Oracle透明数据加密 (TDE)

--- 数据安全实战演练系列(一)

公益讲座11：00准时开始，请大家先浏览云技术微信公众号技术文章。资料会在各群同步发布，已入群客户请勿重复入群！

20-21

数据库和云讲座群

甲骨文云技术公众号

B站专家系列课程

* 活动最终解释权归甲骨文公司所有

基于 Oracle 数据库
免费企业数据健康检查

- 及时了解数据库健康状况，发现并解决潜在问题
- 维护数据库系统良好状态，保护数据资产的安全
- 提升数据库性能、稳定性和安全性，降低业务风险

免费咨询热线：

400-699-8888

Oracle 透明数据加密 (TDE)

甲骨文技术公益课 - 数据库专场

Jim Kong

2023 年 6 月 30 日 11:00

线上直播

ORACLE

深入了解Oracle透明数据加密(TDE)

数据安全实战演练系列(一)

孔令鑫

2023/06/30

内容

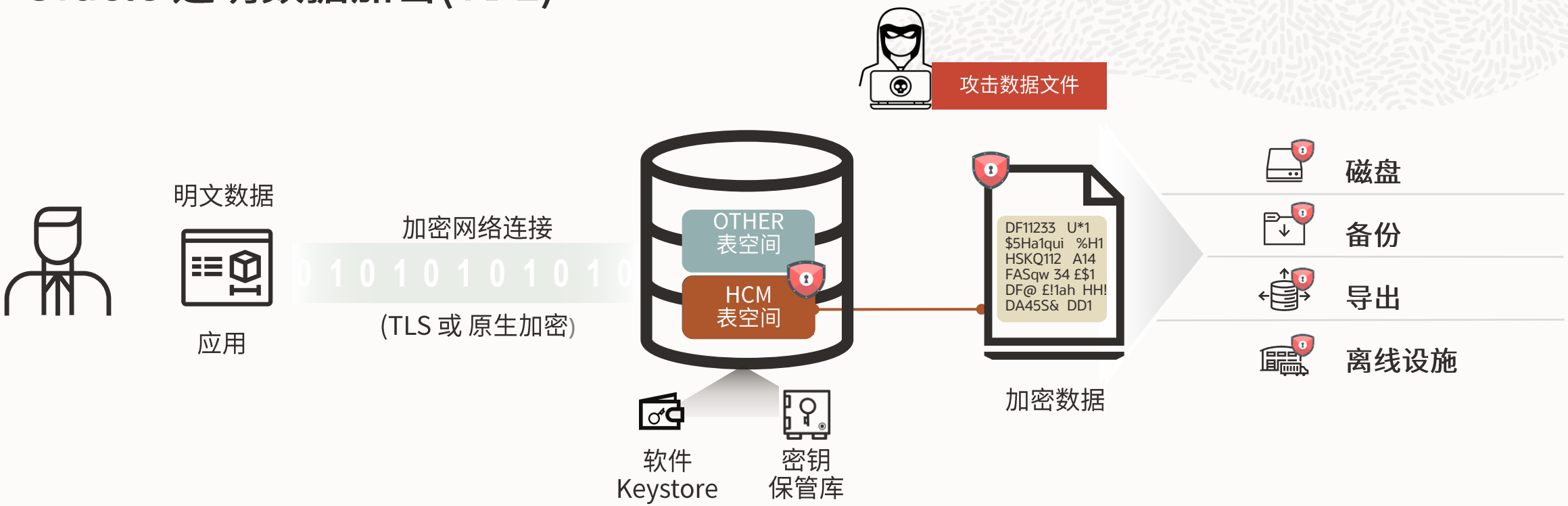
深入了解Oracle透明数据加密(TDE)

- TDE 架构以及持续优化
- TDE 如何使用
- TDE 动手实践
- TDE 配置注意事项
- TDE 优势

TDE架构以及持续优化

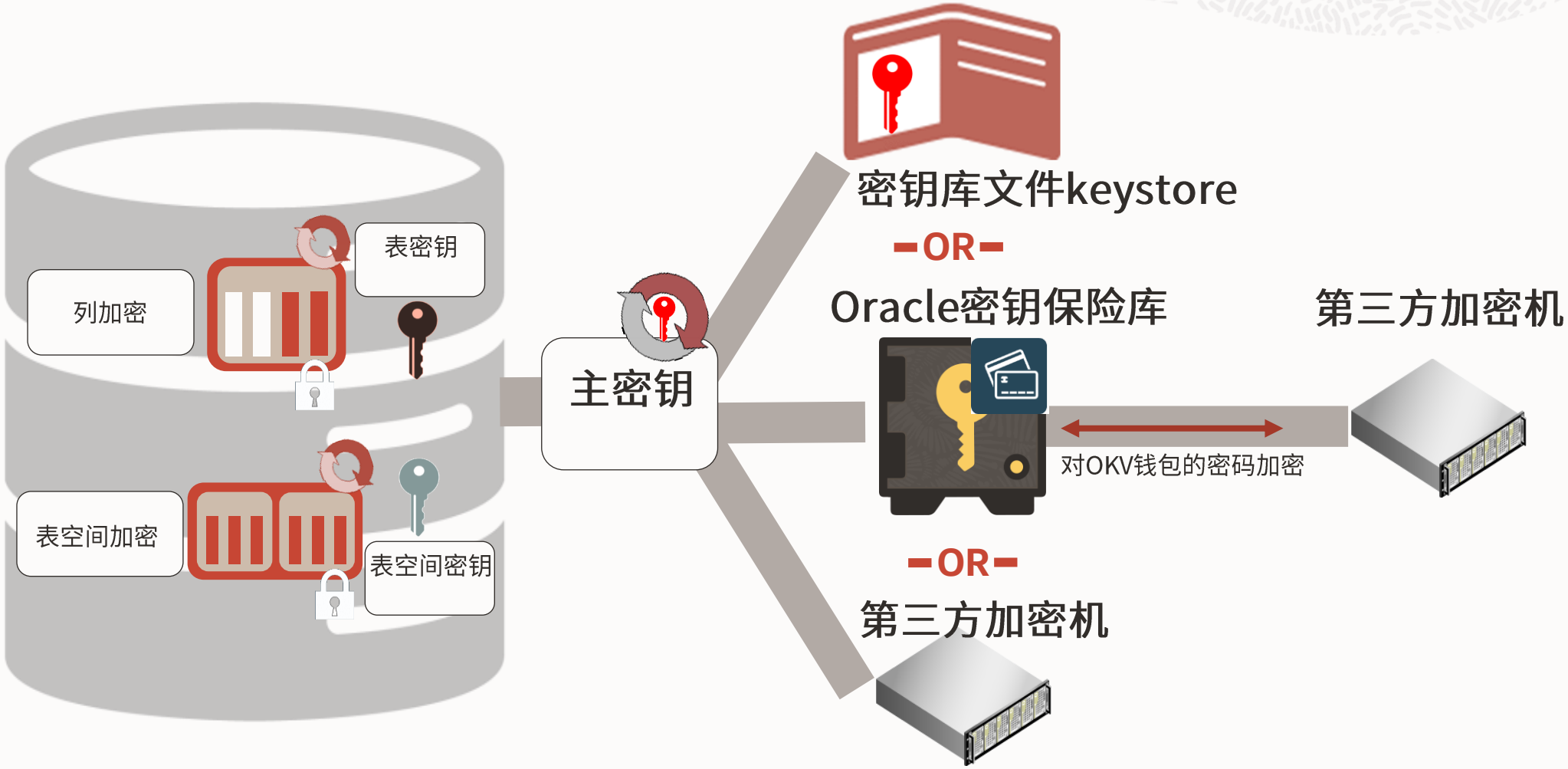
高级安全

Oracle 透明数据加密(TDE)



Oracle数据库默认情况下，数据文件未加密。
静态数据，磁盘文件、备份、导出数据进行加密
执行查询时，加密后的数据将为请求者透明解密，无需改变应用

Oracle透明数据加密--架构及密钥管理



Oracle透明数据加密--持续增强

Oracle Database 12.1.0.2, 12.2.0.1

- 在线表空间加密和主密钥切换
- 引入ARIA和SEED加密算法
- 职责分离：DBA无需知道keystore密码
- 对新的表空间进行默认加密

Oracle Database 18c

- WALLET_ROOT取代了对sqlnet.ora的依赖性
- 用户可以使用自己的密钥作为主密钥
- 支持加密数据字典表中的敏感数据
- Rman：restore|duplicate as encrypted|decrypted用于控制恢复和复制操作中否需要加解密。

Oracle Database 19c

- 每个PDB的密钥库
- 设置DB默认加密算法(*)
- 加密SYSTEM、SYSAUX、TEMP和UNDO表空间
- 加密LOB定位器签名密钥

Oracle Database 21c

- 改进职责分离：数据库保险库命令规则现在适用于ADMINSTER KEY MANAGEMENT语句
- 可以对移动的pdb数据库进行加密保护
- 通过DBCA创建加密的数据库

TDE支持Oracle数据库的所有核心功能

数据库技术	产品集成	TDE SUPPORT
High Availability	Real Application Clusters, Sharding, (Active) Data Guard	
Backup and Restore	Oracle RMAN, Oracle Secure Backup	
Import and Export	Oracle Data Pump	
Database Replication	Oracle GoldenGate	
Pluggable Databases	Oracle Multitenant Option	
Engineered Systems	Oracle Exadata Smart Scan	
Storage Management	Oracle ACFS	
Data Compression	Oracle Standard, Advanced, Exadata Hybrid Columnar Compression	

如何使用 TDE

高级安全

表空间加密 vs. 列加密

TDE可以对单个表列和表空间进行加密

加密表空间的优点:

- 不需要跟踪要加密的列和列的特征，如索引和约束等
- 不干扰Exadata混合列压缩（EHCC）和 smart scan
- 利用英特尔（AES-NI）和SPARC CPU中的特殊指令加速加密操作，速度非常快

加密现有数据

1. 将数据重新组织到一个加密的表空间中
   - 从未加密的表空间导出，并导入到加密的表空间
   - 离线表移动
     - ALTER TABLE <table_name> MOVE TABLESPACE <encrypted tablespace name>;
   - 在线表移动
     - ALTER TABLE <table_name> MOVE ONLINE TABLESPACE <encrypted tablespace name>;

2. 将现有的表空间从未加密的转换为加密的
   - 离线表空间转换
     - ALTER TABLESPACE <unencrypted tablespace name> ENCRYPTION OFFLINE USING ‘AES256’ ENCRYPT;
   - 在线表空间转换
     - ALTER TABLESPACE <unencrypted tablespace name> ENCRYPTION ONLINE USING ‘AES256’ ENCRYPT FILE_NAME_CONVERT = (‘<existing file name>, ‘<new file name>);

表空间加密转换

问题	Offline Encryption	Online Encryption
什么时候可以运行转换?	表空间处于离线 数据库处于挂起阶段(mount)	表空间处于在线状态 数据库处于读写模式(open , read/write)
Data Guard环境下，如何加密转换?	手动加密主库和备库 先手动加密备库，然后切换主备，以减少停机时间	手动加密主库后，备库会自动完成加密，无法直接在备库上运行在线加密
需要额外的存储空间吗?	No	Yes, 加密转换过程中会创建一个新的加密文件，并在完成后删除原始文件
可以并行运行加密操作吗?	Yes, 可以在多个用户会话下,对数据文件级别运行并行的加密转换。（ALTER DATABASE DATAFILE 'user_01.dbf' ENCRYPT）	Yes, 可以在多个用户会话下，对表空间级别运行并行加密转换。
如果加密转换的SQL语句未能完成，该如何处理?	重新运行加密或解密SQL语句，以确保表空间内的所有数据文件都被一致加密或解密。	可以将表空间解密回原来的状态，或者通过使用ALTER TABLEPSPACE的ENCRYPTION ONLINE FINISH ENCRYPT子句恢复加密。
Available in	Release 11.2.0.4 +	Release 12.2 +

加密总是会带来一些开销

对查询响应时间的影响

表空间加密

- 通常很低，特别是在Exadata上。
- 极少情况下（比如较低的缓冲区使用）会较高。

对数据库存储的影响

- 对于表空间加密，影响非常小，每个数据文件增加一个数据块
- 对于列加密，增加1到52个字节的长度（填充SALT或MAC）

性能受到加密的目标影响

表空间

- 加密整个表空间（所有数据文件）
- 表空间密钥（表空间中所有数据文件使用的相同密钥）
- 默认算法: AES 128
- 数据在从数据文件读入buffer cache或通过直接路径读取时被解密
- 对性能的影响往往是一致的，并且不改变查询的执行计划

列

- 加密一个表中的一个或多个列
- 表的密钥（一个表中所有加密的列使用的是同一个密钥）
- 默认算法。AES 192
- 数据在被移入PGA时被解密（在buffer cache中保持加密）。
- 对性能的影响因查询执行计划的不同而有很大差异。在某些情况下，索引可能无法使用，导致查询退回到全表扫描。

调整TDE性能的建议

Column Encryption

- 加密一小部分列
- 可以选择关闭完整性检查
- 在完成加列密后，重建列索引

Tablespace Encryption

- 适当地设置SGA大小
- 使用Advanced Compression 或 Columnar Compression来压缩数据
- 使用提供CPU加密加速的硬件和软件
- 如果在Exadata上运行，确保开启smart scan

TDE常问问题

问：透明数据加密 (TDE) 提供什么?

- TDE 透明地加密 Oracle 数据库中的静态数据。 它可以阻止操作系统未经授权尝试访问存储在文件中的数据库数据，而不会影响应用程序使用 SQL 访问数据的方式。

问：TDE 对业务应用程序是否有影响?

- TDE 对业务应用程序是透明的，不需要更改应用程序。 加密和解密发生在数据库存储级别，对应用程序使用的 SQL 接口没有影响（无论是入站 SQL 语句，还是出站 SQL 查询结果）。

问：应该使用 TDE 列加密还是 TDE 表空间加密?

- 我们的建议是使用 TDE 表空间加密。 在大多数情况下，TDE 表空间加密具有更好、更一致的性能特征。

问：数据在网络上是否保持加密状态?

- 使用 TDE 加密的数据在从数据库文件中读取时被解密。 如果此数据在网络上传输，它将以明文形式存在。 对于网络数据加密可以使用 Oracle 的网络加密或 TLS 对传输中的数据进行加密。 这将加密通过 SQL*Net 进出 Oracle 数据库的所有数据。

TDE常问问题

问：TDE 可以使用哪些加密算法?

- TDE 支持 AES256、AES192（TDE 列加密的默认值）、AES128（TDE 表空间加密的默认值）、ARIA128、ARIA192、ARIA256、GOST256、SEED128 和 3DES168

问：是否可以使用第 3 方加密算法代替 TDE 提供的算法?

- 不支持插入其他加密算法
- 从 Oracle Database 18c 开始，用户可以创建用户定义的主加密密钥，而不是要求始终在数据库中生成 TDE 主加密密钥（自带密钥 (BYOK)）。

问：TDE 与 Oracle 已经提供的加密工具包有何不同?

- DBMS_CRYPTO 包可用于手动加密数据库中的数据。 这种方法需要付出大量工作来管理加密解密逻辑， 并产生性能开销。 TDE 表空间加密不需要更改应用程序，对最终用户透明，并提供自动化的内置密钥管理

TDE 动手实践

高级安全

演示

1. 如何启用透明数据加密
2. 如何创建密钥库或钱包
3. 如何加密现有表空间
4. 如何加密新创建的表空间
5. 如何替换密钥

TDE配置注意事项

高级安全

配置TDE的注意事项

1. 新的TDE初始化参数WALLET_ROOT和TDE_CONFIGURATION
   - 通过sqlnet.ora中的条目进行的TDE设置已被弃用
     - ENCRYPTION_WALLET_LOCATION
   - 配置了WALLET_ROOT后，以下的目录结构对于TDE是必须的。

   - 基于Wallet的 TDE 设置:

TDE_CONFIGURATION = ‘KEYSTORE_CONFIGURATION=FILE’;
WALLET_ROOT/tde ← 包含有密码保护的（和（本地）自动打开的）钱包
WALLET_ROOT/tde_seps ← 自动打开钱包，存放钱包的密码（"外部存储"）。

   - OKV-based TDE setup:

TDE_CONFIGURATION = ‘KEYSTORE_CONFIGURATION=OKV|FILE’;
WALLET_ROOT/okv ← 包含有密码保护的OKV客户端
WALLET_ROOT/tde ← 自动打开的钱包包含OKV密码(自动打开OKV)
WALLET_ROOT/tde_seps ← 自动打开钱包，存放钱包的密码（"外部存储"）

配置TDE的注意事项

2. 可以调整数据库的默认算法（AES128）
   - 基于Wallet的TDE, 在运行”create keystore "命令之前
   - 基于OKV 的TDE , 在运行“set key”命令之前
   - 在数据库11.2.0.4 ... 19c中，可以通过一个 参数
   _tablespace_encryption_default_algorithm 并且只允许AES128, AES192, AES256
   - 在数据库21c和更高版本中，所有支持的算法都可以应用{ AES128 | AES192 | AES256 | ARIA128 | ARIA192 | ARIA256 | GOST256 | SEED128 | 3DES168 } tablespace_encryption_default_algorithm

3. 什么时候会无法返回先前状态“point of no return”？
   - 在数据库中若启用了TDE并创建Key，则数据库和Wallet建立起了一对一映射
   - 如果在一个ADG环境中, ADG会将同样的设置在备库上运行一遍，然而如果客户中途不想用TDE了，在删除了TDE wallet, 尽管没有加密任何表空间，但会导致备库系统不可用，并且主库也会处于不稳定的状态

配置TDE的注意事项

4. 为什么要在PDB中单独设置密钥?
   - 可以一次性为CDB和所有的PDB设置密钥，但是我们希望为PDB密钥添加标签，以便在PDB被克隆/重新定位到另一个CDB时更容易识别。

5. Re-key操作需要数据库的停机吗?
   - 不需要；替换TDE主密钥是一个非常轻量级的操作，重新加密数据加密密钥，对数据库的可用性没有影响。

6. 每个PDB的密钥库在什么时候和哪里可用?
   - 从19.11开始的任何企业版（32235513补丁），从19.14开始没有补丁
   - 目前只支持基于Wallet的和OKV的TDE设置
   - 需要配置WALLET_ROOT和TDE_CONFIGURATION参数

配置TDE的注意事项 - 隔离的PDBs

7. 容器数据库
   - administer key management create keystore identified by “pwd-A”;
   - administer key management set key identified by “pwd-A” container = current;

   - Pluggable Database联合模式
     - administer key management set key identified by “pwd-A”;

   - Pluggable Database隔离模式
     - administer key management create keystore identified by “pwd-B”;
     - administer key management set key identified by “pwd-B”

TDE优势

高级安全

Oracle数据库透明加密的优势

与存储层或应用层加密方案相比，Oracle数据库透明加密TDE具有更多优势：

- Oracle数据库组件，**无需安装其他组件**；并针对 Oracle 数据库进行了**优化**
- **透明**，一旦启动，无需管理员干预。数据在添加到数据库时被透明地加密，并为授权的数据库会话透明地解密
- 安全，**自动生成密钥**并存储在本地密钥库或 Oracle Key Vault (OKV)
- 自动为**RMAN 备份加密**，无需生成另一个密钥，所有密钥都存储在数据库密钥库中
- **Data Pump加密**发生在导出过程中，在创建导出和加密操作之间没有数据被盗的风险
- 如果存储介质或数据文件被盗，敏感数据会受到保护 - 数据在数据库中已被**加密**
- 支持**在线加密和离线加密**

ORACLE
Advanced Security

* 活动最终解释权归甲骨文公司所有

基于 Oracle 数据库
免费企业数据健康检查

- 及时了解数据库健康状况，发现并解决潜在问题
- 维护数据库系统良好状态，保护数据资产的安全
- 提升数据库性能、稳定性和安全性，降低业务风险

免费咨询热线：

400-699-8888

数据库和云讲座群

20-21

甲骨文云技术公众号

技术专家1V1深入交流