Oracle10g第2版新特性之SQL和PL_SQL PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/285/2021_2022_Oracle10g_E7_c67_285693.htm 透明数据加密 对于加密，许多用户深感矛盾：他们既感兴趣，又因意识密钥管理的复杂性而感到慎重，如果处理不当，则会导致设置的效率低下。加密和解密值还会带来相关的性能开销，这使得大部分应用程序架构师不太乐于接受该过程。结果是，很多系统设计根本没有加密，只是构筑了强大的外围防护，如强大的口令和适当的授权方案。 但是，请想象一下如果整个服务器被盗了，甚至只是磁盘被盗，这些磁盘可以装配在具有相同操作系统的服务器上，然后其中的数据将被销毁殆尽。或者有一个的 DBA 品行不端，在日常业务活动中恶意突破了外围防护，然后将您所有重要的客户信息洗劫一空。在这两种情况下，如果所涉及的商业机构是在加利福尼亚州（可能不久之后在美国的其他州），它们在法律上有责任将安全漏洞的情况通知给所有受到影响的客户。 在上述罕见（但确是事实）的情况中，认证方案没有实际意义。这就是为什么对于那些将安全作为头等大事的机构而言，透明数据加密 (TDE) 是一个如此有用的特性；它支持加密，同时将密钥管理的复杂性交给数据库引擎来处理。同时，它允许 DBA 在不必实际看到数据的情况下管理数据库表。 在 Oracle 数据库 10g 第 2 版中使用 TDE 时，可以随时地对表中的一列或多列进行加密；只需将列定义为加密形式即可，不用编写代码。请记住，加密需要使用密钥和算法对输入值进行加密。TDE 为特定的表生成单独的密钥。这种方法方便了密钥管理却也更易被他们窃取，所以数据库提供

了另一种密钥 万能密钥 ，它可以在数据库级别上设置。表密钥是利用万能密钥进行加密的，要获得表密钥就需要这个万能密钥。因此，对列进行解密时需要万能密钥和表密钥。万能密钥存储在数据库外一个称为“ 钱夹 ”的地方 默认位置在 $ORACLE_BASE/admin/$Oracle_SID/wallet。在概念上，它类似于下图。 在配置 TDE 之后 或者更明确地说是配置了钱夹和万能密钥之后 您可以使用它来保护数据值。要为表的一列加密，需要使用以下 SQL： create table accounts(acc_no number not null,first_name varchar2(30) not null,last_name varchar2(30) not null,SSN varchar2(9) ENCRYPT USING AES128,acc_type varchar2(1) not null,folio_id number ENCRYPT USING AES128,sub_acc_type varchar2(30),acc_open_dt date not null,acc_mod_dt date,acc_mgr_id number) 在这里，您在列 SSN 和 FOLIO_ID 上使用了 TDE，它们现在以加密方式存储在表本身。但是，当用户从表中选择时，她看到以明文表示的数据，因为在检索过程中已经完成了解密。如果磁盘被盗，则包含在表段中的信息仍然保持加密状态。盗窃者需要表密钥才能看到加密的值，但是要获得表密钥，他需要万能密钥，而万能密钥存储在外部，因此无法获得。 注意列 SSN 和 FOLIO_ID 后面的子句，这些子句指定 ENCRYPT 使用 128 位高级加密标准。 数据库拥有预先配置的钱夹。要设置钱夹口令，可使用命令： alter system set encryption key authenticated BY "topSecret". 如果还未创建钱夹，该命令将先创建钱夹，然后将口令设置为“ topSecret ”（区分大小写）。然后您就可以开始在表的创建和更改期间将加密用于列定义。 为外部表加密 在以上示例中，我使用散列表为列加密。您还可以在外

部表上使用 TDE。例如，如果您希望生成一个包含 ACCOUNTS 的数据的转储文件，以便发送到不同的地点，则可以使用简单的 ENCRYPT 子句。 create table account_extorganization external(type Oracle_datapumpdefault directory dump_dirlocation (accounts_1_ext.dmp,accounts_2_ext.dmp,accounts_3_ext.dmp,accounts_4_ext.dmp))parallel 4as0select ACC_NO,FIRST_NAME,LAST_NAME,SSN ENCRYPT IDENTIFIED BY "topSecret",ACC_TYPE,FOLIO_ID ENCRYPT IDENTIFIED BY "topSecret",SUB_ACC_TYPE,ACC_OPEN_DT,ACC_MOD_DTfrom accounts. 在文件 accounts_*_ext.dmp 中，SSN 和 FOLIO_ID 的值不会是明文，而是加密形式。如果您希望使用这些文件作为外部表，则必须提供 topSecret 作为口令以读取这些文件。 在这里您可以看到，TDE 是访问控制的理想补充（而不是替代）。