Auditing with Unified Auditing

## Using Mixed Auditing Mode

In this topic, you will use the mixed auditing mode.

* When a database is upgraded from a previous release, before you decide to switch to the unified auditing mode,  you can use the mixed mode by creating a policy with CREATE AUDIT POLICY command and then enabling it with AUDITcommand. If you do not wish to create a new policy, you can simply enable one of the predefined policies - ORA\_SECURECONFIG or ORA\_ACCOUNT\_MGMT or ORA\_DATABASE\_PARAMETER. Either of this puts the database is mixed auditing mode. The old audit syntax continues to work and the old audit destinations continues to be written to.
* When a database is created, mixed auditing mode is used by default through the predefined enabled policy ORA\_SECURECONFIG. But unified auditing mode is not yet enabled.

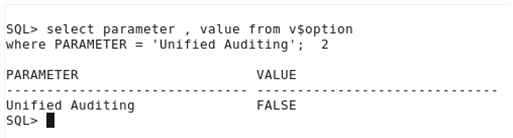
Verify that unified auditing is not enabled by default. A new database orcl has been recently created.

**. oraenv**

**[enter orcl at the prompt]**

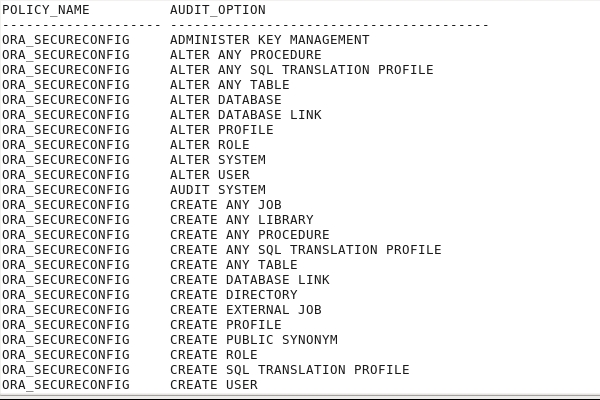
**sqlplus / as sysdba**

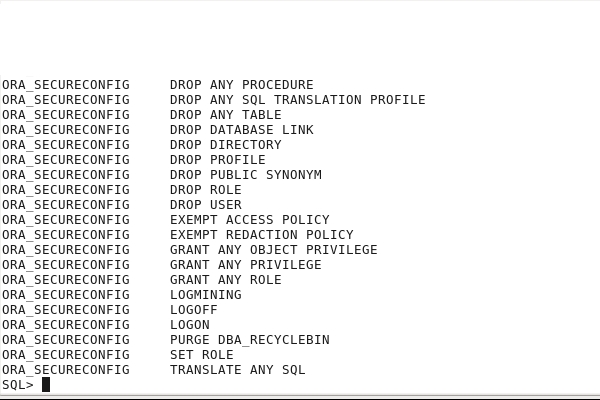
**select parameter , value from v$option   
where PARAMETER = 'Unified Auditing';**



Check the existence of the predefined ORA\_SECURECONFIG audit policy.

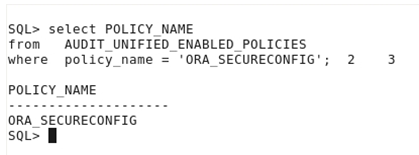
**col POLICY\_NAME format A20  
col AUDIT\_OPTION format A40  
set PAGES 100  
select POLICY\_NAME, AUDIT\_OPTION   
from   AUDIT\_UNIFIED\_POLICIES   
where  policy\_name =  'ORA\_SECURECONFIG'  order by 2 ;**





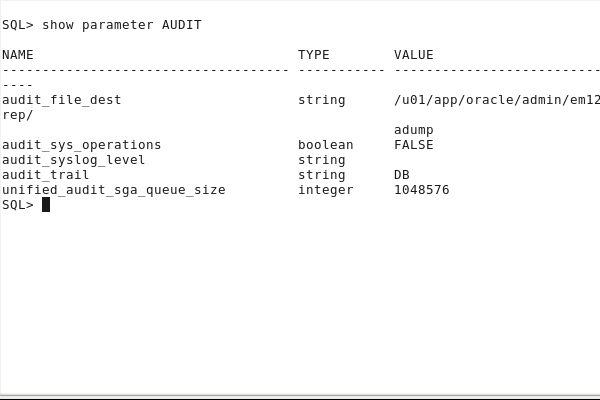
Verify that the predefined ORA\_SECURECONFIG audit policy is enabled by default.

**select POLICY\_NAME   
from   AUDIT\_UNIFIED\_ENABLED\_POLICIES   
where  policy\_name = 'ORA\_SECURECONFIG';**



Verify all AUDIT parameters at instance level.

**show parameter AUDIT**

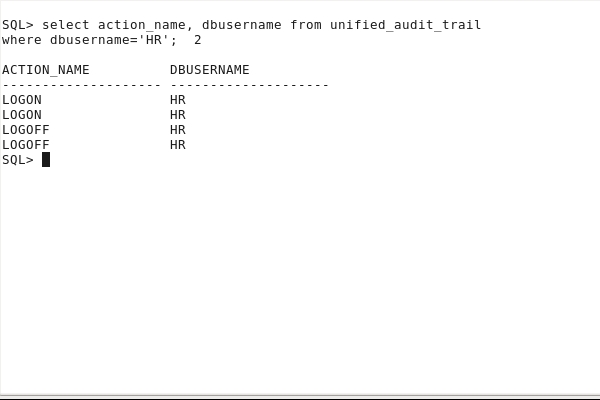


Is user connection still audited?  Verify that audit data is recorded as it is in an 11g Oracle Database although the CREATE SESSION privilege is only audited for LBACSYS, DVSYS and DVF users.

**connect hr/oracle\_4U  
connect hr/oracle\_4U**

**connect / as sysdba**

**col dbusername format A20  
col action\_name format A20  
select action\_name, dbusername from unified\_audit\_trail   
where dbusername='HR';**



## Enabling the Unified Auditing Mode

In this topic, you enable the unified auditing mode.

Stop all Oracle processes: databases, listener and Enterprise Manager.

**shutdown immediate  
exit**  
  
**ps -ef | grep pmon**  
  
**. oraenv**

**[enter cdb1 at the prompt]**

**sqlplus / as sysdba  
shutdown immediate  
exit**

**lsnrctl stop**

**cd /u01/app/oracle/product/middleware/oms  
export OMS\_HOME=/u01/app/oracle/product/middleware/oms  
$OMS\_HOME/bin/emctl stop oms**

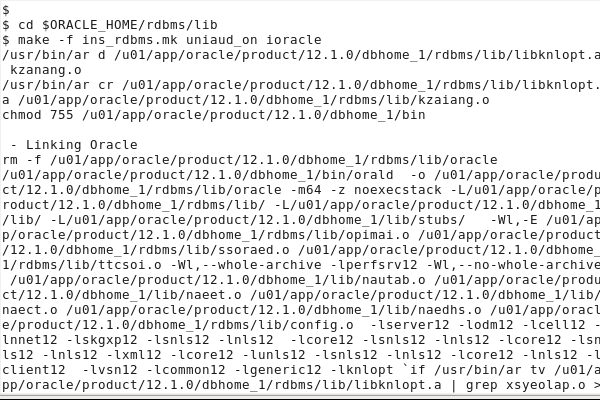
**. oraenv**

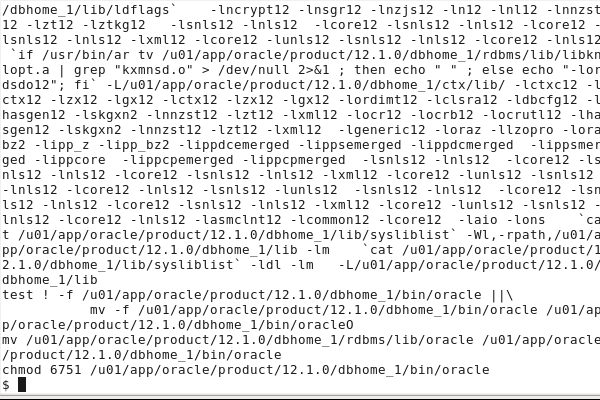
**[enter emrep at the prompt]**

**sqlplus / as sysdba  
shutdown immediate  
exit**

Relink Oracle with the uniaud\_on option.

**cd $ORACLE\_HOME/rdbms/lib  
make -f ins\_rdbms.mk uniaud\_on ioracle**





Restart all Oracle processes: Enterprise Manager, listener, databases.For the purpose of the demonstration, only the orcl database instance needs to be started and the listener.

**. oraenv**

**[enter orcl at the prompt]**

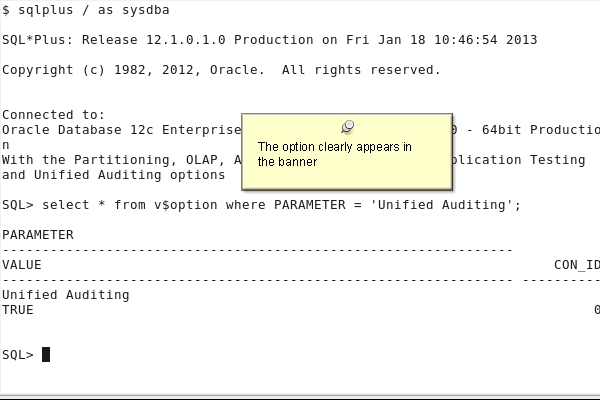
**sqlplus / as sysdba  
startup  
exit**

**lsnrctl start**

Verify that unified auditing is now enabled.

**sqlplus / as sysdba**

**select \* from v$option where PARAMETER = 'Unified Auditing';**



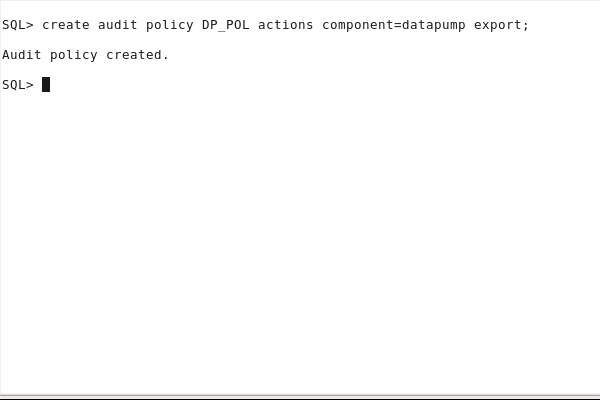
## Auditing RMAN and Oracle Data Pump Operations

In this topic, you audit Oracle Data Pump and Recovery Manager operations.

### Oracle Data Pump Auditing

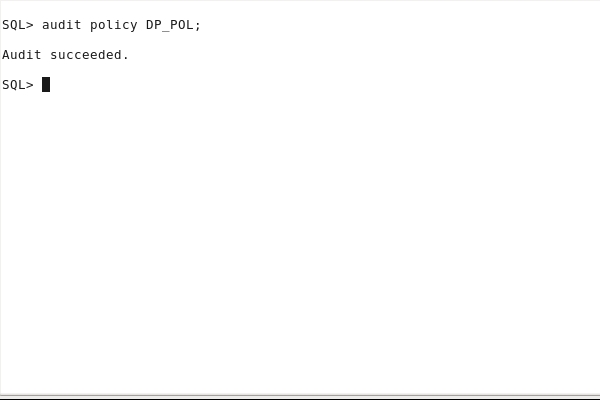
Create a DP\_POL for the Oracle Data Pump component , and more specifically for export operations.

**create audit policy DP\_POL actions component=datapump export;**

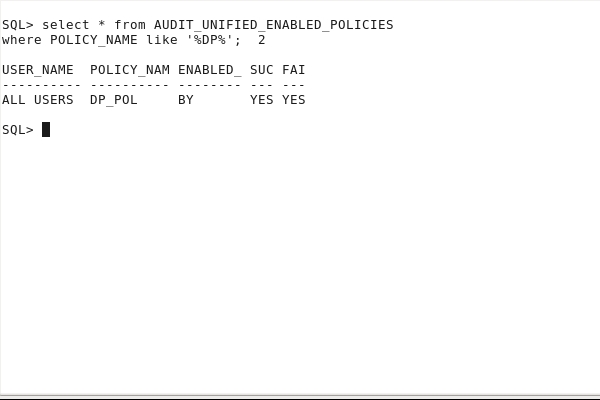


Enable the audit policy.

**audit policy DP\_POL;**



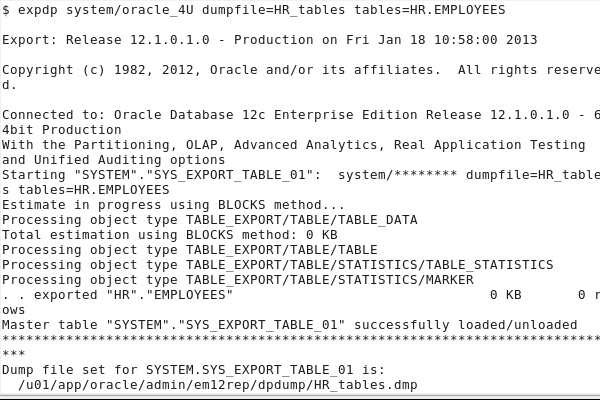
Verify that the audit policy is enabled.col user\_name format A10  
col policy\_name format A10  
select \* from AUDIT\_UNIFIED\_ENABLED\_POLICIES   
where POLICY\_NAME like '%DP%';



exit

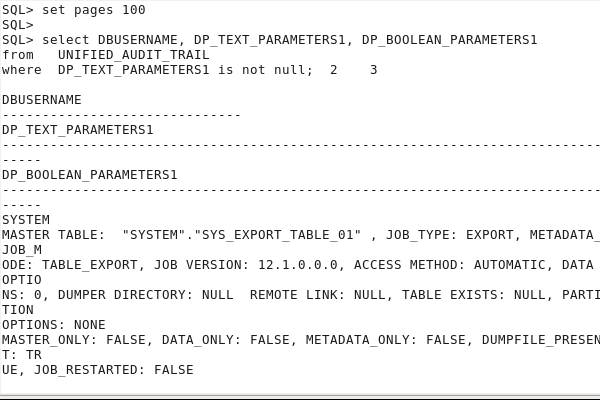
Perform an export operation.

**rm /u01/app/oracle/admin/orcl/dpdump/HR\_tables.dmp   
expdp system/oracle\_4U dumpfile=HR\_tables tables=HR.EMPLOYEES**



View the resulting audit data.

**sqlplus system/oracle\_4U  
   
set pages 100  
select DBUSERNAME, DP\_TEXT\_PARAMETERS1, DP\_BOOLEAN\_PARAMETERS1  
from   UNIFIED\_AUDIT\_TRAIL   
where  DP\_TEXT\_PARAMETERS1 is not null;**



If the audited data is still in memory, you cannot see it. We do not want to wait until the background process flushes the data to disk.

**EXEC SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

Now you can view the resulting audit data.

**select DBUSERNAME, DP\_TEXT\_PARAMETERS1, DP\_BOOLEAN\_PARAMETERS1  
from   UNIFIED\_AUDIT\_TRAIL   
where  DP\_TEXT\_PARAMETERS1 is not null;**

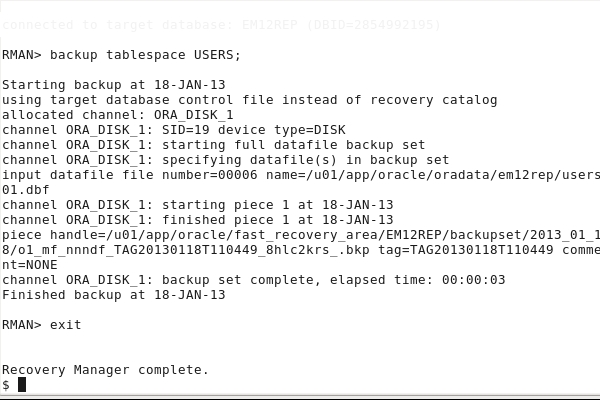
**exit**

### RMAN Auditing

You want to audit Recovery Manager backup, restore and recover operations.You do not have to create any audit policy for RMAN operations. RMAN is audited by default.  
Backup any of the tablespaces of the database.

**rman target /  
backup tablespace USERS;**

**exit;**

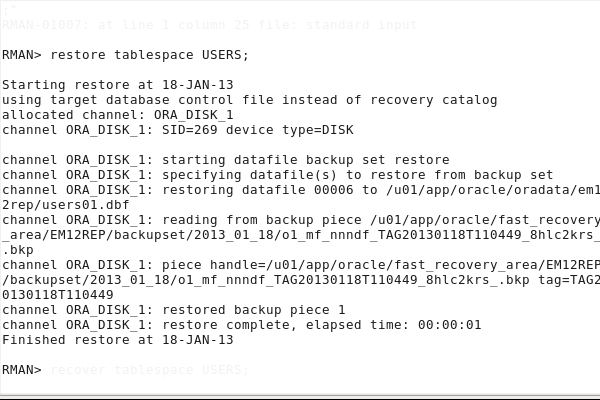


Remove the USERS tablespace datafile.

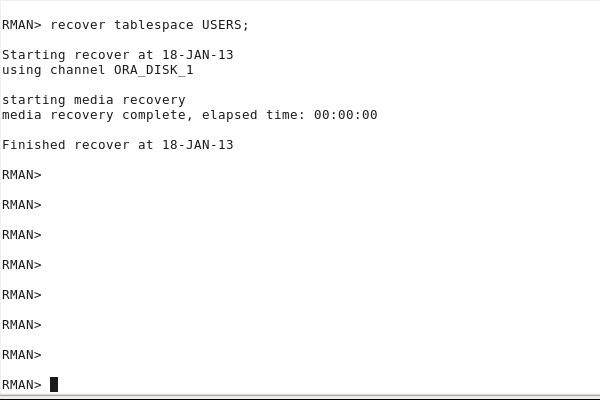
**sqlplus / as sysdba  
select file\_name from dba\_data\_files where tablespace\_name='USERS';  
!rm /u01/app/oracle/oradata/em12rep/users01.dbf**  
  
**alter tablespace users offline immediate;**  
exit

Restore and recover the USERS tablespace datafile.

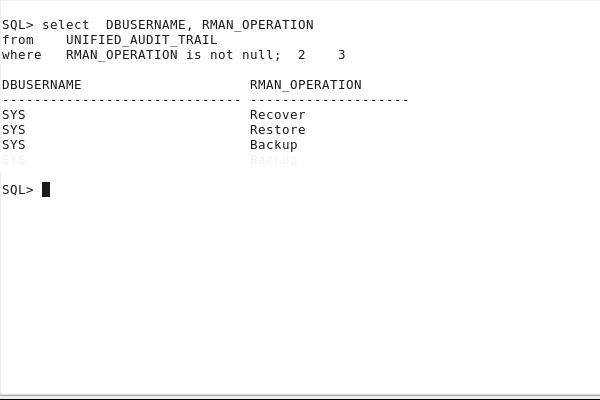
**rman target /  
restore tablespace USERS;**



**recover tablespace USERS;**



**exit;**View the resulting audit data.  
  
**sqlplus / as sysdba  
alter tablespace users online;**select  DBUSERNAME, RMAN\_OPERATION   
from    UNIFIED\_AUDIT\_TRAIL   
where   RMAN\_OPERATION is not null;



If the audited data is still in memory, you cannot see it. We do not want to wait until the background process flushes the data to disk.

**exec SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

Now you can view the resulting audit data.

**select DBUSERNAME, RMAN\_OPERATION   
from UNIFIED\_AUDIT\_TRAIL   
where RMAN\_OPERATION is not null;**

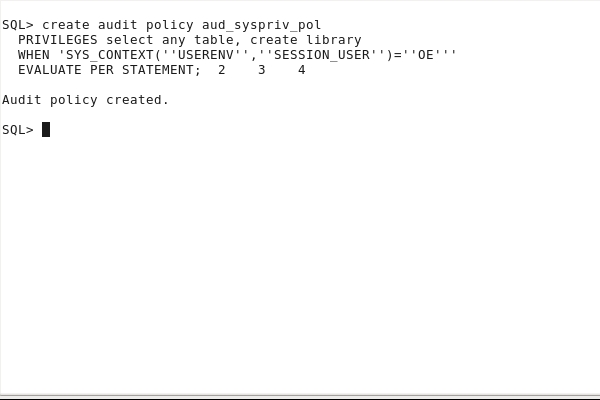
## Creating Audit Policies to Audit Privileges, Actions and Roles

In this topic, you create audit policies to audit operations that use object and system privileges, roles and perform specific actions.

### Creating a Privilege Audit Policy

Create an audit policy that will audit the user OE using the SELECT ANY TABLE or CREATE LIBRARY system privileges and this for each statement executed. Grant the SELECT ANY TABLE to the user OE.

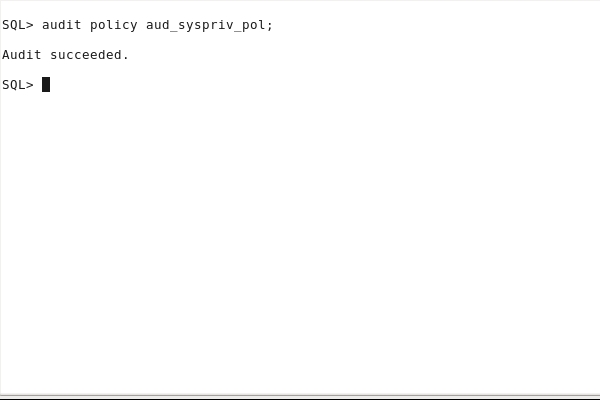
**create audit policy aud\_syspriv\_pol   
  PRIVILEGES select any table, create library  
  WHEN 'SYS\_CONTEXT(''USERENV'',''SESSION\_USER'')=''OE'''  
  EVALUATE PER STATEMENT;**



**grant SELECT ANY TABLE to oe;**

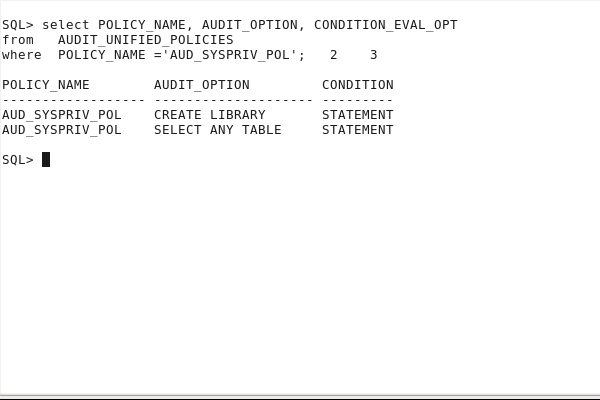
Enable the audit policy.

**audit policy aud\_syspriv\_pol;**



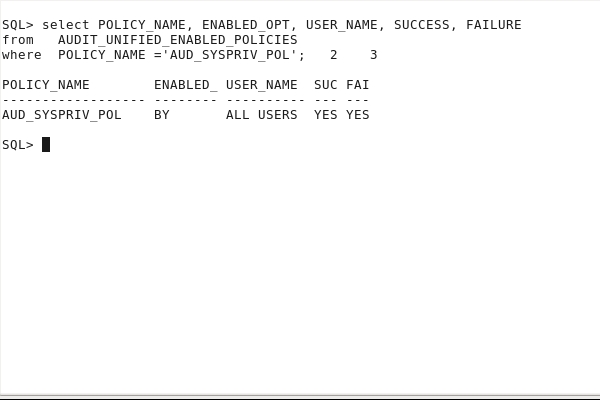
View the audit policy options.

col audit\_option format A20  
col policy\_name format A18  
select POLICY\_NAME, AUDIT\_OPTION, CONDITION\_EVAL\_OPT  
from   AUDIT\_UNIFIED\_POLICIES  
where  POLICY\_NAME ='AUD\_SYSPRIV\_POL';



Verify that the audit policy is enabled.

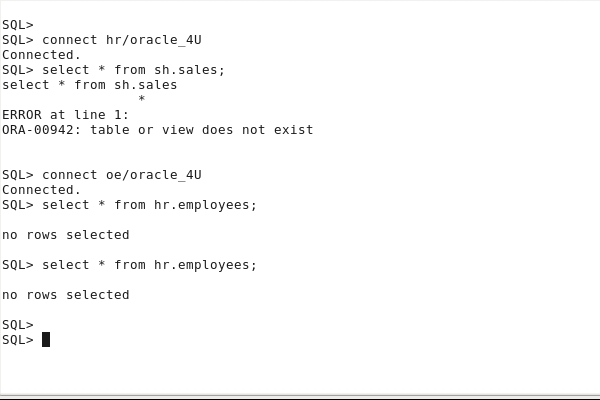
col user\_name format A10  
col policy\_name format A18  
select POLICY\_NAME, ENABLED\_OPT, USER\_NAME, SUCCESS, FAILURE  
from AUDIT\_UNIFIED\_ENABLED\_POLICIES  
where POLICY\_NAME ='AUD\_SYSPRIV\_POL';



Perform an audited operation.

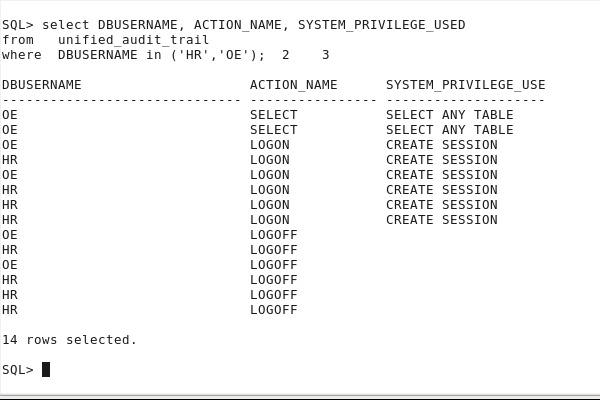
**connect hr/oracle\_4U   
select \* from sh.sales;**

**connect oe/oracle\_4U  
select \* from hr.employees;  
select \* from hr.employees;**



View the resulting audit data.

**connect system/oracle\_4U  
  
col action\_name format A16  
col policy\_name format A18  
col system\_privilege\_used format A20  
select DBUSERNAME, ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED   
from unified\_audit\_trail  
where DBUSERNAME in ('HR','OE');**



You notice that there are not any records related to HR statements due to the condition defined in the audit policy definition, except those due to the existence of the predefined ORA\_SECURECONFIG audit policy  (explained in the first section).

If the audited data is still in memory, you cannot see it. We do not want to wait until the background process flushes the data to disk.

**exec SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

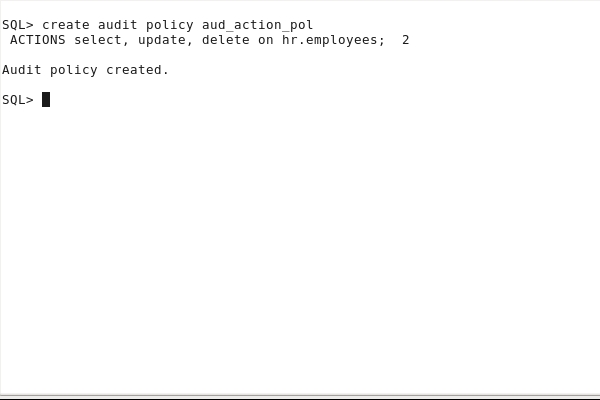
Now you can view the resulting audit data.

**select DBUSERNAME, ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED   
from   unified\_audit\_trail  
where  DBUSERNAME in ('HR','OE');**

### Creating an Action Audit Policy

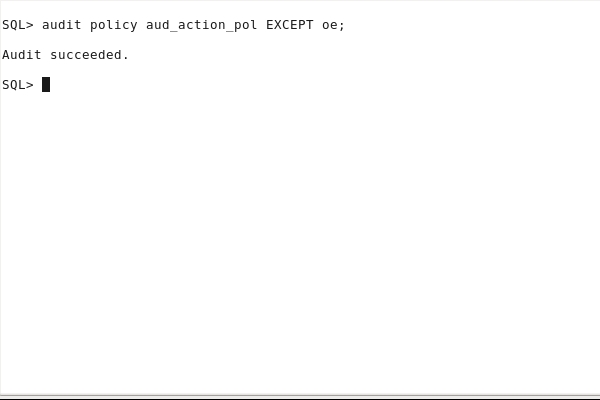
Create an audit policy that will audit any user performing any select or update operation on any object using an object or system privilege, or deleting rows from the HR.EMPLOYEES table.

**create audit policy aud\_action\_pol   
 ACTIONS select, update, delete on hr.employees;**



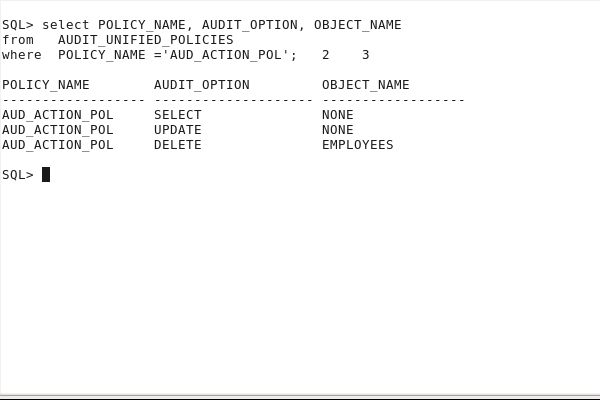
Enable the audit policy for all users except OE.

**audit policy**aud\_action\_pol EXCEPT oe**;**



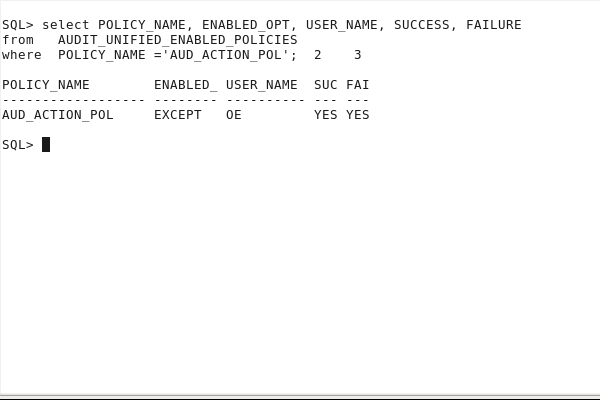
View the audit policy options.

col audit\_option format A20  
col policy\_name format A18  
col object\_name format A18  
select POLICY\_NAME, AUDIT\_OPTION, OBJECT\_NAME  
from AUDIT\_UNIFIED\_POLICIES  
where POLICY\_NAME ='AUD\_ACTION\_POL';



Verify that the audit policy is enabled.

col user\_name format A10  
col policy\_name format A18  
select POLICY\_NAME, ENABLED\_OPT, USER\_NAME, SUCCESS, FAILURE  
from AUDIT\_UNIFIED\_ENABLED\_POLICIES  
where POLICY\_NAME ='AUD\_ACTION\_POL';

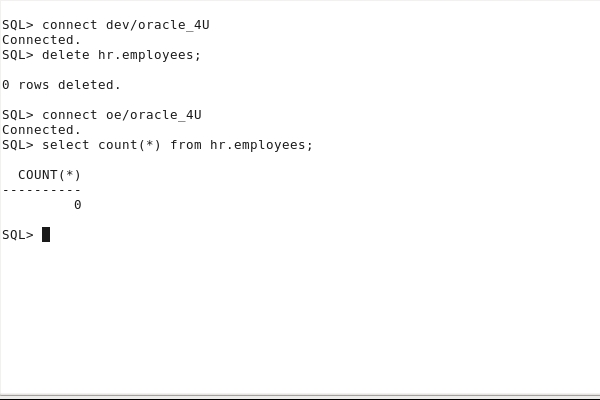


Perform an audited operation. First create a new user DEV and grant appropriate privileges to DEV to execute operations.

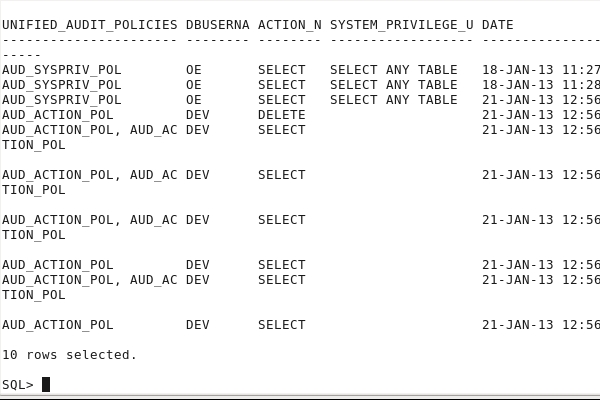
**create user DEV identified by oracle\_4U;  
grant create session to DEV;  
connect hr/oracle\_4U  
grant delete on hr.employees to DEV;**

**connect dev/oracle\_4U   
delete hr.employees;**

**connect oe/oracle\_4U  
select count(\*) from hr.employees;**



View the resulting audit data.  
  
connect system/oracle\_4U  
  
set pages 100  
col dbusername format A8  
col action\_name format A8  
col "DATE" format A20  
col  system\_privilege\_used format A18  
col unified\_audit\_policies format a22  
select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME, ACTION\_NAME,  
       SYSTEM\_PRIVILEGE\_USED,   
       to\_char(EVENT\_TIMESTAMP,'DD-MON-YY HH:MI') "DATE"  
from unified\_audit\_trail  
where  DBUSERNAME in ('DEV','OE')  
and    ACTION\_NAME not in ('LOGON', 'LOGOFF')  
order by 4;



If the audited data is still in memory, you cannot see it. We do not want to wait until the background process flushes the data to disk.

**exec SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

Now you can view the resulting audit data.

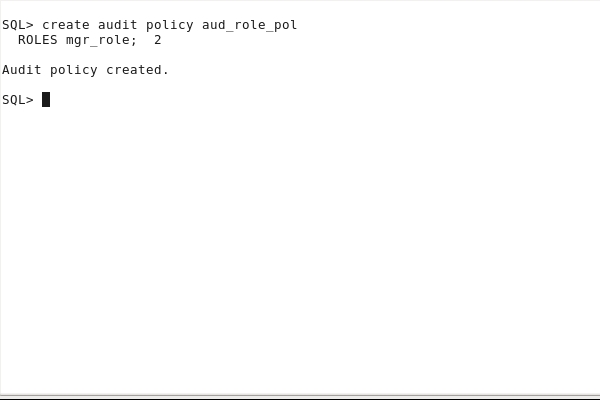
**select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME, ACTION\_NAME,  
       SYSTEM\_PRIVILEGE\_USED,   
       to\_char(EVENT\_TIMESTAMP,'DD-MON-YY HH:MI') "DATE"  
from unified\_audit\_trail  
where  DBUSERNAME in ('DEV','OE')  
and    ACTION\_NAME not in ('LOGON', 'LOGOFF')  
order by 4;**

### Creating a Role Audit Policy

Create an audit policy that will audit all users while using the MGR\_ROLE role.

**create user JIM identified by oracle\_4U;  
  
create role MGR\_ROLE;  
grant create tablespace to MGR\_ROLE;  
grant MGR\_ROLE, create session to JIM;**

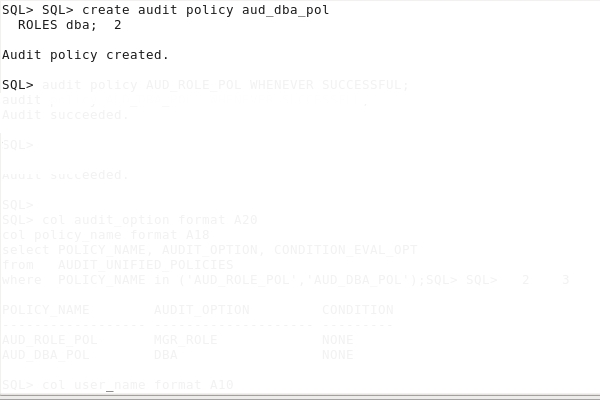
**create audit policy aud\_role\_pol   
  ROLES mgr\_role;**



Create an audit policy that will audit all users as soon as these users use the DBA role. Create a DBA\_JUNIOR user granted the DBA role.

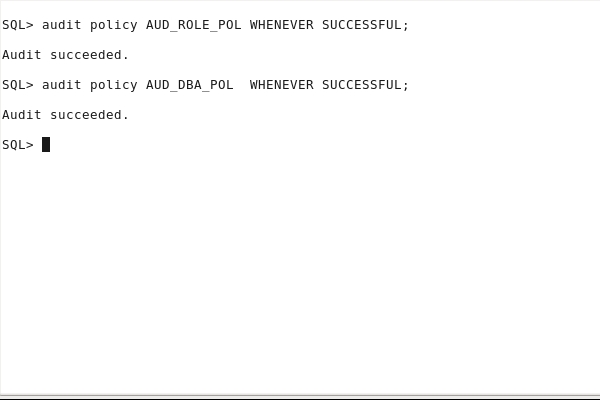
**create user DBA\_JUNIOR identified by oracle\_4U;  
grant DBA to DBA\_JUNIOR;**

**create audit policy aud\_dba\_pol   
  ROLES dba;**



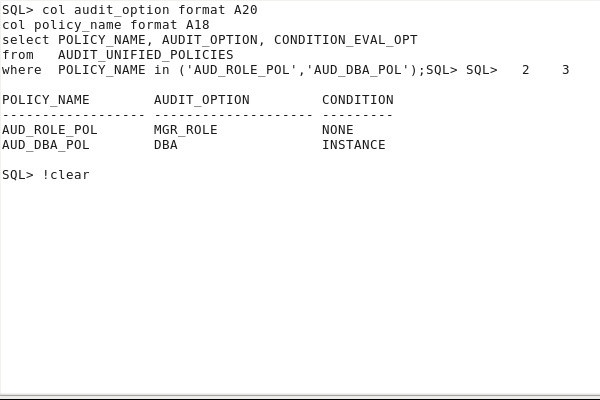
Enable the audit policies whenever the execution completed successfully only.

**audit policy AUD\_ROLE\_POL WHENEVER SUCCESSFUL;**  
**audit policy AUD\_DBA\_POL  WHENEVER SUCCESSFUL;**



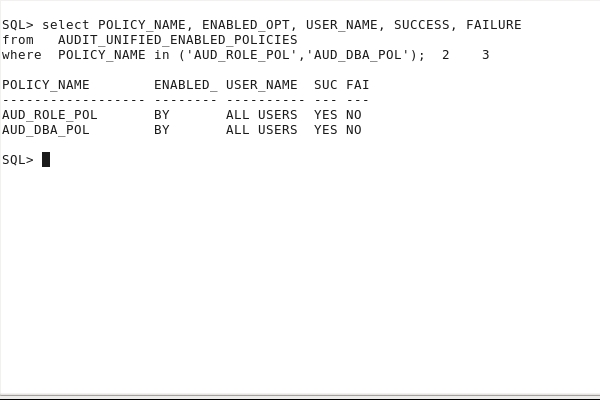
View the audit policy options.

**col audit\_option format A20  
col policy\_name format A18  
select POLICY\_NAME, AUDIT\_OPTION, CONDITION\_EVAL\_OPT  
from   AUDIT\_UNIFIED\_POLICIES  
where  POLICY\_NAME in ('AUD\_ROLE\_POL','AUD\_DBA\_POL');**



Verify that the audit policy is enabled.

**col user\_name format A10  
col policy\_name format A18  
select POLICY\_NAME, ENABLED\_OPT, USER\_NAME, SUCCESS, FAILURE  
from   AUDIT\_UNIFIED\_ENABLED\_POLICIES  
where  POLICY\_NAME in ('AUD\_ROLE\_POL','AUD\_DBA\_POL');**



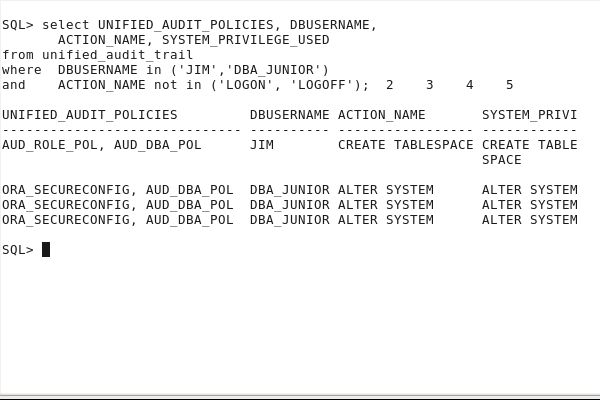
Perform an audited operation for both role type audited policies.

**connect jim/oracle\_4U   
create tablespace test datafile '/tmp/test01.dbf' size 10m;  
  
connect dba\_junior/oracle\_4U  
alter system set job\_queue\_processes=200;  
alter system set job\_queue\_processes=100;**



View the resulting audit data.

**connect system/oracle\_4U  
   
set pages 100  
col dbusername format A10  
col action\_name format A17  
col unified\_audit\_policies format A30  
col system\_privilege\_used format A12  
select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME,   
ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED,   
from unified\_audit\_trail  
where DBUSERNAME in ('JIM','DBA\_JUNIOR')  
and ACTION\_NAME not in ('LOGON', 'LOGOFF')  
and UNIFIED\_AUDIT\_POLICIES like '%AUD\_ROLE\_POL%'  
or UNIFIED\_AUDIT\_POLICIES like '%AUD\_DBA\_POL%');**



If the audited data is still in memory, flush the data to disk.

**exec SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

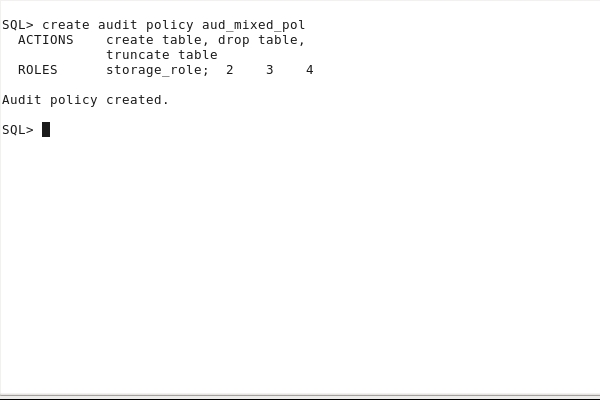
Now you can view the resulting audit data.

**select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME,   
       ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED    
from unified\_audit\_trail  
where  DBUSERNAME in ('JIM','DBA\_JUNIOR')  
and    ACTION\_NAME not in ('LOGON', 'LOGOFF')  
and    (UNIFIED\_AUDIT\_POLICIES like '%AUD\_ROLE\_POL%'  
        or UNIFIED\_AUDIT\_POLICIES like '%AUD\_DBA\_POL%');**

### Creating a Mixed Audit Policy

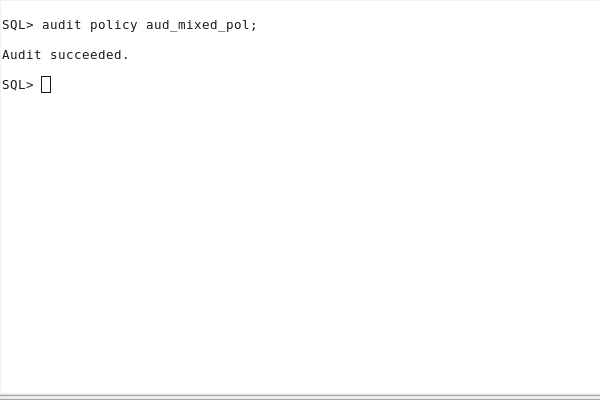
Create an audit policy that will audit all users while using the STORAGE\_ROLE role or performing any action related to tables.

**create role storage\_role;  
grant drop tablespace to storage\_role;  
grant storage\_role to dev;  
  
grant drop any table to jim;  
  
create audit policy aud\_mixed\_pol  
  ACTIONS    create table, drop table,   
             truncate table  
  ROLES      storage\_role;**



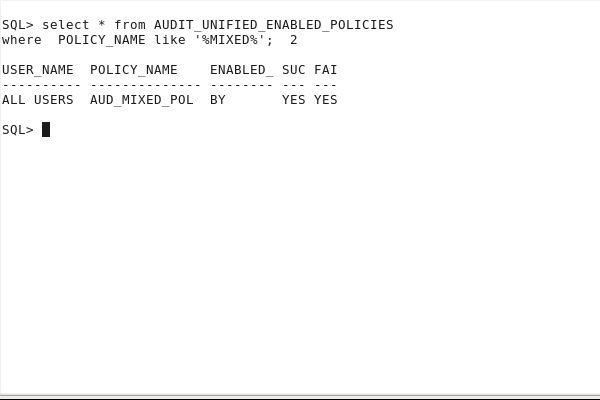
Enable the audit policy.

**audit policy aud\_mixed\_pol;**



Verify that the audit policy is enabled.

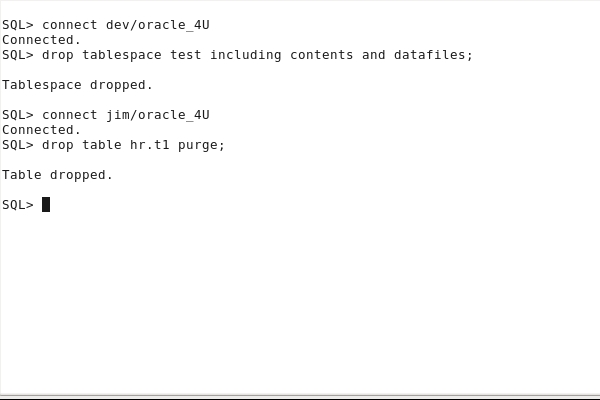
col user\_name format A10  
col policy\_name format A14  
select \* from AUDIT\_UNIFIED\_ENABLED\_POLICIES   
where  POLICY\_NAME like '%MIXED%';



Perform an operation.

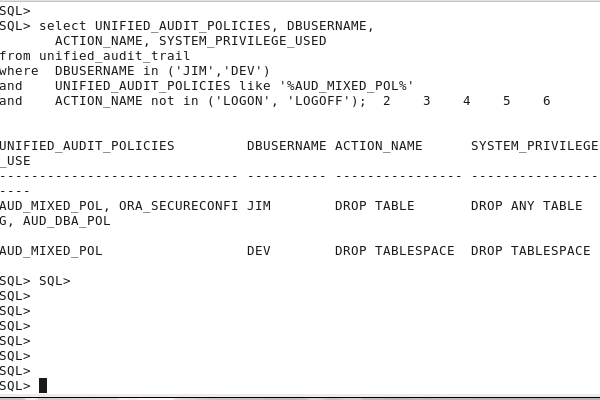
**connect dev/oracle\_4U   
drop tablespace test including contents and datafiles;**

**connect jim/oracle\_4U   
drop table hr.t1 purge;**



View the resulting audit data.

**connect system/oracle\_4U  
   
col action\_name format A16  
col policy\_name format A18  
col role format A10  
col system\_privilege\_used format A20  
select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME,   
       ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED    
from unified\_audit\_trail  
where  DBUSERNAME in ('JIM','DEV')  
and    UNIFIED\_AUDIT\_POLICIES like '%AUD\_MIXED\_POL%'  
and    ACTION\_NAME not in ('LOGON', 'LOGOFF');**



If the audited data is still in memory, flush the data to disk.

**exec SYS.DBMS\_AUDIT\_MGMT.FLUSH\_UNIFIED\_AUDIT\_TRAIL**

Now you can view the resulting audit data.

**sqlplus system/oracle\_4U**

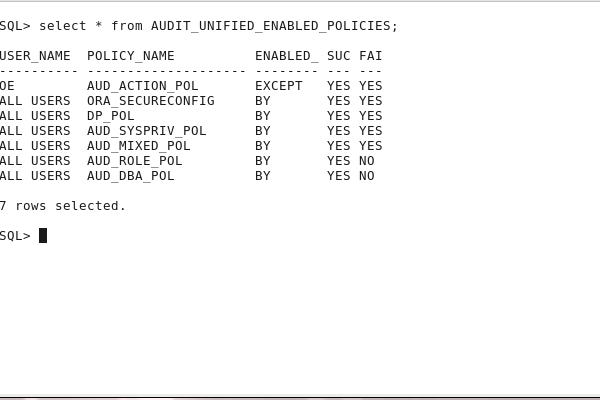
**col action\_name format A16  
col policy\_name format A18  
col role format A10  
col system\_privilege\_used format A20  
select UNIFIED\_AUDIT\_POLICIES, DBUSERNAME,   
       ACTION\_NAME, SYSTEM\_PRIVILEGE\_USED    
from unified\_audit\_trail  
where  DBUSERNAME in ('JIM','DEV')  
and    UNIFIED\_AUDIT\_POLICIES like '%AUD\_MIXED\_POL%'  
and    ACTION\_NAME not in ('LOGON', 'LOGOFF');**

## Disabling and Deleting Audit Policies

In this topic, you disable audit policies without dropping them, and then you drop audit policies.

Display the list of enabled audit policies.

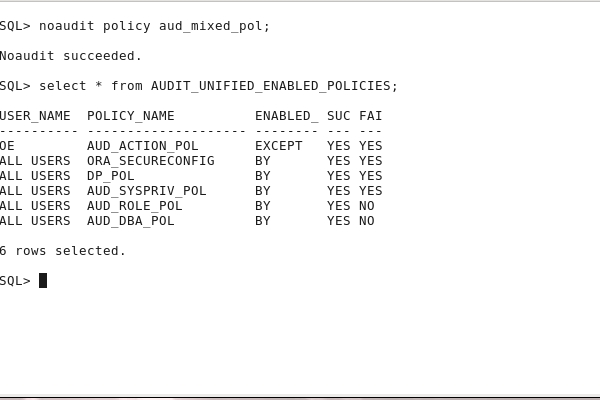
**connect / as sysdba  
col policy\_name format A20  
select \* from AUDIT\_UNIFIED\_ENABLED\_POLICIES;**



Disable the AUD\_MIXED\_POL audit policy.

**noaudit policy aud\_mixed\_pol;**

**select \* from AUDIT\_UNIFIED\_ENABLED\_POLICIES;**

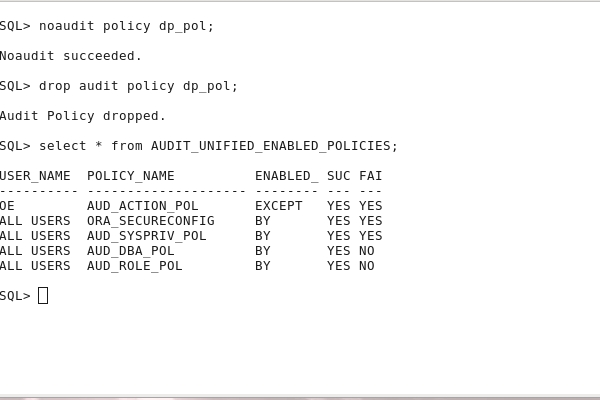


Drop the DP\_POL audit policy. You will see that an audit policy can only be dropped after being disabled.

**drop audit policy dp\_pol;**



**noaudit policy dp\_pol;  
drop audit policy dp\_pol;  
select \* from AUDIT\_UNIFIED\_ENABLED\_POLICIES;**

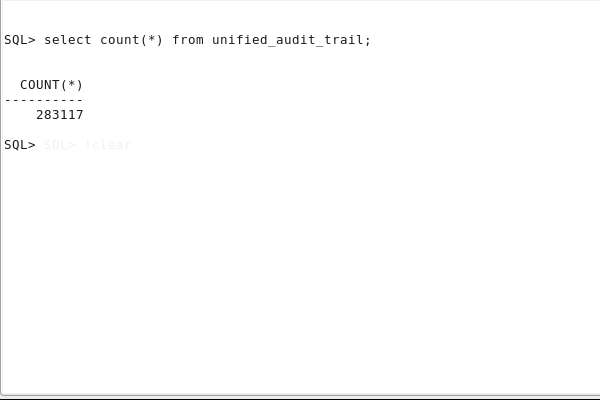
 

## Performing Audit Data Cleanup

In this topic, you clean up all audited data from AUDSYS tables stored in SYSAUX tablespace.

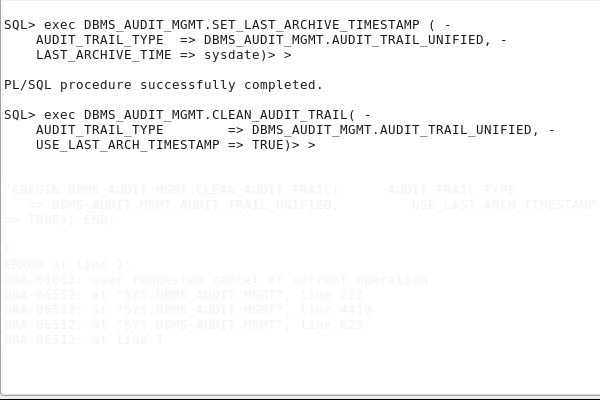
You can perform the cleanup manually.

**select count(\*) from unified\_audit\_trail;**



**exec DBMS\_AUDIT\_MGMT.SET\_LAST\_ARCHIVE\_TIMESTAMP ( -  
     AUDIT\_TRAIL\_TYPE  => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_UNIFIED, -  
     LAST\_ARCHIVE\_TIME => sysdate)**

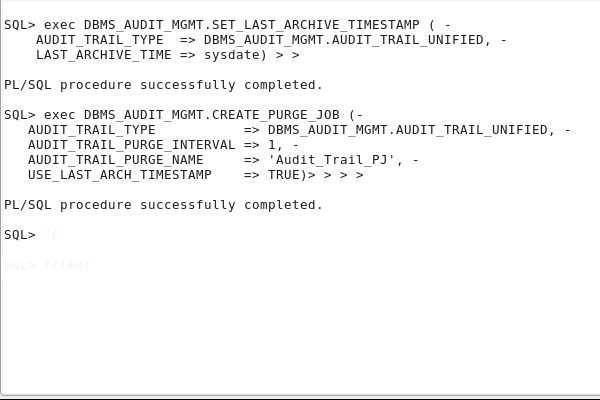
**exec DBMS\_AUDIT\_MGMT.CLEAN\_AUDIT\_TRAIL( -  
     AUDIT\_TRAIL\_TYPE        => DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_UNIFIED, -      
     USE\_LAST\_ARCH\_TIMESTAMP => TRUE)**



You can also schedule the cleanup.

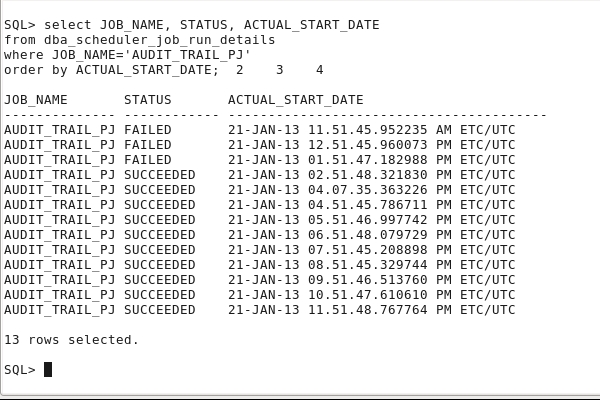
**exec DBMS\_AUDIT\_MGMT.SET\_LAST\_ARCHIVE\_TIMESTAMP ( -  
     AUDIT\_TRAIL\_TYPE = DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_UNIFIED, -  
     LAST\_ARCHIVE\_TIME = sysdate)**

**exec DBMS\_AUDIT\_MGMT.CREATE\_PURGE\_JOB (-  
     AUDIT\_TRAIL\_TYPE = DBMS\_AUDIT\_MGMT.AUDIT\_TRAIL\_UNIFIED, -  
     AUDIT\_TRAIL\_PURGE\_INTERVAL = 1, -  
     AUDIT\_TRAIL\_PURGE\_NAME = 'Audit\_Trail\_PJ', -  
     USE\_LAST\_ARCH\_TIMESTAMP = TRUE)**



View the cleanup job executions.

**col JOB\_NAME format A14  
col STATUS format A12  
col ACTUAL\_START\_DATE format A40  
  
select JOB\_NAME, STATUS, ACTUAL\_START\_DATE  
from dba\_scheduler\_job\_run\_details  
where JOB\_NAME='AUDIT\_TRAIL\_PJ'  
order by ACTUAL\_START\_DATE;**



Check if audit data has been purged.

**select count(\*) from unified\_audit\_trail;**

