



ORACLE Oracle 数据库技术丛书(2)

ORACLE 8.1.6

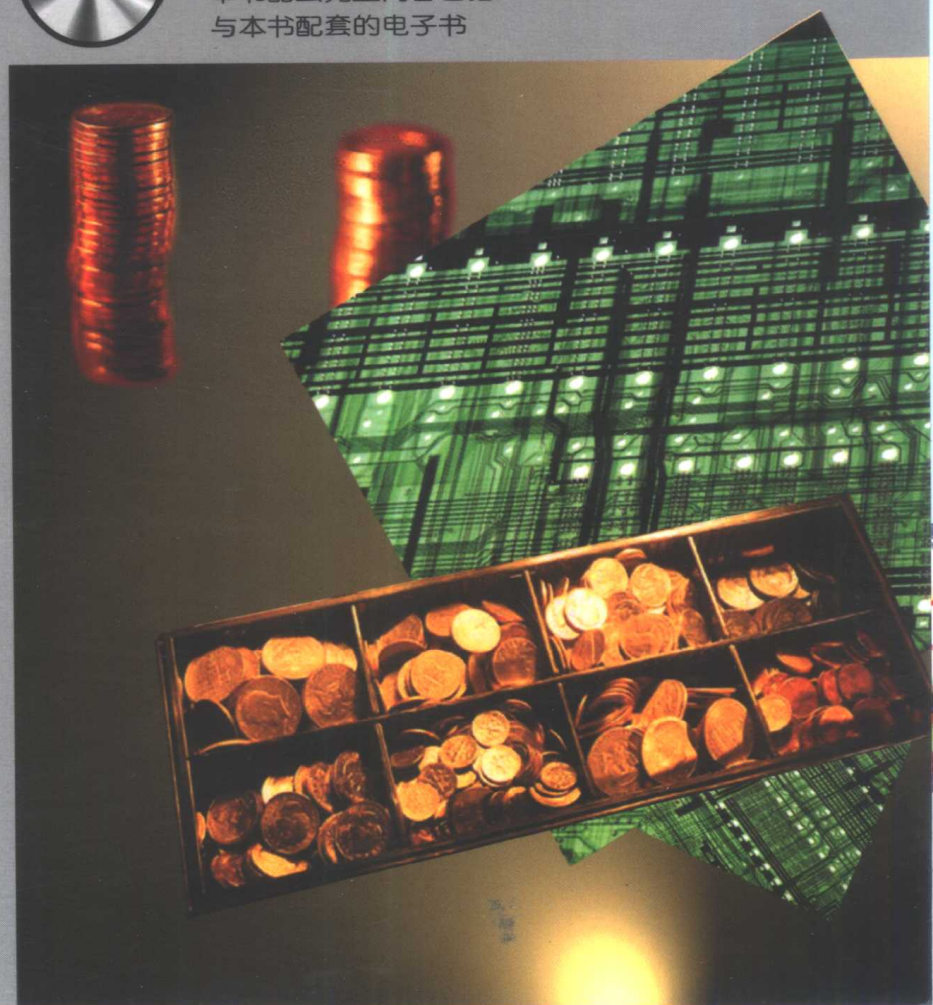
System Security & Network Administration Guide

系统安全与网络管理指南

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(2)

ORACLE 8.1.6

System Security & Network Administration Guide

系统安全与网络管理指南

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



987775



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 4 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。本书第二篇是 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 4 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。

本书既可以作为 Oracle 数据库高级安全管理员和网络管理员及应用程序管理、开发人员的技术参考书，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（2）
书 名： Oracle 8.1.6 系统安全与网络管理指南
文 本 著 作 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： 周凤明 纪红
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 34.375 印张 789 千字
版 次 / 印 次： 2000 年 10 月第 1 版 2001 年 5 月第 2 次印刷
印 数： 5001~8000 册
本 版 号： ISBN 7-900044-94-9/TP·94
定 价： 75.00 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：徐国祥 苏成君 孙兆林等

JSS4P / 12

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

第一篇 Oracle 高级安全管理指南

第一部分 Oracle 高级安全特性

1 Oracle 高级安全机制概述..... 3	7 配置 SecurID 认证..... 57
1.1 Oracle 高级安全机制概述..... 4	7.1 系统要求..... 57
1.2 Oracle 高级安全机制的特性..... 5	7.2 已知的限制..... 57
1.3 Oracle 高级安全机制的结构..... 9	7.3 对 SecurID 进行认证..... 57
1.4 通过网络协议边界进行安全数据传输..... 11	7.4 为 SecurID 认证创建用户..... 61
1.5 系统要求..... 11	7.5 使用 SecurID 认证..... 62
1.6 配置 Oracle 网络认证..... 12	7.6 配置 SecurID 认证中的疑难问题解答..... 65
1.7 Oracle 高级安全机制的限制..... 13	8 配置 Identix 生物测定认证..... 67
2 配置数据加密及数据完整性..... 14	8.1 概述..... 67
2.1 Oracle 高级安全机制的加密算法..... 14	8.2 生物测定认证服务的结构..... 68
2.2 Oracle 高级安全机制的数据完整性..... 16	8.3 先决条件..... 69
2.3 基于 Diffie-Hellman 的密钥管理..... 16	8.4 启用生物测定认证..... 71
2.4 配置数据加密及数据完整性..... 17	8.5 管理生物测定认证服务..... 73
3 小型 JDBC 支持..... 22	8.6 使用生物测定认证识别用户身份..... 74
3.1 有关 Java 的实现..... 22	8.7 配置过程中的疑难问题解答..... 75
3.2 配置参数..... 24	9 配置 DCE GSSAPI 认证..... 76
4 配置 RADIUS 认证..... 26	9.1 配置 DCE GSSAPI 认证..... 76
4.1 RADIUS 概述..... 26	10 配置安全套接层认证..... 79
4.2 RADIUS 认证模式..... 27	10.1 Oracle 环境下的 SSL..... 79
4.3 启用 RADIUS 认证及帐户管理..... 30	10.2 Oracle 环境外的 SSL..... 82
4.4 登录数据库..... 39	10.3 SSL 同其他认证方法联合使用..... 82
5 配置 CyberSafe 认证..... 41	10.4 SSL 使用过程中的问题..... 84
5.1 启用 CyberSafe 认证..... 41	10.5 启用 SSL..... 84
5.2 配置 CyberSafe 认证适配器过程中 的疑难问题解答..... 46	11 选择和组合认证方法..... 98
6 配置 Kerberos 认证..... 48	11.1 使用用户名和口令进行连接..... 98
6.1 启用 Kerberos 认证..... 48	11.2 取消 Oracle 高级安全认证..... 98
6.2 Kerberos 认证服务适配器的实用工具..... 54	11.3 为实现多认证方法而配置 Oracle..... 99
6.3 配置 Kerberos 认证过程中的疑难 问题解答..... 55	
	第二部分 Oracle DCE 集成
	12 Oracle DCE 集成概述..... 101

12.1	系统要求.....	101
12.2	向后兼容性.....	101
12.3	DCE 概述.....	102
12.4	Oracle DCE 集成概述.....	102
13	为 Oracle DCE 集成配置 DCE.....	105
13.1	任务 1: 创建新的主要责任者和帐户.....	105
13.2	任务 2: 在 Keytab 文件中安装 服务器关键字.....	106
13.3	任务 3: 使用 Oracle DCE 集成 配置和应用 DCE CDS.....	106
14	为 Oracle DCE 集成配置 Oracle.....	108
14.1	DCE 的地址参数.....	108
14.2	配置服务器.....	109
14.3	创建和命名外部认证的帐户.....	110
14.4	设置 DCE 集成的外部角色.....	111
14.5	作为使用 DCE 的 SYSDBA 或 SYSOPER 连接 Oracle 数据库.....	112
14.6	配置客户机.....	114
14.7	为使用 DCE CDS 命名配置客户机.....	116
15	在 Oracle DCE 中与 Oracle 数据 库建立连接.....	119
15.1	启动接听者.....	119
15.2	在 DCE 中与 Oracle 数据库服务器 建立连接.....	120
16	分布式计算环境与非分布式计算环境的 互操作性.....	121
16.1	DCE 环境外的客户机与 DCE 环境 中的 Oracle 服务器建立连接.....	121
16.2	样本参数文件.....	121
16.3	当 CDS 不可访问时, 使用 tnsnames.ora 文件进行名称查询.....	123

第三部分 Oracle 8i 安全/目录集成

17	管理企业用户安全.....	125
17.1	企业用户安全机制概述.....	125
17.2	用户-模式分离 (User/Sche ma Separation).....	132
17.3	当前用户数据库链接.....	135
17.4	Oracle 企业用户安全部件.....	136

17.5	安装和配置 Oracle 企业用户安全.....	137
17.6	企业用户登录疑问解答.....	144
18	使用 Oracle 证书夹管理器.....	146
18.1	概述.....	146
18.2	有关安全的概念.....	147
18.3	和 Oracle 应用程序服务器一起使用 Oracle 证书夹管理器.....	148
18.4	启动 Oracle 证书夹管理器.....	148
18.5	管理证书夹.....	148
18.6	管理可信证书.....	151
19	Oracle 企业登录助手.....	156
19.1	关于 Oracle 企业登录助手.....	156
19.2	启动 Oracle 企业登录助手.....	156
19.3	启用自动登录机制.....	157
19.4	终止自动登录服务.....	157
19.5	修改一个证书夹的口令.....	157
20	使用 Oracle 企业安全管理器.....	159
20.1	简介.....	159
20.2	安装与配置 Oracle 企业安全管理器.....	160
20.3	Oracle 企业安全管理器导航.....	162
20.4	管理企业数据库、域和用户.....	164
20.5	管理安全管理员.....	175

第四部分 附录

附录 A	数据加密和完整性参数.....	178
A.1	Sqlnet.ora 示例文件.....	178
A.2	加密和数据完整性参数.....	181
附录 B	认证参数.....	185
B.1	客户机和服务器使用 CyberSafe 认证 的参数.....	185
B.2	客户机和服务器使用 Identix 认证的 参数.....	185
B.3	客户机和服务器使用 Kerberos 认证的 参数.....	187
B.4	客户机和服务器使用 SecurID 认证 的参数.....	187
B.5	客户机和服务器使用 RADIUS 认证 的参数.....	188
B.6	客户机和服务器使用 SSL 认证的参数.....	191

附录 C 使用 RADIUS 集成认证设备	194
C.1 关于 RADIUS 询问—应答用户接口	194
C.2 定制 RADIUS 询问—应答用户接口	194
附录 D Oracle 高级安全 FIPS140-1 设置	196
D.1 配置参数	196
D.2 安装后的检查	197
D.3 状态信息	198
附录 E Oracle 数据库安全的 LDAP 目录模式	199
E.1 结构对象类	199
E.2 属性	199
E.3 访问控制	200
附录 F Java SSL 的 Oracle 实现	202

F.1 Oracle Java SSL 特性	202
F.2 Oracle Java SSL 支持的 SSL 密码集	203
F.3 使用 Oracle 证书夹管理器管理证书 和密钥	203
F.4 Oracle Java SSL 示例	203
F.5 通过类的层次结构扩展 Java SSL 程序包	217
F.6 接口层次结构	218
F.7 oracle.security.ssl	218
F.8 oracle.security.cert	236
词汇表	245

第二篇 Oracle Net8 管理指南

第一部分 Net8 概述和概念

1 Net8 简介	255
1.1 Net8 概述	255
1.2 Oracle 连接概述	257
1.3 配置概述	257
2 Net8 概念	260
2.1 网络环境	260
2.2 连接操作	261
2.3 例外操作	263
2.4 Net8 连接模型	263
2.5 客户端连接选项	270
2.6 监听者的服务注册	272
2.7 连接负载均衡	274
2.8 通过服务名称而非 SID 标识的数据库标识	277
2.9 通过命名方法的服务解析	279
2.10 Net8 和 LDAP 兼容的目录服务器	281
3 Net8 体系结构	292
3.1 透明网络基底	292
3.2 堆栈通信概述	292
3.3 典型 Net8 客户端/服务器环境里的 堆栈通信	293
3.4 客户端连接到目录服务器的栈通信	296

3.5 JDBC 客户端的堆栈通信	297
3.6 Oracle8i JServer 客户端的堆栈通信	299
4 Net8 产品和工具	301
4.1 Net8 客户端	301
4.2 Net8 服务器	301
4.3 Oracle 协议	301
4.4 Oracle 连接管理器	303
4.5 Oracle 名称	306
4.6 外部命名服务	314
4.7 认证方法	314
4.8 Oracle 高级安全	314
4.9 管理工具	315
5 规划你的网络	318
5.1 网络规划概述	318
5.2 定义你的网络布局	318
5.3 解析名称到连接描述符	319
5.4 提高大规模网络的性能	320
5.5 网络规划小结	322

第二部分 配置

6 配置命名方法	323
6.1 配置概述	323
6.2 理解连接描述符	324
6.3 配置模型	324

6.4	配置本地命名方法	325
6.5	配置目录命名方法	332
6.5	配置 Oracle 名称方法	350
6.7	配置主机命名方法	367
6.8	配置外部命名方法	369
7	配置监听者	375
7.1	配置概述	375
7.2	listener.ora 文件修改之后重新启动 监听者	377
7.3	配置监听者协议地址	377
7.4	配置一个使用非缺省地址的监听者	380
7.5	处理大容量的连接请求	381
7.6	配置静态服务信息	381
7.7	配置预产生专有服务器	383
8	启用高级 Net8 特性	386
8.1	配置高级网络地址和连接数据信息	386
8.2	配置透明应用程序失败恢复	393
8.3	为名称解析配置客户端属性	395
8.4	配置高级文档信息	399
8.5	配置优先 Oracle 名称服务器	401
8.6	配置 Oracle 连接管理器特性	402
8.7	配置到非 Oracle 数据库服务的连接	412
9	配置多线程服务器	419
9.1	概述	419
9.2	用 MTS_DISPATCHER 参数配置 MTS	420
9.3	启用连接缓冲特性	423
9.4	资源分配	423
9.5	在客户端使用 MTS	423

9.6	在客户端覆盖 MTS	424
10	启用 Net8 程序员增强特性	425
10.1	Net8 OPEN	425
10.2	UNIX 客户端编程	430

第三部分 Net8 测试和疑难解答

11	建立连接和测试网络	432
11.1	连接到数据库	432
11.2	测试网络	438
12	疑难解答	445
12.1	诊断 Net8	445
12.2	解决最通常的错误消息	448
12.3	来自域的疑难解答技巧	451
12.4	使用日志和跟踪文件解决网络问题	452
12.5	日志错误信息	452
12.6	跟踪错误信息	463
12.7	联系 Oracle 客户支持部门	482

第四部分 参考

A	控制实用程序	483
A.1	操作模式	483
A.2	监听者实用程序 (LSNRCTL)	484
A.3	Oracle 名称控制实用程序 (NAMESCTL)	500
A.4	Oracle 连接管理器控制实用程序 (CMCTL)	534

第一篇

Oracle 高级安全管理指南

第一部分 Oracle 高级安全特性

本书在第一部分中主要介绍了用户如何在 Net8 的 8.1.6 版网络下配置数据加密、数据完整性及用户认证。其中也涉及到在指定端口下如何安装和配置 Oracle 高级安全特性。

在本书的各章节中，将会介绍关于 Oracle 高级安全机制的相关特性的一般知识。

- 第 1 章，“Oracle 高级安全机制概述”
- 第 2 章，“配置数据加密及数据完整性”
- 第 3 章，“小型 JDBC 支持(Thin JDBC Support)”
- 第 4 章，“配置 RADIUS 认证”
- 第 5 章，“配置 CyberSafe 认证”
- 第 6 章，“配置 Kerberos 认证”
- 第 7 章，“配置 SecurID 认证”
- 第 8 章，“配置 Identix 生物身份测定认证”
- 第 9 章，“配置 DCE GSSAPI 认证”
- 第 10 章，“配置安全套接层认证”
- 第 11 章，“选择和组合认证方法”

DCE 集成相关知识：

请参考第二部分，“Oracle DCE 集成”。

安全及目录集成：

请参考第三部分，“Oracle8i 安全/目录集成”。

1 Oracle 高级安全机制概述

本章主要介绍了 Oracle 高级安全机制（过去为 Oracle 高级网络选项）的数据加密、数据完整性以及用户认证 3 个特性，这 3 个特性在使用 Net8 的网络产品中均可以得到。如 Oracle8i、Oracle Designer、Oracle Developer，以及其他任意 Oracle 公司或第三方支持的 Net8 产品。

本章主要包括以下内容：

- Oracle 高级安全机制概述
- Oracle 高级安全机制的特性
- Oracle 高级安全机制的结构
- 通过网络协议边界进行安全数据传输
- 系统要求



- 配置 Oracle 网络认证
- Oracle 高级安全机制的限制

1.1 Oracle 高级安全机制概述

Oracle 高级安全机制（过去为 Oracle 高级安全网络选项和安全网络服务）提供了一套综合安全特性，来保护企业内部网络及与 Internet 连接的扩展联合网络。并且，还提供了一个集成网络加密和认证方法的单一源点、单一签名服务及安全协议。通过集成工业标准，Oracle 高级安全机制为 Oracle 网络及更高层网络提供了前所未有的安全保障。

本节主要包括以下两个内容：

- 在分布式环境下的网络安全
- 数据保密性所面临的威胁

1.1.1 在分布式环境下的网络安全

Oracle 数据库支持着世界最大最受欢迎的网站。在世界范围内，多数全球规模的公司配置的分布式数据库，以及客户/服务器的应用软件，都是基于 Net8 和 Oracle8i 的。这种分布式计算应用的增多，正迎合了大量信息迅速增长的需要。可以说，现在的公司是建立在计算机上的。雇员档案、金融档案、产品测试信息以及其他敏感重要数据，已经从文档室里移到了文件结构中。大量关键、敏感的数据保存在计算机中，也使这些数据本身更容易受到安全性威胁。

1.1.2 数据保密性所面临的威胁

在分布式环境下，随着分布数据量的增加，也带来了严重的安全威胁，包括下列各种威胁：

- 数据篡改
- 数据偷听及盗窃
- 伪造用户身份
- 管理多个口令

数据篡改

在分布式环境下，某些怀有恶意的第三方，可能会篡改在站点之间传输的数据，进行计算机犯罪。

数据偷听及盗窃

在 Internet 及广域网 WAN 环境下，许多公共媒体及私人网络要通过一些不安全的地段来架设他们的网络，尤其是易受攻击的微波和卫星通信或服务器，经常将一些有用的数据暴露给任何感兴趣的组织。在一幢大楼或一个校园里的局域网 LAN 环境下，一些内部人员可以通过物理配线轻而易举的在网络上安装监听器以偷听正在传输的数据。

伪造用户身份

在分布式环境下，伪造一个用户身份，从而使得获取对重要信息的访问权变得更加容易。系统如何能够确定从客户 B 连接到服务器 A 的用户 Pat 是真正的用户？此外，在分布式环境下，犯罪分子还可以劫持网络上的连接，那么用户如何能够确定客户 B 和服务器 A 的真正身份？实际中，从记录职员的服务器 A 到记录职员薪水的服务器 B 的一项事务处理，在传输过程中可能被别人截取，并被重新传输到一个伪造的终端服务器 B 上。

管理多个口令

在分布式系统中，用户通常需要记忆多个应用软件和服务的口令。例如，一位程序开发人员就需要知道工作站开发软件的口令、微机系统口令、用于生成文档的 PC 机口令、以及用于测试、报错、管理配置的多台计算机或企业内部互连网络的口令等。

通常用户采取以下几个方法管理多个帐户口令：

- 若用户可以自己设置口令，则他们可能选择极易被猜到的口令，如用户名、用户自编字符串、或可以在词典中查找到的单词等。所有这些口令都容易受到词典攻击。
- 用户可能会将这些口令标准化，即在所有机器上口令一致。因而，这些标准化的口令一旦被盗取，那么必将导致大范围内的信息泄漏。即使这些口令稍有不同，也可以通过一个口令而破解其他口令。
- 那些使用复杂口令的用户通常将口令记录在很容易被攻击者找到的地方，并且用户自己有时也可能忘记这些口令。因此，这需要用户相应的管理及配套计划。
- 以上提到的三种口令管理方法都严重地损害了口令的保密性及服务的安全性，而且，针对这些帐户和口令的管理也是一项非常复杂、耗时、开销大的工作。

1.2 Oracle 高级安全机制的特性

Oracle 高级安全机制可以应付上面提到的分布式环境下的威胁。以下是将要在本节中介绍的几个 Oracle 高级安全机制特性：

- 数据保密性
- 数据完整性
- 认证
- 单一签名协议
- 授权

1.2.1 数据保密性

Oracle 高级安全机制保证在采用以下两种加密算法进行数据传输时，数据不被泄露。

- RSA 加密算法
- DES 加密算法

RSA 加密算法

RSA 加密算法是采用了 RSA 数据保密 RC4 加密算法的加密模块。此算法通过使用一个秘密的、对每一会话随机产生的独一无二的密钥，对包括数据值、SQL 语句、存储过程及存储数值在内的所有网络通信，进行安全保护。客户和服务端可以单独或同时提出请求或



要求使用该算法来保证数据的安全。Oracle 的最优化工具可以为最小的业务操作提供一个高级安全防护。并且,在 RC4 算法中,Oracle 提供了 40 比特、56 比特及 128 比特的加密密钥。

自从 Oracle 高级安全机制中的 RSA RC4 40 比特及 56 比特加密算法的使用符合美国政府关于加密产品出口规定以后,Oracle 公司提供了一个媒体(media)国际版本,将其出口到少数几个国家之外的其他国家,并允许一些国家通过这套软件来保护其在全球范围内的业务操作。

DES 加密算法

美国数据加密标准 DES(Data Encryption Standard)通常应用于金融业和其他行业。Oracle 高级安全机制提供了一个标准的、最优化的 56 比特密钥的 DES 加密算法。由于过去美国出口法规在这一方面的限制,Oracle 也提供了一个 DES40 算法,这一算法综合了 DES 加密算法和国际上通用的 40 比特密钥算法。由于 DES56 算法已经允许出口,因此,现在使用的 DES40 算法具有向后兼容性。用户可以选择加密算法为自己在网络上传输的数据进行加密,并可以为不同类型数据的传输设置不同的安全等级。

更多的信息 关于这方面更多的知识,请参考第 2 章“配置数据加密及数据完整性”和附录 A“数据加密和完整性参数”。

1.2.2 数据完整性

为保证数据在传输时不被篡改、删除、重传,Oracle 高级安全机制使用 MD5 算法的密码校验和,随机产生一个安全报文摘要,并把它加入到每一个要通过网络发送的信息包里。

而且,Oracle 高级安全机制的特性 SSL 允许使用保密散列算法 SHA(Secure Hash Algorithm)。该算法比 MD5 慢一些,但是它可以产生更大的报文摘要,针对那些强行碰撞攻击及逆转攻击(inversion attacks)提供更可靠的安全保护。

1.2.3 认证

在分布式环境下,创建用户认证是首要的任务。否则,在限制用户权限方面可信程度不高。通常,口令是最为常用的认证方法。Oracle 高级安全机制综合使用了各种强有力的认证服务方法,在其 8.1.6 版中,通过 Oracle 认证适配器(authentication adapter)进行认证,而这种适配器支持各种第三方认证服务。

许多 Oracle 高级安全机制的认证方法采用集中式认证。这种认证对用户、客户和服务器的可信程度较高。拥有这样一套集中式认证软件,对所有网络成员(客户机到服务器、服务器到服务器、用户到客户机及服务器)身份是一种有效的认证方法,它能够锁定那些网络上伪造用户身份的结点。

1.2.4 单一签名

集中式认证也为用户提供了单一签名认证方法。该方法允许用户使用一个口令去访问多个帐户和应用软件,这消除了需要多个口令的必要性,并简化了系统管理员对用户帐户及口令的管理。

图 1-1 表示集中式网络认证服务的典型操作过程。

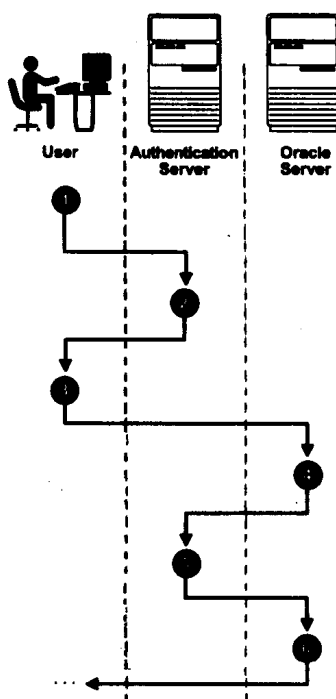


图 1-1 集中式网络认证服务

Oracle 高级安全机制支持下列几种认证方法：

- SSL 认证
- RADIUS 认证
- Kerberos 和 CyberSafe 认证
- 灵通卡认证 (RADIUS-Compliant)
- 令牌卡认证 (SecurID or RADIUS-Compliant)
- 生物测定认证
- 大型 ISM

SSL 认证

安全套接层 SSL (Secure Sockets Layer) 是一个应用于网络连接的工业标准协议。SSL 提供了认证、数据加密、数据完整性服务，并且提供了一个公开密钥基础结构 PKI (Public Key Infrastructure)。

Oracle 高级安全机制的 SSL 特性在任何客户机和服务器之间的保密通信中使用，尤其是用户还可以使用 SSL 对以下两种情况进行认证：

- 一个客户机或服务器到一个或多个 Oracle 服务器
- 一个 Oracle 服务器到任何一个客户机

SSL 特性可以单独使用，也可以综合使用其他 Oracle 高级安全机制所支持的认证方法。例