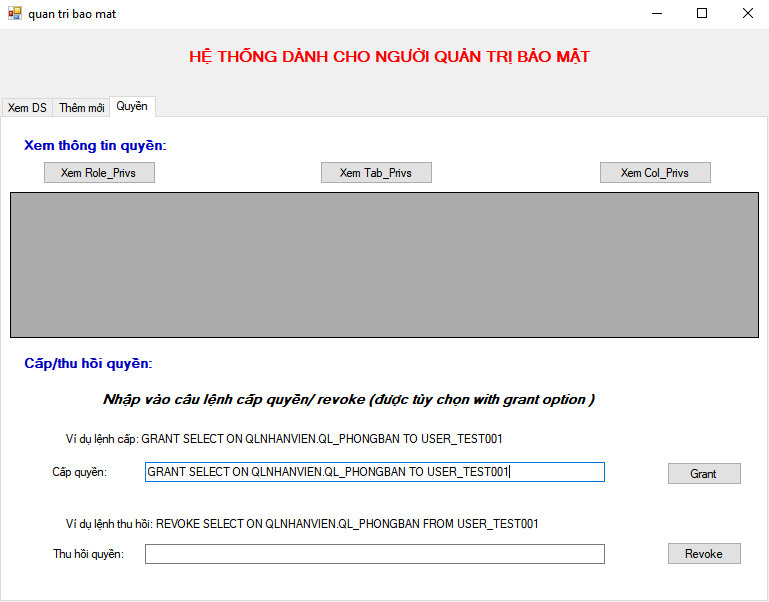


Kiểm tra kết quả: User đã tạo thành công

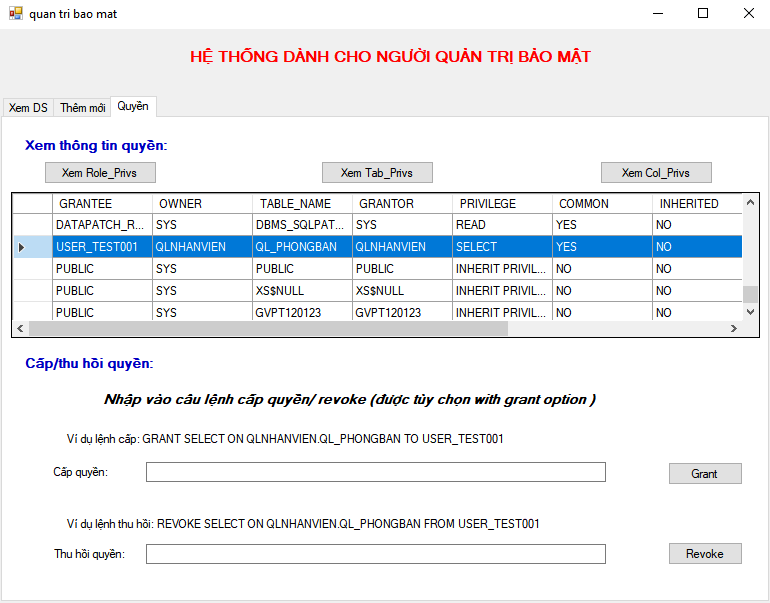


Cấp quyền/thu hồi quyền bên tab Quyền:

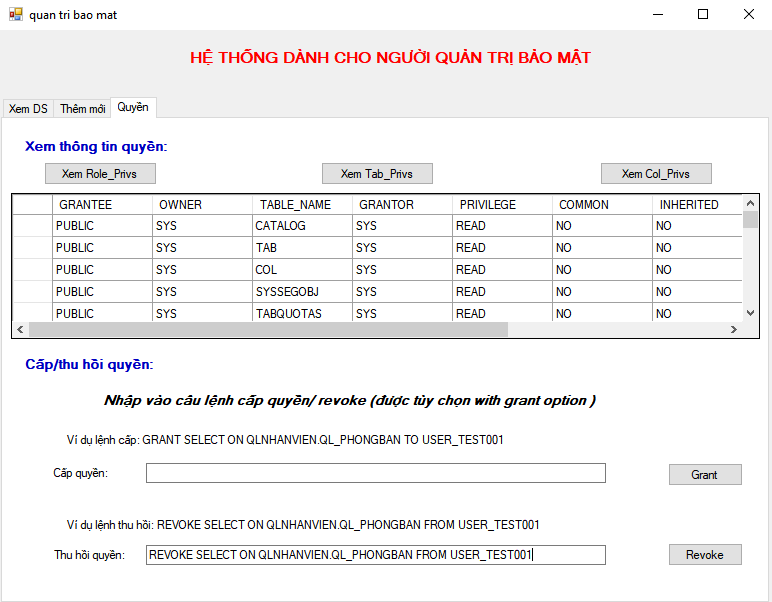
Câu lệnh: GRANT SELECT ON QLNHANVIEN.QL\_PHONGBAN TO USER\_DEMO\_TEST cấp quyền select cho user USER\_DEMO\_TEST:



Kiểm tra kết quả: quyền select đã được cấp cho User:



Câu lệnh: REVOKE SELECT ON QLNHANVIEN.QL\_PHONGBAN FROM USER\_DEMO\_TEST thu hồi lại quyền



Sau khi thực hiện câu lệnh thì quyền select của User đã bị thu hồi.

### Kiểm tra dữ liệu nhật ký hệ thống

***Về Audit***:

Bất cứ database user hợp pháp nào cũng có thể thiết lập lựa chọn giám sát đối với câu lệnh, quyền và đối tượng bất cứ khi nào. Tuy nhiên hệ csdl Oracle không sinh thông tin audit cho Standart database audit trail trừ khi csdl giám sát được kích hoạt

Có thể xemt ham số khởi tạo ban đầu ảnh hưởng tsoiw audit bằng câu lệnh:

SHOW PARAMETER AUDIT;

Để kích hoạt chức năng giám sát, thực hiện câu lệnh:

ALTER SYSTEM SET audit\_trail = DB SCOPE = SPFILE;

DB: Bật chức năng giám sát và các bảng ghi giám sát sẽ được lưu trong database audit trail

Để sử dụng lệnh AUDIT thiết lập lựa chọn về câu lệnh và quyền thì cần phải có quyền AUDIT SYSTEM.

Câu lệnh xóa toàn bộ bảng ghi:

DELETE FROM SYS.AUD$

Một số lệnh giám sát AUDIT:

|  |
| --- |
| ♣Giám sát tất cả các câu lệnh liên quan đến ROLE (create, alter, drop, set) không quan tâm câu lệnh được thực hiện thành công hay không:  AUDIT ROLE;  Giám sát tất cả câu lệnh liên quan đến ROLE nếu câu lệnh thực hiện thành công:  AUDIT ROLE WHENEVER SUCCESSFUL;  ♣Giám sá câu lệnh select hay update của bảng:  AUDIT SELECT, UPDATE TABLE;  Giám sát câu lệnh phát sinh bởi user USER01 và USER02 đối với câu truy vấn hay update một bảng nào đó:  AUDIT SELECT, UPDATE TABLE BY USER01, USER02;  Giám sát cho mỗi câu truy vấn tới bảng NHANVIEN trong với kết quả câu truy vấn không thành công:  AUDIT SELECT ON NHANVIEN WHENEVER NOT SUCCESSFUL;  Giám sát câu lệnh sử dụng quyền hệ thống DELETE ANY TABLE (giám sát xóa):  AUDIT DELETE ANY TABLE;  Giám sát cho mỗi câu lệnh insert và update bảng NHANVIEN:  AUDIT INSERT, UPDATE ON NHANVIEN;  Có thể thiết lập mặc định lựa chọn giám sát  Giám sát mặc định cho các đối tượng được tạo ra trong tương lai:  AUDIT ALTER, GRANT, INSERT, UPDATE, DELETE ON DEFAULT;  → Bất kì đối tượng nào được tạo ra sau đó sẽ tự động bị giám sát với đặc tả được lựa chọn đó khi chức năng giám sát được kích hoạt  - Nếu tạo ra một bảng thì Oracle tự động giám sát các câu lệnh ALTER, GRANT, INSERT, UPDATE, DELETE liên quan đến bảng này.  - Nếu tạo ra một view thì Oracle sẽ tự động giám sát các câu lệnh GRANT, INSERT, UPDATE, DELETE liên quan đến view này.  - Nếu tạo ra một procedure, function, package thì Oracle sẽ tự động giám sát các câu lệnh ALTER hay GRANT liên quan đến nó.  Tắt giám sát trên câu lệnh:  NOAUDIT ALL;  Tắt giám sát trên quyền:  NOAUDIT ALL PRIVILEGES;  Tắt giám sát trên đối tượng:  NOAUDIT DELETE ON NHANVIEN;  NOAUDIT SELECT, INSERT, DELETE ON NHANVIEN.LUONG; |

Xem thông tin audit tại các view:

DBA\_AUDIT\_TRAIL

DBA\_AUDIT\_EXISTS

DBA\_AUDIT\_OBJECT

DBA\_AUDIT\_POLICIES

DBA\_AUDIT\_POLICY\_COLUMNS

DBA\_AUDIT\_SESSION

DBA\_AUDIT\_STATEMENT

DBA\_COMMON\_AUDIT\_TRAIL

DBA\_FGA\_AUDIT\_TRAIL

DBA\_OBJ\_AUDIT\_OPTS

DBA\_PRIV\_AUDIT\_OPTS

DBA\_REPAUDIT\_ATTRIBUTE

DBA\_REPAUDIT\_COLUMN

DBA\_STMT\_AUDIT\_OPTS

***Kịch bản Audit đề xuất quản lý nhân viên của bệnh viện:***

Tạo user QLNHANVIEN, cấp quyền connect và dba cho QLNHANVIEN

Đăng nhập vào QLNHANVIEN, tạo các bảng, user cho việc mô tả kịch bản theo dõi hệ thống phân tích dữ liệu nhật ký (các hoạt động truy vấn của nhân viên, quản lý).

--tạo bảng

QL\_NHANVIEN(MANV, HOTEN, MAPB, LUONG)

QL\_PHONGBAN(MAPB, TENPB, TRPHG)

--tạo user

user Nhan vien: NV001

user Truong phong: NV101

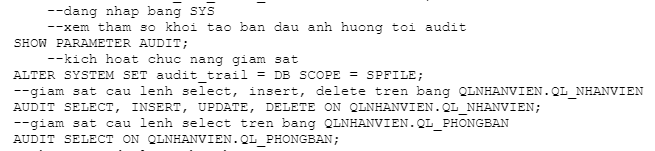
--insert dòng dữ liệu giúp mô tả kết quả các câu truy vấn, kết quả audit

Cài đặt một số chính sách bảo mật cho phép nhân viên, trưởng phòng được thao tác trên cơ sở dữ liệu tùy theo vai trò (sử dụng cơ chế bảo mật VPD).

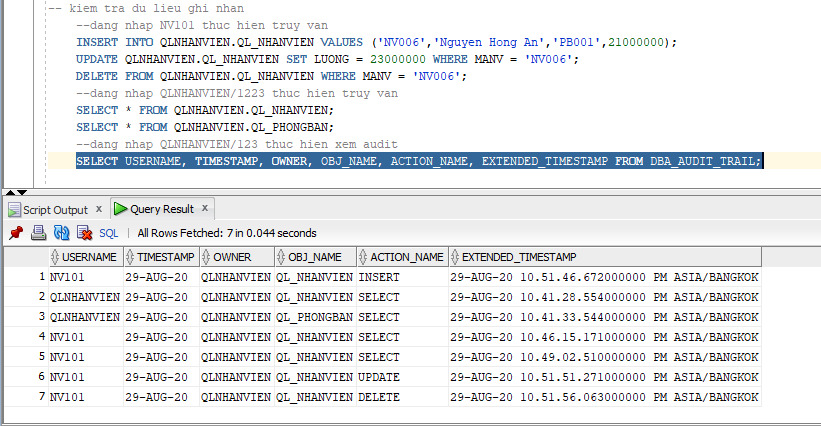
--Nhân viên chỉ được xem thông tin của chính mình

--Trưởng phòng được xem tất cả thông tin trên bảng phòng ban, trừ mã trưởng phòng (dòng không được phép xem sẽ hiển thị NULL). trưởng phòng được xem toàn bộ và cập nhật thông tin nhân viên

Đăng nhập SYS để kích hoạt và thiết lập AUDIT:



Kết quả audit:



***Cài đăt ghi nhật ký Audit một số thông tin ở hệ thống Bệnh Viên đã cài đặt:***

Đang nhập SYS để kích hoạt AUDIT:

Dựa vào các chính sách bảo mật yêu cầu có một số đề suất ghi nhật ký AUDIT sau (các bảng chứa dữ liệu quan trọng, cần giám sát, ghi lại các hoạt động của user trên các bảng):

- Ghi nhật ký audit thêm, xóa, sửa trên bảng BACSI, NHANVIEN

- Ghi nhật ký audit them xóa sửa trên bảng PHONGBAN nếu thành công

- Ghi nhật ký auditupdate luong, select PHUCAP

- Ghi nhật ký auditthêm sửa THUTUC

Tiến hành kích hoạt và cài đặt AUDIT trên bảng.

Xem thông tin nhật ký Audit trên bảng bằng lệnh: SELECT \* FROM DBA\_AUDIT\_TRAIL;

***\* Note:***

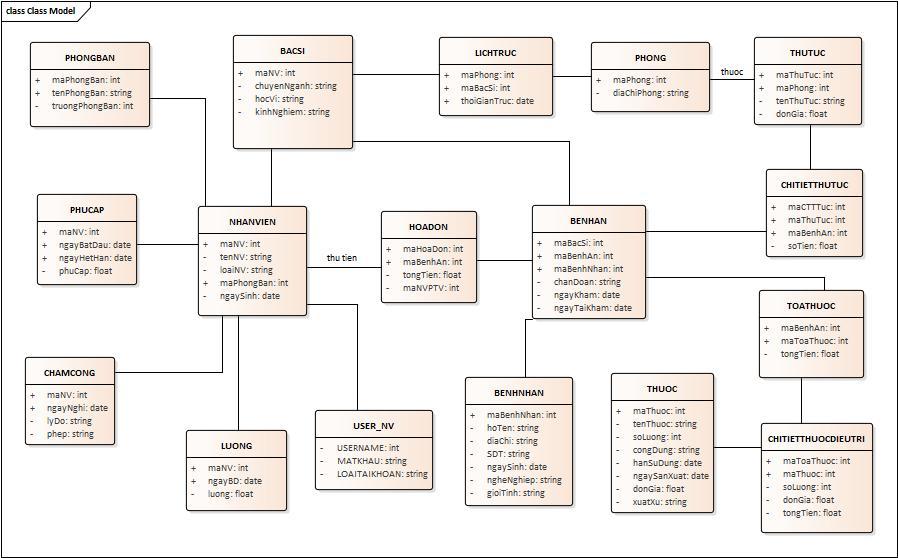
Nếu muốn dùng tài khoản khác để giám sát AUDIT thì phải execute 2 gói sau:

GRANT EXECUTE ON DBMS\_FGA TO <Tên tài khoản>;

GRANT SELECT ON DBA\_FGA\_AUDIT\_TRAIL <Tên tài khoản>;

## PHÂN HỆ 2

### Lược đồ cơ sở dữ liệu



### Các chính sách, phân tích, phân loại

* Nhóm quản lý tài nguyên và nhân sự xem, thêm, xóa, sửa, phòng ban, bác sĩ, nhân viên, chấm công, phụ cấp, lịch trực. Xem bảng lương (RBAC)
* Nhóm bộ phận tiếp tân và điều phối bệnh thêm, xóa, sửa, xem bệnh nhân và thêm, xem bệnh án (mã bệnh án, mã bác sĩ, mã bệnh nhân) và xem lịch trực, phòng. (RBAC)
* Nhóm nhân viên phòng tài vụ được phép xem, cập nhật chi tiết thủ tục (số tiền). Được phép xem thủ tục, bệnh án (mã bệnh nhân, mã bác sĩ, mã bệnh án), chi tiết thủ tục. (RBAC)
* Nhóm quản lý tài vụ được xem, chỉnh sửa thủ tục, chi tiết thủ tục. Được xem bệnh án, bệnh nhân.   (RBAC)
* Trưởng phòng ban được phép xem thông tin tất cả nhân viên phòng ban của mình (DAC)
* Tất cả nhân viên (trừ viện trưởng, nhóm quản lý tài nguyên và nhân sự) được xem lương của bản thân mình (VPD)
* 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. (RBAC)
* Xem được bảng: Bệnh án, Chi tiết thủ tục, Bệnh nhân, Toa thuốc, Chi tiết thuốc điều trị
* 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 gồm các bảng. 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. (VPD + RBAC)
* Xem được bảng: Thủ tục, Thuốc
* Xem và cập nhật được bảng: Bệnh án, Toa thuốc, Chi tiết thủ tục, Chi tiết thuốc điều trị của những bệnh nhân mà mình điều trị.
* 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. (RBAC)
* Xem được bảng: Toa thuốc, Chi tiết thuốc điều trị, Thuốc
* Cập nhật được trường “đơn giá”, “tổng tiền” của bảng Chi tiết thuốc điều trị
* Cập nhật được trường “tổng tiền” của bảng Toa thuốc
* 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. (RBAC)
  + Xem được bảng: Nhân viên, Phụ Cấp, Chấm công
  + Thêm thông tin vào bảng: Lương
* Hash mật khẩu trong bảng User sử dụng kĩ thuật hash (password + salt) (Hash)
* Bảng thông báo cho nhân viên sẽ được đánh dấu các mức độ “Không nhạy cảm”, “Nhạy cảm”, “Bí mật”, thuộc các nhóm như “Nhân viên”, “Kế toán”, “Quản lý”, thuộc các khu vực như “Hà Nội”, “Đà Nẵng”, “TP Hồ Chí Minh”. (OLS)
* Mã hóa trường Lương của Bảng Lương (Mã hóa).
* Giám đốc bệnh viện được xem thông tin của tất cả nhân viên gồm (Mã nhân viên, họ tên nhân viên, loại nhân viên, mã phòng ban, ngày sinh, lương (DAC).
  + Xem được bảng: Nhân viên

### Các chính sách đã cài đặt được

* Nhóm quản lý tài nguyên và nhân sự xem, thêm, xóa, sửa, phòng ban, bác sĩ, nhân viên, chấm công, phụ cấp, lịch trực. Xem bảng lương (RBAC)
* Nhóm bộ phận tiếp tân và điều phối bệnh thêm, xóa, sửa, xem bệnh nhân và thêm, xem bệnh án (mã bệnh án, mã bác sĩ, mã bệnh nhân) và xem lịch trực, phòng. (RBAC)
* Nhóm nhân viên phòng tài vụ được phép xem, cập nhật chi tiết thủ tục (số tiền). Được phép xem thủ tục, bệnh án (mã bệnh nhân, mã bác sĩ, mã bệnh án), chi tiết thủ tục. (RBAC)
* Nhóm quản lý tài vụ được xem, chỉnh sửa thủ tục, chi tiết thủ tục. Được xem bệnh án, bệnh nhân.   (RBAC)
* Tất cả nhân viên (trừ viện trưởng, nhóm quản lý tài nguyên và nhân sự) được xem lương của bản thân mình (VPD)
* Trưởng phòng ban được phép xem thông tin tất cả nhân viên phòng ban của mình (DAC)
* 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. (RBAC)
* 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 gồm các bảng. 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. (RBAC, VPD)
* 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. (RBAC)
* 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. (RBAC)
* Giám đốc bệnh viện được xem thông tin của tất cả nhân viên gồm (Mã nhân viên, họ tên nhân viên, loại nhân viên, mã phòng ban, ngày sinh, lương (DAC).
* Nhân viên được xem thông tin của bản thân (RBAC).
* Hash mật khẩu trong bảng User sử dụng kĩ thuật hash (password + salt + username) (Mã hóa)
* Audit nhật ký hệ thống

### Giao diện

A screenshot of a cell phone

Description automatically generated

* Giao diện login dùng để đăng nhập, tùy vào loại tài khoản nào khi nhấn đăng nhập sẽ ra giao diện tương ứng

A screenshot of a cell phone

Description automatically generated

* Đây là giao diện của giám đốc bệnh viện (vừa là bác sĩ vừa là giám đốc). Giám đốc được xem thông tin của tất cả nhân viên trong bệnh viện (DAC)

A screenshot of a cell phone

Description automatically generated

* Chức năng xem thông tin nhân viên của giám đốc

A screenshot of a cell phone

Description automatically generated

* Chức năng kê toa thuốc của bác sĩ

A screenshot of a cell phone

Description automatically generated

* Chức năng xem thông tin cá nhân, mỗi nhân viên chỉ có thể xem thông tin cá nhân của mình

A screenshot of a cell phone

Description automatically generated

* Giao diện bác sĩ cũng giống như giám đốc, nhưng chức năng xem thông tin nhân viên bị che lại và không được sử dụng

A screenshot of a cell phone

Description automatically generated

* Đây là giao diện của nhân viên bán thuốc. Nhân viên bán thuốc chỉ được xem toa thuốc, chi tiết toa thuốc và giá tiền để bán cho khách

## TÀI LIỆU THAM KHẢO

<https://o7planning.org/vi/10363/cac-ham-xu-ly-chuoi-trong-oracle>

<https://stackoverflow.com/questions/20988572/getting-ora-01031-insufficient-privileges-while-querying-a-table-instead-of-ora>

<https://docs.oracle.com/cd/B16240_01/doc/em.102/b40007/policies.htm>

<http://www.oravn.com/post25239.html>

<https://o7planning.org/vi/11309/kiem-soat-chuan-he-thong-database-oracle-audit-standard>

<https://toc.123doc.net/document/795047-chuong-ii-co-so-du-lieu-rieng-ao-vpd-trong-oracle.htm>

<https://text.123doc.net/document/2605348-tim-hieu-ve-co-so-du-lieu-rieng-ao-trong-oracle.htm>

<http://m.antoanthongtin.gov.vn/giai-phap-khac/co-che-an-toan-dua-vao-nhan-va-csdl-tren-oracle-100946>

<https://stackoverflow.com/questions/37567293/an-into-clause-is-expected-in-this-select-statement-when-working-with-plsql?rq=1>

<https://stackoverflow.com/questions/25486543/pls-00428-an-into-clause-is-expected-in-this-select-statement>

<https://csc.edu.vn/lich-khai-giang/lap-trinh-va-csdl>

**~HẾT~**