



Oracle Security in der Praxis

Sicherheit für Ihre Oracle-Datenbank

Inhalt

Vorwort	XI
1 Identifizierung und Authentisierung	1
1.1 Einleitung	2
1.2 Warum ist Authentisierung wichtig?	5
1.3 Starke und schwache Authentisierung	7
1.3.1 Authentisierung über Passwort	7
1.3.2 Starke und schwache Passwörter	8
1.3.3 Externe Benutzer	13
1.4 Passwort- und Benutzerverwaltung in Oracle.....	15
1.4.1 Passwortverwaltung über Profile	15
1.4.2 Passwortverifizierungsfunktionen.....	16
1.4.3 Der externe Passwortspeicher	17
1.5 Authentisierung für Internet-Applikationen	20
1.5.1 Was ist Proxy-Authentisierung?	21
1.5.2 Formen der Proxy-Authentisierung	21
1.6 Enterprise User Security	23
1.6.1 Public-Key-Infrastruktur (PKI).....	25
1.6.2 Konfiguration der Enterprise User Security	28
1.6.3 Passwortverwaltung in OID	39
1.6.4 Enterprise User Proxy	40
1.7 Datenbank-Links	42
2 Kontrolle des Datenzugriffs	45
2.1 Autorisierung durch Benutzer und Rollen	46
2.1.1 Autorisierung auf Benutzerebene.....	46
2.1.2 Rollen	49
2.2 Privilegien	58
2.2.1 Systemprivilegien	58
2.2.2 Objektprivilegien	60
2.3 Kontrolle auf Datenebene.....	61
2.3.1 Zugriffskontrolle über Views, Stored Procedures und Triggers.....	61
2.3.2 Virtual Private Database und Fine-Grained Access Control	69
2.3.3 Oracle Label Security (OLS)	83

3	Datenübertragung	109
3.1	Schutzmaßnahmen für den SQL*Net Listener	111
3.2	Physikalische Zugriffskontrolle.....	112
3.2.1	Beschränkung von IP-Adressen.....	112
3.2.2	Sperrung von IP-Adressen.....	114
3.3	Sichere Übertragung der Passwörter	114
3.4	Verschlüsselung der Daten.....	116
3.4.1	Verschlüsselung des SQL*Net-Verkehrs durch die Advanced Security Option....	117
3.4.2	Verschlüsselung spezieller Schnittstellen und Protokolle.....	122
3.5	Prüfsummen	127
3.5.1	Konfiguration der Prüfsummen	128
3.5.2	Integritätssicherung für spezielle Schnittstellen und Protokolle	128
3.6	Prüfung der Netzwerksicherheit.....	128
3.6.1	Erzwingen der Verschlüsselung und/oder der Prüfsumme	128
3.6.2	SQL*Net Tracing	129
3.7	Performance bei gesicherter Übertragung	130
4	Datenspeicherung und Datensicherung.....	131
4.1	Verschlüsselung der Daten innerhalb der Datenbank.....	133
4.1.1	Transparente Datenverschlüsselung.....	134
4.1.2	DBMS_CRYPTO.....	145
4.2	Die Verschlüsselung von Datensicherungen	151
4.2.1	Verschlüsselung durch die Backup-Software	152
4.2.2	Verschlüsselung mit RMAN.....	152
5	Überwachung.....	157
5.1	Applikatorische Überwachung.....	158
5.1.1	Protokollierung durch eine Logdatei	158
5.1.2	Applikatorisches Logging in der Datenbank	161
5.1.3	Alarmierung.....	163
5.2	Audit durch die Datenbank.....	164
5.2.1	Der AUDIT_TRAIL-Initialisierungsparameter	164
5.2.2	Audit-Dateien, die immer geschrieben werden.....	165
5.2.3	Datenbank oder Datei für die Prüfspur?	166
5.2.4	Audit-Einstellungen.....	167
5.2.5	Das Ausschalten des Audit	178
5.2.6	Audit-Privilegien	179

5.2.7	Auditauswertungen	179
5.2.8	Richtlinien für das Audit.....	188
5.3	Audit auf Datenbene: Fine-Grained Auditing (FGA)	185
5.3.1	Das DBMS_FGA Package.....	187
5.3.2	Der Einsatz von FGA.....	189
5.3.3	Notwendige Privilegien für den Einsatz von FGA.....	190
5.3.4	Ein Beispiel für den Einsatz von FGA.....	191
5.3.5	FGA-Datenbankauswertungen.....	192
5.4	Audit in Oracle Label Security	193
6	Anhang: Sicherheits-Checks für die Datenbank.....	197
6.1	Architektur	198
6.2	Physikalische Sicherheit.....	199
6.3	Benutzer	199
6.4	Passwörter	199
6.5	Privilegien und Rollen.....	199
6.6	Überwachung	200
	Literatur	201
	Register.....	203

1 Identifizierung und Authentisierung



Im ersten Kapitel geht es um Identifizierung und Authentisierung, also darum, als welche Person Sie sich gegenüber der Datenbank ausweisen; neben der Autorisierung, die wir im nächsten Kapitel behandeln, ist dies einer der Grundpfeiler der Sicherheit, wenn Sie mit Oracle arbeiten.

1.1 Einleitung

In den Anfangstagen der IT hatte Sicherheit vornehmlich zwei Aspekte: den physikalischen und den humanen. Unter physikalischem Aspekt verstehe ich hier in erster Linie den Zugang zum Computer. Die physikalische Sicherung des Computers bestand damals im Wesentlichen darin, dass er in einem gut verschlossenen Raum stand, zu dem nur autorisiertes Personal Zutritt hatte. Diese Art der Sicherung hat nach wie vor ihre Berechtigung und existiert auch noch heute; IT-Profis sind Serverräume wohl vertraut.

Auch der zweite Sicherheitsaspekt, der humane, ist nach wie vor aktuell und der bei weitem schwierigere. Zum einen geht es hier darum, dafür zu sorgen, dass nur autorisiertes Personal Zugriff auf den Computer und die Programme hat. Das ist aber nur ein Teilaspekt der Sicherheit. Zum anderen sollte sichergestellt werden, dass kein Schaden durch die eigenen Mitarbeiter verursacht wird. Für den Großteil der Sicherheitsverletzungen sind nicht die viel beschworenen Hacker, sondern die eigenen Mitarbeiter verantwortlich. Dabei braucht es sich auch nicht um böse Absicht zu handeln, manchmal genügen Fehler, wie sie immer wieder vorkommen. Natürlich gibt es auch den frustrierten Angestellten, der sich rächen will, aber das ist nur ein möglicher Verursacher. Die Kunst besteht hier darin, die Sicherheitslücken schnell zu entdecken und zu schließen.

Die Vernetzung der Computer untereinander und speziell das Internet haben eine zusätzliche Dimension ins Spiel gebracht. Jetzt war es plötzlich möglich, auf Computer zuzugreifen, die ganz woanders standen. Es war nicht mehr notwendig, dass man direkt vor dem Computer saß. Der Computer konnte in einem anderen Raum, in einer anderen Stadt oder sogar auf einem anderen Kontinent stehen. Das eröffnete natürlich auch auf der Gefährdungsseite ganz neue Angriffsszenarien. Um an die Daten eines Computers zu kommen, genügte es jetzt, Zugriff auf den Computer zu erlangen, der physikalische Zugang war nicht mehr notwendig. Dies und die rasante Ausbreitung des Internet führten vor einigen Jahren zu Architekturen, in denen der Zugang zum Rechner über das Internet über eine demilitarisierte Zone (DMZ) erfolgt.

Eine DMZ ist immer von Firewalls umgeben. Dabei reguliert zumindest ein Firewall die Kommunikation zwischen DMZ und Internet und ein weiterer Firewall übernimmt die Kommunikation zwischen DMZ und Intranet. Die eigentlichen Nutz- und Firmendaten stehen

im Intranet. Ein Firewall ist quasi ein Netzwerkrouter, der nur bestimmte Ports und Netzwerkprotokolle durchlässt. Durch die Abschottung des Intranets über die vorgelagerte DMZ soll gewährleistet werden, dass keine illegalen Meldungen/Protokolle vom Internet ins Intranet gelangen (und umgekehrt) und dass in Falle einer Übernahme eines Rechners durch einen Angreifer der Angriff auf den betroffenen Rechner beschränkt bleibt.

Selbstverständlich können auch mehrere DMZ-Zonen eingerichtet werden, typischerweise steht ja auch ein Applikationsserver, der die Präsentation der Daten übernimmt und seinerseits die Daten vom und ins Intranet überträgt, in einer DMZ.

Passwörter und ihre Nachteile

Moderne Computer arbeiten im Regelfall mit einem Betriebssystem, das den Benutzer zwingt, sich mit einem Namen und einem Passwort anzumelden. Diese Form der Authentisierung ist nach wie vor die gebräuchlichste. Sie wird nicht nur bei der Anmeldung im System, sondern ganz generell beim Arbeiten mit irgendwelchen Programmen verwendet. Man spricht hier auch von einem Berechtigungsnachweis (englisch Credential), wobei die Identifikation des Benutzers auch über andere Formen der Authentisierung – als Beispiel sei hier eine Chipkarte (englisch SmartCard) genannt -- erfolgen kann. Ein Credential aus dem täglichen Leben, das wir alle kennen, ist der Personalausweis. Ich verwende hier die Begriffe Identifizierung und Authentisierung gleichbedeutend, obwohl sie das streng genommen nicht sind (und auch Authentisierung noch von Authentifizierung unterschieden werden kann); wesentlich ist hier nur, dass der Benutzer eindeutig identifiziert wird.

Dabei braucht es sich beim Benutzer nicht um einen Menschen zu handeln, es kann ebenso gut ein anderer Computer oder auch nur ein anderes Programm sein.

Immer, wenn Sie mit der Datenbank arbeiten, müssen Sie sich vorher bei der Datenbank mit Benutzernamen und Passwort anmelden, eine anonyme Anmeldung gibt es bei Oracle nicht. Der Benutzer kann dabei in der Datenbank selbst angelegt sein oder auch als so genannter Enterprise-Benutzer in einem LDAP-Server, der dann seinerseits die Autorisierung für die Datenbank übernimmt, definiert werden. Hier können an Stelle von Passwörtern digitale Zertifikate verwendet werden. Eine weitere Möglichkeit schließlich ist die Autorisierung des Oracle-Benutzers durch das Betriebssystem; diese Variante ist sehr gut für Stapelverarbeitungen geeignet, da sie normalerweise kein zusätzliches Passwort benötigt; der Benutzer wurde ja schon durch das Betriebssystem identifiziert.

Passwörter bescheren uns allerdings ein gravierendes Problem: sie können erraten werden. Um das Erraten zu erschweren, werden oft bestimmte Anforderungen an ein Passwort gestellt: Neben einer Mindestlänge – 8 oder 12 Zeichen sind zum Beispiel ganz gute Werte – wird oft auch gefordert, dass das Passwort aus Klein- und Großbuchstaben besteht und mindestens ein Sonderzeichen oder eine Zahl enthält. Eine bekannte Form von Passwörtern, die uns allen aus dem täglichen Leben vertraut ist, sind beispielsweise Geheimnummern (auch persönliche Identifikationsnummer oder kurz PIN genannt), die nur aus Zahlen bestehen und für die Authentisierung an Geldautomaten und Handys benutzt werden.

Der große Vorteil von Passwörtern liegt sicher darin, dass die Kosten für Implementierung und Unterhalt relativ gering sind. Der große Nachteil ist, wie schon erwähnt, der relativ schwache Schutz. Man spricht bei der Authentisierung über Passwörter auch von schwacher Authentisierung.

Stärkere Formen der Authentisierung basieren zum Beispiel auf örtlichen Einschränkungen – der Zugang ist nur direkt am Computer oder von bestimmten Rechnern aus möglich – oder Dingen, die man besitzt. Solche Dinge können Chipkarten, Softwarelizenzschlüssel oder digitale Zertifikate sein. Biometrische Merkmale, die mit speziellen Geräten wie Fingerabdrucklesern und Irisscannern überprüft werden, bieten offensichtlich den stärksten Schutz, erfordern aber auch die größten Investitionen.

Selbstverständlich können und werden die verschiedenen Methoden auch kombiniert eingesetzt: Am Bankautomaten benötigen Sie Bankkarte und Geheimnummer (und Geld auf dem Konto, sonst gibt's auch nichts ...).

Passwörter werden aber wohl mit der Zeit verschwinden oder zumindest nicht mehr dieselbe Stellung wie heute einnehmen; neulich habe ich im Supermarkt schon ein Sonderangebot für einen Fingerabdruckleser gesehen.

Starke Authentisierung kann in einer Oracle-Umgebung mit der Oracle Advanced Security Option (ASO), die zusätzlich installiert und lizenziert werden muss, konfiguriert werden. Neben ASO ist bei diesen Formen der Authentisierung zusätzliche Hard- und/oder Software notwendig. ASO unterstützt RADIUS und damit auch SecureID, Entrust, Kerberos und SSL. Die Authentisierung über SSL wird im Folgenden noch im Detail beschrieben, für die Details zu RADIUS und Kerberos verweise ich Sie auf Teil 3 in [ORAASO102] und [ORAEUS102].

Bei der Authentisierung gibt es ein weiteres Problem: Normalerweise arbeitet ein Benutzer nicht nur mit einer Applikation, sondern mit mehreren, was bedeutet, dass er sich bei jeder Applikation neu anmelden muss. Sie ahnen wahrscheinlich jetzt schon, wo das Problem liegt, oder kennen es bereits: Versuchen Sie mal, sich 20 unterschiedliche Passwörter zu merken. Das ist kein Spaß.

Eine Lösung hier verspricht Single Sign On (SSO). SSO bedeutet, Sie authentisieren sich nur ein einziges Mal auf einer Portal- oder Webseite und können dann auf alle Rechner und Dienste, für die Sie autorisiert sind, zugreifen, ohne sich neu anmelden zu müssen. Der SSO-Mechanismus übernimmt dann die weitere Authentisierung für Sie. Nachteilig ist hier natürlich, dass ein Hacker, falls er die Identität eines regulären Benutzers gestohlen hat, sofort Zugriff auf alle Systeme hat. Aus diesem Grunde empfiehlt es sich, bei SSO-Systemen stärkere Autorisierungsformen zu verwenden. Andererseits benötigen Sie gerade bei einem SSO-Portal einen Mechanismus, der auch die Anbindung von externen Applikationen erlaubt; das ist wiederum am einfachsten über Benutzername und Passwort zu realisieren. In einer Oracle-Umgebung kann SSO über Oracle Application Server Single Sign-On (OracleAS SSO) realisiert werden.

1.2 Warum ist Authentisierung wichtig?

Authentisierung ist in Oracle-Systemen vor allem deshalb so wichtig, weil Oracle nur anhand Ihres Benutzernamens bestimmt, welche Privilegien Sie haben. Es gibt keine anonyme Anmeldung an eine Oracle-Datenbank. Egal, wie die Anmeldung erfolgt, letzten Endes existiert immer ein Benutzer in der Oracle-Datenbank, und dieser Benutzername entscheidet, was Sie machen können und was nicht. Dabei können die Rechte und Privilegien des Benutzers, wenn man mal von den durch Oracle bereitgestellten vordefinierten Benutzern absieht, ganz unabhängig vom Namen des Benutzers definiert werden.

Die Liste der aktiven Benutzer sehen Sie übrigens immer im Data Dictionary View V\$SESSION. Das SELECT in der folgenden Abfrage verwendet die Bedingung USERNAME IS NOT NULL, um die Oracle-internen so genannten Hintergrundprozesse auszuschließen, und die Bedingung PIECE=0, um nur die ersten 64 Zeichen des Benutzerkommandos anzuzeigen. Da sich der gleiche Benutzer theoretisch – praktisch kommt das aus verschiedenen Gründen auch sehr häufig vor – mehrmals an derselben Datenbank anmelden kann, gibt es in Oracle noch den so genannten Session Identifier oder kurz SID genannt. Damit können unterschiedliche Sessions des gleichen Benutzers unterschieden werden:

Listing 1.1 Benutzer inklusive verwendetem SQL

```
SQL> select sid,username as user, sql_text
  2 from v$session, v$sqltext
  3 where sql_address=address
  4 and piece=0 and username is not null
  5 order by username;
```

```
SID USER      SQL_TEXT
---
145 SYSTEM select sid,username,sql_text from v$session, v$sqltext where
```

Wie man in der obigen Abfrage sieht, ist der Frager in diesem Beispiel gleichzeitig auch der einzige aktive Benutzer.

Einen Benutzer legen Sie in Oracle im SQL mit dem Befehl CREATE USER an. Dabei kann der Benutzername bis zu 30 Bytes lang werden, und Sie können als Benutzernamen eigentlich alle Zeichen verwenden, die in [ORASQL102] als gültig aufgeführt werden. Oracle empfiehlt allerdings, dass Sie nur Zeichen aus dem ASCII- oder EBCDIC-Zeichensatz verwenden. Dem kann ich mich nur anschließen: So können Sie Portierungsprobleme, die eventuell eines Tages beim Wechsel der Plattform Ihrer Datenbank entstehen könnten, von vornherein ausschließen.

Daneben existieren in Oracle bereits einige vordefinierte Benutzer, am bekanntesten sind hier sicher SYS und SYSTEM. SYS ist quasi der Meta-User der Datenbank. Nach dem Anlegen der Datenbank gehören die internen Strukturen der Datenbank diesem Benutzer. Die vordefinierten Benutzer schauen wir im nächsten Abschnitt noch ein wenig genauer an. Diese Benutzer hatten lange Zeit Default-Passwörter. Auch das verschwindet zwar langsam, doch es besteht zumindest seit Version 9i bei der Installation die Möglichkeit, für

SYS und SYSTEM Passwörter zu setzen. Auch sind die meisten Default-Benutzer seit Version 9i nach der Installation gesperrt. Aber es gibt ja noch jede Menge Nicht-Oracle-Software, die Default-Benutzer verwenden. Das ist immer noch eine der besten Einbruchsmöglichkeiten in eine Oracle-Datenbank; die Default-Benutzer besitzen zum Teil recht mächtige Privilegien.



Deshalb gilt:
Verwenden Sie nie Default-Passwörter!

Eine sehr vollständige Liste der Default-Benutzer und -Passwörter inklusive der entsprechenden Check-Programme finden Sie im Internet auf den Seiten von Pete Finnigan (<http://www.petefinnigan.com>).

Ein Benutzer kann nur einmal in einer Oracle-Datenbank existieren. Falls Sie also einen bereits bestehenden Benutzer noch mal anlegen wollen, erhalten Sie den Fehler ORA-1920.

Die Befehle ALTER/CREATE USER sind ganz gut für Batch-Verarbeitungen geeignet, es gibt aber auch komfortablere Möglichkeiten. Eine davon ist die Database Control Console, die mit Version 10g eingeführt wurde. Database Control Console ist eine abgespeckte Form des Oracle Enterprise Managers und lässt sich recht einfach mit dem Kommando „emca config dbcontrol“ anlegen. Während der Oracle Enterprise Manager einen zentralen Einstiegspunkt für die Verwaltung mehrerer Datenbanken bietet, funktioniert die Database Control Console nur gegen die Datenbank, für die sie konfiguriert wurde. Wie Abbildung 1.1 zeigt, ist damit auf einfache Art das Anlegen eines Benutzers möglich:

The screenshot shows the Oracle Enterprise Manager 10g Database Control interface. The main title is "ORACLE Enterprise Manager 10g Database Control". The breadcrumb navigation is "Datenbank-Instance: orcl > Benutzer > Erstellen Benutzer". The user is logged in as "Angemeldet als SYSMAN". The page title is "Erstellen Benutzer". There are buttons for "SQL anzeigen", "Abbrechen", and "OK". The form has several tabs: "Allgemein", "Rollen", "Systemberechtigungen", "Objektberechtigungen", "Quota", "Berechtigungen für Nutzungsgruppen wechseln", and "Proxy-Benutzer". The "Allgemein" tab is active. The form fields include: "Name" (required), "Profil" (dropdown menu set to "DEFAULT"), "Berechtigungsprüfung" (dropdown menu set to "Kennwort"), "Kennwort eingeben" (required), "Kennwort bestätigen" (required), "Default Tablespace" (text input), "Temporärer Tablespace" (text input), and "Status" (radio buttons for "Gesperrt" and "Sperre aufgehoben", with "Sperre aufgehoben" selected). There is a checkbox for "Kennwort läuft jetzt ab" and a note: "Bei der Auswahl Kennwort wird die Rolle über Kennwort autorisiert." At the bottom, there are buttons for "SQL anzeigen", "Abbrechen", and "OK".

Abbildung 1.1 Anlegen eines Benutzers mit der Database Control Console

Register

A

- ACCESSED GLOBALLY 72
- ACCOUNT LOCK 15
- ACCOUNT UNLOCK 15
- adapters 117
- ADD_POLICY 75, 76, 79, 80
- Advanced Encryption Standard 119
 - siehe auch AES*
- AES 126, 130, 137, 141, 152
- AES (Verschlüsselungsalgorithmus) 119, 130
- ALL_AUDIT_POLICIES 192
- ALL_AUDIT_POLICY_COLUMNS 192
- ALL_CONTEXT 73
- ALL_CONTROL (OLS) 97
- ALL_ENCRYPTED_COLUMNS 143
- ALL_POLICIES 81
- ALL_POLICY_CONTEXTS 81
- ALL_POLICY_GROUPS 81
- ALL_SA_POLICIES 107
- ALL_SOURCE 50
- ALL_UPDATABLE_COLUMNS 64
- ALTER ANY TABLE-Privileg 59
- ALTER SYSTEM 136
- ALTER SYSTEM SET ENCRYPTION KEY 136
- ALTER SYSTEM SET WALLET CLOSE 143
- ALTER SYSTEM SET WALLET OPEN
 - IDENTIFIED BY 142
- ALTER USER 15, 22, 49, 115
- ALTER USER-Privileg 12, 47
- ANY-Privileg 59, 175
- APPLY_TABLE_POLICY 93, 103
- asymmetrische Verschlüsselung 117
- AUD\$ 165, 167
- AUDIT 164
- AUDIT AUDIT 173
- AUDIT BY ACCESS 171
- AUDIT BY SESSION 171
- AUDIT DELETE TABLE 186
- AUDIT EXECUTE 186
- AUDIT GRANT 173
- AUDIT INSERT TABLE 186
- AUDIT NETWORK 170
- AUDIT NOT EXISTS 176
- AUDIT ON DEFAULT 175
- AUDIT READ 173
- AUDIT SESSION 167, 186
- AUDIT SESSION WHENEVER NOT SUCCESSFUL 186
- AUDIT SYSTEM 179
- AUDIT SYSTEM AUDIT 178
- AUDIT TABLE 177, 186
- Audit Trail 164 *siehe auch Prüfspur*
- AUDIT UPDATE TABLE 186
- Audit von An- und Abmeldungen 167 ff.
- Audit von Objekten 171 ff.
- AUDIT_ACTIONS 170
- AUDIT_COLUMN_OPTS (FGA) 189
- AUDIT_CONDITION 189
- AUDIT_CONDITION (FGA) 189
- AUDIT_FILE_DEST 164, 189, 192
- AUDIT_SYS_OPERATIONS 169
- AUDIT_SYSLOG_LEVEL 166
- AUDIT_TRAIL 164, 165, 181, 187, 189, 194
- AUTHENTICATED USING PASSWORD 22
- AUTHENTICATION_SERVICES 124
- Authentisierung
 - durch das Betriebssystem 13
 - über SSL 14, 37
- AUTHID CURRENT_USER 52, 69
- autonome Transaktion 162

B

- Brute-Force-Angriff 150

C

CA 24
 Caesars Verschlüsselung 116
 Caller's Rights Prozedur 69
 Certificate Revocation List *siehe* CRL 25
 Certification Authority 24 *siehe auch* CA
 CHAR_TO_LABEL 95, 102
 CHECK_CONTROL (OLS) 97, 103
 CHECKSUMMING_SERVER 128
 CHECKSUMMING_TYPES_SERVER 128
 CLEAR_ALL_CONTEXT 72
 CLEAR_CONTEXT 72
 CLEAR_IDENTIFIER 74
 CLIENT_IDENTIFIER 71
 CLIENT_INFO 71, 74
 CN 26
 Common Name 26 *siehe auch* CN
 COMPACCESS-Privileg (OLS) 100
 Compartment (OLS) 89
 COMPATIBLE 75, 134, 152
 CONFIGURE ENCRYPTION (RMAN)
 153, 155
 Connection Pool 20
 CONNECT-Rolle 56, 176
 CONTEXT_SENSITIVE (Policy) 78
 CONVERT 148
 CREATE ANY CONTEXT 71
 CREATE CONTEXT 71
 CREATE DATABASE LINK 42
 CREATE DIRECTORY 159
 CREATE PUBLIC DATABASE LINK 43
 CREATE ROLE 49, 51, 55, 56, 115
 CREATE SESSION-Privileg 8, 22, 34, 59
 CREATE TABLE-Privileg 58
 CREATE USER 56
 CREATE_COMPARTMENT 90
 CREATE_LABEL 91, 102
 CREATE_LEVEL 88
 CREATE_POLICY 87
 CREATE_POLICY_GROUP 81
 CREATE_WRAPPED() 143
 createProxyConnection() 23
 Credential 3

CRL 25

CRYPTO_SEED 121

CURRENT_SCHEMA 71

CURRENT_USER-Klausel 43

D

Data Encryption Standard 119 *siehe auch* DES
 Datenbank beim OID-Server registrieren 28
 DB_DOMAIN 42
 DB_NAME 42
 DBA_AUDIT_EXISTS 183
 DBA_AUDIT_OBJECT 183
 DBA_AUDIT_POLICIES 192
 DBA_AUDIT_POLICY_COLUMNS 192
 DBA_AUDIT_SESSION 183
 DBA_AUDIT_STATEMENT 183
 DBA_AUDIT_TRAIL 183
 DBA_COMMON_AUDIT_TRAIL 183, 184,
 193
 DBA_CONTEXT 81
 DBA_ENCRYPTED_COLUMNS 143
 DBA_FGA_AUDIT_TRAIL 193
 DBA_GLOBAL_CONTEXT 81
 DBA_POLICIES 81
 DBA_POLICY_CONTEXTS 81
 DBA_POLICY_GROUPS 81
 DBA_ROLE_PRIVS 48, 57
 DBA_ROLES 57
 DBA_SA_AUDIT_OPTIONS 195
 DBA_SA_POLICIES 107
 DBA_SOURCE 50
 DBA_SYS_PRIVS 176
 DBA_TRIGGERS 143
 DBA_UPDATABLE_COLUMNS 64
 DBA_USERS 8, 9, 12, 48
 DBA-Rolle 57
 DBMS_APPLICATION_INFO 74
 DBMS_FGA 187, 190
 DBMS_OBFUSCATION_TOOLKIT 146
 DBMS_RLS 75
 DBMS_SESSION 72
 DBMS_SESSION.IS_ROLE_ENABLED 49, 57
 DBMS_SESSION.SET_ROLE 51

dd 138
DEFAULT_ADMIN_CONTEXT 29
Default-Passwörter 5
Definer's Rights Prozedur 69
DELETE_CONTROL (OLS) 96
DELETE_POLICY_GROUP 81
DELETE-Privileg 60
DES 130, 146
Diffie-Hellman Authentisierung 126
Digitales Zertifikat 23
DISABLE_POLICY 77
Distinguished Name 14, 22, 126
DIT 26
DMZ 2
DN 14, 26 *siehe auch Distinguished name*
der Datenbank 38
DROP_POLICY 77
DYNAMIC (Policy) 77
dynamische WHERE-Klausel (FGAC) 75

E

ENABLE_POLICY 77
ENCRYPT USING-Klausel 137
ENCRYPTION_SERVER 121
ENCRYPTION_TYPES_SERVER 121
ENCRYPTION_WALLET_LOCATION 135
Enterprise Domain 34
Enterprise Security Manager 34, 56
EXECUTE_CATALOG_ROLE 190
EXECUTE-Privileg 60, 68, 77, 87, 194
EXECUTE-Privileg (FGA) 190
EXEMPT ACCESS POLICY 101
expdp 144
EXTERNAL (PASSWORD-Eintrag im Data
Dictionary) 12, 13

F

FAILED_LOGIN_ATTEMPTS 15
FGA_LOG\$ 167, 187, 193
Firewall 3
Flashback (und FGA) 189
FOR UPDATE-Option 65
FULL-Privileg (OLS) 100

G

getAnyTaggedProxyConnection() 23
getProxyConnection() 22
GLOBAL (PASSWORD-Eintrag im Data
Dictionary) 12
GLOBAL_NAMES 42
Globale Benutzer 33
siehe auch Globales Schema
Globales Schema 33
GRANT 55, 56, 58, 60, 116
GRANT ANY OBJECT PRIVILEGE 60
GRANT ANY PRIVILEGE 59
GRANT CONNECT THROUGH 21, 51, 54
GRANT CONNECT THROUGH ENTERPRISE
USERS 22, 40
Groß- oder Kleinschreibung in OID 17
Groß- und Kleinschreibung (Client Identifier) 74
Groß- und Kleinschreibung (TDE) 136
Group (OLS) 90

H

Hashwert (DBMS_CRYPT) 149
Hashwert (für Passwortspeicherung) 150
Hashwert (Passwort) 8, 11
Hidden Column 86, 93
Historisierung von Daten 163
HTTP 20
HTTPS 117

I

IDENTIFIED EXTERNALLY 13, 55, 71
IDENTIFIED GLOBALLY 34, 71
IDENTIFIED USING 51
Identität 28
impdp 145
INDEX-Option (FGAC) 77
INSERT_CONTROL (OLS) 96
INSERT-Privileg 60, 69
IP_ADDRESS 71
IP-Sperre (OID) 114
IT-Grundschriftzhandbuch 198

J

JDBC Proxy-Verbindung 54

K

Kerberos 28

Key-preserved 64

Kryptographie 116

L

Label Based Access Control 86

LABEL_DEFAULT (OLS) 96, 98, 102, 103

LABEL_UPDATE (OLS) 97

LABEL_UPDATE-Privileg (OLS) 100

LBAC_DBA-Rolle 87

LBACSYS 84, 107

LDAP 26

ldap.ora 28

LDAP_DIRECTORY_ACCESS 31

ldapbind 38

Level (OLS) 88

LINK\$ 8, 116

LIST_CONTEXT 73

listener.ora 110, 123

Loopback (Datenbank-Link) 43

M

MAC 150

Man-In-The-Middle-Angriff 127

Master Key 134, 135, 142, 145

MERGE 173

MERGE_Privileg 60

Message Authentication Code 150

siehe auch MAC

mkstore 18

N

Nachteile von Passwörtern 3

Namensbereich (Applikationskontext) 70

NCSC C2 166

NLS_LANG 148, 149

NO_CONTROL (OLS) 97

NOAUDIT 164, 178

O

OCA 124, 136

OCA 25

siehe auch Oracle Certification Authority

OCIAttrSet() 22, 71

Offline Backup 152, 154

OID 14, 26, 38, 55

OID (SSL-Konfiguration) 37

oiddas 34

OLS-Administrator 87

OLS Label 85

OLS-Policy 85

Online Backup 152

ON-LOGON-Trigger 52, 54, 73

ON-LOGON-Trigger (OLS) 97

OPS\$-User 14

ORA-00942 62, 68

ORA-00956 176

ORA-01017 186

ORA-01045 59

ORA-01718 178

ORA-01733 63

ORA-01956 55

ORA-02003 71

ORA-06553 150

ORA-12401 103

ORA-1403 139

ORA-1920 6

ORA-28000 48

ORA-28001 15

ORA-28003 16

ORA-28112 192

ORA-28168 51

ORA-28338 137

ORA-28365 143

ORA-28368 136

ORA-39173 145

ORACLE

SECURITY.PASSWORD 30

Oracle Certification Authority 25

Oracle Directory Manager 26

oracle.net.crypto_checksum_client (JDBC Thin)

128

oracle.net.crypto_checksum_types_client
(JDBC Thin) 128
oracle.net.encrypted_client (JDBC Thin) 122
oracle.net.encrypted_types_client (JDBC Thin)
122
ORACLE.SECURITY.DN 30
OracleContext (OID) 33
OS_AUTHENT_PREFIX 14
OS_ROLES 55

P

Padding 148
Password Checker 9
PASSWORD EXPIRE 15
PASSWORD_LIFE_TIME 15
PASSWORD_REUSE_MAX 15
PASSWORD_REUSE_TIME 15
PASSWORD-Kommando (SQL*Plus) 115
PASSWORD-Spalte im Data Dictionary 10, 12
Passwort-Mindestanforderungen 3, 11
PIN 3
PKCS#10 26
PKCS#12 24
PKCS#5 148
PL/SQL Wrapper 50
Policy-Gruppe SYS_DEFAULT 80
Prädikat (OLS) 104
Privileg 46
PROFILE_ACCESS-Privileg (OLS) 99
PROXY_USERS 54

Prüfspur 164, 172, 179
Prüfspur (absichern) 179
Public-Key-Verschlüsselung 117
Purity Level 76

R

RA 25
RC4 119
RDBMS_SERVER_DN 31
READ_CONTROL (OLS) 96, 104
READ-Privileg (OLS) 100, 105
Realm 28

Registration Authority 25 *siehe auch RA*
REMOTE_OS_AUTHENT 14
RESOURCE-Rolle 57
REVOKE 55
RMAN 152
ROLE_ROLE_PRIVS 48, 57
ROLE_SYS_PRIVS 49, 57
ROLE_TAB_PRIVS 49, 57

S

SA_AUDIT_ADMIN 194
SA_COMPONENTS 90
SA_LABEL_ADMIN 91
SA_POLICY_ADMIN 93
SA_SESSION 99
SA_SYSDBA 87, 91
SA_USER_ADMIN 98
SA_USER_NAME 99
SALT 137, 141
Schattentabelle 67, 163
Schnelles Erzeugen großer Datenmengen 141
SCOTT 48
SEC_RELEVANT_COLS 79
SEC_RELEVANT_COLS_OPT 80
Secure Access 86
secure application role 51
secure external password store 17
SELECT_CATALOG_ROLE 107
SES_ACTIONS (Audit) 181
Session Pooling 70
SESSION REC 180
SESSION_CONTEXT 73
SESSION_ROLES 49, 57
SESSION_SCHEMA 71
SET ENCRYPTION (RMAN) 154, 155
SET ROLE 49, 50
SET_ACCESS_PROFILE 99
SET_CLIENT_INFO 74
SET_COMPARTMENTS 98, 99
SET_CONTEXT 72
SET_DEFAULT_LABELS 99
SET_GROUPS 98, 99
SET_IDENTIFIER 72, 74

- SET_PROG_PRIVS 106
 SET_ROW_LABEL 102
 SET_USER_LABELS 98
 SET_USER_PRIVS 99
 SGA 110
 Shared Schema 33, 56
 SHARED_CONTEXT_SENSITIVE (Policy) 78
 SHARED_STATIC (Policy) 78
 SHOW_ENCRYPTION (RMAN) 156
 Sichtbarmachen der Policy-Spalte (OLS) 94
 Speicherort für die Prüfspur 165
 SQL*Net 110
 SQL*Net Alias 110
 SQL-Befehle 66
 SQLNET.CRYPTO_SEED 121
 SQLNET.ENCRYPTION_SERVER 121
 SQLNET.ENCRYPTION_TYPES_SERVER
 121
 sqlnet.ora 110, 113, 121, 128, 129, 135
 SSL 37, 123
 SSL Cipher Suite 125
 SSL_CIPHER_SUITES 129
 SSL_CLIENT_AUTHENTICATION 126
 SSL_SERVER_CERT_DN 126
 SSO 4
 Standardport (SQL*Net) 124
 Standardverzeichnis (Wallet) 18
 StatelessConnectionPool 23
 STATIC (Policy) 77
 SYS 47
 SYS_CONTEXT 52, 53, 70, 74, 75
 SYS_CONTEXT (Performance) 78
 SYSDBA 59, 176, 184
 SYSMAN 48
 SYSOPER 59
 SYSTEM 47
 System Global Area 110 *siehe auch SGA*
 SYSTEM_PRIVILEGE_MAP 58, 175
- T**
- TABLE_PRIVILEGE_MAP 60
 TCP.VALIDNODE_CHECKING 113
 TCPS 123
 TDE 134
 TERMINAL 71
 Test auf lokalen Datenbankservers 52, 104
 Test auf Zeitraum 8 - 18 Uhr 58
 Test auf Zeitraum Montag bis Freitag (OLS) 105
 TLS 37, 123
 TNS_ADMIN 120, 135
 tnsnames.ora 110, 126
 TO_DATA_LABEL 92
 TO_LBAC_DATA_LABEL 102
 TRACE_DIRECTORY_CLIENT 129
 TRACE_FILE_CLIENT 129
 TRACE_LEVEL_CLIENT 129
 TRACE_TIMESTAMP_CLIENT 129
 TRACE_UNIQUE_CLIENT 129
 Transparent Data Encryption 134
 siehe auch TDE
 TRUNCATE TABLE 177
 Trusted Oracle 84
 Two-Task-Architektur 110
- U**
- UNLIMITED TABLESPACE 57
 UPDATE_CONTROL (OLS) 96
 UPDATE-Privileg 60
 US7ASCII 148
 USER (Pseudospalte) 162
 USER_AUDIT_POLICY_COLUMNS 192
 USER_AUDIT_TRAIL 183
 USER_DUMP_DEST 192
 USER_ENCRYPTED_COLUMNS 143
 USER_POLICIES 81
 USER_POLICY_CONTEXTS 81
 USER_POLICY_GROUPS 81
 USER_ROLE_PRIVS 48, 57
 USER_SA_SESSION 107
 USER_UPDATABLE_COLUMNS 64
 USERENV 70
 UTL_FILE 159
 UTL_FILE_DIR 159
 UTL_I18N 147
 UTL_MAIL 191
 UTL_RAW 146

V

v\$parameter 182
V\$RMAN_CONFIGURATION 156
V\$RMAN_ENCRYPTION_ALGORITHMS
152, 156
V\$SESSION 5, 74
V\$VPD_POLICY 81
V\$XML_AUDIT_TRAIL 183, 193
VVALIDNODE_CHECKING 113
Verschlüsselung von Oracle-Datenbankdateien
133
Verstecken der Policy-Spalte (OLS) 94

W

Wallet 124
mit automatischer Anmeldung 143, 153
neu anlegen (Passwort vergessen) 32

Wallet (Standardverzeichnis) 18
siehe auch Standardverzeichnis (Wallet)
Wallet Manager 24
WALLET_LOCATION 18, 30, 39, 124, 125,
135, 136
WALLET_OVERRIDE 18
WE8ISO8859P1 148
WITH READ ONLY 63
WRITE_CONTROL (OLS) 96
WRITEACROSS-Privileg (OLS) 100
WRITEDOWN-Privileg (OLS) 100
WRITEUP-Privileg (OLS) 100

X

X509v3 24

Z

Zertifikat 23