**Practices for Lesson 5:**

**Auditing**

**Practices for Lesson 5**

**Practices Overview**

In the practices for this lesson, you enable unified audit, configure for Data Pump export

auditing, and audit export and RMAN operations. You then view the audited data in the

UNIFIED\_AUDIT\_TRAIL view.

**Practice 5-1: Enabling Unified Auditing**

**Overview**

In this practice, you enable unified auditing.

**Tasks**

1. Shut down all Oracle processes of all instances

a. Shut down the listener.

$ **. oraenv**

[ORACLE\_SID = [orcl] ? **orcl2**

The Oracle base remains unchanged with value /u01/app/oracle

$

$ **lsnrctl stop**

LSNRCTL for Linux: Version 12.1.0.0.2 - Production on 05-JUL-

2012 09:13:24

Copyright (c) 1991, 2012, Oracle. All rights reserved.

Connecting to

(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1521)))

The command completed successfully

$

b. Shut down all instances.

$ **ps -ef | grep pmon**

oracle 5111 1 0 Sep07 ? 00:00:31 ora\_pmon\_orcl

oracle 18211 1 0 Sep05 ? 00:00:53 ora\_pmon\_em12rep

oracle 25014 1 0 Sep07 ? 00:00:28 ora\_pmon\_cdb2

oracle 30114 29015 0 23:38 pts/3 00:00:00 grep pmon

$

1) Shut down the orcl2 instance.

$ **sqlplus / as sysdba**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining and Real Application

Testing options

SQL> **shutdown immediate**

Database closed.

Database dismounted.

ORACLE instance shut down.

SQL> **EXIT**

$

2) Shut down the cdb2 instance.

$ **. oraenv**

[ORACLE\_SID = [orcl2] ? **cdb2**

The Oracle base remains unchanged with value /u01/app/oracle

$

$ **sqlplus / as sysdba**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining and Real Application

Testing options

SQL> **shutdown immediate**

Database closed.

Database dismounted.

ORACLE instance shut down.

SQL> **EXIT**

$

3) Shut down the em12rep instance if you are using EM Cloud Control. Otherwise skip to Step 4.

a) Stop the OMS.

$ **cd /u01/app/oracle/product/middleware/oms**

$ **export OMS\_HOME=/u01/app/oracle/product/middleware/oms**

$ **$OMS\_HOME/bin/emctl stop oms**

Oracle Enterprise Manager Cloud Control 12c Release 2

Copyright (c) 1996, 2012 Oracle Corporation. All rights

reserved.

Stopping WebTier...

WebTier Successfully Stopped

Stopping Oracle Management Server...

Oracle Management Server Successfully Stopped

Oracle Management Server is Down

$

b) Shut down the repository database instance em12rep.

$ **. oraenv**

[ORACLE\_SID = [orcl] ? **orcl**

The Oracle base remains unchanged with value /u01/app/oracle

$

$ **sqlplus / as sysdba**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining and Real Application

Testing options

SQL> **shutdown immediate**

Database closed.

Database dismounted.

ORACLE instance shut down.

SQL> **EXIT**

$

4) Verify that all instances are down.

$ **ps -ef | grep pmon**

oracle 5165 13370 0 09:14 pts/0 00:00:00 grep pmon

$

2. Enable the Unified Audit option.

$ **cd $ORACLE\_HOME/rdbms/lib**

$ **make -f ins\_rdbms.mk uniaud\_on ioracle**

**ORACLE\_HOME=$ORACLE\_HOME**

/usr/bin/ar d

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/libknlopt.a

kzanang.o

/usr/bin/ar cr

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/libknlopt.a

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/kzaiang.o

chmod 755 /u01/app/oracle/product/12.1.0/dbhome\_1/bin

- Linking Oracle

rm -f /u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/oracle

/u01/app/oracle/product/12.1.0/dbhome\_1/bin/orald -o

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/oracle -m64 -z

noexecstack -L/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/

-L/u01/app/oracle/product/12.1.0/dbhome\_1/lib/ -

L/u01/app/oracle/product/12.1.0/dbhome\_1/lib/stubs/ -Wl,-E

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/opimai.o

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/ssoraed.o

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/ttcsoi.o -Wl,-

-whole-archive -lperfsrv12 -Wl,--no-whole-archive

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/nautab.o

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/naeet.o

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/naect.o

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/naedhs.o

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/config.o -

lserver12 -lodm12 -lcell12 -lnnet12 -lskgxp12 -lsnls12 -lnls12

-lcore12 -lsnls12 -lnls12 -lcore12 -lsnls12 -lnls12 -lxml12 -

lcore12 -lunls12 -lsnls12 -lnls12 -lcore12 -lnls12 -lclient12 -

lvsn12 -lcommon12 -lgeneric12 -lknlopt `if /usr/bin/ar tv

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/libknlopt.a |

grep xsyeolap.o > /dev/null 2>&1 ; then echo "-loraolap12" ; fi`

-lskjcx12 -lslax12 -lpls12 -lrt -lplp12 -lserver12 -lclient12

-lvsn12 -lcommon12 -lgeneric12 `if [ -f

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/libavserver12.a ] ;

then echo "-lavserver12" ; else echo "-lavstub12"; fi` `if [ -f

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/libavclient12.a ] ;

then echo "-lavclient12" ; fi` -lknlopt -lslax12 -lpls12 -lrt -

lplp12 -ljavavm12 -lserver12 -lwwg `cat

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/ldflags` -

lncrypt12 -lnsgr12 -lnzjs12 -ln12 -lnl12 -lnro12 `cat

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/ldflags` -

lncrypt12 -lnsgr12 -lnzjs12 -ln12 -lnl12 -lnnz12 -lzt12 -lztkg12

-lmm -lsnls12 -lnls12 -lcore12 -lsnls12 -lnls12 -lcore12 -

lsnls12 -lnls12 -lxml12 -lcore12 -lunls12 -lsnls12 -lnls12 -

lcore12 -lnls12 -lztkg12 `cat

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/ldflags` -

lncrypt12 -lnsgr12 -lnzjs12 -ln12 -lnl12 -lnro12 `cat

/u01/app/oracle/product/12.1.0/dbhome\_1/lib/ldflags` -

lncrypt12 -lnsgr12 -lnzjs12 -ln12 -lnl12 -lnnz12 -lzt12 -lztkg12

-lsnls12 -lnls12 -lcore12 -lsnls12 -lnls12 -lcore12 -lsnls12 -

lnls12 -lxml12 -lcore12 -lunls12 -lsnls12 -lnls12 -lcore12 -

lnls12 `if /usr/bin/ar tv

/u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/libknlopt.a |

grep "kxmnsd.o" > /dev/null 2>&1 ; then echo " " ; else echo "-

lordsdo12"; fi` -

L/u01/app/oracle/product/12.1.0/dbhome\_1/ctx/lib/ -lctxc12 -

lctx12 -lzx12 -lgx12 -lctx12 -lzx12 -lgx12 -lordimt12 -lclsra12

-ldbcfg12 -lhasgen12 -lskgxn2 -lnnz12 -lzt12 -lxml12 -locr12 -

locrb12 -locrutl12 -lhasgen12 -lskgxn2 -lnnz12 -lzt12 -lxml12 -

lgeneric12 -loraz -llzopro -lorabz2 -lipp\_z -lipp\_bz2 -

lippdcemerged -lippsemerged -lippdcmerged -lippsmerged -

lippcore -lippcpemerged -lippcpmerged -lsnls12 -lnls12 -

lcore12 -lsnls12 -lnls12 -lcore12 -lsnls12 -lnls12 -lxml12 -

lcore12 -lunls12 -lsnls12 -lnls12 -lcore12 -lnls12 -lsnls12 -

lunls12 -lsnls12 -lnls12 -lcore12 -lsnls12 -lnls12 -lcore12 -

lsnls12 -lnls12 -lxml12 -lcore12 -lunls12 -lsnls12 -lnls12 -

lcore12 -lnls12 -lasmclnt12 -lcommon12 -lcore12 -laio -lons

`cat /u01/app/oracle/product/12.1.0/dbhome\_1/lib/sysliblist` -

Wl,-rpath,/u01/app/oracle/product/12.1.0/dbhome\_1/lib -lm

`cat /u01/app/oracle/product/12.1.0/dbhome\_1/lib/sysliblist` -

ldl -lm -L/u01/app/oracle/product/12.1.0/dbhome\_1/lib

test ! -f /u01/app/oracle/product/12.1.0/dbhome\_1/bin/oracle ||\

mv -f

/u01/app/oracle/product/12.1.0/dbhome\_1/bin/oracle

/u01/app/oracle/product/12.1.0/dbhome\_1/bin/oracleO

mv /u01/app/oracle/product/12.1.0/dbhome\_1/rdbms/lib/oracle

/u01/app/oracle/product/12.1.0/dbhome\_1/bin/oracle

chmod 6751 /u01/app/oracle/product/12.1.0/dbhome\_1/bin/oracle

$

3. Restart the processes.

a. Restart the database orcl only.

$ **. oraenv**

[ORACLE\_SID = [cdb2] ? **orcl**

The Oracle base remains unchanged with value /u01/app/oracle

$

$ **sqlplus / as sysdba**

Connected to an idle instance.

SQL> **startup mount**

ORACLE instance started.

Total System Global Area 847630336 bytes

Fixed Size 2266072 bytes

Variable Size 557845544 bytes

Database Buffers 285212672 bytes

Redo Buffers 2306048 bytes

Database mounted.

SQL> **ALTER DATABASE ARCHIVELOG;**

Database altered.

SQL> **ALTER DATABASE OPEN;**

Database altered.

SQL> **EXIT**

$

You can see that the Unified Auditing option is enabled in the SQL\*Plus banner.

b. Restart the listener.

$ **lsnrctl start**

LSNRCTL for Linux: Version 12.1.0.0.2 - Production on 05-JUL-

2012 09:37:38

Copyright (c) 1991, 2012, Oracle. All rights reserved.

Starting /u01/app/oracle/product/12.1.0/dbhome\_1/bin/tnslsnr:

please wait...

TNSLSNR for Linux: Version 12.1.0.0.2 - Production

System parameter file is

/u01/app/oracle/product/12.1.0/dbhome\_1/network/admin/listener.o

ra

Log messages written to

/u01/app/oracle/diag/tnslsnr/host01/listener/alert/log.xml

Listening on:

(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))

Listening on:

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=host01.example.com)(PO

RT=1521)))

Connecting to

(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1521)))

STATUS of the LISTENER

------------------------

Alias LISTENER

Version TNSLSNR for Linux: Version 12.1.0.0.2

- Production

Start Date 05-JUL-2012 09:37:38

Uptime 0 days 0 hr. 0 min. 0 sec

Trace Level off

Security ON: Local OS Authentication

SNMP OFF

Listener Parameter File

/u01/app/oracle/product/12.1.0/dbhome\_1/network/admin/listener.o

ra

Listener Log File

/u01/app/oracle/diag/tnslsnr/host01/listener/alert/log.xml

Listening Endpoints Summary...

(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1521)))

(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=host01.example.com)(PO

RT=1521)))

The listener supports no services

The command completed successfully

$

**Practice 5-2: Auditing Data Pump Export**

**Overview**

In this practice, you create an audit policy to audit Data Pump export operations. Then you will

view the audited data after the export is completed.

**Assumptions**

Practice 5-1 successfully enabled unified audit.

**Tasks**

1. Create a DP\_POLICY for the component Data Pump, and more specifically for export

operations.

$ **sqlplus system/password**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining, Real Application

Testing

and Unified Auditing options

SQL> **create audit policy DP\_POL actions COMPONENT=datapump**

**export;**

Audit policy created.

SQL>

2. Enable the audit policy.

SQL> **audit policy DP\_POL;**

Audit succeeded.

SQL>

3. Verify that the policy exists.

SQL> **col user\_name format A10**

SQL> **col policy\_name format A10**

SQL> **SELECT \* FROM AUDIT\_UNIFIED\_ENABLED\_POLICIES**

2 **where POLICY\_NAME like '%DP%';**

USER\_NAME POLICY\_NAM ENABLED\_ SUC FAI

---------- ---------- -------- --- ---

ALL USERS DP\_ POL BY YES YES

SQL> **EXIT**

$

4. Perform an export operation. Before exporting, ensure that the dump file does not exist;

else, the export command will fail.

$ **rm /u01/app/oracle/admin/orcl/dpdump/HR\_tables.dmp**

rm: cannot remove

`/u01/app/oracle/admin/orcl/dpdump/HR\_tables.dmp': No such file

or directory

$ **expdp system/password dumpfile=HR\_tables tables=HR.EMPLOYEES**

Connected to: Oracle Database 12c Enterprise Edition Release

12.1.0.0.2 - 64bit Production

With the Partitioning, OLAP, Data Mining, Real Application

Testing

and Unified Auditing options

Starting "SYSTEM"."SYS\_EXPORT\_TABLE\_01": system/\*\*\*\*\*\*\*\*

…………..

Processing object type

TABLE\_EXPORT/TABLE/GRANT/OWNER\_GRANT/OBJECT\_GRANT

Processing object type TABLE\_EXPORT/TABLE/COMMENT

Processing object type TABLE\_EXPORT/TABLE/INDEX/INDEX

Processing object type TABLE\_EXPORT/TABLE/CONSTRAINT/CONSTRAINT

Processing object type

TABLE\_EXPORT/TABLE/INDEX/STATISTICS/INDEX\_STATISTICS

Processing object type

TABLE\_EXPORT/TABLE/CONSTRAINT/REF\_CONSTRAINT

Processing object type TABLE\_EXPORT/TABLE/TRIGGER

Processing object type

TABLE\_EXPORT/TABLE/STATISTICS/TABLE\_STATISTICS

Processing object type TABLE\_EXPORT/TABLE/STATISTICS/MARKER

. . exported "HR"."EMPLOYEES" 17.06

KB 107 rows

Master table "SYSTEM"."SYS\_EXPORT\_TABLE\_01" successfully

loaded/unloaded

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Dump file set for SYSTEM.SYS\_EXPORT\_TABLE\_01 is:

/u01/app/oracle/admin/orcl/dpdump/HR\_tables.dmp

Job "SYSTEM"."SYS\_EXPORT\_TABLE\_01" successfully completed at Thu

Jul 5 10:08:37 2012 elapsed 0 00:00:23

$

5. View the resulting audit data. If the result shows no rows, then proceed with step 6, else

you will get the result of step 7.

$ **sqlplus system/password**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining, Real Application

Testing and Unified Auditing options

SQL> **select DBUSERNAME, DP\_TEXT\_PARAMETERS1,**

2 **DP\_BOOLEAN\_PARAMETERS1**

3 **from UNIFIED\_AUDIT\_TRAIL**

4 **where DP\_TEXT\_PARAMETERS1 is not null;**

no rows selected

SQL>

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

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

PL/SQL procedure successfully completed.

SQL>

7. View the resulting audit data.

SQL> **/**

DBUSERNAME

------------------------------

DP\_TEXT\_PARAMETERS1

--------------------------------------------------------------

DP\_BOOLEAN\_PARAMETERS1

--------------------------------------------------------------

**SYSTEM**

MASTER TABLE: "SYSTEM"."SYS\_EXPORT\_TABLE\_01" , JOB\_TYPE:

EXPORT, METADATA\_JOB\_M

ODE: TABLE\_EXPORT, JOB VERSION: 12.0.0.0.0, ACCESS METHOD:

AUTOMATIC, DATA OPTIO

NS: 0, DUMPER DIRECTORY: NULL REMOTE LINK: NULL, TABLE EXISTS:

NULL, PARTITION

OPTIONS: NONE

MASTER\_ONLY: FALSE, DATA\_ONLY: FALSE, METADATA\_ONLY: FALSE,

DUMPFILE\_PRESENT: TR

UE, JOB\_RESTARTED: FALSE

SQL> **exit**

$

**Practice 5-3: Auditing RMAN Backups**

In this practice, you perform RMAN backups. Then you will view the audited data after RMAN

backups are completed. You do not have to create any audit policy for RMAN operations.

RMAN is by default audited.

**Assumptions**

Practice 9-1 successfully enabled unified audit.

**Tasks**

1. Perform a RMAN backup of the USERS tablespace.

$ **rman target /**

connected to target database: ORCL2(DBID=1315477536)

RMAN> **backup tablespace USERS;**

Starting backup at 05-JUL-12

using target database control file instead of recovery catalog

allocated channel: ORA\_DISK\_1

channel ORA\_DISK\_1: SID=52 device type=DISK

channel ORA\_DISK\_1: starting full datafile backup set

channel ORA\_DISK\_1: specifying datafile(s) in backup set

input datafile file number=00006

name/u01/app/oracle/oradata/orcl/users01.dbf

channel ORA\_DISK\_1: starting piece 1 at 05-JUL-12

channel ORA\_DISK\_1: finished piece 1 at 05-JUL-12

piece

handle=/u01/app/oracle/fast\_recovery\_area/ORCL/backupset/2012\_07

\_05/o1\_mf\_nnndf\_TAG20120705T102453\_7zbtvp2x\_.bkp

tag=TAG20120705T102453 comment=NONE

channel ORA\_DISK\_1: backup set complete, elapsed time: 00:00:01

Finished backup at 05-JUL-12

RMAN> **exit;**

Recovery Manager complete.

$

2. Perform a restore and recover after removing the USERS tablespace file.

a. Find the data file name of the USERS tablespace and remove the file.

$ **sqlplus / as sysdba**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Advanced Analytics, Real

Application Testing and Unified Auditing options

SQL> **select name from v$datafile;**

NAME

--------------------------------------------------------------

/u01/app/oracle/oradata/orcl/system01.dbf

/u01/app/oracle/oradata/orcl/example01.dbf

/u01/app/oracle/oradata/orcl/sysaux01.dbf

/u01/app/oracle/oradata/orcl/undotbs01.dbf

/u01/app/oracle/oradata/orcl/users01.dbf

SQL> **!rm /u01/app/oracle/oradata/orcl/users01.dbf**

SQL>

b. Put the tablespace OFFLINE.

SQL> **alter tablespace users offline immediate;**

Tablespace altered.

SQL> **exit**

$

c. Restore and recover the data file.

$ **rman target /**

connected to target database: ORCL2(DBID=1315477536)

RMAN> **restore tablespace USERS;**

Starting restore at 05-JUL-12

using target database control file instead of recovery catalog

allocated channel: ORA\_DISK\_1

channel ORA\_DISK\_1: SID=59 device type=DISK

channel ORA\_DISK\_1: starting datafile backup set restore

channel ORA\_DISK\_1: specifying datafile(s) to restore from

backup set

channel ORA\_DISK\_1: restoring datafile 00006 to

/u01/app/oracle/oradata/orcl/users01.dbf

channel ORA\_DISK\_1: reading from backup piece

/u01/app/oracle/fast\_recovery\_area/ORCL/backupset/2012\_07\_05/o1\_

mf\_nnndf\_TAG20120705T102453\_7zbtvp2x\_.bkp

channel ORA\_DISK\_1: piece

handle=/u01/app/oracle/fast\_recovery\_area/ORCL/backupset/2012\_07

\_05/o1\_mf\_nnndf\_TAG20120705T102453\_7zbtvp2x\_.bkp

tag=TAG20120705T102453

channel ORA\_DISK\_1: restored backup piece 1

channel ORA\_DISK\_1: restore complete, elapsed time: 00:00:01

Finished restore at 05-JUL-12

RMAN> **recover tablespace USERS;**

Starting recover at 05-JUL-12

using channel ORA\_DISK\_1

starting media recovery

media recovery complete, elapsed time: 00:00:00

Finished recover at 05-JUL-12

RMAN> **exit;**

$

d. Put the tablespace USERS back online.

$ **sqlplus system/password**

Connected to:

Oracle Database 12c Enterprise Edition Release 12.1.0.0.2 -

64bit Production

With the Partitioning, OLAP, Data Mining, Real Application

Testing and Unified Auditing options

SQL> **alter tablespace USERS online;**

Tablespace altered.

SQL>

3. View the resulting audit data. If the result shows no rows, then proceed with step 4, else

you will get the result of step 5.

SQL> **select DBUSERNAME, RMAN\_OPERATION**

2 **from UNIFIED\_AUDIT\_TRAIL**

3 **where RMAN\_OPERATION is not null;**

no rows selected

SQL>

4. If the audited data is still in memory, flush the data to disk. But it is possible that the audit

data is already flushed in the audit tables.

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

PL/SQL procedure successfully completed.

5. View the resulting audit data.

SQL> **/**

DBUSERNAME RMAN\_OPERATION

------------------------ --------------------

SYS Recover

SYS Restore

SYS Backup

SQL> **exit**

$