Bài thực hành số 9

STANDARD AUDITING

❖ *Tóm tắt nội dung:*

- Khái quát về Database Auditing
- Kích hoạt các lựa chọn của Standard Auditing
- Statement Auditing
- Privilege Auditing
- Schema Object Auditing

I. Khái quát về Database Auditing

1. Định nghĩa

- Auditing là hoạt động giám sát và ghi lại những hành động của người dùng trên cơ sở dữ liệu. Được dựa trên các hoạt động cá nhân như loại câu lệnh SQL thực thi, hay dựa trên sự kết hợp các yếu tố bao gồm tên, ứng dụng, thời gian… Các chính sách bảo mật có thể dẫn đến việc audit khi những phần tử cụ thể trong CSDL Oracle bị truy cập hay thay thế.
- Auditing nhìn chung được sử dụng:
  - ✓ Cho phép giải trình những hành động hiện tại tham gia vào một schema, bảng, dòng riêng biệt, hay một nội dung cụ thể nào đó.
  - ✓ Ngăn cản user khỏi hành động không thích hợp dựa trên trách nhiệm phải giải trình đó.
  - ✓ Điều tra các hoạt động đáng ngờ. Ví dụ, nếu một user không được phép xóa dữ liệu từ một bảng nào đó thì người quản trị bảo mật sẽ ghi lại tất cả những kết nối CDSL và tất cả những hành động xóa các dòng từ bảng trong CSDL dù thành công hay không thành công.
  - ✓ Thông báo cho người giám sát rằng có user bất hợp phát đang thao tác hay xóa dữ liệu hay user có nhiều quyền hệ thống hơn sự cho phép.

- ✓ Giám sát và thu thập dữ liệu về các hoạt động CSDL cụ thể. Ví dụ, người quản trị CSDL có thể thu thập thống kê về thông tin các bảng đang được update, hay bao nhiêu users cùng truy cập vào thời điểm cực đỉnh.

2. Các kiểu giám sát (Types of Auditing)

- Oracle cho phép giám sát theo 2 lựa chọn tập trung hoặc mở rộng.
  - ✓ Sự thực thi câu lệnh thành công, hoặc không thành công, hoặc cả hai.
  - ✓ Mỗi lần thực thi câu lệnh trong mỗi session của user, hay bất kì khi nào mà câu lệnh được thực thi.
  - ✓ Hoạt động của tất cả các user hay của một user cụ thể nào đó.
- Có bốn kiểu giám sát:
  - ✓ **Statement auditing:** chia thành hai nhóm
    - Câu lệnh DDL: Ví dụ AUDIT TABLE giám sát tất cả các câu lệnh CREATE và DROP TABLE.
    - Câu lệnh DML: Ví dụ AUDIT SELECT TABLE giám sát tất cả câu lệnh SELECT trên bảng và trên view.
  - ✓ **Privilege auditing:** Kiểm tra việc sử dụng quyền hệ thống, ví dụ AUDIT CREATE TABLE. Privilege auditing được chú trọng hơn statement auditing vì nó chỉ kiểm tra việc sử dụng một số quyền nhất định. Có thể đặt privilege auditing giám sát những user được lựa chọn hay giám sát mọi user.
  - ✓ **Schema object auditing:** Kiểm tra câu lệnh cụ thể trên đối tượng schema cụ thể, ví dụ AUDIT SELECT ON employees. Schema object auditing luôn áp dụng cho tất cả các user.
  - ✓ **Fine-grained auditing:** Kiểm tra dữ liệu truy xuất và các hoạt động dựa trên nội dung của dữ liệu đó. Ví dụ: Sử dụng DBMS_FGA, người quản trị bảo mật tạo ra một chính sách kiểm tra trên một bảng. Nếu bất kì dòng nào trả về từ câu lệnh DML thỏa điều kiện kiểm tra thì một mục về sự kiện kiểm tra sẽ được chèn vào trong audit trail.

3. Audit Records và Audit Trails:

- Những thông tin được audit sẽ được lưu trong data dictionary table, gọi là **database**

audit trail, hoặc lưu trong operating system files, gọi là **operating system audit trail.**

- **Database audit trail**
  - ✓ Database audit trail gồm một bảng có tên là SYS.AUD$ thuộc shema SYS của từ điển dữ liệu trong mỗi CSDL Oracle. Chúng ta có thể sử dụng một số view để xem thông tin trong bảng này, ví dụ: DBA_AUDIT_TRAIL.
  - ✓ Chứa những loại thông tin khác nhau, phụ thuộc vào những sự kiện được giám sát và tập các lựa chọn giám sát. Mỗi bản ghi audit bao gồm những thông tin sau:
    - Database user name (DATABASE USER)
    - Operating system login user name (CLIENT USER)
    - Instance number (không có trong Operation System…)
    - Process identifier
    - Session identifier
    - Terminal identifier
    - Name of the schema object accessed
    - Operation performed or attempted (ACTION)
    - Completion code of the operation
    - Date & time stamp in UTC format (không có trong Operation System Audit Trail)
    - System privileges used (PRIVILEGE)
  - ✓ **Chú ý:** Audit trail không lưu thông tin về giá trị của dữ liệu dù nó liên quan đến trong câu lệnh được giám sát. Ví dụ, giá trị dữ liệu mới và giá trị dữ liệu cũ của hàng được update không được lưu lại khi câu lệnh UPDATE được giám sát. Tuy vậy, đối với phương pháp fine-grained auditing thì có khác.

- **Operating System Audit Trail**
  - ✓ Oracle cho phép bản ghi dấu audit (audit trail records) được trực tiếp ghi vào operating system audit trail nếu hệ điều hành tạo một audit trail sẵn cho Oracle. Nếu không thì bản audit sẽ được ghi vào file bên ngoài CSDL, với định dạng tương tự như các file dấu tích Oracle (Oracle trace) khác.

- ✓ Oracle cho phép một hoạt động nào đó vẫn tiếp tục được giám sát, thậm chí khi operating system audit trail (hay file bên ngoài chứa bản ghi audit) không được phép ghi lại bản ghi audit do nó bị đầy. Tuy nhiên, nếu cấu hình auditing sử dụng **database audit trail** để lưu bản ghi audit thì sẽ loại bỏ khả năng mất thông tin audit, bởi vì hệ CSDL Oracle ngăn ngừa sự kiện được audit khỏi xảy ra nếu audit trail không thể tiếp nhận bản ghi database audit cho câu lệnh đó.

II. Quản lí Standard Audit Trail

1. Kích hoạt Standard Auditing

- Bất cứ database user hợp pháp nào cũng có thể thiết lập lựa chọn giám sát đối với câu lệnh, quyền và đối tượng bất cứ khi nào. Tuy nhiên hệ CSDL Oracle không sinh thông tin audit cho *Standart database audit trail* trừ khi CSDL giám sát được kích hoạt. Người quản trị bảo mật thường có trách nhiệm điều khiển việc giám sát này.
- Auditing là chức năng mặc định trong Oracle server. Có thể dùng câu lệnh `Show parameter audit` để xem các tham số khởi tạo ban đầu.

```
SHOW PARAMETER AUDIT;
NAME                    TYPE      VALUE
---------------------   --------  ----------------------
audit_file_dest         string    C:\ORACLEXE\APP\ORACLE\
                                      ADMIN\XE\ADUMP
audit_sys_operations    boolean   FALSE
audit_trail             string    NONE
```

- 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}`

  Trong đó:

  - ✓ `none` – Disable chức năng giám sát.
  - ✓ `db` – Bật chức năng giám sát và các bản ghi giám sát được sẽ được lưu trong

database audit trail (`SYS.AUD$`).

- ✓ `os` - Bật chức năng giám sát với các bản ghi giám sát được ghi vào operating system audit trail.
- ✓ `xml` - Bật chức năng giám sát với các bản ghi giám sát được sẽ được lưu như file OS có định dạng XML.

- Tham số `AUDIT_SYS_OPERATIONS` dùng để enable hay disable giám sát các hoạt động của những user kết nối vào hệ thống với quyền SYSDBA hay SYSOPER, bao gồm user SYS. Khi đó tất cả các bản ghi giám sát được ghi vào OS audit trail.
- Tham số `AUDIT_FILE_DEST` đặc tả đường dẫn đến thư mục của hệ điều hành dùng để lưu audit trail khi các lựa chọn {`OS; XML; XML, EXTENDED`} được sử dụng. Nó cũng là vị trí lưu các bản ghi giám sát của user `SYS` khi tham số `AUDIT_SYS_OPERATIONS = true`.
- Để kích hoạt chức năng giám sát, làm theo các bước sau (Đăng nhập bằng tài khoản SYS với quyền SYSDBA trong CMD):

```
ALTER SYSTEM SET audit_trail = db SCOPE = SPFILE;
System altered.

SHUTDOWN IMMEDIATE;
Database closed.
Database dismounted.
ORACLE instance shut down.

STARTUP MOUNT;
ORACLE instance started.
Database mounted.

ALTER DATABASE OPEN;
Database opened.
```

2. Kích hoạt lựa chọn Standard Auditing

- Để sử dụng lệnh AUDIT thiết lập lựa chọn về câu lệnh và quyền thì bạn nhất thiết

phải có quyền AUDIT SYSTEM. Còn để thiết lập các lựa chọn giám sát đối tượng bạn phải làm chủ đối tượng bị giám sát hay có quyền AUDIT ANY.

- Lệnh AUDIT thiết lập lựa chọn giám sát câu lệnh và quyền có thể bao gồm mệnh đề BY để cụ thể danh sách những user hay application proxy để giới hạn tầm vực của câu lệnh và lựa chọn giám sát quyền.
  - ✓ BY SESSION/ BY ACCESS
    - BY SESSION:

      Ghi một record cho tất cả các câu lệnh SQL cùng loại và tất cả các hoạt động cùng loại được thực hiện trên cùng một đối tượng schema trong cùng một session. Tuy nhiên nếu sử dụng operating system trail để theo dấu giám sát (khi đó tham số AUDIT_TRAIL được gán giá trị OS), thì CSDL sẽ lưu nhiều record vào file đó ngay cả khi bạn sử dụng mệnh đề BY SESSION.
    - BY ACCESS:

      Ghi một record cho mỗi câu lệnh và hoạt động được audit. Nếu đặc tả lựa chọn câu lệnh hay quyền hệ thống là giám sát câu lệnh DDL thì CSDL sẽ tự động giám sát theo BY ACCESS không quan tâm bạn sử dụng mệnh đề BY SESSION hay BY ACCESS. Ngoài ra, nếu người dùng không đặc tả thì mặc định là BY SESSION.
  - ✓ WHENEVER SUCCESSFUL/ WHENEVER NOT SUCCESSFUL
    - WHENEVER SUCCESSFUL giám sát những lệnh thành công.
    - WHENEVER NOT SUCCESSFUL giám sát những lệnh thất bại hay kết quả lỗi. Nếu loại bỏ hai mệnh đề này thì Oracle cũng sẽ ghi lại sự giám sát không quan tâm câu lệnh có thành công hay không.

3. Disable lựa chọn Standard Auditing

- Câu lệnh NOAUDIT để tắt các lựa chọn giám sát.
- Mệnh đề WHENEVER để tắt các giám sát đối với các câu lệnh được thực hiện thành công hay không thành công. Nếu không sử dụng mệnh đề đó thì chức năng giám sát sẽ tắt cả đối với trường hợp thành công hay thất bại.
- Mệnh đề BY SESSION/BY ACCESS không được hỗ trợ trong câu lệnh NOAUDIT.

4. Điều khiển sự phát triển và kích thước của Standard Audit Trail

- Nếu audit trail đầy dẫn tới không một bản ghi giám sát nào được ghi thêm vào thì những câu lệnh AUDIT không thể thực thi thành công cho tới khi audit trail trống trở lại. Do đó, người quản trị bảo mật phải điều khiển sự phát triển và kích thước của audit trail.
- Khi chức năng giám sát được kích hoạt và các bản ghi giám sát được sinh ra thì dung lượng của audit trail phụ thuộc hai yếu tố:
  - ✓ Số lựa chọn giám sát được sử dụng.
  - ✓ Tần số thực hiện các câu lệnh được giám sát.
- Để điều khiển sự phát triển của audit trail, bạn có thể sử dụng phương pháp:
  - ✓ Enable và disable giám sát CSDL. Nếu nó được enable thì các bản ghi giám sát được sinh ra và lưu trữ trong audit trail. Nếu disable thì các bản ghi sẽ không được sinh ra.
  - ✓ Chọn lọc kĩ những lựa chọn giám sát được kích hoạt. Nếu nhiều lựa chọn giám sát được kích hoạt thì những bản ghi giám sát không cần thiết có thể làm đầy audit trail.
  - ✓ Quản lí chặt khả năng giám sát đối tượng. Điều đó có thể được thực hiện bằng hai cách khác nhau:
    - Người quản trị bảo mật làm chủ tất cả các đối tượng và quyền hệ thống AUDIT ANY không cấp cho bất kì một user nào khác.
    - Tất cả các đối tượng chứa trong những schema mà không tương ứng với database user thực sự (user đó không được cấp quyền CREATE SESSION) và người quản trị bảo mật là user duy nhất có quyền AUDIT ANY.
  - ✓ Xóa một số bản ghi trong audit trail để vừa giải phóng vùng nhớ vừa làm thuận tiện cho việc quản lí audit trail.

Ví dụ:

Xóa toàn bộ bản ghi được sinh ra do kết quả của việc giám sát bảng EMP:

```
DELETE FROM SYS.AUD$ WHERE obj$name = 'EMP';
```

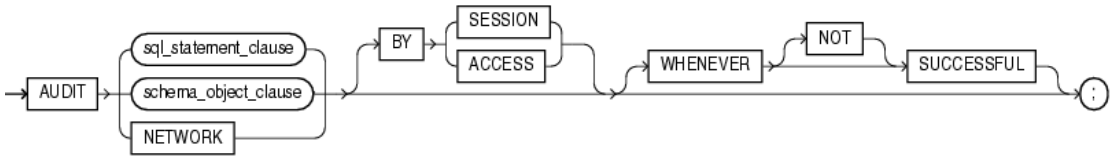
Chú ý: Chỉ có user SYS, hoặc user có quyền DELETE ANY TABLE, hoặc user

được SYS gán quyền DELETE trên SYS.AUD$ mới có thể thực hiện câu lệnh trên.

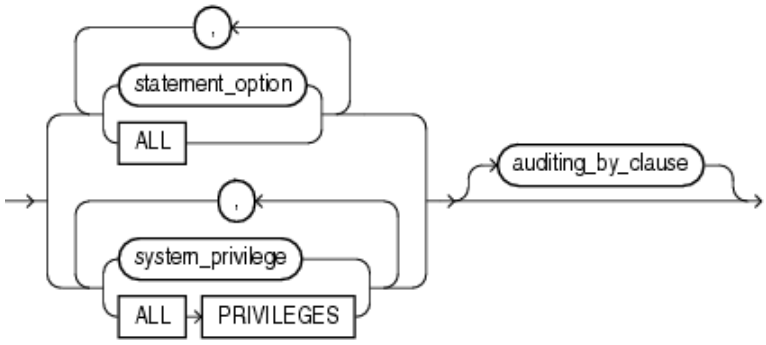
III. Cú pháp

A. Lý thuyết

1. audit::=

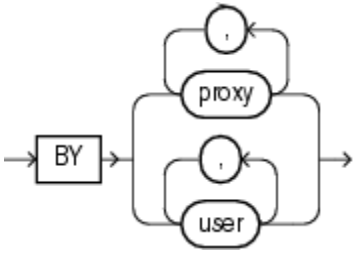


2. sql_statement_clause::=



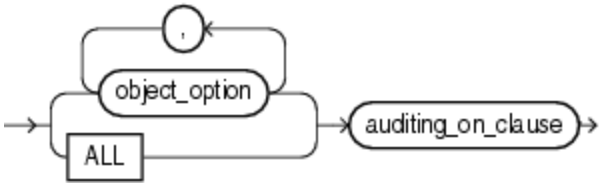
Chú ý: Oracle khuyên rằng nên đặc tả lựa chọn quyền hệ thống và câu lệnh để giám sát hơn là nêu chúng qua các role hoặc shortcuts.

3. auditing_by_clause::=



Giám sát chỉ những câu lệnh SQL gọi bởi những user cụ thể. Nếu không sử dụng mệnh đề này thì Oracle sẽ giám sát câu lệnh của tất cả user.

4. schema_object_clause::=

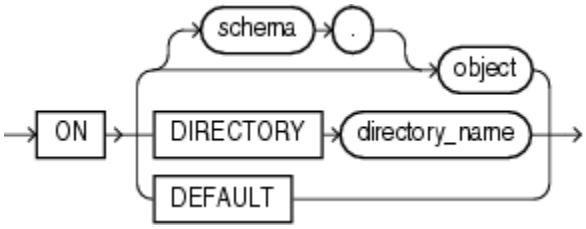


Giám sát các hoạt động trên những đối tượng schema.

Object_option: đặc tả hoạt động cụ thể cho việc giám sát. Ví dụ như `ALTER, COMMENT, AUDIT, DELETE, EXECUTE, GRANT, INSERT, READ,…`

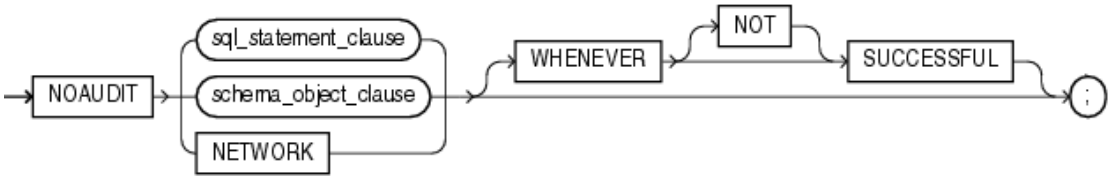
ALL: là một shortcut tương ứng với tất cả các object options cho các loại đối tượng.

5. auditing_on_clause::=



- auditing_on_clause: đặc tả đối tượng schema riêng biệt được giám sát.
- ON DEFAULT: thiết lập những lựa chọn audit đối tượng mặc định cho những đối tượng được tạo ra sau đó. Sau khi thiết lập tùy chọn này, bất kì đối tượng nào được tạo ra sau đó sẽ được giám sát tự động với tùy chọn đó. Những tùy chọn audit mặc định cho một view luôn là sự kết hợp của tùy chọn audit của tất cả các bảng cơ sở của view đó. Có thể xem lựa chọn giám sát mặc định hiện tại bằng cách truy vấn ALL_DEF_AUDIT_OPTS.
- Khi thay đổi tùy chọn audit mặc định, tùy chọn audit cho những đối tượng được tạo lúc trước vẫn giữ nguyên. Bạn có thể thay đổi tùy chọn audit cho đối tượng đã tồn tại chỉ bằng đặc tả đối tượng trong mệnh đề ON của câu lệnh AUDIT.

6. noaudit::=



B. Thực hành

1. Giám sát câu lệnh SQL liên quan đến ROLE

- Giám sát tất cả các câu lệnh SQL liên quan đến ROLE (create, alter, drop, set) không quan tâm câu lệnh được thực hiện thành công hay không:

```
AUDIT ROLE;
```

- Kiểm tra tác dụng của câu lệnh audit trên:

```
conn system/password;
create role test;

select username, timestamp, obj_name, action_name
from dba_audit_trail where username = 'SYSTEM';

USERNAME     TIMESTAMP      OBJ_NAME   ACTION_NAME
--------     ---------      --------   -----------
SYSTEM       11-NOV-12      TEST       CREATE ROLE
```

- Giám sát tất cả câu lệnh liên quan đến ROLE mà thực hiện thành công:

```
AUDIT ROLE WHENEVER SUCCESSFUL;
```

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 SELECT TABLE, UPDATE TABLE;
```

- Giám sát câu lệnh SELECT hay UPDATE một bảng hoặc view nào đó được thực hiện bởi user hr và oe:

```
AUDIT SELECT TABLE, UPDATE TABLE BY hr, oe;
```

3. Giám sát quyền xóa bảng

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

```
AUDIT DELETE ANY TABLE;
```

4. Giám sát quyền liên quan tới Directories

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

```
AUDIT CREATE ANY DIRECTORY;
```

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

```
AUDIT DIRECTORY;
```

- Giám sát mỗi câu lệnh đọc file từ đường dẫn bfile_dir:

```
AUDIT READ ON DIRECTORY bfile_dir;
```

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;
```

- 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;
```

6. Giám sát insert và update trên bảng

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

```
AUDIT INSERT, UPDATE ON oe.customers;
```

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;
```

- Bất kì đối tượng nào được tạo ra sau đó sẽ tự động bị giám sát với đặc tả được lựa chọn đó (trong trường hợp chức năng giám sát được kích hoạt)
  - ✓ Nếu tạo ra một bảng thì Oracle tự động giám sát các câu lệnh `ALTER, GRANT, INSERT, UPDATE, DELETE` liên quan đến bảng này.
  - ✓ Nếu tạo ra một view thì Oracle sẽ tự động giám sát các câu lệnh `GRANT, INSERT, UPDATE, DELETE` liên quan đến view này.
  - ✓ Nếu tạo ra một procedure, package, hay function thì Oracle sẽ tự động giám sát các câu lệnh `ALTER` hay `GRANT` liên quan đến nó.

8. Tắt giám sát

- Tắt giám sát trên câu lệnh:

```
NOAUDIT ALL;
```

- Tắt giám sát trên quyền:

```
NOAUDIT ALL PRIVILEGES;
```

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

- Tắt giám sát trên đối tượng:

```
NOAUDIT SELECT ON hr.employees;
NOAUDIT INSERT, UPDATE ON oe.customers;
```

- Để tắt giám sát trên đối tượng cụ thể thì bạn phải là chủ đối tượng đó. Để tắt giám sát trên đối tượng thuộc schema của user khác hay tắt giám sát mặc định trên đối tượng thì bạn phải có quyền hệ thống AUDIT ANY.

9. Các view của Audit Trail

- Các bản ghi giám sát được lưu trong bảng AUD$ thuộc schema SYS. Nội dung của nó có thể được xem trực tiếp hoặc qua các view.

View	Mô tả
STMT_AUDIT_OPTION_MAP	Chứa thông tin về các loại audit option.
AUDIT_ACTIONS	Chứa thông tin về các loại audit action.
ALL_DEF_AUDIT_OPTS	Chứa các option mặc định của giám sát trên đối tượng sẽ được áp dụng khi đối tượng được tạo ra. (-/-: no default auditing, S/-: auditing whenever successful, -/S: auditing whenever not successful)
DBA_STMT_AUDIT_OPTS	Chứa các option audit trong hệ thống hiện hành.
DBA_PRIV_AUDIT_OPTS	Thông tin các quyền hệ thống được audit.
DBA_OBJ_AUDIT_OPTS USER_OBJ_AUDIT_OPTS	Thông tin các option audit trên tất cả các đối tượng.
DBA_AUDIT_TRAIL USER_AUDIT_TRAIL	Liệt kê tất cả thông tin trong audit trail.
DBA_AUDIT_OBJECT USER_AUDIT_OBJECT	Chứa thông tin giám sát liên quan đến tất cả đối tượng trong hệ thống.
DBA_AUDIT_SESSION USER_AUDIT_SESSION	Liệt kê tất cả thông tin giám sát liên quan đến câu lệnh CONNECT và DISCONNECT.
DBA_AUDIT_STATEMENT USER_AUDIT_STATEMENT	Liệt kê tất cả thông tin giám sát liên quan đến câu lệnh GRANT, REVOKE, AUDIT, NOAUDIT, và ALTER SYSTEM.
DBA_AUDIT_EXISTS	Liệt kê tất cả thông tin giám sát gây ra bởi option BY AUDIT NOT EXISTS.
DBA_AUDIT_POLICIES	Liệt kê tất cả chính sách audit trong hệ thống.
DBA_FGA_AUDIT_TRAIL	Liệt kê tất cả thông tin giám sát của fine-grained audit.
DBA_COMMON_AUDIT_TRAIL	Liệt kê tất cả thông tin giám sát của standard audit và fine-grained audit.

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.
2. Thực hiện giám sát các hành vi xem, thêm, sửa, xóa dòng trên bất kì bảng nào của user audit_test.
3. Đăng nhập vào tài khoản user audit_test. Thực hiện chuỗi hành động sau
   a. Tạo bảng tên TAB (bảng TAB chỉ có một cột ID có kiểu là NUMBER)
   b. Insert giá trị vào bảng TAB.

c. Update giá trị vừa insert vào.

d. Xem tất cả dữ liệu của bảng TAB.

e. Xóa tất cả dữ liệu trong bảng TAB.

f. Xóa bảng TAB.

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.