ORACLE DATABASE 12c

ORACLE ADVANCED SECURITY

具备加密和数据编辑特性，实现隐私与合规性

加密特性

- 对数据库列或整个表空间中的应用程序数据加密
- 内置加密密钥生命周期管理，配有辅助的密钥轮换
- 行业标准算法，包括 AES（128、192 和 256 位密钥）
- Intel® AES-NI 和 Oracle SPARC T 系列提供硬件加速
- Oracle Exadata 集成，与 Oracle RMAN、ASM、RAC、Advanced Compression、Active Data Guard 和 GoldenGate 等数据库技术直接集成

编辑特性

- 动态编辑，限制应用程序中敏感信息的暴露
- 声明式编辑策略，在数据库中集中管理
- 多个编辑转换，可用于不同的应用场景
- 使用 Oracle Enterprise Manager 进行策略管理，与 Oracle SQL Developer 直接集成

客户收益

- 在当前和原有应用程序中保持透明且一致的数据安全性
- 高速实现
- 易于部署和管理
- 完全支持 Oracle Multitenant 选件

Oracle Database 12c 中包含的 Oracle Advanced Security 提供业界领先的加密和数据编辑功能，对于保护敏感应用程序数据至关重要。透明数据加密和数据编辑有助于防止未经授权的用户访问应用程序层、操作系统、备份介质和数据库导出中的敏感信息。Oracle Advanced Security 完全支持 Oracle Multitenant 选件，并与 Oracle 集成式系统相集成，从而实现无与伦比的性能。

Oracle Advanced Security 概述

保护数据需要使用一种纵深防御的方法，其中包括预防、检测和管理控制。Oracle Advanced Security 预防控制可帮助满足众多的法规要求、防止数据侵犯以及保护隐私相关信息。例如，信用卡数据可在存储中自动加密，同时在离开数据库之前在查询结果中自动动态编辑。这两种功能对遵守隐私法规和支付卡行业数据安全标准（PCI-DSS）至关重要。

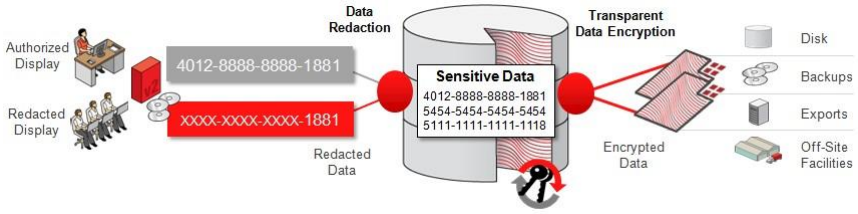

图 1. Oracle Advanced Security

透明数据加密

透明数据加密 (TDE) 通过加密静态数据，可防止从数据库环境之外对敏感数据进行未经授权的访问。通过检查数据库文件的内容，防止特权和未经授权的操作系统用户直接访问敏感信息。此外，针对数据库存储介质和备份被盗、丢失或不当弃用的情形，TDE 也能提供保护。

由于数据写入存储时自动加密，从存储中读取时自动解密，所以该解决方案对应用程序是透明的。在数据库层和应用程序层实施的访问控制将保持有效。SQL 查询永远不会改变，且不需要更改任何应用程序代码或配置。

TDE 利用 Oracle 数据库缓存优化，因此加密和解密过程非常快速。此外，TDE 还利用 Intel® AES-NI 和 Oracle SPARC T 系列平台中基于 CPU 的硬件加速，包括 Oracle Exadata 和 SPARC SuperCluster。TDE 还进一步受益于 Exadata 智能扫描和 Exadata 混合列压缩，前者使之可在多个存储单元上并行快速解密数据，后者使之减少了执行的加密操作的总次数。

ORACLE 甲骨文

相关产品

Oracle Database 12*c* 纵深防御安全性解决方案：

- Oracle Database Vault
- Oracle Data Masking
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

TDE 提供双层的加密密钥管理架构，包括数据加密密钥和主加密密钥。主密钥存储在数据库之外的一个 Oracle Wallet 中。内置的密钥管理功能提供辅助的密钥轮换特性（无需重新加密所有数据），并对密钥的整个生命周期进行管理。

TDE 可轻松部署。默认情况下，作为数据库安装的一部分进行安装。现有数据可以通过使用 Oracle 联机表重新定义进行加密，无需生产系统停机，或在维护期间脱机加密。此外，TDE 还可随时直接与 Oracle 自动存储管理协同工作。

编辑敏感数据以适当显示

数据编辑可以在应用程序显示敏感数据之前在查询结果中对其进行选择性地动态编辑，从而未经授权的用户无法查看这些敏感数据。它支持在访问相同数据的各个应用程序模块之间一致地编辑数据库列。数据编辑可将对应用程序的更改降至最低，因为它不改变内部数据库缓冲区、缓存或存储中的实际数据，而且当经过转换的数据返回到应用程序时，将保留原始数据的类型和格式。数据编辑不会影响数据库运营活动，如备份和恢复、升级和修补以及高可用性集群。

与依赖应用程序编码和新软件组件的旧式方法不同，数据编辑策略直接在数据库内核中实施。声明式策略可应用不同的数据转换方式，如部分编辑、随机编辑和完全编辑。编辑可以是有条件的、基于数据库跟踪的或由应用程序传递给数据库的不同因素，如用户标识、应用程序标识或客户端 IP 地址。编辑格式库为常用类型的敏感信息（如信用卡号和身份证号）提供预配置的列模板，供您从中选择。一旦启用后，策略将立即实施，即使是活动会话也是如此。

保护企业数据

TDE 和数据编辑作为纵深防御安全策略的一部分，非常容易管理。Oracle Enterprise Manager 提供便捷、全面的管理控制台。还提供命令行 API。

TDE 和数据编辑完善了其他数据库特性，同时还可与常用 Oracle 数据库工具相集成。例如，TDE 表空间加密可与 Oracle Recovery Manager 无缝协作，以生成经过加密和压缩的备份。

Oracle Advanced Security 完全支持 Oracle Multitenant 选件。当可插拔数据库移至新的多租户容器数据库时，TDE 和数据编辑仍将有效，可在运输过程中保护可插拔数据库。