Oracle Audit Vault

Oracle 白皮书
2008 年 7 月

企业安全性面临的挑战

满足合规性要求及降低安全侵犯风险是现在企业面临的首要安全挑战。对大量安全事件的调查显示，及时调查审计数据有助于尽早检测未授权的活动并降低由此带来的财务损失。政府和学术机构的各项研究和调查得出的结论是，相当大一部分数据侵犯都来自内部人员，即那些对系统及其数据至少具有一定级别访问权限的内部人员。世界各地的政府已经颁布了各种与财务控制、医疗保健和隐私相关的法规。

美洲
- **Sarbanes-Oxley (SOX)**
- **医疗保险携带和责任法案 (HIPAA)**
- **CA SB 1386 和其他州立隐私法律**
- **支付卡行业数据安全标准**
- **FDA CFR 21 Part 11**
- **FISMA（联邦信息安全管理法）**

欧洲、中东和非洲
- **欧盟隐私指导方针**
- **英国 2006 年公司法**

亚太地区
- **金融工具交换法 (J- SOX)**
- **第九号法案：审计改革和公司信息披露法案（澳大利亚）**

全球
- **国际会计标准**
- **新巴塞尔协议（全球银行）**
- **OECD 公司治理指引**

图 1.0 — 隐私与合规性

Sarbanes-Oxley (SOX)、医疗保险携带和责任法案 (HIPAA) 等众所周知的法规以及支付卡行业数据安全标准 (PCI-DSS) 等行业规范使得信息保护已成为企业面临的首要问题。随着安全威胁变得越来越复杂，监视功能正成为纵深防御架构越来越重要的组成部分。当前，使用审计数据作为安全资源在很大程度上还是一个手动过程，需要管理员和审计人员从多个位置手动收集审计数据。

Oracle Audit Vault

Oracle Audit Vault 自动将审计数据整合到安全的信息库中，实现了高效的监视和报告。Oracle Audit Vault 是一个能够提供安全信息库、内置报告、事件警报和职责分离的功能强大的解决方案。基于 Oracle 行业领先的技术而构建，Oracle Audit Vault 使用 Oracle 数据安全性对审计数据进行端到端保护。Oracle Audit Vault 使用 Oracle 分区和压缩技术实现了高度可伸缩性。Oracle Audit Vault 的最新版本提供增强的现成合规性报告和审计收集，其中包括对 Microsoft SQL Server 2000 和 2005 数据库的支持。

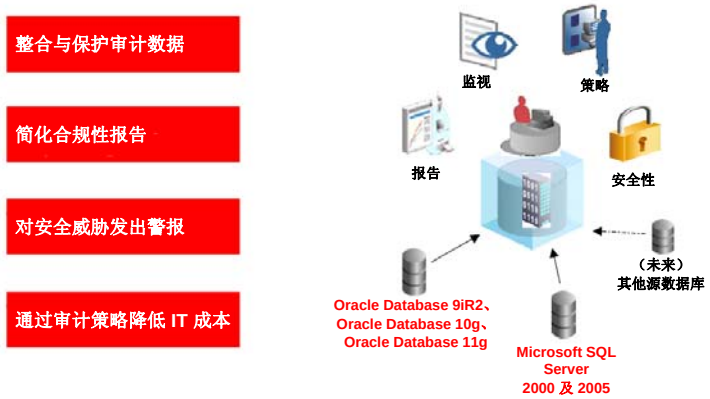

图 2.0 — Oracle Audit Vault 概述

Oracle Audit Vault 的核心是基于 Oracle 行业领先的数据仓库技术构建的并由 Oracle 行业领先的安全产品保护的安全数据信息库。内置的报告和事件警报通过减少检测潜在问题所需的时间和人力帮助企业更好地满足外部法规和内部策略要求，并能够显示强制性控制正在有效执行。通过 Oracle Audit Vault 控制台，数据安全管理员和审计人员可以直接管理、比较和供应整个企业的 Oracle 数据库审计设置，从而降低总体维护成本。

合规性和安全性报告

Oracle Audit Vault 为监视包括特权用户活动和数据库结构更改在内的各种活动提供了功能强大的内置报告。这些报告提供对活动的可见性以及关于人员、事件、时间和地点的详细信息。Oracle Audit Vault 最新版本提供基于广泛流行的 Oracle Application Express 技术构建的激动人心的新报告界面。新的报告提供易于使用的界面，能够创建丰富多彩的图表并定制报表格式。可以重新排列或删除报告列。通过建立规则可以自动高亮显示特定行，使报告用户可以迅速发现可疑或未授权活动。报告将包括 Oracle 和 Microsoft SQL Server 数据库的审计信息，提供整个企业内活动的总体信息。Oracle Audit Vault 提供大量按领域（如合规性和警报）分类的标准审计评估报告。这些现成的报告包括数据库帐户管理、角色和权限管理、对象管理和登录失败的相关信息。还可以使用 Oracle Business Intelligence、Oracle BI Publisher 和第三方报告工具构建其他报告，以满足特定的合规性和安全性要求。有关信息库表的详细信息可以参考 Oracle Audit Vault 管理员指南。

图 3.0 — Oracle Audit Vault 报告界面

安全和监视警报

Oracle Audit Vault 为安全人员提供了对试图进行未授权访问或滥用系统权限的活动进行检测并发出警报的功能。Oracle Audit Vault 可以为系统定义和用户定义的审计事件生成警报。Oracle Audit Vault 持续监视收集到的审计数据并评估活动是否符合定义的警报条件。警报可与任何可审计的数据库事件相关联，包括更改应用程序表和创建特权用户等系统事件。例如，当有人试图访问敏感的业务信息时会生成警报。Oracle Audit Vault 界面提供了导致警报的各种活动的图形化摘要。其中包括警报活动概要和警报数量最多的一些数据源。Oracle Audit Vault 用户可以点击概要图形下钻到更详细的报告。用于生成报告的警报按其关联的源进行分组。还可以按事件所属的事件类别和警报的严重程度（警告、严重或信息）进行分组。

审计策略

Oracle Audit Vault 对 Oracle 数据库审计设置进行集中管理，以简化 IT 安全人员和内部审计人员的工作。很多企业需要针对特定的审计事件或审计策略对系统实施主动监视。在大多数环境下，需要手动定义和管理这些审计设置。IT 安全人员必须与内部审计人员一起定义数据库的审计设置。此外，内部审计人员需要定期与 IT 安全人员一起确认审计设置未被更改。

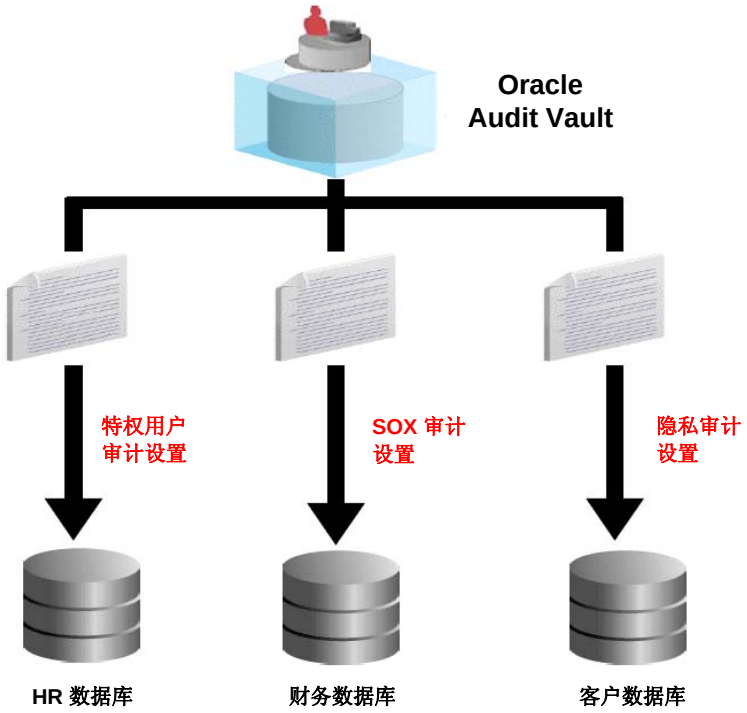

图 4.0 — Oracle Audit Vault 策略

有时将一个给定数据库上使用的审计设置的集合叫做“审计策略”。Oracle Audit Vault 提供了从 Audit Vault 控制台集中定义审计策略的功能。这样内部审计人员和 IT 安全人员可以更轻松地管理整个企业内的审计设置并向外部审计人员展示合规性和重复控制。

安全性和可伸缩性

审计数据是业务活动的重要记录。必须保证审计数据不被更改，以确保基于审计数据的报告和调查的完整性。Oracle Audit Vault 将审计数据存储在使用 Oracle 行业领先的数据库安全技术构建的安全信息库中。及时将审计数据从源系统传输给 Oracle Audit Vault 对于防止入侵者修改审计数据和掩盖行踪至关重要。可以将 Oracle Audit Vault 配置为近乎实时地传输审计数据。Oracle Audit Vault 可以保护审计数据在网络传输和 Oracle Audit Vault 内部传输期间的安全。在从源系统传输审计数据期间，可以对其进行加密，以防任何人在传输期间读取或篡改数据。

在 Oracle Audit Vault 内部，对审计数据的访问将基于职责分离原则进行严格控制。通过 Oracle 分区可以根据业务需求对审计数据进行物理分区。可以对 Oracle Audit Vault 进行 Oracle 真正应用集群 (RAC) 授权，以提高可伸缩性和可用性。

总结

审计数据在帮助组织维护高安全性和满足内部及外部策略要求方面发挥着越来越重要的作用。对大量安全事件的调查显示，对活动和敏感数据访问进行监视可以显著降低多种安全侵犯对财务的影响。Oracle Audit Vault 通过自动将审计数据整合到安全、可伸缩的信息库中，帮助组织提高安全性。按照功能领域（如合规性）分类的大量现成的报告使安全和法规执行人员能够轻松访问 Oracle 和 Microsoft SQL Server 数据库中的审计数据。内置的警报功能使安全和法规执行人员能够快速检测和调查潜在问题。集中的策略简化了整个企业内的数据库审计设置并有助于显示合规性证明。借助 Oracle Audit Vault 提供的详细文档，可以使用 Oracle BI Publisher 或其他第三方报告工具创建定制报告。Oracle Audit Vault 未来版本还将包括对其他数据库和数据源的支持。

甲骨文（中国）软件系统有限公司

北京总部

地址：北京市朝阳区建国门外大街1号，国贸大厦2座2208室
邮编：100004
电话：(86.10) 6535-6688
传真：(86.10) 6505-7505

北京上地6号办公室

地址：北京市海淀区上地信息产业基地，上地西路8号，上地六号大厦D座702室
邮编：100085
电话：(86.10) 8278-7300
传真：(86.10) 8278-7373

上海分公司

地址：上海市卢湾区湖滨路222号，企业天地商业中心1号楼16层
邮编：200021
电话：(86.21) 2302-3000
传真：(86.21) 6340-6055

广州分公司

地址：广州市天河北路233号，中信广场53楼5301&5308室
邮编：510613
电话：(86.20) 8513-2000
传真：(86.20) 3877-1026

成都分公司

地址：成都市人民南路二段18号，四川川信大厦20层A&D座
邮编：610016
电话：(86.28) 8619-7200
传真：(86.28) 8619-9573

大连分公司

地址：大连软件园东路23号，大连软件园国际信息服务中心2号楼五层502号A区
邮编：116023
电话：(86.411) 8465-6000
传真：(86.411) 8465-6499

济南分公司

地址：济南市泺源大街150号，中信广场11层1113单元
邮编：250011
电话：(86.531) 8518-1122
传真：(86.531) 8518-1133

甲骨文软件研究开发中心（北京）有限公司

地址：北京市海淀区中关村软件园孵化器2号楼A座一层
邮编：100094
电话：(86.10) 8278-6000
传真：(86.10) 8282-6455

甲骨文研究开发中心（深圳）有限公司

地址：深圳市南山区高新南一道飞亚达大厦16层
邮编：518057
电话：(86.755) 8396-5000
传真：(86.755) 8601-3837

沈阳分公司

地址：沈阳市沈河区青年大街219号，华新国际大厦17层D单元
邮编：110016
电话：(86.24) 2396 1175
传真：(86.24) 2396 1033

南京分公司

地址：南京市玄武区洪武北路55号，置地广场19层1911室
邮编：210028
电话：(86.25) 8476-5228
传真：(86.25) 8476-5226

杭州分公司

地址：杭州市西湖区杭大路15号，嘉华国际商务中心702室
邮编：310007
电话：(86.571) 8717-5300
传真：(86.571) 8717-5299

西安分公司

地址：西安市高新区科技二路72号，零壹广场主楼1401室
邮编：710075
电话：(86.29) 8833-9800
传真：(86.29) 8833-9829

福州分公司

地址：福州市五四路158号，环球广场1601室
邮编：350003
电话：(86.591) 8801-0338
传真：(86.591) 8801-0330

重庆分公司

地址：重庆市渝中区邹容路68号，大都会商厦1611室
邮编：400010
电话：(86.23) 6370-8898
传真：(86.23) 6370-8700

深圳分公司

地址：深圳市南山区高新南一道飞亚达大厦16层
邮编：518057
电话：(86.755) 8396-5000
传真：(86.755) 8601-3837

甲骨文亚洲研发中心（上海）

地址：上海市杨浦区淞沪路290号，创智天地10号楼512-516单元
邮编：200433
电话：86-21-6095 2500
传真：86-21-6095 2555

Oracle Audit Vault
2008 年 7 月
作者：Tammy Bednar、Paul Needham

公司网址：http://www.oracle.com（英文）
中文网址：http://www.oracle.com/cn（简体中文）
销售中心：800-810-0161
售后服务热线：800-810-0366
培训服务热线：800-810-9931

欢迎访问：
http://www.oracle.com（英文）
http://www.oracle.com/cn（简体中文）