**AUDIT**

1. **Audit là gì?**  
   Auditing là hoạt động theo dõi và lưu vết lại các hoạt động thao tác của người dùng vào

dữ liệu. Trong Oracle, người quản trị có thể cấu hình để thực hiện audit lại các hoạt

động trong của cả người dùng trong cơ sở dữ liệu lẫn những người dùng không có trong

cơ sở dữ liệu, giới hạn audit với một số lệnh cụ thể hay audit một số role cụ thể trong

dữ liệu.

1. **Mục đích sử dụng Audit.**  
   - Theo dõi sự xuất hiện của câu lệnh SQL trong các phiên người dùng tiếp theo. Bạn có thể theo dõi sự xuất hiện của một câu lệnh SQL cụ thể hoặc của tất cả các câu lệnh SQL được ủy quyền bởi một đặc quyền hệ thống cụ thể. Hoạt động kiểm tra trên các câu lệnh SQL chỉ áp dụng cho các phiên tiếp theo, không áp dụng cho các phiên hiện tại.  
   - Theo dõi hoạt động trên một đối tượng lược đồ cụ thể. Hoạt động kiểm tra trên các đối tượng lược đồ áp dụng cho các phiên hiện tại cũng như các phiên tiếp theo.
2. **Kích hoạt Audit**  
   - Sử dụng câu lệnh <show parameter audit\_trail;> để kiểm tra AUDIT\_TRAIL đã bật hay chưa?  
   - AUDIT\_TRAIL mặc định là NONE nên ta phải thiết lập lại value của AUDIT\_TRAIL.  
   - Câu lệnh <alter system set audit\_trail=db, extended scope=spfile;>  
   - Restart lại database bằng câu lệnh < shutdown immediate; startup;>
3. **Fine Grained Auditing.**  
   **a. Cấp quyền execute DBMS\_FGA và select FGA\_LOG$ cho admin.**  
   - GRANT EXECUTE ON DBMS\_FGA TO ad;  
   - GRANT SELECT ON SYS.FGA\_LOG$ TO ad;  
     
   **b. Thực hiện audit các hành vi.**  
   \* Chính sách 1: Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.  
   - FGA trên bảng PHANCONG cho hành động UPDATE trên trường THOIGIAN.  
     
   \* Chính sách 2: Những người đã đọc trên trường LUONG và PHUCAP của người khác.  
   - FGA trên bảng NHANVIEN cho hành động SELECT trên trường LUONG và PHUCAP với điều kiện VAITRO = ’TaiChinh’ hoặc VAITRO = ’GiamDoc’.  
     
   \* Chính sách 3: Một người không thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.  
   - FGA trên bảng NHANVIEN cho hành động UPDATE trên trường LUONG và PHUCAP với điều kiện VAITRO != ’TaiChinh’.

**c. Kiểm tra audit.**  
- SELECT DBUID, LSQLTEXT, NTIMESTAMP# FROM SYS.FGA\_LOG$ order by NTIMESTAMP# desc;

1. **Standard Auditing.**  
   **a. Cấp quyền select DBA\_AUDIT\_TRAIL cho admin.**  
   - GRANT SELECT ON dba\_audit\_trail TO ad;  
     
   **b. Thực hiện audit hệ thống.**  
   \* Chính sách 4: Kiểm tra nhật ký hệ thống.  
   - Theo dõi các hành vi (SELECT, INSERT, UPDATE, DELETE) của các USER trên hệ thống.  
   - Theo dõi các hành vi thất bại và thành công.  
     
   **c. Kiểm tra audit.**  
   - select username, EXTENDED\_TIMESTAMP ,obj\_name, action\_name, sql\_text from dba\_audit\_trail order by EXTENDED\_TIMESTAMP desc;