

# ***Oracle Security***

## ***Seminarunterlage***

***Version: 12.17***



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  
Karl-Schurz-Straße 19a  
D-33100 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  
Welser Straße 9  
D-86368 Gersthofen  
Tel.: (+49) 08 21 / 507 492 – 0  
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

ORDIX AG  
Gewerbegebiet Süd-West Park  
Südwestpark 67/2  
D-890449 Nürnberg  
Tel.: (+49) 0 52 51 / 10 63 - 0  
Fax.: (+49) 01 80 / 1 67 34 90

Internet: <http://www.ordix.de>

Email: [seminare@ordix.de](mailto:seminare@ordix.de)

# Inhaltsverzeichnis

<b>1</b>	<b>Gesetzliche Grundlagen .....</b>	<b>10</b>
1.1	Überblick .....	11
1.2	Standards .....	12
1.3	IT Grundschutz (BSI) .....	13
1.3.1	Bundesamt für die Sicherheit in der Informationstechnologie .....	13
1.3.2	Dokumente .....	14
1.3.3	Datenbank Sicherheitskonzept .....	15
1.4	Datenschutzgesetz .....	16
1.4.1	Definitionen .....	16
1.4.2	Personenbezogene Daten .....	17
1.4.3	Besondere personenbezogene Daten .....	18
1.4.4	Umgang mit personenbezogenen Daten .....	19
1.4.5	Speicherung von personenbezogenen Daten .....	20
1.4.6	Recht auf informelle Selbstbestimmung .....	21
1.4.7	Auskunftsrecht .....	22
1.4.8	Weitere Rechte .....	23
1.4.9	Zugriffskontrolle .....	24
1.5	Kritische Infrastrukturen (KRITIS) .....	25
1.5.1	IT Sicherheitsgesetz .....	25
1.5.2	Sektoren .....	26
1.5.3	Brancheneinteilung .....	27
1.6	Definition Datensicherheit .....	29
<b>2</b>	<b>Sicherheit für Benutzer und Passwörter .....</b>	<b>30</b>
2.1	Benutzerverwaltung .....	31
2.1.1	Der CREATE USER Befehl .....	33
2.1.2	Datenbankbenutzer in der CDB und PDB .....	35
2.1.3	Verwaltung von globalen und lokalen Benutzern .....	36
2.1.4	Schema Only Accounts ab 18c .....	37
2.1.5	Der ALTER USER Befehl .....	38
2.1.6	Account Locking / Expiration .....	40
2.1.7	Der DROP USER Befehl .....	42
2.1.8	Last Login Information ab 12c .....	43
2.1.9	Limitierung von Ressourcen über Profile .....	44
2.1.9.1	Der CREATE PROFILE Befehl .....	46
2.1.9.2	Aktivierung von Profilen zur Limitierung von Ressourcen .....	47
2.1.9.3	Inactive Account Time .....	48
2.2	Passwortschutz und -verwaltung .....	49
2.2.1	Historie .....	49
2.2.2	Passwortverwaltung über Profile .....	50
2.2.2.1	Änderungen am Standard Benutzerprofil .....	52
2.2.3	Passwort-Verifizierungsfunktion utlpwdmg.sql .....	53
2.2.3.1	Verbesserte Passwort-Verifizierungsfunktion .....	55
2.2.3.2	Neuerungen in 12c .....	56
2.2.3.3	Passwort Versionen .....	57
2.2.3.4	Passwort Sicherheit (Hashes) .....	58
2.2.4	Password Hashing .....	60
2.2.5	Prüfung auf Standardkennwörter .....	64
2.3	Automatisch generierte Benutzer .....	67
2.3.1	Gruppen von Standardbenutzern .....	69
2.3.1.1	Administrative Benutzer .....	70
2.3.1.2	Benutzer für ORACLE-Optionen .....	72
2.3.1.3	Applikatorische Benutzer .....	74
2.3.2	Was ist zu tun? .....	76
2.4	Zusammenfassung .....	77
<b>3</b>	<b>Authentifizierung .....</b>	<b>79</b>
3.1	Einleitung .....	80

3.2	Anmeldeprozess (O3/O5 LOGON) von Oracle .....	82
3.2.1	Ablauf des O5LOGON Anmeldeprozesses .....	83
3.3	Security Settings in Oracle 11g .....	85
3.4	Externe Benutzer .....	87
3.4.1	Authentifizierung durch das Betriebssystem .....	87
3.4.2	Betriebssystemauthentifizierung in der Tenant Technologie .....	89
3.5	Passwortdateien für Datenbankadministratoren .....	92
3.5.1	Verwaltung der Passwortdatei .....	94
3.5.2	Separation of Duty for Database Administration in 12c .....	96
3.5.3	SYSASM Privileg in 11g .....	97
3.6	Secure External Password Store .....	100
3.6.1	Hinweise und Befehle zur Verwaltung .....	103
3.7	SYSDBA Strong Authentication in 11g .....	105
3.8	Anwendungsbenutzer eindeutig identifizieren .....	106
3.8.1	Client Identifier .....	107
3.8.2	Proxy-Authentifizierung .....	108
<b>4</b>	<b>Autorisierung .....</b>	<b>110</b>
4.1	Konzept .....	111
4.2	Privilegien .....	113
4.2.1	Der GRANT Befehl für Systemprivilegien .....	113
4.2.2	Der GRANT Befehl für Objektprivilegien .....	114
4.2.3	Der REVOKE Befehl .....	115
4.2.4	System-Privilegien .....	117
4.2.4.1	Eingeschränkte Leseberechtigungen aus das DD .....	118
4.3	Rollenkonzept .....	119
4.3.1	Der CREATE ROLE Befehl .....	120
4.3.2	Globale und Lokale Rollen .....	121
4.3.3	Der DROP ROLE Befehl .....	122
4.3.4	Default Roles .....	123
4.3.5	Der SET ROLE Befehl .....	124
4.3.6	Secure Application Roles .....	125
4.3.7	Vordefinierte Rollen .....	128
4.3.7.1	Resource Role Default Privileges in 12c .....	129
4.3.8	Code-Based Security .....	130
4.4	Access Control Listen (ACLs) – Kontrolle der Netzwerkzugriffe aus der Datenbank .....	131
4.4.1	Access Control Listen (ACLs) in Oracle 11g – Implementierung .....	132
4.4.2	Access Control Listen (ACLs) in Oracle 11g – Anwendung .....	133
4.5	Database Vault .....	134
4.5.1	Einschränkung von Privilegien .....	134
4.5.2	Aufgabenverteilung und Funktionstrennung .....	136
4.6	Privilege Capturing .....	138
<b>5</b>	<b>FGAC VPD .....</b>	<b>139</b>
5.1	Einleitung in FGAC .....	140
5.1.1	Ausgangslage .....	140
5.1.2	Beispiel .....	141
5.1.2.1	Ausgangslage .....	141
5.1.3	Standardsicherheit bei ORACLE: Auf Objektebene .....	142
5.1.3.1	Lösung 1: Views .....	143
5.1.3.2	Lösung 2: Dynamische Views .....	144
5.1.3.3	Lösung 3: Dynamische Views mit Zugriffstabelle .....	145
5.1.3.4	Problem beim Arbeiten mit Views .....	146
5.2	Vorteile von Fine Grained Access Control .....	148
5.2.1	Begriffsklärung: FGA – FGAC? .....	150
5.3	Arbeiten mit FGAC .....	151
5.3.1	FGAC: Arbeiten mit Dynamischen Prädikaten .....	152
5.3.2	DBMS_RLS – So arbeitet FGAC .....	153
5.3.2.1	add_policy .....	153
5.3.2.2	Funktion .....	154

5.3.2.3	Environment Variable .....	155
5.3.2.4	Transiente View .....	156
5.3.3	Beispiel: Einfache Policy erzeugen .....	157
5.3.4	Ideen der Zugriffssteuerung .....	159
5.3.5	Nötige Zugriffsrechte .....	160
5.3.6	DBMS_RLS – administrative Schnittstelle für Policies .....	161
5.3.7	Kontext .....	162
5.3.7.1	Typen eines Kontextes .....	162
5.3.7.2	Erstellen eines Kontextes .....	163
5.4	Spaltenbasierte Sicherheit .....	167
5.5	VPD Neuerungen in 12c .....	169
5.6	Oracle Label Security .....	170
<b>6</b>	<b>Data Redaction und Transparent Sensitive Data Protection (TSDP) .....</b>	<b>171</b>
6.1	Data Redaction .....	172
6.1.1	Begriffsklärung .....	172
6.1.2	Methoden .....	173
6.1.3	EXEMPT Redaction Policy .....	174
6.1.4	Prozeduren .....	175
6.1.5	Einschränkungen .....	176
6.1.6	add_policy .....	177
6.1.7	Update_full_redaction_values .....	179
6.1.8	Alter_policy .....	180
6.1.9	Random Redaction .....	182
6.1.10	Regexp Redaction .....	183
6.1.11	Data Redaction Views .....	184
6.1.12	Schnittstellen / Abgrenzung .....	185
6.2	Data Sensitive Transparent Protection (TSDP) .....	187
6.2.1	Vorgehensweise .....	187
6.2.2	Erstellen Sensitive Type / Definition der sensitiven Spalten .....	188
6.2.3	Policy erstellen .....	189
6.2.4	Verknüpfung und Aktivierung .....	190
6.2.5	TSDP Aktivierung .....	191
<b>7</b>	<b>Auditing, FGA .....</b>	<b>192</b>
7.1	ORACLE Auditing Modi - Historie .....	193
7.2	Auditing bevor 12c .....	194
7.3	Auditing in 12c – Mixed Mode .....	195
7.4	Auditing in 12c – Pure Mode .....	196
7.5	Überblick .....	197
7.6	Mandatory Auditing .....	198
7.6.1	Mandatory Auditing UNIX .....	199
7.6.2	Mandatory Auditing Microsoft .....	200
7.7	SYS Auditing .....	201
7.8	Standard Auditing .....	202
7.8.1	Aktivierung .....	202
7.8.2	Möglichkeiten .....	204
7.8.3	Beispiele Statement Auditing .....	205
7.8.4	Beispiele Einschränkungen .....	206
7.8.5	„Enhanced Default Security Settings“ in Oracle 11g .....	208
7.8.6	Auditing auf Session- und Statement-Ebene (ab 11g R2) .....	210
7.8.7	Views .....	211
7.9	Fine-Grained Auditing (FGA) .....	212
7.9.1	Erstellen einer FGA Policy .....	213
7.9.2	Auswirkung der FGA Policy .....	214
7.9.3	FGA Data Dictionary Views .....	215
7.9.4	Audit auf Spalten und mit inhaltlichen Beziehungen .....	216
7.9.4.1	Das Audit fokussieren: Audit Columns .....	216
7.9.4.2	Das Audit weiter fokussieren: Audit Conditions .....	217
7.9.5	FGA Policies verwalten .....	218

7.9.6	FGA Policy und Views.....	219
7.9.6.1	FGA Policy wirkt auch bei Abfragen über Views.....	219
7.9.6.2	Eine FGA Policy speziell für eine View erstellen.....	220
7.9.7	Zusammenspiel von FGA Policies .....	221
7.9.8	Weitere mögliche Anwendungen .....	222
7.10	Auditing über OS/syslog.....	224
7.11	Applikatorisches (Value-based) Auditing .....	226
7.12	Audit-Daten verwalten: Package DBMS_AUDIT_MGMT .....	228
7.13	Unified Auditing .....	232
7.13.1	Überblick .....	232
7.13.2	Unified Auditing - Mixed Mode .....	233
7.13.3	Aktivierung.....	234
7.13.4	Funktionsumfang.....	235
7.13.5	Ablageort und Zugriff.....	236
7.13.6	Separation of Duty für Audit Administratoren.....	237
7.13.7	Schreib-Modus .....	238
7.13.8	Beispiele.....	239
7.13.9	Auditing Data Pump .....	240
7.13.10	Auditing über OS/syslog (Unified Auditing) .....	241
7.13.11	Löschen von Audit Einträgen .....	243
7.13.12	Export der Auditdaten.....	244
7.13.13	VPD Policies (12.2) .....	245
7.14	Besonderheiten des Auditings in der Tenant Architektur.....	246
7.15	Oracle Audit Vault .....	247
7.15.1	Überblick und Funktionsumfang.....	247
7.15.2	Anforderungen.....	249
7.15.3	Architektur und Komponenten.....	250
<b>8</b>	<b>Datenbankverschlüsselung.....</b>	<b>254</b>
8.1	Datenverschlüsselung in der Datenbank .....	255
8.2	Symmetrische Verschlüsselung .....	256
8.3	Programmatische Verschlüsselung .....	257
8.3.1	DBMS_OBFUSCATION_TOOLKIT .....	257
8.4	DBMS_CRYPTO.....	258
8.4.1	Funktionen und Prozeduren .....	258
8.4.2	Verschlüsselungsalgorithmen .....	260
8.4.3	Hash-Funktionen .....	261
8.5	Vergleich DBMS_CRYPTO und DBMS_OBFUSCATION_TOOLKIT .....	263
8.5.1	Padding .....	264
8.5.2	Cypher Block Chaining.....	266
8.5.3	Schlüsselmanagement.....	267
8.6	Transparente Datenverschlüsselung (TDE).....	268
8.6.1	Das Oracle Wallet .....	268
8.6.1.1	Graphik .....	268
8.6.1.2	Überblick.....	269
8.6.1.3	Grundlegende Verwaltung.....	270
8.6.2	Transparente Spaltenverschlüsselung.....	272
8.6.2.1	Überblick.....	272
8.6.2.2	Transparente Verschlüsselung – je Spalte .....	274
8.6.2.3	Salt-Prinzip .....	276
8.6.3	Verschlüsselung von Tablespace.....	278
8.6.3.1	Transparente Datenverschlüsselung.....	278
8.6.3.2	Online Verschlüsselung von Tablespace .....	279
8.6.3.3	Offline Verschlüsselung von Tablespace .....	281
8.6.3.4	Vorteile und Einschränkungen .....	282
8.6.4	Wallet Management .....	283
8.6.4.1	Auto-Login Wallet .....	285
8.6.5	TDE und Hardware Security Module (HSM) .....	287
8.6.6	Keystore Management.....	289
8.6.6.1	Zusammenführung (Merging) von Software Keystores.....	290

8.6.6.2	Backup und Restore des Keystores .....	291
8.6.6.3	Zugriff mehrerer Datenbanken auf ein Wallet .....	292
8.6.6.4	Verschieben von Keystores.....	293
8.6.6.5	Migration einer verschlüsselten Datenbank auf einen neuen Server....	294
8.6.6.6	Passwortwechsel des Keystores.....	295
8.6.7	Management des Master Encryption Keys .....	296
8.6.7.1	Anlegen eines Master Encryption Keys.....	297
8.6.7.2	Aktivierung eines Schlüssels.....	298
8.6.7.3	Export des Master Encryption Keys .....	299
8.6.7.4	Import des Master Encryption Keys .....	300
8.7	Data Pump Encryption .....	301
8.7.1	Überblick .....	301
8.7.2	Parameter.....	302
8.8	Verschlüsselte Backups mit RMAN .....	304
8.8.1	Arten der Backupverschlüsselung.....	305
8.8.1.1	Passwort-Modus.....	306
8.8.1.2	Transparenter Modus .....	307
8.8.1.3	Dualer Modus .....	308
<b>9</b>	<b>Oracle Net.....</b>	<b>309</b>
9.1	Listener.....	310
9.1.1	Angriffspunkte .....	310
9.2	Standard-Ports .....	311
9.3	Connection Manager.....	312
9.3.1	Überblick .....	312
9.3.2	Multiplexing .....	313
9.3.3	Protocol Switch.....	314
9.3.4	Zugangskontrolle.....	315
9.3.5	Architektur .....	316
9.3.6	Regelwerk .....	318
9.3.6.1	Grundlagen.....	318
9.3.6.2	Beispiele.....	319
9.3.7	Absicherung .....	321
9.4	Advanced Security Option.....	322
9.4.1	Überblick .....	322
9.4.2	Netzwerkverschlüsselung Vor /Nachteile.....	323
9.4.3	Verschlüsselungsmethoden .....	324
9.4.4	Leistungsmerkmale .....	325
9.4.5	Client/Server Versionen und Verschlüsselung.....	329
9.4.6	Vor- und Nachteile.....	330
9.4.7	Integrität .....	332
9.4.7.1	Überblick.....	332
9.4.7.2	Aktivierung.....	333
9.4.7.3	Parameter CRYPTO_SEED.....	334
9.4.7.4	Parameter CRYPTO_CHECKSUM.....	335
9.4.7.5	Beispielkonfiguration .....	337
9.4.8	Verschlüsselung.....	338
9.4.8.1	Diffie Hellmann Algorithmus .....	338
9.4.8.2	Parameter.....	340
9.4.8.3	Algorithmen .....	341
9.4.9	SSL-basierte Authentifizierung.....	342
9.4.9.1	Grundlagen.....	342
9.4.9.2	Vor- und Nachteile.....	344
9.4.9.3	SSL und Oracle .....	345
9.4.9.4	Aufbau einer SSL-Verbindung in der Oracle Umgebung .....	346
9.4.9.5	Konfiguration .....	347
9.4.9.6	Wallet erstellen .....	349
9.4.9.7	Digitales Zertifikat .....	351
9.4.9.8	Zertifikate einfügen.....	353
9.4.9.9	SSL Listener Konfiguration.....	355



9.4.9.10	Konfiguration des Clients .....	357
9.4.9.11	Fazit.....	358
9.5	Oracle Net Logging und Tracing.....	359
9.5.1	Oracle Net Logging de-/aktivieren.....	361
9.5.2	Oracle Net Tracing de-/aktivieren .....	363
9.5.3	Oracle Net Logging und Tracing im ADR (11g) .....	365
<b>10</b>	<b>Sonstiges .....</b>	<b>367</b>
10.1	Database Links .....	368
10.1.1	Grundlagen.....	368
10.1.2	Konzept .....	370
10.1.3	Infos.....	372
10.1.4	Sicherheit ab 12.2 .....	373
10.2	init.ora Parameter.....	374
10.2.1	O7_DICTIONARY_ACCESSIBILITY .....	374
10.2.2	REMOTE_OS_AUTHENT .....	375
10.2.3	SQL92_SECURITY .....	376
10.2.4	UTL_FILE_DIR.....	377
10.2.4.1	Oracle Directories.....	378
10.2.4.2	„EXECUTE“ Privileg auf Verzeichnisobjekte.....	379
10.2.5	Export-Files .....	381
10.2.6	glogin.sql .....	382
10.2.7	Verify Function .....	383
10.3	Allgemeines.....	384
10.4	Beispiel.....	385
10.5	Strategien zur Vermeidung .....	386
10.6	Einsatz des Packages DBMS_ASSERT .....	389
10.7	Trigger.....	391
10.7.1	Trigger Allgemein .....	391
10.7.2	Fehlermanagement .....	392
10.7.3	Security .....	393
10.8	LogMiner .....	394
10.8.1	Einleitung.....	394
10.8.2	Zugriff auf das Data Dictionary.....	396
10.8.3	Security .....	397
10.9	Critical Patch Updates.....	398
10.10	Release Update (RU) vs. Release Update Revision (RUR) .....	400
<b>11</b>	<b>Data Masking .....</b>	<b>401</b>
11.1	Was ist Data Masking? .....	402
11.2	Warum Data Masking?.....	404
11.3	Anforderungen .....	405
11.4	Vorgehen.....	407
11.5	Verfügbarkeit mit Data Pump .....	409
11.6	Verfügbarkeit mit Oracle EM.....	414
11.7	Database Masking and Subsetting .....	424
<b>12</b>	<b>Direkte Anbindung Oracle an Active Directory .....</b>	<b>425</b>
12.1	Oracle 12c – Gesamtbild.....	426
12.2	Zentrale Benutzerverwaltung (Oracle 12c) .....	428
12.3	Zentrale Benutzerverwaltung ab Oracle 18c.....	430
12.4	Übersichtsbild.....	431
12.5	Konfigurationsmöglichkeiten .....	432
12.6	Authentifizierungsmethoden.....	433
12.7	Rechtevergabe .....	434
12.8	Bewertung .....	435
<b>13</b>	<b>Projektansatz .....</b>	<b>436</b>
13.1	Zusammenfassung der Security Anforderungen .....	437
13.2	Dokumente .....	438



13.3	Datenbank Security Handbuch .....	439
13.3.1	Verantwortlichkeiten .....	440
13.3.2	Inventar .....	441
13.3.3	Patch Management .....	442
13.3.4	Benutzer .....	443
13.3.5	Passworte .....	444
13.3.6	Authentifizierung.....	445
13.3.7	Auditing .....	446
13.3.8	Anonymisierung.....	447
13.3.9	Verschlüsselung.....	448
13.3.10	Change Management.....	449
13.3.11	Backup & Recovery.....	450
13.3.12	Sonstiges.....	451
13.4	Security Dokument je Datenbank / Applikation.....	452
<b>14</b>	<b>Übungen.....</b>	<b>453</b>
14.1	Sicherheit für Benutzer und Passwörter .....	454
14.2	Delayed Failed Login, OPS\$User, PW-File .....	455
14.3	Secure External Password Store .....	456
14.4	Auf Benutzerebene: Privilegien.....	457
14.5	Auf Benutzerebene: Rollen .....	458
14.6	Access Control Listen (ACLs) .....	459
14.7	FGAC .....	460
14.8	Data Redaction .....	461
14.9	SYS und Mandatory Auditing .....	462
14.10	Standard Auditing (DDL) .....	463
14.11	Standard Auditing (DML).....	464
14.12	Value-Based Auditing.....	465
14.13	FGA Auditing.....	466
14.14	FGA Auditing auf Spalten.....	467
14.15	Unified Auditing .....	468
14.16	Verschlüsselung DBMS_OBFUSCATION_TOOLKIT .....	469
14.17	TDE Tablespace, Data Pump und RMAN Encryption .....	470
14.18	GLOGIN.sql und Verify_Function .....	471
14.19	Data Masking .....	472