**Bài thực hành số 14**

**ÔN TẬP**

1. Viết một thủ tục (procedure) cho phép in ra thông tin các tài nguyên (resource limits) mà người dùng được gán thông qua profile. Trước khi xuất ra màn hình, thủ tục phải kiểm tra xem các tài nguyên được liệt kê bên dưới có đang ở trạng thái UNLIMITED hay không. Nếu tài nguyên đó đang là UNLIMITED thì thay đổi nó thành giá trị được nêu bên dưới rồi mới xuất ra màn hình:
* thời hạn sử dụng password là 90 ngày
* gia hạn password là 15 ngày
* số lần nhập sai password là 3

(Thủ tục có 1 thông số truyền vào là username)

1. Cho bảng có cấu trúc như sau thuộc schema của sec\_manager:

*employee(empno, ename, email, salary, deptno)*

Chi tiết:

* empno (number) : mã số nhân viên
* ename (varchar2) : tên nhân viên
* email (varchar2) : email của nhân viên
* salary (number): lương nhân viên
* deptno (number) : mã số phòng ban của nhân viên

Hãy dùng kỹ thuật ***Row-level Security*** bảo vệ cho bảng **employee** theo chính sách được mô tả dưới đây:

* Nhân viên thuộc phòng ban này không được phép xem hay chỉnh sửa bất kỳ thông tin nào của những nhân viên thuộc phòng ban khác.
* Các nhân viên được phép xem (select) các thông tin của những người trong cùng phòng ban.
* Nhân viên không được phép insert/delete trên bảng.
* Nhân viên chỉ có thể update thông tin email của bản thân mình. Những thông tin cá nhân còn lại không được phép chỉnh sửa.

Lưu ý:

* Tên của nhân viên (ename) chính là username mà nhân viên đó dùng để log in vào hệ thống. (Sinh viên có thể dùng hàm USER trả về username của người dùng hiện tại)
* Sinh viên phải viết cả policy function và các lệnh gán policy function cho table **employee**.
* Sinh viên có thể viết 1 hay nhiều policy function để hiện thực chính sách trên.
* Các *policy function* tạo ra thuộc schema của user sec\_manager và user sec\_manager là người gán các policy function cho *employee*.
1. Cho bảng có cấu trúc như sau thuộc schema của sec\_manager:

*employee(empno, ename, email , salary, deptno,manager)*

Chi tiết:

* empno (number) : mã số nhân viên
* ename (varchar2) : tên nhân viên
* email (varchar2) : email của nhân viên
* salary (number): lương nhân viên
* deptno (number) : mã số phòng ban của nhân viên
* manager(number): mã số người quản lý của phòng ban mà nhân viên thuộc về

Hãy dùng kỹ thuật ***Row-level Security*** bảo vệ cho bảng **employee** theo chính sách được mô tả dưới đây:

* Nhân viên hay quản lý thuộc phòng ban này không được phép xem hay chỉnh sửa bất kỳ thông tin nào của những nhân viên thuộc phòng ban khác.
* Nhân viên thuộc phòng ban nào chỉ được xem (*select*) thông tin của các nhân viên thuộc cùng phòng ban với mình ngoại trừ lương (*salary*). Mỗi nhân viên chỉ có thể xem lương của bản thân họ.
* Nhân viên không có quyền chỉnh sửa (*insert, update, delete*) bất cứ thông tin gì, kể cả thông tin của chính nhân viên đó.
* Chỉ có người quản lý từng phòng ban được phép *select, insert, update, delete* tất cả các thông tin của các nhân viên thuộc phòng ban mình quản lý.

Lưu ý:

* Tên của nhân viên (ename) chính là username mà nhân viên đó dùng để log in vào hệ thống. (Sinh viên có thể dùng hàm USER trả về username của người dùng hiện tại)
* Sinh viên phải viết cả policy function và các lệnh gán policy function cho table **employee**.
* Sinh viên có thể viết 1 hay nhiều policy function để hiện thực chính sách trên.
* Các *policy function* tạo ra thuộc schema của user sec\_manager và user sec\_manager là người gán các policy function cho *employee*.
1. Viết một thủ tục (procedure) cho phép tìm trong số các quyền hệ thống và quyền đối tượng của một user, nếu có quyền nào có tùy chọn WITH ADMIN OPTION/WITH GRANT OPTION thì in ra thông tin về quyền đó, thu hồi lại quyền đó và cấp lại quyền đó cho user nhưng không có tùy chọn WITH ADMIN OPTION/WITH GRANT OPTION. Thủ tục có interface như sau:

***Change\_privilege\_option(p\_username VARCHAR2)***

Thông tin in ra của quyền hệ thống là tên của quyền. Thông tin in ra của quyền đối tượng bao gồm tên của quyền, đối tượng của quyền và schema sở hữu đối tượng đó.

1. Viết hàm kiểm tra xem username và password nhập vào có trùng khớp với username và password của Oracle hay không.