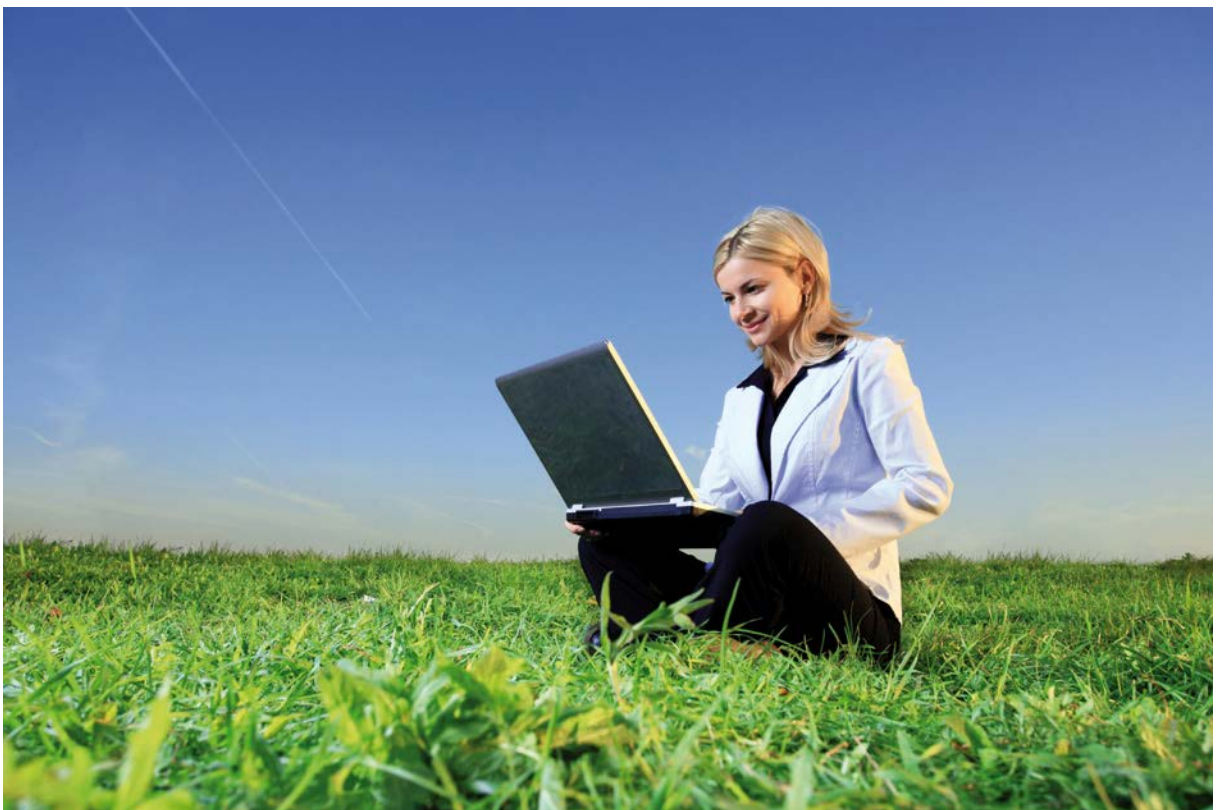


# **Oracle Security**

## **Seminarunterlage**

**Version: 11.06**



Dieses Dokument wird durch die ORDIX AG veröffentlicht.

Copyright ORDIX AG. Alle Rechte vorbehalten.

Alle Produkt- und Dienstleistungs-Bezeichnungen sind Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen und beziehen sich auf Eintragungen in den USA oder USA-Warenzeichen.

Weitere Logos und Produkt- oder Handelsnamen sind eingetragene Warenzeichen oder Warenzeichen der jeweiligen Unternehmen.

Kein Teil dieser Dokumentation darf ohne vorherige schriftliche Genehmigung der ORDIX AG weitergegeben oder benutzt werden.

## Adressen der ORDIX AG

Die ORDIX AG besitzt folgende Geschäftsstellen

ORDIX AG  
Westernmauer 12-16  
D-33098 Paderborn  
Tel.: (+49) 0 52 51 / 10 63 - 0  
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG  
An der alten Ziegelei 5  
D-48157 Münster  
Tel.: (+49) 02 51 / 9 24 35 – 00  
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG  
Marlene-Dietrich-Str. 5  
D-89231 Neu-Ulm  
Tel.: (+49) 07 31 / 9 85 88 – 550  
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG  
Kreuzberger Ring 13  
D-65205 Wiesbaden  
Tel.: (+49) 06 11 / 7 78 40 – 00  
Fax.: (+49) 01 80 / 1 67 34 90

ORDIX AG  
Wikingerstraße 18-20  
D-51107 Köln  
Tel.: (+49) 02 21 / 8 70 61 – 0  
Fax.: (+49) 01 80 / 1 67 34 90

Sie können die ORDIX AG von der ganzen Welt aus durch folgende Internet Adresse kontaktieren:  
<http://www.ordix.de>

Sie können uns weiterhin über die Email-Adressen [training@ordix.de](mailto:training@ordix.de) oder [info@ordix.de](mailto:info@ordix.de) kontaktieren

## Inhaltsverzeichnis

<b>1</b>	<b>Sicherheit für Benutzer und Passwörter .....</b>	<b>8</b>
1.1	Benutzerverwaltung .....	9
1.1.1	Der CREATE USER Befehl .....	11
1.1.2	Der ALTER USER Befehl .....	13
1.1.3	Account Locking / Expiration.....	15
1.1.4	Der DROP USER Befehl.....	17
1.1.5	Limitierung von Ressourcen über Profile .....	18
1.1.5.1	Der CREATE PROFILE Befehl .....	20
1.1.5.2	Aktivierung von Profilen zur Limitierung von Ressourcen .....	22
1.2	Passwortschutz und -verwaltung .....	23
1.2.1	Historie .....	23
1.2.2	Passwortverwaltung über Profile .....	24
1.2.2.1	Änderungen am Standard Benutzerprofil.....	26
1.2.3	Passwort-Verifizierungsfunktion utlpwdmg.sql .....	27
1.2.3.1	Verbesserte Passwort-Verifizierungsfunktion .....	28
1.2.4	Case-Sensitive Passwörter.....	29
1.2.4.1	Passwort Versionen .....	30
1.2.4.2	Datenbank-Links und Case-Sensitivität .....	31
1.2.5	Passwort Hashing .....	33
1.2.6	Prüfung auf Standardkennwörter .....	36
1.3	Automatisch generierte Benutzer .....	39
1.3.1	Gruppen von Standardbenutzern.....	41
1.3.1.1	Administrative Benutzer .....	42
1.3.1.2	Benutzer für ORACLE-Optionen .....	44
1.3.1.3	Applikatorische Benutzer .....	46
1.3.2	Was ist zu tun?.....	48
1.4	Zusammenfassung .....	49
1.5	Übungen .....	51
1.6	Lösungen .....	53
<b>2</b>	<b>Authentifizierung.....</b>	<b>56</b>
2.1	Einleitung .....	57
2.2	Anmeldeprozess (O3/O5 LOGON) von Oracle .....	59
2.2.1	Ablauf des O5LOGON Anmeldeprozesses .....	60
2.3	Delayed Failed Logins .....	62
2.4	Security Settings in Oracle 11g .....	63
2.5	Externe Benutzer .....	65
2.5.1	Authentifizierung durch das Betriebssystem.....	65
2.6	Passwortdateien für Datenbankadministratoren.....	67
2.6.1	Verwaltung der Passwortdatei .....	69
2.6.2	Case-sensitive Passwortdatei in 11g.....	71
2.6.3	SYSASM Privileg in 11g .....	72
2.7	Secure External Password Store.....	75
2.7.1	Hinweise und Befehle zur Verwaltung .....	78
2.8	SYSDBA Strong Authentication in 11g.....	80
2.9	Proxy-Authentifizierung.....	81
2.10	Übungen .....	83
2.11	Lösungen .....	85
<b>3</b>	<b>Autorisierung.....</b>	<b>88</b>
3.1	Konzept.....	89
3.2	Privilegien .....	91
3.2.1	Der GRANT Befehl für Systemprivilegien .....	91
3.2.2	Der GRANT Befehl für Objektprivilegien .....	92
3.2.3	Der REVOKE Befehl .....	93
3.2.4	Systemprivilegien.....	95

3.3	Rollenkonzept .....	96
3.3.1	Der CREATE ROLE Befehl.....	97
3.3.2	Der DROP ROLE Befehl.....	98
3.3.3	Default Roles.....	99
3.3.4	Der SET ROLE Befehl .....	100
3.3.5	Secure Application Roles.....	101
3.3.6	Vordefinierte Rollen .....	104
3.4	Access Control Listen (ACLs) – Kontrolle der Netzwerkzugriffe aus der Datenbank.....	105
3.4.1	Access Control Listen (ACLs) in Oracle 11g – Implementierung .....	106
3.4.2	Access Control Listen (ACLs) in Oracle 11g – Anwendung .....	108
3.5	Database Vault .....	110
3.5.1	Einschränkung von Privilegien.....	110
3.5.2	Aufgabenverteilung und Funktionstrennung.....	113
3.6	Übungen .....	115
3.7	Lösungen .....	118
<b>4</b>	<b>FGAC VPD.....</b>	<b>120</b>
4.1	Einleitung in FGAC .....	121
4.1.1	Ausgangslage .....	121
4.1.2	Standardsicherheit bei ORACLE: Auf Objektebene .....	122
4.1.3	Beispiel.....	123
4.1.3.1	Ausgangslage.....	123
4.1.3.2	Lösung1: Views.....	125
4.1.3.3	Lösung2: Dynamische Views.....	126
4.1.3.4	Lösung 3: Dynamische Views mit Zugriffstabelle .....	127
4.1.3.5	Problem beim Arbeiten mit Views .....	128
4.2	Vorteile von Fine Grained Access Control.....	130
4.2.1	Begriffsklärung: FGA – FGAC?.....	132
4.3	Arbeiten mit FGAC.....	133
4.3.1	FGAC: Arbeiten mit Dynamischen Prädikaten.....	134
4.3.2	DBMS_RLS – So arbeitet FGAC .....	135
4.3.2.1	add_policy .....	135
4.3.2.2	Funktion.....	136
4.3.2.3	Environment Variable.....	137
4.3.2.4	Transiente View .....	138
4.3.3	Beispiel: Einfache Policy erzeugen.....	139
4.3.4	Ideen der Zugriffssteuerung.....	141
4.3.5	Nötige Zugriffsrechte.....	142
4.3.6	DBMS_RLS – administrative Schnittstelle für Policies .....	143
4.3.7	Kontext.....	144
4.3.7.1	Typen eines Kontextes.....	144
4.3.7.2	Erstellen eines Kontextes.....	145
4.4	Neuerungen unter ORACLE 10g .....	150
4.5	Oracle Label Security.....	152
4.6	Übungen .....	153
4.7	Lösungen .....	155
<b>5</b>	<b>Auditing FGA.....</b>	<b>161</b>
5.1	Überblick.....	162
5.2	Mandatory Auditing.....	163
5.2.1	Mandatory Auditing UNIX .....	164
5.2.2	Mandatory Auditing Microsoft .....	165
5.3	SYS Auditing.....	166
5.4	Standard Auditing .....	167
5.4.1	Aktivierung .....	167
5.4.2	Möglichkeiten .....	169
5.4.3	Beispiele Statement Auditing.....	170
5.4.4	Beispiele Einschränkungen.....	171
5.4.5	„Enhanced Default Security Settings“ in Oracle 11g .....	173

5.4.6	Auditing auf Session- und Statement-Ebene (ab 11g R2).....	175
5.5	Views.....	176
5.6	Auditing über OS/syslog .....	177
5.7	Applikatorisches (Value-based) Auditing .....	179
5.8	Fine-Grained Auditing (FGA) .....	181
5.8.1	Erstellen einer FGA Policy .....	182
5.8.2	Auswirkung der FGA Policy .....	183
5.8.3	FGA Data Dictionary Views .....	184
5.8.4	Audit auf Spalten und mit inhaltlichen Beziehungen.....	185
5.8.4.1	Das Audit fokussieren: Audit Columns.....	185
5.8.4.2	Das Audit weiter fokussieren: Audit Conditions .....	186
5.8.5	FGA Policies verwalten .....	187
5.8.6	„Reichweite“ der FGA Policy.....	188
5.8.7	FGA Policy und Views .....	190
5.8.7.1	FGA Policy wirkt auch bei Abfragen über Views.....	190
5.8.7.2	Eine FGA Policy speziell für eine View erstellen .....	191
5.8.8	Zusammenspiel von FGA Policies .....	192
5.8.9	Weitere mögliche Anwendungen .....	193
5.9	Audit-Daten verwalten: Package DBMS_AUDIT_MGMT .....	195
5.10	Oracle Audit Vault.....	199
5.10.1	Überblick und Funktionsumfang .....	199
5.10.2	Anforderungen .....	201
5.10.3	Architektur und Komponenten .....	202
5.10.4	Installation und Konfiguration.....	206
5.10.5	Definition des Auditing .....	209
5.10.6	Audit Vault Services .....	214
5.10.6.1	Alerts .....	214
5.10.6.2	Reports.....	216
5.10.7	Schutz der Audit-Daten .....	220
5.11	Übungen .....	222
5.12	Lösungen .....	229
<b>6</b>	<b>Datenspeicherung und -sicherung: Verschlüsselung .....</b>	<b>236</b>
6.1	Datenverschlüsselung in der DB .....	237
6.2	DBMS_OBFUSCATION_TOOLKIT .....	238
6.2.1	Grundlagen .....	238
6.2.2	Beispiel.....	240
6.2.3	Zeichenkettenlänge.....	242
6.3	DBMS_CRYPTO.....	244
6.3.1	Grundlagen .....	244
6.3.2	Einsatz der Verschlüsselung.....	249
6.3.3	Einschränkungen bei der Datenverschlüsselung.....	252
6.3.4	Schlüsselmanagement.....	253
6.4	Transparente Datenverschlüsselung (TDE) .....	254
6.4.1	Aufsetzen eines Wallet .....	256
6.4.2	Verschlüsselung von Tabellenspalten .....	258
6.4.2.1	Verschlüsselung von indizierten und FK-Spalten .....	260
6.4.2.2	Salt-Prinzip .....	262
6.4.3	Verschlüsselung von Tablespaces .....	263
6.4.4	Auswirkungen der Verschlüsselung auf die Performance und Speicher.....	267
6.4.5	Wallet Management .....	269
6.4.5.1	Oracle Wallet Manager (OWM).....	271
6.4.5.2	Auto-Login Wallet .....	272
6.4.5.3	Local Auto-Login Wallet (ab 11g R2) .....	274
6.4.6	TDE und Hardware Security Module (HSM).....	275
6.4.6.1	HSM-basierte TDE implementieren .....	277
6.4.7	Securefile LOBs .....	279
6.5	Verschlüsselung von Export-Daten mit Data Pump .....	281
6.5.1	Data Pump und Transparente Datenverschlüsselung (10gR2).....	281

6.5.2	Data Pump Encryption in Oracle 11g .....	283
6.6	Verschlüsselte Backups mit RMAN .....	287
6.6.1	Arten der Backupverschlüsselung .....	289
6.6.1.1	Transparenter Modus .....	290
6.6.1.2	Passwort-Modus .....	290
6.6.1.3	Dualer Modus .....	290
6.6.2	Konfiguration von verschlüsselten Backups .....	291
6.6.3	Backup und Recovery mit verschlüsselten Backups .....	292
6.7	Übungen .....	294
6.8	Lösungen .....	296
<b>7</b>	<b>Oracle Net .....</b>	<b>299</b>
7.1	Listener .....	300
7.1.1	Angriffspunkte .....	300
7.1.2	Listener Password .....	302
7.2	Standard-Ports .....	304
7.3	Connection Manager .....	305
7.3.1	Überblick .....	305
7.3.2	Multiplexing .....	306
7.3.3	Protocol Switch .....	307
7.3.4	Zugangskontrolle .....	308
7.3.5	Architektur .....	309
7.3.6	Regelwerk .....	311
7.3.6.1	Grundlagen .....	311
7.3.6.2	Beispiele .....	312
7.3.7	Absicherung .....	314
7.4	Advanced Security Option .....	315
7.4.1	Überblick .....	315
7.4.2	Leistungsmerkmale .....	316
7.4.3	Vor- und Nachteile .....	318
7.4.4	Integrität .....	321
7.4.4.1	Überblick .....	321
7.4.4.2	Aktivierung .....	322
7.4.4.3	Parameter CRYPTO_SEED .....	323
7.4.4.4	Parameter CRYPTO_CHECKSUM .....	324
7.4.4.5	Beispielkonfiguration .....	326
7.4.5	Verschlüsselung .....	327
7.4.5.1	Diffie Hellmann Algorithmus .....	327
7.4.5.2	Parameter .....	329
7.4.5.3	Algorithmen .....	330
7.4.6	SSL-basierte Authentifizierung .....	331
7.4.6.1	Grundlagen .....	331
7.4.6.2	Vor- und Nachteile .....	333
7.4.6.3	SSL und Oracle .....	334
7.4.6.4	Aufbau einer SSL-Verbindung in der Oracle Umgebung .....	336
7.4.6.5	Konfiguration .....	337
7.4.6.6	Wallet erstellen .....	338
7.4.6.7	Digitales Zertifikat .....	340
7.4.6.8	Zertifikate einfügen .....	342
7.4.6.9	SSL Listener Konfiguration .....	344
7.4.6.10	Konfiguration des Clients .....	345
7.4.6.11	Fazit .....	346
7.5	Oracle Net Logging und Tracing .....	347
7.5.1	Oracle Net Logging de-/aktivieren .....	349
7.5.2	Oracle Net Tracing de-/aktivieren .....	351
7.5.3	Oracle Net Logging und Tracing im ADR (11g) .....	353
<b>8</b>	<b>Sicherheitslücken .....</b>	<b>355</b>
8.1	Database Links .....	356

8.1.1	Grundlagen .....	356
8.1.2	Konzept .....	358
8.1.3	Infos .....	360
8.2	init.ora Parameter .....	361
8.2.1	O7_DICTIONARY_ACCESSIBILITY .....	361
8.2.2	REMOTE_OS_AUTHENT .....	361
8.2.3	SQL92_SECURITY .....	361
8.2.4	UTL_FILE_DIR .....	362
8.2.4.1	Oracle Directories .....	363
8.2.4.2	„EXECUTE“ Privileg auf Verzeichnisobjekte .....	364
8.2.5	Export-Files .....	366
8.2.6	glogin.sql .....	367
8.2.7	Verify Function .....	368
8.3	SQL Injection .....	369
8.3.1	Definition SQL Injection .....	369
8.3.1.1	Wertübergabe .....	372
8.3.1.2	Strategien zur Vermeidung .....	373
8.3.1.3	Bind Variablen .....	375
8.3.1.4	Übergabewerte prüfen .....	376
8.3.1.5	Fine Grained Access Control (FGAC) nutzen .....	376
8.3.1.6	Einsatz des Packages DBMS_ASSERT .....	377
8.4	Trigger .....	379
8.4.1	Trigger Allgemein .....	379
8.4.2	Fehlermanagement .....	380
8.4.3	Security .....	381
8.5	LogMiner .....	382
8.5.1	Einleitung .....	382
8.5.2	Zugriff auf das Data Dictionary .....	384
8.5.3	Security .....	385
8.6	Critical Patch Updates .....	386
8.7	Übungen .....	388
8.8	Lösungen .....	389
<b>9</b>	<b>Data Masking .....</b>	<b>391</b>
9.1	Data Masking im EM .....	392
9.1.1	Definition des Data Masking .....	392
9.1.2	Kennzeichen des Data Masking .....	393
9.1.3	Features des Data Masking .....	394
9.1.4	Ablauf des Data Masking .....	395
9.1.5	Beispiel des Data Masking .....	397
9.2	Data Masking Erstellung .....	398
9.2.1	Beispiel des EM – Aufruf .....	398
9.2.2	Beispiel der EM – Definitionserstellung .....	399
9.2.3	Beispiel der EM – Skriptgenerierung .....	400
9.2.4	Beispiel des EM – Datenbankklon .....	401
9.3	Data Masking und Datapump .....	402
9.4	Übungen .....	405
9.5	Lösungen .....	406