

# Oracle 12c R2 New Security Features

An overview on the latest security features

Stefan Oehrli




Trivadis  
makes IT  
easier.

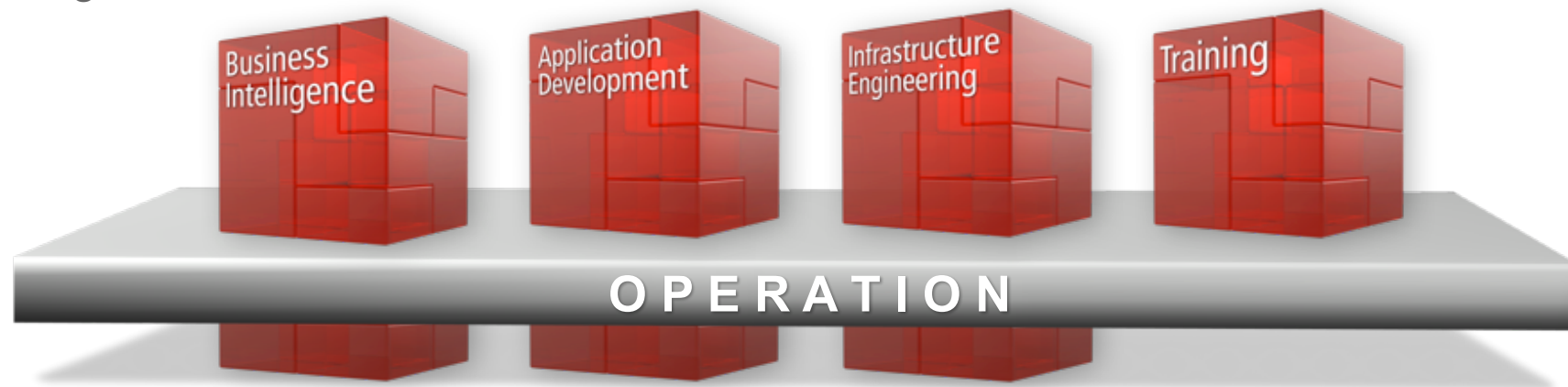
BASEL ▪ BERN ▪ BRUGG ▪ DÜSSELDORF ▪ FRANKFURT A.M. ▪ FREIBURG I.BR. ▪ GENF  
HAMBURG ▪ KOPENHAGEN ▪ LAUSANNE ▪ MÜNCHEN ▪ STUTTGART ▪ WIEN ▪ ZÜRICH

**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

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

### IT Experience

- Consultant for DB Admin and DB security solutions
- Admin of complex and heterogeneous DB Systems
- Head of DBA Team

### Specialization

- DB Security and Operation
- Security Concepts
- Security Reviews
- Oracle Backup & Recovery

### Skills

- Backup & Recovery
- Oracle Advanced Security
- Oracle AVDF und DB Vault
- Oracle Directory Services
- Team / Project Management

# ■ Agenda

1. Authentication
2. Authorization
3. Auditing
4. Confidentiality of Data
5. Network
6. Summary

# Authentication

## ■ Password Hash's

- Oracle patchset 12.1.0.2 introduced SHA-2 support for 12c password version
  - New additional password verifier respectively hash in spar4 column
- Strong password verifiers by default
  - `ALLOWED_LOGON_VERSION_SERVER` defaults to 12 (use to be 8)
  - By default just the 11g and 12c password verifier (hash) is created
  - 10g password verifier is only created with `ALLOWED_LOGON_VERSION_SERVER` set to 11
- Higher security but less compatibility
  - There are still plenty of applications which can not handle case sensitive passwords



## ■ Automatic Account Locking

- Lock inactive users, e.g. lock user which have not logged in for n days
  - Set `INACTIVE_ACCOUNT_TIME` in an Oracle profile
  - Value between 15 and 24855 or set to `UNLIMITED`
  - `LAST_LOGIN` time is used
- New columns in **DBA\_USERS** according to `cdenv.sql`
  - `LOCAL_TEMP_TABLESPACE` – Default local temporary tablespace for the user
  - `INHERITED` – Was user definition inherited from another container
  - `DEFAULT_COLLATION` – User default collation
  - `IMPLICIT` – Is this user a common user created by an implicit application

# ■ Kerberos Authentication

- Revision of Kerberos stack (again... 🤔)
  - KERBEROS5PRE not used anymore
  - Supports the MIT Kerberos 5 Release 1.8
  - Supports the environment variable **KRB5\_TRACE**
    - ➔ finally some kind of a Kerberos Trace file



```
[6809] 1473350974.161563: Resolving hostname mneme08.postgasse.org.  
[6809] 1473350974.162656: Sending initial UDP request to dgram 192.168.56.71:88  
[6809] 1473350974.163829: Received answer (1373 bytes) from dgram 192.168.56.71:88  
[6809] 1473350974.164486: Response was not from master KDC  
[6809] 1473350974.164533: Decoding FAST response  
[6809] 1473350974.164668: TGS reply is for soe@POSTGASSE.ORG -> krbtgt/POSTGASSE.ORG@POSTGASSE.ORG  
with session key aes256-cts/9C94  
[6809] 1473350974.164745: Got cred; 0/Success  
[6824] 1473350974.172743: Storing soe@POSTGASSE.ORG -> krbtgt/POSTGASSE.ORG@POSTGASSE.ORG in  
FILE:/u00/app/oracle/network/admin/krbcache
```

# ■ Kerberos Authentication

## ■ Introduction of **okcreate**

- Simplify the creation of keytabs from the KDC or a service endpoint
- But okcreate does use ssh to get the keytab from KDC (MS AD and SSH!?)

## ■ Generic **krb5.conf** to enable realm and KDC information to be automatically retrieved from the DNS information

- Automatic KDC discovery when configuring OCI Clients
- No need to deploy krb5.conf file on clients, just the **sqlnet.ora** with basic settings
- No krb5.conf means also less misconfiguration

# ■ Kerberos Authentication

- It does work sort of...

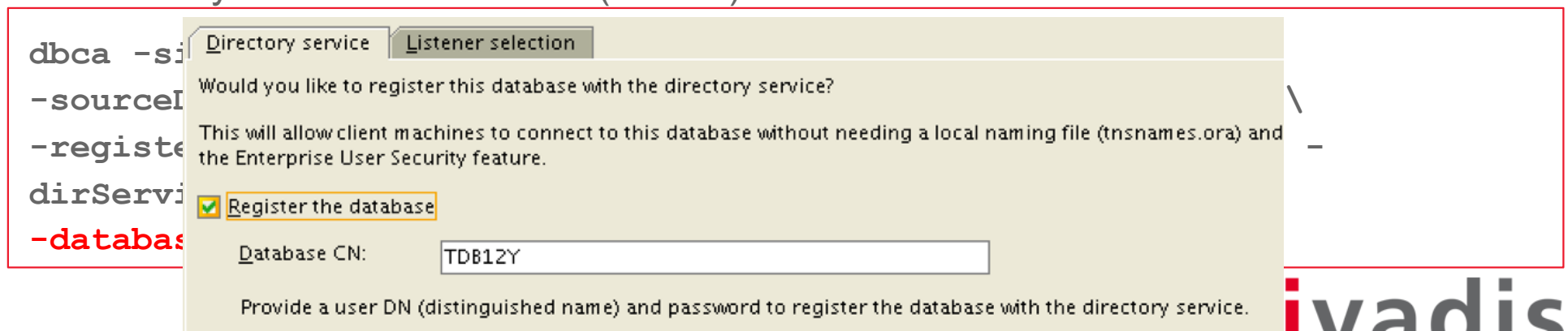
```
SQL> connect /@TDB12X
Connected.
SQL> show user
USER is "SOE@POSTGASSE.ORG"
SQL> exit
Disconnected from Oracle Database 12c Enterprise Edition Release 12.2.0.0.2 - 64bit
With the Partitioning, OLAP, Advanced Analytics and Real Application Testing options
ORA-24550: signal received: [si_signo=11] [si_errno=0] [si_code=128] [si_int=0] [si_ptr=(nil)]
[si_addr=(nil)]
kpedbg_dmp_stack()+400<-kpeDbgCrash()+210<-kpeDbgSignalHandler()+121<-skgesig_sigactionHandler()+272<-
__sighandler()<-_int_free()+1040<-nauztk5adisconnect()+3900<-snau_dis()+1462<-nadisc()+323<-
nnsnadisc()+339<-nsclose()+723<-nioqds()+417<-upidhs()+213<-kputdtch()+513<-aficntdta()+107<-
aficexf()+43<-aficex()+366<-afiexi()+1086<-aficmd()+2926<-aficfd()+3053<-aficdr()+151<-afidrv()+5613<-
main()+105<-__libc_start_main()+253
Segmentation fault (core dumped)
```

**Quote:** Kerberos is Hell, but as soon as it does work, it's nice and cosy...

...and now a bit cosier

# ■ Enterprise User Security

- SSL / TLS Version and Vulnerabilities still somehow around
  - LDAP Issue with EUS and SSL v3 Bug 19285025
  - Oracle 12.2. EUS with OUD is broken Bug/Patch 26093306
- Custom name entry for the Database in the Oracle Directory
- Undocumented Parameter in **dbca** -databaseCN
  - Useful for Oracle DataGuard to register DB Unique Name
  - Already available since 12.1 (hidden)



## ■ Enterprise User Security

- SSL / TLS Version and Vulnerabilities still somehow around
  - LDAP Issue with EUS and SSL v3 Bug 19285025
  - Oracle 12.2. EUS with OUD is broken Bug/Patch 26093306
- Custom name entry for the Database in the Oracle Directory
- Undocumented Parameter in **dbca** -databaseCN
  - Useful for Oracle DataGuard to register DB Unique Name
  - Already available since 12.1 (hidden)

```
dbca -silent -configureDatabase \  
-sourceDB TDB12X -sysDBAUserName sys -sysDBAPassword manager \  
-registerWithDirService true -dirServiceUserName cn=orcladmin -  
dirServicePassword manager -walletPassword TVD04manager \  
-databaseCN TE122
```

# ■ Enterprise User Security

- SSL / TLS Version and Vulnerabilities still somehow around
  - LDAP Issue with EUS and SSL v3 Bug 19285025
  - Oracle 12.2. EUS with OUD is broken Bug/Patch 26093306
- Custom name entry for the Database in the Oracle Directory
- Undocumented Parameter in **dbca** -databaseCN
  - Useful for Oracle DataGuard to register DB Unique Name
  - Already available since 12.1 (hidden)

Directory service | Listener selection

Would you like to register this database with the directory service?

This will allow client machines to connect to this database without needing a local naming file (tnsnames.ora) and the Enterprise User Security feature.

Register the database

Database CN:

Provide a user DN (distinguished name) and password to register the database with the directory service.

# Authorization



## ■ Administrative Privileges / SYSRAC Roles

- The **SYSRAC** Administrative Privilege allows the **SYSRAC** user to manage Oracle Real Application Clusters
- Users with **SYSRAC** can
  - **start, mount** instance and open database
  - **stop, unmount** instance and close database
  - Register Database Set Listener and configure Service
  - This right allows the user to execute different activities without seeing data
  - The session user is "SYSRAC"

## ■ Multitenant Security

- Ability to set the identity of the OS user for PDBs
- Define OS user by **PDB\_OS\_CREDENTIAL**
- Create a credential with **DBMS\_CREDENTIAL.CREATE\_CREDENTIAL**

```
BEGIN DBMS_CREDENTIAL.CREATE_CREDENTIAL (  
    credential_name => 'CDB1_PDB1_OS_USER', username => 'os_admin',  
    password => 'password');  
END;
```

- Limited OS interactions
  - External jobs that do not already have an operating system credential specified
  - External table pre-processors
  - PL/SQL library executions

## ■ PDB Lockdown Profile

- PDB Lockdown Profiles to Restrict Operations on PDBs
  - Restrict functionality available to users in a given PDB
  - Eg. disable specific privileges of ALTER SYSTEM
  - PDB profiles custom security policies for an application
  - Designed for both Cloud and non-Cloud environments
- Designed for Use Case where Identities are shared...
  - ... at os level when DB interact with OS
  - ... at network level eg. Network access features like UTL\_TCP, UTL\_HTTP, etc
  - ... Inside the DB when access common user or objects
  - ... when using administrative features and xml features

# ■ PDB Lockdown Profile

## Default PDB Lockdown Profiles

- PRIVATE\_DBAAS, restrictions suitable for private Cloud DBaaS deployments
  - Same DBA for all PDB, different User, different Applications
- SAAS, restrictions suitable for SaaS deployments
  - Same DBA for all PDB, different User, same Applications
- PUBLIC\_DBAAS, restrictions suitable for public Cloud DBaaS deployments
  - Different DBA for each PDB, different User, different Applications

# ■ PDB Lockdown Profiles

## ■ Create a Lockdown Profiles

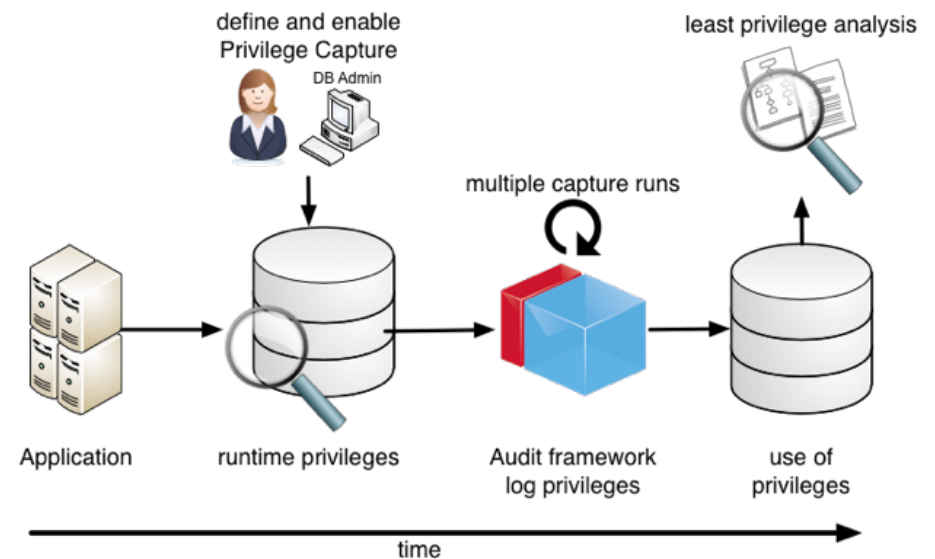
```
CREATE LOCKDOWN PROFILE scott_pdb;  
ALTER LOCKDOWN PROFILE scott_pdb DISABLE STATEMENT = ('ALTER SYSTEM');  
ALTER LOCKDOWN PROFILE scott_pdb ENABLE STATEMENT = ('ALTER SYSTEM')  
clause = ('kill session');
```

## ■ Enable Lockdown Profiles on PDB level

```
connect admin@pdb1  
ALTER SYSTEM SET PDB_LOCKDOWN = scott_pdb SCOPE = SPFILE;  
ALTER PLUGGABLE DATABASE scott_pdb CLOSE;  
ALTER PLUGGABLE DATABASE scott_pdb OPEN;
```

# ■ Privilege Analysis Improvements

- Additional privilege capture for rights and invoker's rights, Code Based Access Control and Secure Application Role use
- Unused privilege grants
  - Capture Report indicates with privileges where not used
- Multiple capture runs
  - Define multiple capture runs
  - Run comparison report
  - Identify changes and progress simplify “least privilege”



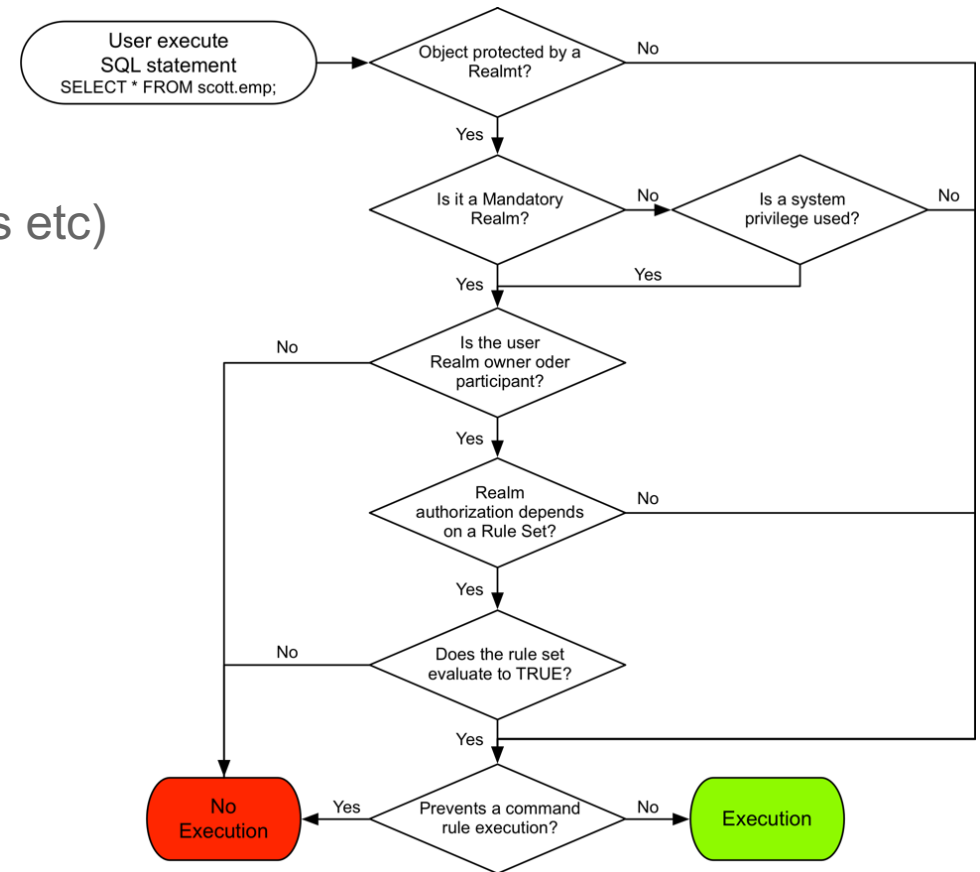
# Database Vault Improvements

## ■ DB Vault Simulation Mode

- Enable DB Vault (realms, command rules etc)
- Report security violations
- Access to objects is not blocked
- Verify DB Vault, Application Certification, verify changes etc

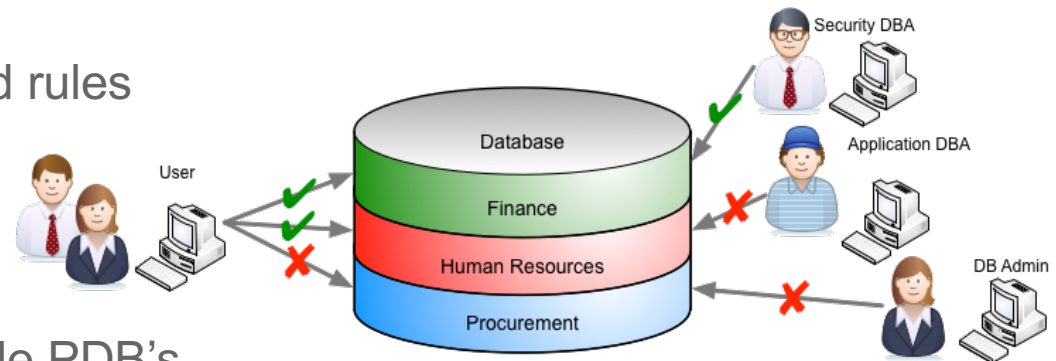
## ■ New data dictionary view

DVSYSDBA.DV\_TRAINING\_LOG  
to analyze simulation



# Database Vault Improvements

- Oracle Database Vault Policies
  - Group / Manage realms and command rules that belong together
- Common Realms and Command Rules
  - Created in the CDB
  - Centrally managed and used in multiple PDB's
- Changed Default Value for SQL92\_SECURITY
  - New Default Value TRUE (set to TRUE any way when enable DB Vault)
  - Requires an explicit SELECT privilege to DELETE / UPDATE a table
- DB Vault introduce support for Flashback Technology and ILM
  - Control access to objects when using Oracle Flashback features
  - Eg. protect PURGE TABLE, PURGE INDEX, FLASHBACK TABLE etc





# Auditing

## ■ Audit Policy Enhancements

- Enable audit policy for groups of users through roles
  - New clause **BY USERS WITH GRANTED ROLES** for **AUDIT** and **NOAUDIT**
- Define a new audit policy audit any select on **SYS.USER\$**

```
CREATE AUDIT POLICY audit_test01 ACTIONS SELECT ON sys.user$;
```

- Enable it for all user having the **DBA** role

```
AUDIT POLICY audit_test01 BY USERS WITH GRANTED ROLES dba;
```

# ■ Audit Policy Enhancements

## ■ Additional Attributes in AUDIT\_UNIFIED\_ENABLED\_POLICIES

- ENTITY\_NAME captures the user name or role name
- ENTITY\_TYPE indicates if the entity name is a USER or a ROLE
- ENABLED\_OPT displays BY and EXCEPT for policies that are enabled on users, but displays **INVALID** for policies that are enabled on roles

```
SELECT * FROM audit_unified_enabled_policies;
```

USER_NAME	POLICY_NAME	ENABLED_OPT	ENABLED_OPTION	ENTITY_NAME	ENTITY_TYPE	SUC	FAI
	AUDIT_TEST01	<b>INVALID</b>	BY GRANTED ROLE	DBA	ROLE	YES	YES
ALL USERS	ORA_SECURECONFIG	BY	BY USER	ALL USERS	USER	YES	YES
ALL USERS	ORA_LOGON_FAILURES	BY	BY USER	ALL USERS	USER	NO	YES

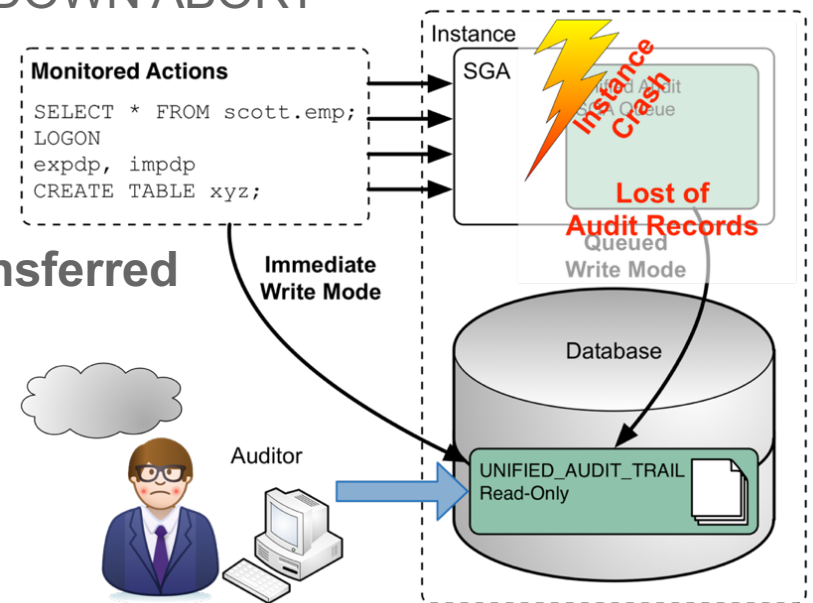
## ■ Unified Audit Enhancements

- New audit events for Oracle database real application security
  - AUDIT\_GRANT\_PRIVILEGE
  - AUDIT\_REVOKE\_PRIVILEGE
- Capture Oracle virtual private database predicates
  - New column RLS\_INFO in UNIFIED\_AUDIT\_TRAIL, DBA\_AUDIT\_TRAIL, V\$XML\_AUDIT\_TRAIL and DBA\_FGA\_AUDIT\_TRAIL
  - Detailed information about the VPD predicates

```
SQL> SELECT rls_info FROM unified_audit_trail WHERE rls_info IS NOT NULL;
RLS_INFO
-----
((POLICY_TYPE=[3] 'VPD'), (POLICY_SCHEMA=[6] 'SECUSR'),
(POLICY_NAME=[10] 'EMP_POLICY
```

# ■ New Unified Audit Trail

- 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
  - Data is written automatically in a new internal relational table
  - Existing unified audit records have to be **transferred**
- Default Write Mode still set to QUEUED
  - Can be changed by dbms\_audit\_mgmt
  - Impact?



# Confidentiality of data

# ■ Transparent Sensitive Data Protection TSDP

- Define sensitive data types in the database and classify the data to be protect
- Protecting a Class with appropriate TSDP policies
  - Protection of data / columns with VPD or Data Redaction
  - Use / definition of uniform policies for all classified data
- Assignment of TSDP policies in other databases
  - Company-wide protection of sensitive data
- New TSDP Policies covering the following security features
  - Unified auditing policies
  - Fine-grained auditing policies
  - Transparent Data Encryption column encryption

# ■ Data Redaction

- Create named data redaction policy expressions
  - Reuse a named expression in multiple redaction policies
  - Updates made to a named policy expression apply to all the column associations

- Ability to display redacted data using null values
  - New function parameter `DBMS_REDACT.NULLIFY`

- Additional expression function support for data redaction policies
  - `SUBSTR`, `LENGTH`, `LENGTHB`, `LENGTHC`, `LENGTH2`, and `LENGTH4`

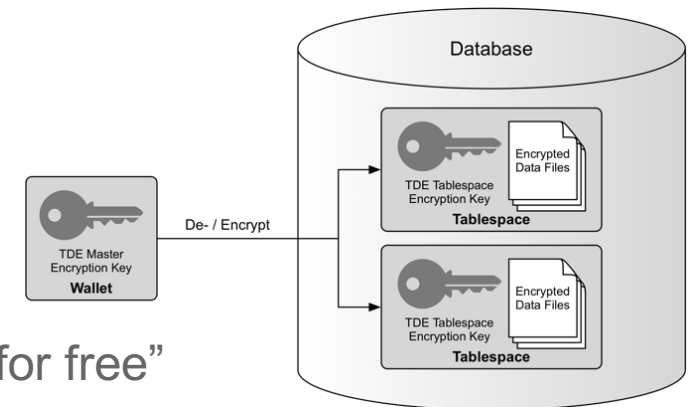
- Enhanced support for redacting unstructured data
  - Regular expression-based redaction for `CLOB` and `VCLOB` data types
  - Oracle 12c R1 did only support full redaction for `CLOB/VCLOB` eg. display **[redacted]**

Original -> Redacted	
✓ Random Redaction	4022-5231-5531-9855 -> 4042-6344-0547-9855 09/30/73 -> 11/30/73
✓ RegExp Redaction	94025-2450 -> 94025-[hidden] tom.lee@acme.com -> [redacted]@acme.com
✓ Partial Redaction	068-35-2299 -> ***-**-2299 D1L86YZV8K -> D1*****8K
✓ Full Redaction	05/24/75 -> 01/01/01 11 Rock Bluff Dr. -> XXXXXXXXX



# ■ Overview Transparent Data Encryption

- 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



## ■ TDE Initialization Parameter

- Introduction of initialization parameter `ENCRYPT_NEW_TABLESPACES`
  - New tablespaces will be encrypted with AES128
  - That's Oracle's "Cloud Databases are always encrypted"
  - TDE encryption wallet has to be configured on opened beforehand
- Possible values are
  - `CLOUD_ONLY`                      Only tablespaces in the Cloud are encrypted
  - `ALWAYS`                              Any new tablespaces are encrypted
  - `DDL`                                      Specified by the DDL Statement
- Although there is a hidden parameter `_default_encrypt_alg` its currently not possible to change the default encryption algorithm
- There are a couple of other hidden parameter related to encryption

# ■ Hidden Parameter

## ■ Some hidden Parameter related to encryption

Parameter	Instance	Description
<code>_backup_encrypt_opt_mode</code>	4294967294	specifies encryption block optimization mode
<code>_db_disable_temp_encryption</code>	FALSE	Disable Temp Encryption for Spills
<code>_db_flash_cache_encryption</code>	FALSE	Set <code>_db_flash_cache_encryption</code> to enable flash cache encryption
<code>_db_writer_coalesce_encrypted_buffers</code>	TRUE	Coalescing for encrypted buffers
<code><b>_default_encrypt_alg</b></code>	0	default encryption algorithm
<code>_kdlxp_lobencrypt</code>	FALSE	enable lob encryption - only on SecureFiles
<code>_override_datafile_encrypt_check</code>	FALSE	if TRUE, override datafile tablespace encryption cross check
<code>_stats_encryption_enabled</code>	TRUE	Enable statistics encryption on sensitive data
<code>_use_hybrid_encryption_mode</code>	FALSE	Enable platform optimized encryption in hybrid mode
<code>_use_platform_encryption_lib</code>	TRUE	Enable platform optimized encryption implementation
<code>encrypt_new_tablespaces</code>	ALWAYS	whether to encrypt newly created tablespaces

# ■ TDE Software Keystore

- Support to store software keystore in ASM....

```
ENCRYPTION_WALLET_LOCATION=  
  (SOURCE=  
    (METHOD=FILE)  
    (METHOD_DATA=(DIRECTORY=+disk1/mydb/wallet)))
```

- Configure an external keystore to store the credentials for the software keystore
  - Store the key for the key somewhere else... eg. the **cwallet.sso** file
  - Location specified with init.ora parameter  
EXTERNAL\_KEYSTORE\_CREDENTIAL\_LOCATION
  - Avoid hard-coding the password in a scripts but it is not AUTOLOGIN
  - Different PDBs can use the same external credential store

## ■ Prepare Software Keystore for TDE

### ■ Create the TDE software keystore (wallet)

```
ADMINISTER KEY MANAGEMENT CREATE KEYSTORE  
'/u00/app/oracle/admin/TDB12X/tde_wallet' IDENTIFIED BY TVD04manager;  
  
ADMINISTER KEY MANAGEMENT CREATE LOCAL AUTO_LOGIN KEYSTORE FROM KEYSTORE  
'/u00/app/oracle/admin/TDB12X/tde_wallet' IDENTIFIED BY TVD04manager;
```

### ■ Open the wallet and create a master key

```
ADMINISTER KEY MANAGEMENT SET KEYSTORE OPEN IDENTIFIED BY TVD04manager;  
  
ADMINISTER KEY MANAGEMENT SET KEY USING TAG 'initial_TDE_master'  
IDENTIFIED BY TVD04manager WITH BACKUP;
```

## ■ Create new TDE Tablespaces

- Adjust Initialization parameter ENCRYPT\_NEW\_TABLESPACES to ALWAYS

```
ALTER SYSTEM SET encrypt_new_tablespaces=ALWAYS SCOPE=both;
```

- Create a new tablespace using the default algorithm

```
CREATE TABLESPACE tde_aes128 DATAFILE  
'/u02/oradata/TDB12X/tde_aes12801TDB12X.dbf'  
SIZE 10M AUTOEXTEND ON MAXSIZE 100M;
```

- Create a new tablespace with explicitly set encryption with algorithm AES256

```
CREATE TABLESPACE tde_aes256 DATAFILE  
'/u02/oradata/TDB12X/tde_aes25601TDB12X.dbf' SIZE 10M AUTOEXTEND ON  
MAXSIZE 100M ENCRYPTION USING 'AES256' ENCRYPT;
```

## ■ Review the new TDE Tablespaces

- The view V\$ENCRYPTED\_TABLESPACES provides information on
  - Encryption algorithm
  - Amount of encrypted / decrypted blocks

```
SQL> col name for a12
```

```
SQL> SELECT name, encryptionalg, status, blocks_encrypted,  
2 blocks_decrypted FROM v$encrypted_tablespaces e,  
3 v$tablespace t WHERE e.TS#=t.TS#;
```

NAME	ENCRYPT	STATUS	BLOCKS_ENCRYPTED	BLOCKS_DECRYPTED
TDE_AES128	AES128	NORMAL	769	0
TDE_AES256	AES256	NORMAL	46	0
TDE_ARIA256	ARIA256	NORMAL	46	0

# ■ 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/TDB12X/users01TDB12X.dbf' ENCRYPT;
```

## ■ Bring the tablespace online

```
ALTER TABLESPACE users ONLINE NORMAL;
```



# ■ 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 additional encryption algorithms

### ■ SEED and ARIA for South Korea...

- SEED is a block cipher algorithm with 128bit Blocks and 128bit Keys developed in the late 1990's
- ARIA is a block cipher algorithm similar to AES with 128bit Blocks and variable Keys (128, 192 or 256) developed in the 2003

### ■ GOST for Russia...

- GOST is a block cipher algorithm similar to DES with 64bit Blocks / 256bit Keys developed in the 1970's

## ■ Weiter Verbesserungen für TDE

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');
```

- Rekey – re-encrypt each block with the new Master Key
  - Deep rekey with **REKEY** clause. Each block will be encrypted.

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

# Network

## ■ Network

- No significant "New Security Features" for Oracle network SQLNet
- Existing problems and vulnerabilities
  - SSL / TLS Poodle Vulnerability
  - LDAP problems with EUS and SSL v3 Bug 19285025
  - Memory Leak when using the integrity checks with the new SHA Checksums
- Support new encryption algorithms
  - Analogous to the algorithms used for TDE
  - SEED128 with a key length of 128-bit
  - ARIA128, ARIA192 with ARIA256 corresponding key lengths
  - GOST256 with a key length of 256-bit

# Summary

- Not as many new security features like for Oracle 12c Release 1
  - But a few reasonable improvements
  - Some “must have” for cloud environments
- Finally live conversion of tablespaces including encrypt, decrypt and rekey

# Questions and Answers

Stefan Oehrli  
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55  
[stefan.oehrli@trivadis.com](mailto:stefan.oehrli@trivadis.com)

