Oracle 12c R2 New Security Features

Ein Überblick über die aktuellsten Security Features

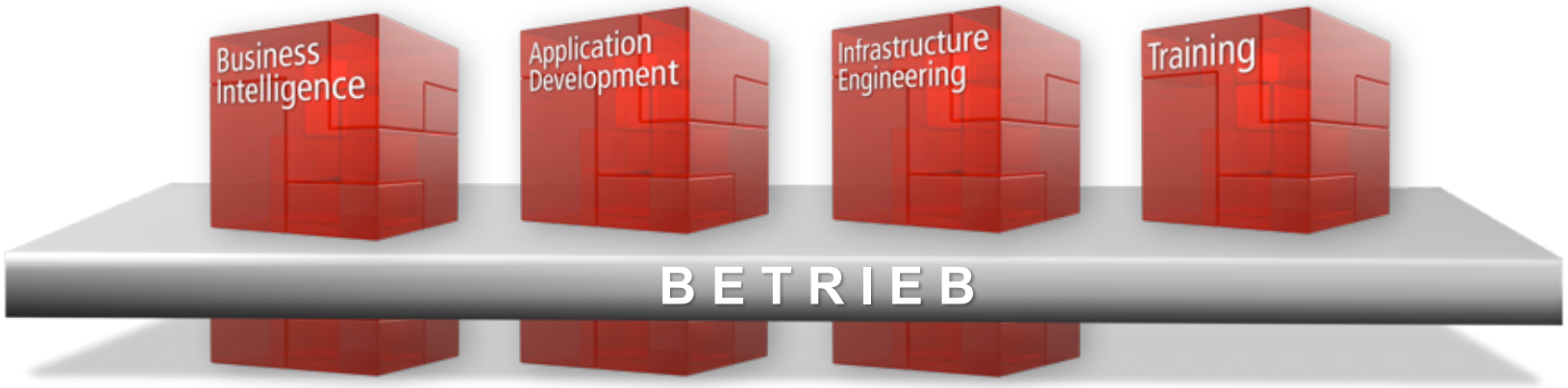
Stefan Oehrli

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

trivadis
makes IT easier.

Unser Unternehmen.

Trivadis ist führend bei der IT-Beratung, der Systemintegration, dem Solution Engineering und der Erbringung von IT-Services mit Fokussierung auf ORACLE - und Microsoft -Technologien in der Schweiz, Deutschland, Österreich und Dänemark. Trivadis erbringt ihre Leistungen aus den strategischen Geschäftsfeldern:



Trivadis Services übernimmt den korrespondierenden Betrieb Ihrer IT Systeme.

trivadis makes IT easier.

Mit über 600 IT- und Fachexperten bei Ihnen vor Ort.

- 14 Trivadis Niederlassungen mit über 600 Mitarbeitenden.
- Über 200 Service Level Agreements.
- Mehr als 4'000 Trainingsteilnehmer.
- Forschungs- und Entwicklungsbudget: CHF 5.0 Mio.
- Finanziell unabhängig und nachhaltig profitabel.
- Erfahrung aus mehr als 1'900 Projekten pro Jahr bei über 800 Kunden.

trivadis makes IT easier.

Technik allein bringt Sie nicht weiter.

Man muss wissen, wie man sie richtig nutzt.

trivadis
makes IT easier.

Stefan Oehrli

Solution Manager BDS SEC

- Seit 1997 IT-Bereich tätig
- Seit 2008 bei der Trivadis AG
- Seit 2010 Disziplin Manager SEC INFR
- Seit 2014 Solution Manager BDS Security

IT Erfahrung

- DB Administration und DB Security Lösungen
- Administration komplexer, heterogenen Umgebungen
- Datenbank Teamleiter

Spezialgebiet

- Datenbank Sicherheit Security und Betrieb
- Security Konzepte
- Security Reviews
- Oracle Backup & Recovery

Skills

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

trivadis
makes IT easier.

Agenda

1. Authentifizierung
2. Autorisation
3. Auditing
4. Vertraulichkeit der Daten
5. Netzwerk
6. Zusammenfassung

Authentifizierung

Password Hash‘s

- Mit Oracle Patch Set 12.1.0.2 wird SHA-2 Support für 12C Password Version
  - Neuer zusätzlicher Password Hash in der Spalte *spare4* in *user$*
- Standardmässig starke Password Hash‘s
  - Standardwert von ALLOWED_LOGON_VERSION_SERVER ist 12 war früher 8
  - Standardmässig wird nur der 11g und 12c Password Hash erzeugt
  - 10g Password Hash werden nur erstellt wenn ALLOWED_LOGON_VERSION_SERVER auf 11 steht
- Höhere Sicherheit aber reduzierte Komplexität
  - Es gibt immer noch eine Unzahl von Anwendungen, welche nicht mit Case Sensitiven Passwörter umgehen können

Automatische Sperrung von Accounts

- Sperren der inaktiven Benutzer bzw. sperren von Benutzer die n Tagen nicht mehr eingeloggt waren
  - Setzen von INACTIVE_ACCOUNT_TIME in einem Oracle Profile
  - Wert zwischen 15 u d 24855 oder auf UNLIMITED gesetzt
  - LAST_LOGIN_TIME wird verwendet
- Neue Spalten in DBA_USERS gemäss cdenv.sql
  - LOCAL_TEMP_TABLESPACE – Standard Lokales Temp Tablespace
  - INHERITED – Wurde dieser Benutzer durch einen weiteren Container vererbt
  - DEFAULT_COLLATION – Standard Kollation vom Benutzer
  - IMPLICIT – Ist dieser Benutzer ein allgemeiner Benutzer oder impliziert durch eine Applikation erstellt

Kerberos Authentifizierung

- Der Kerberos Stack überarbeitet (schon wieder…)
  - KERBEROS5PRE wird nicht mehr verwendet
  - Support für MIT Kerberos 5 Release 1.8
  - Support die Umgebungsvariable KRB5_TRACE
    ➡ Endlich etwas wie eine Kerberos Trace Datei

```
[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 Authentifizierung

- Neues Tool **okcreate**
  - Vereinfacht das erstellen des Keytab Files auf dem KDC oder einem Service End Point
  - **okcreate** verwendet ssh um die keytab Datei vom KDC zu kopieren
    MS AD und SSH!?
- Generisches ***krb5.conf*** für das automatische festlegen des Realms und der KDC Informationen abhängig von den DNS Einträgen
  - Automatisches KDC Discovery für OCI Clients
  - Es ist nicht nötig die *krb5.conf* Datei auf Clients zu verteilen, es braucht lediglich ein *sqlnet.ora* mit Grundeinstellungen
  - Kein *krb5.conf* bedeutet auch weniger Fehlkonfigurationen

Kerberos Authentifizierung

- Es funktioniert so einigermassen...

Zitat: Kerberos ist die Hölle, aber sobald es einmal läuft ist schön und gemütlich…

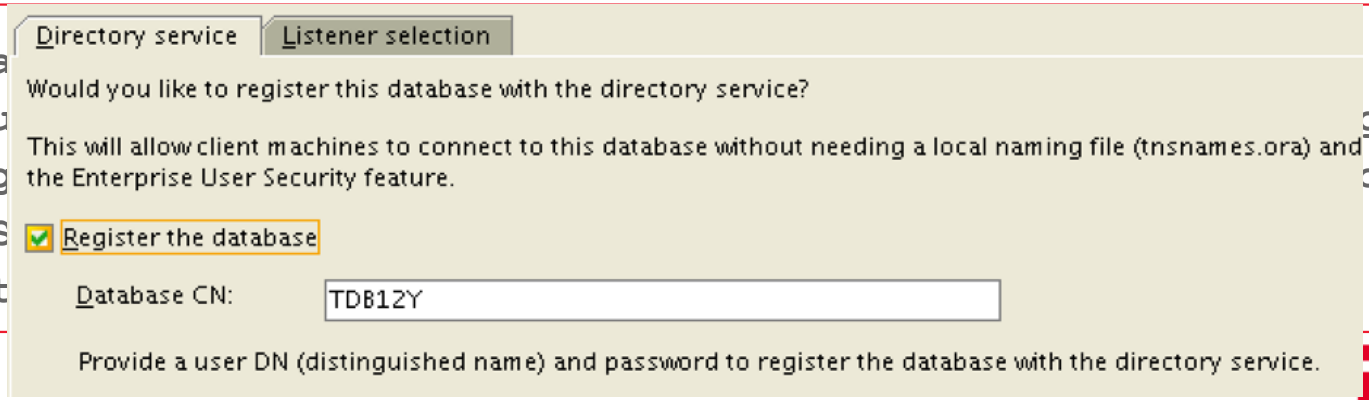
…und jetzt etwas gemütlicher

```
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 Beta
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<-
nsnadisc()+339<-nsclose()+723<-nioqds()+417<-upidhs()+213<-kpudtch()+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)
```

Enterprise User Security

- SSL / TLS Version und Sicherheitslücken sind immer noch da
  - ORA-28030 EUS Problem mit LDAP und SSL v3 Bug 19285025
- Kundenspezifischer DB / Service Name im Verzeichnis
- Nicht dokumentierter Parameter in **dbca** -databaseCN
  - Nützlich für Oracle DataGuard und dir Registrierung des DB Unique Name
  - Bereits in 12.1 vorhanden (hidden)

```
dbca
-sou                                                    ger \
-reg                                                    dmin -
dirS
-dat
```



Autorisation

Administrative Privilegien / Rollen SYSRAC

- Das SYSRAC Administrative Privileg erlaubt dem SYSRAC Benutzer das verwalten des Oracle Real Application Clusters
- Benutzer mit SYSRAC dürfen
  - **start**, **mount** der Instanz und öffnen der Datenbank
  - **stop**, **unmount** der Instanz und schliessen der Datenbank
  - Registrieren einer Database set des Listener und Konfigurieren von Services
  - Abfragen der entsprechenden DBA_xyz, GV$, und V$ Views aber ohne das Recht **SELECT ANY TABLES**
  - Session Benutzer ist ”SYSRAC”

PDB Betriebssystem Benutzer

- Möglichkeit einen OS Benutzer für die PDB festzulegen
- Definieren des OS Benutzers mit **PDB_OS_CREDENTIAL**
- Erstellen der Credential mit **DBMS_CREDENTIAL.CREATE_CREDENTIAL**

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

- Einschränken der Betriebssystem Interaktionen
  - Dezidierter Benutzer für externe Jobs
  - Per-Prozessoren für Externe Tabellen
  - Ausführung von PL/SQL Library

PDB Lockdown Profile

- PDB Lockdown Profile um Operationen auf PDBs zu einzuschränken
  - Einschränkung der Funktionalität für Benutzer in einer bestimmten PDB
  - Z.B. ausschalten von spezifischen ALTER SYSTEM Privilegien
  - PDB Profile für kundenspezifische Sicherheitspolicies für eine Anwendung
  - Entwickelt sowohl für Cloud wie auch für On-Premises Umgebungen
- Entwickelt für Use Case wo Identities geteilt werden…
  - … auf OS Eben wenn die DB mit dem OS interagiert
  - ... auf Netzwerk Ebene z.B. bei der Verwendung von UTL_TCP, UTL_HTTP, etc.
  - ... Innerhalb der DB wenn auf Allgemeine User / Objekte zugegriffen wird
  - … Wenn Administrative Features und xml Features verwendet werden

PDB Lockdown Profile

Standard PDB Lockdown Profiles

- PRIVATE_DBAAS, Einschränkungen für private Cloud DBaaS
  - Gleicher DBA für alle PDB, verschiedene Benutzer, verschiedene Anwendungen
- SAAS, Einschränkungen für SaaS Implementierungen
  - Gleicher DBA für alle PDB, verschiedene Benutzer, gleiche Anwendungen
- PUBLIC_DBAAS, Einschränkungen für public Cloud DBaaS
  - Verschiedene DBA für jeden PDB, verschiedene Benutzer, verschiedene Anwendungen

Authorization – PDB Lockdown Profiles

- Erstellen eines Lockdown Profiles

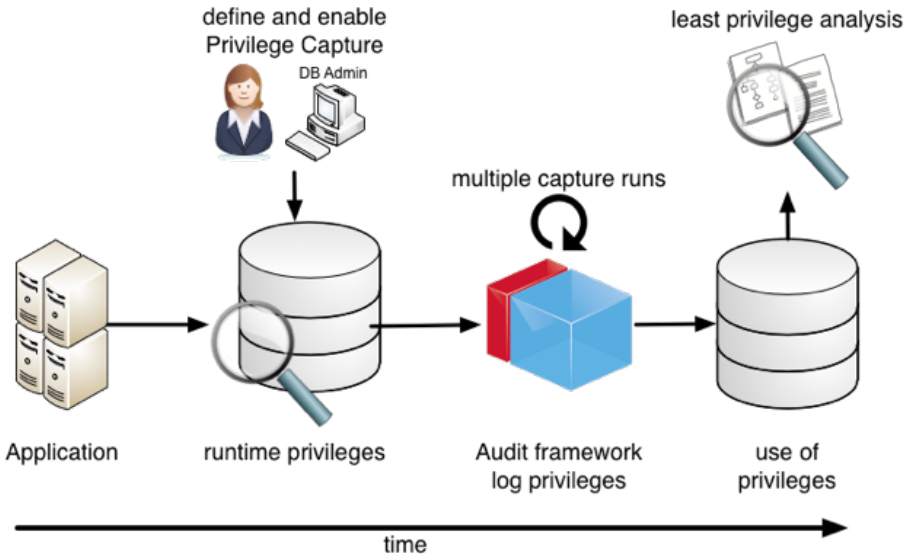
```
CREATE LOCKDOWN PROFILE scott_pdb;
ALTER LOCKDOWN PROFILE scott_pdb DISABLE STATEMENT = ('ALTER SYSTEM');
ALTER LOCKDOWN PROFILE scott_pdb ENABLE STATEMENT = ('ALTER SYSTEM')
clause = ('kill session');
```

- Einschalten des Lockdown Profiles auf PDB Ebene

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

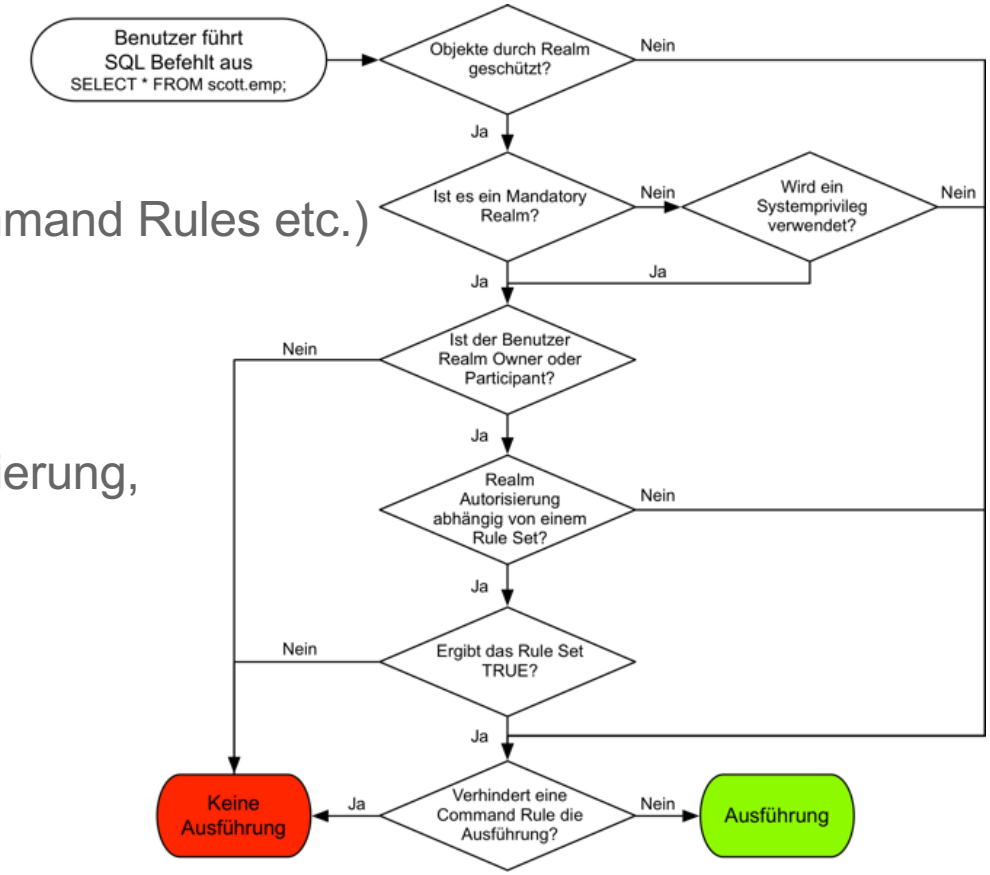
Privilege Analysis improvements

- Erfassung von weiteren Privilegien wie Invoker's Rights, Code Based Access Control und Secure Application Role
- Nichtverwendete Privilegien
  - Capture Report zeigt welche Privilegien nicht verwendet wurden
- Mehrere Capture Runs
  - Definition von mehreren Capture Runs
  - Vergleich der Report
  - Identifikation von Änderungen, einfacheres Umsetzen von "least privilege"



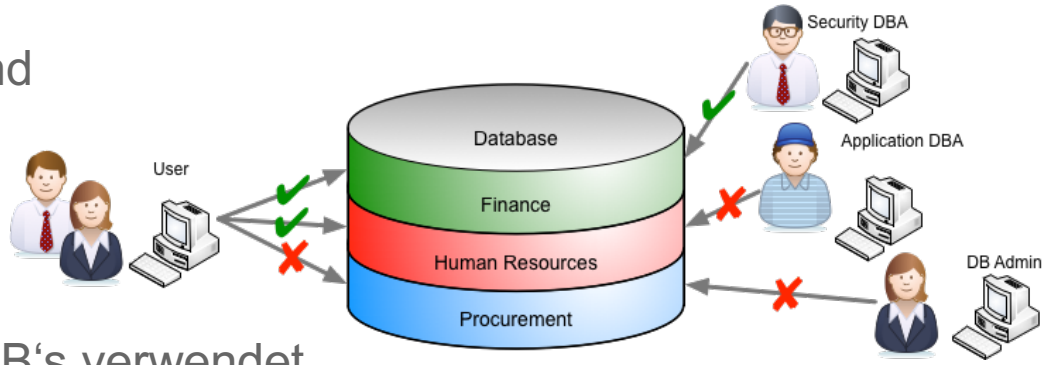
Database Vault Verbesserungen

- DB Vault Simulationsmodus
  - Einschalten von DB Vault (Realms, Command Rules etc.)
  - Rapportieren von Sicherheitsverstössen
  - Zugriff auf die Objekte ist nicht blockiert
  - Prüfen von DB Vault, Applikation Zertifizierung, Prüfen von Änderungen etc.
- Neue Data Dictionary View DVSYS.DBA_DV_TRAINING_LOG zum Analysieren der Simulation



Database Vault Verbesserungen

- Oracle Database Vault Policies
  - Gruppieren von Realms und Command Rules welche zusammen gehören
- Common Realms und Command Rules
  - Erstellt in der CDB
  - Zentral Verwaltet und in mehreren PDB‘s verwendet



- Verhalten von SQL92_SECURITY geändert
  - Neuer Standartwert TRUE (wird sowieso beim einschalten von DBV TRUE)
- DB Vault unterstütz Flashback Technology und ILM
  - Zugriffskontrolle von Objekten die Oracle Flashback Features nutzen
  - Z.B. Schutz von PURGE TABLE, PURGE INDEX, FLASHBACK TABLE etc.

Auditing

Unified Audit Policies

- Aktivieren einer Audit Policy für eine Gruppe von Benutzer durch Rollen
  - Neue Klausel **`BY USERS WITH GRANTED ROLES`** für **`AUDIT`** und **`NOAUDIT`**
- Definieren einer neuen Audit Policy

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

- Für alle Benutzer mit der DBA Rolle aktivieren

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

Unified Audit Policies

- Zusätzliche Attribute in AUDIT_UNIFIED_ENABLED_POLICIES
  - ENTITY_NAME Captures Benutzer oder Rollen Name
  - ENTITY_TYPE Zeigt an, ob es ein USER oder eine ROLE ist
  - ENABLED_OPT Zeigt BY und EXCEPT für Policies, welche aktiviert sind, aber zeigt INVALID für Policies, welche auf eine Rolle eingeschaltet wurden

```
SELECT * FROM audit_unified_enabled_policies;

USER_NAME   POLICY_NAME         ENABLED_OPT ENABLED_OPTION   ENTITY_NAME ENTITY_TYPE SUC FAI
----------- ------------------- ----------- ---------------- ----------- ----------- --- ---
            AUDIT_TEST01        INVALID     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
```

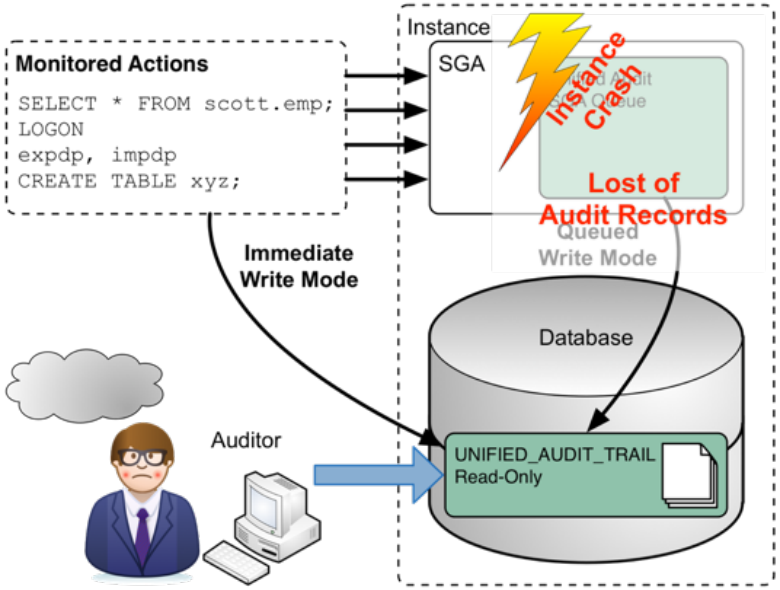
Auditing

- Neue Audit Events für 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 und DBA_FGA_AUDIT_TRAI

```
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
```

Neuer Unified Audit Trail

- Deprecation von UNIFIED_AUDIT_SGA_QUEUE_SIZE
  - Audit Daten werden sofort in eine interne relationale Table geschrieben
  - Kein Datenverlust im Fall eines Instance Crash / SHUTDOWN ABORT
- Abschaffung von Flush der Audit Trail Records
  - Daten werden sofort in eine interne relationale Table geschrieben
  - Existierende Unified Audit Records müssen **Transferiert** werden
- Default Write Mode aber weiterhin auf QUEUED
  - Lässt sich auch ändern
  - Einfluss auf das Verhalten?



trivadis makes IT easier.

Vertraulichkeit der Daten

Transparent Sensitive Data Protection TSDP

- Festlegen von Sensitiven Datentypen innerhalb der Datenbank
- Klassifizierung der zu schützenden Daten
  - Z.B Sensitive Spalten mit Lohn, Kreditkarten Nummern etc.
- Schutz einer Klasse mit entsprechenden TSDP Policies
  - Schutz der Daten / Spalten mit VPD oder Data Redaction
  - Verwendung / Definition von einheitlichen Policies für alle klassifizierten Daten
- Neue TSDP Policies unterstützen die folgenden Security Features
  - Unified Auditing Policies
  - Fine-grained Auditing Policies
  - Transparent Data Encryption column encryption

Data Redaction

- Erstellen von Named Data Redaction Policy Expressions
  - Wieder verwenden von Named Expressions in verschiedenen Policies
  - Updates werden in einer Named Policy Expressions gemacht, sind in allen zugewiesenen Policies aktiv
- Erweiterung der Unterstütze Funktionen für Data Redaction Policies
  - SYS_CONTEXT, XS_SYS_CONTEXT, SUBSTR, LENGTH, LENGTHB, LENGTHC, LENGTH2, and LENGTH4
- Erweiterter Support für Redaction von Unstrukturierten Daten
  - Redaction von CLOB and VCLOB basierend auf Regulären Ausdrücken
  - Oracle 12c R1 unterstützt nur Full Redaction für CLOB/VCLOB. Daten werden als ***[redacted]*** angezeigt.

Transparent Data Encryption TDE

- TDE Tablespaces **live / online** Konvertierung
  - Verschlüsseln, Entschlüsseln oder Rekey eines vorhandenen Tablespaces
  - Keine Datenreorganisation nötig wie bis anhin
  - TDE Migration läuft im Hintergrund … Ist nicht ganz “Gratis”
- Möglichkeit zum **entschlüsseln** eines Tablespaces
- Komplette Verschlüsselung einer DB inklusive internen Tablespaces
  - SYSTEM, SYSAUX und UNDO
- TDE Tablespace offline Konvertierun
  - DataGuard physische Standby verschlüsseln und anschliessend Switchover...
  - Offline Tablespace für Tablespace verschlüsseln

TDE Standard Algorithmus

- Einführung eines neuen Initialisierungsparameter ENCRYPT_NEW_TABLESPACES
  - Neue Tablespaces werden mit **AES128** verschlüsselt
  - Die Oracle Variante von “Cloud Databases are always encrypted”
  - TDE Wallet muss vorgängig konfiguriert und geöffnet sein
- Mögliche Werte
  - CLOUD_ONLY — Nur Tablespace in der Cloud sind verschlüsselt
  - ALWAYS — Jedes neue Tablespace ist verschlüsselt
  - DDL — Verschlüsselung nur durch Angabe in DDL Statement
- Standard Algorithmus nicht anpassbar
  - Auch nicht mit verstecktem Parameter **_default_encrypt_alg**

Versteckte Parameter

- Einige verstecktem Parameter zu Encryption

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

Software Keystore

- Support von ASM zum speichern von Software Keystore....

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

- Konfiguration eines externen Keystore zum Speichern der Credentials des Software Keystore
  - Alternatives Abspeichern des Schlüssels für den Schüssel z.B **cwallet.sso**
  - Lokal mit einen Init.ora Parameter definiert EXTERNAL_KEYSTORE_CREDENTIAL_LOCATION
  - Vermeiden, dass Passwörter Hardcoded in Scripts abgespeichert werden

Vorbereiten des Software Keystore für TDE

- Erstellen des 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;
```

- Öffnen des Wallet und erstellen eines 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;
```

Tablespaces Anlegen

- Anpassen des Initialisierungsparameter ENCRYPT_NEW_TABLESPACES

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

- Erstellen eines Tablespaces mit dem Default Algorithmus

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

- Erstellen eines Tablespaces mit expliziten setzen des Algorithmus AES256

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

Prüfen der neuen TDE Tablespaces

- Die View V$ENCRYPTED_TABLESPACES Informiert über
  - Encryption Algorithmus
  - Menge der verschlüsselten / entschlüsselten Blöcke

```
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 Verschlüsselung von Tablespaces

- Tablespace offline nehmen

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

- Einschalten der Verschlüsselung für Tablespace **USERS** mit Tablespace Name oder mit Datafile Name
  - Verwendung des default Algorithmus für die offline Konvertierung
  - Alternative Algorithmen sind nur mit online Verschlüsselung möglich

```
ALTER TABLESPACE users ENCRYPTION OFFLINE ENCRYPT;
ALTER DATABASE DATAFILE '/u01/oradata/TDB12X/users01TDB12X.dbf' ENCRYPT;
```

- Tablespace online bringen

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

Online Verschlüsselung von Tablespaces

- Kompatible Parameter muss mindestens 12.2.0.0.0 sein
- Einschalten der Verschlüsselung mit dem GOST 256bit Algorithmus
  - Verschlüsselte Blöcke sind in V$ENCRYPTED_TABLESPACES angegeben

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

- Unterbrochene Verschlüsselung, Entschlüsselung oder Rekey kann man mit der Klause **FINISH** beenden

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

- Mehrere Optionen für FILE_NAME_CONVERT
- Alte Dateien werden am Schluss entfernt...

Weiter Verbesserungen für TDE

TDE Unterstützt weitere Verschlüsselungsalgorithmen

- SEED und ARIA für South Korea…
  - SEED ist ein Block Cipher Algorithmus mit 128bit Blöcken und 128bit Keys entwickelt in den 1990's
  - ARIA ist ein Block Cipher Algorithmus ähnlich zu AES mit 128bit Blöcken und variablen Schlüsseln (128, 192 or 256) entwickelt in 2003
- GOST für Russland …
  - GOST ist ein Block Cipher Algorithmus ähnlich zu DES mit 64bit Blöcken / 256bit Keys entwickelt in den 1970's

Weiter Verbesserungen für TDE

TDE Unterstützt Entschlüsselung und Rekey

- Verschlüsselte Tablespaces können komplett entschlüsselt werden
  - Verschlüsselung in der Cloud und entschlüsselt On-Premises

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

- ReKey - neu Verschlüsslung jedes Blockes mit dem neuen Master Key
  - Deep rekey mit der **REKEY** Klause. Jeder Block wird neu verschlüsselt.

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

Netzwerk

Netzwerk

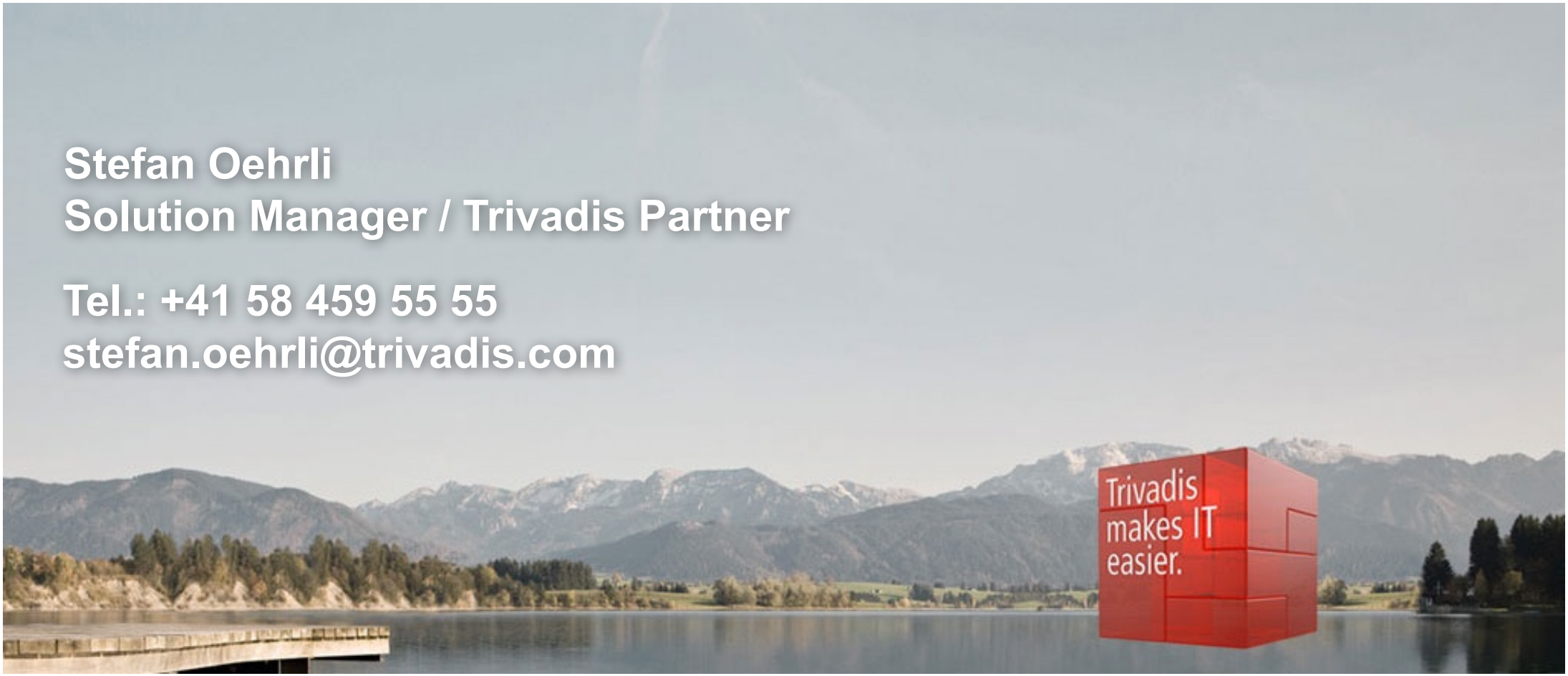
- Keine massgeblichen ”New Security Features” bei Oracle Netz
- Bestehende Probleme und Sicherheitslücken
  - SSL / TLS Poodle Vulnerability
  - LDAP Problem mit EUS und SSL v3 Bug 19285025
  - Memory Leak bei der Integritätsprüfung mit den neuen SHA Checksums
- Unterstützung von neuen Verschlüsselungsalgorithmen
  - Analog den Algorithmen bei TDE
  - SEED128 mit einer Schlüssellänge von 128-bit
  - ARIA128, ARIA192 und ARIA256 mit den entsprechenden Schlüssellängen
  - GOST256 mit einer Schlüssellänge von 256-bit

Zusammenfassung

- Nicht so viele neue Security Features wie für Oracle 12c Release 1
  - Aber ein paar sinnvolle Verbesserungen
  - Einige “must have” für Cloud Umgebungen
- Endlich eine Möglichkeit, bestehende Tablespaces zu verschlüsseln

Stefan Oehrli
Solution Manager / Trivadis Partner

Tel.: +41 58 459 55 55
stefan.oehrli@trivadis.com



trivadis
makes IT easier.