Auditing the Oracle Database

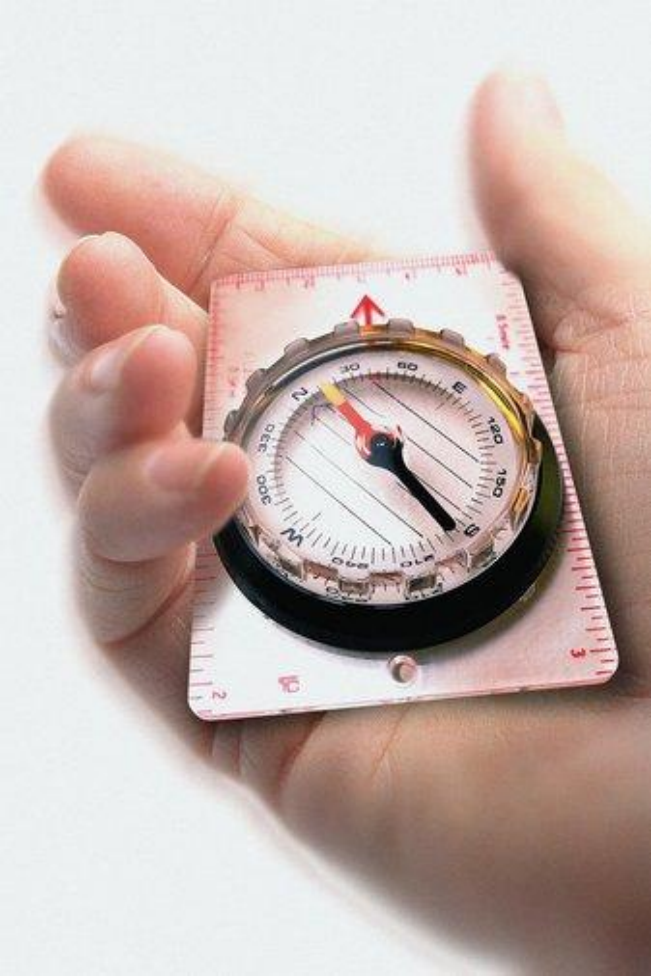
The International Institute of SUPINFO Information Technology

www.supinfo.com

SUPINFO Official SOC Curriculum

Course objectives

By completing this course, you will:



- **Audit database activity**

Course topics

Course's plan:

- Monitoring for Suspicious Activity
- Standard Database Auditing
- Value-based Auditing
- Fine-Grained Auditing (FGA)
- Labs

Monitoring for Suspicious Activity

Introduction

- You will have to accept that users have privileges that could be dangerous. All you can do is monitor their use of those privileges and track what they are actually doing with them.
- Oracle provides several auditing techniques:
  - SYSDBA auditing to audit all SYSDBA activity
  - Database auditing
  - Value-based auditing
  - Fine-grained auditing

Introduction

Auditing of any type increases the amount of work that the database must do. In order to limit this workload, you should focus your auditing closely and not track events of minimal significance.

Audit Tool Comparisons

Type of Audit	What is Audited?	What is in the Audit Trail?
Standard database auditing	Privileges used including objects access	Fixed set of data
Value-based auditing	Data changed by DML statements	Administrator defined
Fine-Grained auditing (FGA)	SQL statements (insert, update, delete, and select) based on content	Fixed set of data including the SQL statement

Auditing SYSDBA Activity

- The **AUDIT_SYS_OPERATIONS** instance parameter must be set to **TRUE** (default is **FALSE**).
- As users with **SYSDBA** or **SYSOPER** privileges can be connected with the database closed, audit trail must be stored outside of the database.
- Every statement issued by a user connected **AS SYSDBA** or **AS SYSOPER** is written out to the operating system's audit trail:
  - Windows: Windows Application Log
  - Unix: controlled by **AUDIT_FILE_DEST** parameter, by default: **$ORACLE_HOME/rdbms/audit**

Auditing `SYSDBA` Activity

- The DBA must not have access to the audit records, either there would be no point in creating them.
- As a result of fact, system administrator must not have access to **`SYSDBA`** privileges.
- On Unix, this parameter should point to a directory on which Oracle owner has write permission but the Unix ID used by the DBA does not.

Part 1 Stop-and-think

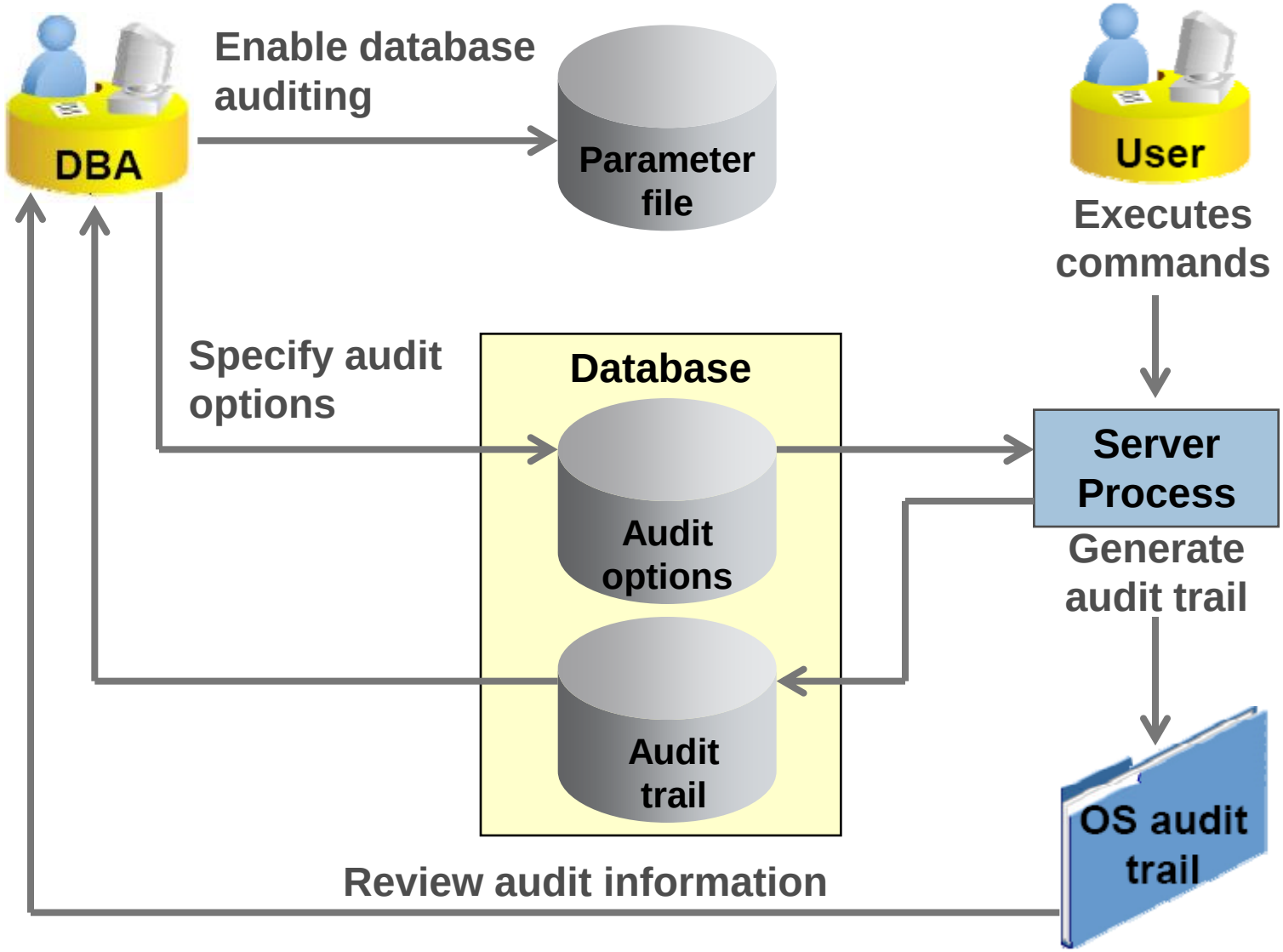
Do you have any questions ?

Standard Database Auditing

`AUDIT_TRAIL` parameter

- Enabled through the **`AUDIT_TRAIL`** parameter
  - **`NONE`**: Disables collection of audit records
  - **`DB`**: Enables auditing with records stored in the database, in a data dictionary table
  - **`OS`**: Enables auditing with records stored in the operating system audit trail
- Can audit:
  - Login events
  - Exercise of system privileges
  - Exercise of object privileges
  - Use of SQL statements

Audit process



Specifying Audit Options

- SQL statement auditing

```
AUDIT table;
```

- System privilege auditing (nonfocused and focused)

```
AUDIT select any table, create any trigger;
AUDIT select any table BY hr BY SESSION;
```

- Object privilege auditing (nonfocused and focused)

```
AUDIT ALL ON hr.employees;
AUDIT UPDATE, DELETE ON hr.employees BY ACCESS;
```

- Session auditing

```
AUDIT session whenever not successful;
```

Viewing Auditing Options

Data Dictionary View	Description
ALL_DEF_AUDIT_OPTS	Default Audit Options
DBA_STMT_AUDIT_OPTS	Statement Auditing Options
DBA_PRIV_AUDIT_OPTS	Privilege Auditing Options
DBA_OBJ_AUDIT_OPTS	Schema Object Auditing Options

Viewing Auditing Results

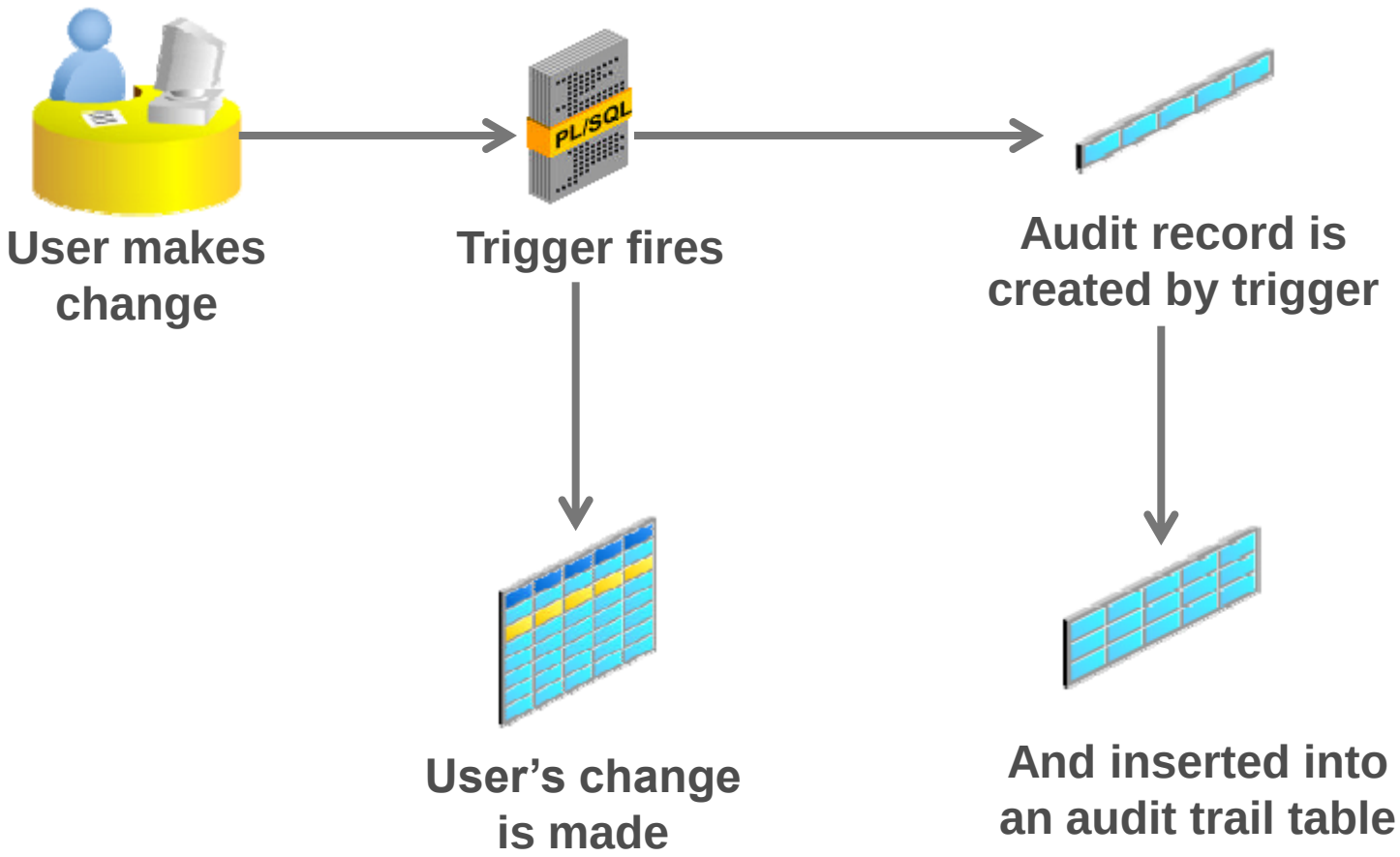
Audit Trail View	Description
DBA_AUDIT_TRAIL	All audit trail entries
DBA_AUDIT_EXISTS	Records for AUDIT EXISTS/NOT EXISTS
DBA_AUDIT_OBJECT	Records concerning schema objects
DBA_AUDIT_STATEMENT	Statement auditing records

Part 2 Stop-and-think

Do you have any questions ?

Value-Based Auditing

Introduction



Trigger creation

```
CREATE OR REPLACE TRIGGER system.creditrating_audit
AFTER UPDATE OF creditrating
ON oe.customers
REFERENCING NEW AS NEW OLD AS OLD
FOR EACH ROW
BEGIN
IF :old.creditrating != :new.creditrating THEN
   INSERT INTO system.creditrating_audit
   VALUES (sys_context('userenv','os_user'),
       SYSDATE, sys_context('userenv','ip_address'),
       :new.cust_id ||' credit rating changed from
       '||:old.creditrating||
       ' to '||:new.creditrating);
END IF;
END;
/
```

Tip

Auditing through triggers is a much slower process than database auditing, but it does give you more information.

Part 3 Stop-and-think

Do you have any questions ?

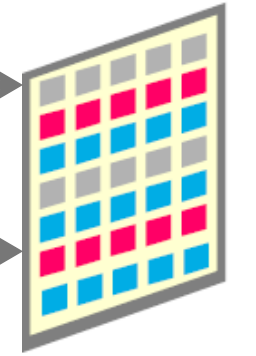
Fine-Grained Auditing (FGA)

Introduction

- Monitors data access based on content
- Audits **SELECT** or **INSERT**, **UPDATE**, **DELETE**
- Can be linked to a table or view
- May fire a procedure
- Is administered with the **DBMS_FGA** package

Policy: **AUDIT_EMPS_SALARY**

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



employees

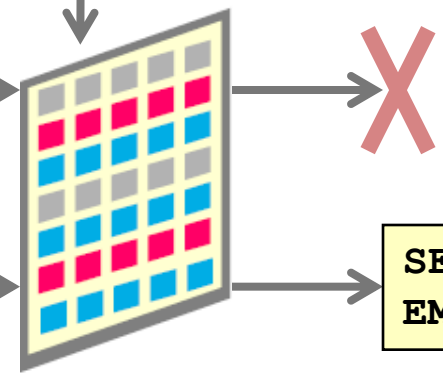
FGA Policy

- Defines:
  - Audit criteria
  - Audit action
- Is created with: **DBMS_FGA .ADD_POLICY**

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

```
SELECT name, job_id
FROM   employees;
```

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



employees

SECURE.LOG_ EMPS_SALARY

DBMS_FGA Package

Subprogram	Description
ADD_POLICY	Creates an audit policy 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

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

```
PL/SQL procedure successfully completed.
```

Triggering Audit Events

- The following SQL statements cause an audit:

```
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:

```
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 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

```
SELECT to_char(timestamp, 'YYMMDDHH24MI')
            AS timestamp,
       db_user, policy_name, sql_bind, sql_text
FROM   dba_fga_audit_trail;
```

TIMESTAMP	DB_USER	POLICY_NAME	SQL_BIND	SQL_TEXT
201221740	SYSTEM	AUDIT_EMPS_SALARY	#1(4):1000	SELECT count(*) FROM hr.employees WHERE department_id = 10 AND salary > :b1

FGA Guidelines

- To audit all statements, use a null condition.
- If you try to add a policy that already exists, error **`ORA-28101`** is raised.
- The audited table or view must already exist when you create the policy.
- If the audit condition syntax is invalid, an **`ORA-28112`** is raised when the audited object is accessed.
- If the audit column does not exist in the table, no rows are audited.
- If the event handler does not exist, no error is returned and the audit records is still created.

Part 4 Stop-and-think

Do you have any questions ?

Summary

Monitoring for Suspicious Activity

Fine-Grained Auditing (FGA)

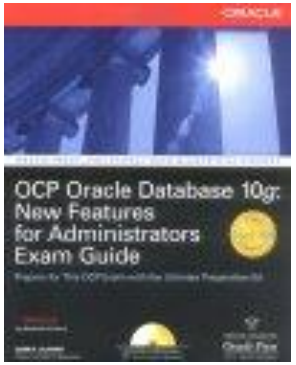
Standard Database Auditing

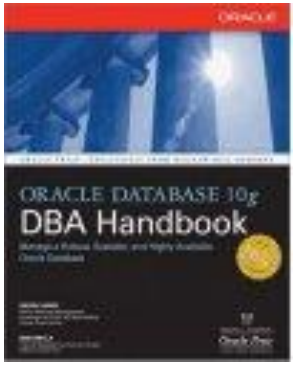
Value-based Auditing

For more

If you want to go into these subjects more deeply, …

Publications





http://www.oracle.../bookstore/

Courses

Cursus: Merise & SQL

Cursus: PL/SQL

Cursus: DBA1 & DBA2

Cursus: DWH, OAS & BIS

Web sites

http://www.labo-oracle.com

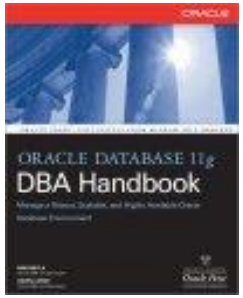
http://www.oracle.com

http://otn.oracle.com

Certifications

1Z0-042

1Z0-043



THE INTERNATIONAL INSTITUTE OF

SUPINFO

INFORMATION TECHNOLOGY

Congratulations

You have successfully completed
the SUPINFO course n°14

Oracle Technologies
Auditing the Oracle Database

The end


The International Institute of
SUPINFO
Information Technology