**Bài thực hành số 12**

**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

# Khái quát về Database Auditing

1. **Định nghĩa:**

* Auditing là hoạt động giám sát và ghi lại…. Được dựa trên các hoạt động cá nhân như thực hiện câu lệnh SQL, 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 đang 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 trung cập vào thời điểm cực đỉnh.

1. **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. (Rất được chú trọng). 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.

1. **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.**
* **Bản ghi Audit (Audit trail records)**
* Chứa những loại thông tin khác nhau, phụ thuộc vào những sự kiện được giám sát và tập các lựa chọn giám sát. Thông tin sau đây được bao gồm trong mỗi bản ghi audit:
* 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 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 mà luôn bị giám sát được tiếp tục, thậm chí khi mà operating system audit trail ( hay file hệ điều hành chứa bản ghi audit) không được phép ghi lại bản ghi audit do nó bị đầy. Tuy nhiên, chú ý rằng cấu hình auditing để sử dụng **database audit trail** loại bỏ được điểm yếu này, 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.

# 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. Các tham số khởi tạo ban đầu ảnh hưởng đến hành vi của nó có thể được xem bằng cách sử dụng câu lệnh.

SQL> 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 bị bất 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 or false – chức năng giám sát bị bất hoạt.
* db or true – Bật chức năng giám sát và các bản ghi giám sát được sẽ được lưu trong database audit trail (SYS.AUD$).
* xml- Bật chức năng giám sát với các bản ghi giám sát được sẽ được lưu như file OS có định dạng XML.
* os- Bật chức năng giám sát với các bản ghi giám sát được ghi vào operating system audit trail.
* Tham số AUDIT\_SYS\_OPERATIONS dùng để kích hoạt hay bất hoạt 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 cho audit trail khi các lựa chọn OS, XML, EXTENDED được sử dụng. Nó cũng là vị trí lưu các bản ghi giám sát khi tham số AUDIT\_SYS\_OPERATIONS = true
* Để kích hoạt chức năng giám sát, làm theo các bước sau

SQL> ALTER SYSTEM SET audit\_trail=db SCOPE=SPFILE;

System altered.

SQL> SHUTDOWN

Database closed.

Database dismounted.

ORACLE instance shut down.

SQL> STARTUP

ORACLE instance started.

Database mounted.

Database opened.

SQL>

1. **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 bản ghi đơn cho tất cả các câu lệnh SQL cùng loại thực thi trên cùng những đối tượng schema trong cùng một session. Tuy nhiên nếu sử dụng operating system trail cho theo dấu giám sát (khi đó tham số AUDIT\_FILE\_DEST được gán giá trị OS), thì CSDL sẽ viết nhiều mục vào file theo dấu ngay cả khi bạn sử dụng mệnh đề BY SESSION.

* BY ACCESS:

Ghi một bản ghi cho mỗi lần truy xuất. Nếu đặc tả lựa chọn câu lệnh hay quyền hệ thống mà 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 thì nếu không đặc tả thì BY SESSION là mặc định.

* + - 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.

1. **Bất hoạt lựa chọn Standard Auditing**

* Câu lệnh NOAUDIT để tắt các lựa chọn giám sát của Oracle 10G.
* 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.

1. **Điều khiển sự phát triển và kích cỡ 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 cỡ 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:
* Kích hoạt và bất hoạt giám sát CSDL. Nếu nó được kích hoạt thì các bản ghi giám sát được sinh ra và lưu trữ trong audit trail. Nếu nó bất hoạt 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:
  + - Nhà quản trị bảo mật làm chủ tất cả các đối tượng và quyền hệ thống AUDIT ANY không bị 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 trong audit trail:

DELETE FROM SYS.AUD$;

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

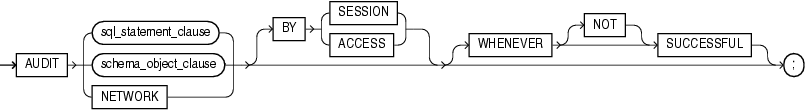
DELETE FROM SYS.AUD$

WHERE obj$name = ‘EMP’;

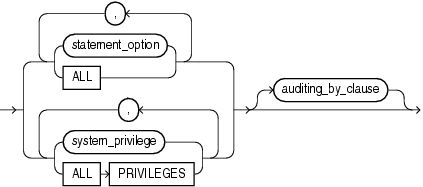
Chú ý: Chỉ có user SYS (user có quyền DELETE ANY TABLE), hay user đượcSYS gán quyền DELETE trên SYS.AUD$ mới có thể thực hiện những câu lệnh trên.

# Cú pháp

1. **Lý thuyết**
2. audit::=

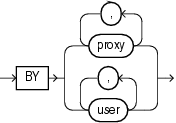


1. sql\_statement\_clause::=



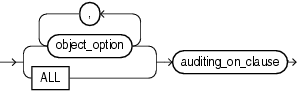
Chú ý: Oracle khuyên rằng nên đặc tả lựa chọn quyền hệ thống và câu lệnh để giám sát hơn là nêu chung qua các role hoặc shortcuts.

1. 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.

1. schema\_object\_clause::=

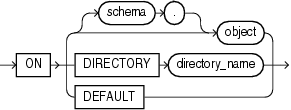


Giám sát các hoạt động trên những đối tượng schema.

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

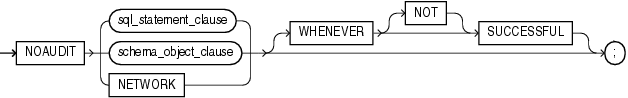
ALL: là một shortcut tương ứng với tất cả các object options cho các loại đối tượng.

1. auditing\_on\_clause::=



* auditing\_on\_clause: đặc tả đối tượng schema riêng biệt được giám sát.
* ON DEFAULT: thiết lập những lựa chọn đối tượng cụ thể trở thành những lựa chọn đối tượng mặc định cho những đối tượng được tạo ra sau đó. Sau khi thiết lập những lựa chọn giám sát mặc định, bất kì đối tượng nào được tạo ra sau đó thì được giám sát tự động với những lựa chọn đó. Những lựa chọn giám sát mặc định cho một view luôn là sự kết hợp của lựa chọn giám sát cho 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 lựa chọn giám sát mặc định, lựa chọn giám sát cho những đối tượng được tạo lúc trước vẫn giữ nguyên. Bạn có thể thay đổi lựa chọn giám sát cho đối tượng đã tồn tại chỉ bằng đặt tả đối tượng trong mệnh đề ON của câu lệnh AUDIT.

1. noaudit::=



1. **Thực hành**
2. **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;

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

AUDIT ROLE WHENEVER SUCCESSFUL;

1. **Giám sát truy vấn và update câu lệnh SQL**

* 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 phát ra bởi user hr và oe mà truy vấn hay update một bảng hoặc view nào đó:

AUDIT SELECT TABLE, UPDATE TABLE BY hr, oe;

1. **Giám sát xóa**

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

AUDIT DELETE ANY TABLE;

1. **Giám sát câu lệnh 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;

1. **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;

1. **Giám sát chèn và update trên bảng**

* Giám sát cho mỗi câu lệnh chèn và update một hàng trong bảng customers của schema oe:

AUDIT INSERT, UPDATE

ON oe.customers;

1. **Thiết lập mặc định cho lựa chọn giám sát**

* 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.

1. **Tắt giám sát**

* Tắt giám sát trên câu lệnh:

NOAUDIT ALL;

* Tắt giám sát trên quyền:

NOAUDIT ALL PRIVILEGES;

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

* Tắt giám sát trên đối tượng:

NOAUDIT DELETE

ON emp;

NOAUDIT SELECT, INSERT, DELETE

ON jward.dept;

* Để tắt giám sát trên đối tượng cụ thể thì bạn phải là chủ của đối tượng đó. Để tắt giám sát trên đối tượng của một 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.

1. **Các view của Audit Trail**

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

SELECT view\_name

FROM dba\_views

WHERE view\_name LIKE 'DBA%AUDIT%'

ORDER BY view\_name;

VIEW\_NAME

------------------------------

DBA\_AUDIT\_EXISTS

DBA\_AUDIT\_OBJECT

DBA\_AUDIT\_POLICIES

DBA\_AUDIT\_POLICY\_COLUMNS

DBA\_AUDIT\_SESSION

DBA\_AUDIT\_STATEMENT

DBA\_AUDIT\_TRAIL

DBA\_COMMON\_AUDIT\_TRAIL

DBA\_FGA\_AUDIT\_TRAIL

DBA\_OBJ\_AUDIT\_OPTS

DBA\_PRIV\_AUDIT\_OPTS

DBA\_REPAUDIT\_ATTRIBUTE

DBA\_REPAUDIT\_COLUMN

DBA\_STMT\_AUDIT\_OPTS

14 rows selected.

# 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
   1. Tạo bảng tên TAB (bảng TAB chỉ có một cột ID có kiểu là NUMBER)
   2. Insert giá trị vào bảng TAB.
   3. Update giá trị vừa insert vào.
   4. Xem tất cả dữ liệu của bảng TAB.
   5. Xóa tất cả dữ liệu trong bảng TAB.
   6. 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.