



ORACLE Oracle 数据库技术丛书(1)

ORACLE 8.1.6

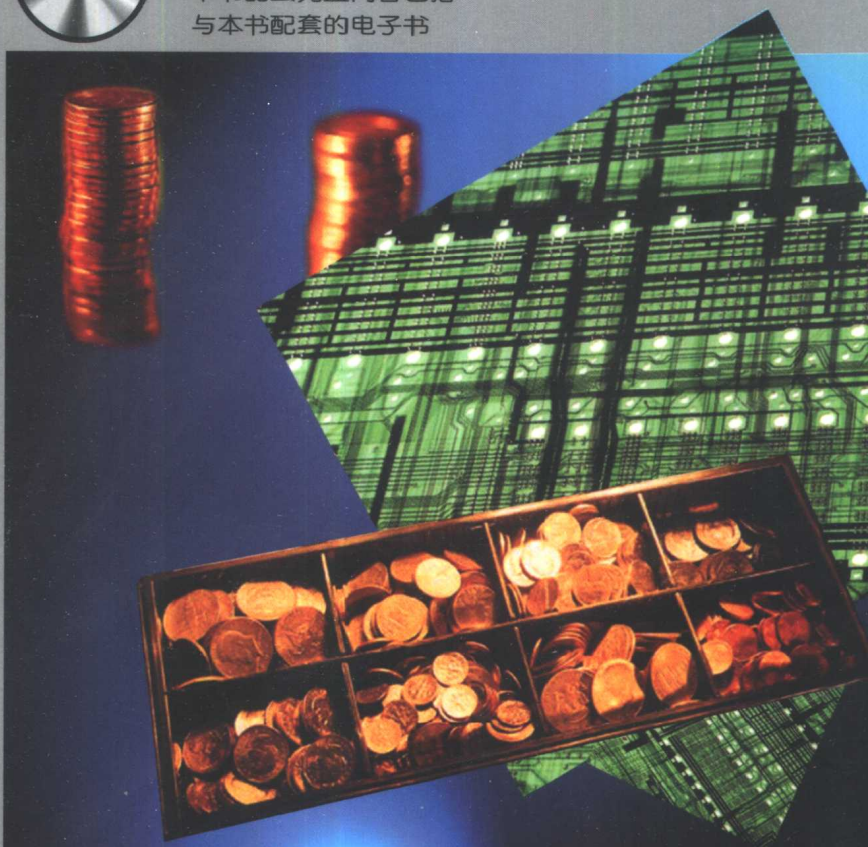
Administrator's Guide

管理员指南

本丛书编委会 主编



本书配套光盘内容包括：
与本书配套的电子书



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn



ORACLE Oracle 数据库技术丛书(1)

ORACLE 8.1.6

Administrator's Guide

管理员指南

本丛书编委会 主编



本书配套光盘内容包括：
与本书配套的电子书



988039



北京希望电子出版社
Beijing Hope Electronic Press
www.bhp.com.cn

内 容 简 介

本书是“Oracle 数据库技术丛书”之一，全套书共 5 册。本书全面讲述了基本的 Oracle 数据库管理、配置以及存储，数据库的安全和资源管理等知识。

全书共分 6 个部分。第一部分：基本的数据库管理，其中包括 Oracle 8i 数据库管理员的典型任务，Oracle 8i 数据库的启动、创建和关闭；第二部分：数据库的配置，其中讲述了过程、控制文件、重复日志以及作业序列的管理；第三部分是数据库存储；第四部分：规划对象，内容包括表、索引、簇以及模式对象的管理；第五部分：数据库的安全，讲述了安全策略的建立、用户与资源的管理以及审计数据库的使用；第六部分：数据库资源管理，描述了如何使用数据库资源管理器分配资源。

本书内容全面、系统，由浅入深，既可以作为数据库管理员、应用程序管理员的参考书，也可以作为高等院校相关专业教学、自学用教材以及社会各种 Oracle 系统培训用教材。

本书光盘内容包括与本书配套的电子书。

- 系 列 名： Oracle 数据库技术丛书（1）
书 名： Oracle 8.1.6 管理员指南
文 本 著 者： 本丛书编委会 编写
C D 制 作 者： 希望多媒体创作中心
C D 测 试 者： 希望多媒体测试部
责 任 编 辑： 柴文强 郑明红 周 艳 郭淑珍
出版、发行者： 北京希望电子出版社
地 址： 北京海淀路 82 号 100080
网址： www.bhp.com.cn E-mail: lwm@hope.com.cn
电话： 010-62562329,62541992,62637101,62637102,62633308,62633309
(发行和技术支持)
010-62613322-215 (门市) 010-62531267 (编辑部)
- 经 销： 各地新华书店、软件连锁店
- 排 版： 希望图书输出中心
C D 生 产 者： 北京中新联光盘有限责任公司
文 本 印 刷 者： 北京广益印刷厂
规 格 / 开 本： 787×1092 1/16 开本 23.125 印张 527 千字
版 次 / 印 次： 2000 年 10 月第 1 版 2000 年 10 月第 1 次印刷
印 数： 0001~5000 册
本 版 号： ISBN 7-900044-93-0/TP·93
定 价： 50.00 元(1CD, 含配套书)

说明：凡我社图书及其配套光盘若有缺页、倒页、脱页、自然破损，本社负责调换。

Oracle 数据库技术丛书

编委会名单

主 编：奥克拉·马尔

副主编：夏尔·杰克 本杰明·卡里基 沈 鸿

编 委：(按姓氏笔划排序)

纪 红 刘大伟 刘晓融 海尔默·劳尔

基尔斯腾·扬 陆卫民 张长富 陈河南

卡里亚诺夫·波尔加 柯里奇·金巴

徐建华 袁勤勇 帕金斯·赫尔墨斯

本书执笔人：袁勤勇 邓静 李学群等

序

Oracle 系统以其先进的数据库、服务器、企业商务应用技术和丰富的应用开发与决策支持工具，以及针对设计、开发、客户三方的电子商务解决方案和 Internet 应用，在国内企事业单位、科研院校得到广泛应用。为满足 Oracle 技术的深入应用所带来的对技术资料的要求，我们与国内外有关专家共同组织编写了《Oracle 数据库技术丛书》。全套书共 5 册，全面反映了 Oracle 最新技术和应用。它们分别如下：

(1)《Oracle 8.1.6 管理员指南》：全面讲述了 Oracle 数据库基本管理、配置、存储、数据库的安全和资源管理等知识。

本书共分 6 个部分。第一部分“基本的数据库管理”，其中包括 Oracle 8i 数据库管理员的典型任务，Oracle 8i 数据库的启动、创建和关闭；第二部分“数据库的配置”，其中讲述了过程、控制文件、重复制日志以及作业序列的管理；第三部分介绍数据库存储；第四部分“规划对象”，内容包括表、索引、簇以及模式对象的管理；第五部分“数据库安全”，讲述了安全策略的建立、用户与资源的管理以及审计数据库的使用；第六部分“数据库资源管理”，描述了如何使用数据库资源管理器分配资源。

(2)《Oracle 8.1.6 系统安全与网络管理指南》：主要讲述了 Oracle 的高级网络安全特性。

本书共分两篇。第一篇“Oracle 高级安全管理指南”，分为四个部分，全面详细介绍了关于 Oracle 8i 数据库平台高级安全特性的相关机制。内容主要涵盖 Oracle 高级安全特性、Oracle 分布式计算环境 (DCE) 集成和 Oracle 安全/目录集成等主题共计 20 章，以及 6 个附录。第一部分介绍 Oracle 高级安全特性，第二部分介绍 Oracle DCE 集成，第三部分介绍 Oracle 8i 安全/目录集成，第四部分是附录及一个词汇表。本书第二篇“Oracle Net8 管理指南”，讲述了 Net8 的使用以及如何利用 Net8 来配置 Oracle 的高级安全特性。该篇分四个部分，共计 12 章和一个附录。主要内容包括：Net8 简介，Net8 概念，Net8 体系结构，Net8 产品和工具，规划网络、配置命名方法，配置监听者，配置多线程服务器，打开 Net8 程序员增强特性，建立连接和测试网络、问题解决和控制实用程序。通过本书的学习，读者可以熟练掌握 Oracle 高级安全特性的配置和管理。

(3)《Oracle 8.1.6 核心管理技术大全》：全面系统地介绍了 Oracle 8i 数据仓库技术的基本知识和使用方法，Oracle WebDB 的使用环境以及它在建立应用程序和创建 Oracle Web 站点两个方面的应用，并对如何管理和使用 Oracle 分布式数据库系统进行了详细描述。

本书由三篇构成。第一篇“Oracle 8i 数据仓库技术”，共分 5 个部分。第一部分介绍了数据仓库的基本概念；第二部分讨论了有关数据仓库的逻辑设计问题；第三部分讲述了有关数据仓库的物理设计问题；第四部分描述了处理管理数据仓库的任务，包括 ETT（提取、传输、转换）以及装载和刷新；第五部分讨论了有关提高数据仓库性能的方法，包括模式、SQL 分析、调整并行执行以及查询重写等，并在本篇最后给出了一个中英文对照的术语表。第二篇“Oracle 8i 分布式数据库系统”，由 3 部分组成。第一部分介绍了分布式数据库的基本概念，同时说明了 Oracle 分布式数据库系统的特点和用法，以及如何管理、开发分布式数据库系统应用程序的方法和途径；第二部分阐述了分布式事务、两阶段提交的实现和分布式事务的管理；第三部分描述了异构分布式事务的概念和管理方法。第三篇“Oracle Web 数据库应用”由 4 部分构成，第一部分详细介绍了建立应用程序所涉及的各个环节，包括如何创建新的用户和角色，如何在数据库中建立各种数据库对象以及如何创建组件等；第二部分分别叙述了 WebDB 站点的有关创建、设计和管理方面的问题，包括如何利用各种向导和导航条进行操作，如何控制用户对站点中各种文

件夹的访问；第三部分主要讨论了如何控制用户对报表的访问，包括对报表服务器和打印机的访问；第四部分附录说明了完成本篇练习的前提。

(4)《Oracle 8.1.6 开发指南》：主要介绍了 Oracle 8i 数据库性能设计与优化，以及数据库管理的备份和恢复技术。

本书由两篇构成。第一篇“Oracle 8i 性能设计与优化”分 4 部分共 24 章。第一部分“性能优化知识”，包括理解 Oracle 性能优化，性能优化方法两章；第二部分“设计人员和开发人员的应用程序设计优化技术”，包括应用程序和系统性特性，优化性能，EXPLAIN PLAN 使用说明，SQL Trace 和 TKPROF 使用说明，优化程序提示使用说明，收集统计信息，优化 SQL 语句和 Plain Stability 使用说明等七章；第三部分“设计人员和 DBA 应用程序工具”，包括诊断工具概述，数据访问方法，管理共享 SQL 和 PL/SQL 区域，Oracle Trace 使用说明，动态性能视图，诊断系统性能故障和事务模式等六章；第四部分“优化实例性能”，包括优化 CPU 资源，优化内存分配，优化 I/O，优化资源争用，优化网络，优化操作系统和优化实例恢复性能等七章。本篇内容丰富，涵盖了大型数据库性能设计与优化中的大部分内容，具有很强的启发性，可谓既有广度，又有相当的深度。第二篇“Oracle 8i 的备份与恢复”分两部分共 7 章。第一部分“开发备份和恢复战略”，包括备份和恢复概述，管理数据结构和开发备份和恢复战略等三章；第二部分“实施操作系统备份和恢复”，包括实施操作系统备份，实施介质管理，介质管理实例，实施操作系统表空间的时间点恢复共四章。本篇详细讲述了 Oracle 8i 数据库的备份和恢复的方方面面，内容全面、新颖，结构清晰，示例丰富翔实，实用性很强，是广大用户掌握大型数据库系统理论和实践的首选用书。

(5)《Oracle 8.1.6 应用系统使用指南》：由“Oracle 销售分析系统管理指南”和“Oracle 现金管理系统应用”两篇组成，介绍了 Oracle 的两个应用系统。

本书第一篇阐述了 Oracle 销售分析器的基本概念、安装方法及其性能。该篇由 14 章和两个附录组成，内容包括：Oracle 销售分析器介绍，管理员的职责，分析器的安装，构造数据库及片断，使用 Express 数据库和分类，建立客户访问、Web 访问、数据库安全机制，为客户访问建立通信，限定对数据库的访问范围，定制数据库、客户端界面，以及控制数据显示等，附录给出了分类描述和初始化文件描述。第二篇讨论了一个 Oracle 财务管理软件的应用，共分 6 章，旨在指导读者如何更有效地使用“Oracle 现金管理系统”软件。内容包括：现金管理系统过程的概述，现金管理系统设置，加载银行报告书，调节银行报告书，现金预测，查询和报表等；附录 A、B、C 列出了关于导航路径、简述选项和功能安全性等信息。

本丛书内容全面新颖，结构清晰，叙述详细，事例翔实，技术内涵高，指导性强，既可以作为 Oracle 数据库系统管理员、网络安全管理员、应用与开发人员、维护和技术支持人员必备的技术指导书，也可以作为高等院校相关专业教学、自学用教材和社会各种 Oracle 系统培训用教材。

我们特别感谢美国伯克利大学计算机系奥克拉·马尔教授，Oracle 加拿大研究中心高级研究员夏尔·杰克教授和美国卡内基梅隆大学计算机系本杰明·卡里基教授，本丛书就是在他们的大力帮助和协调下才得以完成。感谢 Oracle 美国研究中心高级研究员海尔默·劳尔教授、卡内基梅隆大学计算机系基尔斯腾·扬教授、Oracle 公司数据仓库专家卡里亚诺夫·波尔加博士、美国麻省理工大学计算机系帕金斯·赫尔墨斯教授和柯里奇·金巴教授，由于他们的技术指导和全力参与，本丛书才得以及时完稿。真诚感谢参与本丛书编写的全体专家和技术人员，是他们的积极配合和努力，才使本丛书如期付梓出版。最后，向本丛书的读者表示诚挚的谢意，感谢你们的相知。

Oracle 数据库技术丛书编委会

2000 年 8 月 15 日

目 录

第一部分 基本数据库管理

1 Oracle 数据库管理员	1
1.1 Oracle 用户的类型	1
1.2 数据库管理安全性和权限	3
1.3 数据库管理员认证	4
1.4 密码文件管理	6
1.5 数据库管理员实用程序	11
1.6 数据库管理员的优先权	11
1.7 区别 Oracle 数据库软件版本	14
2 创建 Oracle 数据库	16
2.1 创建数据库之前应考虑的事项	16
2.2 Oracle 数据库配置助理(DBCA)	18
2.3 手工创建 Oracle 数据库	21
2.4 安装参数	26
2.5 数据库创建之后应考虑的事项	32
2.6 初始化调整指导	33
3 启动与关闭	34
3.1 启动数据库	34
3.2 更改数据库的可用性	38
3.3 关闭数据库	39
3.4 挂起和继续执行数据库	41
3.5 使用初始化参数文件	42

第二部分 Oracle 服务器配置

4 管理 Oracle 进程	44
4.1 服务器进程	44
4.2 配置多线程服务器的 Oracle	47
4.3 跟踪 Oracle 后台进程	50
4.4 管理并行查询选项的进程	54
4.5 管理外部应用程序的进程	55
4.6 结束会话	57

5 管理控制文件	59
----------------	----

5.1 什么是控制文件	59
5.2 控制文件指南	59
5.3 创建控制文件	60
5.4 创建控制文件之后的故障排除	63
5.5 删除控制文件	64
6 管理联机重做日志	65
6.1 什么是联机重做日志	65
6.2 规划联机重做日志	67
6.3 创建联机重做日志组和成员	71
6.4 联机重做日志的重命名和重定位	72
6.5 删除联机重做日志组和成员	73
6.6 强制日志切换	75
6.7 校验重做日志文件中的块	75
6.8 清除联机重做日志文件	75
6.9 列出关于联机重做日志的信息	76
7 管理存档重做日志	77
7.1 什么是存档重做日志	77
7.2 在存档日志和非存档日志之间选择	78
7.3 控制存档模式	80
7.4 确定存档目标	83
7.5 指定日志传输模式	85
7.6 管理存档目标失败	87
7.7 调整存档性能	89
7.8 显示存档重做日志信息	91
7.9 控制由存档日志程序产生的踪迹 输出	92
7.10 使用日志采集器来分析联机重做 日志和存档重做日志	93
8 管理作业队列	101
8.1 SNP 后台进程	101
8.2 管理作业队列	102
8.3 查看作业队列信息	109

第三部分 数据库存储

9 表空间管理	111
9.1 表空间管理的指南	111
9.2 创建表空间	112
9.3 管理表空间的地址分配	117
9.4 改变表空间的工作效率	120
9.5 只读表空间	121
9.6 删除表空间	125
9.7 使用 DBMS_SPACE_ADMIN 程序包	125
9.8 在数据库之间移动表空间	127
9.9 查看表空间信息	136
10 管理数据文件	139
10.1 管理数据文件的方针	139
10.2 向一个表空间创建和增加数据 文件	141
10.3 变更数据文件的尺寸	141
10.4 改变数据文件的可用性	143
10.5 重命名和重新部署数据文件	144
10.6 校验数据文件中的数据块	146
10.7 查看数据文件的相关信息	146
11 管理回退段	148
11.1 管理回退段的方针	148
11.2 创建回退段	151
11.3 改变回退段	152
11.4 明确地给回退段分派事务处理	155
11.5 删除回退段	155
11.6 监视回退段信息	155

第四部分 模式对象

12 模式对象管理指南	158
12.1 管理数据块的空间	158
12.2 事务项设置 (INITRANS 和 MAXTRANS 参数)	162
12.3 设置储存参数	162
12.4 释放空间	166
12.5 了解数据类型的空间使用	169
13 管理数据表	170
13.1 管理数据表的方针	170

13.2 创建表	175
13.3 改变表	176
13.4 删除表	179
13.5 索引管理表	180
14 管理索引	187
14.1 索引管理指南	187
14.2 创建索引	191
14.3 改变索引	195
14.4 监视索引的空间使用	195
14.5 删除索引	196
15 管理分区数据表和索引	197
15.1 什么是分区的表和索引	197
15.2 分区方法	197
15.3 创建分区	200
15.4 维护分区	203
15.5 分区表和索引实例	218
16 管理簇	221
16.1 管理簇指南 7	221
16.2 创建簇	224
16.3 改变簇	225
16.4 删除簇	226
17 管理散列簇	228
17.1 是否应该使用散列簇	228
17.2 创建散列簇	229
17.3 改变散列簇	232
17.4 删除散列簇	233
18 管理视图、序列和别名单元	234
18.1 管理视图	234
18.2 管理序列	241
18.3 管理别名单元	242
19 模式对象的常规管理	244
19.1 在单一操作中创建多表和 多视图	244
19.2 模式对象重命名	245
19.3 分析表、视图和簇	245
19.4 截断表和簇	250
19.5 启用和禁用触发器	251
19.6 管理完整性约束	252
19.7 管理对象相关性	258

19.8	管理对象名称解析.....	260
19.9	为数据字典改变存储参数.....	260
19.10	显示有关模式对象的信息.....	262
20	解决数据块讹误的问题.....	267
20.1	修正数据块讹误的选项.....	267
20.2	关于 DBMS_REPAIR 程序包.....	267
20.3	使用 DBMS_REPAIR 程序包.....	268
20.4	DBMS_REPAIR 示例.....	271

第五部分 数据库安全

21	建立安全策略.....	277
21.1	系统安全策略.....	277
21.2	数据安全策略 (Data Security Policy).....	278
21.3	用户安全策略.....	279
21.4	口令管理策略 (Password Management Policy).....	284
21.5	审计策略.....	289
22	用户和资源管理.....	290
22.1	会话和用户许可.....	290
22.2	用户身份验证.....	294
22.3	Oracle 用户.....	298
22.4	使用概要文件管理资源.....	302
22.5	列举数据库用户和 PROFILE 的相关信息.....	305
22.6	示例.....	309

23	用户权限管理和角色管理.....	310
23.1	识别用户权限.....	310
23.2	管理用户角色.....	311
23.3	授权用户权限和角色.....	315
23.4	取消用户权限和角色.....	317
23.5	授予权限和取消权限何时生效.....	320
23.6	运用操作系统或运用网络授权.....	321
23.7	权限和角色信息列表.....	323
24	数据库使用审计.....	327
24.1	审计准则.....	327
24.2	创建和删除数据库审计踪迹试图.....	328
24.3	管理审计踪迹信息.....	329
24.4	查看数据库审计踪迹信息.....	336
24.5	通过数据库触发器进行审计.....	339

第六部分 数据库资源管理

25	数据库资源管理器.....	341
25.1	什么是数据库资源管理器.....	341
25.2	管理数据库资源管理器.....	342
25.3	创建和管理资源规划.....	344
25.4	管理资源用户组.....	350
25.5	启用数据库资源管理器.....	352
25.6	举例.....	352
25.7	数据库资源管理器视图.....	355

第一部分 基本数据库管理

第一部分介绍数据库管理职责的概况，并描述了数据库的创建，以及怎样启动和关闭数据库事例。它包含下列三章：

- 第1章“Oracle 数据库管理员”
- 第2章“创建 Oracle 数据库”
- 第3章“启动和关闭”

1 Oracle 数据库管理员

本章描述管理 Oracle 服务器的人——数据库管理员的职责。

包括下列专题：

- Oracle 用户类型
- 数据库管理员的安全性和权限
- 数据库管理员授权
- 密码文件管理
- 数据库管理员实用程序
- 数据库管理员的优先级
- 标识 Oracle 数据库软件版本

1.1 Oracle 用户的类型

在用户站点，用户类型及其职责可能不同。例如，在一个大型站点上，数据库管理员的职责可以分给几个人。

本节包括下列专题：

- 数据库管理员
- 安全官员
- 应用程序开发人员
- 应用程序管理员
- 数据库用户
- 网络管理员

1.1.1 数据库管理员

因为 Oracle 数据库系统可以非常大，且拥有很多用户，所以必须有人或有一组人管理系统。数据库管理员（DBA）就是这样的管理人员。每一个数据库至少需要一个人来承担



管理职责。

数据库管理员的职责包括：

- 安装并更新 Oracle 服务器和应用程序工具。
- 分配系统存储，为数据库系统规划将来的存储需求。
- 在应用程序开发人员设计了应用程序以后，创建主数据库存储结构（表空间）。
- 一旦应用程序开发人员完成应用程序的设计以后，创建主对象（表、视图、索引）。
- 必要时，根据应用程序开发人员所给的信息，修改数据库结构。
- 控制并监视用户对数据库的访问。
- 监视并优化数据库性能。
- 计划数据库信息的备份和性质。
- 在磁带上维护归档数据。
- 备份并恢复数据库。
- 与 Oracle 公司联系，寻求技术支持。

1.1.2 安全官员

在有些情况下，数据可能有一个或多个安全官员。安全官员主要从事下列工作：登记用户，控制并监视用户对数据的访问，维护系统安全性。如果你的站点有单独的安全官，你可以不负责这些职责。

1.1.3 应用程序开发人员

应用程序开发人员设计、实施数据库应用程序。应用程序开发人员的职责包括：

- 设计并开发数据库应用程序
- 为应用程序设计数据库结构
- 估计应用程序的存储需求
- 为应用程序规定数据库结构的修改
- 向数据库管理员传达上述信息
- 在开发过程中调整应用程序
- 在开发过程中建立应用程序的安全评价

1.1.4 应用程序管理员

一个 Oracle 系统也可能拥有一个或多个应用程序管理员。应用程序管理员负责特定应用程序的管理需求。

1.1.5 数据库用户

数据库用户通过应用程序或实用程序与数据库进行交互。用户职责通常包括：

- 在允许的地方，输入、修改、删除数据
- 生成数据报表

1.1.6 网络管理员

在一些系统中，也许有一个或多个网络管理员。网络管理员负责管理 Oracle 联网产品，

如 Net8。

参见 欲了解在一个分布式环境中网络管理的有关信息, 请参见“*Oracle8i Distributed Database Systems*”。

1.2 数据库管理安全性和权限

要在 Oracle 中完成管理任务, 用户需要数据库及其运行所在的服务器操作系统的额外权限。对数据库管理员的帐号的访问必须严格访问。

本节包括下列专题:

- 数据库管理员的操作系统帐号
- 数据库管理员用户名
- DBA 角色

1.2.1 数据库管理员的操作系统帐号

要完成数据库管理任务, 必须能够执行操作系统命令。取决于执行 Oracle 的操作系统, 数据库管理员可能需要操作系统帐号或 ID 来获取对操作系统的访问。这样, 数据库管理员的操作系统帐号可能需要比数据库用户更多的操作系统特权或访问权制。虽然数据库管理员不需要把 Oracle 文件存储在自己的帐号中, 但必须能访问这些文件。

参见 区分数据库管理员帐号的方法是操作系统专用的。详见有关操作系统专用的 Oracle 文档。

1.2.2 数据库管理员用户名

数据库自动创建两个用户帐号, 并为他们授予 DBA 角色。这两个用户帐号是:

- SYS (初始密码: CHANGE_ON_INSTALL)
- SYSTEM (初始密码: MANAGER)

下面几节中将介绍这两个用户名。

注意 要防止对数据字典表的不恰当的访问, 必须在创建 Oracle 数据后立即改变 SYS 和 SYSTEM 用户点的密码。

你也许至少要创建一个管理员用户, 用于完成日常的管理任务。

SYS

数据库新建时, 用户 SYS 自动创建, 并被授予 DBA 角色, 该用户由密码 CHANGE_ON_INSTALL 来标识。

数据库数据字典的所有基表和视图都存储在 SYS 模式中。这些基表和视图对于 Oracle 操作是至关重要的。要维护数据字典的一致性, SYS 模式中的表都只能由 Oracle 处理; 它们绝对不能由任何用户或数据库管理员进行修改, 任何人都不要在用户 SYS 的模式中创建任何表。但是, 如果有必要, 用户可以改变数据字典设置的存储参数。

大多数数据库绝对不应该用 SYS 帐号进行连接。用户可以使用 SYS 帐号连接到数据库, 但只能在 Oracle 技术人员或文档指导下才能进行。



SYSTEM

数据库创建时，用户 **SYSTEM** 也自动创建，并授予该数据库的所有系统特权，用户 **SYSTEM** 由密码 **MANAGER** 标识。

SYSTEM 用户创建显示管理信息的表和视图，以及 **Oracle** 工具使用的表和视图。绝对不要在 **SYSTEM** 模式中创建与单个用户有关的表。

1.2.3 DBA 角色

每个 **Oracle** 数据库都会自动创建命名为 **DBA** 的预定义角色。该角色包含所有数据库系统特权。因此，该角色功能强大，应该只授予全功能的数据库管理员。

1.3 数据库管理员认证

数据库管理员必须经常进行一些特殊操作，如关闭、启动数据库。因为这些操作不能由普通数据库用户实施，数据库管理员用户名需要更安全的认证机制。

本节包括下列专题：

- 选择认证方式
- 使用操作系统认证
- **OSOPER** 和 **OSDBA**
- 使用认证密码文件

1.3.1 选择认证方式

下列认证数据库管理员的方法取代 **Oracle** 老版本提供的 **CONNECT INTERNAL** 语法。为了支持向后兼容，**CONNECT INTERNAL** 继续使用。

- 操作系统认证
- 密码文件

根据用户是希望管理在数据库驻留的同一台机器的数据库，还是管理来自单个远程客户的多个不同数据库，用户可以在操作系统认证或密码文件之间进行选择，以认证数据库管理员。图 1-1 演示了数据库管理员认证模式。

在大多数操作系统上，数据库管理员的 **OS** 认证包括在特殊组中放置数据库管理员的 **OS** 用户名（在 **UNIX** 中是 **DBA** 组），或者给予 **OS** 用户名特殊的进程权力。

数据库使用密码文件来记录已授予管理员权限的数据库用户名。

参见 在 “*Oracle8i Concepts*” 中有关于用户认证的更多信息。

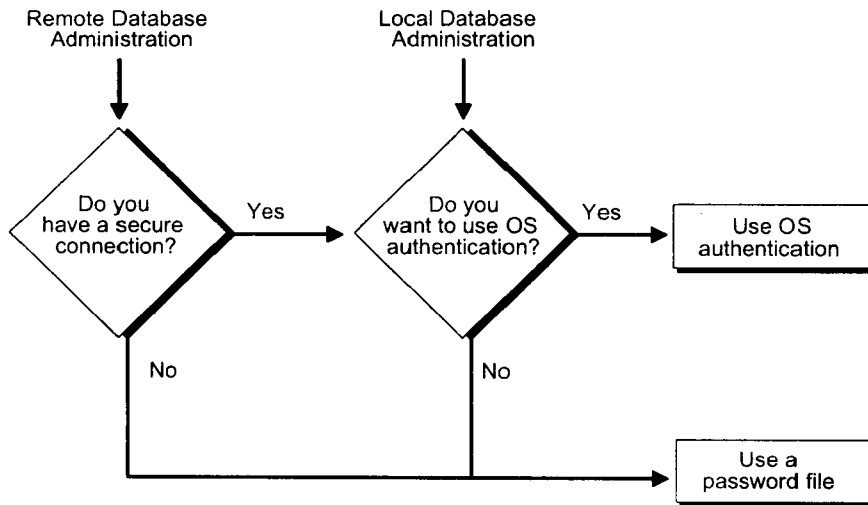


图 1-1 数据库管理员认证方法

1.3.2 使用操作系统认证

如果你选择操作系统认证，那么你可以使操作系统认证用户实施数据库管理操作。

1. 建立由操作系统认证的用户。
2. 确保初始参数 REMOTE-LOGIN-PASSIVORDFILE 设置为 NONE，NONE 是该参数的缺省值。
3. 通过键入下列 SQL* plus 命令中的一个，已认证用户应该能够连接到本地数据库，或通过安全连接，连接到一个远程数据库：

```
CONNECT /AS SYSOPER
CONNECT /AS SYSDBA
```

如果用户使用 Oracle 的老版本，以 INTERNAL 方式成功连接，那么用户应该能够使用在步骤 3 中的新语法继续连接。

注意 要使用 OS 认证，连接为 SYSOPER 或 SYSDBA，用户不必需要 SYSOPER 或 SYSDBA 系统特权。相反，服务器在操作系统级验证用户已经授予合适的 OSDBA 或 OSOPER 角色。

CONNECT 是 SQL*Plus 命令，欲了解有关其用法和句法的信息，可参见“*SQL*Plus User's Guide and Reference*”。

1.3.3 OSOPER 和 OSDBA

两个特殊的操作系统角色：OSOPER 和 OSDBA 控制着在使用操作系统认证时的数据库管理员的注册。

OSOPER 允许用户进行下列操作：STARTUP、SHUTDOWN、ALTER DATABASE OPEN/MOUNT、ALTER DATABASE BACKUP、ARCHIVE LOG 和 RECOVER，并包括 RESTRICTED SESSION 权限。



OSDBA 包含 ADMIN OPTION 的所有系统权限、OSOPER 角色；允许进行 CREATE DATABASE 和基于时间的恢复。

对于你所使用的操作系统，OSOPER 和 OSDBA 可以拥有不同的名字和功能。

OSOPER 和 OSDBA 角色只能通过操作系统授予用户。它们不能通过 GRANT 语句来授予，也不能取消或丢弃。当用户以管理员权限进行登录且 REMOTE-LOGIN-PASSWORDFILE 设置为 NONE 时，Oracle 与操作系统进行通信，试图首先启用 OSDBA，如果不成功，然后启用 OSOPER。如果这两个操作都失败，则连接失败。怎样通过操作系统授予这些权限是与操作系统相关的。

如果正在进行远程数据库管理，那么应该阅读 Net8 文档，来判断是否在使用安全连接。最普通的连接协议，如 TCP/IP 和 DECnet 是不安全的，不管你正在使用哪个 Net8 版本。

参见 欲了解有关数据库管理员的 OS 认证信息，请参见专门针对操作系统的 Oracle 文档。

1.3.4 使用密码文件认证

如果已经决定使用密码文件来认证进行数据库管理的用户，那么必须完成下面介绍的步骤。每一个步骤都将在本章中的后续几节中详细介绍。

1. 使用 ORAPWP 实用程序创建密码文件。

```
ORAPWD FILE=filename PASSWORD=Password ENTRIES=max-users
```

2. 把 REMOTE-LOGIN-PASSWORDFILE 初始化参数设置为 EXCLUSIVE。

3. 通过使用 SQL，为每个需要进行数据库管理的用户授予合适的权限，在密码文件中加入用户。下面是一个实例：

```
GRANT SYSDBA TO SCOTT;  
GRANT SYSOPER TO SCOTT;
```

SYSDBA 权限允许用户实施与 OSDBA 相同的操作。同样，SYSOPER 权限允许用户实施与 OSOPER 相同的操作。

4. 已授权的原用户现在应该能够通过使用类似于下面的命令连接到数据库。

```
CONNECT scott/tiger a acct.hq.com As SYSDBA
```

1.4 密码文件管理

可以使用密码文件创建实用程序 ORAPWD 来创建密码文件；或者，对于选定的操作系统，可以创建该文件，作为标准安装的一部分。

本节包括下列专题：

- 使用 ORAPWD
- 设置 REMOTE-LOGIN-PASSWORDFILE
- 在密码文件中加入用户
- 以管理员权限连接
- 维护密码文件

参见 参见专门针对操作系统的 Oracle 文档，以了解使用实用程序来安装密

码文件的信息。

1.4.1 使用 ORAPWD

如果调用密码文件创建实用程序，而不提供任何参数，那么系统将显示一则消息，表示该命令的正确用法如下面的样本输出。

```
orapwd
Usage: orapwd file=<fname> password=<password> entries=<users>
where
file - name of password file (mand),
password - password for SYS and INTERNAL (mand),
entries - maximum number of distinct DBAs and OPERs (opt),
There are no spaces around the equal-to (=) character.
```

例如，下面的命令创建名为 ACCT.PWD 的密码文件，该文件允许有 30 个不同密码的授权用户。该文件最初由以 SYSOPER 或 SYSDBA 连接的用户以密码 SECRET 来创建。

```
ORAPWD FILE=acct.pwd PASSWORD=secret ENTRIES=30
```

下面介绍 PRAPWD 实用程序的参数。

FILE (文件)

该参数设置欲创建的密码文件的名定。必须规定该文件的全路径名。该文件的内容是加密的，也就是用户不可读的。该参数是强制的。

密码文件所允许的文件名类型是与操作系统有关的。有些平台要求密码文件必须是特定格式，且位于特定目录中。其它平台允许使用环境变量来指定密码文件的名字和位置。欲了解在各种平台上允许的文件名和位置，请参见与操作系统相关的 Oracle 文档。

如果使用 Oracle Parallel Server，运行多个 Oracle 事例，那么每个事例的环境变量应该指向相同的密码文件。

警告 保护密码文件和标识密码文件位置的环境变量，这对于系统的安全性是非常重要的。拥有访问这些文件和变量的能力的用户，都潜在地威胁系统的安全性。

PASSWORD (密码)

该参数设置 SYSOPER 和 SYSDBA 的密码。如果在连接到数据库以后，你发出 ALTER USER 语句来改变密码，那么，存储在数据字典中的密码和存储在密码文件中的密码都被更新。仅仅是为了向下兼容，系统才支持 INTERNAL 用户。该参数是强制的。

ENTRIES (条目)

该参数指定密码文件接受的条目数。它对应于允许以 SYSDBA 或 SYSOPER 连接到数据库的不同用户的数量。可以输入的实际条目数可以稍高，因为 ORAPWD 实用程序将继续指定密码项，直到操作系统块填满。例如，如果操作系统块大小为 512 字节，它将容纳 4 个密码项，所分配的密码项数目将始终是 4 的倍数。

因为用户不断地从密码文件中加入并删除，所以文件中条目可以重新使用。如果你希望指定 REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE，并允许给用户授予 SYSOPER 和 SYSDBA 权限，那么该参数是必需的。



警告 当用户超出这个权制时，用户必须创建一个新的密码文件。要避免这种情况的发生，应该选择一个比自己想像的更大的数字。

1.4.2 设置 REMOTE_LOGIN_PASSWORDFILE

除了创建密码文件以外，还必须把初始参数 REMOTE_LOGIN_PASSWORDFILE 设置为合适的值。可识别的值在下面介绍。

注意 要启动一个数据事例，你必须指定数据库名字和参数文件，来初始化事例设置。用户可以使用 Nets 指定一个全限定的远程数据库名字。但是，初始化参数文件和任何相关的文件，例如配置文件都必须存在于客户机上。也就是，参数文件必须位于用户启动事例所在的机器。

NONE

把参数设置为 NONE，将导致 Oracle 的行为好象密码文件不存在。即，通过不安全的连接，不允许有授权的连接。NONE 是该参数的缺省值。

EXCLUSIVE

EXCLUSIVE 密码文件只能用于一个数据库。只有 EXCLUSIVE 文件能包含不同于 SYSOPER 和 SYSDBA 的用户名，使用 EXCLUSIVE 密码文件，允许你为单个用户授予 SYSDBA 和 SYSOPER 系统特权，并让用户以他们自身进行连接。

SHARED

SHARED 密码文件可以用于多个数据库。但是，SHARED 密码文件只能识别 SYSDBA 和 SYSOPER 用户；你不能在 SHARED 密码文件中加入用户。所有需要 SYSDBA 和 SYSOPER 权限的用户必须使用相同的名字 SYS 和密码进行连接。如果要让单个 DBA 管理多个数据库，那么该选项非常有用。

建议 要达到最高的安全级，你应该在创建密码文件以后立即把 REMOTE_LOGIN_PASSWORDFILE 文件初始化参数设置为 EXCLUSIVE。

1.4.3 在密码文件中加入用户

当你为用户授予 SYSDBA 或 SYSOPER 特权时，该用户的名字和权限信息加入到密码文件。如果没有 EXCLUSIVE 密码文件，即如果初始参数 REMOTE_LOGIN_PASSWORDFILE 为 NONE 或 SHARED，那么，如果你试图授予这些权限，会接收到错误消息。

用户至少拥有这两个权限之一时，用户名保留在密码文件中。当取消用户的最新权限时，该用户从密码文件中删除。

创建密码文件，并在其中加入新用户

1. 按照创建密码文件的指令操作。
2. 把 REMOTE_LOGIN_PASSWORDFILE 初始参数设置为 EXCLUSIVE。
3. 以 SYSDBA 权限进行连接，下面是一个例子：

```
CONNECT SYS/change_on_install AS SYSDBA
```

4. 启动事例，创建数据库，装载并打开现有的数据库。