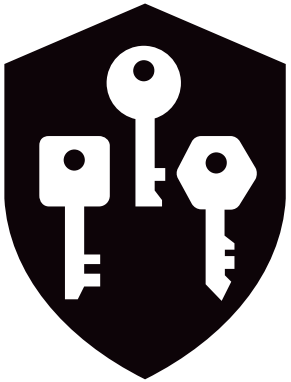


ORACLE
TRANSPARENT DATA ENCRYPTION

(TDE)

EM AMBIENTES

ORACLE 19c

Eu dedico essa palestra ao maior bem da minha vida, meu filho.

O Pai te ama!

MARTIM S. M. NOGUEIRA

JOAO NOGUEIRA - JN

Sou um professional com mais de 10 anos de experiência em banco de dados. Implementações de diversos Projetos envolvendo a camada de segurança da informação com Oracle Advanced Security:

Oracle Database Vault.
Oracle Database Firewall.
Oracle Audit Vault.
Oracle Database Masking e Subsetting.
Oracle Advanced Security (OAS) .
Oracle Redaction.
Data Safe
Cloud Guard
WAF

JOAO NOGUEIRA

CERTIFICAÇÕES

ORACLE
Certified Expert
Oracle Database 12*c*: Oracle RAC and Oracle Grid Infrastructure Administrator

ORACLE
EXADATA ADMINISTRATION

ORACLE
Certified Specialist
Oracle Exadata 11g Certified Implementation Specialist

ORACLE
Certified Expert
Oracle Database SQL

ORACLE
Certified Professional
Oracle Database 12*c* Administrator

ORACLE
Certified Professional

ORACLE
Certified Expert
Oracle Database 11*g* Performance Tuning

ORACLE
Certified Professional
Oracle Database 12*c* Administrator

ORACLE
Certified Professional
Database Cloud Administrator

ORACLE
Certified Associate
Oracle Database 11*g* Administrator

ORACLE
Certified Professional
Oracle Database 11*g* Administrator

ORACLE
Certified
Associate
Oracle Cloud Infrastructure Architect
2019

ORACLE
Certified Expert
Oracle Database 12*c* Performance Management and Tuning

ORACLE
Certified Expert

ORACLE
Certified Specialist

O QUE SERÁ APRESENTADO

TDE
ORACLE 19C

1 - INTRODUÇÃO - TRANSPARENT DATA ENCRYPTION (TDE)

2 - COMO CONFIGURAR O TDE NO 19C (OVERVIEW POR TABLESPACE)

3 - PARÂMETRO - ENCRYPT_NEW_TABLESPACES

4 - CRIPTOGRAFIA POR COLUNA

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

6 - BÔNUS – ORACLE KEY VAULT

INTRODUÇÃO TRANSPARENT DATA ENCRYPTION (ORACLE TDE)

Segurança de banco de dados

1- INTRODUÇÃO - TRANSPARENT DATA ENCRYPTION (TDE)

TDE
ORACLE 19C

- **Essa tecnologia Oracle TDE é muito importante na camada de segurança da informação. Muito bem endereçada para atender os requisitos de SOX,PCI, compliances e LGPD.....**

- **O Oracle TDE como a nome já diz, e totalmente transparente para aplicação, não é necessário ajustar nada do lado da aplicação ou instalar qualquer agente. O TDE é uma "feature" do Advanced Security, para o banco de dados Oracle e Mysql (Enterprise).**

- **A Transparent Data Encryption (TDE) permite criptografar dados confidenciais armazenados em tabelas e ou tablespaces.**

Mentalidade voltada à segurança

1- INTRODUÇÃO - TRANSPARENT DATA ENCRYPTION (TDE)

TDE
ORACLE 19C

- **Para usar o TDE, não precisamos dos privilégios SYSKM ou ADMINISTER KEY MANAGMENT. Somente para configuração e administração das master key.**

  Para trabalhar com TDE precisamos apenas dos grants, abaixo:

  CREATE TABLE
  ALTER TABLE
  CREATE TABLESPACE
  ALTER TABLESPACE.

- **Podemos criptografar os dados sensíveis no nível de “column” ou “tablespace”.**

- **A criptografia de “Tablespace” tem a vantagem de criptografar em massa e o caching para fornecer desempenho.**

COMO CONFIGURAR O TDE ORACLE 19C

Segurança de banco de dados

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

ETAPAS – “STEP BY STEP” para configurar o TDE no 19c (TABLESPACE)

01 – Configurando Wallet_Root e tde_configuration

02 – Criando o password do TDE

03 – Abrindo o “Keystore”

04 – Implementando “autologin”

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

01 – Configurando Wallet_Root e tde_configuration

```
[oracle@hol ~]$ mkdir -p /home/oracle/orcl/encryption_wallet/
[oracle@hol ~]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Thu Jun 15 23:30:51 2023
Version 19.9.0.0.0

Copyright (c) 1982, 2020, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.9.0.0.0

SQL> alter system set wallet_root='/home/oracle/orcl/encryption_wallet/' scope=spfile;
```

```
SQL> alter system set tde_configuration="keystore_configuration=file";

System altered.

SQL> show parameters tde_configuration

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
tde_configuration                    string      keystore_configuration=file
```

```
show parameter wallet_root;
show parameter tde_configuration;
NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------------------------
wallet_root                          string      /home/oracle/orcl/encryption_wallet/
tde_configuration                    string      keystore_configuration=file
```

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

02 – Criando o password do TDE

```
SQL> administer key management create keystore identified by SoAlegria##2019;

keystore altered.

SQL> !ls -lorth /home/oracle/orcl/encryption_wallet/
total 0
drwxr-x---. 2 oracle 25 Jun 15 23:54 tde

SQL> !ls -lorth /home/oracle/orcl/encryption_wallet/tde
total 4.0K
-rw-------. 1 oracle 2.5K Jun 15 23:54 ewallet.p12
```

```
SQL> set pages 400 lines 300;
SQL> select * from v$ENCRYPTION_WALLET;

WRL_TYPE
--------------------
WRL_PARAMETER
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
STATUS                         WALLET_TYPE          WALLET_OR KEYSTORE FULLY_BAC
------------------------------ -------------------- --------- -------- ---------
FILE
/home/oracle/orcl/encryption_wallet//tde/
CLOSED                         UNKNOWN              SINGLE    NONE     UNDEFINED
```

Podemos notar na tela acima, que o wallet encontra-se fechado no primeiro momento. Vamos abrir e configurar o backup nos próximos slides.

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

02 - Criando o password do TDE

```
SQL> administer key management set keystore open identified by SoAlegria##2019 container=all;

keystore altered.

SQL>  select * from v$ENCRYPTION_WALLET;

WRL_TYPE             WRL_PARAMETER
     STATUS                         WALLET_TYPE          WALLET_OR KEYSTORE FULLY_BAC     CON_
-------------------- --------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
FILE                 /home/oracle/orcl/encryption_wallet//tde/
     OPEN_NO_MASTER_KEY      PASSWORD             SINGLE     NONE      UNDEFINED          1
```

Mesmo abrindo com a chave master o wallet, ficará com status de “Open_no_master_key”. No próximo slide, vamos abrir e configurar o backup.

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

03 – Abrindo o “Keystore”

```
SQL> administer key management set key using tag 'masterkeyTDE' identified by SoAlegria##2019 with backup using 'masterkeybackupTDE';

keystore altered.

SQL> select * from v$ENCRYPTION_WALLET;

WRL_TYPE             WRL_PARAMETER
     STATUS                         WALLET_TYPE          WALLET_OR KEYSTORE FULLY_BAC     CON_ID
-------------------- ------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
```

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

04 – Implementando “auto-login”

```
SQL> administer key management create  auto_login keystore from keystore identified by SoAlegria##2019;

keystore altered.

SQL> select * from v$ENCRYPTION_WALLET;

WRL_TYPE             WRL_PARAMETER
     STATUS                         WALLET_TYPE          WALLET_OR KEYSTORE FULLY_BAC     CON_ID
-------------------- ------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
------------------------------------------------------------------------------------------------------------------------
FILE                 /home/oracle/orcl/encryption_wallet//tde/
     OPEN                           AUTOLOGIN            SINGLE     NONE      NO                    1
FILE
```

2 - COMO CONFIGURAR O TDE NO 19C

TDE
ORACLE 19C

Validando o certificado ewallet

```
[oracle@orcl03 tde]$ orapki wallet display -wallet ewallet.p12
Oracle PKI Tool Release 19.0.0.0.0 - Production
Version 19.4.0.0.0
Copyright (c) 2004, 2023, Oracle and/or its affiliates. All rights reserved.

Enter wallet password:
Requested Certificates:
Subject:        CN=oracle
User Certificates:
Oracle Secret Store entries:
ORACLE.SECURITY.DB.ENCRYPTION.ARvv0DoVGE9Vv17Y0ekfhZcAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.ASUQFLD7fk8qv0VzROaM72AAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.DB.ENCRYPTION.MASTERKEY
ORACLE.SECURITY.ID.ENCRYPTION.
ORACLE.SECURITY.KB.ENCRYPTION.
ORACLE.SECURITY.KM.ENCRYPTION.ARvv0DoVGE9Vv17Y0ekfhZcAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.KM.ENCRYPTION.ASUQFLD7fk8qv0VzROaM72AAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.KT.ENCRYPTION.ARvv0DoVGE9Vv17Y0ekfhZcAAAAAAAAAAAAAAAAAAAAAAAAAAAA
ORACLE.SECURITY.KT.ENCRYPTION.ASUQFLD7fk8qv0VzROaM72AAAAAAAAAAAAAAAAAAAAAAAAAAAA
Trusted Certificates:
[oracle@orcl03 tde]$
```

PARÂMETRO

ENCRYPT_NEW_TABLESPACES

3 - PARÂMETRO ENCRYPT_NEW_TABLESPACES

ENCRYPT_NEW_TABLESPACES. disponível (12.2.0.1)

- **CLOUD_ONLY =** Quando configurado esse parâmetro, assim que uma tablespace de dados é criada no Oracle Cloud, ele é criptografado de forma transparente com o “Advanced Encryption Standard 128 (AES 128)”.

- **ALWAYS =** Quando configurado esse parâmetro, automaticamente na criação de uma tablespace ela será criptografada.

- **DDL =** Quando configurado esse parâmetro, as tablespaces não serão criptografadas automaticamente.

3 - PARÂMETRO ENCRYPT_NEW_TABLESPACES

TDE
ORACLE 19C

ENCRYPT_NEW_TABLESPACES

```
SQL> alter system set encrypt_new_tablespaces='ALWAYS';

System altered.

SQL> show parameters encrypt_new_tablespaces

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------
encrypt_new_tablespaces              string      ALWAYS
SQL> set line 32000 pages 32000;
SQL>  select TABLESPACE_NAME,ENCRYPTED from dba_tablespaces;

TABLESPACE_NAME                ENC
------------------------------ ---
SYSTEM                         NO
SYSAUX                         NO
UNDOTBS1                       NO
TEMP                           NO
PDB1_USERS                     NO
TBSPRD01                       NO

6 rows selected.

SQL>
```

O parâmetro por default vem como “CLOUD ONLY”, nesse exemplo ajustamos para “ALWAYS”

```
SQL> CREATE TABLESPACE TBSPRD02 datafile '/u02/oradata/CDB2

Tablespace created.

SQL>  select TABLESPACE_NAME,ENCRYPTED from dba_tablespaces

TABLESPACE_NAME                ENC
------------------------------ ---
SYSTEM                         NO
SYSAUX                         NO
UNDOTBS1                       NO
TEMP                           NO
PDB1_USERS                     NO
TBSPRD01                       NO
TBSPRD02                       YES

7 rows selected.
```

Nesse exemplo, como está habilitado o valor “ALWAYS”, sempre que criar uma tablespaces automaticamente será criptografada

CRIPTOGRAFIA POR COLUNA

Segurança de banco de dados

4 - CRIPTOGRAFIA POR COLUNA

TDE
ORACLE 19C

CRIPTOGRAFIA POR COLUNA

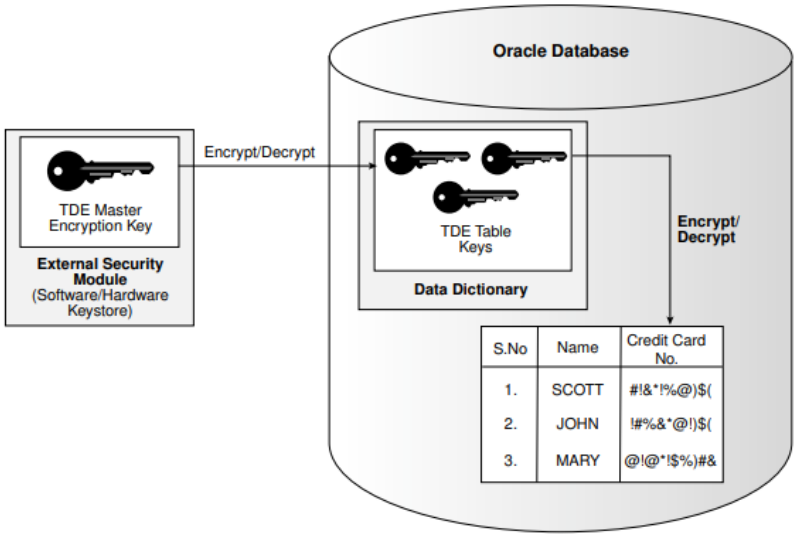
A criptografia de coluna TDE usa a arquitetura baseada em chave de duas camadas para criptografar de forma transparente e descriptografar colunas de tabela.

A TDE master encryption key **é armazenada em um keystore, que pode ser uma:**

Oracle Wallet ;

Oracle Key Vault ;

Oracle Cloud Infrastructure Ou Cloud Vault
Key Management System (KMS).



4 - CRIPTOGRAFIA POR COLUNA

TDE
ORACLE 19C

EXEMPLO DE CRIPTOGRAFIA POR COLUNA

```
SQL> select * from apprh.pessoas;

 MATRICULA NOME                                SALARIO
---------- ------------------------------ ----------
     10001 ANTONIO NUNES                       10000
     10002 RAIMUNDO NONATO                     10000
```

```
SQL> EXIT
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
[oracle@hol ~]$ strings /u02/oradata/CDB2/pdb1/tbsprd01_01.dbf | grep -i RAIMUNDO
RAIMUNDO NONATO
RAIMUNDO NONATO4
[oracle@hol ~]$
```

```
SQL> create table APPRH.PESSOAS (MATRICULA number, NOME varchar2(30) encrypt, SALARIO number encrypt) TABLESPACE TBSPRD01 ;

Table created.
```

```
SQL> select TABLE_NAME,COLUMN_NAME,ENCRYPTION_ALG from dba_encrypted_columns where OWNER='APPRH';

TABLE_NAME
--------------------------------------------------------------------------------
COLUMN_NAME
--------------------------------------------------------------------------------
ENCRYPTION_ALG
------------------------------
PESSOAS
NOME
```

```
[oracle@hol ~]$ strings /u02/oradata/CDB2/pdb1/tbsprd01_enc_01.dbf | grep -i RAIMUNDO
[oracle@hol ~]$
```

4 - CRIPTOGRAFIA POR COLUNA

EXEMPLO: COMO DES-CRIPTOGRAFAR UMA COLUNA

```
SQL> ALTER TABLE APPRH.PESSOAS MODIFY (SALARIO DECRYPT);

Table altered.

SQL> select TABLE_NAME,COLUMN_NAME,ENCRYPTION_ALG from dba_encrypted_columns where OWNER='APPRH';

no rows selected

SQL>
```

4 - CRIPTOGRAFIA POR COLUNA

TDE
ORACLE 19C

LIMITAÇÕES DE CRIPTOGRAFIA POR COLUNA

```
SQL> create table PESSOAS (MATRICULA number, NOME varchar2(30), SALARIO number encrypt) TABLESPACE TBSPRD01 ;
create table PESSOAS (MATRICULA number, NOME varchar2(30), SALARIO number encrypt) TABLESPACE TBSPRD01
                                                           *
ERROR at line 1:
ORA-28336: cannot encrypt SYS owned objects


SQL>
```

Não é possível criptografar colunas no dono “sys”

Não use TDE column encryption com as seguintes "database features":
Index types other than B-tree
Range scan com procura através de index
Sincronismo change data capture (CDC)
Transportable tablespaces
Colunas que tenham sido criadas com "identity columns“

Além disso, você não pode usar a criptografia de coluna TDE para criptografar colunas usadas em "foreign key constraints".

4 - CRIPTOGRAFIA POR COLUNA

TDE
ORACLE 19C

“DATA TYPES” SUPORTADOS

BINARY_DOUBLE
BINARY_FLOAT
CHAR
DATE
INTERVAL DAY TO SECOND
INTERVAL YEAR TO MONTH
NCHAR
NUMBER
NVARCHAR2
RAW (legacy or extended)
TIMESTAMP
VARCHAR2 (legacy or extended)

Se você deseja criptografar objetos binários grandes (LOBs), pode usar o Oracle SecureFiles.

BACKUP RMAN (FISICO)

E

DATAPUMP (LÓGICO)

COM

CRIPTOGRAFIA

Segurança de banco de dados

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

BACKUP RMAN COM CRIPTOGRAFIA

```
RMAN> show all;

using target database control file instead of recovery catalog
RMAN configuration parameters for database with db_unique_name CDB2 are:
CONFIGURE RETENTION POLICY TO REDUNDANCY 1; # default
CONFIGURE BACKUP OPTIMIZATION OFF; # default
CONFIGURE DEFAULT DEVICE TYPE TO DISK; # default
CONFIGURE CONTROLFILE AUTOBACKUP ON; # default
CONFIGURE CONTROLFILE AUTOBACKUP FORMAT FOR DEVICE TYPE DISK TO '%F'; # default
CONFIGURE DEVICE TYPE DISK PARALLELISM 1 BACKUP TYPE TO BACKUPSET; # default
CONFIGURE DATAFILE BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE ARCHIVELOG BACKUP COPIES FOR DEVICE TYPE DISK TO 1; # default
CONFIGURE MAXSETSIZE TO UNLIMITED; # default
CONFIGURE ENCRYPTION FOR DATABASE OFF; # default
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
CONFIGURE COMPRESSION ALGORITHM 'BASIC' AS OF RELEASE 'DEFAULT' OPTIMIZE FOR LOAD TRUE ; # default
CONFIGURE RMAN OUTPUT TO KEEP FOR 7 DAYS; # default
CONFIGURE ARCHIVELOG DELETION POLICY TO NONE; # default
CONFIGURE SNAPSHOT CONTROLFILE NAME TO '/u01/app/oracle/product/19/dbs/snapcf_CDB2.f'; # default

RMAN> CONFIGURE ENCRYPTION FOR DATABASE ON;

new RMAN configuration parameters:
CONFIGURE ENCRYPTION FOR DATABASE ON;
new RMAN configuration parameters are successfully stored
```

```
SQL> select algorithm_id, algorithm_name, algorithm_description, is_default from v$rman_encryption_algorithms;

ALGORITHM_ID ALGORITHM_NAME                                                      ALGORITHM_DESCRIPTION                                                            IS_
------------ ---------------------------------------------------------------- -------------------------------------------------------------------------------- ---
           1 AES128                                                           AES 128-bit key                                                                  YES
           2 AES192                                                           AES 192-bit key                                                                  NO
           3 AES256                                                           AES 256-bit key                                                                  NO
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

BACKUP RMAN COM CRIPTOGRAFIA

```
Recovery Manager: Release 19.0.0.0.0 - Production on Fri Jun 16 03:48:10 2023
Version 19.9.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

connected to target database: CDB2 (DBID=753780962)

RMAN>  show encryption algorithm;

using target database control file instead of recovery catalog
RMAN configuration parameters for database with db_unique_name CDB2 are:
CONFIGURE ENCRYPTION ALGORITHM 'AES128'; # default
```

```
RMAN> set decryption identified by 'HaKunaBatata##12345';

executing command: SET decryption

RMAN>
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

BACKUP RMAN COM CRIPTOGRAFIA

```
RMAN> restore spfile from '/home/oracle/restoredb/spfilecdb2.ora';

Starting restore at 18-JUN-23
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=11 device type=DISK

channel ORA_DISK_1: restoring spfile from AUTOBACKUP /home/oracle/restoredb/spfilecdb2.ora
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of restore command at 06/18/2023 01:01:46
ORA-19870: error while restoring backup piece /home/oracle/restoredb/spfilecdb2.ora
ORA-19913: unable to decrypt backup
ORA-28365: wallet is not open

RMAN>
```

```
RMAN> restore controlfile from '/home/oracle/restoredb/CDB2_20230618_32_1_CONTROL';

Starting restore at 18-JUN-23
using target database control file instead of recovery catalog
allocated channel: ORA_DISK_1
channel ORA_DISK_1: SID=245 device type=DISK

channel ORA_DISK_1: restoring control file
RMAN-00571: ===========================================================
RMAN-00569: =============== ERROR MESSAGE STACK FOLLOWS ===============
RMAN-00571: ===========================================================
RMAN-03002: failure of restore command at 06/18/2023 02:03:25
ORA-19870: error while restoring backup piece /home/oracle/restoredb/CDB2_20230618_32_1_CONTROL
ORA-19913: unable to decrypt backup
ORA-28365: wallet is not open

RMAN>
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

BACKUP RMAN COM CRIPTOGRAFIA

```
[oracle@orcl03 tde]$ scp * 192.168.15.52:/home/oracle/orcl/encryption_wallet/tde/
oracle@192.168.15.52's password:
cwallet.sso
ewallet_2023061522184469_masterkeybackupTDE.p12
ewallet_2023061522271742_backupTDEPDB1.p12
ewallet.p12
[oracle@orcl03 tde]$
```

Transferência do wallet para o destino, onde será realizado o restore.

```
RMAN> restore controlfile from '/home/oracle/restoredb/CDB2_20230618_32_1_CONTROL';

Starting restore at 18-JUN-23
using channel ORA_DISK_1

channel ORA_DISK_1: restoring control file
channel ORA_DISK_1: restore complete, elapsed time: 00:00:01
output file name=/u02/oradata/CDB2/control01.ctl
output file name=/u02/fast_recovery_area/CDB2/control02.ctl
Finished restore at 18-JUN-23

RMAN>
```

Após a transferência do wallet inteiro podemos continuar o restore

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

BACKUP RMAN COM CRIPTOGRAFIA

```
Recovery Manager complete.
[oracle@hol restoredb]$ sqlplus / as sysdba

SQL*Plus: Release 19.0.0.0.0 - Production on Sun Jun 18 02:11:34 2023
Version 19.3.0.0.0

Copyright (c) 1982, 2019, Oracle.  All rights reserved.


Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0

SQL> alter database open resetlogs;

Database altered.

SQL> set line 32000 pages 32000
SQL> select STATUS,WRL_PARAMETER WALLET_DIR,WALLET_TYPE from V$ENCRYPTION_WALLET;

STATUS                         WALLET_DIR
ALLET_TYPE
------------------------------ --------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
OPEN                           /home/oracle/orcl/encryption_wallet//tde/
UTOLOGIN
```

Importante, a base de origem está com autologin, como transferimos todas as chaves do TDE, para o local de destino, após o restore e recover não é necessário abrir o wallet.

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

BACKUP RMAN COM CRIPTOGRAFIA

```
[oracle@hol restoredb]$ cd /home/oracle/orcl/encryption_wallet//tde/
[oracle@hol tde]$ ls
cwallet.sso  ewallet_2023061522184469_masterkeybackupTDE.p12  ewallet_2023061522271742_backupTDEPDB1.p12  ewallet.p12
[oracle@hol tde]$ ls -lorth
total 28K
-rw-------. 1 oracle 5.8K Jun 18 02:05 cwallet.sso
-rw-------. 1 oracle 2.5K Jun 18 02:05 ewallet_2023061522184469_masterkeybackupTDE.p12
-rw-------. 1 oracle 4.1K Jun 18 02:05 ewallet_2023061522271742_backupTDEPDB1.p12
-rw-------. 1 oracle 5.7K Jun 18 02:05 ewallet.p12
[oracle@hol tde]$ rm -f *
[oracle@hol tde]$ ls
[oracle@hol tde]$ pwd
/home/oracle/orcl/encryption_wallet/tde
```

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
NOT_AVAILABLE                  /home/oracle/orcl/encryption_wallet//tde/
NKNOWN
NOT_AVAILABLE
```

```
SQL>  create temporary tablespace temp03 tempfile '/u02/oradata/CDB2/temp03.dbf'  size 10m;
 create temporary tablespace temp03 tempfile '/u02/oradata/CDB2/temp03.dbf'  size 10m
*
ERROR at line 1:
ORA-28365: wallet is not open
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

DATAPUMP COM CRIPTOGRAFIA

```
SQL> ALTER TABLE APPRH.PESSOAS MODIFY (SALARIO encrypt);

Table altered.

SQL>  select * from DBA_ENCRYPTED_COLUMNS;

OWNER                                                                                                                            TABLE_NAME
 COLUMN_NAME                                                                                                                      ENCRYPTION_ALG                SAL INTEGRITY_AL
-------------------------------------------------------------------------------------------------------------------------------- ------------------------------ ---------- ------------
---- --- ------------
APPRH                                                                                                                            PESSOAS
 SALARIO                                                                                                                          AES 192 bits key              YES SHA-1
```

```
Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Starting "SYS"."SYS_EXPORT_TABLE_05":  "/******** AS SYSDBA" directory=expdados dumpfile=exptablepessoas.dmp tables=APPRH.PE
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
Processing object type TABLE_EXPORT/TABLE/TABLE
. . exported "APPRH"."PESSOAS"                           6.070 KB      20 rows
ORA-39173: Encrypted data has been stored unencrypted in dump file set.
Master table "SYS"."SYS_EXPORT_TABLE_05" successfully loaded/unloaded
******************************************************************************
Dump file set for SYS.SYS_EXPORT_TABLE_05 is:
  /home/oracle/Downloads/exptablepessoas.dmp
Job "SYS"."SYS_EXPORT_TABLE_05" successfully completed at Tue Jun 20 01:00:03 2023 elapsed 0 00:00:11
```

Nesse exemplo não foi configurado nenhum valor de criptografia, os dados são descriptografados.

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

DATAPUMP COM CRIPTOGRAFIA

```
[oracle@hol Downloads]$ strings exptablepessoas.dmp | grep -i SAL
  <STRMTABLE_T><VERS_MAJOR>1</VERS_MAJOR><VERS_MINOR>2 </VERS_MINOR><VERS_DP
E><FDO>0000006001240F050B0C030C0C0504050D06090708050505050F05050505050A050
0</FDO><OBJ_NUM>23965</OBJ_NUM><OWNER_NAME>APPRH</OWNER_NAME><NAME>PESSOAS</
NTCOL_NUM>1</INTCOL_NUM><SEGCOL_NUM>1</SEGCOL_NUM><COL_SORTKEY>1</COL_SORTKE
A</NAME><TYPE_NUM>2</TYPE_NUM><LENGTH>22</LENGTH><NOT_NULL>0</NOT_NULL><CHAR
OL_NUM>2</COL_NUM><INTCOL_NUM>2</INTCOL_NUM><SEGCOL_NUM>2</SEGCOL_NUM><COL_S
ERTY2><NAME>NOME</NAME><TYPE_NUM>1</TYPE_NUM><LENGTH>30</LENGTH><NOT_NULL>0<
>23965</OBJ_NUM><COL_NUM>3</COL_NUM><INTCOL_NUM>3</INTCOL_NUM><SEGCOL_NUM>3<
<PROPERTY2>0</PROPERTY2><NAME>SALARIO</NAME><TYPE_NUM>2</TYPE_NUM><LENGTH>22
_LIST></STRMTABLE_T></ROW></ROWSET>
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

DATAPUMP COM CRIPTOGRAFIA

```
Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Starting "SYS"."SYS_EXPORT_TABLE_05":  "/******** AS SYSDBA" directory=expdados dumpfile=exptablepessoas2.dmp tables=APPRH.PESSOAS logfile=exptablepessoas.log encryption_password=******** ENCRYPTION_MODE=PA
SSWORD
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
Processing object type TABLE_EXPORT/TABLE/TABLE
. . exported "APPRH"."PESSOAS"                           6.078 KB      20 rows
Master table "SYS"."SYS_EXPORT_TABLE_05" successfully loaded/unloaded
******************************************************************************
Dump file set for SYS.SYS_EXPORT_TABLE_05 is:
  /home/oracle/Downloads/exptablepessoas2.dmp
Job "SYS"."SYS_EXPORT_TABLE_05" successfully completed at Tue Jun 20 01:20:04 2023 elapsed 0 00:00:10
```

```
[oracle@hol Downloads]$ strings exptablepessoas2.dmp | grep -i SAL
fHVSAlk
[oracle@hol Downloads]$
```

```
Connected to: Oracle Database 19c Enterprise Edition Relea
ORA-31626: job does not exist
ORA-31637: cannot create job SYS_IMPORT_TABLE_01 for user
ORA-06512: at "SYS.KUPV$FT", line 1142
ORA-06512: at "SYS.KUPV$FT", line 1744
ORA-06512: at "SYS.DBMS_SYS_ERROR", line 95
ORA-06512: at "SYS.KUPV$FT_INT", line 1099
ORA-39244: Event to disable dropping null bit image header
ORA-06512: at "SYS.DBMS_SYS_ERROR", line 86
ORA-06512: at "SYS.KUPC$QUE_INT", line 2002
ORA-28365: wallet is not open
ORA-06512: at "SYS.KUPC$QUE_INT", line 1918
ORA-06512: at "SYS.KUPC$QUEUE_INT", line 493
ORA-06512: at "SYS.KUPV$FT_INT", line 981
ORA-06512: at "SYS.KUPV$FT", line 1646
ORA-06512: at "SYS.KUPV$FT", line 1103
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

DATAPUMP COM CRIPTOGRAFIA

```
---------------------------------------- ---------- ----------
/home/oracle/orcl/encryption_wallet//tde OPEN       AUTOLOGIN
/

                                         OPEN       AUTOLOGIN
                                         OPEN       AUTOLOGIN

SQL> exit
Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Produc
Version 19.9.0.0.0
[oracle@orcl03 admin]$ impdp c##ebolabr/welcome1@pdb1  directory=impdados dumpfile=e

Import: Release 19.0.0.0.0 - Production on Tue Jun 20 02:38:20 2023
Version 19.9.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Master table "C##EBOLABR"."SYS_IMPORT_TABLE_01" successfully loaded/unloaded
Starting "C##EBOLABR"."SYS_IMPORT_TABLE_01":  c##ebolabr/********@pdb1 directory=imp
Processing object type TABLE_EXPORT/TABLE/TABLE
Processing object type TABLE_EXPORT/TABLE/TABLE_DATA
. . imported "APPRH"."PESSOAS"                           6.070 KB      20 rows
Processing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
Processing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
Job "C##EBOLABR"."SYS_IMPORT_TABLE_01" successfully completed at Tue Jun 20 02:38:37
```

5 - BACKUP RMAN E DATAPUMP COM CRIPTOGRAFIA

TDE
ORACLE 19C

DATAPUMP COM CRIPTOGRAFIA

```
[oracle@orcl03 admin]$ impdp c##ebolabr/welcome1@pdb1  directory=impdados dumpfi

Import: Release 19.0.0.0.0 - Production on Tue Jun 20 02:41:44 2023
Version 19.9.0.0.0

Copyright (c) 1982, 2019, Oracle and/or its affiliates.  All rights reserved.

Connected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Produc
ORA-39002: invalid operation
ORA-39174: Encryption password must be supplied.
```

impdp c##ebolabr/welcome1@pdb1 directory=impdados
dumpfile=exptablepessoas2.dmp tables=APPRH.PESSOAS
logfile=imptablepessoas.log encryption_password=welcome1

```
onnected to: Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
aster table "C##EBOLABR"."SYS_IMPORT_TABLE_01" successfully loaded/unloaded
tarting "C##EBOLABR"."SYS_IMPORT_TABLE_01":  c##ebolabr/********@pdb1 directory=impdados dumpfile=exptablepessoas2.dmp tables=APPRH.PESSOAS logfile=imptablepessoas.log encryption_password=*******
rocessing object type TABLE_EXPORT/TABLE/TABLE
rocessing object type TABLE_EXPORT/TABLE/TABLE_DATA
 . imported "APPRH"."PESSOAS"                             6.078 KB      20 rows
rocessing object type TABLE_EXPORT/TABLE/STATISTICS/TABLE_STATISTICS
rocessing object type TABLE_EXPORT/TABLE/STATISTICS/MARKER
ob "C##EBOLABR"."SYS_IMPORT_TABLE_01" successfully completed at Tue Jun 20 02:46:05 2023 elapsed 0 00:00:10
```

BÔNUS

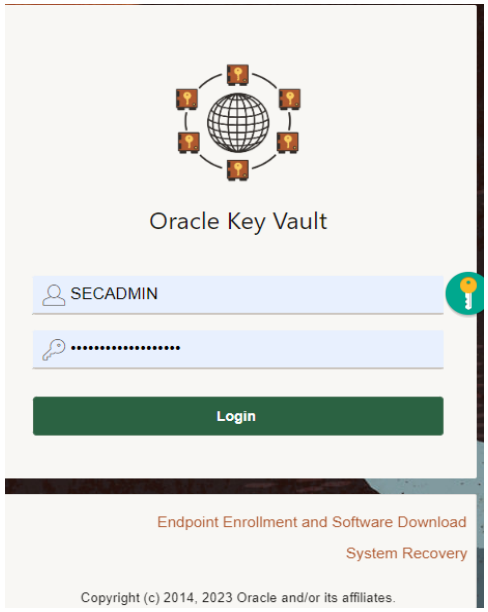
ORACLE

KEY VAULT

21

6 ORACLE KEY VAULT (OKV)

TDE
ORACLE 19C

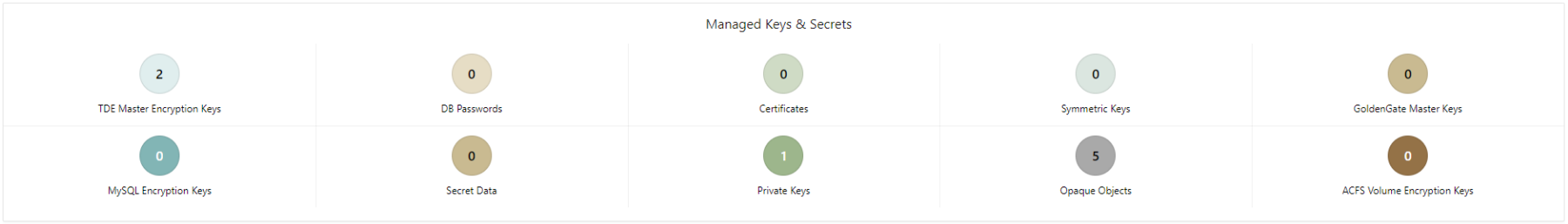


O Oracle Key Vault é um dispositivo de gerenciamento de chaves e segredos tolerante a falhas, altamente disponível e escalável, seguro e compatível com os padrões, onde você pode armazenar, gerenciar e compartilhar
seus objetos de segurança.

Para aumentar a disponibilidade de chaves e segredos, você pode instalar o Oracle Key Vault como um multimestre cluster com até 16 nós (distribuídos geograficamente).

Construído em Oracle Linux, Oracle Database, recursos de segurança do Oracle Database como
Oracle Transparent Data Encryption, Oracle Database Vault, Oracle Virtual Private Database,
e tecnologia Oracle GoldenGate, Oracle Key Vault centralizado, altamente disponível e solução de segurança escalável.

ORACLE KEY VAULT (OKV)



Um objeto de segurança contém dados críticos fornecidos por um usuário. Objetos de segurança que você podem gerenciar com o Oracle Key Vault incluem chaves de criptografia, Wallets Oracle, keystores Java (JKS), keystores Java Cryptography Extension (JCEKS) e arquivos de credenciais.

Arquivos de credenciais pode incluir chaves privadas SSH (usadas para autenticação de chave pública para servidores remotos (para exemplo de instâncias de computação OCI) ou senhas de contas de banco de dados para execução autônoma de scripts de manutenção agendados regularmente.

MUITO OBRIGADO!

CONTATO
TELEFONE - 11 98489-3633
EMAIL – jcnogueira.Oliveira@gmail.com