

HANSER

Oracle Security in der Praxis

Sicherheit für Ihre Oracle-Datenbank

ISBN 3-446-40436-8

Inhaltsverzeichnis

Weitere Informationen oder Bestellungen unter
<http://www.hanser.de/3-446-40436-8> sowie im Buchhandel

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