

■ ■ ■ Neue Security Features mit Oracle 11g



Sven Vetter
Technology Manager
Principal Consultant, Partner

DOAG Regio
München, 09.12.2009

trivadis
makes IT easier. ■ ■ ■

Basel · Baden · Bern · Lausanne · Zürich · Düsseldorf · Frankfurt/M. · Freiburg i. Br. · Hamburg · München · Stuttgart · Wien

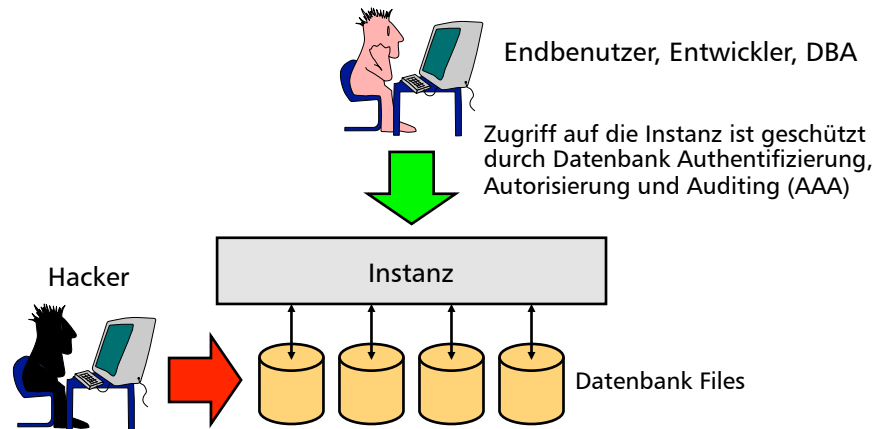
Agenda



Daten sind
immer im Spiel.

- Tablespace Encryption
- Local Auto-Open Wallet
- "Secure by Default"
- Besserer Passwortschutz
- Ausführen von Scripts per External Tables
- Diverses

Motivation



Tablespace Encryption (1)



- Transparent Data Encryption wurde mit Oracle Database 10.2 eingeführt, hatte dort aber einige Einschränkungen:
 - Es konnten nur einzelne Spalten verschlüsselt werden
 - Nicht alle Datentypen konnten verschlüsselt werden (Long, LOB)
 - Während Operationen waren die Daten nicht verschlüsselt, so dass eventuell unverschlüsselte und vertrauliche Daten im TEMP-Tablespace oder im REDO sichtbar waren
 - Ausschliesslich B*Tree Indizes werden unterstützt (keine FBI)
 - Index Range Scans werden nur bei Abfragen auf Gleichheit unterstützt
 - Fremdschlüssel können nicht auf verschlüsselten Spalten definiert werden
- Alle diese Einschränkungen wurden mit Oracle Database 11g aufgehoben



Tablespace Encryption (2)



- Es können nun Tablespaces komplett verschlüsselt werden
- Ist nur beim Anlegen des Tablespaces einschaltbar ☹
- Alle Daten im Tablespace (einschliesslich Lobs, Indexes, ...) sind verschlüsselt – ausser BFILES
- Daten bleiben verschlüsselt bei Dateioperationen wie Joins und Sorts, damit sind sie auch verschlüsselt in UNDO, REDO und TEMP
- Daten sind nicht verschlüsselt im Shared Memory!

Vorgehen



- Identisch wie bei Oracle Database 10g wird mit folgendem Befehl ein Master-Key in einem Wallet erstellt:

```
ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY {password}
```

- Existiert noch kein Wallet, wird ein neues erzeugt, wenn der Pfad \$ORACLE_BASE/admin/\$ORACLE_SID/wallet existiert
- Im Wallet muss Autologin eingeschaltet sein (gefährlich!) – oder es muss nach dem Mounten (oder Öffnen) der Datenbank geöffnet werden:

```
ALTER SYSTEM SET WALLET OPEN IDENTIFIED BY {password}
```

Tablespace erzeugen



- Nun können verschlüsselte Tablespaces erzeugt werden
- Beispiel:

```
CREATE TABLESPACE enc_test
DATAFILE SIZE 50M
ENCRYPTION USING 'AES256'
DEFAULT STORAGE (ENCRYPT)
```

- Als Verschlüsselungsalgorithmen können 3DES168, AES128, AES192 oder AES256 gewählt werden

Auswirkungen – Performance



- Daten müssen beim Schreiben verschlüsselt, beim Lesen entschlüsselt werden – dies benötigt Ressourcen...
- Folgender Performance-Impact wurde gemessen (Tabelle mit 150'000 Zeilen, Tablespace verschlüsselt mit AES256):

Operation	Impact
Massen-Insert (zeilenweise)	10%
Massen-Deletes/Updates	10%
Massen-Insert (IDL)	1%
Full-Table Scan	1%
Index-Scan	<1%

- CPU-Verbrauch ist höher
- Grösse der Datenfiles ändert sich bei Verschlüsselung nicht

Auswirkungen – Tools



- EXP exportiert keine Daten aus verschlüsselten Tablespaces:

```
exp enc_test/manager file=test.dmp tables=test_enc
...
EXP-00111: Table TEST_ENC resides in an Encrypted
Tablespace ENC_TEST and will not be exported
...
```

- EXPDP exportiert die Daten unverschlüsselt in das Dump-File (es sei denn, ENCRYPTION ist definiert)
- RMAN lässt den Tablespace verschlüsselt
Das bedeutet, bei einer Recovery muss das Wallet vorhanden sein!

Agenda



- Tablespace Encryption
- Local Auto-Open Wallet
- "Secure by Default"
- Besserer Passwortschutz
- Ausführen von Scripts per External Tables
- Diverses

Wallet Management



- Für diverse Oracle Features wird ein Wallet gebraucht:
 - Verschlüsselung von sensiblen Daten in Datenfiles
 - Verschlüsselung von Backups und Exports
 - SSL-Verbindung (Verschlüsselung, Integritätsprüfung und Autorisierung)
- Wallet entspricht dem PKCS#12-Standard
- Im Wallet können sowohl Zertifikate als auch (seit Oracle 10.2) Passwörter gespeichert werden
- Wallet kann z.B. durch mkstore angelegt werden

11.1.0.6

Wallet Management – Auto Login (bis 11.1.0.6)



- Durch mkstore ist per Default "Auto Login" eingeschaltet
- Hat aber einige Konsequenzen:
 - Es wird eine zweite Datei (cwallet.sso) erzeugt, durch welche bestimmte Operationen ohne Passwortabfrage möglich sind
 - Das normalerweise verschlüsselte Wallet kann von der Datenbank abgefragt werden
 - Änderungen benötigen noch das Passwort
 - Das Wallet kann einschliesslich sso-Datei auf einen anderen Rechner kopiert werden – und ist auch dort geöffnet – und kann für Entschlüsselungen gebraucht werden!



Local Auto-Open Wallet



- Seit Oracle 11.2 (und zurückportiert auf 11.1.0.7) kann nun mit einem **Local** Auto-Open Wallet gearbeitet werden
- Dies bleibt nur auf der gleichen Maschine geöffnet
- Wird es auf einen anderen Rechner kopiert, muss es einmalig wieder (local) geöffnet werden
- Wird mit orapki angelegt (oder geändert):


```
orapki wallet create -wallet <wallet_location> \
  -auto_login_local
```
- (nicht dokumentiert) funktioniert auch mkstore mit der Option **-createLSSO**

Agenda



- Tablespace Encryption
- Local Auto-Open Wallet
- "Secure by Default"
- Besserer Passwortschutz
- Ausführen von Scripts per External Tables
- Diverses

"Secure by Default"

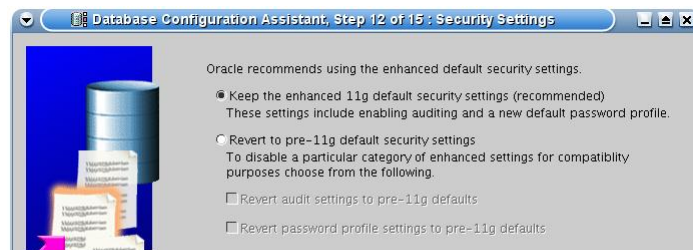


- Mit "Secure by Default" meint Oracle, dass die Datenbank durch diverse Massnahmen out-of-the-box sicherer ist, als eine vergleichbare 10g-Installation
- Dazu gehören:
 - Standardmässiges Auditing
 - Eingebauter Passwort-Komplexitäts-Checker
 - Eingebautes Benutzer-Profil
 - Fine-Grained Access Control bei Netzwerk Call-outs aus der Datenbank

Standardmässiges Auditing (1)



- Der DBCA fragt ab, ob die "Enhanced default security settings" eingeschaltet werden sollen:



- Oracle empfiehlt, diese Frage mit "ja" zu beantworten und bietet die Wahl mit 11gR2 nicht mehr an...
- Dies hat aber einige Auswirkungen:
 - Platzbedarf im SYSAUX-Tablespace (kein automatisches Löschen)
 - Eventueller Performance-Impact

Standardmässiges Auditing (2)



- Eingeschaltet ist dann (Auszug aus Oracle Dokumentation):

ALTER ANY PROCEDURE	CREATE ANY JOB	DROP ANY TABLE
ALTER ANY TABLE	CREATE ANY LIBRARY	DROP PROFILE
ALTER DATABASE	CREATE ANY PROCEDURE	DROP USER
ALTER PROFILE	CREATE ANY TABLE	EXEMPT ACCESS POLICY
AUDIT ROLE BY ACCESS	CREATE EXTERNAL JOB	GRANT ANY OBJECT PRIVILEGE
ALTER SYSTEM	CREATE PUBLIC DATABASE LINK	GRANT ANY PRIVILEGE
ALTER USER	CREATE SESSION	GRANT ANY ROLE
AUDIT SYSTEM	CREATE USER	
AUDIT SYSTEM BY ACCESS	DROP ANY PROCEDURE	

- Ausgeführt wird das Script `seconf.sql` automatisch aus `catproc.sql` (immer!!)
- Werden die "Enhanced default security settings" nicht eingeschaltet, werden nach dem Anlegen der DB diese wieder ausgeschaltet...



Verbesserte Passwort-Verifizierungs-Funktion



- Die durch das Script `utlpwdmg.sql` erzeugte Passwortfunktion wurde verbessert/erweitert:
 - Passwort mindestens 8 Stellen (alt: 4 Stellen)
 - Passwort ungleich `<username>1 - <username>100` (neu)
 - Passwort ungleich rückwärts geschriebener Username (neu)
 - Passwort ungleich DB-Name (neu)
 - Passwort ungleich `<DB-Name>1 - <DB-Name>100` (neu)
 - Mehr "einfache" Wörter werden getestet (`user1234`, `password1`, ...)
 - Passwort ungleich `oracle1 - oracle100` (neu)
- Das Script wird weiterhin nicht automatisch ausgeführt
- Sollte es aber ausgeführt werden, ändert es das Default-Profile, welches für alle Benutzer gilt!!

Standardmässige Passwortprüfung im Default-Profile



- Werden bei der Installation der Datenbank die "Enhanced default security settings" eingeschaltet, wird das Standardprofile wie folgt angepasst:

```
SQL> SELECT resource_name, limit
2 FROM dba_profiles
3 WHERE profile='DEFAULT';
```

RESOURCE_NAME	LIMIT
FAILED_LOGIN_ATTEMPTS	10
PASSWORD_LIFE_TIME	180
PASSWORD_REUSE_TIME	UNLIMITED
PASSWORD_REUSE_MAX	UNLIMITED
PASSWORD_VERIFY_FUNCTION	NULL
PASSWORD_LOCK_TIME	1
PASSWORD_GRACE_TIME	7



- DBAs und Batch-Benutzer müssen dann Passwörter ändern!!

Fine-Grained Access für Netzwerk-Callouts (1)



- Hat ein Benutzer EXECUTE-Rechte auf eines der folgenden Packages, kann er an beliebige Hosts Informationen schicken:
 - UTL_TCP
 - UTL_SMTP
 - UTL_MAIL
 - UTL_HTTP
 - UTL_INADDR
- Mit dem neuen Package DBMS_NETWORK_ACL_ADMIN können nun Access Control Listen erzeugt werden, mit denen definiert wird, welcher Benutzer an welchen Host Callouts durchführen kann

Fine-Grained Access für Netzwerk-Callouts (2)



- Dies geht aber leider nur, wenn XDB installiert ist...

```
exec dbms_output.put_line(utl_inaddr.get_host_name);
BEGIN dbms_output.put_line(utl_inaddr.get_host_name); END;
```

```
*
ERROR at line 1:
ORA-24248: XML DB extensible security not installed
ORA-06512: at "SYS.UTL_INADDR", line 4
ORA-06512: at "SYS.UTL_INADDR", line 35
ORA-06512: at line 1
```



- Ansonsten kann nur ein SYSDBA diese 5 Packages nutzen...

Fine-Grained Access für Netzwerk-Callouts (3)



- ACL definieren

```
BEGIN
DBMS_NETWORK_ACL_ADMIN.CREATE_ACL (
  acl          => 'scott_trivadis.xml',
  description  => 'Allow scott to connect to trivadis',
  principal   => 'SCOTT',
  is_grant    => TRUE,
  privilege    => 'connect'
);
END;
/

BEGIN
DBMS_NETWORK_ACL_ADMIN.ASSIGN_ACL (
  acl          => 'scott_trivadis.xml',
  host         => 'www.trivadis.com'
);
END;
/
```

Agenda



Daten sind
immer im Spiel.

- Übersicht
- Tablespace Encryption
- "Secure by Default"
- Besserer Passwortschutz
- Erweiterungen im Database Control

11.1.0.6

Besserer Passwortschutz – Übersicht



- Bis Oracle Database 10g war es einfach, Passwörter von einer Datenbank auf eine andere zu übertragen, um z.B. zu versuchen, diese dort zu hacken
- Der Zeichensatz der Passwörter war begrenzt, da die Passwörter nicht case-sensitiv waren
- Es gab diverse Passwort-Checker auf dem Markt, die über Wörterbücher oder per Brute-Force-Attack recht schnell Passwörter herausbekamen
- Die ersten beiden Punkte wurden mit Oracle Database 11g verbessert
- Inzwischen gibt es aber wieder genügend Hackertools, da der Passwort-Algorithmus im wesentlichen bekannt ist...

Case sensitive Passwörter



- Mit folgendem Initialisierungsparameter wird festgelegt, ob die Passwörter case sensitiv sind:

```
SEC_CASE_SENSITIVE_LOGON = TRUE | FALSE
```

- Achtung: Gut prüfen, ob der Default-Wert mit Ihrer Applikation wirklich funktioniert!
- Z.B. TOAD wandelt vor dem Anmelden alle Passwörter in Grossbuchstaben um...
- Bei der Migration bleiben zuerst alle Passwörter case insensitiv, bis das Passwort erstmalig in 11g geändert wird



Neuer Passwort Algorithmus



- Passwörter über das Netzwerk werden neu mit dem Industriestandard AES verschlüsselt
- In SYS.USER\$.SPARE4 wird das Passwort zusätzlich mit einem Salt zusammengesetzt und ein Hash mit SHA-1 gebildet
- Dadurch sind direkte Updates auf USER\$.PASSWORD nicht mehr möglich
- "ALTER USER <username> IDENTIFIED BY VALUES ..." geht aber weiterhin... (Passwort ist nicht case-sensitive)
- In USER\$.PASSWORD wird immer noch das Passwort identisch wie in 10g (in Grossschreibung) abgespeichert, so dass Hackertools das Passwort identisch ermitteln können – und dann nur noch auf Gross-Kleinschreibung testen müssen...

Check auf Standardpasswörter



- Über eine neue View kann einfach kontrolliert werden, ob die Standardpasswörter der von Oracle angelegten Benutzer geändert wurden:

```
SELECT * FROM dba_users_with_defpwd;
```

```
USERNAME
```

```
-----
```

```
DIP
```

```
HR
```

```
OUTLN
```

```
EXFSYS
```

```
SCOTT
```

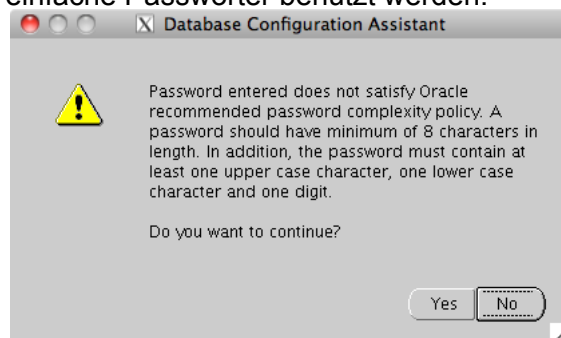
```
SYSTEM
```

```
...
```

Passwort-Check im DBCA



- Im Database Configuration Assistant wird nun überprüft, ob zu einfache Passwörter benutzt werden:



- Leider kann man dann über diesen Hinweis einfach hinweggehen...

Agenda



Daten sind
immer im Spiel.

- Tablespace Encryption
- Local Auto-Open Wallet
- "Secure by Default"
- Besserer Passwortschutz
- Ausführen von Scripts per External Tables
- Diverses

11.2.0.0

External Tables und Scripts



- External Tables wurden erweitert, so dass vor dem Bearbeiten der ASCII-Datei ein Script gestartet werden kann
- Folgende Einsatzzwecke sind u.a. vorstellbar:
 - Entpacken der Datei
 - Abholen der Datei per SCP/FTP
 - Verzeichnisinhalt ausgeben
 - ...
- Das Script muss die Daten per Standardoutput ausgeben
- → http://www.oracle.com/global/de/community/dbadmin/tips/external_tables/index.html
- → http://sven.svenvetter.com/sven/2009/12/04/external_table1/

External Tables und Scripts – Beispiel (1)



- Einfaches Script (ls1.sh):

```
/bin/ls -ls /tmp/
```

- Externe Tabelle:

```
CREATE TABLE test_ls (line varchar2(80))
ORGANIZATION EXTERNAL
(
  TYPE oracle_loader
  DEFAULT DIRECTORY data_dir
  ACCESS PARAMETERS
  (
    RECORDS DELIMITED BY NEWLINE
    PREPROCESSOR script_dir:'ls1.sh'
  )
  LOCATION ('prodDelta.gz')
)
REJECT LIMIT UNLIMITED NOPARALLEL;
```

External Tables und Scripts – Beispiel (2)



- Output:

```
SQL> SELECT * FROM test_ls;
```

```
LINE
```

```
-----
```

```
total 16
4 drwxr-xr-x 2 oracle dba 4096 2009-12-04 16:29 hspcrfdata_ora
4 drwxr-xr-x 2 sntrsrv sntrsrv 4096 2009-12-04 16:10 hspcrfdata_sn
4 drwxrwxrwt 2 root root 4096 2009-12-04 16:10 VMwareDnD
4 drwx----- 2 root root 4096 2009-12-04 16:10 vmware-root
```

- Natürlich könnte man Name, Grösse, Datum, ... noch in einzelne Felder legen

External Tables, Scripts, Oracle 11.1 und DBV



- Diese Möglichkeit wurde auch in Oracle 11.1 (ab 11.1.0.7) implementiert
- Einzige Anpassung: Im Script muss zwingend der Shebang (`#!/bin/bash`) eingetragen sein
- Das Feature ist nicht verfügbar mit Oracle Database Vault Fehlermeldung:

```
ORA-29913: error in executing ODCIEXTTABLEOPEN callout
ORA-29400: data cartridge error
KUP-04094: preprocessing cannot be performed if Database Vault
is installed
```

External Tables, Scripts und Sicherheitsbedenken



- Um diese Scripte ausführen zu können, benötigt der Benutzer das (neue) Execute-Privileg auf das Directory-Object
- Da ein DBA dies natürlich hat – und ein DBA ausserdem das "CREATE ANY DIRECTORY"-Privileg hat, kann er sich aus PL/SQL heraus selbst Scripte schreiben (`utl_file`) – und diese dann ausführen
- Damit hat er vollen Zugriff auf das Betriebssystem (als Oracle-Software-Owner)
- Deswegen: Die Erstellung und das Ändern von Directory-Objekten muss dringend überwacht werden (Auditing, Audit Vault)



Agenda



Daten sind
immer im Spiel.

- Tablespace Encryption
- Local Auto-Open Wallet
- "Secure by Default"
- Besserer Passwortschutz
- Ausführen von Scripts per External Tables
- Diverses

11.1.0.7

Audit Data Management



- Neues Package DBMS_AUDIT_MGMT zur Administration der Audit Tabellen
 - SYS.AUD\$
 - SYS.FGA_LOG\$
- Verschieben der Audit-Tabellen aus dem System Tablespace

```
BEGIN
  DBMS_AUDIT_MGMT.SET_AUDIT_TRAIL_LOCATION(
    AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_AUD_STD,
    AUDIT_TRAIL_LOCATION_VALUE => 'TBS_AUDIT');
END;
```

- Nutzung als SYS oder mit EXECUTE Privileg

Security – Audit Data Management



- DBMS_AUDIT_PACKAGE ermöglicht auch das automatische Löschen der Inhalte von
 - Audit Trail Tabellen
 - OS-Files und XML Audit Files
- Purgen aller Audit Trail Typen über den "Last Archive Timestamp"
 - Timestamp kann selbst gesetzt werden oder wird von Audit Vault gesetzt
 - DB, OS und XML
- Scheduler Job Konfiguration für periodisches Löschen von Audit Trail Sätzen (Periode frei konfigurierbar)

Erweiterungen im Database Control



- "Enterprise Security Manager" und "Oracle Policy Manager" im Database Control integriert (bis 10g nur als Java-Tools)


Virtual Private Database Policies


Virtual Private Database Policies enable to build applications that enforce row-level security policies at the object (table, view or synonym) level by attaching security policies to objects and dynamically appending predicates (WHERE clauses) to SQL statements that query them.

Policy Advanced

Security Policies can be applied to Tables, Views or Synonyms (Synonyms to tables and views only) to provide row level security also known as Fine Grained Access Control (FGAC).

Search
Specify an object name to list the policies associated with it. Optionally provide a policy name to filter the data that is displayed in the result.

Schema Name 

Object Name 

Policy Name

1-10 of 14

Select Policy	Object Name	Schema	Object Type	Policy Group	Enabled	
<input checked="" type="radio"/>	TVD\$TUN_EMP_POLICY	EMP	TVD\$TUN	TABLE	SYS_DEFAULT	<input checked="" type="checkbox"/>
<input type="radio"/>	TVD\$TUN_EMP_POLICY	EMP	TVDEXPERT	TABLE	SYS_DEFAULT	<input checked="" type="checkbox"/>

Erweiterungen im Database Control – LogMiner



■ Beispiel des Ergebnisses

Summary
 Matching Transactions **1** Query Filter **where seg_owner = 'SCOTT' and table_name = 'EMP'**
 Matching Redo Records **14** Total Time **10 seconds**

The results show transactions containing redo records that matched the query filter. Transactions may contain other redo records. Click on a Transaction ID to view all of the redo records in a transaction. The results can be filtered further by searching the sql redo.

Transaction Results

Search SQL Redo: View By: ▾

Transaction ID	DB User	Commit Timestamp	Redo Transaction Summary - Updates (upd), Inserts (ins), Records Deletes (del), Other (oth)
04000B00C3020000	SCOTT	Nov 18, 2007 8:36:37 PM	14 SCOTT.EMP (14 upd)

Transaction Details

Transaction ID **04000B00C3020000** Start SCN **696729** Start Time **Nov 18, 2007 8:36:35 PM**
 DB User **UNKNOWN** Commit SCN **696733** Commit Time **Nov 18, 2007 8:36:37 PM**
 OS User Machine Name

SCN	Operation	Schema	Table	SQL Redo
696733	START			set transaction read write;
696733	UPDATE	SCOTT	EMP	update "SCOTT"."EMP" set "SAL" = 801 where "SAL" = 800 and ROWID = 'AAA05xAAMAAAAeAAA';
696733	UPDATE	SCOTT	EMP	update "SCOTT"."EMP" set "SAL" = 1601 where "SAL" = 1600 and ROWID = 'AAA05xAAMAAAAeAAB';

Security – Kernaussagen



- Es wird einfacher, eine sicherere Datenbank zu installieren
- Tablespace Encryption wird für vertrauliche Daten eine wichtige Option werden
- Oracle unternimmt viel, um sicherzustellen, dass wirklich nur die richtige Person die richtigen Daten lesen kann
- Mit externen Tabellen können bessere Jobabläufe programmiert werden
- Leider wird immer noch viel Altlast mitgeschleppt (Passwortalgorithmus, ...)

ORACLE 11G RELEASE 2

Unsere Datenbank-Tools:
Kosteneffizient, flexibel, sicher und 11g R2 ready!

Erhalten Sie einen komprimierten Überblick in unserem eintägigen TechnoCircle Oracle Database 11g Release 2: Wir konzentrieren uns dabei auf die Kern Features – besprechen diese aber umso detaillierter!

Gern beraten wir Sie persönlich!

Mehr erfahren:

- Beratungsanfrage
- Oracle 11g R2 TechnoCircle
- Oracle Warehouse Builder 11g Release 2

ORACLE[®] 11g
DATABASE

mehr zu 11g?

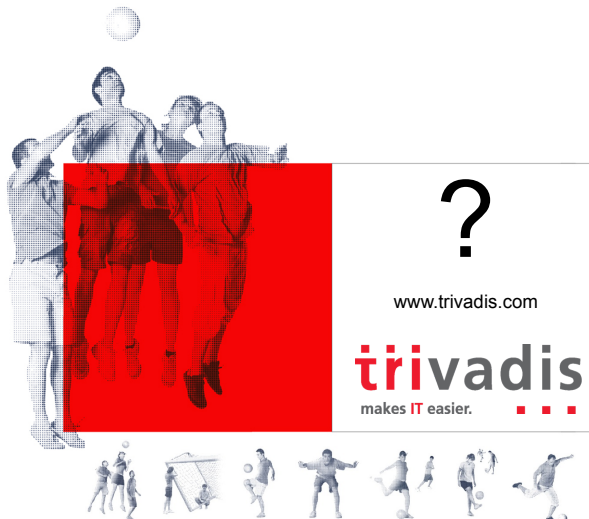
**TechnoCircle
München,
20.01.2010**

Oracle Database 11g – New Security Features

41

© 2009 **trivadis**
makes IT easier.

■ ■ ■ Vielen Dank!



Basel · Baden · Bern · Lausanne · Zürich · Düsseldorf · Frankfurt/M. · Freiburg i. Br. · Hamburg · München · Stuttgart · Wien