Bài thực hành số 10

FINE-GRAINED AUDITING

❖ *Tóm tắt nội dung:*

- Giới thiệu về Fine-grained Auditing
- Các chính sách Fine-grained Auditing
- Sử dụng gói DBMS_FGA trong Oracle

I. Fine-grained Auditing

1. Giới thiệu

- Ngoài trừ sử dụng câu lệnh AUDIT để ghi nhận và giám sát việc sử dụng các quyền hệ thống, truy xuất đối tượng, sử dụng các lệnh hoặc nhóm câu lệnh, ta còn có thể mở rộng việc giám sát bằng cách sử dụng trigger để tuỳ chỉnh điều kiện giám sát và nội dung giám sát được lưu trữ. Ví dụ ta có thể ghi nhận lại một bản ghi giám sát khi lương của một nhân viên tăng lên 10%. Để sử dụng trigger auditing, ta cần tạo bảng phụ để lưu dữ liệu của quá trình audit, sau đó định nghĩa một trigger để ghi nhận lại dữ liệu thoả điều kiện cần giám sát vào bảng trên. Ưu điểm của trigger auditing là có thể thực hiện audit trên từng hàng, từng cột cho từng câu lệnh cần giám sát một cách có chọn lọc và giảm bớt những dữ liệu không cần thiết khi thực hiện audit.
- Tuy nhiên hai tiêu chí của audit không thể thực hiện bởi standard auditing và trigger auditing là tối thiểu những giám sát không cần thiết và chỉ ra những truy cập gây hại.
- Fine-grained auditing (FGA) có thể thỏa mãn những yêu cầu đó. Với FGA, ta có thể đặt ra nhiều điều kiện giám sát chi tiết hơn. Ta không cần phải thiết lập thông số cho AUDIT_TRAIL để kích hoạt chức năng này, mà chỉ cần tạo ra các chính sách FGA rồi áp dụng chúng trên các hoạt động hay các đối tượng cụ thể mà ta muốn giám sát. Dữ liệu giám sát được của FGA sẽ lưu trong bảng

SYS.FGA_LOG$ và được truy cập thông qua view DBA_FGA_AUDIT_TRAIL.

2. Ưu thế của Fine-grained Auditing so với Trigger Auditing

- Trigger được gọi mỗi khi một hàng được xử lí và tạo ra một bản ghi giám sát chỉ khi một cột thích hợp bị thay đổi bởi một câu lệnh DML. Fine-grainned auditing chỉ giám sát một lần cho mỗi chính sách. Cụ thể, nó sẽ giám sát khi cột được giám sát xuất hiện trong một loại lệnh DML xác định, hoặc bị thay đổi bởi câu lệnh hoặc nằm trong điều kiện lọc (ví dụ nằm trong mệnh đề WHERE) của câu lệnh.
- Trigger không thể giám sát hành vi của một instead-of trigger khác trên cùng đối tượng, trong khi fine-grained auditing hỗ trợ cho cả table và views.

3. Chính sách trong Fine-grained Auditing

- Chính sách FGA có thể theo dõi việc truy xuất dữ liệu dựa trên nội dung của dữ liệu đó. Sử dụng chính sách, ta có thể chỉ rõ cột nào và điều kiện khi nào ta mới cần phải ghi lại việc truy xuất đó. Ta cũng có thể cung cấp thêm tên hàm mà ta muốn thực thi khi một sự kiện giám sát xảy ra. Hàm đó có thể nhắc nhở hoặc cảnh báo cho người quản trị hay xử lí lỗi và các bất thường.

4. Hàm xử lí sự kiện

- Trong chính sách FGA ta có thể xác định điều kiện khi nào dữ liệu được truy xuất sẽ gây ra một sự kiện giám sát và sử dụng các hàm xử lí sự kiện để nhắc nhở nhà quản trị khi sự kiện đó xảy ra. Ví dụ, một công ty có thể cho phép nhân viên HR truy cập thông tin về lương mà không bị giám sát, nhưng khi số lương được truy xuất lớn hơn $500,000 thì sẽ bị giám sát. Khi có việc đó xảy ra hệ thống sẽ cảnh báo cho nhà quản trị.
- Cơ chế thực hiện cảnh báo đó được thực hiện nhờ vào một hàm, cú pháp như sau:

```
PROCEDURE fname(
   object_schema VARCHAR2,
   object_name VARCHAR2,
   policy_name VARCHAR2)
AS ...
```

Trong đó:

- ✓ *fname*: tên của thủ tục
- ✓ *object_schema:* tên của schema chứa bảng bị giám sát.
- ✓ *object_name*: tên của bảng bị giám sát.
- ✓ *policy_name:* tên của chính sách

5. Hàm và các cột giám sát trong Fine-grained Auditng

- Ta có thể dùng một hàm tự định nghĩa để xác định điều kiện cho chính sách và xác định cột nào cần được giám sát để tinh lọc chính sách giám sát. Ví dụ, hàm đó có thể tạo ra một bản ghi giám sát chỉ khi mức lương lớn hơn $250,000 bị truy cập.
- Chỉ rõ cột giám sát có thể giúp giảm các trường hợp sai cũng như các bản ghi không cần thiết, bởi vì việc giám sát chỉ cần được thực hiện khi một cột cụ thể được tham khảo đến trong câu truy vấn.
- Ta cũng có thể chỉ rõ rằng việc giám sát chỉ xảy ra khi tất cả các cột giám sát đều được tham khảo đến, hoặc chỉ một trong các cột giám sát được tham khảo. Ví dụ, một công ty có thể chỉ mong muốn ghi lại sự truy cập thông tin về lương khi tên của nhân viên cũng bị truy cập, bởi vì nếu chỉ xem thông tin về lương không mà không biết tên người sở hữu số lương đó cũng vô nghĩa.

6. Điều kiện giám sát NULL

- Điều kiện giám sát (audit_condition) là NULL được hiểu là một điều kiện đúng. Dạng điều kiện "1=1" không còn được sử dụng như trong Oracle 9i vì nó không có được kết quả mong muốn một cách đáng tin cậy. NULL sẽ vẫn tạo ra được sự giám sát kể cả khi không có dòng nào được xử lí, do đó tất cả mọi hoạt động trên cột giám sát (audit_column) với chính sách đó đều được ghi lại.
- **Lưu ý**:
  - ✓ Sử dụng chuỗi rỗng không tương đương với giá trị NULL.
  - ✓ Nếu NULL hoặc không có điều kiện giám sát nào được đặc tả, thì bất kì hành động nào tác động lên một bảng được áp dụng chính sách đó đều tạo ra một audit record, dù cho có không có dòng nào được trả về từ câu truy vấn.

II. Gói DBMS_FGA trong Oracle

- Gói DBMS_FGA cung cấp chức năng bảo mật FGA. Để có thể quản lý các chính sách giám sát, ta cần phải có quyền thực thi trên DBMS_FGA (EXECUTE ON DBMS_FGA).

1. Thủ tục ADD_POLICY

- Thủ tục này dùng để tạo ra các chính sách giám sát. Số chính sách giám sát tối đa trên một bảng hoặc view là 256.
- Cú pháp:

```
DBMS_FGA.ADD_POLICY(
    object_schema   VARCHAR2,
    object_name     VARCHAR2,
    policy_name     VARCHAR2,
    audit_condition VARCHAR2,
    audit_column    VARCHAR2,
    handler_schema  VARCHAR2,
    handler_module  VARCHAR2,
    enable          BOOLEAN,
    statement_types VARCHAR2,
    audit_trail     BINARY_INTEGER IN DEFAULT,
    audit_column_opts BINARY_INTEGER IN DEFAULT);
```

- Tham số

Tên	Mô tả	Mặc định
object_schema	Tên của schema chứa đối tượng bị giám sát (Nếu NULL thì hệ thống sẽ lấy schema của user hiện tại)	NULL
object_name	Tên của object bị giám sát.	-
policy_name	Tên của chính sách, tên này phải duy nhất	-
audit_condition	Điều kiện một hàng được giám sát. NULL có nghĩa là hàng nào cũng sẽ bị giám sát.	NULL

Tên	Mô tả	Mặc định
audit_column	Những cột sẽ được kiểm tra mỗi khi truy cập. Chúng có thể bao gồm những cột ẩn. Giá trị mặc định NULL nghĩa là giám sát sẽ xảy ra nếu bất kì cột nào bị truy cập hoặc ảnh hưởng.	NULL
handler_schema	Schema chứa hàm xử lí sự kiện. Mặc định NULL sẽ lấy schema của user hiện tại.	NULL
handler_module	Tên hàm xử lí sự kiện. Hàm này được gọi chỉ sau khi hàng đầu tiên thỏa điều kiện giám sát được xử lí trong câu truy vấn. Nếu hàm này bị lỗi với một ngoại lệ nào đó thì câu lệnh SQL bị giám sát sẽ cũng không thể thực thi được.	NULL
enable	Giá trị này bằng TRUE có nghĩa là chính sách này được kích hoạt.	TRUE
statement_types	Kiểu câu lệnh SQL mà chính sách này áp dụng vào: INSERT, UPDATE, DELETE, hay chỉ là SELECT.	SELECT
audit_trail	Nơi ghi lại các bản ghi giám sát.	DB+EXTENDED
audit_column_opts	Câu lệnh bị giám sát khi câu truy vấn tham khảo tới một trong những cột được chỉ ra trong tham số audit_column (ANY_COLUMNS) hay phải tham khảo tới tất cả các cột được chỉ ra trong đó (ALL_COLUMNS).	ANY_COLUMNS

- Chú ý về tham số !audit_trail:
  - ✓ audit_trail => DBMS_FGA.DB : bản ghi giám sát sẽ được ghi vào bảng SYS.FGA_LOG$ của cơ sở dữ liệu, ngoại trừ cột SQL Text và SQL Bind.
  - ✓ audit_trail => DBMS_FGA.DB+EXTENDED : bản ghi giám sát sẽ được ghi vào bảng SYS.FGA_LOG$ của cơ sở dữ liệu và lưu thêm hai cột SQL Text và SQL Bind.
  - ✓ audit_trail => DBMS_FGA.XML: bản ghi giám sát sẽ được ghi vào file

XML, file này được lưu trong hệ điều hành và không chứa hai cột SQL Text và SQL Bind.

- ✓ audit_trail => DBMS_FGA.XML+EXTENDED: bản ghi giám sát sẽ được ghi vào file XML, file này được lưu trong hệ điều hành và chứa hai cột SQL Text và SQL Bind.
- ✓ Các thông số của audit_trail nằm trong view ALL_AUDIT_POLICIES.

2. Thủ tục DISABLE_POLICY

- Thủ tục này để tắt một chính sách giám sát.
- Cú pháp

```
DBMS_FGA.DISABLE_POLICY(
    object_schema   VARCHAR2,
    object_name     VARCHAR2,
    policy_name     VARCHAR2 );
```

- Tham số

Tên	Mô tả
object_schema	Tên của schema chứa đối tượng bị giám sát.
object_name	Tên của đối tượng bị giám sát.
policy_name	Tên của chính sách.

3. Thủ tục ENABLE_POLICY

- Thủ tục này cho phép kích hoạt một chính sách giám sát.
- Cú pháp

```
DBMS_FGA.ENABLE_POLICY(
    object_schema   VARCHAR2,
    object_name     VARCHAR2,
    policy_name     VARCHAR2,
    enable          BOOLEAN);
```

- Tham số

Tên	Mô tả
object_schema	Tên của schema chứa đối tượng bị giám sát.
object_name	Tên của đối tượng bị giám sát.
policy_name	Tên của chính sách.
enable	Giá trị mặc định là TRUE để kích hoạt chính sách.

4. Thủ tục DROP_POLICY

- Thủ tục này để xoá bỏ một chính sách giám sát.
- Cú pháp

```
DBMS_FGA.DROP_POLICY(
   object_schema   VARCHAR2,
   object_name     VARCHAR2,
   policy_name     VARCHAR2 );
```

- Tham số

Tên	Mô tả
object_schema	Tên của schema chứa đối tượng bị giám sát.
object_name	Tên của đối tượng bị giám sát.
policy_name	Tên của chính sách.

III. Thực hành

- Tạo user audit_admin để quản lý chính sách. Kết nối bằng tài khoản SYS để cấp quyền thực thi trên gói DBMS_FGA và các quyền cần thiết:

```
CREATE USER audit_admin IDENTIFIED BY auditadmin
QUOTA 500M ON USERS;

GRANT CREATE SESSION TO audit_admin;
GRANT EXECUTE ON DBMS_FGA TO audit_admin;
GRANT SELECT ON DBA_FGA_AUDIT_TRAIL TO audit_admin;
```

```
GRANT SELECT, INSERT, UPDATE, DELETE ON hr.employees TO
audit_admin;
GRANT CREATE TABLE, CREATE PROCEDURE TO audit_admin;
```

- Giám sát tất cả các câu lệnh (INSERT , UPDATE, DELETE, SELECT) trên bảng EMPLOYEES thuộc schema HR để theo dõi những câu truy vấn mà truy cập đến cột lương của nhân viên thuộc phòng ban có id bằng 80.

```
conn audit_admin/auditadmin;
BEGIN
     DBMS_FGA.ADD_POLICY(
       object_schema   => 'HR',
       object_name     => 'EMPLOYEES',
       policy_name     => 'CHK_HR_EMP',
       audit_condition => 'DEPARTMENT_ID = 80',
       audit_column    => 'SALARY',
       statement_types => 'INSERT,UPDATE,DELETE,SELECT',
       audit_trail     => DBMS_FGA.DB+DBMS_FGA.EXTENDED);
END;
/
```

- Những câu lệnh sau sẽ gây ra giám sát:

```
SELECT salary FROM hr.employees
WHERE department_id = 80;

SELECT * FROM hr.employees
WHERE department_id = 80;

SELECT count(*) FROM hr.employees
WHERE department_id = 80 and salary > 10000;
```

- Câu lệnh sau không gây ra giám sát:

```
SELECT count(*) FROM hr.employees
```

```
WHERE department_id = 80;

SELECT * FROM hr.employees
WHERE first_name = 'Steven' and last_name = 'King';
```

- Kiểm tra kết quả giám sát:

```
conn audit_admin/auditadmin;
SELECT * FROM DBA_FGA_AUDIT_TRAIL;
```

- Hủy bỏ chính sách này ta dùng thủ tục DROP_POLICY:

```
conn audit_admin/auditadmin;
BEGIN
     DBMS_FGA.DROP_POLICY(
     object_schema     => 'HR',
     object_name       => 'EMPLOYEES',
     policy_name       => 'CHK_HR_EMP');
END;
/
```

- Xoá tất cả các bản ghi giám sát của FGA:

```
CONN SYS/ AS SYSDBA
DELETE FROM FGA_LOG$;
COMMIT;
```

- Ta bổ sung thêm vào chính sách yêu cầu mỗi khi sự kiện giám sát xảy ra thì hệ thống sẽ ghi một bản ghi giám sát vào một bảng phụ. Với yêu cầu đó, ta cần tạo một bảng để lưu kết quả giám sát và một hàm xử lí sự kiện như dưới đây:

```
conn audit_admin/auditadmin;
CREATE TABLE fga_tab (
schema_name  VARCHAR2(30),
table_name  VARCHAR2(30),
policy_name VARCHAR2(30));
```

```
CREATE OR REPLACE PROCEDURE fga_handler (sname VARCHAR2,
tname VARCHAR2, pname VARCHAR2)
AS
PRAGMA AUTONOMOUS_TRANSACTION;
BEGIN
  INSERT INTO fga_tab VALUES (sname, tname, pname);
  COMMIT;
END fga_handler;
/
```

- Tạo chính sách với hàm xử lý sự kiện trên:

```
conn audit_admin/auditadmin;
BEGIN
   DBMS_FGA.ADD_POLICY(
      object_schema     => 'HR',
      object_name       => 'EMPLOYEES',
      policy_name       => 'CHK_HR_EMP',
      audit_condition   => 'DEPARTMENT_ID = 80',
      audit_column      => 'salary,first_name,last_name',
      handler_schema    => 'audit_admin',
      handler_module    => 'fga_handler',
      enable            =>  FALSE,
      statement_types   => 'INSERT,UPDATE,SELECT,DELETE',
      audit_trail       => DBMS_FGA.DB+DBMS_FGA.EXTENDED,
      audit_column_opts => DBMS_FGA.ALL_COLUMNS);
END;
/
```

- Lúc tạo chính sách ta đã tắt chính sách đó bằng tham số:

```
enable  =>  FALSE
```

- Vì vậy sau này khi nào ta muốn kích hoạt chính sách đó ta có thể dùng thủ tục ENABLE _POLICY

```
conn audit_admin/auditadmin;
```

```
BEGIN
DBMS_FGA.ENABLE_POLICY(
     object_schema     => 'HR',
     object_name       => 'EMPLOYEES',
     policy_name       => 'CHK_HR_EMP',
     enable            => TRUE);
END;
/
```

- Thực hiện một số câu lệnh SELECT:

```
SELECT salary
FROM hr.employees
WHERE department_id = 80;

SELECT *
FROM hr.employees
WHERE salary >10000;

SELECT first_name, last_name, salary, department_id
FROM hr.employees
WHERE salary > 10000;
```

- Kiểm tra kết quả giám sát:

```
conn audit_admin/auditadmin;
SELECT * FROM DBA_FGA_AUDIT_TRAIL;
SELECT * FROM fga_tab;
```

IV. BÀI TẬP

1. Tạo bảng ACCOUNTS thuộc schema của user ACCMASTER

ACCNO	ACCNAME	BAL
1	Alex	10000
2	Bill	15000
3	Charlie	20000
4	David	25000

2. Hiện thực chính sách: giám sát khi một user nào đó truy xuất vào bảng ACCOUNTS và xem số dư lớn hơn hoặc bằng 20000.

3. Giả sử ta có chính sách:

```
1  begin
2       dbms_fga.add_policy (
3          object_schema   => 'ACCMASTER',
4          object_name     => 'ACCOUNTS',
5          policy_name     => 'ACC_MAXBAL',
6          audit_column    => 'ACCNO, BAL',
7          audit_condition => 'BAL >= 20000',
8          handler_schema  => 'ACCMASTER',
9          handler_module  => 'FGA_SEND_MAIL'
10        audit_column_opts => dbms_fga.all_columns
11      );
12 end;
```

Câu lệnh nào sau đây gây ra giám sát:

a. `select * from accounts;`

b. `select accname from accounts where bal > 20000;`

c.
```
select accname from accounts
where bal > 20000 and accno >= 3;
```

d.
```
select accname from accounts
where bal > 20000 and accno < 3;
```