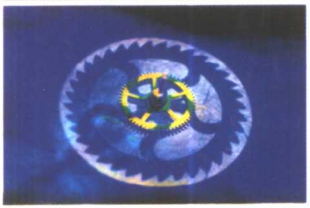
网络管理与技术丛书

Oracle管理系列

Oracle 8i

安全管理

Oracle管理系列 编委会



能在所有主要的平台上运行

完全支持所有的工业标准

多用户、共享式的信息仓模式

基于模型的方法来设计和实现

中国人民大学出版社

CHINA RENMIN UNIVERSITY PRESS

网络管理与技术丛书
Oracle 管理系列

Oracle 8i
安全管理

Oracle 管理系列 编委会

中国人民大学出版社

图书在版编目（CIP）数据

Oracle 8i 安全管理/Oracle 管理系列 编委会编著
北京：中国人民大学出版社,2001
（网络管理与技术丛书·Oracle 管理系列）

ISBN 7-300-03750-X/G·781
I. O…
II. O…
III. 关系数据库-数据库管理系统-Oracle 8i-安全技术
IV. TP311.138

中国版本图书馆 CIP 数据核字（2001）第 14251 号

网络管理与技术丛书
Oracle 管理系列
Oracle 8i 安全管理
Oracle 管理系列 编委会

出版发行：中国人民大学出版社
（北京中关村大街 31 号　邮编 100080）
邮购部：62515351　门市部：62514148
总编室：62511242　出版部：62511239
经　　销：新华书店
印　　刷：涿州市星河印刷厂

开　　本：787×960 毫米 1/16　印张：21
2001 年 4 月第 1 版　2001 年 4 月第 1 次印刷
字　　数：520 000　印数：1~5000 册

定　　价：29.00 元
（图书出现印装问题，本社负责调换）

Oracle 管理系列 编委会

出 版 说 明

20 世纪的偶像是原子，
21 世纪的偶像是网络，
网络就是我们的未来！

美国《连线》主编凯文·凯利在《网络经济的十种策略》中的这一论断令人发聋振聩。

我们的时代正走向信息时代、网络时代。网络已远远越出技术的层面，它渗透到我们生活的各个方面，它重塑了这个时代的政治、经济、文化，改变了我们的生活方式、交往方式和思维方式，它好像被激活的高速裂变的细胞，扩散到社会有机体的各个部位，像活跃的蜂群笼罩着我们这个星球的表面。网络代表着新时代，网络象征着新生活。

网络离不开技术。计算机信息技术是网络社会的主角，那么掌握计算机技术意味着应对未来挑战的必不可少的手段。计算机将是我们生活中不可缺少的内容，学会计算机技术也是在未来生活中生存的一个必不可少的条件。

但是，仅仅依靠技术的进步而忽视人文关怀，人就成了被异化的“单向度”的机器，互联网世界应是最具人性化的“以人为本”的世界，互联网一方面体现着技术的发展，它同时也推动着经济的繁荣、管理的创新、文化的丰富以及社会的全面进步。

作为在人文社会科学有影响的出版机构，中国人民大学出版社一直关注着这场网络革命，早在 1997 年就推出了一套在业界引起广泛影响的“网络文化丛书”。今天，我们又在 IT 行业在全球迅猛发展，向各行各业渗透并引发新一轮产业革命的时候，及时组织了很多专家、教授、编程人员，出版具有自己特色的电脑图书，即把技术及其技术在经济、管理、法律等方面的应用紧密结合，从而形成自己的出书特色。

中国人民大学出版社版计算机图书像其他人大版图书一样比较全面、严谨、严肃。本系列图书几乎全部是关于网络、信息方面的知识。丛书共计 5 个系列，40 余本——计算机综合知识、网页设计及网络编程、UNIX 系统及网络管理、Oracle 数据库、信息管理。内容涉及到网络的方方面面：网络基础知识、网页制作、网络编程、数据库工程、系统平台、网络信息系统、网络安全、软件体系结构以及网站的筹建、管理等等。

本套丛书从整体上具有计算机图书固有的特点：

新——正式的版本、最新的版本
博——最常用软件、功能最强大软件
势——论述网络、领导大势
快——最快捷的工具书
通——内容系统、深入浅出
雅——版面沉稳、雅致

ZAN 03/06

实——内容丰富、尽晓网络

总之，这套丛书系统地、全面地介绍了网络方面的知识，用户可以选择适合于自己的图书，可以循序渐进地系统学习，同时也可以做为随身“博士”，随时帮助解决实际的问题；既有“入门”知识，又可以达到“入室”水准。这样，通过这套丛书的系统学习，我们将在信息爆炸的未来占有一席之地，搏击，以网制胜未来。

本套丛书编写时间较短，书中难免有不足之处，请读者指出，我们会尽快改进。

中国人民大学出版社

内 容 简 介

本书以 Oracle 数据库为主要对象，由浅入深、循序渐进地介绍了关于数据库安全方面的知识。全书共分为 13 章，从威胁数据库安全的现象、相应的解决策略到防火墙技术等都包括其中，特别对 Oracle 数据库安全原理进行了讨论。每一章之后都有小结，便于读者理解全书内容。

前　言

目前，Oracle 数据库是应用最广泛的数据库之一。它是一种大型远程网络数据库，可以在多个操作系统（Windows、Windows NT 等）平台上应用。它提供有很好的安全机制，而且还在不断地改进和升级。Oracle 数据库给用户以应用上的极大方便和安全感。

鉴于以上述情况，我们编写了这套 Oracle 数据库系列丛书。该丛书一共 6 册，从各个方面介绍了 Oracle 数据库的知识。丛书内容由浅入深，适合于对 Oracle 数据库有不同熟悉程度的用户阅读；6 本专册分别针对某一方面的问题进行集中论述，对 Oracle 数据库用户有很大的参考价值。

本书的主要内容分为 13 章。第 1 章先从总体上介绍一些关于数据库安全的知识。第 2、第 3 章针对 Oracle 远程网络数据库的特点，介绍关于对网络的风险如何进行分析和预防的知识。接下来第 4 章到第 8 章介绍的是有关 Oracle 数据库的安全原理的知识；其中前 4 章主要介绍 Oracle 数据库自身采取的安全机制和策略；第 8 章补充介绍了一些有关 Oracle 安全的一些常见问题和知识。第 9 章主要通过实例来讲解 Oracle 数据库安全原理如何应用于一个数据库系统；第 10 章到第 13 章讲解如何对数据库进行前台保护，主要介绍了防火墙的知识。

本书阅读对象主要是数据库管理员，为他们提供一些关于数据库安全方面的参考；同时也欢迎其他广大 Oracle 数据库用户阅读本书，从中了解一些数据库安全知识，以防在实际工作中由于自己操作不当而造成对于数据库安全的威胁。

编　者

2001 年 1 月

目　录

第一部分　数据库安全与网络风险分析 1
第 1 章　数据库的安全和完整性约束 1
1.1　数据库的安全 1
1.1.1　视图和查询修改 2
1.1.2　访问控制 3
1.1.3　数据加密 6
1.1.4　跟踪审查 6
1.2　统计数据库的安全简介 7
1.3　完整性约束 7
1.3.1　完整性约束的类型 7
1.3.2　完整性约束的说明 8
1.3.3　完整性约束的实施 9
1.4　数据库加密技术介绍 9
1.4.1　数据库密码系统的基本流程 9
1.4.2　数据库加密的特点 10
1.4.3　数据库加密的范围 11
1.4.4　数据库加密对数据库管理系统原有功能的影响 11
1.5　Oracle 数据库 12
1.5.1　什么是 Oracle 12
1.5.2　Oracle 产品 13
1.5.3　Oracle 安全策略 15
1.5.4　Oracle 8 22
1.6　本章小结 23
第 2 章　威胁网络安全的因素 24
2.1　概述 24
2.2　安全威胁的类型 24
2.3　操作系统安全的脆弱性 25
2.4　协议安全的脆弱性 25

2.5 数据库管理系统安全的脆弱性 26
2.6 人为因素 26
2.7 本章小结 26
第 3 章 威胁网络安全的现象与相应的防范策略 27
3.1 概论 27
3.2 数据完整性和安全 28
3.2.1 数据完整性 28
3.2.2 安全 34
3.3 数据完整性和安全威胁的一般解决方法 38
3.3.1 提高数据完整性的工具 38
3.3.2 减少安全威胁的工具 51
3.4 本章小结 64
第二部分 Oracle 数据库安全原理 65
第 4 章 Oracle 数据库的环境安全 65
4.1 安全管理策略 65
4.2 Oracle 用户管理 66
4.2.1 用户账号的主要用途 67
4.2.2 创建、修改和删除用户 67
4.2.3 外部标识用户 74
4.3 不同类型的权限 75
4.3.1 具有 connect 特权的用户 75
4.3.2 具有 resource 特权的用户 76
4.3.3 具有 DBA 特权的用户 76
4.3.4 两种系统级权限 76
4.3.5 授予系统级权限 77
4.3.6 系统权限的收回 80
4.3.7 检查存在的系统权限 80
4.3.8 对象级权限 81
4.3.9 授予对象级权限 82
4.3.10 对象级权限类型 83
4.4 角色 90
4.4.1 使用角色管理特权的优点 90

4.4.2 建立角色应遵循的准则 91
4.4.3 Oracle 预定义角色 91
4.4.4 角色的作用 92
4.4.5 创建、修改和删除角色 93
4.4.6 授予角色系统级和对象级权限 94
4.4.7 授予和收回角色 94
4.4.8 允许和禁止角色 96
4.4.9 操作系统允许的角色 97
4.4.10 用户的缺省角色 97
4.4.11 角色的数据字典视图 98
4.4.12 角色的缺陷 101
4.6 本章小结 103
第 5 章 审计数据库使用并控制资源和口令 104
5.1 审计 104
5.1.1 为什么要审计 105
5.1.2 准备审计跟踪 106
5.1.3 维护审计表 106
5.1.4 控制系统审计 107
5.1.5 控制审计对象 111
5.1.6 评审审计记录 113
5.2 配置文件和系统资源 114
5.2.1 组合的资源限度 115
5.2.2 创建配置文件 116
5.2.3 分派配置文件 117
5.2.4 更改配置文件 118
5.2.5 删除配置文件 118
5.3 配置文件与口令管理 118
5.3.1 创建口令管理配置文件项 119
5.3.2 检查口令复杂性 121
5.3.3 防止口令重用 122
5.3.4 口令的编码与技巧 123
5.4 本章小结 126

第 6 章 Oracle 8 为提高数据系统安全性而采用的技术 127
6.1 特权 127
6.1.1 特权（OS 级） 127
6.1.2 特权（在数据库中） 127
6.2 日志 129
6.2.1 redo 日志和脱机 redo 日志 130
6.2.2 重演日志 131
6.3 回滚段 143
6.3.1 管理回滚段 143
6.3.2 决定回滚段的个数 145
6.3.3 估计回滚段大小 145
6.3.4 添加回滚段 147
6.3.5 创建回滚段 147
6.3.6 public 和 private 回滚段 148
6.3.7 更改回滚段 148
6.3.8 删除和收缩回滚段 149
6.4 临时段 150
6.4.1 使用临时段 150
6.4.2 估计临时表空间大小 150
6.4.3 设置临时表空间的存储选项 151
6.4.4 管理临时段 152
6.5 在内存/CPU 方面的技术改进 153
6.5.1 Windows NT 性能监视器 153
6.5.2 后台进程 154
6.5.3 跟踪文件和实例报警文件 155
6.5.4 系统全局区（SGA） 157
6.5.5 分页和对换 157
6.5.6 存储器需求 157
6.5.7 共享池 159
6.5.8 数据库缓冲区高速缓存 169
6.5.9 重演日志缓冲区高速缓存 170
6.5.10 CPU 的繁忙程度 171

6.5.11　使 CPU 功能最大化 173
6.5.12　会话控制 173
6.5.13　综述 176
6.6　数据库备份技术 177
6.6.1　备用数据库设施 177
6.6.2　调整数据库备份 180
6.6.3　调整数据库恢复 183
6.6.4　备份数据库的技巧 184
6.6.5　主备份阶段 187
6.7　对付 DBA 错误的方法 187
6.7.1　后台进程跟踪文件 187
6.7.2　数据库自由空间 188
6.7.3　用户临时段 189
6.7.4　失控进程 190
6.7.5　双任务研究 190
6.8　有效资源管理 191
6.8.1　提交语句的频率 191
6.8.2　利用 PL/SQL 的光标管理 192
6.9　本章小结 193
第 7 章　Oracle 数据库备份技术与系统恢复 194
7.1　概述 194
7.1.1　备份的必要性 194
7.1.2　备份的内容 194
7.1.3　备份的时机 195
7.2　了解 Oracle 8 备份选项 195
7.2.1　故障类型 195
7.2.2　存档数据库 195
7.2.3　备份选项 201
7.3　选择并实现备份策略 206
7.3.1　选择备份策略 206
7.3.2　考虑使用 recovery manager 207
7.3.3　进行脱机（冷）备份 209

7.3.4 进行联机（热）备份 211
7.3.5 创建后备数据库 212
7.3.6 复制用于灾难 215
7.4 使用 Oracle 8 中增加的备份 216
7.5 rman 命令 217
7.6 数据库恢复 221
7.6.1 理解恢复的必要性并设法避免失败 221
7.6.2 恢复策略 222
7.6.3 分析故障并决定恢复选项 224
7.6.4 恢复一般数据文件的损失 225
7.6.5 恢复回滚表空间中丢失的数据文件 227
7.6.6 恢复系统表空间的损失 231
7.6.7 恢复控制文件的损失 233
7.6.8 恢复联机重演日志的损失 234
7.7 本章小结 236
第 8 章 与 Oracle 数据库安全有关的知识和技术介绍 237
8.1 Oracle 数据库密码文件的使用和维护 237
8.1.1 概要 237
8.2 Oracle 常见错误代码的分析与解决 240
8.3 如何解决 Oracle 数据库中的瓶颈问题 246
8.4 在 Oracle 中利用角色增强应用系统安全性 251
8.5 本章小结 253
第 9 章 数据库安全原理应用 254
9.1 权限 254
9.2 监控重要的数据库统计信息 255
9.2.1 查看数据库内部 255
9.2.2 重要的统计数字 257
9.3 审计 259
9.4 数据备份和恢复 260
9.4.1 风险管理 260
9.4.2 如何应用备份和恢复时需要的重要数据结构 264
9.4.3 备份 266

9.4.4　制作备份的频度 268
9.4.5　恢复 268
第三部分　网络数据库系统前台防护 273
第 10 章　为什么要进行前台防护 273
10.1　本章小结 274
第 11 章　Web 站点上数据的安全 275
11.1　访问限制类型 275
11.1.1　通过 IP 地址或域名限制 275
11.1.2　用户名/口令的安全性 276
11.1.3　加密的工作原理 277
11.2　本章小结 277
第 12 章　CGI 介绍 278
12.1　CGI 简介 278
12.2　CGI 的危险性 278
12.3　CGI 如何工作 279
12.4　CGI 数据的译码加密和解译 280
12.5　理解脆弱性 280
12.6　本章小结 281
第 13 章　防火墙 282
13.1　防火墙的基本概念 282
13.1.1　防火墙 282
13.1.2　防火墙的作用 283
13.1.3　包过滤 284
13.1.4　代理服务器 284
13.2　检查防火墙部件 286
13.2.1　双宿主主机 286
13.2.2　堡垒主机 289
13.2.3　过滤子网 295
13.2.4　应用层网关 296
13.3　防火墙类型 299
13.3.1　最常见的防火墙类型 299
13.3.2　网络级防火墙 299

13.3.3 应用级防火墙.....300
13.3.4 其他种类的防火墙.....300
13.3.5 动态防火墙.....301
13.4 设计防火墙的一般原则.....302
13.5 一些实用的防火墙介绍.....304
13.5.1 病毒防火墙（金山毒霸）.....304
13.5.2 WithGate 防火墙.....305
13.5.3 天网防火墙个人版简介.....312

第一部分　数据库安全与网络风险分析

第 1 章　数据库的安全和完整性约束

数据库是共享资源，因此我们不仅要充分利用它，而且要保护它。对数据库的破坏一般来自下列 4 个方面：

（1）系统故障。

（2）并发所引起的数据不一致。

（3）人为的破坏，例如数据被不该知道的人访问甚至篡改或破坏。

（4）输入或更新数据库的数据有误，更新事务未遵守保持数据库一致性的原则。

对付第 1 种破坏的措施，是采用备份技术和系统恢复技术。

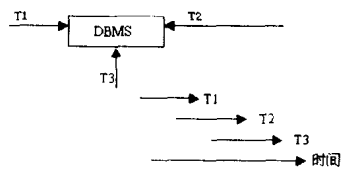


图 1-1　并发访问

对付第 2 种破坏的措施，可以采用并发访问控制的方法。并发访问如图 1-1 所示，图中 DBMS 为数据库管理系统（Data Base Management System），T1、T2、T3 为访问数据库的事务。

在数据库系统中，经常有多个事务并发地执行，每个事务含有若干有序的操作。这些操作由数据库系统安排其执行的顺序，安排的原则是：既要交叉执行以充分利用系统的资源，又要避免访问冲突。

有关数据库第 3 种破坏问题的解决方法，统称为数据库安全。

有关数据库第 4 种破坏问题的解决方法，统称为完整性约束。

1.1　数据库的安全

数据库安全从字面上理解有很多含义，诸如防火、防盗、防掉电、防破坏等都应属于这个范畴。