11

Implementing Oracle Database Auditing

Objectives

After completing this lesson, you should be able to:

- Describe DBA responsibilities for security and auditing
- Enable standard database auditing
- Specify audit options
- Review audit information
- Maintain the audit trail

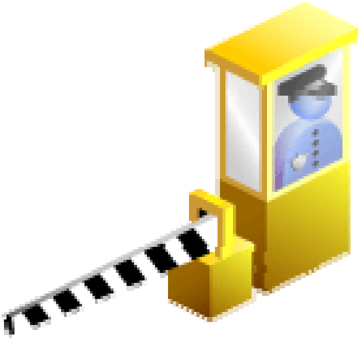
Separation of Responsibilities

- Users with DBA privileges must be trusted.
  - Abuse of trust
  - Audit trails protecting the trusted position
- DBA responsibilities must be shared.
- Accounts must never be shared.
- The DBA and the system administrator must be different people.
- Separate operator and DBA responsibilities.

Database Security

A secure system ensures the confidentiality of the data that it contains. There are several aspects of security:

- Restricting access to data and services
- Authenticating users
- Monitoring for suspicious activity



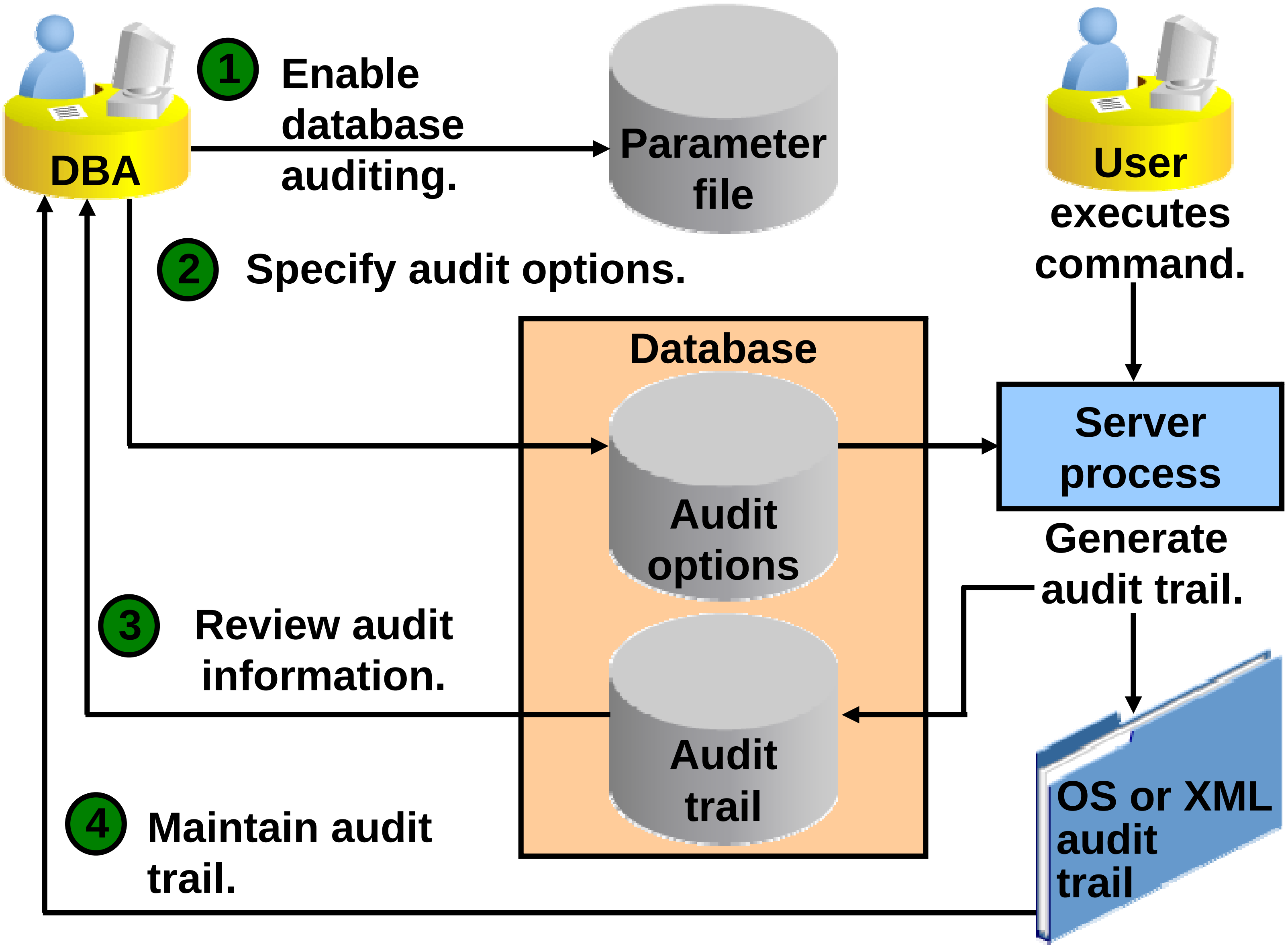
Monitoring for Compliance

Monitoring or auditing must be an integral part of your security procedures.

Review the following:

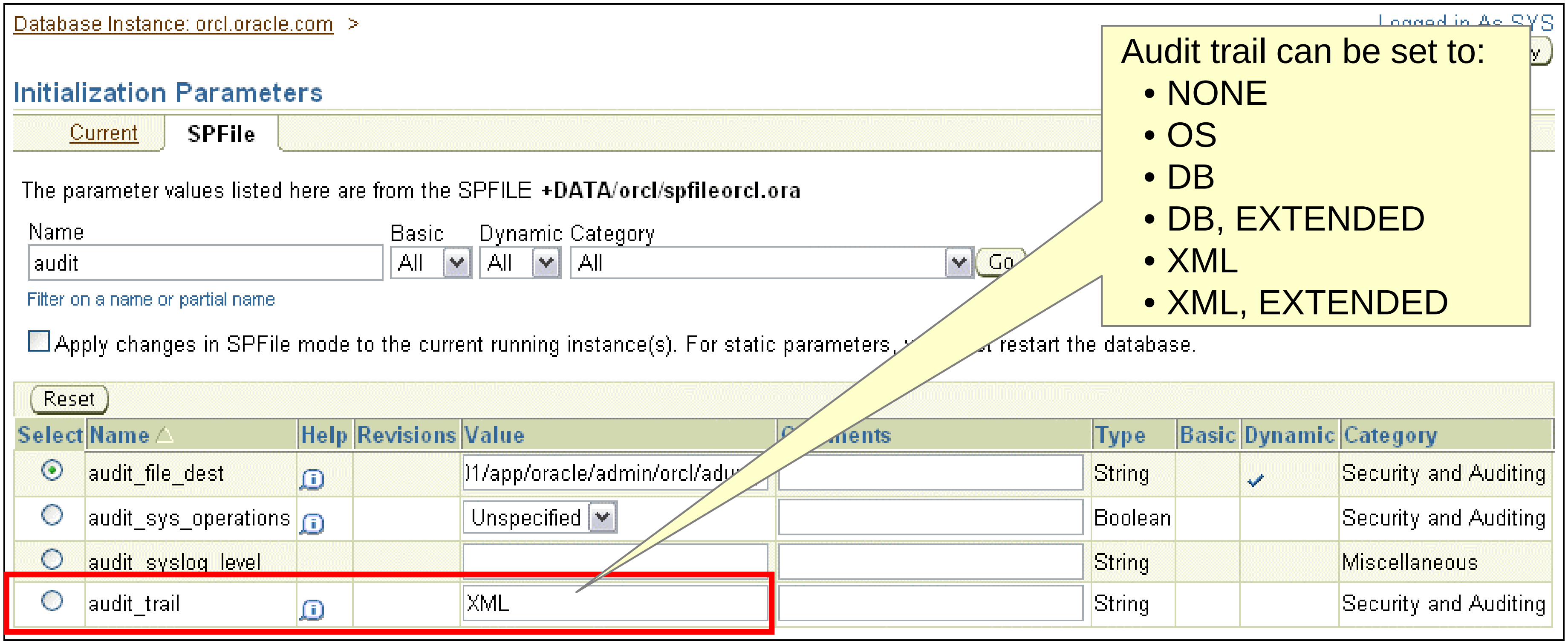
- Mandatory auditing
- Standard database auditing
- Value-based auditing
- Fine-grained auditing (FGA)
- SYSDBA (and SYSOPER) auditing

Standard Database Auditing



Configuring the Audit Trail

Use `AUDIT_TRAIL` to enable database auditing.



Database Instance: orcl.oracle.com >

Logged in As SYS

Initialization Parameters

The parameter values listed here are from the SPFILE **+DATA/orcl/spfileorcl.ora**

Name	Basic	Dynamic	Category
audit	All	All	All

Filter on a name or partial name

□ Apply changes in SPFile mode to the current running instance(s). For static parameters, t restart the database.

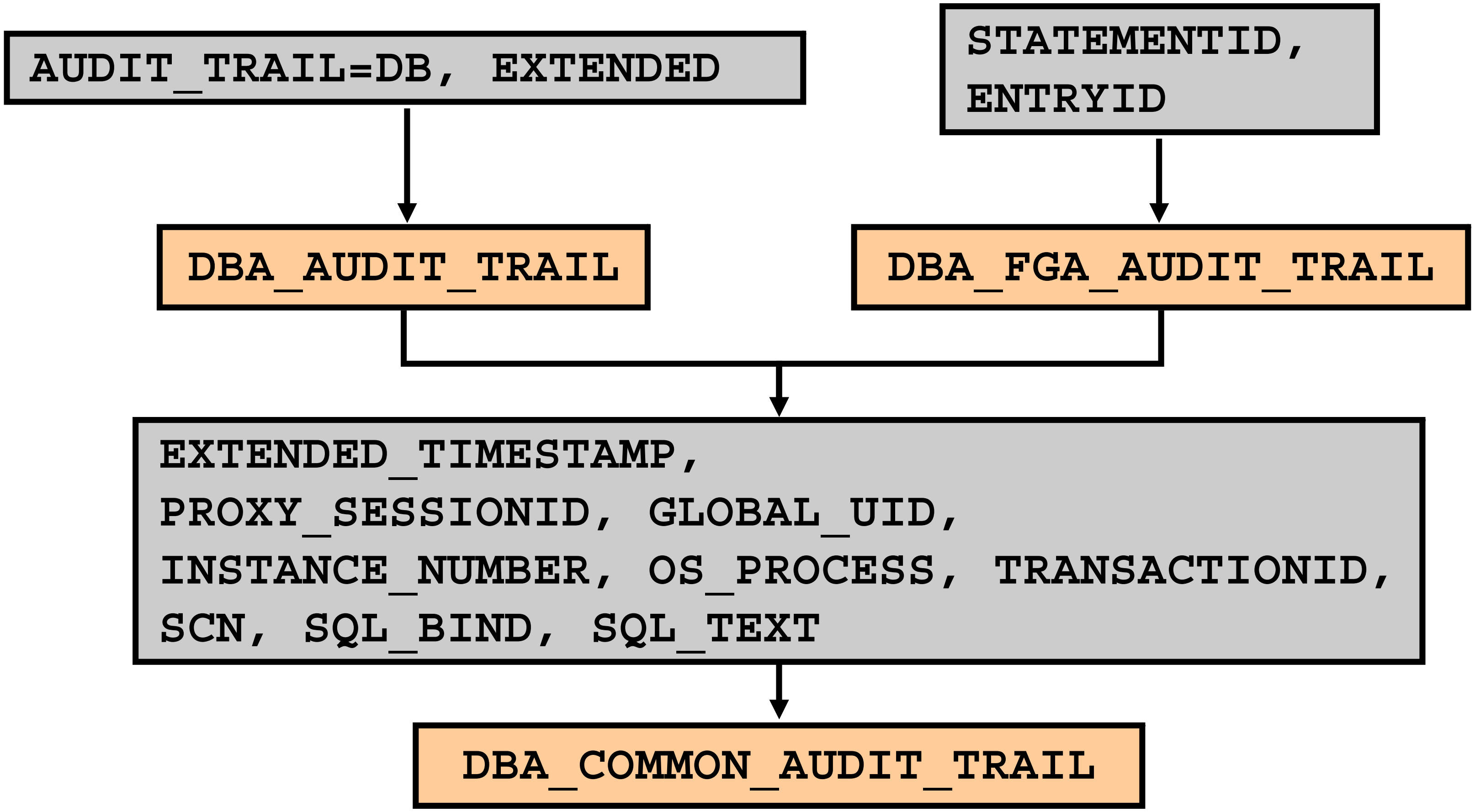
Select	Name △	Help	Revisions	Value	Comments	Type	Basic	Dynamic	Category
●	audit_file_dest	ⓘ		)1/app/oracle/admin/orcl/adu		String		✓	Security and Auditing
○	audit_sys_operations	ⓘ		Unspecified		Boolean			Security and Auditing
○	audit_syslog_level					String			Miscellaneous
○	audit_trail	ⓘ		XML		String			Security and Auditing

Audit trail can be set to:
- NONE
- OS
- DB
- DB, EXTENDED
- XML
- XML, EXTENDED

```
ALTER SYSTEM SET AUDIT_TRAIL='XML' SCOPE=SPFILE;
```

Restart database after modifying this static initialization parameter.

Uniform Audit Trails



AUDIT_TRAIL=DB, EXTENDED

STATEMENTID, ENTRYID

DBA_AUDIT_TRAIL

DBA_FGA_AUDIT_TRAIL

EXTENDED_TIMESTAMP, PROXY_SESSIONID, GLOBAL_UID, INSTANCE_NUMBER, OS_PROCESS, TRANSACTIONID, SCN, SQL_BIND, SQL_TEXT

DBA_COMMON_AUDIT_TRAIL

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):

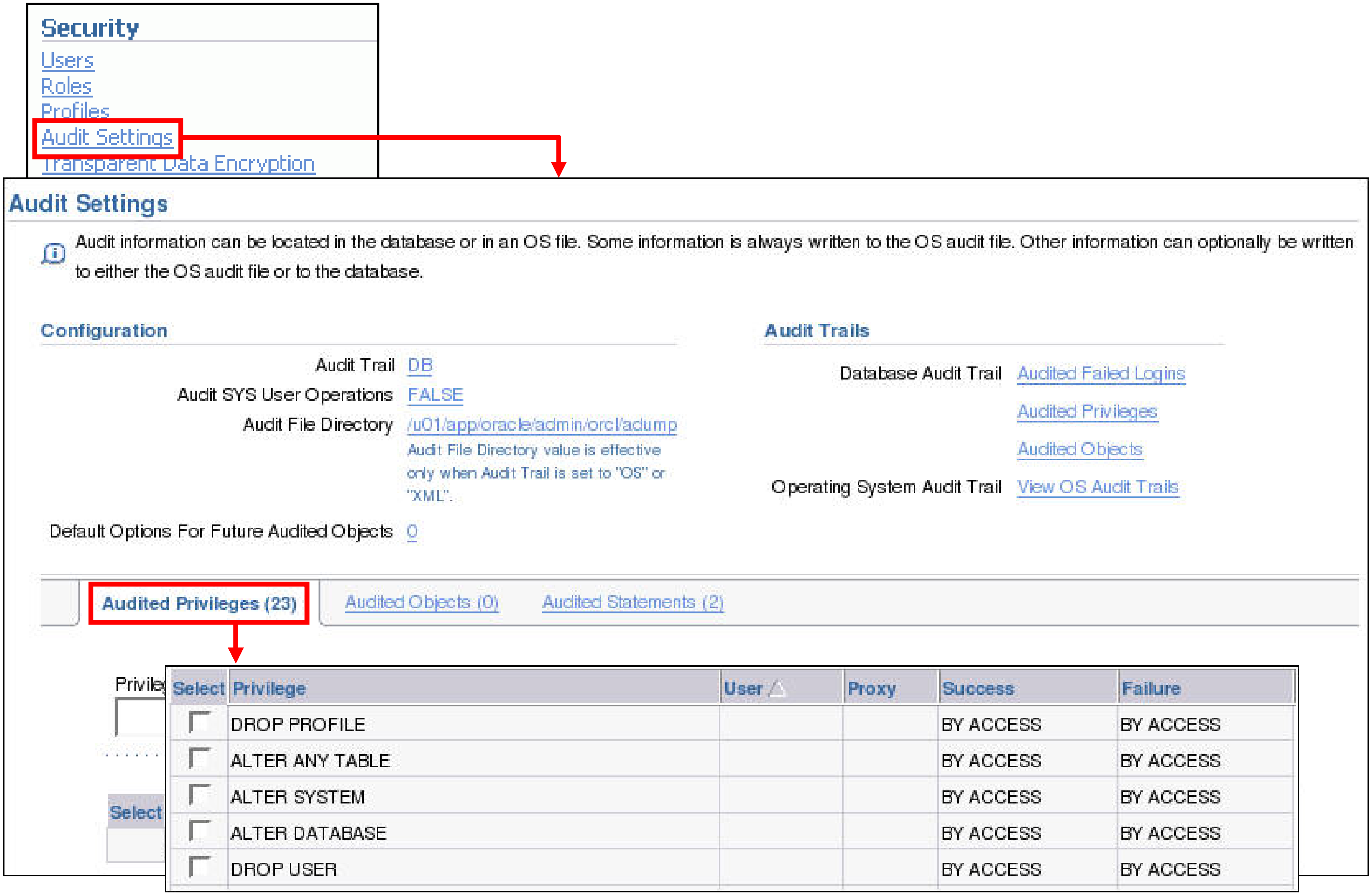
```
AUDIT ALL on hr.employees;
AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

Default Auditing

Privileges Audited by Default
ALTER ANY PROCEDURE
ALTER ANY TABLE
ALTER DATABASE
ALTER PROFILE
ALTER SYSTEM
ALTER USER
AUDIT SYSTEM
CREATE ANY JOB
CREATE ANY LIBRARY
CREATE ANY PROCEDURE
CREATE ANY TABLE
CREATE EXTERNAL JOB
CREATE PUBLIC DATABASE LINK
CREATE SESSION
CREATE USER
GRANT ANY OBJECT PRIVILEGE
GRANT ANY PRIVILEGE
GRANT ANY ROLE
DROP ANY PROCEDURE
DROP ANY TABLE
DROP PROFILE
DROP USER
EXEMPT ACCESS POLICY

Statements Audited by Default
SYSTEM AUDIT BY ACCESS
ROLE BY ACCESS

Enterprise Manager Audit Page



Audit Settings

Audit information can be located in the database or in an OS file. Some information is always written to the OS audit file. Other information can optionally be written to either the OS audit file or to the database.

Configuration

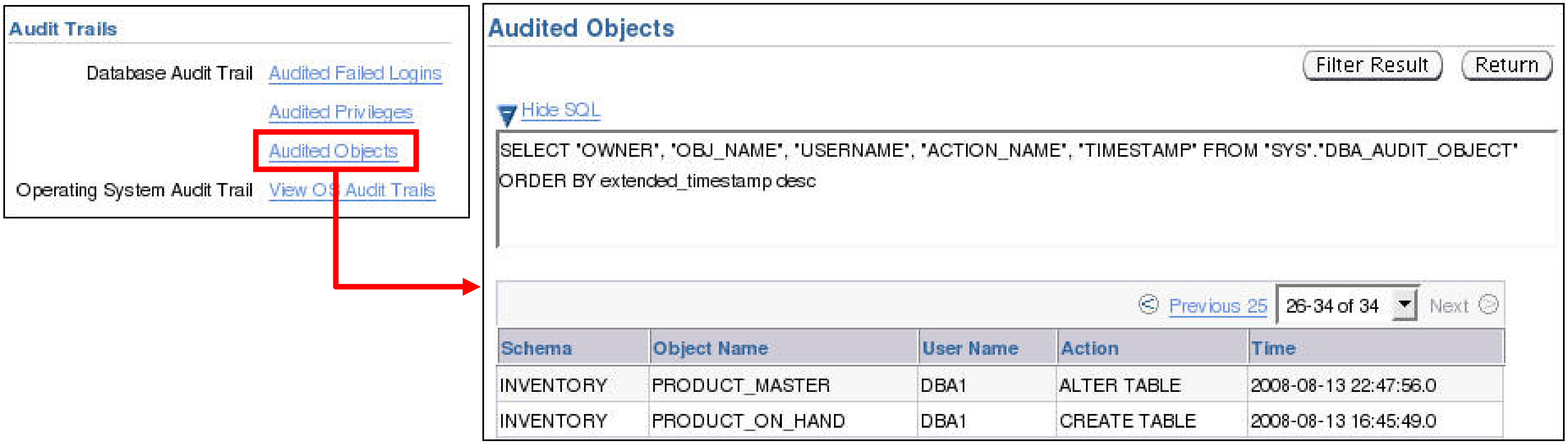
Audit Trail	DB
Audit SYS User Operations	FALSE
Audit File Directory	/u01/app/oracle/admin/orcl/adump Audit File Directory value is effective only when Audit Trail is set to "OS" or "XML".
Default Options For Future Audited Objects	0

Audit Trails

Database Audit Trail	Audited Failed Logins Audited Privileges Audited Objects
Operating System Audit Trail	View OS Audit Trails

Select	Privilege	User △	Proxy	Success	Failure
□	DROP PROFILE			BY ACCESS	BY ACCESS
□	ALTER ANY TABLE			BY ACCESS	BY ACCESS
□	ALTER SYSTEM			BY ACCESS	BY ACCESS
□	ALTER DATABASE			BY ACCESS	BY ACCESS
□	DROP USER			BY ACCESS	BY ACCESS

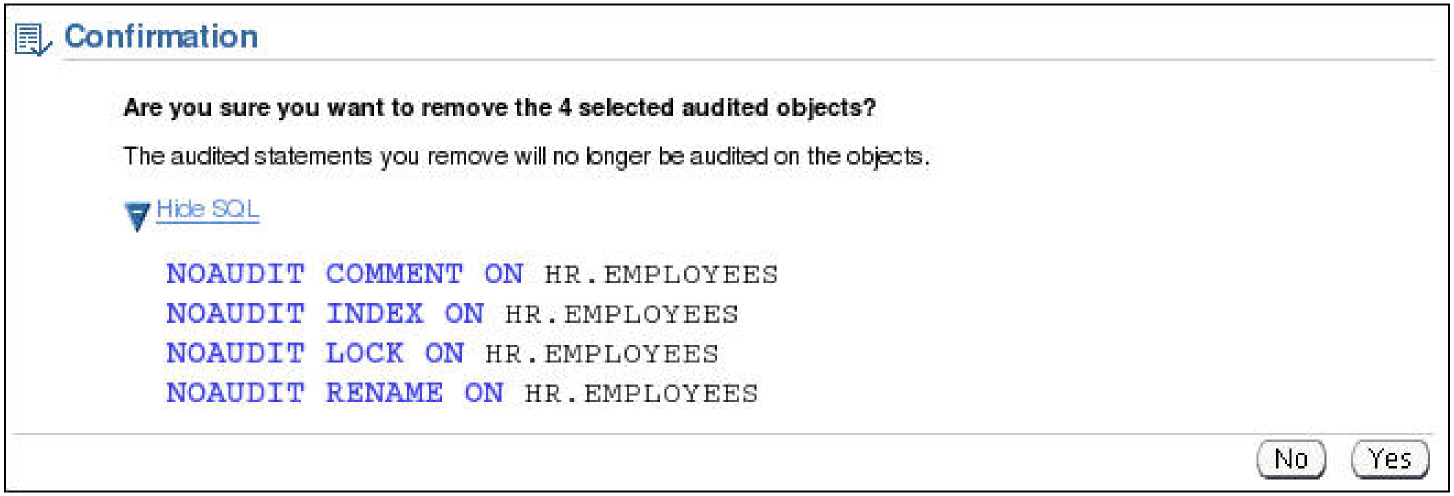
Using and Maintaining Audit Information



```
SELECT 'OWNER', 'OBJ_NAME', 'USERNAME', 'ACTION_NAME', 'TIMESTAMP' FROM 'SYS'.'DBA_AUDIT_OBJECT'
ORDER BY extended_timestamp desc
```

Schema	Object Name	User Name	Action	Time
INVENTORY	PRODUCT_MASTER	DBA1	ALTER TABLE	2008-08-13 22:47:56.0
INVENTORY	PRODUCT_ON_HAND	DBA1	CREATE TABLE	2008-08-13 16:45:49.0

Disable audit options if you are not using them.

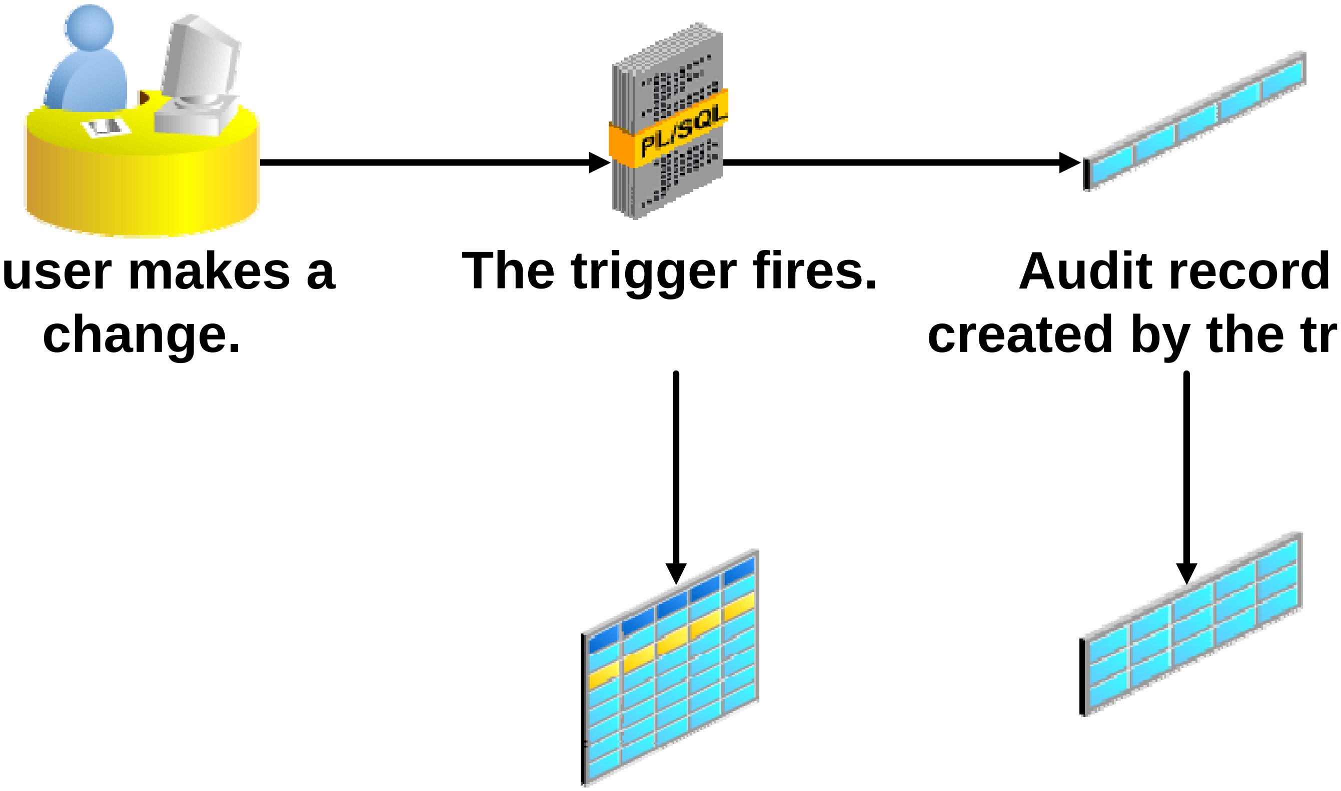


Are you sure you want to remove the 4 selected audited objects?

The audited statements you remove will no longer be audited on the objects.

```
NOAUDIT COMMENT ON HR.EMPLOYEES
NOAUDIT INDEX ON HR.EMPLOYEES
NOAUDIT LOCK ON HR.EMPLOYEES
NOAUDIT RENAME ON HR.EMPLOYEES
```

Value-Based Auditing



A user makes a change.

The trigger fires.

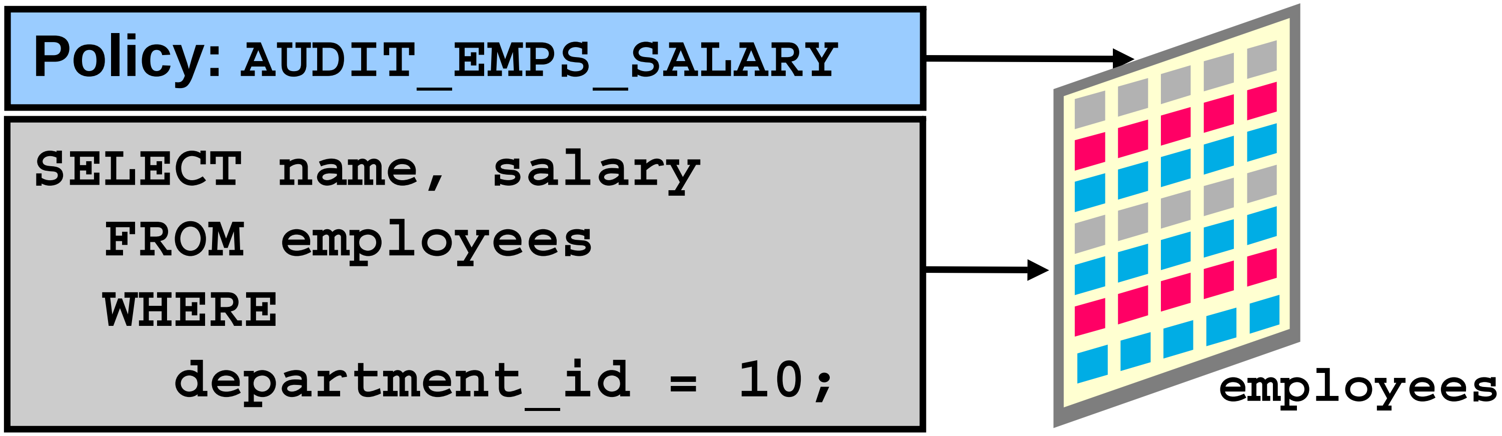
Audit record is created by the trigger.

User's change is made.

Audit record is inserted into an audit trail table.

Fine-Grained Auditing

- Monitors data access on the basis of content
- Audits SELECT, INSERT, UPDATE, DELETE, and MERGE
- Can be linked to one or more columns in a table or view
- May execute a procedure
- Is administered with the DBMS_FGA package



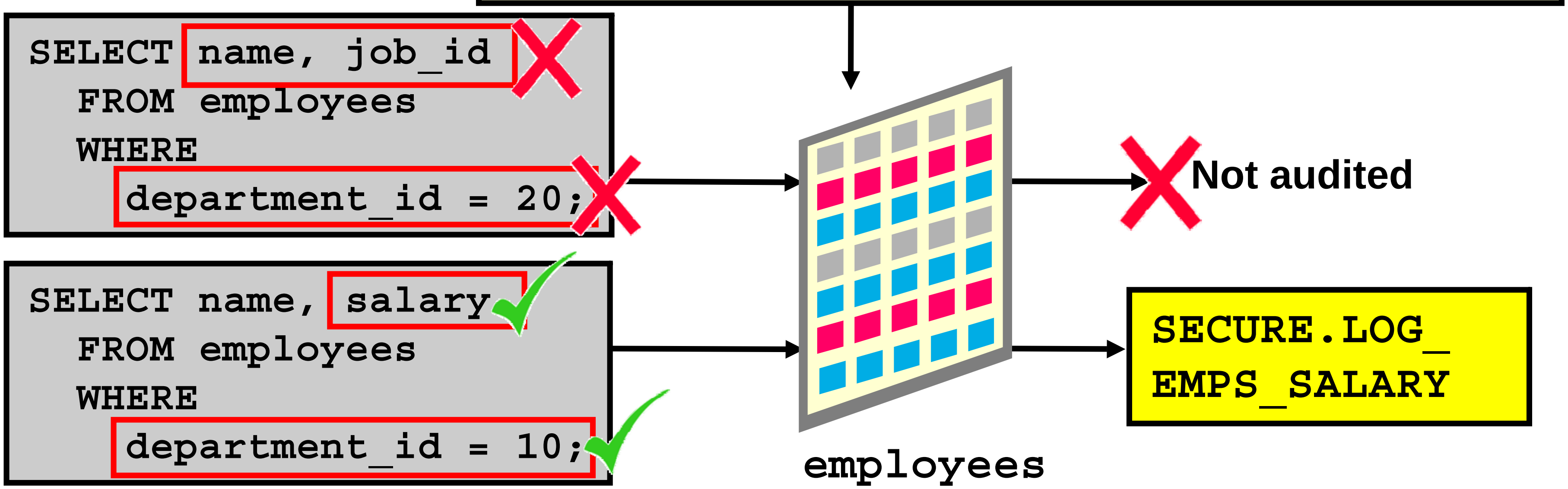
Policy: AUDIT_EMPS_SALARY

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

FGA Policy

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

```
dbms_fga.add_policy (
 object_schema    => 'HR',
 object_name      => 'EMPLOYEES',
 policy_name => 'audit_emps_salary',
 audit_condition=>  'department_id=10',
 audit_column     => 'SALARY,COMMISSION_PCT',
 handler_schema   => 'secure',
 handler_module   => 'log_emps_salary',
 enable           => TRUE,
 statement_types => 'SELECT,UPDATE');
```



```
SELECT name, job_id
  FROM employees
  WHERE
    department_id = 20;
```

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

Audited DML Statement: Considerations

- Records are audited if the FGA predicate is satisfied and the relevant columns are referenced.
- `DELETE` statements are audited regardless of columns specified.
- `MERGE` statements are audited with the underlying `INSERT`, `UPDATE`, and `DELETE` generated statements.

Not audited because none of the records involved are for department 10.

```
UPDATE hr.employees
SET salary = 1000
WHERE commission_pct = .2;
```

```
UPDATE hr.employees
SET salary = 1000
WHERE employee_id = 200;
```

FGA Guidelines

- To audit all rows, use a `null` audit condition.
- To audit all columns, use a `null` audit column.
- Policy names must be unique.
- The audited table or view must already exist when you create the policy.
- If the audit condition syntax is invalid, an `ORA-28112` error is raised when the audited object is accessed.
- If the audited 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 record is still created.

SYSDBA Auditing

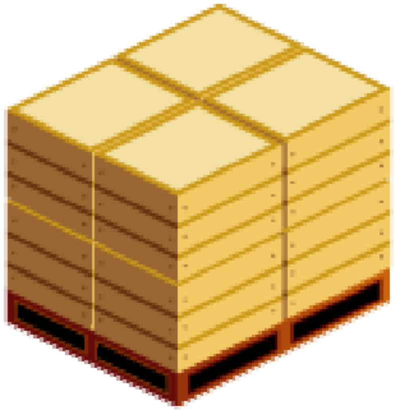
Users with SYSDBA or SYSOPER privileges can connect when the database is closed.

- Audit trail must be stored outside the database.
- Connections as SYSDBA or SYSOPER are always audited.
- You can enable additional auditing of SYSDBA or SYSOPER actions with AUDIT_SYS_OPERATIONS.
- You can control the audit trail with AUDIT_FILE_DEST.

Maintaining the Audit Trail

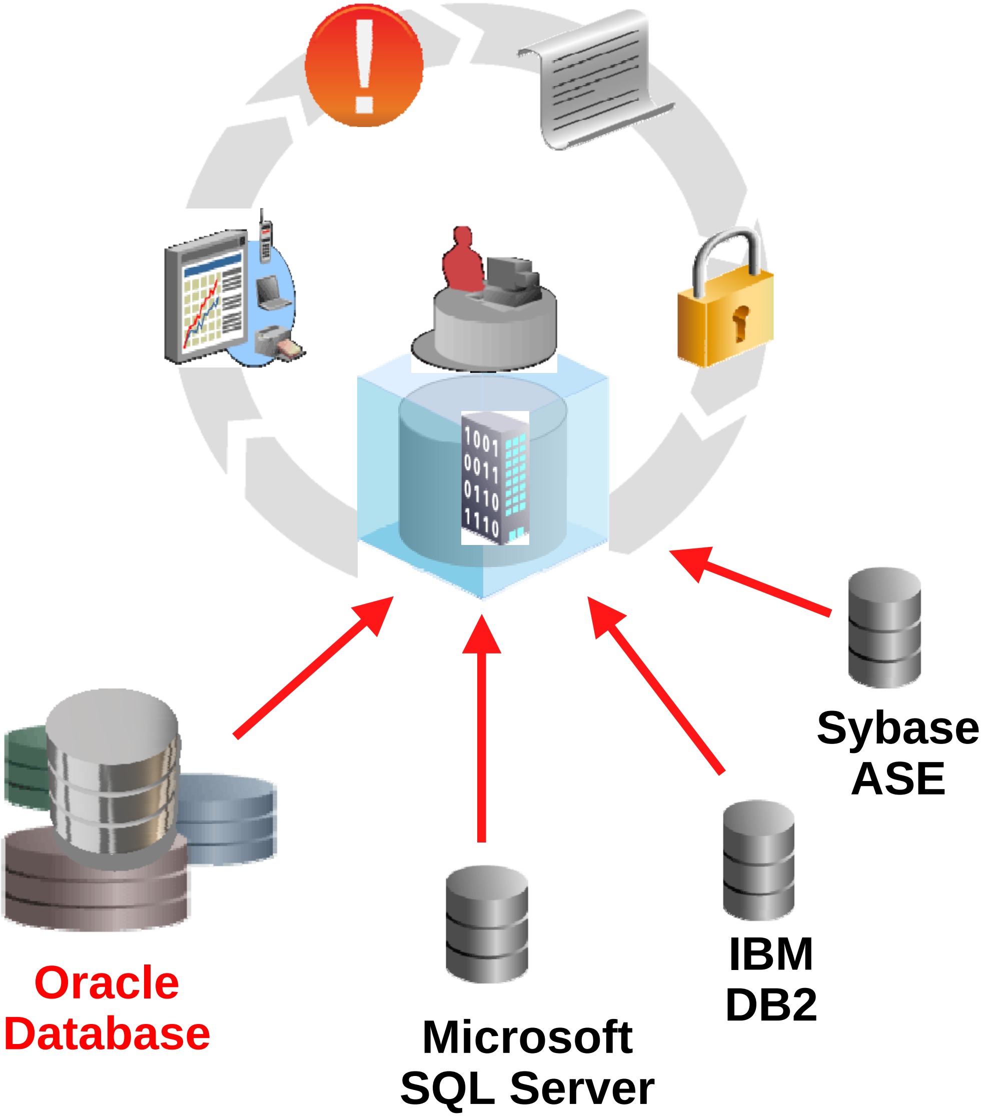
The audit trail should be maintained with the following best-practice guidelines:

- Review and store old records.
- Prevent storage problems.
- Avoid loss of records.



Oracle Audit Vault

- Consolidate and secure audit data
  - Oracle 9*i* Release 2 and higher
  - SQL Server 2000, 2005
  - IBM DB2 UDB 8.5 & 9.2
  - Sybase ASE 12.5 - 15.0
  - Secure and scalable
  - Cleanup of source Oracle audit data
- Centralized reporting
  - Updated reports interface using widely popular Oracle Application Express
  - Standard reports for compliance
  - New custom reports
- Alert on security threats
  - Detect and alert on security relevant events



Quiz

Standard database auditing captures the before and after changes of a DML transaction.

1. True
2. False

Quiz

Auditing of `SYSDBA` and `SYSOPER` actions is enabled by default.

1. True
2. False

Summary

In this lesson, you should have learned how to:

- Describe DBA responsibilities for security and auditing
- Enable standard database auditing
- Specify audit options
- Review audit information
- Maintain the audit trail

Practice 11 Overview: Implementing Oracle Database Security

This practice covers the following topics:

- Enabling standard database auditing
- Specifying audit options for the HR.JOBS table
- Updating the table
- Reviewing audit information
- Maintaining the audit trail