



Oracle Security

Seminarunterlage

Version: 13.03

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
Südwestpark 67/2
D-90449 Nürnberg
Tel.: (+49) 0 52 51 / 10 63 - 0
Fax.: (+49) 01 80 / 1 67 34 90

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

Email: seminare@ordix.de

Inhaltsverzeichnis

1	Gesetzliche Grundlagen	10
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
2	Sicherheit für Benutzer und Passwörter	30
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	45
2.1.9.2	Aktivierung von Profilen zur Limitierung von Ressourcen.....	46
2.1.9.3	Inactive Account Time	47
2.2	Passwortschutz und -verwaltung	48
2.2.1	Historie	48
2.2.2	Passwortverwaltung über Profile	49
2.2.2.1	Default Werte bei Profile Parameter ab 21c.....	51
2.2.2.2	Änderungen am Standard Benutzerprofil	52
2.2.2.3	Minimum Password Length	53
2.2.2.4	Password Rollover Time.....	54
2.2.3	Passwort-Verifizierungsfunktion utlpwdmg.sql.....	55
2.2.3.1	Verbesserte Passwort-Verifizierungsfunktion.....	57
2.2.3.2	Neuerungen in 12c	58
2.2.3.3	Passwort Versionen.....	59
2.2.3.4	Password Sicherheit (Hashes)	60
2.2.4	Password Hashing	62
2.2.5	Prüfung auf Standardkennwörter	65
2.3	Automatisch generierte Benutzer.....	68
2.3.1	Was ist zu tun?.....	70
2.4	Zusammenfassung.....	71
3	Authentifizierung	73
3.1	Einleitung.....	74
3.2	Anmeldeprozess (O3/O5 LOGON) von Oracle	76

3.2.1	Ablauf des O5LOGON Anmeldeprozesses.....	77
3.3	Security Settings in Oracle 11g.....	79
3.4	Externe Benutzer	81
3.4.1	Authentifizierung durch das Betriebssystem.....	81
3.5	Passwortdateien für Datenbankadministratoren	83
3.5.1	Verwaltung der Passwortdatei	85
3.5.2	Separation of Duty for Database Administration in 12c	87
3.6	Secure External Password Store	89
3.6.1	Hinweise und Befehle zur Verwaltung	92
3.7	SYSDBA Strong Authentication in 11g	94
3.8	Anwendungsbenutzer eindeutig identifizieren	96
3.8.1	Client Identifier	97
3.8.2	Proxy-Authentifizierung	98
4	Autorisierung	100
4.1	Konzept	101
4.2	Privilegien	103
4.2.1	Der GRANT Befehl für Systemprivilegien	103
4.2.2	Der GRANT Befehl für Objektprivilegien	104
4.2.3	Der REVOKE Befehl	105
4.2.4	System-Privilegien.....	107
4.2.4.1	Eingeschränkte Leseberechtigungen aus das DD	108
4.3	Rollenkonzept.....	109
4.3.1	Der CREATE ROLE Befehl	110
4.3.2	Globale und Lokale Rollen	111
4.3.3	Der DROP ROLE Befehl	112
4.3.4	Default Roles	113
4.3.5	Der SET ROLE Befehl.....	114
4.3.6	Secure Application Roles	115
4.3.7	Vordefinierte Rollen	118
4.3.8	Code-Based Security	119
4.4	Access Control Listen (ACLs) – Kontrolle der Netzwerkzugriffe aus der Datenbank	120
4.4.1	Access Control Listen (ACLs) in Oracle 11g – Implementierung	121
4.4.2	Access Control Listen (ACLs) in Oracle 11g – Anwendung.....	122
4.5	Database Vault.....	123
4.5.1	Einschränkung von Privilegien	123
4.5.2	Aufgabenverteilung und Funktionstrennung	125
4.6	Privilege Capturing	127
5	FGAC VPD	128
5.1	Einleitung in FGAC.....	129
5.1.1	Ausgangslage.....	129
5.1.2	Beispiel.....	130
5.1.2.1	Ausgangslage	130
5.1.3	Standardsicherheit bei ORACLE: Auf Objektebene.....	131
5.1.3.1	Lösung 1: Views	132
5.1.3.2	Lösung 2: Dynamische Views	133
5.1.3.3	Lösung 3: Dynamische Views mit Zugriffstabelle.....	134
5.1.3.4	Problem beim Arbeiten mit Views	135
5.2	Vorteile von Fine Grained Access Control	137
5.2.1	Begriffsklärung: FGA – FGAC?	139
5.3	Arbeiten mit FGAC	140
5.3.1	FGAC: Arbeiten mit Dynamischen Prädikaten	141
5.3.2	DBMS_RLS – So arbeitet FGAC	142
5.3.2.1	add_policy	142
5.3.2.2	Funktion.....	143
5.3.2.3	Environment Variable	144
5.3.2.4	Transiente View	145
5.3.3	Beispiel: Einfache Policy erzeugen	146
5.3.4	Ideen der Zugriffssteuerung	148

5.3.5	Nötige Zugriffsrechte	149
5.3.6	DBMS_RLS – administrative Schnittstelle für Policies	150
5.3.7	Kontext	151
5.3.7.1	Typen eines Kontextes	151
5.3.7.2	Erstellen eines Kontextes	152
5.4	Spaltenbasierte Sicherheit	156
5.5	VPD Neuerungen in 12c	158
5.6	Oracle Label Security	159
6	Data Redaction und Transparent Sensitive Data Protection (TSDP)	160
6.1	Data Redaction.....	161
6.1.1	Begriffsklärung	161
6.1.2	Methoden	162
6.1.3	EXEMPT Redaction Policy	163
6.1.4	Prozeduren	164
6.1.5	Einschränkungen.....	165
6.1.6	add_policy	166
6.1.7	Update_full_redaction_values	168
6.1.8	Alter_policy	169
6.1.9	Random Redaction.....	171
6.1.10	Regexp Redaction	172
6.1.11	Data Redaction Views	173
6.1.12	Schnittstellen / Abgrenzung	174
6.2	Data Sensitive Transparent Protection (TSDP)	176
6.2.1	Vorgehensweise	176
6.2.2	Erstellen Sensitive Type / Definition der sensitiven Spalten	177
6.2.3	Policy erstellen	178
6.2.4	Verknüpfung und Aktivierung	179
6.2.5	TSDP Aktivierung	180
7	Auditing, FGA	181
7.1	ORACLE Auditing Modi - Historie	182
7.2	Auditing bevor 12c	183
7.3	Auditing in 12c – Mixed Mode	184
7.4	Auditing in 12c – Pure Mode	185
7.5	Überblick	186
7.6	Mandatory Auditing	187
7.6.1	Mandatory Auditing UNIX.....	188
7.6.2	Mandatory Auditing Microsoft.....	189
7.7	SYS Auditing	190
7.8	Standard Auditing.....	191
7.8.1	Aktivierung.....	191
7.8.2	Möglichkeiten	193
7.8.3	Beispiele Statement Auditing	194
7.8.4	Beispiele Einschränkungen	195
7.8.5	„Enhanced Default Security Settings“ in Oracle 11g.....	197
7.8.6	Auditing auf Session- und Statement-Ebene (ab 11g R2)	199
7.8.7	Views.....	200
7.9	Fine-Grained Auditing (FGA)	201
7.9.1	Erstellen einer FGA Policy	202
7.9.2	Auswirkung der FGA Policy.....	203
7.9.3	FGA Data Dictionary Views.....	204
7.9.4	Audit auf Spalten und mit inhaltlichen Beziehungen	205
7.9.4.1	Das Audit fokussieren: Audit Columns	205
7.9.4.2	Das Audit weiter fokussieren: Audit Conditions	206
7.9.5	FGA Policies verwalten	207
7.9.6	FGA Policy und Views.....	208
7.9.6.1	FGA Policy wirkt auch bei Abfragen über Views	208
7.9.6.2	Eine FGA Policy speziell für eine View erstellen.....	209
7.9.7	Zusammenspiel von FGA Policies	210

7.9.8	Weitere mögliche Anwendungen	211
7.10	Auditing über OS/syslog.....	213
7.11	Applikatorisches (Value-based) Auditing	215
7.12	Audit-Daten verwalten: Package DBMS_AUDIT_MGMT	217
7.13	Unified Auditing	221
7.13.1	Überblick.....	221
7.13.2	Unified Auditing - Mixed Mode	222
7.13.3	Aktivierung.....	223
7.13.4	Funktionsumfang	224
7.13.5	Ablageort und Zugriff.....	225
7.13.6	Separation of Duty für Audit Administratoren.....	226
7.13.7	Beispiele	227
7.13.8	Change Effective Immediately	228
7.13.9	Auditing Data Pump	229
7.13.10	Auditing über OS/syslog (Unified Auditing)	230
7.13.11	Löschen von Audit Einträgen	232
7.13.12	Export der Auditdaten.....	233
7.13.13	VPD Policies (12.2)	234
7.14	Besonderheiten des Auditings in der Tenant Architektur.....	235
7.15	Oracle Audit Vault	236
7.15.1	Überblick und Funktionsumfang.....	236
7.15.2	Anforderungen.....	237
7.15.3	Architektur und Komponenten.....	238
8	Datenbankverschlüsselung.....	242
8.1	Datenverschlüsselung in der Datenbank	243
8.2	Symmetrische Verschlüsselung.....	244
8.3	Programmatische Verschlüsselung.....	245
8.3.1	DBMS_OBFUSCATION_TOOLKIT	245
8.4	DBMS_CRYPTO	246
8.4.1	Funktionen und Prozeduren	246
8.4.2	Verschlüsselungsalgorithmen	248
8.4.3	Hash-Funktionen	249
8.5	Vergleich DBMS_CRYPTO und DBMS_OBFUSCATION_TOOLKIT.....	251
8.5.1	Padding	252
8.5.2	Cypher Block Chaining.....	254
8.5.3	Schlüsselmanagement.....	255
8.6	Transparente Datenverschlüsselung (TDE).....	256
8.6.1	Das Oracle Wallet	256
8.6.1.1	Graphik	256
8.6.1.2	Überblick.....	257
8.6.1.3	Grundlegende Verwaltung.....	258
8.6.2	Transparente Spaltenverschlüsselung	260
8.6.2.1	Überblick.....	260
8.6.2.2	Transparente Verschlüsselung – je Spalte.....	262
8.6.2.3	Salt-Prinzip	264
8.6.3	Verschlüsselung von Tablespaces.....	266
8.6.3.1	Transparente Datenverschlüsselung.....	266
8.6.3.2	Online Verschlüsselung von Tablespaces	267
8.6.3.3	Offline Verschlüsselung von Tablespaces	268
8.6.3.4	Vorteile und Einschränkungen	269
8.6.4	Wallet Management	270
8.6.4.1	Auto-Login Wallet	272
8.6.5	TDE und Hardware Security Module (HSM)	274
8.6.6	Keystore Management	276
8.6.6.1	Zusammenführung (Merging) von Software Keystores.....	277
8.6.6.2	Backup und Restore des Keystores	278
8.6.6.3	Zugriff mehrerer Datenbanken auf ein Wallet	279
8.6.6.4	Verschieben von Keystores.....	280
8.6.6.5	Migration einer verschlüsselten Datenbank auf einen neuen Server....	281

8.6.6.6	Passwortwechsel des Keystores	282
8.6.7	Management des Master Encryption Keys	283
8.6.7.1	Anlegen eines Master Encryption Keys	284
8.6.7.2	Aktivierung eines Schlüssels	285
8.6.7.3	Export des Master Encryption Keys	286
8.6.7.4	Import des Master Encryption Keys	287
8.7	Data Pump Encryption	288
8.7.1	Überblick	288
8.7.2	Parameter	289
8.8	Verschlüsselte Backups mit RMAN	290
8.8.1	Arten der Backupverschlüsselung	291
8.8.1.1	Passwort-Modus	292
8.8.1.2	Transparenter Modus	293
8.8.1.3	Dualer Modus	294
9	Oracle Net	295
9.1	Listener	296
9.1.1	Angriffspunkte	296
9.2	Standard-Ports	297
9.3	Connection Manager	298
9.3.1	Überblick	298
9.3.2	Multiplexing	299
9.3.3	Protocol Switch	300
9.3.4	Zugangskontrolle	301
9.3.5	Architektur	302
9.3.6	Regelwerk	304
9.3.6.1	Grundlagen	304
9.3.6.2	Beispiele	305
9.3.7	Absicherung	307
9.4	Advanced Security Option	308
9.4.1	Überblick	308
9.4.2	Netzwerkverschlüsselung Vor /Nachteile	309
9.4.3	Verschlüsselungsmethoden	310
9.4.4	Leistungsmerkmale	311
9.4.5	Client/Server Versionen und Verschlüsselung	315
9.4.6	Vor- und Nachteile	316
9.4.7	Integrität	318
9.4.7.1	Überblick	318
9.4.7.2	Aktivierung	319
9.4.7.3	Parameter CRYPTO_CHECKSUM	320
9.4.7.4	Beispielkonfiguration	322
9.4.8	Verschlüsselung	323
9.4.8.1	Diffie Hellmann Algorithmus	323
9.4.8.2	Parameter	325
9.4.8.3	Algorithmen	326
9.4.9	SSL-basierte Authentifizierung	327
9.4.9.1	Grundlagen	327
9.4.9.2	Vor- und Nachteile	329
9.4.9.3	SSL und Oracle	330
9.4.9.4	Aufbau einer SSL-Verbindung in der Oracle Umgebung	331
9.4.9.5	Konfiguration	332
9.4.9.6	Wallet erstellen	334
9.4.9.7	Digitales Zertifikat	336
9.4.9.8	Zertifikate einfügen	338
9.4.9.9	SSL Listener Konfiguration	340
9.4.9.10	Konfiguration des Clients	342
9.4.9.11	Fazit	343
9.5	Interpretation von SID als Service Name	344
9.6	Oracle Net Logging und Tracing	345
9.6.1	Oracle Net Logging de-/aktivieren	347

9.6.2	Oracle Net Tracing de-/aktivieren	349
9.6.3	Oracle Net Logging und Tracing im ADR (11g)	351
10	Sonstiges	353
10.1	Database Links.....	354
10.1.1	Grundlagen.....	355
10.1.2	Konzept	357
10.1.3	Infos.....	359
10.1.4	Sicherheit ab 12.2	360
10.2	init.ora Parameter.....	361
10.2.1	O7_DICTIONARY_ACCESSIBILITY	361
10.2.2	REMOTE_OS_AUTHENT	362
10.2.3	SQL92_SECURITY	363
10.2.4	UTL_FILE_DIR.....	364
10.2.4.1	Oracle Directories.....	365
10.2.4.2	„EXECUTE“ Privileg auf Verzeichnisobjekte	366
10.2.5	Export-Files	368
10.2.6	glogin.sql	369
10.2.7	Verify Function	370
10.3	Allgemeines.....	371
10.4	Beispiel.....	372
10.5	Strategien zur Vermeidung	373
10.6	Einsatz des Packages DBMS_ASSERT	375
10.7	Trigger	377
10.7.1	Trigger Allgemein	377
10.7.2	Fehlermanagement	378
10.7.3	Security.....	379
10.8	LogMiner	379
10.8.1	Einleitung.....	380
10.8.2	Zugriff auf das Data Dictionary.....	382
10.8.3	Security.....	383
10.9	Critical Patch Updates.....	384
10.10	Release Update (RU) vs. Release Update Revision (RUR)	386
10.11	DBSAT	387
10.11.1	Sicherheitsempfehlungen.....	388
10.12	Architektur	389
10.12.1	Architektur Collector/Reporter	390
10.12.2	Architektur Discoverer	391
10.13	Installation	392
10.14	Aufruf Collector.....	393
10.15	Aufruf Reporter.....	395
10.15.1	Beispiel Report	397
10.16	Aufruf Discoverer	398
11	Data Masking	402
11.1	Was ist Data Masking?	403
11.2	Warum Data Masking?.....	405
11.3	Anforderungen.....	406
11.4	Vorgehen.....	408
11.5	Verfügbarkeit mit Data Pump	410
11.6	Verfügbarkeit mit Oracle EM	415
11.7	Database Masking and Subsetting	425
12	Direkte Anbindung Oracle an Active Directory	426
12.1	Oracle 12c – Gesamtbild.....	427
12.2	Zentrale Benutzerverwaltung (Oracle 12c)	429
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
13	Projektansatz	436
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
14	Übungen	453
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