

# Oracle 18c New Security Features

Enhancements and other improvements


Stefan Oehrli



BASEL ▪ BERN ▪ BRUGG ▪ DÜSSELDORF ▪ FRANKFURT A.M. ▪ FREIBURG I.BR. ▪ GENÈVE  
HAMBURG ▪ KOPENHAGEN ▪ LAUSANNE ▪ MÜNCHEN ▪ STUTTGART ▪ WIEN ▪ ZÜRICH

**trivadis**  
makes IT easier. ■ ■ ■

## ■ Our company.

Trivadis is a **market leader in IT consulting, system integration, solution engineering** and the provision of **IT services** focusing on **ORACLE®** and  **Microsoft** technologies in Switzerland, Germany, Austria and Denmark. We offer our services in the following strategic business fields:



Trivadis Services takes over the interacting operation of your IT systems.

**trivadis**  
makes IT easier. ■ ■ ■

# ■ With over 600 specialists and IT experts in your region.



- 14 Trivadis branches and more than 600 employees
- 200 Service Level Agreements
- Over 4,000 training participants
- Research and development budget: CHF 5.0 million
- Financially self-supporting and sustainably profitable
- Experience from more than 1,900 projects per year at over 800 customers

**trivadis**  
makes IT easier. ■ ■ ■

**Technology on its own won't help you.  
You need to know how to use it properly.**



# ■ Stefan Oehrli



## **Solution Manager BDS SEC / Trivadis Partner**

- Working since 1997 in IT
- Since 2008 with Trivadis AG
- Since 2010 Discipline Manager SEC INFR
- Since 2014 Solution Manager BDS Security

### **IT Experience**

- Database administration and database security solutions
- Administration complex, heterogeneous systems
- IT / Database Team leader

### **Specialization**

- DB security and operation
- Security concepts and their implementation
- Security assessments
- Oracle Backup & Recovery
- Enterprise User Security and Oracle Unified Directory

### **Skills**

- Backup & Recovery
- Oracle Advanced Security
- Oracle AVDF and DB Vault
- Oracle Directory Services
- Team / Project Management
- Trainer O-SEC, O-BR,...



# ■ Agenda

**18<sup>c</sup>** ORACLE<sup>®</sup>  
Database

1. Authentication
2. Authorization
3. Auditing
4. Confidentiality of data
5. Network
6. Conclusion

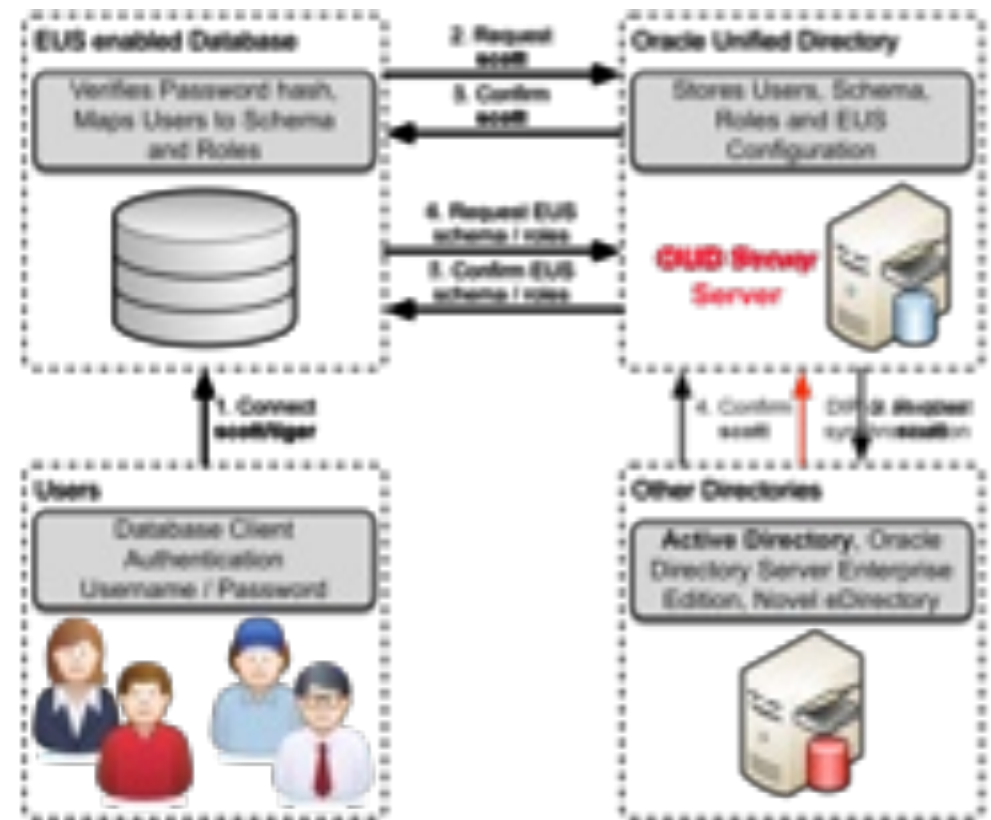
# Authentication

# ■ Authentication Enhancements

- No real enhancements or new features in authorization
- Kerberos still works when already setup on Oracle 12.2.0.1
  - Try to avoid setup Kerberos for 12.1.0.2
- A couple of new sqlnet.ora parameter for SSL certificate
  - see chapter network
- And bit of integration of Active Directory Services with Oracle Database
  - Yes direct integration with Active Directory Services 😊

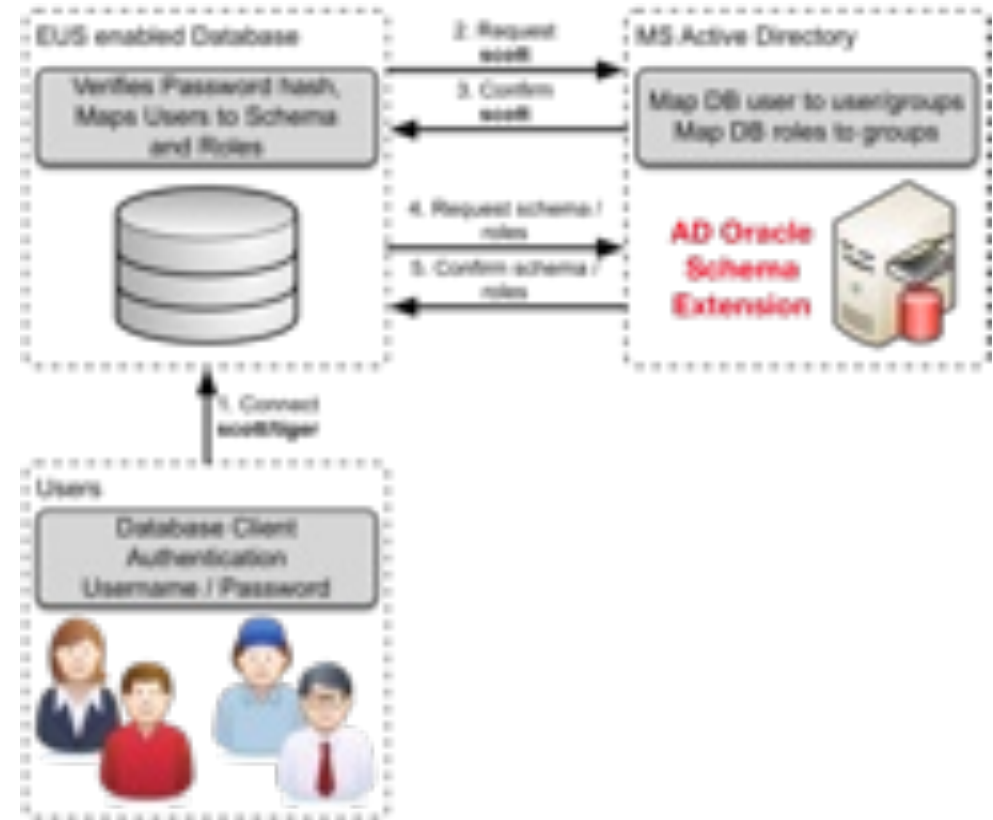
# ■ Integration of MS Active Directory Services using EUS

- Until now, integration with Active Directory also meant to...
  - ...maintain an Oracle Directory
  - ...setup OID or OUD
  - ...configure OUD AD Proxy, DIP etc.
  - ...configure Enterprise User Security
  - ...purchase Directory Server Plus
- Oracle Enterprise User Security has a number of advantages for medium and large environments
- To manage only a few users centrally with EUS means “to crack a nut with a sledgehammer”



# ■ Integration of MS Active Directory Services using CMU

- Centrally Managed User CMU...
  - ...does not require an Oracle Directory
  - ...does not require a license
  - ...allows to manage user via AD
- Supports usual authentication methods
  - Password
  - Kerberos
  - Public key infrastructure (PKI)
- Requires a password filter and AD schema extension
- Requires a AD service account
- Ideal for small environments



# ■ Centrally Managed User with Active Directory

- Directory users that access an Oracle database using a shared schema
  - All user will using the same database schema
- Exclusively map directory users to a private schema
  - Each user has its on database schema with the corresponding direct grants
  - User can have there own database objects
- Mapping a Directory Group to a Global Role
  - Grant additional rights based on AD group membership
- Administrative global users with administrative privileges
  - SYSDBA, SYSOPER, SYSDG, SYSKM, and SYSRAC
  - Can not be granted via through global roles

# ■ Connecting to Microsoft Active Directory (1)

- Step 1: create an MS AD service account
  - Requires read privilege on the directory
  - Requires write privilege to update login / password history information
- Step 2: Install the password filter and extend the MS AD schema
  - Oracle provides the utility **opwdintg.exe** located in **\$ORACLE\_HOME/bin**
  - Is not required for Kerberos or SSL authentication
- Step 3: Install the Oracle Binaries if not yet done

## ■ Connecting to Microsoft Active Directory (2)

### ■ Step 4: Create an **dsi.ora** or **ldap.ora** file

- File specifies the MS AD host, ports etc.
- Can be either dsi.ora or ldap.ora, dsi.ora is preferred over ldap.ora
- CMU can coexist with EUS when eg. CMU use dsi.ora and EUS use ldap.ora
- example dsi.ora file

```
DSI_DIRECTORY_SERVERS = (mneme.postgasse.org:389:636)
DSI_DEFAULT_ADMIN_CONTEXT = "dc=postgasse,dc=org"
DSI_DIRECTORY_SERVER_TYPE = AD
```

- Default location are \$LDAP\_ADMIN, \$ORACLE\_HOME/ldap/admin, \$TNS\_ADMIN or \$ORACLE\_HOME/network/admin

### ■ Step 5: Get the MS AD root certificate

## ■ Connecting to Microsoft Active Directory (3)

### ■ Step 6: Create a wallet for a secure connection

- Add the Oracle directory service account name

```
mkstore -wrl . -createEntry ORACLE.SECURITY.USERNAME oracle18c
```

- Add DN for the Oracle directory service account

```
mkstore -wrl . -createEntry ORACLE.SECURITY.DN \  
CN=oracle18c,CN=Users,DC=postgasse,DC=org
```

- Add password for the Oracle directory service account

```
mkstore -wrl . -createEntry ORACLE.SECURITY.PASSWORD manager
```

- Add the MS AD certificate to the wallet

```
orapki wallet add -wallet . -cert AD_CA_Root_cert.txt -trusted_cert
```

## ■ Connecting to Microsoft Active Directory (4)

### ■ Step 7: Configure the Microsoft Active Directory Connection

- Manually or with dbca although dbca does not support dsi.ora files

```
ALTER SYSTEM SET LDAP_DIRECTORY_ACCESS = 'PASSWORD';  
ALTER SYSTEM SET LDAP_DIRECTORY_SYSAUTH = YES SCOPE=SPFILE;
```

### ■ Step 8: Verify the wallet

```
orapki wallet display -wallet wallet
```

### ■ Step 9: Test the Integration 😊

## ■ Map Centrally Managed User

- Map directory group to share database global user

```
CREATE USER ad_users IDENTIFIED GLOBALLY AS  
'cn=Oracle_18c,ou=Groups,dc=postgasse,dc=org';
```

- Map a directory group to a global role

```
CREATE ROLE global_dba IDENTIFIED GLOBALLY AS  
'cn=DBAs,ou=Groups,dc=postgasse,dc=org';
```

- Exclusively map a directory user to a database global user

```
CREATE USER joe_ad IDENTIFIED GLOBALLY AS  
'cn=Jan Oehrli,ou=People,dc=postgasse,dc=org';
```

## ■ Connect as Centrally Managed User

- Either user principal name (UPN) or DOMAIN\User should work

```
SQL> connect "soe@POSTGASSE.org"@TDB180A
Enter password:
Connected.
```

```
SQL> connect "POSTGASSE\soe"@TDB180A
Enter password:
Connected.
```

- Or Kerberos if configured
  - Don't mix up the accounts 😊

```
okinit hmu@POSTGASSE.ORG
sqlplus /@TDB180A
```

# Authorization

# ■ Enterprise User Security Enhancements

- Enterprise User Security Manager (EUSM) is finally supported ähm documented
  - **eusm** has been available since Oracle 11g
  - So far just a limited documentation in Oracle Support Document 1085065.1 *EUSM, Command Line Tool For EUS Administration and Some EUS Good to Knows* <https://support.oracle.com/epmos/faces/DocumentDisplay?id=1085065.1>
  - Now officially documented in *Oracle® Database Enterprise User Security Administrator's Guide* <https://docs.oracle.com/en/database/oracle/oracle-database/18/dbimi/enterprise-user-security-manager-eusm-command-summary.html>
- Command line tool to setup and configure Enterprise User Security
- Alternative to Oracle Enterprise Manager Cloud Control (which does use the same java classes)

## ■ eusm examples

- Create a mapping for the default domain to schema EUS\_USERS

```
eusm createMapping domain_name="OracleDefaultDomain" map_type=SUBTREE \  
realm_dn="dc=postgasse,dc=org" map_dn="ou=People,dc=postgasse,dc=org" \  
schema=EUS_USERS ldap_host="oudad.postgasse.org" ldap_port=1389 \  
ldap_user_dn="cn=Directory Manager" ldap_user_password="manager"
```

- List mappings for the default domain

```
eusm listMappings domain_name="OracleDefaultDomain" \  
realm_dn="dc=postgasse,dc=org" ldap_host="oudad.postgasse.org" \  
ldap_port=1389 ldap_user_dn="cn=Directory Manager" \  
ldap_user_password="manager"
```

## ■ Other Enterprise User Security Enhancements

- PDBs are no longer restricted to the default wallet location
  - PDBs can have individual wallets specified by `WALLET_LOCATION`
- Support for 12C verifier generated by Oracle Internet Directory
  - The 12C verifier uses a new ZT tag MR-SHA512
  - Also supported in OUD 12c
  - It's a multi-round Password-Based Key Derivation Function (PBKDF2) based keyed-hash message authentication code (HMAC) with SHA512 cryptographic hash functions to provide a strong password verifier

# ■ Schema Only Accounts (1)

- Schema only accounts are accounts without authentication
  - Can have objects as every other account
  - Administrator and non-administrator accounts
  - Use proxy authentication to log into
  - Nevertheless require the corresponding privileges
- Create a schema only account

```
SQL> CREATE USER scott_data NO AUTHENTICATION;
```

- Alter an existing account in both ways

```
SQL> ALTER USER scott_data IDENTIFIED BY tiger;  
SQL> ALTER USER scott_data NO AUTHENTICATION;
```

## ■ Schema Only Accounts (2)

- Grant proxy connect for *scott\_data* to user *scott*

```
SQL> ALTER USER scott_data GRANT CONNECT THROUGH scott;
```

- Proxy connect does only work if *scott\_data* has the corresponding privileges

```
SQL> CONNECT scott[scott_data]/tiger
ERROR:
ORA-01045: user SCOTT_DATA lacks CREATE SESSION privilege; logon denied

SQL> GRANT CREATE SESSION TO tvd scott_data;
SQL> CONNECT scott[scott_data]/tiger
Connected.
```

# ■ PDB Lockdown Profiles Enhancements

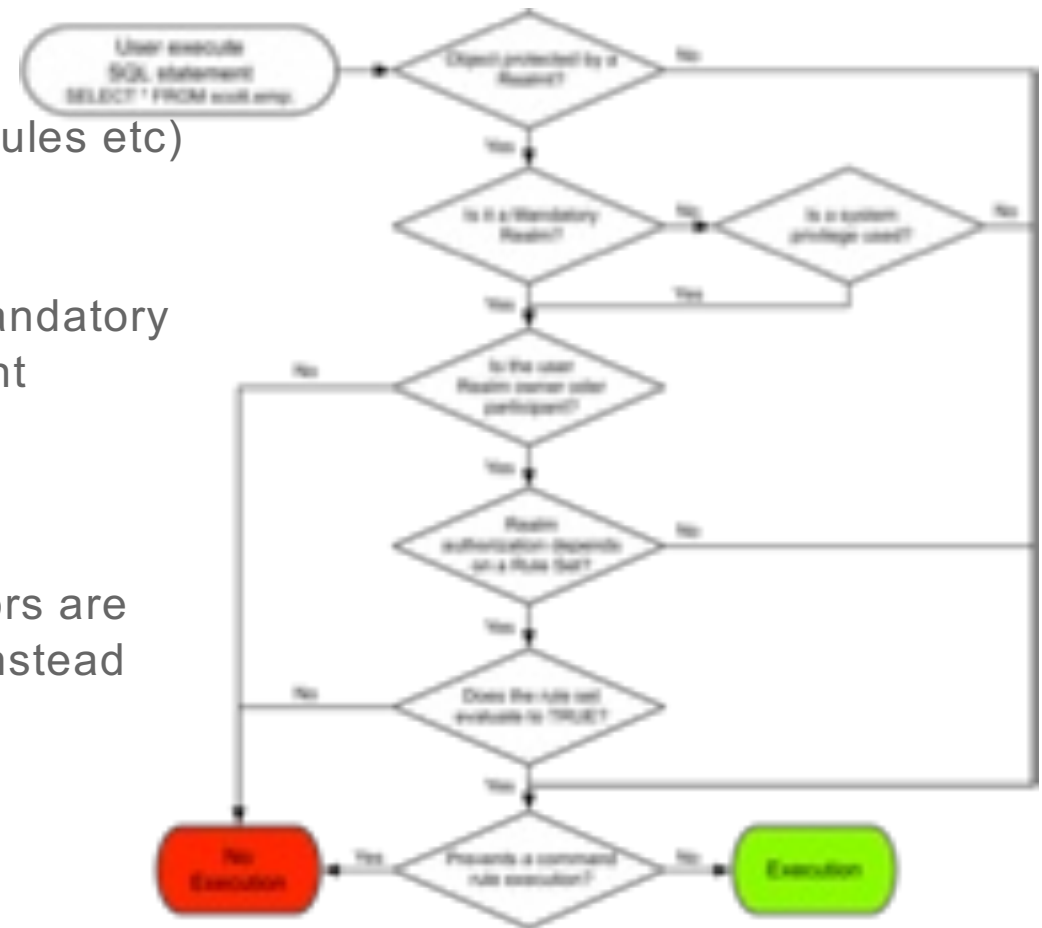
- A PDB lockdown profile is a named set of features that controls a group of operations
- PDB lockdown profiles in the application root, as well as in the CDB root
- Create PDB lockdown profile that is based on another PDB lockdown profile
- New view V\$LOCKDOWN\_RULES to see the lockdown rules
- Developed for Use Case where identities are shared...
  - ... on OS level when DB is interacting with the OS
  - ... cloud environments
  - ... within the DB when access common user / objects
  - ... when administrative features and xml features are used

# ■ Default PDB Lockdown Profiles

- PRIVATE\_DBAAS, limitations for private Cloud DBaaS
  - Same DBA for all PDB, different user and applications
- SAAS, limitations for SaaS implementations
  - Same DBA for all PDB, different user, same applications
- PUBLIC\_DBAAS, limitations for Cloud DBaaS
  - different DBA for each PDB, different user and applications

# ■ Database Vault Simulation Mode Enhancements

- Enable DB Vault (realms, command rules etc)
- Report security violations
- Simulation mode now captures all mandatory realm violations from a SQL statement
- Simulation mode can capture the full call stack information
- The default trusted path context factors are now available as separate columns instead of being concatenated together
- Access to objects is not blocked



## ■ DB Vault improvements

### ■ New Factor Functions

- F\$DV\$\_CLIENT\_IDENTIFIER
- F\$DV\$\_DBLINK\_INFO
- F\$DV\$\_MODULE
- F\$PROXY\_USER

### ■ Authorizations users or roles data pump regular operations in Database Vault

- Fine grained control who is allowed to use data pump
- Configured using DBMS\_MACADM.AUTHORIZE\_DATAPUMP\_USER

### ■ Oracle Database Replay operations are now supported in Oracle Database Vault

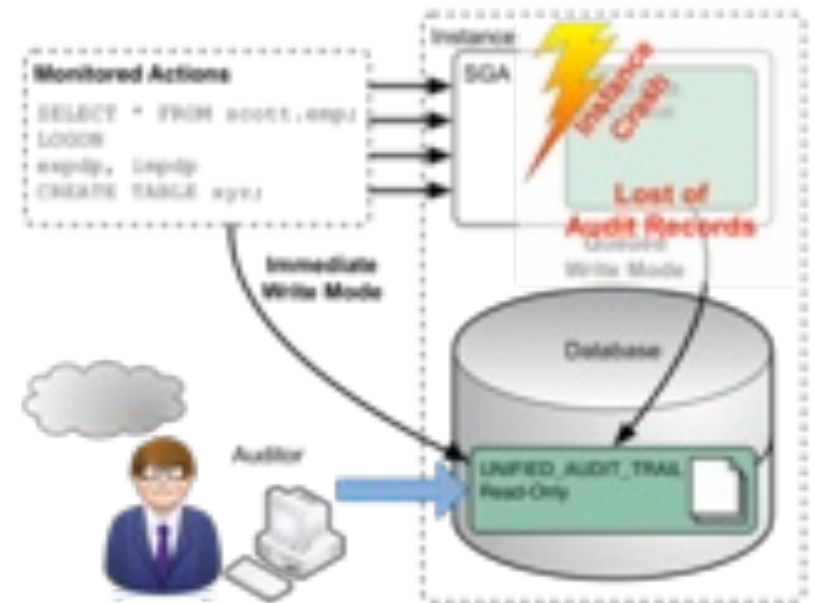


# Auditing

# ■ Unified Audit and queue management

- Deprecation of UNIFIED\_AUDIT\_SGA\_QUEUE\_SIZE
  - Audit Data is written immediately to an internal relational table
  - No data lost in case Instance Crash / SHUTDOWN ABORT
- Deprecation of settings to flush audit trail records to disk
  - Data is written automatically in a new internal relational table
  - Existing unified audit records have to be **transferred**
- Unified Audit is still not enabled by default
  - New databases run in **mixed mode**
  - Pure unified mode by relink the binaries see MOS Note 1567006.1

```
cd $ORACLE_HOME/rdbms/lib  
make -f ins_rdbms.mk uniaud_on ioracle
```



## ■ Unified Audit Trail to SYSLOG or Windows Events (1)

- New static init.ora parameter `UNIFIED_AUDIT_SYSTEMLOG` to write unified audit trail to SYSLOG or Windows event viewer
- Possible values for `UNIFIED_AUDIT_SYSTEMLOG`
  - **FALSE** disables unified audit for SYSLOG (default)
  - **TRUE** writes the syslog values to the Windows Event Viewer (Windows)
  - **facility\_clause.priority\_clause** writes the syslog values to the corresponding SYSLOG facility (Unix)
- Does only work for pure **unified mode** mixed mode is not supported
- Enable unified audit to SYSLOG on Unix

```
SQL> ALTER SYSTEM SET unified_audit_systemlog='LOCAL0.DEBUG' SCOPE=SPFILE;  
  
System altered.
```

## ■ Unified Audit Trail to SYSLOG or Windows Events (2)

### ■ Information in SYSLOG is limited

- Just the changes on the audit infrastructure
- CREATE AUDIT POLICY, AUDIT, DBMS\_AUDIT\_MGMT

### ■ Full audit information only in regular UNIFIED\_AUDIT\_TRAIL

```
Jun 13 12:12:34 urania journal: Oracle Unified Audit[19149]: LENGTH: '161' TYPE:"4" DBID:"3920464478"
SESID:"0" CLIENTID:"" ENTRYID:"3" STMTID:"9" DBUSER:"SYS" CURUSER:"SYS" ACTION:"31" RETCODE:"46357"
SCHEMA:"SYS" OBJNAME:"AUDIT_DEMO"
Jun 13 12:12:34 urania journal: Oracle Unified Audit[19149]: LENGTH: '163' TYPE:"4" DBID:"3920464478"
SESID:"0" CLIENTID:"" ENTRYID:"4" STMTID:"11" DBUSER:"SYS" CURUSER:"SYS" ACTION:"231" RETCODE:"46357"
SCHEMA:"SYS" OBJNAME:"AUDIT_DEMO"
Jun 13 12:12:34 urania journal: Oracle Unified Audit[19431]: LENGTH: '174' TYPE:"4" DBID:"3920464478"
SESID:"2124541458" CLIENTID:"" ENTRYID:"1" STMTID:"4" DBUSER:"SYS" CURUSER:"SYS" ACTION:"47"
RETCODE:"0" SCHEMA:"AUDSYS" OBJNAME:"DBMS_AUDIT_MGMT"
Jun 13 12:12:34 urania journal: Oracle Unified Audit[19431]: LENGTH: '175' TYPE:"4" DBID:"3920464478"
SESID:"2124541458" CLIENTID:"" ENTRYID:"2" STMTID:"12" DBUSER:"SYS" CURUSER:"AUDSYS" ACTION:"47"
RETCODE:"0" SCHEMA:"SYS" OBJNAME:"DBMS_AUDIT_MGMT"
Jun 13
```

## ■ Export / Import Unified Audit Trail (1)

- Unified audit trail can be exported using Oracle Data Pump
  - EXP\_FULL\_DATABASE or IMP\_FULL\_DATABASE is required
- Either full or partial database export and import automatically include audit trails
  - According to documentation just unified audit trail
  - Export log shows standard and fine grained audit including configuration
- Limit export to audit trails be using INCLUDE=AUDIT\_TRAILS
- Data pump import notes
  - Just unified audit trail and its base tables gets imported
  - **Caution!** audit trail data is appended to the existing audit trail table

## ■ Export / Import Unified Audit Trail (2)

### ■ Regular full data pump export

```
expdp system DUMPFILE=TDB180A_full.dmp DIRECTORY=DATA_PUMP_DIR FULL=yes  
...  
. . exported "AUDSYS"."AUD$UNIFIED": "SYS_P281"      1.045 MB      2268 rows
```

### ■ Use INCLUDE=AUDIT\_TRAILS to just export audit trails

```
expdp system DUMPFILE=TDB180A_audit.dmp DIRECTORY=DATA_PUMP_DIR FULL=yes  
INCLUDE=AUDIT_TRAILS
```

## ■ Export / Import Unified Audit Trail (3)

### ■ Excerpt of the data pump export log with INCLUDE=AUDIT\_TRAILS

```
Processing object type DATABASE_EXPORT/POST_SYSTEM_IMP_CALLOUT/MARKER
. . exported "SYS"."KU$ _USER_MAPPING_VIEW"          5.976 KB      31 rows
. . exported "AUDSYS"."AUD$UNIFIED":"SYS_P281"        1.045 MB     2268 rows
. . exported "SYS"."DAM_CONFIG_PARAM$"                6.531 KB      14 rows
. . exported "AUDSYS"."AUD$UNIFIED":"AUD_UNIFIED_P0"    0 KB         0 rows
. . exported "SYS"."AUD$"                             0 KB         0 rows
. . exported "SYS"."DAM_CLEANUP_EVENTS$"              0 KB         0 rows
. . exported "SYS"."DAM_CLEANUP_JOBS$"                0 KB         0 rows
. . exported "SYS"."AUDTAB$TBS$FOR_EXPORT"            5.953 KB       2 rows
. . exported "SYS"."FGA_LOG$FOR_EXPORT"               0 KB         0 rows
Master table "SYSTEM"."SYS_EXPORT_FULL_01" successfully loaded/unloaded
*****
Dump file set for SYSTEM.SYS_EXPORT_FULL_01 is:
/u00/app/oracle/admin/TDB180A/dpdump/TDB180A_audit.dmp
Job "SYSTEM"."SYS_EXPORT_FULL_01" successfully completed at Wed Jun 13 10:41:09 2018 elapsed 0 00:01:05
```

### ■ Standard, fine grained and unified audit trails are exported

## ■ Export / Import Unified Audit Trail (4)

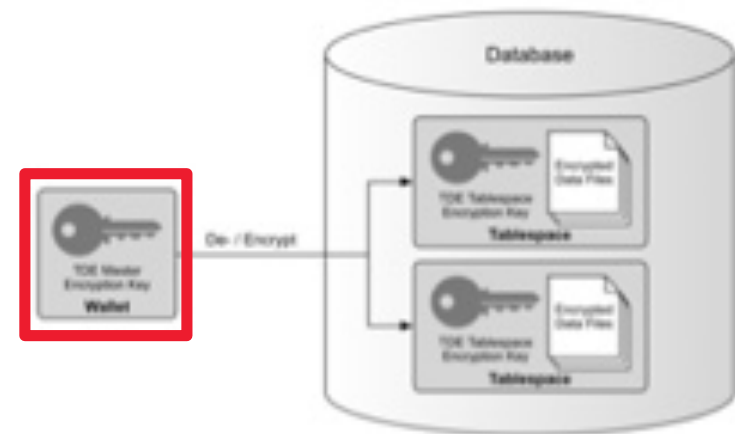
### ■ Excerpt of the data pump import log

```
Processing object type DATABASE_EXPORT/EARLY_OPTIONS/VIEWS_AS_TABLES/TABLE_DATA
. . imported "SYS"."KU$_EXPORT_USER_MAP"                5.976 KB      31 rows
Processing object type DATABASE_EXPORT/EARLY_POST_INSTANCE_IMPCALLOUT/MARKER
Processing object type DATABASE_EXPORT/NORMAL_OPTIONS/TABLE
Processing object type DATABASE_EXPORT/NORMAL_OPTIONS/TABLE_DATA
. . imported "AUDSYS"."AMGT$DP$AUD$UNIFIED":"SYS_P281"    1.045 MB     2268 rows
. . imported "SYS"."AMGT$DP$DAM_CONFIG_PARAM$"            6.531 KB      14 rows
. . imported "AUDSYS"."AMGT$DP$AUD$UNIFIED":"AUD_UNIFIED_P0" 0 KB         0 rows
. . imported "SYS"."AMGT$DP$AUD$"                        0 KB         0 rows
. . imported "SYS"."AMGT$DP$DAM_CLEANUP_EVENTS$"          0 KB         0 rows
. . imported "SYS"."AMGT$DP$DAM_CLEANUP_JOBS$"            0 KB         0 rows
Processing object type DATABASE_EXPORT/NORMAL_OPTIONS/VIEWS_AS_TABLES/TABLE
Processing object type DATABASE_EXPORT/NORMAL_OPTIONS/VIEWS_AS_TABLES/TABLE_DATA
. . imported "SYS"."AMGT$DP$AUDTAB$TBS$FOR_EXPORT"        5.953 KB       2 rows
. . imported "SYS"."AMGT$DP$FGA_LOG$FOR_EXPORT"           0 KB         0 rows
Processing object type DATABASE_EXPORT/NORMAL_POST_INSTANCE_IMPCALLOUT/MARKER
Processing object type DATABASE_EXPORT/FINAL_POST_INSTANCE_IMPCALLOUT/MARKER
Processing object type DATABASE_EXPORT/POST_SYSTEM_IMPCALLOUT/MARKER
Job "SYSTEM"."SYS_IMPORT_FULL_01" successfully completed at Wed Jun 13 11:07:03 2018 elapsed 0 00:00:07
```

# Confidentiality of data

# ■ User-Defined Master Encryption Key (1)

- Use customer conform TDE master encryption keys in Oracle Clouds solutions
- Enhance TDE and wallet security
- Use ADMINISTER KEY MANAGEMENT to create and set user-defined TDE master encryption keys eg.
  - ...create user defined keys
  - ...create user defined keys for later user
  - ...activate user defined keys
- TDE master encryption key and its corresponding ID are not captured by any auditing logs



## ■ User-Defined Master Encryption Key (2)

- Create new user defined TDE master encryption key

```
SQL> ADMINISTER KEY MANAGEMENT CREATE KEY USING TAG  
2 'DBSec18c' IDENTIFIED BY manager WITH BACKUP;
```

- Review v\$encryption\_keys for status of the TDE master encryption keys

```
SQL> SELECT key_id,activation_time FROM v$encryption_keys;
```

KEY_ID	ACTIVATION_TIME
AVGoKqaX7E9Gv41wALd+7ZcAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	
Aa/Rx4mpi0/Wv2GrGkuShl0AAAAAAAAAAAAAAAAAAAAAAAAAAAAA	12-JUN-18 09.16.15.718300 PM

## ■ User-Defined Master Encryption Key (3)

- Specify the key algorithms eg. **AES256**, ARIA256, SEED128, GOST256
- Overall enhance the ADMINISTER KEY MANAGEMENT command
  - One command to administer TDE master encryption key and wallets
  - Supports united and isolated mode for PDB TDE master encryption keys
- Enhance v\$encryption\_wallet view to support new features and information eg.
  - tags, activation, backup and more

# ■ Keystores for Pluggable Database

■ PDB can now have its own keystore instead of one for the entire container database

■ **united mode**

- TDE master encryption key for CDB and PDBs reside in the same keystore
- keys are primarily managed from the CDB root

■ **isolated mode**

- PDB has its own keystore
- TDE master encryption keys are managed from the PDB only

# ■ Encryption Wallet

- New dynamic instance initialization parameter **TDE\_CONFIGURATION** to specify the type of keystore
  - FILE configures a TDE keystore.
  - OKV configures an Oracle Key Vault keystore.
  - HSM configures a hardware security module (HSM) keystore.
- New static initialization parameter **WALLET\_ROOT** to specify the keystore path
  - Primarily for TDE software, hardware or Oracle Key Vault keystores
  - Designate the wallet location for other products as well eg. EUS, SSL, Oracle XML DB or Secure External Password Store
- **WALLET\_ROOT** overrides **SQLNET.ENCRYPTION\_WALLET\_LOCATION**
  - **SQLNET.ENCRYPTION\_WALLET\_LOCATION** is default if **WALLET\_ROOT** not set

# ■ Encrypting Sensitive Credential Data (1)

- Data Dictionary may contain sensitive credential data eg. username and password in
  - SYS.LINK\$
  - SYS.SCHEDULER\$\_CREDENTIAL
- By default this information is just obfuscated but a couple of **de-obfuscation** algorithms are available
- One can manually encrypt the data using ALTER DATABASE DICTIONARY
- A TDE wallet is required to enable encryption
  - Oracle ASO **is not required** for to encrypt sensitive credential in data dictionary
  - Has to be done as SYSKM SYSDBA does not work 😊

## ■ Encrypting Sensitive Credential Data (2)

### ■ Status of data dictionary encryption

```
SQL> SELECT * FROM dictionary_credentials_encrypt;  
  
ENFORCEM  
-----  
ENABLED
```

### ■ Enable data dictionary encryption as SYSKM

```
SQL> conn / as syskm  
Connected.  
SQL> ALTER DATABASE DICTIONARY ENCRYPT CREDENTIALS;  
  
Database dictionary altered.
```

# ■ Oracle Data Pump with Encrypted Data Dictionary Data

- Encrypted data dictionary will cause a warning on data pump exports/imports

```
Processing object type SCHEMA_EXPORT/DB_LINK  
ORA-39395: Warning: object SCOTT.SCOTT_TDB122A.POSTGASSE.ORG requires  
password reset after import
```

- Corresponding database links are invalid
- Reset the database link password using ALTER DATABASE LINK after import

```
SQL> ALTER DATABASE LINK scott_tdb122a.postgasse.org  
2 CONNECT TO scott IDENTIFIED BY tiger;
```

```
Database link altered.
```

# ■ Database Replay

- Database Replay now support encryption of sensitive data
- Encryption is defined when starting a workload capture
- Existing workload captures can also be encrypted
- Supported encryption standards
  - NULL Capture files are not encrypted (the default value)
  - AES128 Capture files are encrypted using AES128
  - AES192 Capture files are encrypted using AES192
  - AES256 Capture files are encrypted using AES256
- Requires a software keystore respectively a TDE wallet

## ■ Just a hint Transparent Data Encryption 12cR2

- TDE tablespace **live / online** conversion
  - Encrypt, decrypt or rekey existing tablespace
  - No Data reorganization required for TDE deployment
  - TDE migration does run in the background... it's not “for free”



- Ability to **decrypt** tablespaces
- Full encryption of database including internal Tablespaces
  - SYSTEM, SYSAUX and UNDO
- TDE Tablespace offline conversion to parallelize, use multiple cores, etc..
  - DataGuard first encrypt physical Standby then switchover...
  - Or encrypt Tablespace by Tablespace

# ■ Offline encryption of existing tablespaces

## ■ Take the Tablespace offline

```
ALTER TABLESPACE users OFFLINE NORMAL;
```

## ■ Enable encryption for tablespace **USERS** by tablespace name or by datafile name

- Using default algorithm for offline conversion
- Alternative algorithm only possible with online encryption

```
ALTER TABLESPACE users ENCRYPTION OFFLINE ENCRYPT;
```

```
ALTER DATABASE DATAFILE '/u01/oradata/TDB122A/users01TDB122A.dbf' ENCRYPT;
```

## ■ Bring the tablespace online

```
ALTER TABLESPACE users ONLINE;
```

# ■ Online encryption of existing tablespaces

- Compatible parameter must be at least 12.2.0.0.0
- Enable encryption specifying the GOST 256bit algorithm
  - Encrypted blocks are shown in V\$ENCRYPTED\_TABLESPACES

```
ALTER TABLESPACE sysaux ENCRYPTION ONLINE USING 'GOST256' ENCRYPT  
FILE_NAME_CONVERT = ('sysaux01TDB122A.dbf', 'sysaux01TDB122A_enc.dbf');
```

- Interrupted encryption, decryption or rekey can be completed with clause **FINISH**

```
ALTER TABLESPACE sysaux ENCRYPTION FINISH ENCRYPT  
FILE_NAME_CONVERT = ('sysaux01TDB122A.dbf', 'sysaux01TDB122A_enc.dbf');
```

- Deep rekey with **REKEY** clause. This is doing a re encryption of each block...
- Multiple option for FILE\_NAME\_CONVERT
- Old file will be removed at the end....

## ■ More improvements for TDE tablespaces

TDE Supports decrypt and rekey

■ Encrypted Tablespaces can be fully decrypted

- Encrypted in the cloud and decrypted on-premises

```
ALTER TABLESPACE sysaux ENCRYPTION ONLINE DECRYPT  
FILE_NAME_CONVERT = ('sysauxTDB122A_enc.dbf', 'sysauxTDB122A.dbf');
```

■ Full rekey of encrypted tablespaces by re-encrypt each block with a new master key

- Deep rekey with **REKEY** clause. Re-encryption of each block

```
ALTER TABLESPACE sysaux ENCRYPTION ONLINE REKEY ENCRYPT  
FILE_NAME_CONVERT = ('sysauxTDB122A_enc.dbf', 'sysauxTDB122A_enc2.dbf');
```

# Network

## ■ A couple of new sqlnet.ora parameter

- ACCEPT\_MD5\_CERTS to accept MD5 signed certificates default is FALSE
  - Replaces ORACLE\_SSL\_ALLOW\_MD5\_CERT\_SIGNATURES environment variable
- ACCEPT\_SHA1\_CERTS to not accept SHA1 signed certificates default is TRUE
- ADD\_SSLV3\_TO\_DEFAULT define if SSL\_VERSION=3.0 is accepted default list of SSL\_VERSIONs default is FALSE
  - TRUE / SSL\_VERSION not defined SSL\_VERSION includes 1.2, 1.1, 1.0, 3.0
  - FALSE / SSL\_VERSION not defined SSL\_VERSION includes 1.2, 1.1, 1.0
- WALLET\_ROOT and TDE\_CONFIGURATION init.ora parameter do override SQLNET.ENCRYPTION\_WALLET\_LOCATION

## ■ More on network

### ■ SSL / TLS / Cipher still a heck of challenge

- SSL / TLS poodle and other vulnerabilities
- Which SSL / TLS is required, requested or supported?
- LDAP problem with EUS and SSL v3 Bug 19285025 and more

### ■ Support of new encryption algorithms (ok that's Oracle 12c R2 ☺ )

- Analog to the algorithms of TDE
- SEED128 with a key length of 128-bit
- ARIA128, ARIA192 und ARIA256 with the corresponding key lengths
- GOST256 with a key length of 256-bit

# Conclusion

- The Killer feature this release is Centrally Managed User with its simple AD integration
  - Ideal solution for central user management in small / midsize environments
  - Not a replacement for Oracle Enterprise User Security
- Many other improvements are due to Oracle's cloud strategy
  - Necessary and meaningful but not earth-shattering

**18<sup>c</sup>** ORACLE<sup>®</sup>  
Database

**trivadis**  
makes IT easier. ■ ■ ■

# Question & Answers

Stefan Oehrli

Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55

stefan.oehrli@trivadis.com



 @stefanoehrli

<http://www.oradba.ch>



**trivadis**  
makes IT easier. ■ ■ ■