2

Auditing DML Statements

Objectives

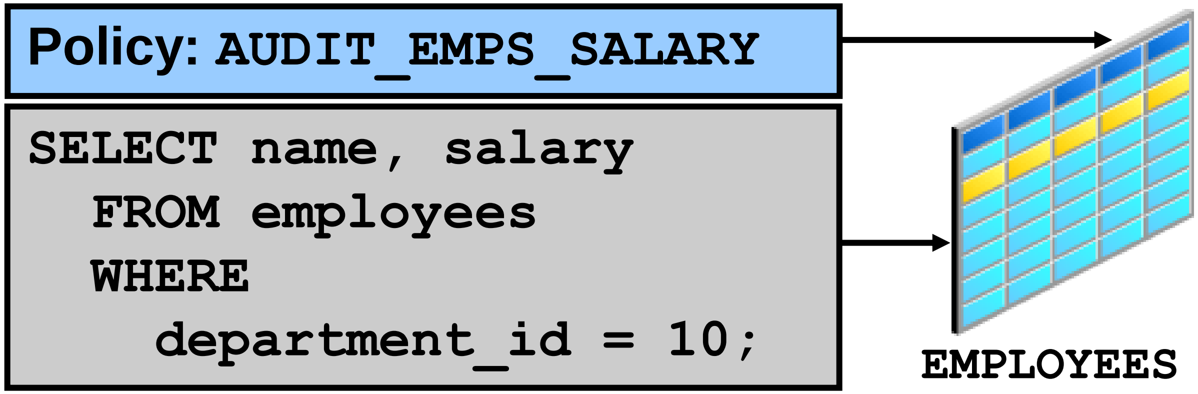
After completing this lesson, you should be able to do the following:

- Implement fine-grained auditing (FGA)
- Maintain FGA policies
- Implement an FGA audit event handler
- Read FGA audit events from the FGA audit trail

Fine-Grained Auditing (FGA)

Policies:

- Monitor data access based on content
- Audit SELECT, INSERT, UPDATE, or DELETE
- Are created on tables or views
- May fire an event handler procedure
- Are administered with the DBMS_FGA package



Policy: AUDIT_EMPS_SALARY

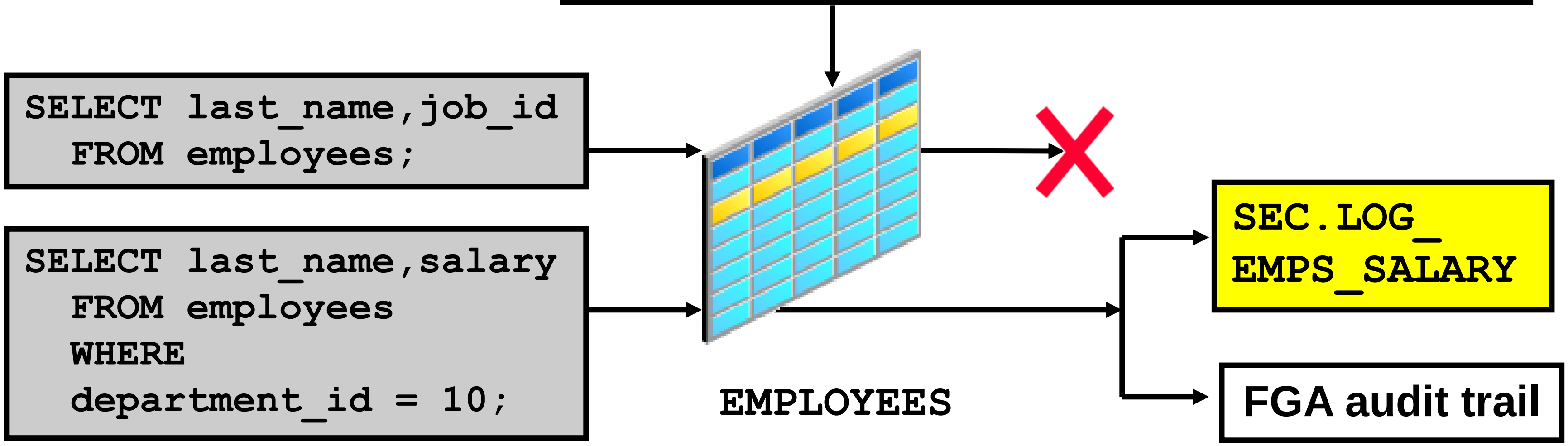
```
SELECT name, salary
  FROM employees
  WHERE
    department_id = 10;
```

FGA Policy

Defines:

- Audit criteria
- Audit action

```
dbms_fga.add_policy (
  object_schema  => 'hr',
  object_name    => 'employees',
  policy_name    => 'audit_emps_salary',
  audit_condition=> 'department_id=10',
  audit_column   => 'salary',
  handler_schema => 'sec',
  handler_module => 'log_emps_salary',
  enable         => TRUE,
  statement_types=> 'select' );
```



```
SELECT last_name,job_id
  FROM employees;
```

```
SELECT last_name,salary
  FROM employees
  WHERE
  department_id = 10;
```

Triggering Audit Events

- The following SQL statements cause an audit event:

```
SELECT count(*)
  FROM hr.employees
  WHERE department_id = 10
    AND salary > &v_salary;
```

```
SELECT salary
  FROM hr.employees;
```

- The following statement does not cause an audit event:

```
SELECT last_name
  FROM hr.employees
  WHERE department_id = 10;
```

Data Dictionary Views

View Name	Description
DBA_FGA_AUDIT_TRAIL	All FGA events
ALL_AUDIT_POLICIES	All FGA policies for objects that the current user can access
DBA_AUDIT_POLICIES	All FGA policies in the database
USER_AUDIT_POLICIES	All FGA policies for objects in the current user schema

DBA_FGA_AUDIT_TRAIL

```
SQL> SELECT to_char(timestamp, 'YYMMDDHH24MI')
  2            AS timestamp,
  3     db_user,
  4     policy_name,
  5     sql_bind,
  6     sql_text
  7   FROM dba_fga_audit_trail;

TIMESTAMP  DB_USER POLICY_NAME       SQL_BIND
---------- ------- ----------------- ----------
SQL_TEXT
-----------------------------------------------
0808272222 HR      AUDIT_EMPS_SALARY   #1(4):1000
SELECT COUNT(*) FROM HR.EMPLOYEES WHERE
DEPARTMENT_ID = 10 AND SALARY > :B1

0808272222 HR      AUDIT_EMPS_SALARY
SELECT salary
FROM hr.employees
```

Quiz

Which of the following types of auditing must you implement to audit the access of a specific column?

a. SQL statement auditing
b. Object privilege auditing
c. Fine-grained auditing

`DBMS_FGA` Package

- Use `DBMS_FGA` to maintain FGA policies.
- Grant the `EXECUTE` privilege only to administrators.
- The `DBMS_FGA` package includes the following subprograms:

Subprogram	Description
`ADD_POLICY`	Creates an audit policy by using the supplied predicate as the audit condition
`DROP_POLICY`	Drops an audit policy
`ENABLE_POLICY`	Enables an audit policy
`DISABLE_POLICY`	Disables an audit policy

Enabling and Disabling an FGA Policy

- Enable a policy:

```
dbms_fga.enable_policy (
  object_schema => 'hr',
  object_name   => 'employees',
  policy_name   => 'audit_emps_salary' );
```

- Disable a policy:

```
dbms_fga.disable_policy (
  object_schema => 'hr',
  object_name   => 'employees',
  policy_name   => 'audit_emps_salary' );
```

Dropping an FGA Policy

```
BEGIN
dbms_fga.drop_policy (
  object_schema => 'hr',
  object_name   => 'employees',
  policy_name   => 'audit_emps_salary');
END;
```

FGA Policy Guidelines

Setting policy parameters

- Audit conditions
  - To audit all statements, use a `NULL` or `TRUE` condition.
  - If the audit condition syntax is invalid, an `ORA-28112` error is raised when the audited object is accessed.
- Audit columns
  - If audit column is set to `NULL`, all columns are audited.
  - If the audit column name is valid but incorrect, the wrong statements are audited.

FGA Policy Errors

- Policy creation errors occur when:
  - The audited table or view does not exist
  - The policy already exists; error `ORA-28101` is raised
  - The audit column does not exist
- Audited SQL statements fail when:
  - The audit condition is invalid
  - The event handler does not exist or is invalid

Maintaining the Audit Trail

Maintaining the audit trail must include:

- Reviewing and storing old records
- Preventing storage problems
- Avoiding loss of records

Summary

In this lesson, you should have learned how to:

- Implement FGA
- Maintain FGA policies
- Implement an FGA audit event handler
- Read FGA audit events from the FGA audit trail