

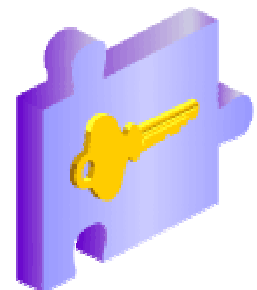
10

Implementing Oracle Database Security

Objectives

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

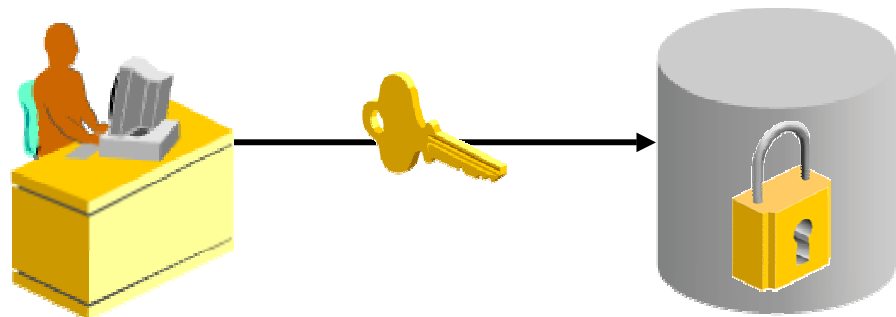
- **Describe your DBA responsibilities for security**
- **Apply the principle of least privilege**
- **Enable standard database auditing**
- **Specify audit options**
- **Review audit information**
- **Maintain the audit trail**



Industry Security Requirements

> **Requirements**
Least Privilege
Auditing
Value-based
FGA
DBA
Sec. Updates

- **Legal:**
 - Sarbanes-Oxley Act (SOX)
 - Health Information Portability and Accountability Act (HIPAA)
 - California Breach Law
 - UK Data Protection Act
- **Auditing**



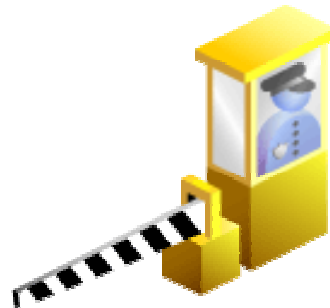
Separation of Responsibilities

- **Users with DBA privileges must be trusted.**
Consider:
 - Abuse of trust
 - That audit trails protect 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**



Principle of Least Privilege

Requirements
> **Least Privilege**
Auditing
Value-based
FGA
DBA
Sec. Updates

- **Install only required software on the machine.**
- **Activate only required services on the machine.**
- **Give OS and database access to only those users that require access.**
- **Limit access to the root or administrator account.**
- **Limit access to the SYSDBA and SYSOPER accounts.**
- **Limit users' access to only the database objects required to do their jobs.**

Applying the Principle of Least Privilege

- **Protect the data dictionary:**

```
O7_DICTIONARY_ACCESSIBILITY=FALSE
```

- **Revoke unnecessary privileges from PUBLIC:**

```
REVOKE EXECUTE ON UTL_SMTP, UTL_TCP, UTL_HTTP,  
UTL_FILE FROM PUBLIC;
```

- **Restrict the directories accessible by users.**
- **Limit users with administrative privileges.**
- **Restrict remote database authentication:**

```
REMOTE_OS_AUTHENT=FALSE
```

Monitoring for Suspicious Activity

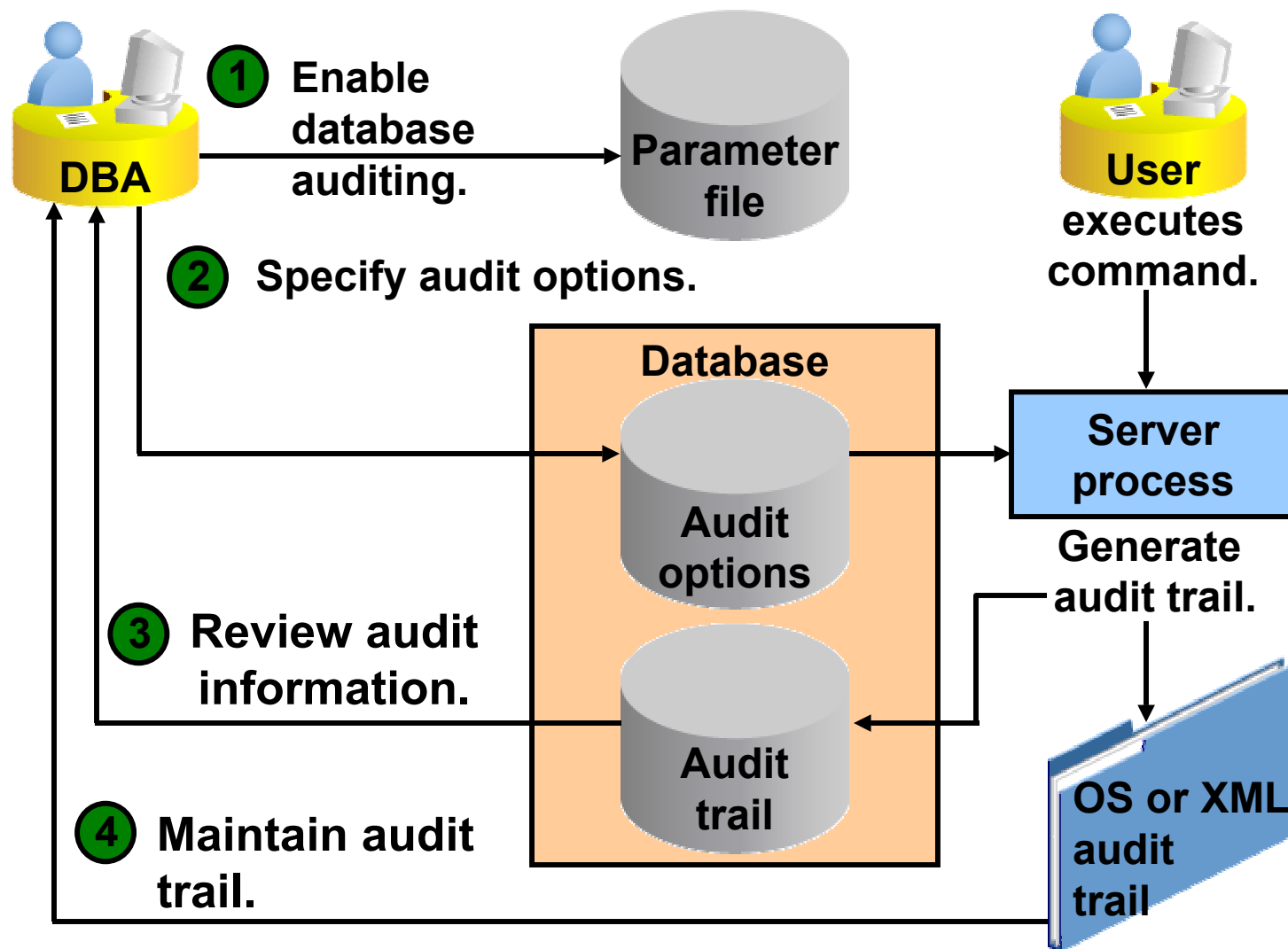
Requirements
Least Privilege
> **Auditing**
Value-based
FGA
DBA
Sec. Updates

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)**
- **DBA auditing**



Standard Database Auditing



Enabling Auditing

Database Instance: [orcl.oracle.com](#) > Initialization Parameters Logged in As SYS

Initialization Parameters

[Show SQL](#) [Revert](#) [Apply](#)

[Current](#) [SPFile](#)

The parameter values listed here are from the SPFILE `/u01/app/oracle/product/10.2.0/db_1/dbs/spfileorcl.ora`

Name Basic Dynamic Category [Go](#)

Filter on a name or partial name

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

[Reset](#)

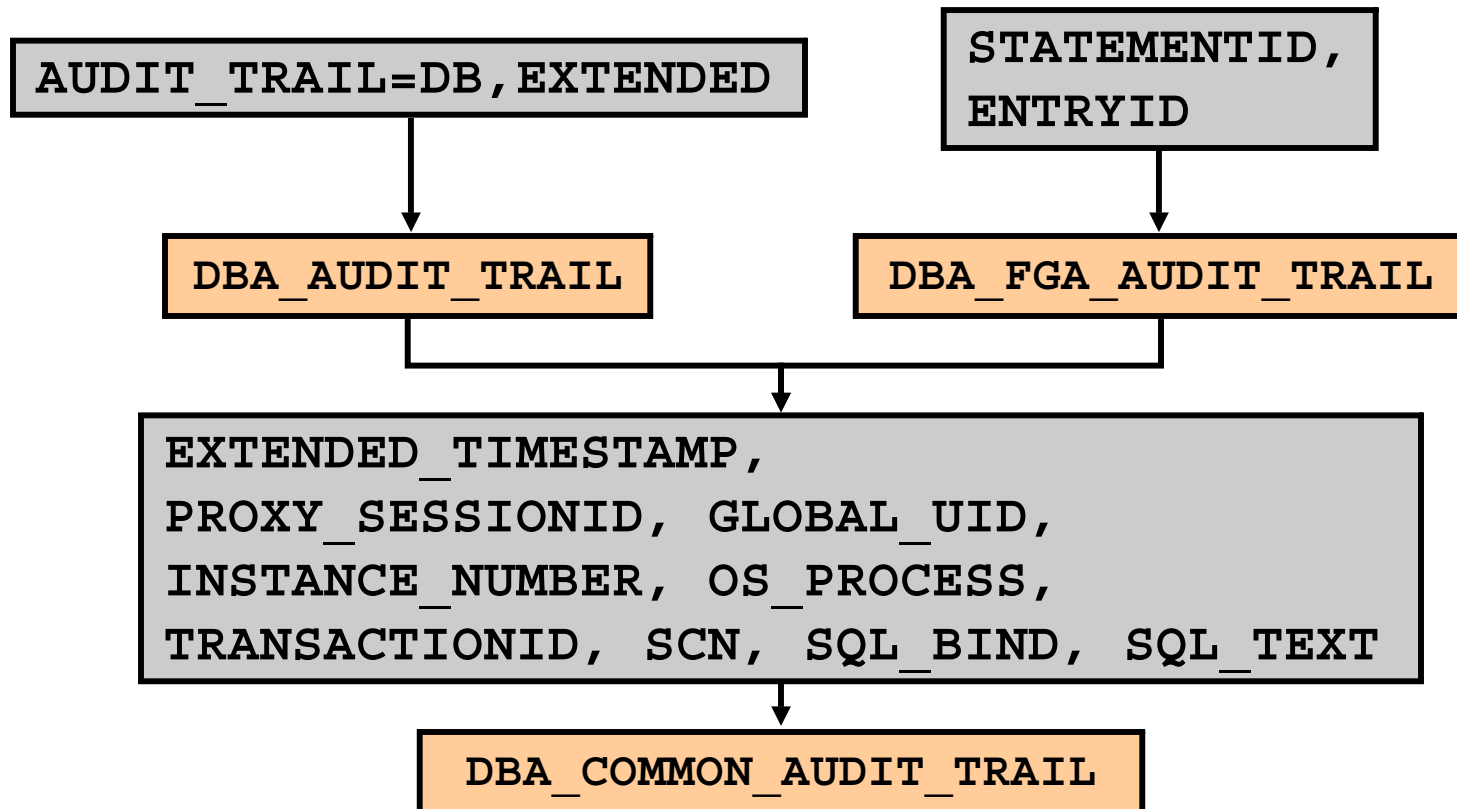
Select	Name	Help	Revisions	Value	Comments	Type	Basic	Dynamic	Category
<input type="radio"/>	audit_file_dest	?		/u01/app/oracle/admin/orcl/ac		String		✓	Security and Auditing
<input type="radio"/>	audit_sys_operations	?		Unspecified		Boolean			Security and Auditing
<input type="radio"/>	audit_syslog_level					String			Miscellaneous
<input type="radio"/>	audit_trail	?		XML		String			Security and Auditing

```
ALTER SYSTEM SET audit_trail="XML" SCOPE=SPFILE;
```

Restart database after modifying a static initialization parameter.

Uniform Audit Trails

Use `AUDIT_TRAIL=DB, EXTENDED` to enable database auditing



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 [XML](#)
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](#)

Audited Privileges (0) [Audited Objects \(1\)](#) [Audited Statements \(0\)](#)

Privilege _____ User [SYS](#) Proxy _____ [Search](#)

Select	Privilege	User	Proxy	Success	Failure
<input type="checkbox"/>	No object found.				

Show SQL

AUDIT DELETE, INSERT, UPDATE ON HR.JOBS BY SESSION

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;
```

Using and Maintaining Audit Information

Audited Objects

Filter Result

Return

▼ Hide SQL

```
SELECT "OBJECT_SCHEMA", "OBJECT_NAME", "DB_USER", "STATEMENT_TYPE",  
"EXTENDED_TIMESTAMP" FROM SYS.DBA_COMMON_AUDIT_TRAIL WHERE (action between 1 and 16) or  
(action between 19 and 29) or (action between 32 and 41) or (action = 43) or (action between 51 and 99) or  
(action = 103) or (action between 110 and 113) or (action between 116 and 121) or (action between 123 and 128)  
or (action between 160 and 162)
```

Schema	Object Name	User Name	Action	Time (In Session's Time Zone)
HR	JOBS	AUDIT_USER	SESSION REC	2005-10-21 17:52:33.783793000 -7:0
HR	JOBS	HR	SESSION REC	2005-10-21 17:52:34.147582000 -7:0

Disable audit options if you are not using them.

Confirmation

No

Yes

Are you sure you want to remove the 3 selected audited objects?

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

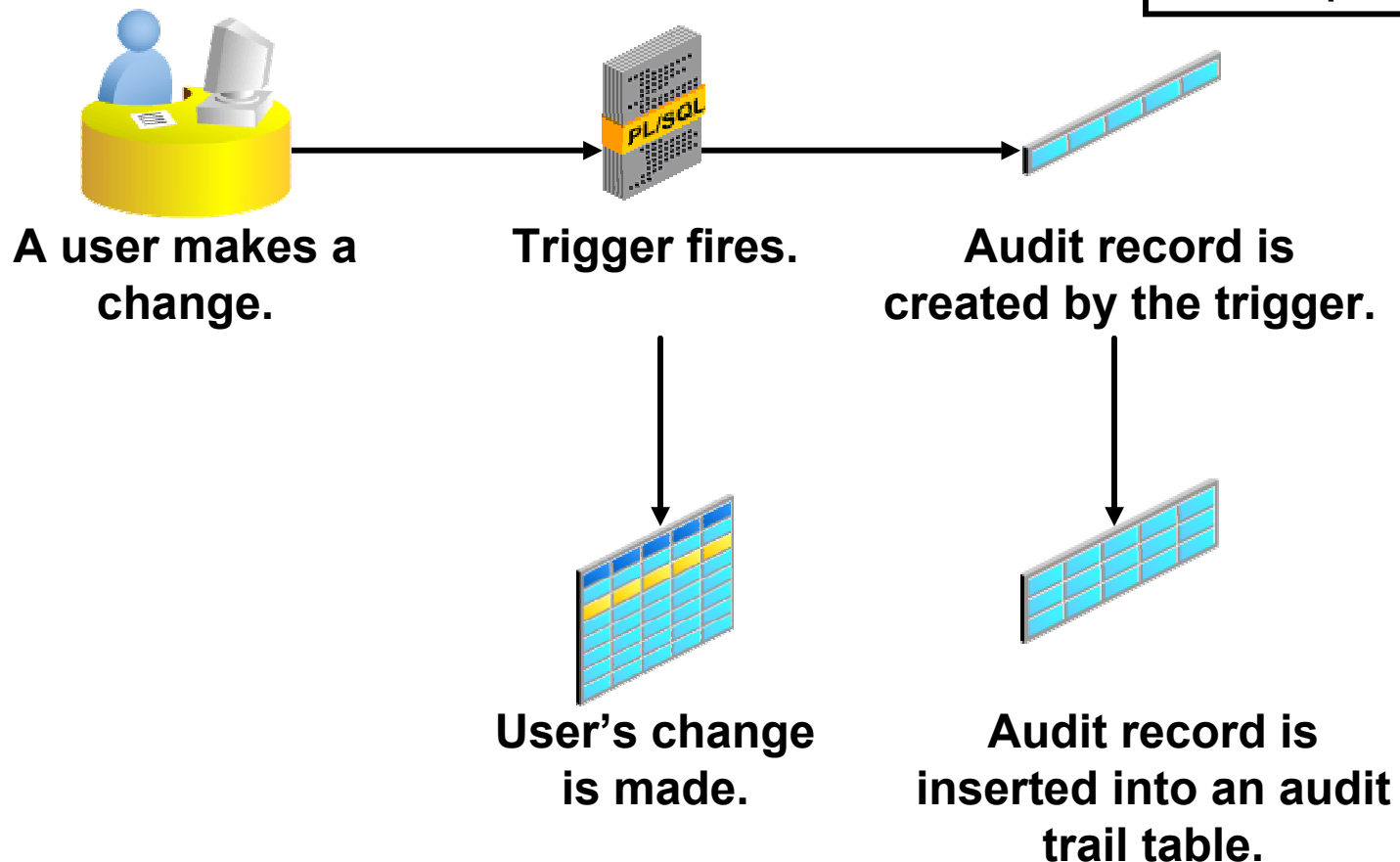
▼ Hide SQL

```
NOAUDIT DELETE ON HR.JOBS  
NOAUDIT INSERT ON HR.JOBS  
NOAUDIT UPDATE ON HR.JOBS
```

```
ALTER SYSTEM SET audit_trail = "NONE" SCOPE=SPFILE
```

Value-Based Auditing

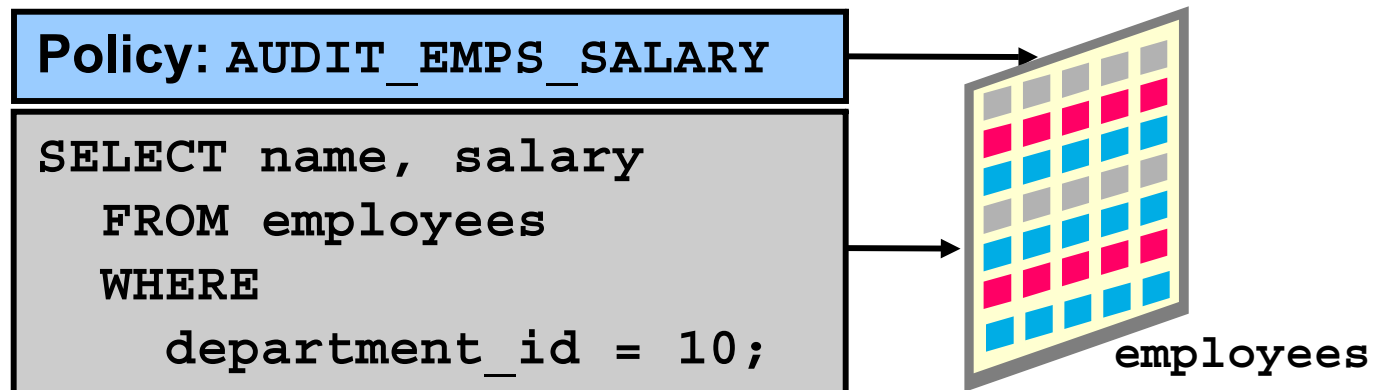
Requirements
Least Privilege
Auditing
> Value-based
FGA
DBA
Sec. Updates



Fine-Grained Auditing

Requirements
Least Privilege
Auditing
Value-based
> FGA
DBA
Sec. Updates

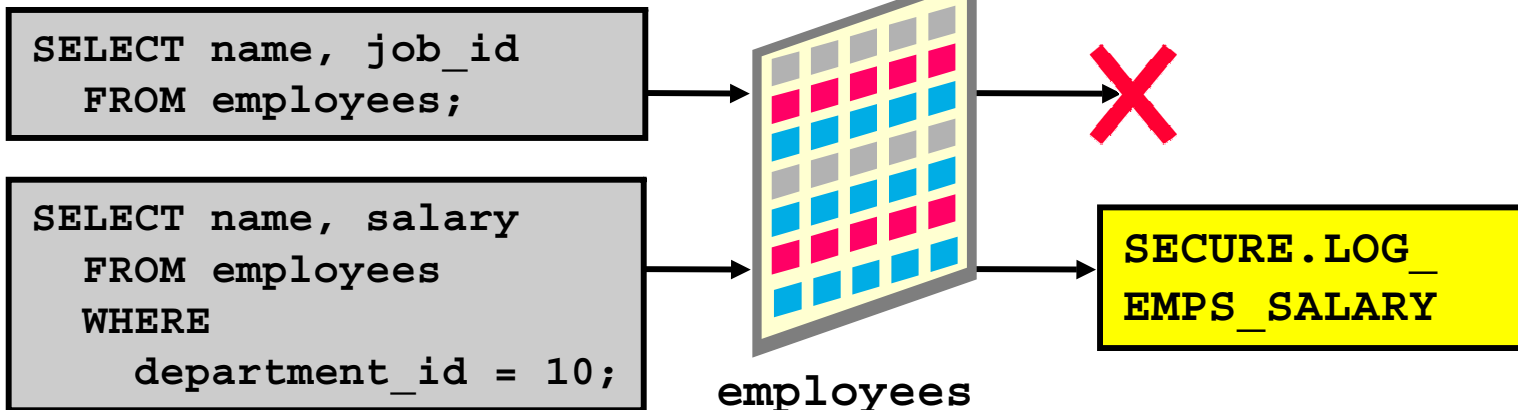
- Monitors data access on the basis of content
- Audits SELECT, INSERT, UPDATE, DELETE, and MERGE
- Can be linked to a table or view, to one or more columns
- May fire a procedure
- Is administered with the DBMS_FGA package



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',  
  handler_schema=> 'secure',  
  handler_module=> 'log_emps_salary',  
  enable       => TRUE,  
  statement_types=> 'SELECT' );
```



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 any specified columns.
- MERGE statements are audited with the underlying INSERT or UPDATE generated statements.

```
UPDATE hr.employees  
SET salary = 10  
WHERE department_id = 10;
```

```
UPDATE hr.employees  
SET salary = 10  
WHERE employee_id = 111;
```



FGA Guidelines

- To audit all statements, use a `null` condition.
- 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.

DBA Auditing

Requirements
Least Privilege
Auditing
Value-based
FGA
> **DBA**
Sec. Updates

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

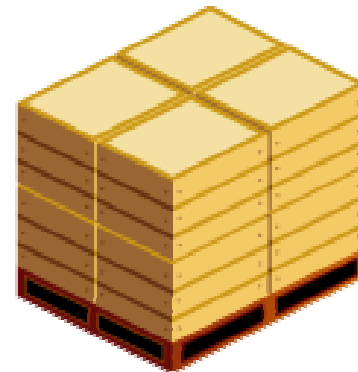
- **Audit trail must be stored outside the database.**
- **Connections as SYSDBA or SYSOPER are always audited.**
- **You can enable additional auditing of SYSDBA or SYSOPER actions with `audit_sys_operations`.**
- **You can control the audit trail with `audit_file_dest`.**



Maintaining the Audit Trail

The audit trail should be maintained. Follow these best practice guidelines:

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

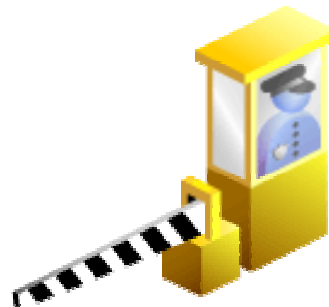


Security Updates

Requirements
Least Privilege
Auditing
Value-based
FGA
DBA

> [Sec. Updates](#)

- Oracle posts security alerts on the Oracle Technology Network Web site at:
<http://www.oracle.com/technology/deploy/security/alerts.htm>
- Oracle database administrators and developers can also subscribe to be notified about critical security alerts via e-mail by clicking the “Subscribe to Security Alerts Here” link.



Applying Security Patches

- **Use the Critical Patch Update process.**
- **Apply all security patches and workarounds.**
- **Contact the Oracle security products team.**



Summary

In this lesson, you should have learned how to:

- **Describe your DBA responsibilities for security**
- **Apply the principle of least privilege**
- **Enable standard database auditing**
- **Specify audit options**
- **Review audit information**
- **Maintain the audit trail**



Practice 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**