**TDE for ACEDQDEV and APMPBTD dbs**

DBA : John Semencar, Arun Tripathi Date : 8/16/2023

Db names : ACEDQDEV, APMPBTD

Db server : xcrxdbw1d

NOTES

=====

this is for single instance, not multi-tenant.

The keystore file "ewallet.p12" lives in the wallet/keystore location.

The auto\_login file "cwallet.sso" lives in the wallet/keystore location.

The wallet bkup files live in the wallet/keystore location.

sqlnet.ora entries for tde are deprecated.

use WALLET\_ROOT and TDE\_CONFIGURATION parms instead.

the “tde” directory is automatically created under WALLET\_ROOT if it does not already exist.

\*\*\* CVSHealth standards:

\*\*\* - wallet location for tde --------> $ORACLE\_BASE/admin/wallet/tde/<DBNAME>

\*\*\* - use AES256 encryption algorithm

In a nustshell:

1. Create a wallet/keystore location

2. Set wallet db parms

3. Create ZOPA-based keystore

4. Open the keystore

5. Set the key

6. Create auto-login keystore

7. Bounce the db

8. Check for autologin

9. Create encrypted tablespace to move or create tables.

**DO IT**

=====

1. Create a wallet/keystore location to hold the master encryption key.

\*\*\* ACEDQDEV \*\*\*

$> mkdir -p $ORACLE\_BASE/admin/wallet/tde/ACEDQDEV

\*\*\* APMPBTD \*\*\*

$> mkdir -p $ORACLE\_BASE/admin/wallet/tde/APMPBTD

2. setup wallet/tde db parms. (must hardcode ORACLE\_BASE)

\*\*\* ACEDQDEV \*\*\*

SQL> alter system set wallet\_root='/orahome/u01/app/oracle/admin/wallet/tde/ACEDQDEV' scope=spfile ;

$> srvctl stop database -d ACEDQDEV\_xcrxdbw1d

$> srvctl start database -d ACEDQDEV\_xcrxdbw1d

SQL> alter system set tde\_configuration ="KEYSTORE\_CONFIGURATION = FILE" scope = both ;

\*\*\* APMPBTD \*\*\*

SQL> alter system set wallet\_root='/orahome/u01/app/oracle/admin/wallet/tde/APMPBTD' scope=spfile ;

$> srvctl stop database -d APMPBTD\_xcrxdbw1d

$> srvctl start database -d APMPBTD\_xcrxdbw1d

SQL> alter system set tde\_configuration ="KEYSTORE\_CONFIGURATION = FILE" scope = both ;

3. Create a ZOPA-based keystore.

( this will create a file "ewallet.p12", which is the keystore )

\*\*\* ACEDQDEV \*\*\*

SQL> administer key management create keystore

'$ORACLE\_BASE/admin/wallet/tde/ACEDQDEV' identified by somePW ;

\*\*\* APMPBTD \*\*\*

SQL> administer key management create keystore

'$ORACLE\_BASE/admin/wallet/tde/APMPBTD' identified by somePW ;

4. Open the keystore.

SQL> administer key management set keystore open identified by somePW ;

5. Set the key.

-- check for key

SQL> select con\_id, key\_id from v$encryption\_keys ;

-- activate and bkup the key

SQL> administer key management set key identified by somePW with bkup ;

-- check for key

SQL> select con\_id, key\_id from v$encryption\_keys ;

SQL> select \* from v$encryption\_wallet ;

6. Create an auto-login keystore.

( this will create a file "cwallet.sso" )

\*\*\* ACEDQDEV \*\*\*

SQL> administer key management create auto\_login keystore from keystore

'$ORACLE\_BASE/admin/wallet/tde/ACEDQDEV' identified by somePW ;

SQL> select \* from v$encryption\_wallet ;

\*\*\* APMPBTD \*\*\*

SQL> administer key management create auto\_login keystore from keystore

'$ORACLE\_BASE/admin/wallet/tde/APMPBTD' identified by somePW ;

SQL> select \* from v$encryption\_wallet ;

\*\*\* Do not remove the PKCS#12 wallet (ewallet.p12 file) after you create the auto login keystore (.sso file).

\*\*\* You must have the PKCS#12 wallet to regenerate or rekey the TDE master encryption key in the future.

7. Bounce the db.

8. Check for auto login :

SQL> select \* from v$encryption\_wallet ;

9. Create an encrypted tablespace.

\*\*\* ACEDQDEV \*\*\*

SQL> create tablespace TACEDQUAL\_ENCRYPT

datafile '+DATA\_01'

size 15g

encryption using 'AES256'

default storage(encrypt) ;

SQL> select tablespace\_name, encrypted from dba\_tablespaces where encrypted='YES' ;

\*\*\* APMPBTD \*\*\*

SQL> create tablespace TAETNAADHOC\_ENCRYPT

datafile '+DATA\_01'

size 7g

encryption using 'AES256'

default storage(encrypt) ;

SQL> select tablespace\_name, encrypted from dba\_tablespaces where encrypted='YES' ;

10. Move tables/indexes containing restricted data to the encrypted tablespace.

\*\*\* ACEDQDEV \*\*\*

SQL> alter table acedqual.ADMIN\_CTRLFRMT\_ERROR move tablespace TACEDQUAL\_ENCRYPT

SQL> alter table acedqual.ADMIN\_DM\_OUTPUT move tablespace TACEDQUAL\_ENCRYPT

SQL> alter table acedqual.ADMIN\_SENT move tablespace TACEDQUAL\_ENCRYPT

SQL> alter index acedqual.ADMIN\_SENT rebuild tablespace TACEDQUAL\_ENCRYPT

\*\*\* APMPBTD \*\*\*

SQL> alter table aetnaadhoc.HMOE\_ACT\_MED\_MEMBER\_LOAD\_CVS move

tablespace TAETNAADHOC\_ENCRYPT

SQL> alter table aetnaadhoc.HMOE\_ACT\_MED\_MEMBER\_LOAD\_1127 move

tablespace TAETNAADHOC\_ENCRYPT

\*\*\* no indexes to encrypt in APMPBTD \*\*\*

the end...