How To Generate A New Master Encryption Key for the TDE [ID 445147.1]

Modified 22-FEB-2012 *Type* HOWTO *Status* PUBLISHED

In this Document

Applies to:

Advanced Networking Option - Version: 10.2.0.3 to 11.2.0.2 - Release: 10.2 to 11.2
Information in this document applies to any platform.
Checked for relevance on 11-Feb-2011

Goal

In order to get the data inserted as encrypted into a table Oracle uses a table encryption key which is unique for each table of the database. All the table encryption keys are encrypted using a master key and stored within the data dictionary. The master key is stored outside of the database into a wallet. The wallet can be either a file or a Hardware Security Module(HSM) . Sometimes when the master key has been compromised it is needed to generate a new master key.

Solution

The statements used to generate a new master key are :

```
alter system set encryption key identified by "oracle1"; -- when using a file

alter system set encryption key identified by usr:passwd; -- when using HSM(this is not available in 10gR2)
```

To check whether a new master key was generated dump the contents of the wallet before and after the operation:

```
[oracle@seclin4 wallet]$ orapki wallet display -wallet .-pwd welcome1
Oracle PKI Tool : Version 11.2.0.2.0 - Production
Copyright (c) 2004, 2010, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
Subject: CN=oracle
User Certificates:
Oracle Secret Store entries:
ORACLE.SECURITY.DB.ENCRYPTION.AV8kySrjGU/rv4vxZLV9/kAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.AXUWrqkVHU9LvysE2PqARpwAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.MASTERKEY
ORACLE.SECURITY.TS.ENCRYPTION.BTJ9EEoIi7O8MokUyaU1SmMCAwAAAAAAAAAAAAAAAAAAAAAAAAAA
Trusted Certificates:
[oracle@seclin4 wallet]$ sqlplus / as sysdba

SQL*Plus: Release 11.2.0.2.0 Production on Wed Feb 22 15:02:48 2012

Copyright (c) 1982, 2010, Oracle. All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.2.0 - 64bit Production
With the Partitioning, Oracle Label Security, OLAP, Data Mining
```

+/- Rate this document

```
and Real Application Testing options

SQL> alter system set encryption key identified by "welcome1";

System altered.

SQL> ! orapki wallet display -wallet . -pwd welcome1
Oracle PKI Tool : Version 11.2.0.2.0 - Production
Copyright (c) 2004, 2010, Oracle and/or its affiliates. All rights reserved.

Requested Certificates:
Subject: CN=oracle
User Certificates:
Oracle Secret Store entries:
ORACLE.SECURITY.DB.ENCRYPTION.AV8kySrjGU/rv4vxZLV9/kAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.AVdps8EplE9Svy/okCRsTNMAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.AXUWrqkVHU9LvysE2PqARpwAAAAAAAAAAAAAAAAAAAAAAAAAAAAA --> This is the new Master Key
ORACLE.SECURITY.DB.ENCRYPTION.MASTERKEY
ORACLE.SECURITY.TS.ENCRYPTION.BTJ9EEoIi7O8MokUyaU1SmMCAwAAAAAAAAAAAAAAAAAAAAAAAAAA
Trusted Certificates:
```

When changing the master key it is recommended to :

1) Backup the database and the wallet file

2) Use the correct wallet password in the IDENTIFIED BY clause:

```
SQL> alter system set wallet open identified by "oracle1";

System altered.

SQL> alter system set encryption key identified by "oracle1234";
alter system set encryption key identified by "oracle1234"
*
ERROR at line 1:
ORA-28353: failed to open wallet

SQL> alter system set wallet open identified by "oracle1";

System altered.
```

The second command failed because a wrong password was used to access the wallet. The value specified via the IDENTIFIED BY is the password of the wallet and not the Master Key. Wallet's password can be changed using OWM.

3) Check the permissions of the wallet file. The owner of the Oracle binaries should be able to write the file. If the wallet is not accessible while changing the master key then the encrypted data may be lost.

Observations:

1) It is possible that more databases are sharing the same wallet file. Whenever one of the databases recreates it's master key the other databases will keep using their own master keys, which are stored within the same wallet file.

If the master keys are stored within a wallet file then running the above statement several times will increase the size of the ***ewallet.p12*** file. On average every 100 master keys are consuming 26KB. Up to 10.2.0.3 the wallet file size is limited to 65KB. Any attempt to regenerate the master key after this limit has been passed will end up with the following error :

```
alter system set encryption key identified by "welcome1"
*
```

```
ERROR at line 1:
ORA-00600: internal error code, arguments: [ztsmstore failed],
[18446744073709550614], [], [], [], [], [], []
```

As of 10.2.0.4 a wallet can grow up to 4GB. Since 100 rekeys generate 26KB if we keep on rekeying every single day we can do it for a very long period(more than 500 years).

2) The auto login wallet (the cwallet.sso file) is automatically updated with the latest keys:

```
SQL> alter system set encryption key identified by "welcome1";

System altered.

SQL> ! ls -ltr
total 16
-rw-r--r-- 1 oracle oinstall 2365 Feb 22 15:11 ewallet.p12
-rw------- 1 oracle oinstall 2442 Feb 22 15:11 cwallet.sso

SQL> alter system set encryption key identified by "welcome1";

System altered.

SQL> ! ls -ltr
total 16
-rw-r--r-- 1 oracle oinstall 2629 Feb 22 15:11 ewallet.p12
-rw------- 1 oracle oinstall 2706 Feb 22 15:11 cwallet.sso

SQL>
```

References

BUG:5985413 - ORA-00600[ZTSMSTORE FAILED] DURING CHANGE OF TDE MASTER KEY
BUG:6161304 - FAILED TO OPEN WALLET WHEN TRYING TO REKEY THE MASTER KEY
NOTE:317311.1 - 10g R2 New Feature TDE : Transparent Data Encryption

Related

Products

- Oracle Database Products > Oracle Database > Net Services > Advanced Networking Option

Keywords

DATA DICTIONARY; ENCRYPTION KEY; OWM; PASSWORD; SECURITY.RDF

Errors

ORA-600[ZTSMSTORE FAILED]; ORA-28353; ZTSMSTORE FAILED

Back to top