# A. Lý thuyết

## II. Quản lí Standard Audit Trail

### 2.1 Kích hoạt Standard Auditing

|  |
| --- |
| SHOW PARAMETER AUDIT; |

A screenshot of a computer

Description automatically generated

Chức năng Audit mặc định không được kích hoạt, nhưng có thể kích hoạt nó bằng cách thiết lập giá trị cho tham số **AUDIT\_TRAIL**

|  |
| --- |
| AUDIT\_TRAIL = {none | os | db | db, extended | xml | xml, extended} |

Chuyển sang CDB$ROOT là cần thiết khi bạn muốn thay đổi một tham số cấp CDB như audit\_trail, vì nếu không, lệnh sẽ chỉ áp dụng cho container hiện tại (PDB), và sẽ không có hiệu lực toàn cục.

Để kích hoạt chức năng giám sát, làm theo các bước sau (Đăng nhập bằng tài khoản SYS với quyền SYSDBA trong CMD):

|  |
| --- |
| ALTER SESSION SET CONTAINER = CDB$ROOT;  ALTER SYSTEM SET audit\_trail = db SCOPE = SPFILE;  SHUTDOWN IMMEDIATE;  STARTUP MOUNT; |

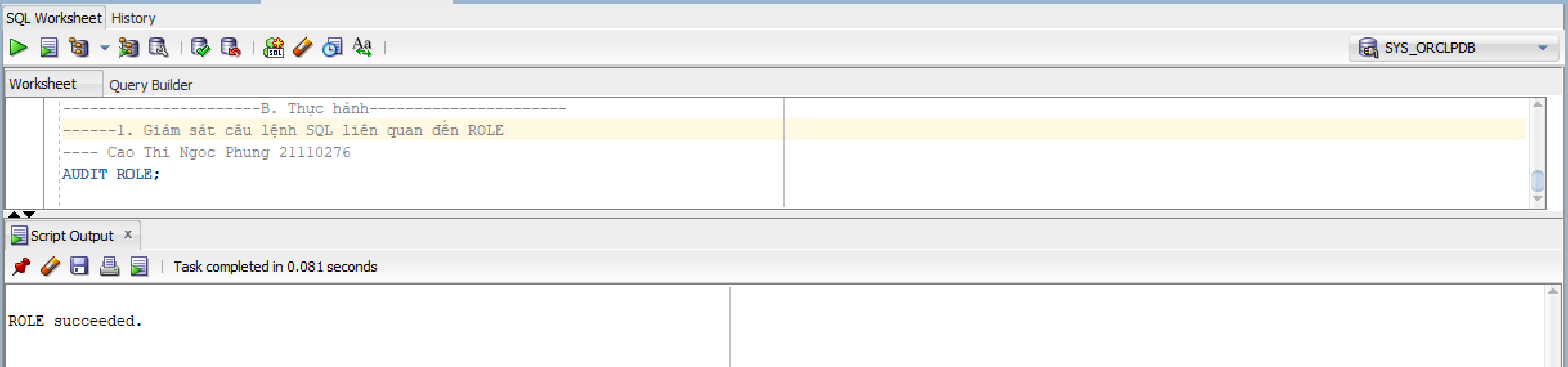
A white rectangular object with yellow squares

Description automatically generated with medium confidence

# B. Thực hành

## 1. Giám sát câu lệnh SQL liên quan đến ROLE

|  |
| --- |
| AUDIT ROLE; |



Kiểm tra tác dụng của câu lệnh audit trên:

|  |
| --- |
| CREATE ROLE test; |

A white rectangular object with black lines

Description automatically generated

|  |
| --- |
| AUDIT ROLE WHENEVER SUCCESSFUL; |

A screenshot of a computer

Description automatically generated

|  |
| --- |
| select username,  timestamp, obj\_name, action\_name  from dba\_audit\_trail  where username = 'SEC\_MGR'; |

A white rectangular object with a yellow stripe

Description automatically generated

## 2. Giám sát câu lệnh SQL select và update

Giám sát cho bất cứ câu lệnh nào truy vấn hay update bất kì bảng nào

|  |
| --- |
| AUDIT ROLE WHENEVER SUCCESSFUL; |

A screenshot of a computer

Description automatically generated

Giám sát câu lệnh SELECT hay UPDATE một bảng / view nào đó được thực hiện bởi user hr

|  |
| --- |
| AUDIT SELECT TABLE, UPDATE TABLE BY hr; |

A white rectangular object with a shadow

Description automatically generated

## 3. Giám sát quyền xóa bảng

Giám sát câu lệnh sử dụng quyền hệ thống DELETE ANY TABLE

|  |
| --- |
| AUDIT DELETE ANY TABLE; |

A white rectangular object with yellow stripes

Description automatically generated

## 4. Giám sát quyền liên quan tới Directories

Giám sát câu lệnh sử dụng quyền hệ thống CREATE ANY DIRECTORY

|  |
| --- |
| AUDIT CREATE ANY DIRECTORY; |

A screenshot of a computer

Description automatically generated

Giám sát lệnh CREATE DIRECTORY (và DROP DIRECTORY) mà không sử dụng quyền hệ thống CREATE DIRECTORY:

|  |
| --- |
| AUDIT DIRECTORY; |

A white rectangular object with yellow lines

Description automatically generated

|  |
| --- |
| CREATE OR REPLACE DIRECTORY ngocphung\_week12 AS 'W:\Oracle\DBSE\_Database\_Security';  AUDIT READ ON DIRECTORY ngocphung\_week12; |

A screenshot of a computer

Description automatically generated

## 5. Giám sát truy vấn trên bảng

Giám sát cho mỗi câu SQL truy vấn tới bảng employees trong schema hr:

|  |
| --- |
| AUDIT SELECT ON hr.employees; |

A screenshot of a computer

Description automatically generated

Giám sát cho mỗi câu truy vấn tới bảng employees trong schema hr và kết quả đó trong CSDL Oracle bị lỗi:

|  |
| --- |
| AUDIT SELECT ON hr.employees  WHENEVER NOT SUCCESSFUL; |

A screenshot of a computer

Description automatically generated

## 6. Giám sát insert và update trên bảng

Giám sát cho mỗi câu lệnh insertvà update một hàng trong bảng customers của schema hr:

|  |
| --- |
| AUDIT INSERT, UPDATE ON hr.customers; |

A white rectangular object with yellow lines

Description automatically generated

## 7. Thiết lập mặc định cho lựa chọn giám sát đối tượng

Đặc tả lựa chọn giám sát mặc định cho các đối tượng được tạo ra trong tương lai:

|  |
| --- |
| AUDIT ALTER, GRANT, INSERT, UPDATE, DELETE  ON DEFAULT; |

A white rectangular object with yellow stripes

Description automatically generated

## 8. Tắt giám sát

Tắt giám sát trên câu lệnh:

|  |
| --- |
| NOAUDIT ALL; |

A white and yellow stripes

Description automatically generated with medium confidence

Tắt giám sát trên quyền:

|  |
| --- |
| NOAUDIT ALL PRIVILEGES; |

A screenshot of a computer

Description automatically generated

**Chú ý:** để disable giám sát câu lệnh và quyền thì phải có quyền hệ thống AUDIT SYSTEM.

|  |
| --- |
| NOAUDIT SELECT ON hr.employees;  NOAUDIT INSERT, UPDATE ON hr.customers; |

A screenshot of a computer

Description automatically generated

# IV. Bài tập

## 1. Tạo user mới với username là audit\_test.

Phân quyền connect, create table và create procedure cho user vừa mới tạo.

|  |
| --- |
| CREATE USER audit\_test IDENTIFIED BY audittest;  GRANT CREATE TABLE TO audit\_test;  GRANT CREATE PROCEDURE TO audit\_test;  GRANT CREATE SESSION TO audit\_test;  ALTER USER audit\_test QUOTA 100M ON USERS; |

A screenshot of a computer

Description automatically generated

## 2. Thực hiện giám sát

Các hành vi xem, thêm, sửa, xóa dòng trên bất kì bảng nào của user audit\_test.

|  |
| --- |
| AUDIT SELECT ON DEFAULT;  AUDIT INSERT ON DEFAULT;  AUDIT UPDATE ON DEFAULT;  AUDIT DELETE ON DEFAULT; |

A screenshot of a computer

Description automatically generated

## 3. Đăng nhập vào tài khoản user audit\_test.

Thực hiện chuỗi hành động sau

### 3.a Tạo bảng tên TAB (bảng TAB chỉ có một cột ID có kiểu là NUMBER)

|  |
| --- |
| CREATE TABLE TAB (ID NUMBER); |

A screenshot of a computer

Description automatically generated

### 3.b Insert giá trị vào bảng TAB.

|  |
| --- |
| INSERT INTO TAB VALUES (1); |

A blue and white stripes

Description automatically generated

### 3.c Update giá trị vừa insert vào.

|  |
| --- |
| UPDATE TAB SET ID = 2 WHERE ID = 1; |

A blue and white line

Description automatically generated

### 3.d Xem tất cả dữ liệu của bảng TAB.

|  |
| --- |
| SELECT \* FROM TAB; |

A blue and white stripes

Description automatically generated

### 3.e Xóa tất cả dữ liệu trong bảng TAB.

|  |
| --- |
| DELETE FROM TAB; |

A screenshot of a computer

Description automatically generated

### 3.f Xóa bảng TAB.

|  |
| --- |
| DROP TABLE TAB; |

A white and yellow striped surface

Description automatically generated

## 4. Đăng nhập vào user system, kiểm tra những hành vi nào được giám sát lại.

Hành vi tạo bảng và xóa bảng của user audit\_test có bị giám sát không? Nếu có hãy giải thích lý do, nếu không hãy tạo câu lệnh giám sát hành vi tạo bảng và xóa bảng của user audit\_test.

|  |
| --- |
| SELECT USERNAME,TIMESTAMP,OWNER,OBJ\_NAME,ACTION\_NAME  from dba\_audit\_trail  WHERE OWNER ='AUDIT\_TEST' |

A screenshot of a computer

Description automatically generated

Hành vi **TẠO BẢNG** và **XÓA BẢNG** của user audit\_test không được giám sát vì trong lệnh AUDIT ban đầu chỉ thiết lập theo dõi các hành vi trên dữ liệu như INSERT, SELECT, UPDATE, và DELETE. Để giám sát hai hành vi này, cần sử dụng lệnh AUDIT CREATE TABLE và AUDIT DROP TABLE. Sau khi bổ sung, các thao tác tạo và xóa bảng sẽ được ghi lại trong bảng DBA\_AUDIT\_TRAIL.

### **4.a Cách giám sát hành vi**

Giám sát hành vi TẠO BẢNG (CREATE TABLE) và XÓA BẢNG (DROP TABLE)

|  |
| --- |
| AUDIT CREATE TABLE BY audit\_test;  AUDIT DROP ANY TABLE; |

A screenshot of a computer

Description automatically generated

Hoặc chỉ định xóa bảng TAB

|  |
| --- |
| CREATE TABLE TAB (I NUMBER);  DROP TABLE TAB; |

A screenshot of a computer

Description automatically generated

Kiểm tra lại

|  |
| --- |
| SELECT USERNAME,TIMESTAMP,OWNER,OBJ\_NAME,ACTION\_NAME  from dba\_audit\_trail  WHERE OWNER ='AUDIT\_TEST' |

A screenshot of a computer

Description automatically generated