

Mc
Graw
Hill Education



Applied Oracle Security: Developing Secure Database
and Middleware Environments

ORACLE®
DATABASE

ORACLE®
FUSION MIDDLEWARE

Oracle 安全实战

——开发安全

中间件环境

Oracle公司首席架构师Edward Screven作序推荐

(美) David C. Knox
Scott G. Gaetjen
孟祥旭 唐扬斌

等著
译



清华大学出版社

Oracle 安全实战——开发安全的 数据库与中间件环境

(美) David C. Knox 等著
Scott G. Gaetjen
孟祥旭 唐扬斌 译

清华大学出版社

北 京

David C. Knox, Scott G. Gaetjen, et al.

Applied Oracle Security: Developing Secure Database and Middleware Environments

EISBN: 978-0-07-161370-5

Copyright © 2010 by The McGraw-Hill Companies, Inc.

All Rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including without limitation photocopying, recording, taping, or any database, information or retrieval system, without the prior written permission of the publisher.

This authorized Chinese translation edition is jointly published by McGraw-Hill Education (Asia) and Tsinghua University Press. This edition is authorized for sale in the People's Republic of China only, excluding Hong Kong, Macao SAR and Taiwan.

Copyright © 2011 by McGraw-Hill Education (Asia), a division of the Singapore Branch of The McGraw-Hill Companies, Inc. and Tsinghua University Press.

版权所有。未经出版人事先书面许可，对本出版物的任何部分不得以任何方式或途径复制或传播，包括但不限于复印、录制、录音，或通过任何数据库、信息或可检索的系统。

本授权中文简体字翻译版由麦格劳-希尔(亚洲)教育出版公司和清华大学出版社合作出版。此版本经授权仅限在中华人民共和国境内(不包括香港特别行政区、澳门特别行政区和台湾)销售。

版权 © 2011 由麦格劳-希尔(亚洲)教育出版公司与清华大学出版社所有。

北京市版权局著作权合同登记号 图字：01-2010-0581

本书封面贴有 McGraw-Hill 公司防伪标签，无标签者不得销售。

版权所有，侵权必究。侵权举报电话：010-62782989 13701121933

图书在版编目(CIP)数据

Oracle 安全实战——开发安全的数据库与中间件环境/(美)诺克斯(Knox, D.C.), (美)格特延(Gaetjen, S.G.) 等著; 孟祥旭, 唐扬斌 译. —北京: 清华大学出版社, 2011.7

书名原文: Applied Oracle Security: Developing Secure Database and Middleware Environments

ISBN 978-7-302-25632-8

I. O… II. ①诺… ②格… ③孟… ④唐… III. 关系数据库—数据库管理系统, Oracle—安全技术 IV. TP311.138

中国版本图书馆 CIP 数据核字(2011)第 096077 号

责任编辑: 王 军 于 平

装帧设计: 孔祥丰

责任校对: 胡雁翎

责任印制: 何 芊

出版发行: 清华大学出版社

地 址: 北京清华大学学研大厦 A 座

<http://www.tup.com.cn>

邮 编: 100084

社 总 机: 010-62770175

邮 购: 010-62786544

投稿与读者服务: 010-62776969, c-service@tup.tsinghua.edu.cn

质 量 反 馈: 010-62772015, zhiliang@tup.tsinghua.edu.cn

印 刷 者: 清华大学印刷厂

装 订 者: 三河市新茂装订有限公司

经 销: 全国新华书店

开 本: 185×260 印 张: 36.75 字 数: 941 千字

版 次: 2011 年 7 月第 1 版 印 次: 2011 年 7 月第 1 次印刷

印 数: 1~4000

定 价: 69.00 元





译者序

本书是 David C. Knox 继 *Effective Oracle Database 10g Security By Design* (McGraw-Hill 出版社 2004 年出版) 之后的又一力作, 得到了 Oracle 官方技术网站 OTN (Oracle Technology Network) 的极力推荐。所有作者都是来自 Oracle 内部的资深研发和工程人员, 很多人曾经是 Oracle Database Vault 等杰出的安全产品研发团队中的成员。他们对于 Oracle 的安全机制如数家珍, 讲解起来可以追根溯源、深入浅出, 对于很多关键机制的讲解更会使您有醍醐灌顶之感。整本书围绕几个简单的安全实例(基于 Oracle 示例数据库)展开, 将各种安全机制和技术融入其中, 相互辅衬, 前后关联。认真读来, 可以更深入地理解如何灵活自如地运用 Oracle 安全机制。

随着社会的进步, 敏感数据越来越多, 人们更加关注自己的隐私问题, 各种法律法规对企业数据操作的监管也越来越严格。在这样的背景下, Oracle 的安全研发人员一直在完善自己的安全机制: 为了解决特权账户带来的风险, 防范内部人员的攻击, 研发了 Oracle Database Vault; 为了符合新的法律规定, 设计实现了更加先进的身份管理策略和细粒度的审计策略。可以说 Oracle 一直在坚持不懈地努力, 尽其所能帮助客户解决安全隐患。而本书无疑是对 11g 中新的安全特性的最权威解读。同时, 在您企业的信息系统中, 使用 Oracle 提供的最新安全防护机制是保护敏感数据的最有效途径。

本书是一本理论性和实践性都很强的书，因为作者相信“您对安全组件的架构和原理了解得越多，就越能够有效地降低安全风险”。所以在使用本书时，要先从宏观上掌握 Oracle 安全体系的整体脉络和原理。如孔子所言“学而不思则罔，思而不学则殆”，在阅读本书的时候，也要“读”“思”并举，尤其要积极思索各种技术的动机和用途，深入理解作者提出的种种安全原理，并将各个分散的部分在头脑中组建成一个有机整体。

“实践出真知”，建议您在阅读的过程中也不断地动手实践，对书中的实例亲自调试运行，最好能够结合自己的工作，做到举一反三，灵活运用。

本书由孟祥旭和唐扬斌翻译。敬请广大读者提供反馈意见，读者可以将意见发到 wkservice@vip.163.com，我们会仔细阅读读者发来的每一封邮件，以求进一步提高今后译著的质量。由于译者水平有限，时间紧迫，故译文中必定存在很多不足之处，希望读者能够谅解，并不吝斧正。真心希望我们的工作能够给您的工作和学习带来帮助，也希望通过您的安全实践给社会带来更多的安全收益！



作者简介

David C. Knox, Oracle 公司解决方案工程部门的高级经理, 现担任 Oracle National Security Group 高级经理。从事该工作之前, 曾担任 Oracle 北美分部销售和咨询解决方案工程师, 得以了解 Oracle 技术体系内部关于解决方案和 R&D 创新的方方面面。还曾担任 Oracle Protected Enterprise & Security Business 的高级经理及 Oracle Information Assurance Center 的主任工程师。

自 1995 年加入 Oracle 起, Knox 曾与许多客户组织一起开展工作, 包括美国国防部、CIA、商务部以及其他许多工商业机构, 这使他对关键商业驱动力及其实现过程有着非常广泛而深入的了解。他在计算机安全领域的专家身份不仅源于他对 Oracle 安全产品和数据库安全技术的全面理解和丰富经验, 也源自他作为一位学者对多层次安全、密码学、LDAP 及 PKI 等理论与技术的深入研究。

Knox 是 *Effective Oracle Database 10g Security By Design* (McGraw-Hill 出版社 2004 年出版) 一书的作者。此外, 他在安全领域的著作还包括: Thomas Kyte 主编的 *Expert One on One Oracle* (Wrox 出版社 2001 年出版) 以及 *Mastering Oracle PL/SQL: Practical Solutions* (Apress 出版社 2003 年出版)。他参与编著了多本 Oracle 技术白皮书。Knox 拥有 University of Maryland 的计算机科学学士学位和 Johns Hopkins University 的计算机科学硕士学位。

Scott G. Gaetjen, 技术经理, Oracle National Security Group, 主要从事安全解决方案的

设计与开发，他以在 Oracle 技术部门 15 年的工作经验，致力于为客户提供更先进的安全防护能力。作为技术负责人和导师参与了众多客户的项目，包括美国国防部、CIA、国土安全部、国民政府和其他金融工业机构等。帮助这些客户实现追求的任务目标的过程，使他能够深入理解操作系统安全、Oracle 数据库安全、J2EE 安全和身份管理等技术。

自 Oracle Database Vault 项目 2004 启动，Gaetjen 就开始参与其研发工作。该产品最终由 Oracle 咨询部门的一个解决方案发展成为了一项独立而强大的 Oracle 软件产品。

Gaetjen 拥有 James Madison University 的数学学士学位以及 University of Maryland University College 的计算机系统管理硕士学位。

Hamza Jahangir 目前担任 Oracle Enterprise Architecture 工作组的主任架构师。他于 2004 年加入 Oracle 公司，已经从事 Oracle 数据库和中间件方面的工作 10 余年。作为架构师，他花费了大量时间为客户提供技术指导，帮助客户更好地理解和应用各种安全产品与技术，以应对来自数据库和中间件领域的各种挑战(如身份管理、访问控制、目录与 J2EE 安全)。

Jahangir 同时还教授安全方面的课程，并且花费很多时间致力于数据库与中间件安全技术的结合，并最终为 Oracle 的用户群体和专业人士提供围绕身份管理、面向服务的架构和 IT 安全方面的支持。此外，他剩余的工作精力主要放在了与企业安全模型相关的新体系结构与解决方案原型的实验上。

如果不工作，他喜欢和家人、朋友以及自己那把传统的尼龙琴弦的吉他呆在一起。他拥有 Northeastern 的计算机科学学士学位，目前正在攻读 Georgetown 的 MBA。

Tyler Muth 是 Public Sector division 的主要技术人员之一。他在美国境内开办了许多 APEX 讨论班，为客户提供体系结构方面的建议，并与他们合作开发应用程序。在 Oracle Technology Days、Oracle User Groups 和他的博客 www.tylermuth.wordpress.com 中，可以看到大量由他提供的讲座。在 Oracle Technology Network 论坛上也不乏他的身影。

在担任现在角色前，Muth 是 APEX 开发小组的早期开发者之一，他在那里工作了 5 年多。他还担任了 Tom Kyte 多部技术书籍的技术审稿人，Tom kyte 是 asktom.oracle.com 的主要参与者，以及零重力生产系统的经理。

Patrick Sack, 技术副总裁，NSG Product Engineering, 负责 Oracle National Security Group 的 Product Engineering 分部。从事这一工作前，曾任 Oracle Protected Enterprise & Security Business 部门的副总裁。职业生涯的大部分时间都在 Oracle Consulting 集团中度过，期间为推动 Oracle 产品的创新发挥了巨大作用。

在 1988 年加入 Oracle 前，Sack 与许多客户组织一起工作过，包括美国国防部、CIA、商务部及其他许多的工业界组织机构。这使他对关键业务驱动力和过程有着非常广泛的了解。他在信息安全方面的专长源自对 Oracle 产品的丰富知识，以及参与过的众多客户项目，包括多层次的安全技术。

Sack 是 Oracle Information Assurance 技术、体系结构和解决方案方面的专家。他曾致力于为客户定制新的安全技术、特性和完整的解决方案，其中就包含用于遵从性的 Database Vault 技术。他是 Oracle 数据库产品中许多新安全特性的主要发起人，如 Oracle Database Vault、Oracle Audit Vault、Oracle Label Security 及细粒度的审计。在 Oracle 公司的美国专利注册中，经常能够看到他的名字，这些专利包括：多数据库安全政策、原级审计、Database Vault、

Mandatory Access Control Base、Dynamic Access Controls 以及审计和跨域安全等。

Sack 了解对于大多数组织机构而言，什么才是关键信息以及相关的安全问题，因此他始终强调数据的可用性、可追溯性和可达性。他拥有 State University of New York 的计算机科学学士学位。

Richard Wark, CISSP, Oracle Enterprise Solutions Group 的主要技术工程师之一，自 2004 年开始协助开发安全和身份管理的解决方案、演示以及培训系统。2002 至 2003 年间，他主要为圣安东尼奥市工作，协助管理一个大型的 ERP 项目。1996 年刚加入 Oracle 时，他是负责全国范围内空军客户的销售顾问。此后，他先后参与了包括银行、航空公司、金融机构和其他许多公司机构的数据安全项目。

在超过 15 年的 Oracle 产品生涯中，Wark 参与过美国政府，以及美国国防部、医疗卫生行业和其他商业组织的数据安全项目。通过不断挑战新的问题，他积累了非常丰富的知识和实践经验，成为了网络安全设计、安全政策创建、业务连续性规划、数据分类、安全数据库配置和大规模实现方面的专家。

加入 Oracle 前，Wark 曾为 Computer Sciences Corporation(CSC)和 Science Applications International Corporation(SAIC)工作，主要从事美国国防部的 Oracle 数据库项目。他的职业生涯的起点是 1991 年，当时他是一名 UNIX 管理员和 Informix 的 DBA。他拥有 University of Texas(San Antonio)的信息系统学士学位。

Bryan Wise 是 Oracle Public Sector 部门的 BI 解决方案专家，其职责是寻找安全和具有创造性的途径帮助组织机构更好地使用所拥有的数据。他 20 世纪 90 年代末加入 Oracle，此前曾服务于美国海军，负责管理所有的数据库，并领导海军核动力学院的应用程序开发和报表工作。

多年来，Wise 积极参与了 Oracle 社区的活动，在 Mid Atlantic Association of Oracle Professionals、Oracle Government Users Group 和 IOUG 的 Business Intelligence, Warehousing and Analytics Special Interest Group 都可以看到他做过的报告。同时，他也是 Oracle BI Publisher 博客的主要作者之一。

除了作为一名 Oracle 技术专家，Wise 将许多时间用于教学，包括开办 Oracle Business Intelligence 的讲习班、在海军核动力学院教授数学课程以及在 University of Maryland University College 教授数据库课程。他拥有 Brigham Young University 的数学学士学位以及 Regis University 的电子商务工程硕士证书。



致 谢

我首先要感谢为本书的诞生而辛勤工作的优秀作者团队，其中每一位都拥有关于本领域难以被超越的专业知识。尽管我写过关于 Oracle 安全的书，但我坚信本书汇集了关于 Oracle 安全技术的最佳实践、概念、思想和建议。我认识到说“我在写一本书”和实际写一本书之间的巨大差别，在此我要真心地感谢本书团队自始至终的努力，我们不仅顺利完成了本书，而且完成得非常出色。感谢 Richard、Pad、Scott、Hamza、Tyler 和 Bryan，感谢你们的坚持不懈和不辞辛劳的工作。

我还要感谢我在 Oracle 的同事和 Oracle 的管理团队。编写本书并不是我的本职工作，感谢他们的巨大支持和鼓励，使我能够获取可用于整个 Oracle 社区的信息。Mark Tatum 和 Glen Dodson 给了我特殊的帮助，而没有 Edward Screven 的支持，本书不可能最终完成。我的团队伙伴——Ed Montes、Fred Justice、Joe Mazzafrro 和 Mark Lunny——在本书的编写过程中一直和我并肩战斗。我要感谢 Vipin Samar 和 Paul Needham 的团队，多年来给予我巨大的支持。Tammy Bednar 则在本书编写的过程中扮演了重要的角色。

最后，我想感谢我的太太 Sandy，以及我的孩子们。Sandy，你再一次给予我这样多的时间和空间(来写这本书)，而我曾经说过再也不会这样了。我能感受到你的牺牲，我明白没有你的支持这一切不可能完成。对于孩子们，我想说真的对不起，在编写本书的过程中没有太多的时间来陪伴你们。我希望你们能明白，虽然爸爸有时候不得不投身辛勤的工作，但在我的心中，你们才是最重要的。我爱你们！现在开始，我们又可以一起捉迷藏了，准备好了吗？

——David Knox

Patrick Sack 想感谢 Glen Dodson 和 Ray Prescott, 他们提供了非常具有创造性的环境, 这样的环境为各种新想法提供了诞生的土壤, 并使这些想法不断发展完善, 最终成为具有商业价值的解决方案所需的文化。谢谢你们, Glen 和 Ray。

Patrick Sack 还要特别感谢 Scott Gaetjen 和 William (Bill) Maroulis 的睿智、积极的态度以及非常投入的专业精神。Scott 和 William 围绕 Database Vault 的概念, 开发了一系列关键的解决方案, 并最终启发了本书中的许多概念和案例。特别向 Scott 和 Bill 致以谢意!

我们想感谢如下的人士, 他们为本书提供了许多灵感和思路, 帮助我们扫清了道路上的障碍, 最终使 Database Vault 成为一个成熟的产品, 他们是 Glen Dodson、Raymond Prescott、Jay Gladney、Jon Bakke、Wendy Delmolino、David Knox、Rusty Austin、Gail Wright、Jack Brinson、Chi Ching Chui(以及他的团队)、Chon Lei、Ben Chang、Vipin Samar、Paul Needham、Daniel Wong、Kamal Tbeileh、Aravind Yalamanchi、Timothy Chorma、Frank Lee、Nina Lewis、Maria Chen、Cindy Li、Matthew Mckerley、Xiaofang Wang、Martin Widjaja、Sumit Jeloka、Patricia Huey、Ernest Chen、James Spiller、Tom Best、Duncan Harris、Howard Smith、Andy Webber 和 Jeff Schaumuller。

我们还想感谢 Oracle NSG(National Security Group, 国家安全工作组)的销售和咨询团队, 以及 Oracle Database Security(数据库安全)开发团队。正是 Oracle 中的这些工作组共同努力, 才将业界最好的安全产品和解决方案呈现在信息技术领域最需要这些技术的客户面前。

——Patrick Sack 与 Scott Gaetjen

我想感谢所有和我一起工作的伙伴, 因为他们的辛勤工作才使得本书最终诞生。特别感谢 David Knox 的指导和一直以来的支持与陪伴。还要感谢 Richard Wark、Pat Davies、Al Kiessel、Matt Piermarini 和 Colin Nurse 方方面面的支持与帮助。最后, 感谢我的两位同胞, Javed 与 Tabassum, 他们始终如一的支持是我前进的动力。感谢你们的爱、关心与陪伴。

——Hamza Jahangir



序 言

Oracle 业务的核心是信息：信息的管理、信息的利用及信息安全。作为 Oracle 的首席架构师，我不仅要确保我们的技术能够为客户创造价值，还包括使之以可靠的方式实现。在我经历过的每一次对客户经理的访问中，都会谈及安全问题，因为其重要性毋庸置疑。今天，安全、隐私及信息的监管对每个人来说都是最重要的事情。对于每个人，它们早已不是“锦上添花”的奢侈品，而是“不可或缺”的实际需求。正因为如此，人们一直都在努力寻找各种途径，确保自己已经完成了满足这些需求所需完成的任务。

本书讲解了从体系结构、设计场景到 Oracle 编码配置等多方面的内容，其目的是帮助 Oracle 客户实现可靠的信息安全系统。本书最引人注目之处在于它完全由 Oracle 内部的专家编写。几位作者都是每天为实际客户寻求安全方案的顶尖工程师。Oracle 的许多产品和技术正是诞生于在这些专家与一线客户实际接触所积累下的丰富经验之上的。

毫无疑问，您一定会在本书中找到非常深入和有价值的信息。建议您从头开始仔细地阅读本书，及时在重要的地方做好书签，当然，最重要的，应该是亲自动手，将其中的方法和建议付诸实践。

——Edward Screven
Oracle 公司首席架构师

目 录

第 I 部分 Oracle 数据库安全 新特性

第 1 章 安全蓝图与新思路	3
1.1 本书内容	4
1.1.1 背景信息	4
1.1.2 内容组织	5
1.2 当前的数据库安全技术	5
1.3 安全动机	8
1.3.1 敏感数据分类	9
1.3.2 原则	10
1.4 安全数据库架构建模	12
1.4.1 架构配置	12

1.4.2 对象所有者账户	13
1.4.3 用户访问账户	14
1.5 开始工作	15
1.5.1 用户配置	16
1.5.2 架构命名	17
1.5.3 安全体系结构检查表	18
1.6 小结	18
第 2 章 透明数据加密	21
2.1 口令学基础	22
2.1.1 加密的目标	22
2.1.2 基础知识	23
2.1.3 加密方法的选择	24
2.1.4 算法与密钥	24

2.2	对数据库中的数据加密	27
2.2.1	数据在何处“休眠”	28
2.2.2	数据保护	28
2.2.3	浏览数据	29
2.2.4	应用示例	31
2.2.5	数据库中的加密	31
2.3	TDE 解决方案	32
2.3.1	作为高级安全选项的 TDE	32
2.3.2	在 Oracle 10g 中配置 TDE	33
2.3.3	Oracle Wallet	34
2.3.4	TDE 的密钥管理	36
2.3.5	在新表中创建加密列	37
2.3.6	查看加密列	40
2.3.7	加密已有列	41
2.3.8	TDE 特别说明	43
2.4	表空间加密: Oracle 11g 的新特性	44
2.5	Oracle 11g 的配置	45
2.5.1	将 TDE 用于 PCI-DSS	46
2.5.2	操作考量	47
2.5.3	加密数据的导出和导入	50
2.5.4	与 HSM 的集成	52
2.6	小结	54
第 3 章	应用审计与 Audit Vault	55
3.1	监管的时代	56
3.2	出于非安全目的的审计	56
3.3	审计数据仓库	57
3.4	审计什么以及何时审计	61
3.4.1	指导原则	61
3.4.2	审计模式	62
3.4.3	其他最佳审计实践	64
3.5	从审计仓库到 Audit Vault	66
3.6	安装选项	68
3.6.1	安装 Audit Vault Server	68
3.6.2	安装 Audit Vault Collection Agent	68

3.6.3	安装说明	72
3.6.4	报表	76
3.6.5	警报	77
3.6.6	管理源数据库的审计政策	80
3.6.7	审计维护	82
3.7	小结	84

第 II 部分 Oracle Database Vault

第 4 章	Database Vault 介绍	89
4.1	安全缺口	90
4.1.1	权限账户的历史	90
4.1.2	安全补救	92
4.1.3	应该具有的安全特性	94
4.2	Database Vault 组件	96
4.2.1	因素	97
4.2.2	规则	97
4.2.3	领域	98
4.2.4	命令规则	100
4.3	安装 Oracle Database Vault	101
4.3.1	安装的 DBV 管理角色	101
4.3.2	管理 Oracle DBV 配置	102
4.3.3	默认的职责分离	106
4.3.4	默认的审计策略	110
4.3.5	与安全相关的默认 DBV 因素	111
4.4	小结	111
第 5 章	Database Vault 基础	113
5.1	领域	114
5.1.1	领域保护模式	118
5.1.2	创建第一个领域	119
5.1.3	领域组件	122
5.2	命令规则	132
5.2.1	命令规则组件	134
5.2.2	命令规则支持的命令	139

5.2.3	DBV CONNECT 命令 规则	139	6.6.6	基于访问路径或运行 上下文的因素	212
5.3	规则集	142	6.6.7	基于时间或顺序条件的 因素	213
5.3.1	规则集的评估模式	143	6.6.8	基于外部数据或事件的 因素	214
5.3.2	规则集审计	144	6.6.9	在应用程序中使用 DBV 因素	214
5.3.3	自定义事件处理程序	145	6.7	基于对象确定 DBV 领域及 领域对象	218
5.3.4	规则配置	147	6.7.1	为领域保护的對象配置 标准的对象级审计	220
5.3.5	DBV 规则集事件函数	150	6.7.2	在领域保护的對象上 配置 RLS	221
5.3.6	在规则集表达式中 使用的 DBV 因素	151	6.8	基于用例参与者确定账户、 角色和 DBV 领域授权	221
5.4	因素	152	6.8.1	DBV 的安全架构	222
5.4.1	创建因素	153	6.8.2	用户访问账户	225
5.4.2	因素标识	158	6.8.3	基于 DBV 安全架构的 示例实现	231
5.4.3	DBV 因素与 OLS 集成	169	6.8.4	后期的配置账户供应	261
5.5	DBV 安全应用程序角色	189	6.9	基于条件建立 DBV 命令规则	261
5.6	小结	193	6.10	基于条件建立 DBV 安全 应用程序角色	274
第 6 章	在自定义应用程序中 使用 DBV	195	6.11	小结	278
6.1	假想的数据库应用环境	196	第 7 章	在已有的应用程序中 使用 DBV	281
6.2	从需求到安全配置 文件设计	197	7.1	捕获审计信息的准备工作	282
6.3	需求分析技术: 用例与 场景	198	7.2	捕获审计数据	283
6.4	确定粗粒度的安全配置 文件	200	7.3	分析审计记录	283
6.5	确定细粒度的安全 配置文件	202	7.3.1	基于对象所有者账户 确定 DBV 领域	285
6.6	基于业务或系统条件确定 DBV 因素	203	7.3.2	DBV 领域保护的對象	286
6.6.1	集中管理为 DBV 因素和 规则设计的 PL/SQL 例程	205	7.3.3	DBV 领域授权	290
6.6.2	基于合规性的因素	209	7.3.4	为 DBV SAR 确定终端 用户访问账户和角色	304
6.6.3	基于利益冲突或职责分离 的因素	210			
6.6.4	基于组织策略的因素	211			
6.6.5	基于身份管理的因素	211			

- 7.3.5 基于条件确定 DBV 命令规则 305
- 7.3.6 基于业务或系统条件确定 DBV 因素 312
- 7.3.7 精化 DBV 策略设计 321
- 7.3.8 部署和验证 DBV 策略 321
- 7.4 将 DBV 与 Oracle 数据库功能集成 323
 - 7.4.1 Oracle Text 324
 - 7.4.2 Oracle Spatial 327
 - 7.4.3 表达式过滤器 328
 - 7.4.4 Oracle 流高级排队 331
 - 7.4.5 透明数据加密 335
 - 7.4.6 Oracle 恢复管理器 336
 - 7.4.7 在领域保护的架构中收集统计信息 338
 - 7.4.8 在领域保护的架构上使用 EXPLAIN PLAN 功能 338
- 7.5 DBV 数据库的高级监控和报警功能 339
 - 7.5.1 使用 OEM GC 对 DBV 进行监控和报警 339
 - 7.5.2 扩展 DBV 规则集的自定义事件处理程序 342
- 7.6 小结 347

第III部分 身份管理

- 第 8 章 身份管理体系结构设计 351
 - 8.1 理解与身份管理相关的问题 352
 - 8.1.1 中央发行机构 352
 - 8.1.2 身份验证 353
 - 8.1.3 身份传递 353
 - 8.2 构建身份管理体系结构 354
 - 8.2.1 身份管理发现 354
 - 8.2.2 身份管理模式 359

- 8.3 Oracle 身份管理解决方案 364
 - 8.3.1 用户供应 364
 - 8.3.2 目录管理 365
 - 8.3.3 身份验证管理 366
 - 8.3.4 授权管理 370
 - 8.3.5 角色挖掘和管理 373
- 8.4 小结 374
- 第 9 章 Oracle 身份管理器 375
 - 9.1 用户供应面临的挑战 375
 - 9.2 OIM 概况 376
 - 9.2.1 用户 377
 - 9.2.2 用户组 377
 - 9.2.3 组织 378
 - 9.2.4 访问策略 378
 - 9.2.5 资源对象 379
 - 9.2.6 IT 资源 380
 - 9.3 用户供应进程 380
 - 9.3.1 全权委托的账户供应 380
 - 9.3.2 自助式供应 381
 - 9.3.3 基于工作流的供应 383
 - 9.3.4 访问策略驱动的供应 384
 - 9.4 用户供应集成 386
 - 9.4.1 预置的连接器的 386
 - 9.4.2 通用技术连接器 386
 - 9.5 调和集成 387
 - 9.6 合规性解决方案 388
 - 9.6.1 验证 388
 - 9.6.2 访问报表 389
 - 9.7 OIM 的部署 390
 - 9.8 小结 392
- 第 10 章 Oracle 目录服务 393
 - 10.1 身份管理与 LDAP 目录 394
 - 10.2 OID 394
 - 10.2.1 OID 体系结构 394
 - 10.2.2 OID 同步 395
 - 10.3 目录虚拟化和 OVD 397
 - 10.3.1 OVD 101 397

10.3.2	OVD 体系结构	398	12.1.2	自定义的用户名与 口令表	446
10.4	使用 OVD	400	12.1.3	授权模式	452
10.4.1	安装 OVD	400	12.2	SQL 注入	455
10.4.2	创建新的 OVD 服务器	400	12.2.1	示例 1: 错误的方法	456
10.4.3	使用本地存储适配器 初始化虚拟 LDAP 树	401	12.2.2	示例 2: 正确的方法	458
10.4.4	集成 OVD 与活动目录 LDAP 服务器	403	12.3	跨站点脚本	460
10.4.5	集成 OVD 与 Oracle 关系数据库	405	12.4	使用数据库安全功能	468
10.4.6	在 OVD 中连接信息	408	12.4.1	VPD	468
10.5	小结	414	12.4.2	细粒度审计	473
			12.5	小结	480
第 IV 部分 Oracle APEX 和 Oracle 商业智能 安全			第 13 章 安全访问 Oracle BI		
第 11 章 APEX 中以 Web 为中心的 安全			481		
11.1	APEX 环境介绍	417	13.1	商业智能安全面临的挑战	482
11.1.1	组件和配置	418	13.1.1	系统用户	483
11.1.2	体系结构	418	13.1.2	数据仓库的安全与事务 系统的安全	483
11.1.3	APEX 与数据库角色	421	13.2	安全的各方面	485
11.1.4	APEX 会话	422	13.3	Oracle BI 访问数据的机制	486
11.2	增强 APEX 实例的安全性	423	13.3.1	体系结构	486
11.2.1	APEX 安全设置	423	13.3.2	连接池	487
11.2.2	增强应用服务器层的 安全性	427	13.3.3	变量	489
11.2.3	使用 mod_security 阻止 基于 Web 的攻击	433	13.4	身份验证与授权	492
11.2.4	SSL/TLS 技术	435	13.4.1	身份验证选项	492
11.3	保护 APEX 数据库架构	441	13.4.2	授权	498
11.4	小结	444	13.5	单点登录	506
第 12 章 APEX 安全编程实践			13.5.1	SSO 选项	506
12.1	身份验证与授权	446	13.5.2	SSO 设置的注意事项	506
12.1.1	身份验证模式	446	13.5.3	使用 Oracle 访问管理器 实现 SSO	507
			13.6	安全环境中的部署	511
			13.6.1	SSL Everywhere	511
			13.6.2	加密的外向连接	512
			13.7	BI 缓存的安全	513
			13.8	面向公众的应用程序	514
			13.8.1	防火墙和隔离区	514
			13.8.2	公共用户	514
			13.9	小结	515

第 14 章 Oracle BI 内容与数据的安全

安全 517

14.1 Web 目录内容安全 518

14.1.1 Web 目录组 518

14.1.2 基于文件夹的安全 519

14.1.3 iBot 安全 519

14.1.4 BI Publisher 目录内容的安全 521

14.2 向数据库传递身份 521

14.3 Oracle BI 表示数据的安全 523

14.3.1 BI 服务器中的安全策略 524

14.3.2 集成 Oracle BI 与数据库安全策略 532

14.3.3 决定何时使用 VPD 或 Oracle BI 的行级安全 539

14.4 Oracle BI 与 Database Vault 541

14.4.1 因素与 Oracle BI 541

14.4.2 领域与 Oracle BI 542

14.5 审计 543

14.5.1 效用跟踪 544

14.5.2 数据库审计 545

14.5.3 结合效用跟踪和数据库审计 546

14.6 具有安全风险的 BI 功能 547

14.6.1 默认权限 547

14.6.2 以代理身份运行 548

14.6.3 直接数据库请求 551

14.6.4 Advanced 选项卡 554

14.6.5 直接访问 BI 服务器 554

14.6.6 Web 服务访问 555

14.7 小结 555

附录 A 使用 Oracle BI 的示例 557