



Oracle Security

Seminarunterlagen

Version: 13.02

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	Gruppen von Standardbenutzern	70
2.3.1.1	Administrative Benutzer.....	71
2.3.1.2	Benutzer für ORACLE-Optionen	73
2.3.1.3	Applikatorische Benutzer.....	75
2.3.2	Was ist zu tun?	77
2.4	Zusammenfassung.....	78

3	Authentifizierung	80
3.1	Einleitung.....	81
3.2	Anmeldeprozess (O3/O5 LOGON) von Oracle.....	83
3.2.1	Ablauf des O5LOGON Anmeldeprozesses.....	84
3.3	Security Settings in Oracle 11g.....	86
3.4	Externe Benutzer	88
3.4.1	Authentifizierung durch das Betriebssystem.....	88
3.4.2	Betriebssystemauthentifizierung in der Tenant Technologie	89
3.5	Passwortdateien für Datenbankadministratoren	91
3.5.1	Verwaltung der Passwortdatei	93
3.5.2	Separation of Duty for Database Administration in 12c	95
3.5.3	SYSASM Privileg in 11g.....	96
3.6	Secure External Password Store	98
3.6.1	Hinweise und Befehle zur Verwaltung	101
3.7	SYSDBA Strong Authentication in 11g	103
3.8	Anwendungsbutzer eindeutig identifizieren	105
3.8.1	Client Identifier	106
3.8.2	Proxy-Authentifizierung	107
4	Autorisierung	109
4.1	Konzept	110
4.2	Privilegien.....	112
4.2.1	Der GRANT Befehl für Systemprivilegien	112
4.2.2	Der GRANT Befehl für Objektprivilegien.....	113
4.2.3	Der REVOKE Befehl	114
4.2.4	System-Privilegien.....	116
4.2.4.1	Eingeschränkte Leseberechtigungen aus das DD	117
4.3	Rollenkonzept.....	118
4.3.1	Der CREATE ROLE Befehl.....	119
4.3.2	Globale und Lokale Rollen	120
4.3.3	Der DROP ROLE Befehl	121
4.3.4	Default Roles	122
4.3.5	Der SET ROLE Befehl.....	123
4.3.6	Secure Application Roles	124
4.3.7	Vordefinierte Rollen.....	127
4.3.7.1	Resource Role Default Privileges in 12c.....	128
4.3.8	Code-Based Security	129
4.4	Access Control Listen (ACLs) – Kontrolle der Netzwerkzugriffe aus der Datenbank	130
4.4.1	Access Control Listen (ACLs) in Oracle 11g – Implementierung.....	131
4.4.2	Access Control Listen (ACLs) in Oracle 11g – Anwendung.....	132
4.5	Database Vault.....	133
4.5.1	Einschränkung von Privilegien	133
4.5.2	Aufgabenverteilung und Funktionstrennung	135
4.6	Privilege Capturing	137
5	FGAC VPD	138
5.1	Einleitung in FGAC.....	139
5.1.1	Ausgangslage.....	139
5.1.2	Beispiel.....	140
5.1.2.1	Ausgangslage.....	140
5.1.3	Standardsicherheit bei ORACLE: Auf Objektebene.....	141
5.1.3.1	Lösung 1: Views	142
5.1.3.2	Lösung 2: Dynamische Views	143
5.1.3.3	Lösung 3: Dynamische Views mit Zugriffstabelle.....	144
5.1.3.4	Problem beim Arbeiten mit Views	145
5.2	Vorteile von Fine Grained Access Control	147
5.2.1	Begriffsklärung: FGA – FGAC?.....	149
5.3	Arbeiten mit FGAC	150
5.3.1	FGAC: Arbeiten mit Dynamischen Prädikaten	151

5.3.2	DBMS_RLS – So arbeitet FGAC	152
5.3.2.1	add_policy	152
5.3.2.2	Funktion	153
5.3.2.3	Environment Variable	154
5.3.2.4	Transiente View	155
5.3.3	Beispiel: Einfache Policy erzeugen	156
5.3.4	Ideen der Zugriffssteuerung	158
5.3.5	Nötige Zugriffsrechte	159
5.3.6	DBMS_RLS – administrative Schnittstelle für Policies	160
5.3.7	Kontext	161
5.3.7.1	Typen eines Kontextes	161
5.3.7.2	Erstellen eines Kontextes	162
5.4	Spaltenbasierte Sicherheit	166
5.5	VPD Neuerungen in 12c	168
5.6	Oracle Label Security	169
6	Data Redaction und Transparent Sensitive Data Protection (TSDP)	170
6.1	Data Redaction	171
6.1.1	Begriffsklärung	171
6.1.2	Methoden	172
6.1.3	EXEMPT Redaction Policy	173
6.1.4	Prozeduren	174
6.1.5	Einschränkungen	175
6.1.6	add_policy	176
6.1.7	Update_full_redaction_values	178
6.1.8	Alter_policy	179
6.1.9	Random Redaction	181
6.1.10	Regexp Redaction	182
6.1.11	Data Redaction Views	183
6.1.12	Schnittstellen / Abgrenzung	184
6.2	Data Sensitive Transparent Protection (TSDP)	186
6.2.1	Vorgehensweise	186
6.2.2	Erstellen Sensitive Type / Definition der sensitiven Spalten	187
6.2.3	Policy erstellen	188
6.2.4	Verknüpfung und Aktivierung	189
6.2.5	TSDP Aktivierung	190
7	Auditing, FGA	191
7.1	ORACLE Auditing Modi - Historie	192
7.2	Auditing bevor 12c	193
7.3	Auditing in 12c – Mixed Mode	194
7.4	Auditing in 12c – Pure Mode	195
7.5	Überblick	196
7.6	Mandatory Auditing	197
7.6.1	Mandatory Auditing UNIX	198
7.6.2	Mandatory Auditing Microsoft	199
7.7	SYS Auditing	200
7.8	Standard Auditing	201
7.8.1	Aktivierung	201
7.8.2	Möglichkeiten	203
7.8.3	Beispiele Statement Auditing	204
7.8.4	Beispiele Einschränkungen	205
7.8.5	„Enhanced Default Security Settings“ in Oracle 11g	207
7.8.6	Auditing auf Session- und Statement-Ebene (ab 11g R2)	209
7.8.7	Views	210
7.9	Fine-Grained Auditing (FGA)	211
7.9.1	Erstellen einer FGA Policy	212
7.9.2	Auswirkung der FGA Policy	213
7.9.3	FGA Data Dictionary Views	214
7.9.4	Audit auf Spalten und mit inhaltlichen Beziehungen	215

7.9.4.1	Das Audit fokussieren: Audit Columns	215
7.9.4.2	Das Audit weiter fokussieren: Audit Conditions	216
7.9.5	FGA Policies verwalten	217
7.9.6	FGA Policy und Views	218
7.9.6.1	FGA Policy wirkt auch bei Abfragen über Views	218
7.9.6.2	Eine FGA Policy speziell für eine View erstellen	219
7.9.7	Zusammenspiel von FGA Policies	220
7.9.8	Weitere mögliche Anwendungen	221
7.10	Auditing über OS/syslog	223
7.11	Applikatorisches (Value-based) Auditing	225
7.12	Audit-Daten verwalten: Package DBMS_AUDIT_MGMT	227
7.13	Unified Auditing	231
7.13.1	Überblick	231
7.13.2	Unified Auditing - Mixed Mode	232
7.13.3	Aktivierung	233
7.13.4	Funktionsumfang	234
7.13.5	Ablageort und Zugriff	235
7.13.6	Separation of Duty für Audit Administratoren	236
7.13.7	Schreib-Modus	237
7.13.8	Beispiele	238
7.13.9	Change Effective Immediately	239
7.13.10	Auditing Data Pump	240
7.13.11	Auditing über OS/syslog (Unified Auditing)	241
7.13.12	Löschen von Audit Einträgen	243
7.13.13	Export der Auditdaten	244
7.13.14	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	248
7.15.3	Architektur und Komponenten	249
8	Datenbankverschlüsselung	253
8.1	Datenverschlüsselung in der Datenbank	254
8.2	Symmetrische Verschlüsselung	255
8.3	Programmatische Verschlüsselung	256
8.3.1	DBMS_OBFUSCATION_TOOLKIT	256
8.4	DBMS_CRYPTO	257
8.4.1	Funktionen und Prozeduren	257
8.4.2	Verschlüsselungsalgorithmen	259
8.4.3	Hash-Funktionen	260
8.5	Vergleich DBMS_CRYPTO und DBMS_OBFUSCATION_TOOLKIT	262
8.5.1	Padding	263
8.5.2	Cypher Block Chaining	265
8.5.3	Schlüsselmanagement	266
8.6	Transparente Datenverschlüsselung (TDE)	267
8.6.1	Das Oracle Wallet	267
8.6.1.1	Graphik	267
8.6.1.2	Überblick	268
8.6.1.3	Grundlegende Verwaltung	269
8.6.2	Transparente Spaltenverschlüsselung	271
8.6.2.1	Überblick	271
8.6.2.2	Transparente Verschlüsselung – je Spalte	273
8.6.2.3	Salt-Prinzip	275
8.6.3	Verschlüsselung von Tablespaces	277
8.6.3.1	Transparente Datenverschlüsselung	277
8.6.3.2	Online Verschlüsselung von Tablespaces	278
8.6.3.3	Offline Verschlüsselung von Tablespaces	279
8.6.3.4	Vorteile und Einschränkungen	280
8.6.4	Wallet Management	281

8.6.4.1	Auto-Login Wallet	283
8.6.5	TDE und Hardware Security Module (HSM)	285
8.6.6	Keystore Management	287
8.6.6.1	Zusammenführung (Merging) von Software Keystores	288
8.6.6.2	Backup und Restore des Keystores	289
8.6.6.3	Zugriff mehrerer Datenbanken auf ein Wallet	290
8.6.6.4	Verschieben von Keystores	291
8.6.6.5	Migration einer verschlüsselten Datenbank auf einen neuen Server	292
8.6.6.6	Passwortwechsel des Keystores	293
8.6.7	Management des Master Encryption Keys	294
8.6.7.1	Anlegen eines Master Encryption Keys	295
8.6.7.2	Aktivierung eines Schlüssels	296
8.6.7.3	Export des Master Encryption Keys	297
8.6.7.4	Import des Master Encryption Keys	298
8.7	Data Pump Encryption	299
8.7.1	Überblick	299
8.7.2	Parameter	300
8.8	Verschlüsselte Backups mit RMAN	301
8.8.1	Arten der Backupverschlüsselung	302
8.8.1.1	Passwort-Modus	303
8.8.1.2	Transparenter Modus	304
8.8.1.3	Dualer Modus	305
9	Oracle Net	306
9.1	Listener	307
9.1.1	Angriffspunkte	307
9.2	Standard-Ports	308
9.3	Connection Manager	309
9.3.1	Überblick	309
9.3.2	Multiplexing	310
9.3.3	Protocol Switch	311
9.3.4	Zugangskontrolle	312
9.3.5	Architektur	313
9.3.6	Regelwerk	315
9.3.6.1	Grundlagen	315
9.3.6.2	Beispiele	316
9.3.7	Absicherung	318
9.4	Advanced Security Option	319
9.4.1	Überblick	319
9.4.2	Netzwerkverschlüsselung Vor /Nachteile	320
9.4.3	Verschlüsselungsmethoden	321
9.4.4	Leistungsmerkmale	322
9.4.5	Client/Server Versionen und Verschlüsselung	326
9.4.6	Vor- und Nachteile	327
9.4.7	Integrität	329
9.4.7.1	Überblick	329
9.4.7.2	Aktivierung	330
9.4.7.3	Parameter CRYPTO_CHECKSUM	331
9.4.7.4	Beispielkonfiguration	333
9.4.8	Verschlüsselung	334
9.4.8.1	Diffie Hellmann Algorithmus	334
9.4.8.2	Parameter	336
9.4.8.3	Algorithmen	337
9.4.9	SSL-basierte Authentifizierung	338
9.4.9.1	Grundlagen	338
9.4.9.2	Vor- und Nachteile	340
9.4.9.3	SSL und Oracle	341
9.4.9.4	Aufbau einer SSL-Verbindung in der Oracle Umgebung	342
9.4.9.5	Konfiguration	343
9.4.9.6	Wallet erstellen	345

9.4.9.7	Digitales Zertifikat	347
9.4.9.8	Zertifikate einfügen	349
9.4.9.9	SSL Listener Konfiguration	351
9.4.9.10	Konfiguration des Clients	353
9.4.9.11	Fazit	354
9.5	Interpretation von SID als Service Name	355
9.6	Oracle Net Logging und Tracing	356
9.6.1	Oracle Net Logging de-/aktivieren	358
9.6.2	Oracle Net Tracing de-/aktivieren	360
9.6.3	Oracle Net Logging und Tracing im ADR (11g)	362
⇒	Sonstiges	364
○	Database Links	365
▪	Grundlagen	365
▪	Konzept	367
▪	Infos	369
▪	Sicherheit ab 12.2	370
○	init.ora Parameter	371
▪	O7_DICTIONARY_ACCESSIBILITY	371
▪	REMOTE_OS_AUTHENT	372
▪	SQL92_SECURITY	373
▪	UTL_FILE_DIR	374
•	Oracle Directories	375
•	„EXECUTE“ Privileg auf Verzeichnisobjekte	376
▪	Export-Files	378
▪	glogin.sql	379
▪	Verify Function	380
○	Allgemeines	381
○	Beispiel	382
○	Strategien zur Vermeidung	383
○	Einsatz des Packages DBMS_ASSERT	385
○	Trigger	387
▪	Trigger Allgemein	387
▪	Fehlermanagement	388
▪	Security	389
○	LogMiner	390
▪	Einleitung	390
▪	Zugriff auf das Data Dictionary	392
▪	Security	393
○	Critical Patch Updates	394
○	Release Update (RU) vs. Release Update Revision (RUR)	396
○	DBSAT	397
▪	Sicherheitsempfehlungen	398
○	Architektur	399
•	Architektur Collector/Reporter	400
•	Architektur Discoverer	401
▪	Installation	402
▪	Aufruf Collector	403
▪	Aufruf Reporter	405
▪	Beispiel Report	407
▪	Aufruf Diascoverer	408
10	Data Masking	412
10.1	Was ist Data Masking?	413
10.2	Warum Data Masking?	415
10.3	Anforderungen	416
10.4	Vorgehen	418
10.5	Verfügbarkeit mit Data Pump	420
10.6	Verfügbarkeit mit Oracle EM	425

10.7	Database Masking and Subsetting	435
11	Direkte Anbindung Oracle an Active Directory	436
11.1	Oracle 12c – Gesamtbild.....	437
11.2	Zentrale Benutzerverwaltung (Oracle 12c)	439
11.3	Zentrale Benutzerverwaltung ab Oracle 18c.....	440
11.4	Übersichtsbild.....	441
11.5	Konfigurationsmöglichkeiten	442
11.6	Authentifizierungsmethoden.....	443
11.7	Rechtevergabe	444
11.8	Bewertung	445
12	Projektansatz	446
12.1	Zusammenfassung der Security Anforderungen	447
12.2	Dokumente	448
12.3	Datenbank Security Handbuch	449
12.3.1	Verantwortlichkeiten	450
12.3.2	Inventar.....	451
12.3.3	Patch Management	452
12.3.4	Benutzer	453
12.3.5	Passworte.....	454
12.3.6	Authentifizierung.....	455
12.3.7	Auditing.....	456
12.3.8	Anonymisierung.....	457
12.3.9	Verschlüsselung	458
12.3.10	Change Management.....	459
12.3.11	Backup & Recovery	460
12.3.12	Sonstiges.....	461
12.4	Security Dokument je Datenbank / Applikation	462
13	Übungen	463
13.1	Sicherheit für Benutzer und Passwörter	464
13.2	Delayed Failed Login, OPS\$User, PW-File	465
13.3	Secure External Password Store	466
13.4	Auf Benutzerebene: Privilegien.....	467
13.5	Auf Benutzerebene: Rollen	468
13.6	Access Control Listen (ACLs)	469
13.7	FGAC	470
13.8	Data Redaction.....	471
13.9	SYS und Mandatory Auditing	472
13.10	Standard Auditing (DDL)	473
13.11	Standard Auditing (DML).....	474
13.12	Value-Based Auditing.....	475
13.13	FGA Auditing	476
13.14	FGA Auditing auf Spalten.....	477
13.15	Unified Auditing	478
13.16	Verschlüsselung DBMS_OBFUSCATION_TOOLKIT	479
13.17	TDE Tablespace, Data Pump und RMAN Encryption.....	480
13.18	GLOGIN.sql und Verify_Function.....	481
13.19	Data Masking	482