

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN**



BÁO CÁO ĐỒ ÁN THỰC HÀNH

Môn: AN TOÀN VÀ BẢO MẬT CƠ SỞ DỮ LIỆU TRONG HTTT

Giảng viên hướng dẫn:

Dr. Phạm Thị Bạch Huệ

MSc. Tiết Gia Hồng

MSc. Lương Vĩ Minh

TP Hồ Chí Minh, ngày 01 tháng 05 năm 2024

MỤC LỤC

A.	GIỚI THIỆU	4
I.	THÔNG TIN NHÓM.....	4
II.	DANH SÁCH CHỨC NĂNG	5
1.	Phân hệ 1:.....	5
2.	Phân hệ 2:.....	5
B.	PHÂN CÔNG VÀ ĐÁNH GIÁ.....	6
I.	PHÂN HỆ 1 – HỆ THỐNG WINDOWS FORM DÀNH CHO NGƯỜI QUẢN TRỊ.....	6
II.	PHÂN HỆ 2 – THỰC HIỆN CHÍNH SÁCH BẢO MẬT TRÊN HỆ THỐNG	7
III.	ĐÁNH GIÁ THÀNH VIÊN	8
C.	PHÂN HỆ 1	9
I.	DANH SÁCH CHỨC NĂNG:	9
1.	Chức năng 1: Xem danh sách tài khoản người dùng trong hệ thống Oracle DB Server. ...	9
2.	Chức năng 2: Xem thông tin về quyền (privileges) của mỗi user/role trên các đối tượng dữ liệu.....	10
3.	Chức năng 3: Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user:	13
3.1.	Thêm user:	13
3.2.	Cập nhật user:	14
3.3.	Xóa user:	15
4.	Chức năng 4: Cho phép tạo mới, xóa role:	16
4.1.	Thêm role:	16
4.2.	Xóa role:.....	17
5.	Chức năng 5: Cho phép thực hiện việc cấp/thu hồi quyền:	18
5.1.	Quyền SELECT, UPDATE cho phép phân quyền tính đến mức cột.	20
6.	Chức năng 6: Cho phép thu hồi quyền hạn từ user/role.....	23
7.	Chức năng 7: Cấp quyền hạn cho user/role.	24
D.	PHÂN HỆ 2: CÁC CHÍNH SÁCH BẢO MẬT	25
I.	CHÍNH SÁCH DAC:.....	25
1.	Khái niệm:.....	25
2.	Nhận xét:.....	25

II. CHÍNH SÁCH RBAC:	26
1. Khái niệm:	26
2. Cài đặt:	26
III. CHÍNH SÁCH VPD:	29
1. Khái niệm:	29
2. Cài đặt:	29
3. Demo	31
4. Những chính sách VPD đã cài đặt	32
5. Nhận xét:	32
IV. CHÍNH SÁCH OLS:	33
1. Khái niệm:	33
2. Cài đặt:	33
V. CHÍNH SÁCH AUDIT:	35
1. Khái niệm:	35
2. Cài đặt:	35
a) Kích hoạt audit toàn hệ thống	35
b) Standard audit	36
c) Fine-grained audit	36
VI. TÀI LIỆU THAM KHẢO:	39

A. GIỚI THIỆU

I. THÔNG TIN NHÓM

NHÓM 05				
STT	MSSV	Họ và tên	Email	Trưởng nhóm
1	21127234	Nguyễn Lê Anh Chi	nlachi21@clc.fitus.edu.vn	
2	21127235	Nguyễn Xuân Quỳnh Chi	nxqchi21@clc.fitus.edu.vn	
3	21127495	Lê Ngô Song Cát	lnscat21@clc.fitus.edu.vn	
4	21127659	Bùi Ngọc Kiều Nhi	bnknh21@clc.fitus.edu.vn	x

II. DANH SÁCH CHỨC NĂNG

1. Phân hệ 1:

PHÂN HỆ 1		
STT	Công việc	% hoàn thành
1.1	Xem danh sách tài khoản user.	100%
1.2	Xem thông tin quyền của (user/role) trên các đối tượng dữ liệu.	100%
1.3	Tạo mới, xóa, sửa (user/role).	100%
1.4	Cấp quyền (user, role, role2user, with grant, mức cột).	100%
1.5	Thu hồi quyền user/role	100%

2. Phân hệ 2:

PHÂN HỆ 2		
STT	Công việc	% hoàn thành
YC1	Giải pháp cấp quyền truy cập cho 6 chính sách CS#i:	100%
	CS#1 – Sử dụng RBAC	100%
	CS#2 – Sử dụng RBAC	100%
	CS#3 – Sử dụng RBAC	100%
	CS#4 – Sử dụng RBAC	100%
	CS#5 – Sử dụng RBAC	100%
	CS#6 – Sử dụng VPD	75%
YC2	Xem thông tin quyền của (user/role) trên các đối tượng dữ liệu.	100%
	Số lượng chức năng đã hoàn tất (trên 8 yêu cầu): 8	100%
YC3	Ghi nhật ký hệ thống	85%
3.1	Kích hoạt/tắt việc ghi nhật ký	70%
3.2	Standard Audit (table/view/SP/Func)	80%
3.3	Fine-grained Audit (Dangky.diem, Nhansu.phucap).	80%
3.4	Xem dữ liệu nhật ký.	80%
YC4	Sao lưu & Phục hồi dữ liệu	0%
	Báo cáo tìm hiểu giải pháp sao lưu & phục hồi, đánh giá, kết luận.	0%
	Hiện thực trên ứng dụng.	0%

B. PHÂN CÔNG VÀ ĐÁNH GIÁ

I. PHÂN HỆ 1 – HỆ THỐNG WINDOWS FORM DÀNH CHO NGƯỜI QUẢN TRỊ

PHÂN HỆ 1			
STT	Công việc	Phân công	Mức độ hoàn thành
1.1	<ul style="list-style-type: none"> Cài đặt chức năng: <ul style="list-style-type: none"> + Xem danh sách tài khoản user + Tạo mới, xóa, sửa user Viết báo cáo. Quay video demo. 	Bùi Ngọc Kiều Nhi	100%
1.2	<ul style="list-style-type: none"> Cài đặt chức năng: <ul style="list-style-type: none"> + Xem thông tin quyền của (user/role) trên các đối tượng dữ liệu. + Thu hồi quyền user/role. Viết báo cáo. Quay video demo. 	Lê Ngô Song Cát	100%
1.3	<ul style="list-style-type: none"> Cài đặt chức năng: <ul style="list-style-type: none"> + Xem danh sách các role. + Tạo mới, xóa, sửa role. Viết báo cáo. Quay video demo. 	Nguyễn Lê Anh Chi	100%
1.4	<ul style="list-style-type: none"> Cài đặt chức năng: <ul style="list-style-type: none"> + Cấp quyền (user, role, role2user, with grant, mức cột). Viết báo cáo. Quay video demo. 	Nguyễn Xuân Quỳnh Chi	100%

II. PHÂN HỆ 2 – THỰC HIỆN CHÍNH SÁCH BẢO MẬT TRÊN HỆ THỐNG

PHÂN HỆ 2			
STT	Công việc	Phân công	Mức độ hoàn thành
2.1	<ul style="list-style-type: none"> Cài đặt chức năng: <ul style="list-style-type: none"> CS#3, CS#4. Ghi nhật ký hệ thống (Audit). Cài đặt giao diện cho người dùng Trưởng đơn vị. Viết báo cáo chính sách RBAC và Audit. Quay video demo. 	Nguyễn Lê Anh Chi	100%
2.2	<ul style="list-style-type: none"> Viết script khởi tạo và grant quyền cho role và user. Cài đặt chức năng: <ul style="list-style-type: none"> CS#1, CS#2. Sao lưu và phục hồi dữ liệu. Cài đặt giao diện cho người dùng Giáo vụ. Viết báo cáo chính sách RBAC. Quay video demo. 	Nguyễn Xuân Quỳnh Chi	80%
2.3	<ul style="list-style-type: none"> Tạo dữ liệu mẫu. Cài đặt chức năng: <ul style="list-style-type: none"> CS#5. Chính sách OLS. Cài đặt giao diện: <ul style="list-style-type: none"> Login. Người dùng Nhân viên. Người dùng Giảng viên. Viết báo cáo chính sách OLS. Quay video demo. 	Bùi Ngọc Kiều Nhi	100%
2.4	<ul style="list-style-type: none"> Viết script khởi tạo Admin và database. Cài đặt chức năng: <ul style="list-style-type: none"> CS#6. Chính sách Mã hóa dữ liệu. Cài đặt giao diện cho người dùng Sinh viên. Viết báo cáo chính sách VPD, Encrypt. Quay video demo. 	Lê Ngô Song Cát	75%

III. ĐÁNH GIÁ THÀNH VIÊN

NHÓM 05			
STT	MSSV	Họ và tên	% đóng góp
1	21127234	Nguyễn Lê Anh Chi	25%
2	21127235	Nguyễn Xuân Quỳnh Chi	25%
3	21127495	Lê Ngô Song Cát	25%
4	21127659	Bùi Ngọc Kiều Nhi	25%

- Source code:

<https://github.com/BNKieuNhi/DataSecurityInfoSys-IntranetDataHub.git>

- Video demo:

- Phân hệ 1: [Demo ATBM CSDL trong HTTT 2024 - Phân hệ 1 - 05 \(youtube.com\)](#)
- Phân hệ 2: [Demo Phân hệ 2 - 05](#)

C. PHÂN HỆ 1

I. DANH SÁCH CHỨC NĂNG:

1. Chức năng 1: Xem danh sách tài khoản người dùng trong hệ thống Oracle DB Server.

The screenshot shows a web application titled "User List" with a menu bar containing "Users", "Roles", "Check Privileges", "Grant Privileges", "Grant Roles", and "Revoke Roles". Below the menu is a search bar labeled "Từ khóa:" with a "Tìm" button. The main content is a table of database users. The user "AMY" with ID 141 is selected. Below the table are input fields for "ID User:", "Username:", and "Password:". At the bottom are five buttons: "Thêm" (green), "Sửa" (blue), "Xóa" (red), "Ghi" (blue), and "Hủy" (grey).

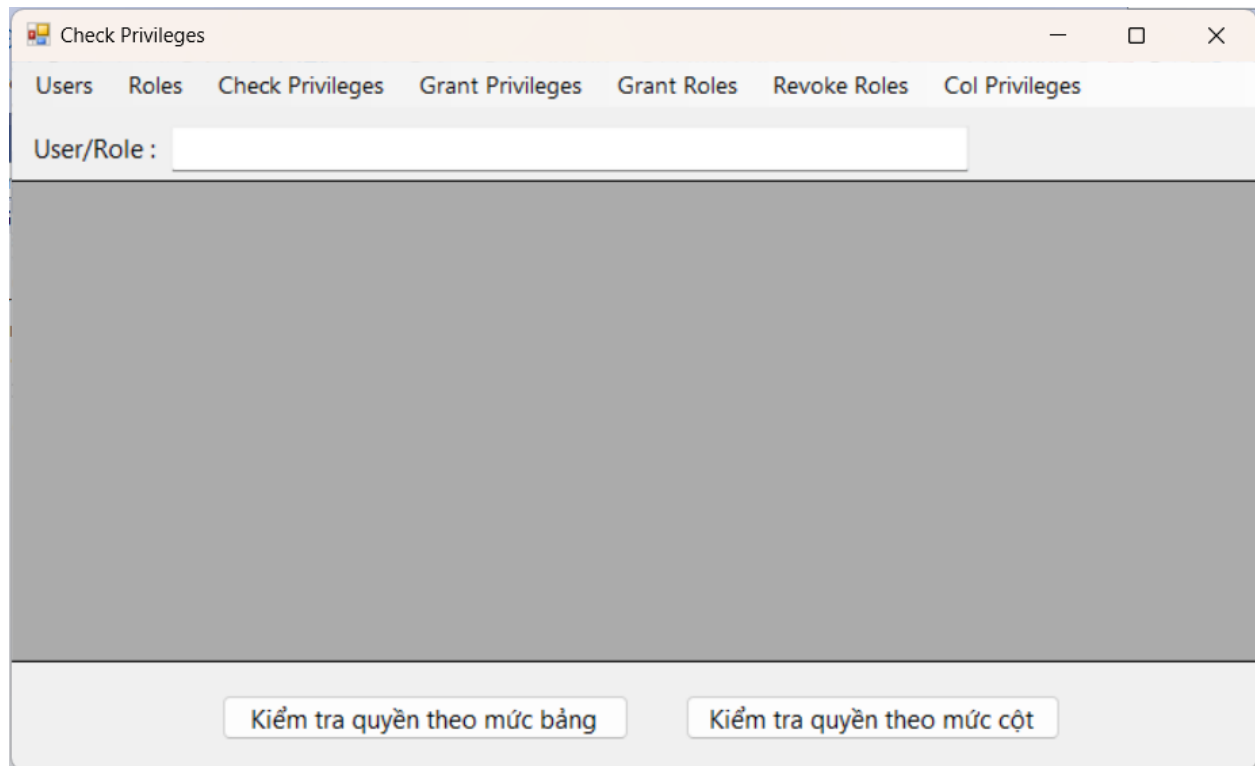
	USERNAME	USER_ID	ACCOUNT_STATU	CREATED
	NAMEMANAGER	147	OPEN	21-Mar-24 12:44 ...
	FRED	139	OPEN	21-Mar-24 12:29 ...
	LYNN	140	OPEN	21-Mar-24 12:29 ...
▶	AMY	141	OPEN	21-Mar-24 12:29 ...
	BETH	142	OPEN	21-Mar-24 12:29 ...
	JOE	138	OPEN	21-Mar-24 12:29 ...
	JONH	137	OPEN	21-Mar-24 12:29 ...
	NHANVIENQUA...	135	OPEN	21-Mar-24 12:17 ...

ID User: 141

Username: AMY Password:

Thêm Sửa Xóa Ghi Hủy

2. Chức năng 2: Xem thông tin về quyền (privileges) của mỗi user/role trên các đối tượng dữ liệu.



Check Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : nhanviencoban

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	NHANVIENCOB...	SYS	DANGKY	SYS	INSERT	NO	NO
	NHANVIENCOB...	SYS	DANGKY	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	DONVI	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	HOCPHAN	SYS	UPDATE	NO	NO
	NHANVIENCOB...	SYS	HOCPHAN	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	NHANSU	SYS	INSERT	NO	NO
	NHANVIENCOB...	SYS	PHANCONG	SYS	DELETE	NO	NO
	NHANVIENCOB...	SYS	PHANCONG	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	SINHVIEN	SYS	SELECT	NO	NO
*							

Kiểm tra quyền theo mức bảng Kiểm tra quyền theo mức cột

Check Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : nhanviencoban

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	NHANVIENCOB...	SYS	V_XEMDIEMTH	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMDIEMTK	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMHK	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMMACT	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMMAHP	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMNAM	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMSOTC	SYS	SELECT	NO	NO
	NHANVIENCOB...	SYS	V_XEMSTLT	SYS	SELECT	NO	NO
*							

Kiểm tra quyền theo mức bảng Kiểm tra quyền theo mức cột

Check Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : NVCB_100

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	NVCB_100	SYS	DONVI	SYS	SELECT	NO	NO
	NVCB_100	SYS	KHMO	SYS	SELECT	NO	NO
	NVCB_100	SYS	SINHVIEN	SYS	SELECT	NO	NO
*							

Kiểm tra quyền theo mức bảng Kiểm tra quyền theo mức cột

Check Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : nvcb_100

	GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE	GRANTABLE	HIERARCHY
▶	NVCB_100	SYS	V_XEMMASV	SYS	SELECT	YES	NO
	NVCB_100	SYS	V_XEMNAM	SYS	SELECT	YES	NO
*							

Kiểm tra quyền theo mức bảng Kiểm tra quyền theo mức cột

3. Chức năng 3: Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user:

3.1. Thêm user:

User List

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles

Từ khóa:

	USERNAME	USER_ID	ACCOUNT_STATU	CREATED
▶	ABC	153	OPEN	25-Mar-24 4:55 PM
	NAMEMANAGER	147	OPEN	21-Mar-24 12:44 ...
	FRED	139	OPEN	21-Mar-24 12:29 ...
	LYNN	140	OPEN	21-Mar-24 12:29 ...
	AMY	141	OPEN	21-Mar-24 12:29 ...
	BETH	142	OPEN	21-Mar-24 12:29 ...
	JOE	138	OPEN	21-Mar-24 12:29 ...
	JONH	137	OPEN	21-Mar-24 12:29 ...
	NHANVIENQUA...	135		2:17 ...

Thông báo
Data Inserted Successfully!

ID User:

Username: Password:

User List

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles

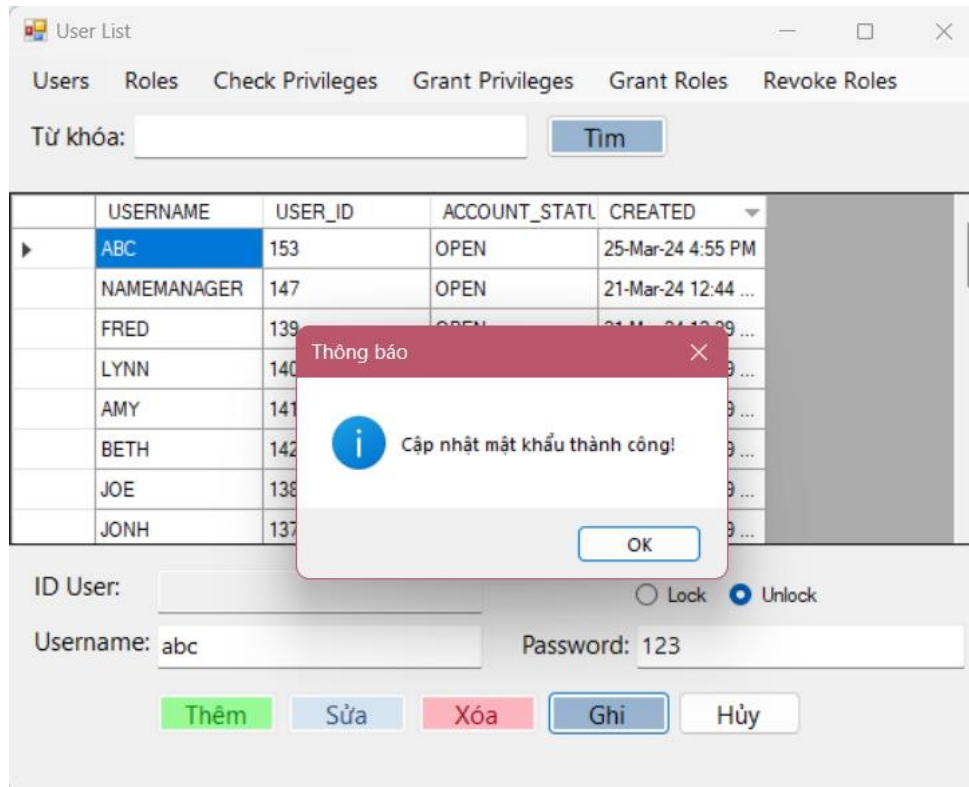
Từ khóa:

	USERNAME	USER_ID	ACCOUNT_STATU	CREATED
▶	ABC	153	OPEN	25-Mar-24 4:55 PM
	NAMEMANAGER	147	OPEN	21-Mar-24 12:44 ...
	FRED	139	OPEN	21-Mar-24 12:29 ...
	LYNN	140	OPEN	21-Mar-24 12:29 ...
	AMY	141	OPEN	21-Mar-24 12:29 ...
	BETH	142	OPEN	21-Mar-24 12:29 ...
	JOE	138	OPEN	21-Mar-24 12:29 ...
	JONH	137	OPEN	21-Mar-24 12:29 ...

ID User:

Username: Password:

3.2. Cập nhật user:



3.3.Xóa user:

User List

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles

Từ khóa:

	USERNAME	USER_ID	ACCOUNT_STATU	CREATED
▶	ABC	153	OPEN	25-Mar-24 4:55 PM
	NAMEMANAGER	147	OPEN	21-Mar-24 12:44 ...
	FRED	139	OPEN	21-Mar-24 12:29 ...
	LYNN	140	OPEN	21-Mar-24 12:29 ...
	AMY	141	OPEN	21-Mar-24 12:29 ...
	BETH	142	OPEN	21-Mar-24 12:29 ...
	JOE	138	OPEN	21-Mar-24 12:29 ...
	JONH	137	OPEN	21-Mar-24 12:29 ...

Thông báo

Xóa người dùng thành công!

OK

ID User:

Username: Password:

☐ CASCADE

User List

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles

Từ khóa:

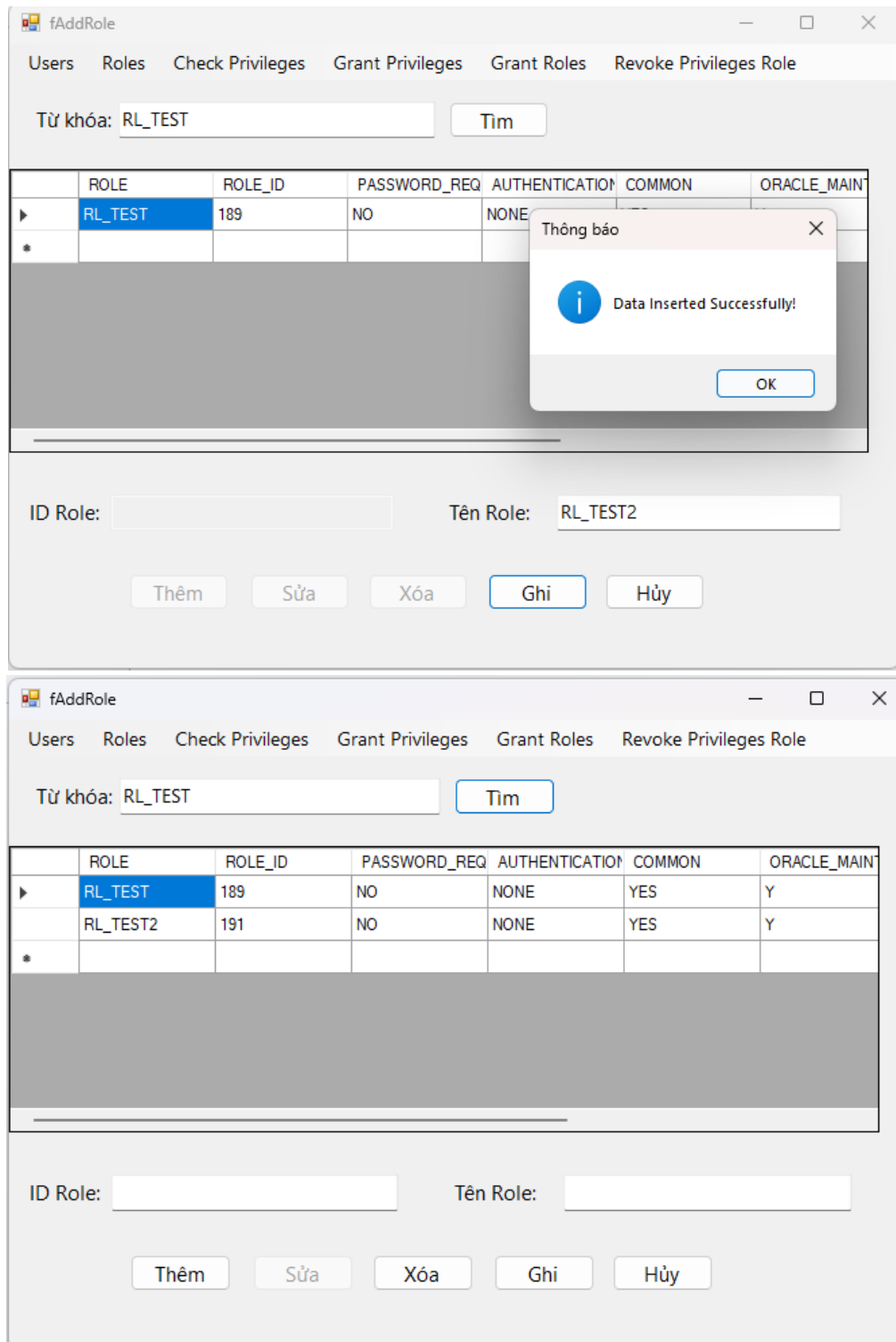
	USERNAME	USER_ID	ACCOUNT_STATU	CREATED
▶	NAMEMANAGER	147	OPEN	21-Mar-24 12:44 ...
	FRED	139	OPEN	21-Mar-24 12:29 ...
	LYNN	140	OPEN	21-Mar-24 12:29 ...
	AMY	141	OPEN	21-Mar-24 12:29 ...
	BETH	142	OPEN	21-Mar-24 12:29 ...
	JOE	138	OPEN	21-Mar-24 12:29 ...
	JONH	137	OPEN	21-Mar-24 12:29 ...
	NHANVIENQUA...	135	OPEN	21-Mar-24 12:17 ...

ID User:

Username: Password:

4. Chức năng 4: Cho phép tạo mới, xóa role:

4.1. Thêm role:



The screenshot shows the fAddRole application interface. The 'Thêm' (Add) button is highlighted in blue. A notification dialog box titled 'Thông báo' (Notification) is displayed, indicating 'Data Inserted Successfully!' with an 'OK' button.

The application interface includes the following elements:

- Navigation Tabs:** Users, Roles, Check Privileges, Grant Privileges, Grant Roles, Revoke Privileges Role.
- Search Bar:** Từ khóa: RL_TEST, with a 'Tìm' (Search) button.
- Table:**

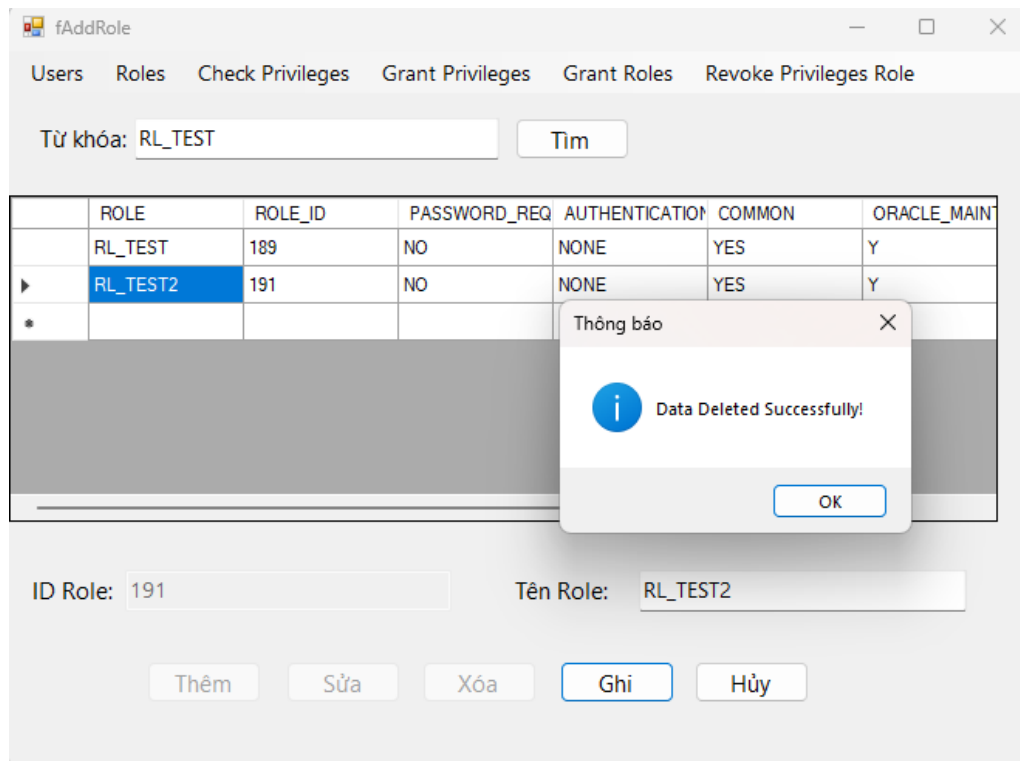
	ROLE	ROLE_ID	PASSWORD_REQ	AUTHENTICATION	COMMON	ORACLE_MAIN
▶	RL_TEST	189	NO	NONE		
*						
- Form Fields:** ID Role: (empty), Tên Role: RL_TEST2.
- Buttons:** Thêm (Add), Sửa (Edit), Xóa (Delete), Ghi (Save), Hủy (Cancel).

The second screenshot shows the application after the 'Thêm' button is clicked. The table now contains two rows:

	ROLE	ROLE_ID	PASSWORD_REQ	AUTHENTICATION	COMMON	ORACLE_MAIN
▶	RL_TEST	189	NO	NONE	YES	Y
	RL_TEST2	191	NO	NONE	YES	Y
*						

The 'Thêm' button is now disabled, and the 'Ghi' (Save) button is highlighted in blue.

4.2.Xóa role:



5. Chức năng 5: Cho phép thực hiện việc cấp/thu hồi quyền:

- Nhập role/ user cần cấp quyền

Grant Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : Nhanviencoban Tim

	Table Name	Select	Select (Grantable)	Insert	Insert (Grantable)	Update	Update (Grantable)
▶	NHANSU	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	SINHVIEN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	DONVI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	HOCPHAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	KHMO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	DANGKY	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	PHANCONG	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
*		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Xác nhận

Grant Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : U_ADMIN Tim

	Table Name	Select	Select (Grantable)	Insert	Insert (Grantable)	Update	Update (Grantable)
▶	NHANSU	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	SINHVIEN	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	DONVI	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	HOCPHAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	KHMO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	DANGKY	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	PHANCONG	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
*		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Xác nhận

Grant Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : akkdjajd Tim

	Table Name	Select	Select (Grantable)	Insert	Insert (Grantable)	Update	Update (Grantable)
*		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Thông báo

Không tìm thấy người dùng/vai trò

OK

Xác nhận

- Cập nhật quyền thành công.

Grant Privileges

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

User/Role : nhanviencoban Tim

	Table Name	Select	Select (Grantable)	Insert	Insert (Grantable)	Update	Update (Grantable)
	NHANSU	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	SINHVIEN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	DONVI	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	HOCPHAN	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	KHMO	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
▶	DANGKY	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	PHANCONG	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
*		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Thông báo

Cập nhật quyền thành công

OK

Xác nhận

5.1. Quyền SELECT, UPDATE cho phép phân quyền tính đến mức cột.

- SELECT (tạo view, grant quyền trên view)

fColumnPriv

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Privileges Role Col Privileges

Nhập Username/ID_Role: NHANVIENCOBAN

	VIEW_NAME	PRIVILEGE	GRANTABLE
	SINHVIEN	SELECT	NO
	DONVI	SELECT	NO
	HOCPHAN	SELECT	NO
	V_XEMPHUCAP	SELECT	NO
▶	V_XEMSOTC	SELECT	NO
*			

Chọn tên bảng và tên cột

Tên bảng: Tên cột:

☐ with GRANT OPTION

- UPDATE

fColumnPriv

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Privileges Role Col Privileges

Nhập Username/ID_Role: NHANVIENCOBAN

	GRANTEE	PRIVILEGE	GRANTABLE
▶	NHANVIENCOB...	UPDATE	NO
	NHANVIENCOB...	UPDATE	NO
	NHANVIENCOB...	UPDATE	NO
	NHANVIENCOB...	UPDATE	NO
*			

Chọn tên bảng và tên cột

Tên bảng: Tên cột:

☐ with GRANT OPTION

fColumnPriv

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Privileges Role Col Privileges

Nhập Username/ID_Role: NHANVIENCOBAN

	GRANTABLE	TABLE_NAME	COLUMN_NAME
▶	IO	SINHVIEN	HOTEN
	IO	SINHVIEN	NGSINH
	IO	HOCPHAN	TENHP
	IO	HOCPHAN	SOSVTD
*			

Chọn tên bảng và tên cột

Tên bảng: Tên cột:

☐ with GRANT OPTION

- SELECT (WITH GRANT OPTION)

fColumnPriv

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Privileges Role Col Privileges

Nhập Username/ID_Role:

	VIEW_NAME	PRIVILEGE	GRANTABLE
▶	V_XEMTENDV	SELECT	YES
*			

Chọn tên bảng và tên cột

Tên bảng: Tên cột:

☐ with GRANT OPTION

- UPDATE (WITH GRANT OPTION)

fColumnPriv

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Privileges Role Col Privileges

Nhập Username/ID_Role:

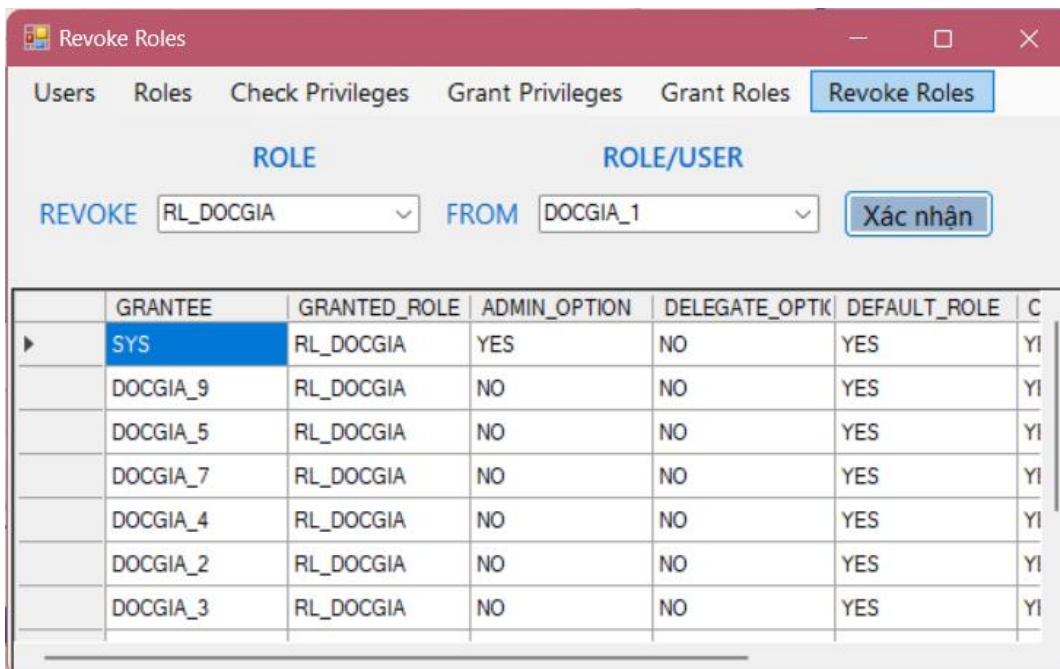
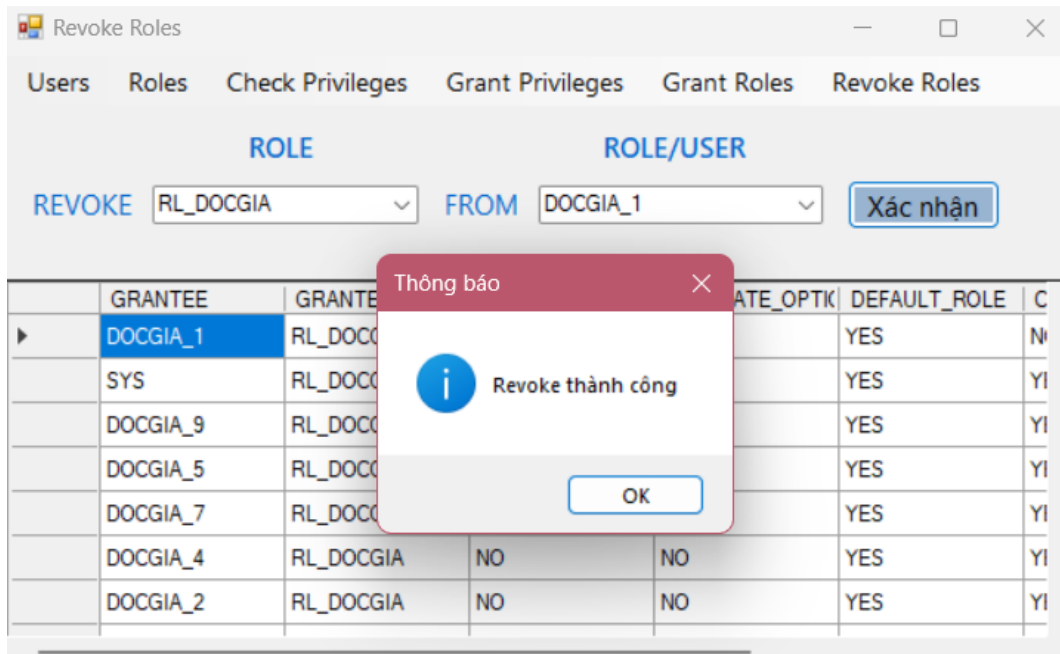
	PRIVILEGE	GRANTABLE	TABLE_NAME
▶	UPDATE	YES	KHMO
*			

Chọn tên bảng và tên cột

Tên bảng: Tên cột:

☐ with GRANT OPTION

6. Chức năng 6: Cho phép thu hồi quyền hạn từ user/role.



7. Chức năng 7: Cấp quyền hạn cho user/role.

Grant Roles

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

ROLE USER

GRANT NHANVIENCOBAN TO JOE **Xác Nhận**

	GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	COMMON
▶	U_ADMIN	NHANVIENCOBAN			YES	NO
	JOHN	NHANVIENCOBAN			YES	NO
	SYS	NHANVIENCOBAN			YES	YES
	NVCB_101	NHANVIENCOBAN			YES	YES
	NVCB_103	NHANVIENCOBAN			YES	YES
	NVCB_105	NHANVIENCOBAN			YES	YES
	NVCB_99	NHANVIENCOBAN	NO	NO	YES	YES
	NVCB_107	NHANVIENCOBAN	NO	NO	YES	YES

Thông báo

i Cập nhật quyền thành công

OK

Grant Roles

Users Roles Check Privileges Grant Privileges Grant Roles Revoke Roles Col Privileges

ROLE USER

GRANT NHANVIENCOBAN TO JOE **Xác Nhận**

	GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DELEGATE_OPTION	DEFAULT_ROLE	COMMON
▶	U_ADMIN	NHANVIENCOBAN	NO	NO	YES	NO
	JOE	NHANVIENCOBAN	NO	NO	YES	NO
	JOHN	NHANVIENCOBAN	NO	NO	YES	NO
	SYS	NHANVIENCOBAN	YES	NO	YES	YES
	NVCB_101	NHANVIENCOBAN	NO	NO	YES	YES
	NVCB_103	NHANVIENCOBAN	NO	NO	YES	YES
	NVCB_105	NHANVIENCOBAN	NO	NO	YES	YES
	NVCB_99	NHANVIENCOBAN	NO	NO	YES	YES

D. PHÂN HỆ 2: CÁC CHÍNH SÁCH BẢO MẬT

I. CHÍNH SÁCH DAC:

1. Khái niệm:

- DAC (Direct Access Control) được sử dụng để phân quyền trên từng đối tượng dữ liệu trực tiếp cho mỗi người dùng khác nhau trong hệ thống bằng câu lệnh GRANT và REVOKE. Các quyền trên đối tượng dữ liệu ở đây bao gồm SELECT, DELETE, INSERT, UPDATE đối với đối tượng Table hoặc View và EXECUTE đối với Stored Procedure hoặc Function.
- DAC được xây dựng và triển khai dựa trên một nguyên lý: Chủ sở hữu sẽ quyết định truy cập với tài nguyên.

2. Nhận xét:

- Cơ chế DAC được đánh giá là đơn giản và dễ cài đặt so với những chính sách khác nhưng sẽ rất khó để quản lý được quyền hạn của từng người dùng trên từng loại tài nguyên nếu số lượng người dùng lớn.
- Ở phân hệ 2 này, mỗi người dùng được cấp username để đăng nhập vào hệ thống với tư cách là người dùng riêng biệt. Tuy rằng có thể sử dụng cơ chế DAC cho việc này nhưng vì số lượng người dùng lớn nên nhóm chủ yếu dùng RBAC để dễ quản lý quyền hạn của từng nhóm người dùng.

II. CHÍNH SÁCH RBAC:

1. Khái niệm:

- RBAC (Role-Based Access Control) là cơ chế phân quyền theo role hay còn gọi là vai trò.
- RBAC hoạt động theo nguyên lý: mO sẽ được phân chia và quản lý theo các nhóm/vai trò. Một chủ thể chỉ có thể truy cập những tài nguyên mà các nhóm/vai trò của chủ thể đó được quyền truy cập.

2. Cài đặt:

- Chia tất cả các users (người dùng) vào 6 Roles:
 - NhanVienCoBan: Quản lý users có vai trò là Nhân viên cơ bản
 - GiangVien: Quản lý users có vai trò là Giảng viên
 - GiaoVu: Quản lý users có vai trò là Giáo vụ
 - TruongDonVi: Quản lý users có vai trò là Trưởng đơn vị
 - TruongKhoa: Quản lý users có vai trò là Trưởng khoa
 - SinhVien: Quản lý users có vai trò là Sinh viên
- Kiểm soát quyền truy cập dữ liệu của users thông qua roles tuân thủ chính sách bảo mật:
 - NhanVienCoBan:
 - + Xem dòng dữ liệu chứa thông tin cá nhân của chính nhân viên đó trên quan hệ NHANSU và chỉ được phép sửa số điện thoại (DT) của chính mình (nếu số điện thoại có thay đổi). → Tạo view V_XEMTTINCANHAN_NHANSU và GRANT quyền SELECT và quyền UPDATE (trên trường DT) trên view cho role này.
 - + Xem tất cả thông tin trên các quan hệ SINHVIEN, DONVI, HOCPHAN, KHMO, nhưng không có quyền ghi trên các quan hệ này. → Grant quyền SELECT trên các quan hệ trên cho role này.
 - GiangVien:
 - + Kế thừa các quyền của role NhanVienCoBan. → GRANT các quyền của role NhanVienCoBan cho role GiangVien; GRANT quyền SELECT và UPDATE trên trường DT trên view V_XEMTTINCANHAN_NHANSU cho role này.
 - + Xem các dòng dữ liệu trên quan hệ PHANCONG có liên quan đến chính giảng viên đó. → Tạo view V_XEMPHANCONG và GRANT quyền SELECT cho role này.
 - + Xem các dòng dữ liệu trên quan hệ DANGKY liên quan đến các lớp học phần mà giảng viên đó được phân công giảng dạy; cập nhật dữ liệu tại các trường liên quan điểm số (DIEMTHI, DIEMTH, DIEMQT, DIEMCK, DIEMTK) trên quan hệ DANGKY của các sinh viên có tham gia lớp học phần mà giảng viên đó được phân công giảng dạy. → Tạo view V_XEMDANGKY và GRANT quyền SELECT và UPDATE (trên các trường DIEMTH, DIEMQT, DIEMCK) trên view cho role này.

- GiaoVu:
 - + Kế thừa các quyền của role NhanVienCoBan. → GRANT các quyền của role NhanVienCoBan cho role GiaoVu; GRANT quyền SELECT và UPDATE trên trường DT trên view V_XEMTTINCANHAN_NHANSU cho role này.
 - + Xem, thêm mới hoặc cập nhật các dòng dữ liệu trên các quan hệ SINHVIEN, DONVI, HOCPHAN, KHMO, theo yêu cầu của trưởng khoa. → GRANT các quyền SELECT, INSERT, UPDATE trên các quan hệ trên cho role này.
 - + Xem tất cả thông tin trên quan hệ PHANCONG và chỉ được phép sửa trên các dòng dữ liệu liên quan các học phần do “Văn phòng khoa” phụ trách. → Tạo view V_XEMPCVPKHOA và GRANT quyền SELECT và UPDATE (chỉ trên các dòng dữ liệu thỏa chính sách bảo mật) trên view cho role này.
 - + Xóa hoặc Thêm mới dữ liệu trên quan hệ ĐANGKY theo yêu cầu của sinh viên trong khoảng thời gian cho phép hiệu chỉnh ĐKHP. → Tạo view V_THEMXOADANGKY và GRANT các quyền SELECT, INSERT, DELETE trên view cho role này.
- TruongDonVi:
 - + Kế thừa các quyền của role GiangVien. → Grant các quyền của role GiangVien cho role này.
 - + Thêm, Xóa hoặc Cập nhật dữ liệu trên quan hệ PHANCONG nhưng chỉ đối với các học phần được phụ trách chuyên môn bởi đơn vị mà mình làm trưởng. → Tạo view V_XEMTTINPCTHEODONVI và GRANT các quyền INSERT, UPDATE, DELETE trên view cho role này.
 - + Xem dữ liệu phân công giảng dạy trên quan hệ PHANCONG của các giảng viên thuộc đơn vị mà mình làm trưởng. → Tạo view V_XEMPCGVCHUNGDONVI và GRANT quyền SELECT trên view cho role này.
- TruongKhoa:
 - + Kế thừa các quyền của role GiangVien. → GRANT các quyền của role GiangVien cho role này.
 - + Thêm, Xóa hoặc Cập nhật dữ liệu trên quan hệ PHANCONG đối với các học phần được quản lý bởi đơn vị “Văn phòng khoa”. → Tạo view V_PHANCONG_VPK và GRANT các quyền INSERT, UPDATE, DELETE trên view cho role này.
 - + Xem, Thêm, Xóa, Cập nhật trên quan hệ NHANSU. → GRANT các quyền SELECT, INSERT, UPDATE, DELELTE trên quan hệ NHANSU cho role này.
 - + Xem dữ liệu trên toàn bộ lược đồ CSDL. → GRANT SELECT ANY TABLE cho role này.

- SinhVien (Sử dụng VPD):
 - + Xem dòng dữ liệu chứa thông tin cá nhân của chính mình và chỉ được phép chỉnh sửa thông tin địa chỉ (DCHI) và số điện thoại (ĐT) của chính sinh viên đó.
 - + Trên quan hệ SINHVIEN, sinh viên chỉ được xem thông tin của chính mình, được
 - + Chỉnh sửa thông tin địa chỉ (DCHI) và số điện thoại liên lạc (DT) của chính sinh viên.
 - + Xem danh sách các học phần (HOCPHAN) và kế hoạch mở môn (KHMO) của chương trình đào tạo mà sinh viên đó đang theo học.
 - + Thêm, Xóa các dòng dữ liệu đăng ký học phần (DANGKY) 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).
 - + Không được chỉnh sửa các trường liên quan đến DIEMSO trên quan hệ DANGKY.

III. CHÍNH SÁCH VPD:

1. Khái niệm:

- Các chính sách VPD (Virtual Private Database) dùng để giới hạn người dùng chỉ có thể truy cập được những dòng cụ thể theo điều kiện của hàm chính sách.

2. Cài đặt:

- Bước 1 : Tạo hàm chính sách tương ứng với yêu cầu.

Ví dụ : Xem danh sách tất cả học phần (HOCPHAN) của chương trình đào tạo mà sinh viên đang theo học thì hàm chính sách tương ứng sẽ là :

```
create or replace FUNCTION SV_POLICY3
(P_SCHEMA VARCHAR2, P_OBJ VARCHAR2)
RETURN VARCHAR2
AS
    MA VARCHAR2(5);
    STRSQL VARCHAR2(2000);
    ROLE_NAME VARCHAR2(100);
    CURSOR CUR IS (SELECT MAHP
                    FROM U_ADMIN.KHMO KH , U_ADMIN.SINHVIEN SV
                    WHERE SV.USERNAME = SYS_CONTEXT('USERENV','SESSION_USER')
                    AND KH.MACT = SV.MACT);
BEGIN
    SELECT MAX(granted_role)
    INTO ROLE_NAME
    FROM dba_role_privs
    WHERE grantee = SYS_CONTEXT('USERENV','SESSION_USER');

    -- Kiểm tra nếu vai trò là SINHVIEN
    IF ROLE_NAME = 'SINHVIEN' THEN
        OPEN CUR;
        LOOP
            FETCH CUR INTO MA;
            EXIT WHEN CUR%NOTFOUND;

            IF (STRSQL IS NOT NULL) THEN
                STRSQL := STRSQL || ',';
            END IF;
            STRSQL := STRSQL || MA;
        END LOOP;
        RETURN 'MAHP IN (' || STRSQL || ')';
    ELSE
        RETURN '1 = 1';
    END IF;
END;
```

- + Khi này hàm chính sách sẽ kiểm tra xem người dùng có phải là SINHVIEN không và lấy ra những mã học phần thuộc chương trình mà user hiện tại đang theo học.
- + Hàm chính sách trả về như sau 'MAHP IN (1,2,3)'.
- Bước 2: Tạo chính sách mới

```
BEGIN
  DBMS_RLS.ADD_POLICY (
    OBJECT_SCHEMA => 'U_ADMIN',
    OBJECT_NAME => 'HOCPHAN',
    POLICY_NAME => 'SV_PC3',
    POLICY_FUNCTION => 'SV_POLICY3',
    FUNCTION_SCHEMA => 'U_ADMIN',
    STATEMENT_TYPES => 'SELECT'
  );
END;
```

- + OBJECT_SCHEMA : Schema chứa đối tượng cần áp dụng chính sách.
- + OBJECT_NAME : Tên của đối tượng cần áp dụng chính sách. Những đối tượng này có thể là một bảng, view.
- + POLICY_NAME : Tên chính sách.
- + POLICY_FUNCTION : Tên hàm chính sách áp dụng lên bảng, view.
- + STATEMENT_TYPES : Loại câu lệnh mà chính sách áp dụng, bao gồm SELECT, INSERT, UPDATE, DELETE.
- + Ngoài ra, hàm tạo chính sách còn có những biến như : SEC_RELEVANT_COLS (những cột thuộc đối tượng cần áp dụng chính sách), UPDATE_CHECK (đối với trường hợp chính sách áp dụng lên câu lệnh INSERT, UPDATE thì chính sách sẽ thực hiện kiểm tra cập nhật hay không).

3. Demo

- Sinh viên chỉ có thể được xem thông tin của chính mình.

```
CREATE OR REPLACE FUNCTION SV_POLICY1
(P_SCHEMA VARCHAR2, P_OBJ VARCHAR2)
RETURN VARCHAR2
AS
    ROLE_NAME VARCHAR2(100);
BEGIN
    -- Lấy tên vai trò của người dùng
    SELECT MAX(granted_role)
    INTO ROLE_NAME
    FROM dba_role_privs
    WHERE grantee = SYS_CONTEXT('USERENV', 'SESSION_USER');

    -- Kiểm tra nếu vai trò là SINHVIEN
    IF ROLE_NAME = 'SINHVIEN' THEN
        RETURN 'USERNAME = SYS_CONTEXT(''USERENV'', ''SESSION_USER'')';
    ELSE
        RETURN '1 = 1';
    END IF;
END;

/
BEGIN
    DBMS_RLS.ADD_POLICY (
    OBJECT_SCHEMA => 'U_ADMIN',
    OBJECT_NAME => 'SINHVIEN',
    POLICY_NAME => 'SV_PC1',
    POLICY_FUNCTION => 'SV_POLICY1',
    FUNCTION_SCHEMA => 'U_ADMIN',
    STATEMENT_TYPES => 'SELECT, UPDATE',
    SEC_RELEVANT_COLS => 'DCHI, DT',
    UPDATE_CHECK => TRUE
    );
END;
```


- + Trước khi tạo hàm chính sách: Sinh viên xem được toàn bộ danh sách sinh viên.

	MASV	HOTEN	PHAI	NGSINH	DCHI	DT	MACT	MANGANH	SOTC
1	1	SONG CA...	Nam	85-09-08	1 DUONG BA TRAC	123456789	CTTT	CNTT	
2	2	Vu ??c	Nam	78-06-17	So 361 DUONG BA TRAC	938922767	CQ	CNTT	
3	3	Vu Phuc	Nam	88-03-06	So 890	628351244	CQ	CNTT	
4	4	Tran Thi	Nam	85-06-26	So 479 TRAN HUNG DAO	713322999	CTTT	CNTT	
5	5	Vo Sang	N?	90-01-30	So 561 VO VAN TAN	510427378	CQ	CNTT	
6	6	Tran Tam	Nam	91-09-07	So 801 LY THUONG ...	406893633	CLC	CNTT	
7	7	Hoang Sang	N?	84-04-19	So 35 TRAN PHU	459944296	CQ	CNTT	
8	8	Tran Ng...	N?	83-05-16	So 158 TRAN PHU	674485630	CTTT	CNTT	
9	9	Hoang T...	Nam	88-03-18	So 844 VO VAN TAN	419864336	CLC	CNTT	
10	10	Le Dat	N?	88-03-03	So 660 PHAM VAN DONG	761943043	CTTT	CNTT	
11	11	Vo Bao	Nam	90-09-11	So 222 HOA MAI	723635629	CTTT	CNTT	1
12	12	Vo Nam	N?	87-06-10	So 47 DUONG BA TRAC	630264273	CTTT	CNTT	

- + Sau khi tạo hàm chính sách : Sinh viên chỉ xem được thông tin của chính mình.

	MASV	HOTEN	PHAI	NGSINH	DCHI	DT	MACT	M...	SOTCTL
1	1	SONG CA...	Nam	85-09-08	1 DUONG BA TRAC	123456789	CTTT	CNTT	8

4. Những chính sách VPD đã cài đặt

- Sinh viên chỉ được cập nhật thông tin cá nhân về số điện thoại và địa chỉ.
- Sinh viên được xem tất cả các danh sách học phần thuộc chương trình mình đang theo học.
- Sinh viên chỉ không được chỉnh sửa những trường liên quan đến điểm số.
- Sinh viên được xem những thông tin học phần đã đăng kí.
- Sinh viên chỉ có thể được xem thông tin của chính mình

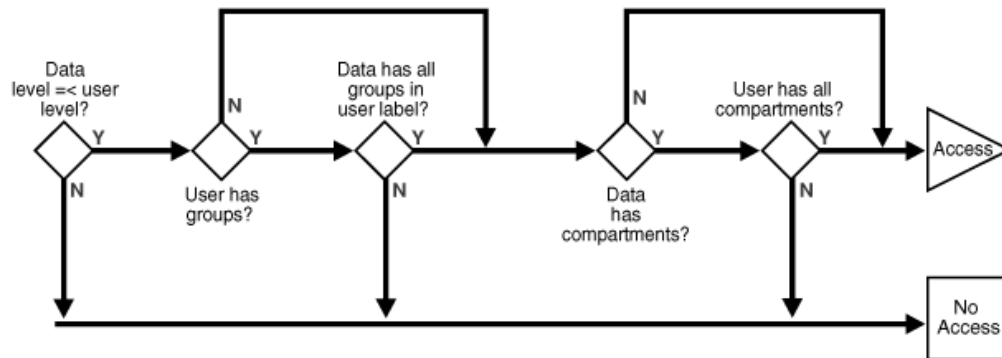
5. Nhận xét:

- Các chính sách VPD giúp cho người quản trị cơ sở dữ liệu có thể thiết lập các giới hạn truy cập cho người dùng theo dòng dữ liệu.
- Dễ dàng điều chỉnh chính sách truy cập.
- Người dùng chỉ được xem phần dữ liệu tương ứng.

IV. CHÍNH SÁCH OLS:

1. Khái niệm:

- OLS (Oracle Label Security) là một phương thức điều khiển quyền truy cập dữ liệu trong một bảng bằng cách gắn nhãn lên từng dòng dữ liệu và từng người dùng. Khi người dùng truy cập vào bảng dữ liệu có chính sách OLS, họ chỉ có thể xem các dòng dữ liệu mà nhãn của họ phù hợp. Các nhãn được phân chia thành ba mức độ: Level, Compartment và Group.
- Thuật toán truy cập:



2. Cài đặt:

- Chính sách OLS ở đồ án này được cài đặt như sau:
 - o Level:
 - + TK: Trưởng khoa (level_num = 600).
 - + TDV: Trưởng đơn vị (level_num = 500).
 - + GV: Giảng viên (level_num = 400).
 - + GVU: Giáo vụ (level_num = 300).
 - + NV: Nhân viên (level_num = 200).
 - + SV: Sinh viên (level_num = 100).
 - o Compartment:
 - + HTTP: Hệ thống thông tin.
 - + CNPM: Công nghệ phần mềm.
 - + KHMT: Khoa học máy tính.
 - + CNTT: Công nghệ thông tin.
 - + TGMT: Thị giác máy tính.
 - + MMT: Mạng máy tính.
 - o Group:
 - + CS1: Cơ sở 1.
 - + CS2: Cơ sở 2.
- Lý do cài đặt:
 - o Level: Phản ánh cấp bậc và quyền hạn của người dùng trong hệ thống.

- Compartment: Phân chia dữ liệu theo ngành học, giúp quản lý và truy cập dữ liệu một cách có hệ thống.
- Group: Phân loại dữ liệu theo cơ sở, giúp tổ chức dữ liệu một cách logic và dễ dàng truy cập.
- Một số nhân được cài đặt trên hệ thống:
 - a) Nhân cho người dùng là Trưởng khoa có thể đọc được toàn bộ thông báo.
→ **u1**: TK:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2
 - b) Nhân cho các Trưởng bộ môn phụ trách Cơ sở 2 có thể đọc được toàn bộ thông báo. dành cho trưởng bộ môn không phân biệt vị trí địa lý.
→ **u2**: TDV:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2
 - c) Nhân cho 01 Giáo vụ có thể đọc toàn bộ thông báo dành cho giáo vụ.
→ **u3**: GVU:HTTT,CNPM,KHMT,CNTT,TGMT,MMT:CS1,CS2
 - d) Nhân của dòng thông báo t1 để t1 được phát tán (đọc) bởi tất cả Trưởng đơn vị.
→ **t1**: TDV/ GV/ GVU/ NV/ SV
 - e) Nhân của dòng thông báo t2 để phát tán t2 đến Sinh viên thuộc ngành HTTT học ở Cơ sở 1.
→ **t2**: SV/ SV::CS1/ SV::CS1,CS2/ SV:HTTT:CS1/ SV:HTTT:CS1,CS2
 - f) Nhân của dòng thông báo t3 để phát tán t3 đến Trưởng bộ môn KHMT ở Cơ sở 1.
→ **t3**: TBM/ TBM::CS1/ TBM::CS1,CS2/ TBM:KHMT:CS1/ TBM:KHMT:CS1,CS2/ GV/ GVU/...
 - g) Nhân của dòng thông báo t4 để phát tán t4 đến Trưởng bộ môn KHMT ở Cơ sở 1 và Cơ sở 2.
→ **t4**: TBM/ TBM::CS1,CS2/ TBM:KHMT:CS1,CS2/ GV/...
 - h) 3 chính sách phát tán dòng dữ liệu khác trên mô hình OLS đã cài đặt:
 - h.1)** Nhân của dòng thông báo t5 để phát tán t5 cho Giảng viên thuộc bộ môn CNPM ở Cơ sở 1:
→ **t5**: GV/ GV::CS1/ GV::CS1,CS2/ GV:CNPM/ GV:CNPM:CS1/ GV:CNPM:CS1,CS2/ GV/ NV/ SV/...
 - h.2)** Hãy cho biết nhân của dòng thông báo t6 để phát tán t6 đến toàn bộ người dùng:
→ **t6**: SV
 - h.3)** Hãy cho biết nhân của dòng thông báo t7 để phát tán t7 đến Nhân viên ở Cơ sở 2:
→ **t7**: NV/ NV::CS2/ NV::CS1,CS2/ SV/ SV::CS1/ SV::CS1,CS2

V. CHÍNH SÁCH AUDIT:

1. Khái niệm:

- Audit là quá trình ghi lại và theo dõi các hoạt động được thực hiện trên dữ liệu hoặc các đối tượng khác trong hệ thống. Thông qua việc audit, người quản trị có thể xác định được ai đã thực hiện các thao tác như truy cập, cập nhật, xóa dữ liệu, hoặc thậm chí là cố gắng truy cập vào các tài nguyên mà họ không được phép.
- Cơ chế này giúp tăng cường bảo mật, tuân thủ quy định và phát hiện sớm các hoạt động không mong muốn trong hệ thống cơ sở dữ liệu.
- Việc ghi nhật ký hệ thống sẽ giúp tăng cường tính bảo mật khi theo dõi các hành vi của người dùng trên cơ sở dữ liệu nhằm phát hiện ra những truy cập trái phép và ghi lại những thay đổi để giúp người quản trị kiểm soát những đối tượng có dấu hiệu thực hiện hành vi gây hại đến dữ liệu.

2. Cài đặt:

a) Kích hoạt audit toàn hệ thống

- Trước khi kích hoạt audit, cần đảm bảo rằng người thực hiện audit phải có đủ quyền hạn để thực hiện các thay đổi liên quan đến audit. Thông thường, người đó cần có quyền DBA hoặc các quyền tương đương.
- Chức năng Audit mặc định không được kích hoạt, nếu muốn sử dụng người dùng có thể kích hoạt bằng câu lệnh sau:

```
ALTER SYSTEM SET AUDIT_TRAIL=DB, EXTENDED SCOPE=SPFILE;
```

- Giải thích về các giá trị của tham số AUDIT_TRAIL: audit_trail = {none | os | db | DB, EXTENDED | xml | xml, extended} trong đó:
 - none : Tắt chế độ audit.
 - os: Bật chế độ audit và các bản ghi của audit sẽ được lưu trong file OS.
 - db: Bật chế độ audit và các bản ghi của audit sẽ được lưu trong database audit trail (SYS.AUD\$).
 - xml: Bật chế độ audit và các bản ghi của audit sẽ được lưu trong file OS có định dạng .xml.
- Ở đây, nhóm dùng chế độ db để dễ truy xuất và hiển thị các bản ghi do audit ghi lại được.
- Sau khi bật chế độ Audit, ta cần reset lại Oracle để thực hiện các thay đổi bằng 2 câu lệnh dưới đây:

```
SHUTDOWN IMMEDIATE;  
STARTUP;
```
- Với chế độ ghi nhật ký thông thường (standard audit), sau khi bật audit ta đã có thể bắt đầu ghi nhật ký bằng việc thiết lập ghi nhật ký những hành vi nào trên những đối tượng dữ liệu nào hoặc được thực hiện bởi những người dùng nào. Một vài thiết lập giám sát câu lệnh và quyền:
 - BY ACCESS: Ghi một record cho mỗi câu lệnh và hoạt động được audit.

- **WHENEVER SUCCESSFUL:** Thực hiện ghi nhật ký đối với những câu lệnh được thực thi thành công. Ví dụ: `AUDIT SELECT ON EMP BY ACCESS WHENEVER SUCCESSFUL` -> Câu lệnh này yêu cầu thực hiện ghi nhật ký đối với những lần thực thi thành công câu lệnh `SELECT` trên bảng `EMP`.
- **WHENEVER NOT SUCCESSFUL:** Thực hiện ghi nhật ký đối với những câu lệnh được thực thi không thành công. Ví dụ: `AUDIT SELECT ON EMP BY ACCESS WHENEVER NOT SUCCESSFUL` -> Câu lệnh này yêu cầu thực hiện ghi nhật ký đối với những lần thực thi **KHÔNG** thành công câu lệnh `SELECT` trên bảng `EMP`.
- Có thể thực hiện audit với các thao tác trên bảng bao gồm tạo, xóa hoặc chỉnh sửa cấu trúc trên bảng bất kì thuộc cơ sở dữ liệu. Ví dụ: `AUDIT DROP ANY TABLE`
-> Thực hiện ghi nhật ký mỗi khi có bảng nào bị xóa.
 - Trên đối tượng dữ liệu: `AUDIT ALL ON [table_name];`
 - Bởi người dùng: `AUDIT SELECT TABLE BY [username];`

b) Standard audit

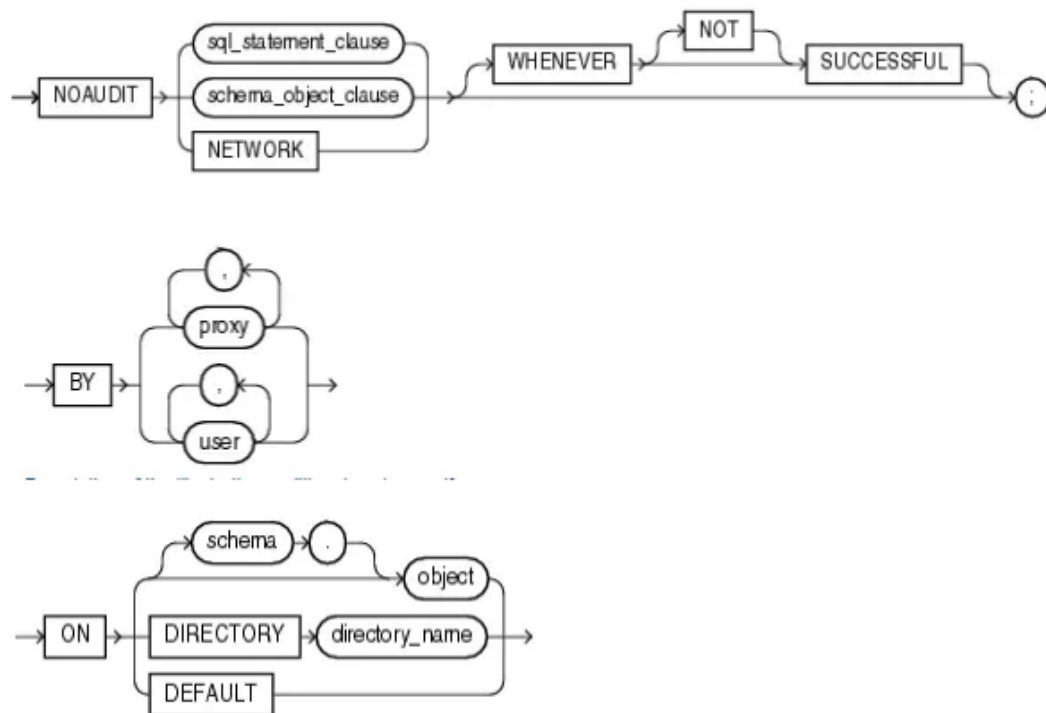
- Chính sách 1: Thực hiện ghi nhật ký tất cả các thao tác của bất kì người dùng nào trên tất cả các bảng thuộc cơ sở dữ liệu.
- Chính sách 2: Thực hiện ghi nhật ký các thao tác được thực thi thành công.
- Chính sách 3: Thực hiện ghi nhật ký các thao tác thực thi không thành công.

c) Fine-grained audit

- Cài đặt các chính sách, sau khi tạo xong các chính sách sẽ tự động được kích hoạt.
- Chính sách 1: Trong cơ sở dữ liệu có 6 nhóm người dùng và yêu cầu ghi nhật ký đối với những hành vi chỉnh sửa điểm số mà người thực hiện không phải vai trò `GIANGVIEN` trong cơ sở dữ liệu.
- Chính sách 2: Thông tin về `PHUCAP` của từng người là thông tin nên được giữ bí mật và mỗi người dùng chỉ nên biết của chính mình để tránh những sự cạnh tranh nơi công sở nên `FGA` được cài đặt lên cột `PHUCAP` thuộc bảng `NHANSU` để theo dõi nếu có những truy cập bất thường.

d) Tắt Audit

- Đối với Standard Audit: Ta có thể sử dụng câu lệnh `NOAUDIT` để dừng việc ghi nhật ký và cấu trúc câu lệnh tương đối giống với khi dùng `AUDIT`.



- Đối với FGA: Sau khi cài đặt, nếu người thực hiện audit không còn muốn dùng những chính sách này có thể DROP_POLICY để xóa hẳn chính sách đó, hoặc sử dụng DISABLE_POLICY để tạm ngừng việc ghi nhật ký theo chính sách này. Người dùng sau đó nếu muốn sử dụng lại có thể ENABLE_POLICY để kích hoạt lại việc ghi nhật ký với những chính sách này với điều kiện chính sách đó vẫn còn tồn tại.

```
--Kích hoạt ghi nhật ký
BEGIN
  DBMS_FGA.ENABLE_POLICY(
    object_schema => 'U_ADMIN',
    object_name   => 'NHANSU',
    policy_name   => 'XEMPHUCAP_CUANGKHAC'
  );
END;

--Tắt audit
BEGIN
  DBMS_FGA.DISABLE_POLICY(
    object_schema => 'U_ADMIN',
    object_name   => 'NHANSU',
    policy_name   => 'XEMPHUCAP_CUANGKHAC'
  );
END;
```


VI. TÀI LIỆU THAM KHẢO:

- [1] [Kiểm soát truy cập an toàn \(viblo.asia\)](https://viblo.asia)
- [2] [Introduction to Auditing \(oracle.com\)](https://oracle.com)
- [3] [Configuring Role-Based Access Control \(RBAC\) \(oracle.com\)](https://oracle.com)
- [4] [MATERIALS - Google Drive](#) (slide lý thuyết)
- [5] Tài liệu hướng dẫn LAB
- [6] HD DAC_RBAC_VPD_OLS.pdf (moodle lớp)