Số thứ tự nhóm trên danh sách đăng ký: 20H3T01-20_1

Mã số sinh viên và họ tên các thành viên:

20120049 - Nguyễn Hải Đăng;

20120138 – Lê Thành Nam;

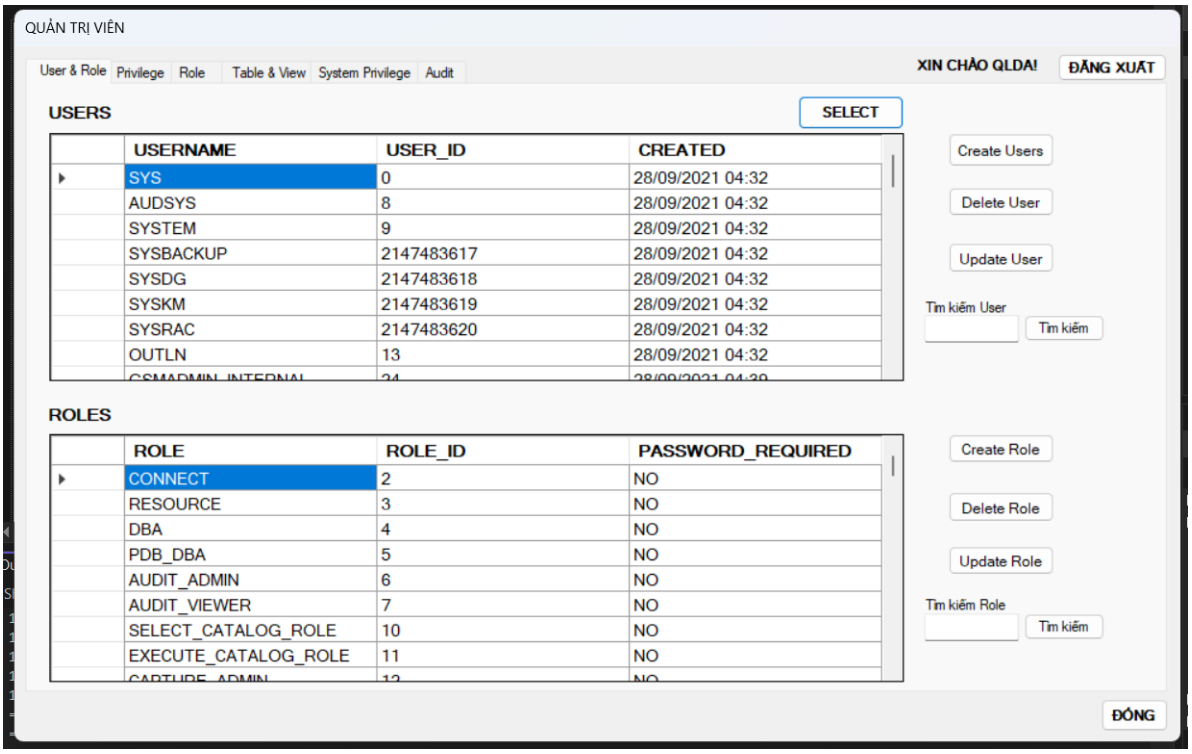
20120187 - Nguyễn Viết Thái;

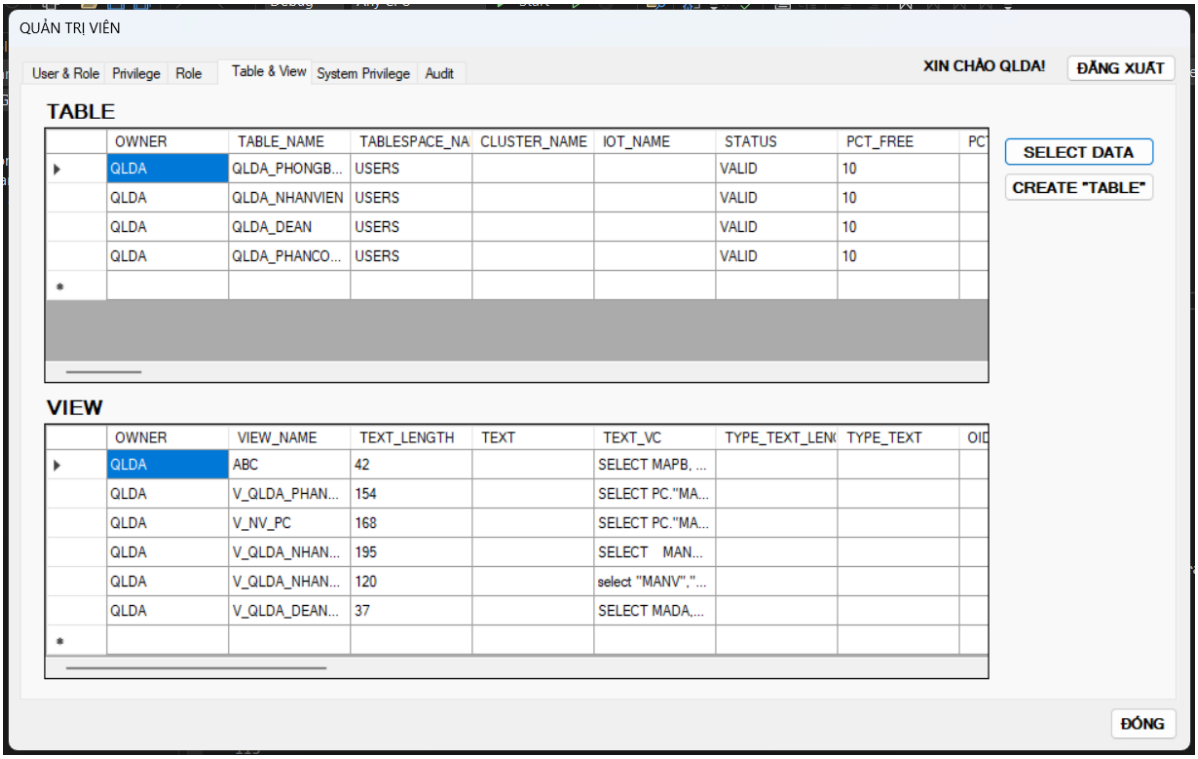
20120289 – Võ Minh Hiếu

Phân hệ	CÔNG VIỆC	NGƯỜI THỰC HIỆN
1	Tạo database + Insert dữ liệu	Lê Thành Nam
1	Xem danh sách người dùng trong hệ thống.	Lê Thành Nam
1	Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.	Nguyễn Viết Thái
1	Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.	Nguyễn Viết Thái
1	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.	Nguyễn Hải Đăng
1	Cho phép thu hồi quyền từ người dùng/ role.	Võ Minh Hiếu
1	Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.	Võ Minh Hiếu
1	Cho phép chỉnh sửa quyền của user/ role.	Nguyễn Hải Đăng
2	Tạo database, Insert dữ liệu, Access Control: Chính sách 1	Lê Thành Nam
2	Access Control: Chính sách 2, 3	Nguyễn Viết Thái
2	Access Control: Chính sách 4, 5	Võ Minh Hiếu
2	Access Control: Chính sách 6; Giải quyết xung đột chính sách	Nguyễn Hải Đăng
2	Mã hóa dữ liệu: Viết các hàm mã hóa, giải mã dữ liệu	Lê Thành Nam
2	Mã hóa dữ liệu: Xây dựng chiến lược mã hóa, viết code mã hóa theo chiến lược đã chọn	Võ Minh Hiếu
2	OLS: Tạo chính sách OLS, gán nhãn người dùng và dữ liệu	Nguyễn Hải Đăng
2	Audit: Ghi vết hệ thống	Nguyễn Viết Thái

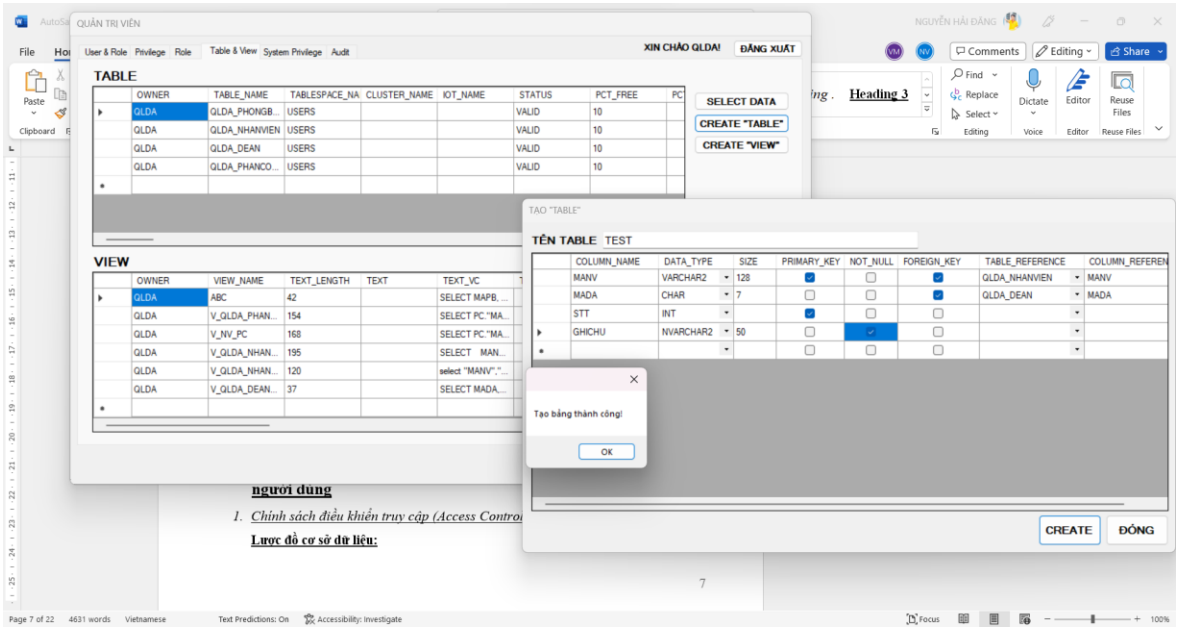
PHÂN HỆ 1:

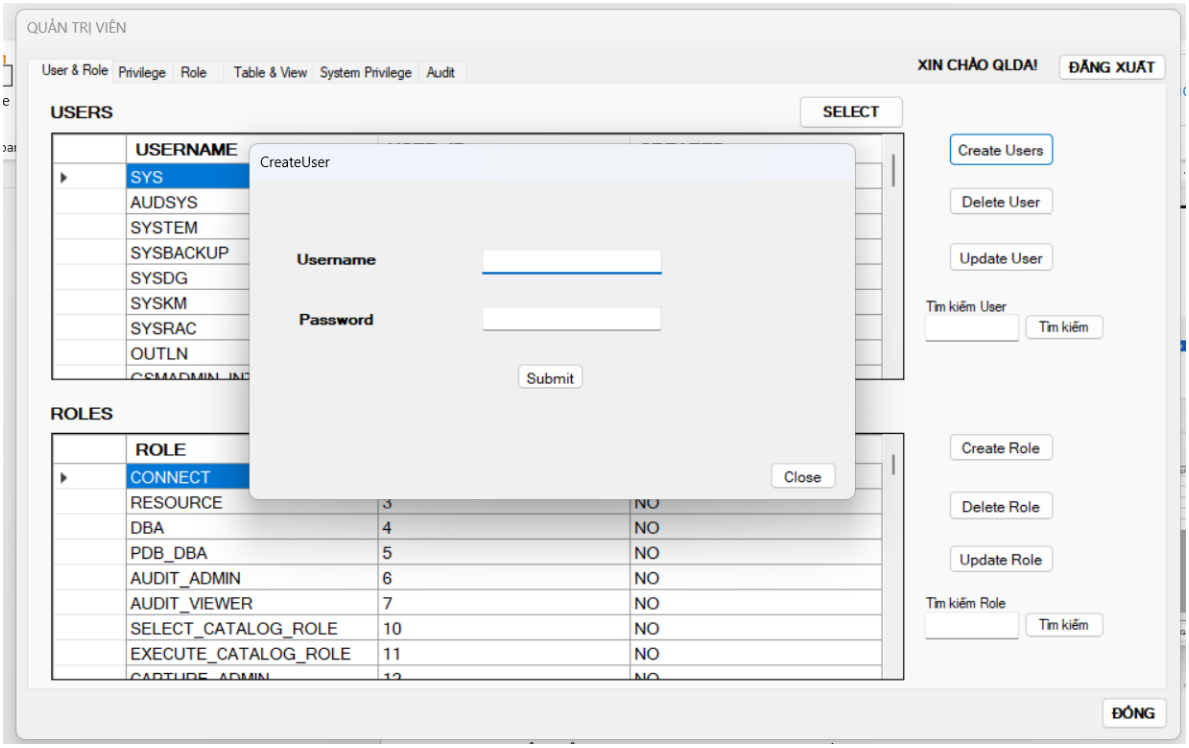
Giao diện xem danh sách tên các đối tượng bạn đã tạo trong trong CSDL (user, role, table, view,...)

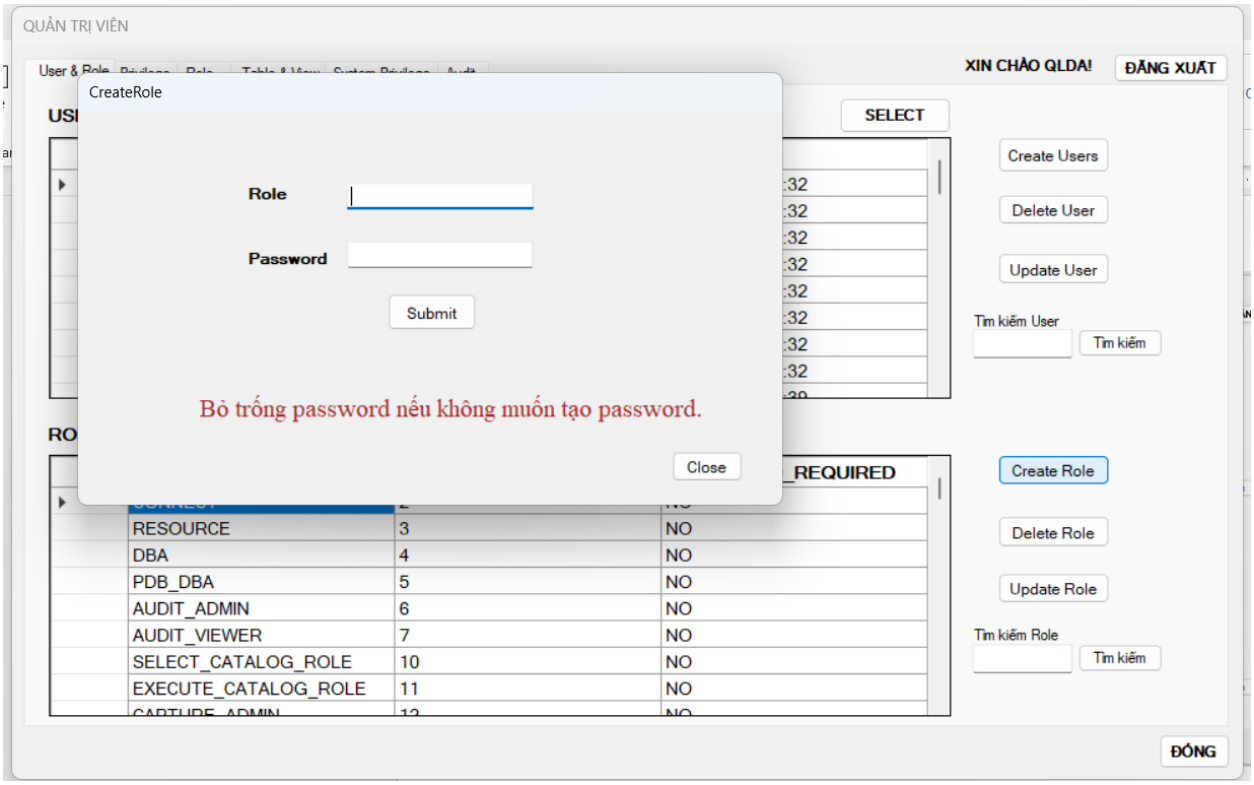




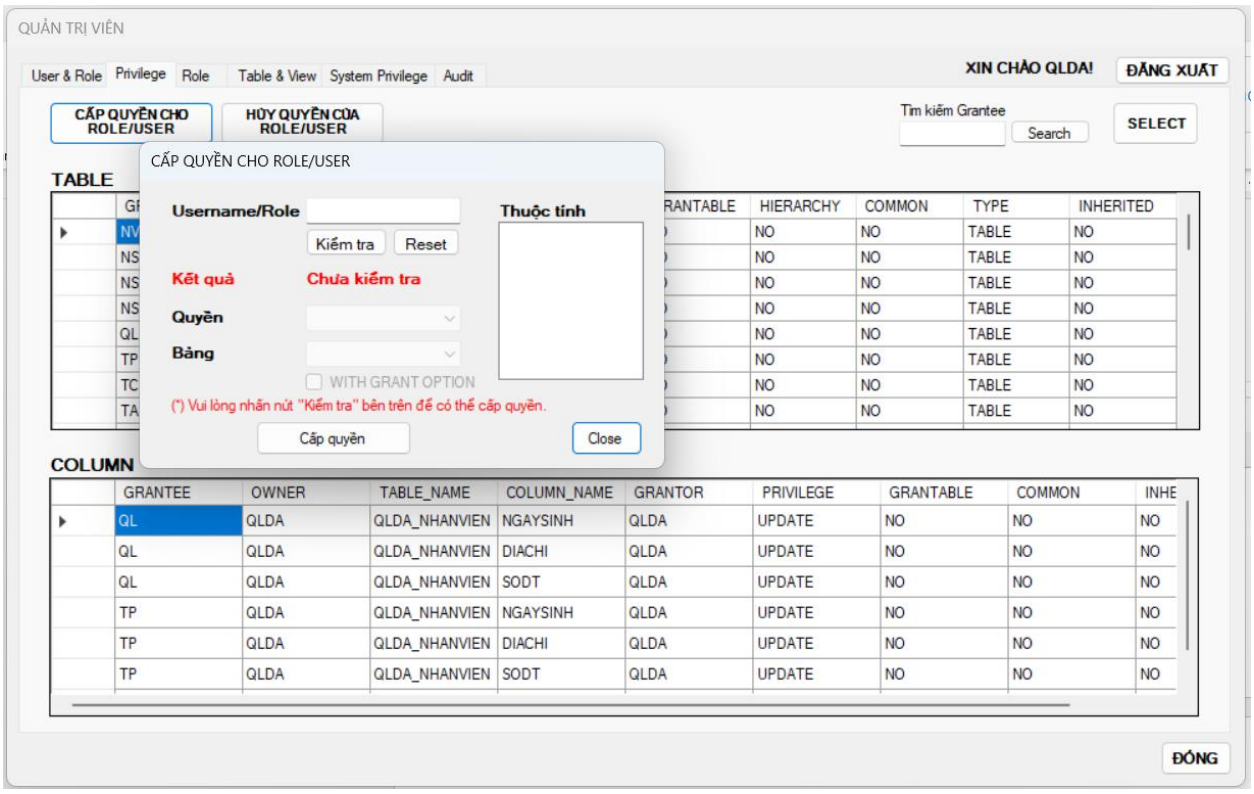
Giao diện cho phép Admin thêm mới đối tượng (table, role, user, ...)

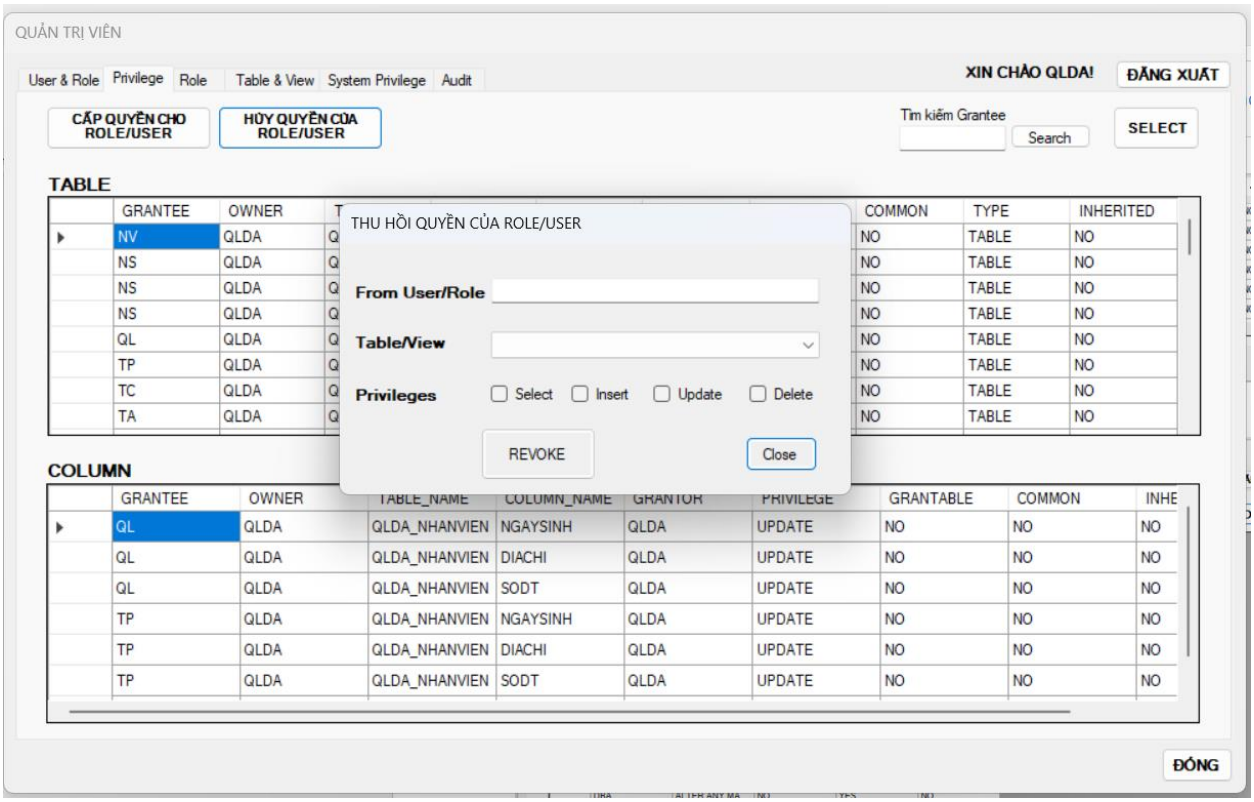


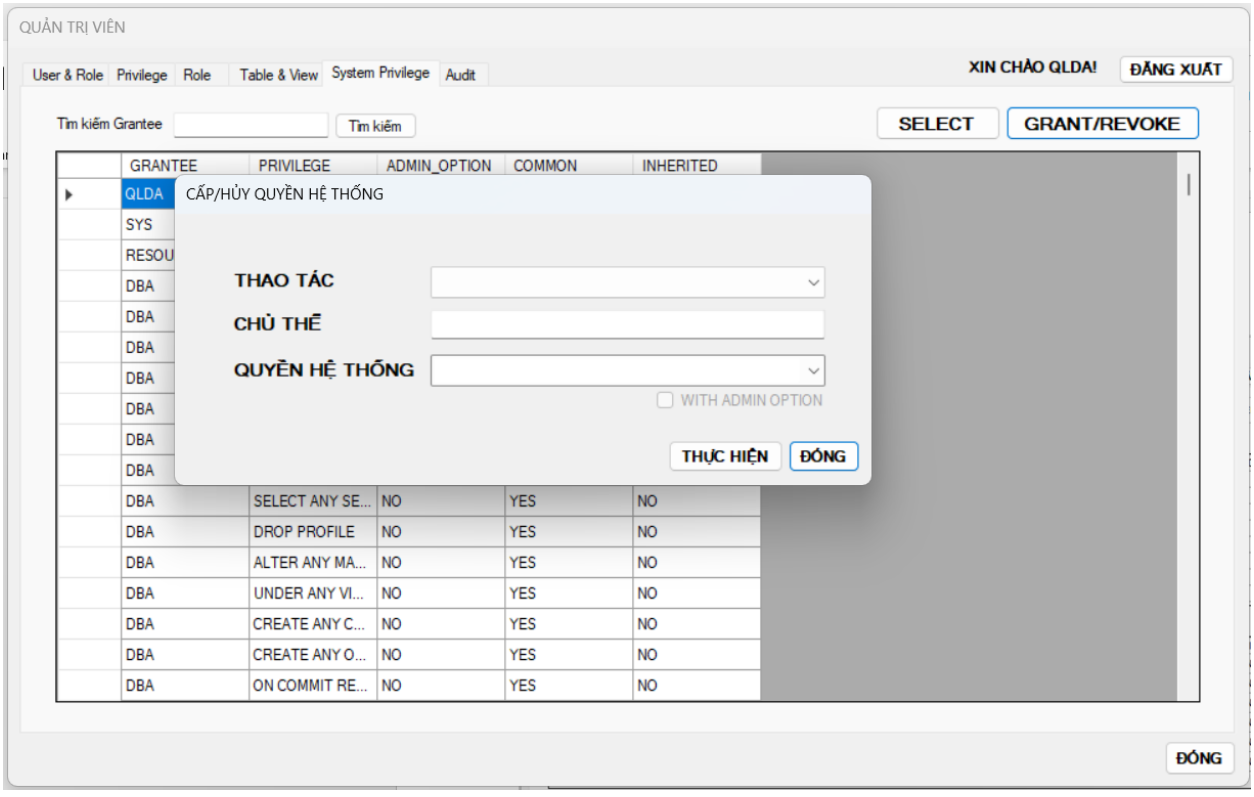




Giao diện cho phép thêm quyền/ Lấy lại quyền của user/ role.

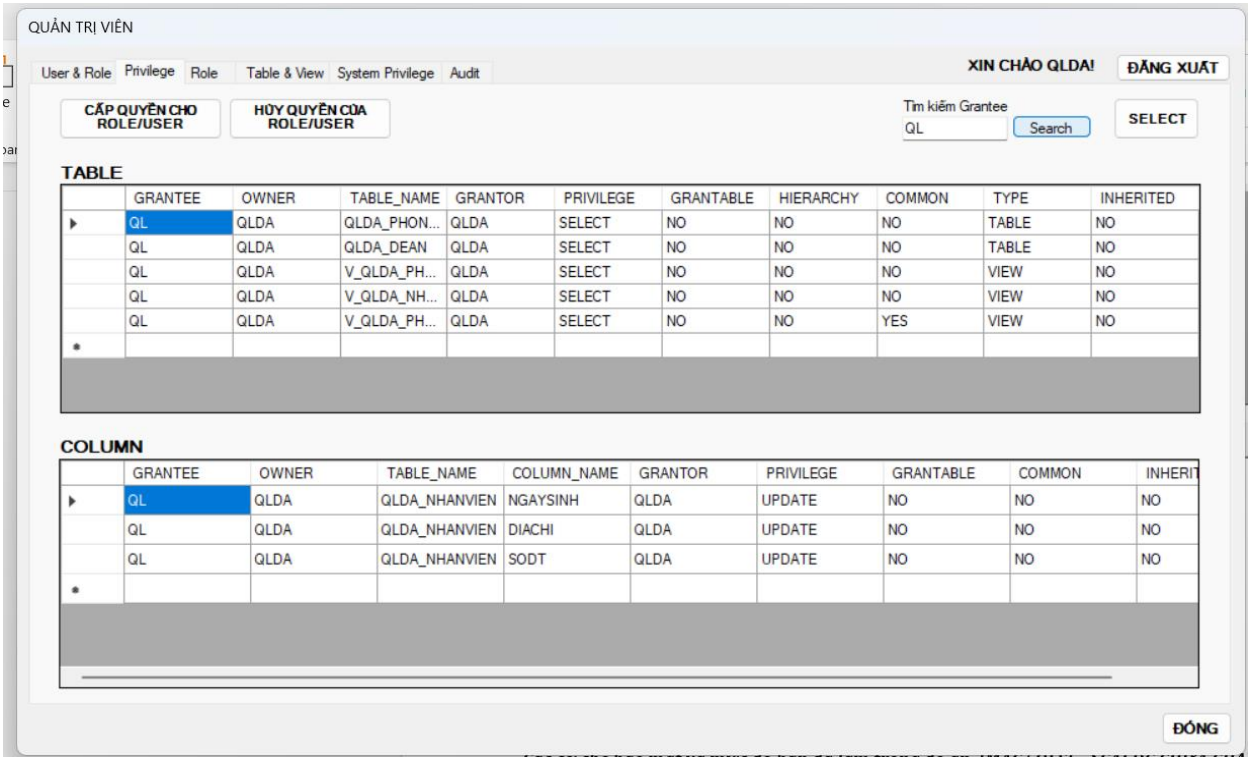


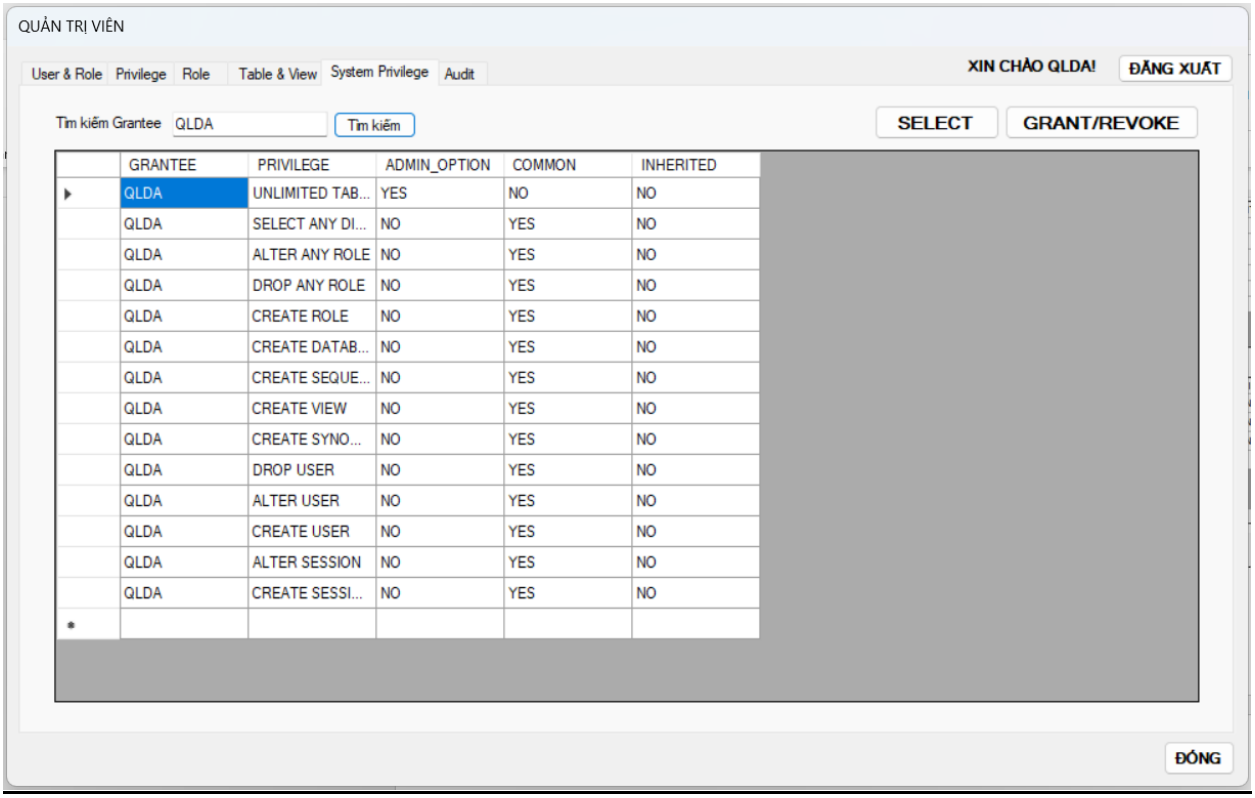


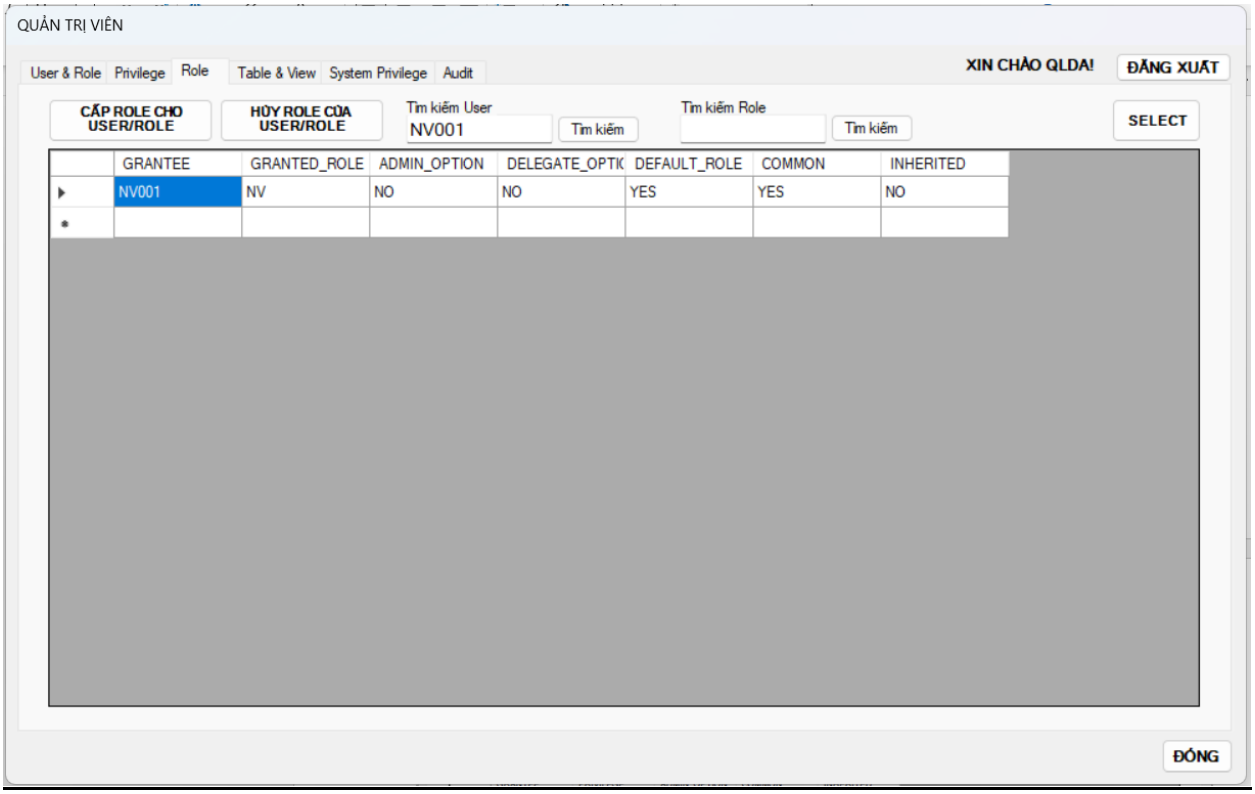


Giao diện cho phép xem quyền của một chủ thể.

(có thể search 1 chủ thể)







<u>PHÂN HỆ 2</u>:

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [DAC+RBAC]

- RBAC: tạo 7 role: Nhân viên (NV), Quản lý (QL), Trưởng phòng (TP), Tài chính (TC), Nhân sự (NS), Trưởng đề án (TA), Giám đốc (GD) và cấp quyền cho các role theo 6 chính sách bảo mật. Sau đó cấp role cho các user.
- RBAC: Có một số chính sách cần sử dụng view và cấp quyền trên view cho các role.
    - NHANVIEN: tạo 2 view V_QLDA_NHANVIEN và V_QLDA_NHANVIEN_NS và cấp quyền trên view cho các role (không cấp quyền thao tác trên table). V_QLDA_NHANVIEN select được toàn bộ quan hệ NHANVIEN (cấp VPD trên view này), V_QLDA_NHANVIEN_NS cũng vậy nhưng thuộc tính LUONG, PHUCAP sẽ bị DECODE thành NULL nếu như người dùng xem LUONG, PHUCAP của người khác **<u>(CBAC)</u>** (cấp VPD trên view này)
    - PHANCONG: tạo 1 view V_QLDA_PHANCONG_QL và cấp quyền trên view này cho Quản lý.

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [VPD]

Tất cả các chính sách đều có sử dụng cơ chế VPD, có thể là trực tiếp trên table hoặc trên các view đã tạo ở trên. Bởi vì cả 6 role đều có vai trò như một nhân viên thông thường, nhưng có một số role được xem nhiều hơn nhân viên thông thường.

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [MAC/ OLS]

→ CÀI ĐƯỢC, ĐÃ CHẠY ĐƯỢC

Ở câu 3, chúng em sử dụng OLS để gán nhãn cho các 3 người dùng ở câu a, cho 2 người dùng ở câu b và c, 2 người dùng cho câu d (kịch bản khác).

Gán nhãn cho các dòng thông báo trong bảng THONGBAO, có 8 dòng thông báo với 8 nhãn khác nhau để kiểm tra độ chính xác của chính sách đã cài.

Cài đặt xem bảng THONGBAO trên ứng dụng cho một vài người dùng.

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [Mã hóa]

Sử dụng chính sách tính toán ra khóa để mã hóa và giải mã dữ liệu. Không cần lưu khóa qua database hay ứng dụng, mỗi nhân viên có một khóa khác nhau.

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [Standard Audit]

Cả 3 yêu cầu a,b,c của câu 4 đều cần dùng FGA vì FGA mới có thể audit trên thuộc tính cụ thể.

Các cơ chế bảo mật và mức độ bạn đã làm trong đồ án. [Fine-Grained Audit]

- Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG (cài trên table).
- Những người đã đọc trên trường LUONG và PHUCAP của người khác (cài trên table và view).
- Một người không thuộc vai trò "Tài chính" nhưng đã cập nhật thành công trên trường LUONG và PHUCAP (cài trên 2 view bởi vì cài trên table sẽ bị lỗi ORA-00600).

Phát biểu các chính sách bảo mật mà bạn đã ép thỏa dùng DAC + RBAC?

Chính sách 1: Những người có VAITRO là "Nhân viên" cho biết đó là một nhân viên bình thường, không kiêm những công việc nào khác. Những người dùng có VAITRO là "Nhân viên" có các quyền được mô tả như sau:

- Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến nhân viên đó.
- Có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.
- Có thể xem dữ liệu của toàn bộ quan hệ PHONGBAN và DEAN.

Chính sách 2: Những người dùng có VAITRO là "QL trực tiếp" nếu họ phụ trách quản lý trực tiếp nhân viên khác. Nhân viên Q là quản lý trực tiếp của nhân viên N, có quyền được mô tả như sau:

- Q có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng dữ liệu trong quan hệ NHANVIEN liên quan đến các nhân viên N mà Q quản lý trực tiếp thì Q được xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP **(CBAC)**.
- Có thể xem các dòng trong quan hệ PHANCONG liên quan đến chính Q và các nhân viên N được quản lý trực tiếp bởi Q.

Chính sách 3: Những người dùng có VAITRO là **"Trưởng phòng"** cho biết đó là một nhân viên kiêm nhiệm thêm vai trò trưởng phòng. Một người dùng T có VAITRO là "Trưởng phòng" có quyền được mô tả như sau:

- T có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng trong quan hệ NHANVIEN liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng thì T có quyền xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.

- Có thể thêm, xóa, cập nhật, **xem** trên quan hệ PHANCONG liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng **(CBAC)**.

Chính sách 4: Những người có VAITRO là "**Tài chính**" cho biết đó là một nhân viên phụ trách công việc tài chính tiền lương của công ty. Một người dùng TC có vai trò "Tài chính" có quyền được mô tả như sau:

- TC có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- TC có quyền xem toàn bộ quan hệ NHANVIEN, có thể chỉnh sửa trên thuộc tính LUONG và PHUCAP (thừa hành ban giám đốc).
- TC có quyền xem toàn bộ quan hệ PHANCONG.

Chính sách 5: Những người có VAITRO là "**Nhân sự**" cho biết đó là một nhân viên phụ trách công tác nhân sự trong công ty. Một người dùng NS có vai trò "Nhân sự" có quyền được mô tả như sau:

- NS có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- Được quyền **xem**, thêm, cập nhật trên quan hệ PHONGBAN.
- Thêm, cập nhật dữ liệu trong quan hệ NHANVIEN với giá trị các trường LUONG, PHUCAP là mang giá trị mặc định là NULL, không được xem LUONG, PHUCAP của người khác và không được cập nhật trên các trường LUONG, PHUCAP **(CBAC)**.

Chính sách 6: Những người dùng có VAITRO là "Trưởng đề án" cho biết đó là nhân viên là trưởng các đề án. Một người dùng là "Trưởng đề án" có quyền được mô tả như sau:

- Có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- Được quyền thêm, xóa, cập nhật, **xem** trên quan hệ ĐEAN.

Phát biểu các chính sách bảo mật bạn đã ép thỏa dùng VPD?

➔ ***Chúng em chỉ lọc ra những chính sách thực sự dùng VPD.***

Chính sách 1: Những người có VAITRO là "Nhân viên" cho biết đó là một nhân viên bình thường, không kiêm những công việc nào khác. Những người dùng có VAITRO là "Nhân viên" có các quyền được mô tả như sau:

- Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến nhân viên đó.
- Có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.

Chính sách 2: Những người dùng có VAITRO là **"QL trực tiếp"** nếu họ phụ trách quản lý trực tiếp nhân viên khác. Nhân viên Q là quản lý trực tiếp của nhân viên N, có quyền được mô tả như sau:

- Q có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng dữ liệu trong quan hệ NHANVIEN liên quan đến các nhân viên N mà Q quản lý trực tiếp thì Q được xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.

Chính sách 3: Những người dùng có VAITRO là "Trưởng phòng" cho biết đó là một nhân viên kiêm nhiệm thêm vai trò trưởng phòng. Một người dùng T có VAITRO là "Trưởng phòng" có quyền được mô tả như sau:

- T có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng trong quan hệ NHANVIEN liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng thì T có quyền xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.
- Có thể thêm, xóa, cập nhật, **xem** trên quan hệ PHANCONG liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng.

Chính sách 4: Những người có VAITRO là "**Tài chính**" cho biết đó là một nhân viên phụ trách công việc tài chính tiền lương của công ty. Một người dùng TC có vai trò "Tài chính" có quyền được mô tả như sau:

- TC có quyền như là một nhân viên thông thường (vai trò "Nhân viên").

Chính sách 5: Những người có VAITRO là "**Nhân sự**" cho biết đó là một nhân viên phụ trách công tác nhân sự trong công ty. Một người dùng NS có vai trò "Nhân sự" có quyền được mô tả như sau:

- NS có quyền như là một nhân viên thông thường (vai trò "Nhân viên").

Chính sách 6: Những người dùng có VAITRO là "Trưởng đề án" cho biết đó là nhân viên là trưởng các đề án. Một người dùng là "Trưởng đề án" có quyền được mô tả như sau:

- Có quyền như là một nhân viên thông thường (vai trò "Nhân viên").

Mô tả level, compartment, group và nhãn của 3 người dùng có vai trò khác nhau trong hệ thống?

Level: Giám đốc > Trưởng phòng > Nhân viên.

Compartment: Mua bán, gia công, sản xuất.

Group: Bắc, Trung, Nam

- 01 giám đốc có thể đọc được toàn bộ dữ liệu: Giám đốc:Mua bán, gia công, sản xuất:Bắc, Trung, Nam
- 01 trưởng phòng phụ trách lĩnh vực sản xuất miền Nam: Trưởng phòng:Sản xuất:Nam
- 01 giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc (có thể đọc được toàn bộ dữ liệu theo đúng cấp bậc và không phân biệt lĩnh vực): Giám đốc:Mua bán, gia công, sản xuất:Bắc

Mô tả chính sách mã hóa mà bạn đã cài đặt?

Thiết lập khóa: sử dụng chính sách tính toán ra khóa

- Không cần phải lưu khóa trong cơ sở dữ vì có phải hạn chế truy cập tới bảng lưu khóa, duy trì việc giám sát truy cập vào bảng và rủi ro đối với việc can thiệp và thay đổi khóa bởi DBA.
- Không sử dụng quản lý khóa bởi ứng dụng nhằm tránh mất khóa khi ứng dụng gặp sự cố.
- Mỗi nhân viên sẽ có một khóa khác nhau nên việc tìm ra tất cả các khóa mà không có công thức sẽ không dễ dàng.

Lưu trữ khóa:

- Vì khóa được tính toán ra nên chúng ta chỉ cần lưu trữ công thức tạo ra khóa bằng cách xóa nó khỏi database và lưu vào thiết bị ngoại vi. Thiết bị này được cất giữ bởi người có thẩm quyền.
- Các lưu trữ này sẽ tránh được cách rủi ro nếu bị đánh cắp cơ sở dữ liệu nhưng không có quyền giải mã.

Phân phối khóa:

- Chỉ cấp quyền giải mã cho một số ROLE nhất định.
- Cấp quyền xem dữ liệu thực thông qua các view, không cấp quyền insert, update trên các view đó.
- Các trigger tự động mã hóa dữ liệu trên các thuộc tính mã hóa vừa được insert, update.

Phục hồi khóa khi người dùng quên khóa:

- Vì khóa được tính toán ra nên không xảy ra việc người dùng quên khóa, user admin chỉ cần sử dụng các PROCEDURE để mã hóa và giải mã, tương tự cho người dùng có quyền.
- Công thức khóa được lưu sang thiết bị ngoại vi nên chỉ cần đảm bảo bảo quản tốt thiết bị ngoại vị thì sẽ không sợ mất khóa.

Thay đổi khóa đồng loạt sau một thời gian:

- Trong công thức tạo ra khóa có tham số là seq, nó là một tham số public, khi cần thay đổi khóa, admin chỉ cần thay đổi tham số seq sẽ đồng loạt tạo ra khóa mới cho tất cả nhân viên.

Các bước thay đổi khóa:

- B1: Xóa trigger auto_encrypted_nhanvien (trigger này sẽ tự động mã hóa dữ liệu khi insert hay update).
- B2: Giải mã dữ liệu với khóa hiện tại.
- B3: Mã hóa dữ liệu với khóa mới (thay đổi tham số seq).
- B4: Bật lại trigger auto_encrypted_nhanvien.

Mô tả các chính sách audit mà bạn đã cài đặt?

Câu a:

```
BEGIN
  DBMS_FGA.ADD_POLICY(
    object_schema     => 'QLDA',
    object_name       => 'QLDA_PHANCONG',
    policy_name       => 'THOIGIAN_PHANCONG_AUDIT',
    audit_column      => 'THOIGIAN',
    audit_condition   => NULL,
    statement_types   => 'UPDATE',
    audit_trail => dbms_fga.db + dbms_fga.extended);
END;
```

Câu b:

Bước 1: Tạo hàm check user audit để kiểm tra xem user dùng view hay dùng table (vì có một số user chỉ được quyền select view). Hàm sẽ trả về 3 nếu đó là QLDA(admin), trả về 1 nếu là người

dùng có role ‘NV’, ‘TA’, ‘GD’, ‘TC’. Trả về 2 nếu đó là người dùng có role ‘QL’, ‘TP’, ‘NS’. Và trả về 0 với những người dùng còn lại.

Bước 2: thiết lập audit dùng hàm DBMS_FGA đối với 2 view là V_QLDA_NHANVIEN và V_QLDA_NHANVIEN_NS.

- Đối với view V_QLDA_NHANVIEN: Thiết lập theo dõi và lưu vết đối với những người dùng có role “TA”, “NV”, “GD”, “TC” nhưng đọc LUONG và PHUCAP của người khác. Chính sách như sau:
- Chính sách sẽ ghi viết theo yêu cầu bằng cách thiết lập điều kiện audit_condition kiểm tra mã nhân viên của trường được SELECT khác với mã nhân viên của người dùng và hàm check user trả về 0 hoặc 1.
- Đối với V_QLDA_NHANVIEN_NS: Thiết lập theo dõi và lưu vết đối với người dùng có role “QL”, “TP”, “NS” nhưng đọc LUONG và PHUCAP của người khác. Chính sách như sau:
- Chính sách sẽ ghi vết theo yêu cầu bằng cách thiết lập điều kiện audit_condition kiểm tra mã nhân viên của trường được SELECT khác với mã nhân viên của người dùng và hàm check user trả về 0 hoặc 2.

Câu c:

Bước 1: Kiểm tra xem có phải người dùng thuộc vài trò “Tài chính” không. Ta sẽ tạo hàm để thực hiện việc này. Kết quả trả về của hàm là 1 thì người dùng thuộc vai trò “Tài chính” (không bị audit), trả về 0 thì người dùng không thuộc vai trò “Tài chính” (bị audit).

Bước 2: Viết audit trên view V_QLDA_NHANVIEN với chính sách như sau:

Chính sách này sẽ ghi vết lại những người dùng thực hiện thao tác UPDATE trên 2 cột LUONG, PHUCAP nhưng không thuộc vai trò “Tài chính” bằng cách thiết lập audit_condition là hàm kiểm tra trả về 0 và audit_column là ‘LUONG, PHUCAP’.

Bước 3: Viết audit trên trên view V_QLDA_NHANVIEN_NS với chính sách như sau:

- Chính sách này sẽ ghi vết lại những người dùng thực hiện thao tác UPDATE trên 2 cột LUONG, PHUCAP nhưng không thuộc vai trò “Tài chính” bằng cách thiết lập audit_condition là hàm kiểm tra trả về 0 và audit_column là ‘LUONG, PHUCAP’.