# Practices for Lesson 22: Implementing Oracle Database Auditing

Practices for Lesson 22: Overview

Overview

In these practices, you will verify Unified Auditing is enabled, create audit users, and create an audit policy.

Practice 22-1: Enabling Unified Auditing

Overview

In this practice, you enable unified auditing.

Assumptions

If this practice has been attempted with the current deployment of the practice environment, reset the original state by executing

/home/oracle/labs/DBMod\_UsersSec/disable\_unified\_aud.sh.

This script removes unified auditing from the Oracle executable, and removes possible unified auditing artifacts created in a prior attempt. Only the orclcdb database will be restarted. This script may display errors that can be safely ignored.

Tasks

Open a terminal and set the Oracle environment for the ORCLCDB database.

Shut down all Oracle processes of all instances.

Shut down the listeners, LISTENER and LISTENER2

Shut down the orclcdb instance and exit sqlplus.

Verify that all instances are down.

If there are any databases still open change the Oracle environment to that database and shut it down.

Confirm all instances are down with another pgreg –lfa smon command.

Enable the unified auditing feature.

Restart the processes.

Change the Oracle Environment to orclcdb.

Restart the listener.

Change your working directory back to /home/oracle

Restart the orclcdb database instance.

Verify that unified auditing is enabled.

Open all PDBs.

Set all databases to open on startup.

Exit from SQL\*Plus.

Exit all terminals.

Practice 22-2: Creating Audit Users

Overview

In this practice you will create audit users: one account to administer the audit settings and another account to be used by the external auditor. These additional users are optional, but are a good practice that provides a clear separation of duties required in many businesses. In this exercise you will create a common user to administer audit policies and another to be used by the external auditor across all PDBs in the ORCLCDB database.

Assumptions

Unified auditing has been enabled in the orclcdb database.

Tasks

Open a terminal, use the . oraenv command to source for database orclcdb, then connect to the ORCLCDB instance as a user with SYSDBA privilege.

Create a database user to be the administrator of the audit settings and policies. Name this user C##AUDMGR. Refer to *Course Practice Environment: Security Credentials* for the ***password*** value. Assign the AUDIT\_ADMIN role to this user.

Create a database user to be used by any person that needs to view the audit data. Name this user C##AUDVWR . Refer to *Practice Environment: Security Credentials* for the ***password*** value. Assign the AUDIT\_VIEWER role to this user.

Exit SQL\*Plus and terminals.

Close all terminals.

Practice 22-3: Creating an Audit Policy

Overview

In this practice, as the C##AUDMGR user you will create an audit policy to monitor activity in the

HR.JOBS table in the ORCLPDB1 database and apply it to multiple users.

Assumptions

The C##AUDMGR user has been created. Several users with DML privileges on HR.JOBS have been created.

Tasks

Invoke SQL\*Plus and connect to the ORCLPDB1 database as the C##AUDMGR user. Create a policy named JOBS\_AUDIT\_UPD that audits all auditable statements for the HR.JOBS table.

Open a terminal and set the environment for the orclcdb database by using oraenv.

Connect to the ORCLPDB1 PDB as the C##AUDMGR user by using SQL\*Plus. Refer to

*Practice Environment: Security Credentials* for the ***password*** value.

Create an audit policy called JOBS\_AUDIT\_UPD to track UPDATE commands issued against the HR.JOBS table.

Enable the audit policy for all users.

Verify the creation of the JOBS\_AUDIT\_UPD policy.

Test the audit policy by connecting as a user that has privileges to update rows in the

HR.JOBS table.

Connect as the JGOODMAN user and update MAX\_SALARY of the President to $50000. Be sure to set HRMANAGER role. Refer to *Practice Environment: Security Credentials* for the ***password*** value.

Connect as the C##AUDMGR user and view the audit trail records for this change. **Note:** Your output may vary from what is shown depending on how many times you have Set Role as the JGOODMAN user. For this practice, you are interested in the row

for the JOBS\_AUDIT\_UPD policy. Refer to *Practice Environment: Security Credentials*

for the ***password*** value.

If you did not see any rows as a result of the query in step 3b, flush the audit records.

**Note:** The default behavior of the Unified Audit Engine is to queue the audit records and write them to the Unified Audit trail as the queue fills. The DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL procedure forces the records in the queue to be written to disk. The audit records are not visible until they are written to the audit trail.

Run the query in step 3b again to view the audit trail records.

Exit from SQL\*Plus.

Disable unified auditing by running the script,

/home/oracle/labs/DBMod\_UsersSec/disable\_unified\_aud.sh

Note: this script will take several minutes to run.

Exit all terminals.