异构平台的数据库安全技术 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/141/2021_2022__E5_BC_82_E6_9E_84_E5_B9_B3_E5_c29_141423.htm 安全策略 异构数据库的安全性包括：机密性、完整性和可用性，数据库在三个层次上的异构，客户机 /服务器通过开放的网络环境，跨不同硬件和软件平台通信，数据库安全问题在异构环境下变得更加复杂。而且异构环境的系统具有可扩展性，能管理分布或联邦数据库环境，每个结点服务器还能自治实行集中式安全管理和访问控制，对自己创建的用户、规则、客体进行安全管理。如由DBA或安全管理员执行本部门、本地区、或整体的安全策略，授权特定的管理员管理各组应用程序、用户、规则和数据库。因此访问控制和安全管理尤为重要。异构环境的数据库安全策略有： 全局范围的身份验证； 全局的访问控制，以支持各类局部访问控制（自主和强制访问控制）； 全局完整性控制； 网络安全管理，包括网络信息加密、网络入侵防护和检测等； 审计技术； 数据库及应用系统安全，如自动的应用系统集成、对象管理等。开发者能定义各个对象的安全性。根据定义的数据库安全性，DBA能迅速准确地通过应用系统给所有数据库对象授权和回收权限。 复杂的口令管理技术 复杂的口令管理技术。包括数据库中多个事务的口令同步；异构数据库间的口令同步，如Oracle 和Unix口令；用户初始的口令更新；强制口令更新；口令可用性、口令的时间限制、口令的历史管理、口令等级设置等。 口令安全漏洞检查和系统终止。包括检查系统终止前登录失败的次数，系统终止前登录成功与登录失败间的时间间隔，跟踪企图登录

的站点地址。 口令加密、审计技术。包括发现口令漏洞,记录口令历史, 记录对表、行、列的访问,记录应用系统的访问等。 安全代理模型 异构数据库是一个为用户提供服务的网络互联的服务器集合。因此应提供全局访问控制（GAC），并对原有安全策略重新进行异构描述。提供联邦访问表，为用户访问、更新存在于不同数据库的数据信息（包括安全信息）提供服务。此表为联邦中每个用户指定对某个实体对象允许的操作，它由存放在某个数据库中的安全信息创建。由于实体对象的集合可能被存放在许多数据库中，应提供特定规则和过程将安全信息转换集成为全局信息。 使用多种代理，全局访问控制（GAC）的安全结构分为三层：协调层、任务层和数据库层，每层有特定的代理强制执行部分联邦安全策略。协调层的任务由系统管理员的代理完成，负责管理整个环境，分派权限给称作任务代理的其他代理，任务代理通过分派访问单个数据库的权限给数据库代理，来控制对整个联邦数据库的访问。比如，由系统管理员分派的完整性保证的任务由完整性管理员完成，数据库功能（如获得用户信息）由用户和数据代理完成。 顶层（Top Level）代理称为委托代理。由它决定联邦中执行任务的类型。这一层的代理关心联邦中所有发生或正在发生的活动。为了获知“ 谁正在做什么 ”，不同代理的信息都存放在一特定的目录里。根据这些信息，顶层代理，向适当的代理委派任务。 中间层（Middle Level）代理称为安全代理。特定的任务（如保持全局完整性）由安全代理完成，它在联邦中可见的范围比顶层代理要窄，完成的任务更具体。安全代理只能看到和它完成同一任务的其他代理。 底层（Bottom Level）代理称为数据代理。由更高层

代理指定完成访问、更新信息任务的代理组成。这些代理是共享数据库和顶层、中间层代理的接口。如用户代理记录某个用户的所有信息，如他/她的标识、对不同对象的不同访问权限等。 DM3的安全技术 DM3的安全体系结构 可信数据库管理系统的体系结构分为两类，第一类是 TCB子集DBMS结构，用DBMS以外的可信计算基(TCB)实现对数据库对象的强制访问控制，此时多级关系被分解成单级或系统级片断，多级安全DBMS将这些片断存在物理上分离的单级对象（如文件、段或物理上分离的硬件设备）中，再对这些分离的单级或系统级对象的访问实行强制访问控制。第二类是可信主体DBMS，由DBMS本身实现强制访问控制的一些或全部责任。 DM3采用可信主体DBMS体系结构，由数据库管理系统实现强制访问控制的功能，它要求操作系统能提供控制，防止绕过DBMS直接对数据库的访问，将概念上的多级数据库存于一个或多个操作系统对象（如文件）中。由多级安全DBMS 给每个数据库对象进行标记，这些数据库对象对操作系统是不可见的，操作系统不能直接对数据库对象进行访问，多级安全DBMS有跨操作系统安全级范围操作的特权。三权分立的安全机制 DM3在安全管理体制方面与其他数据库管理系统不同。绝大多数数据库管理系统采用的是由数据库管理员DBA负责系统的全部管理工作(包括安全管理)。显然，这种管理机制使得DBA的权力过于集中，存在安全隐患。DM3在安全管理方面采用了三权分立的安全管理体制，把系统管理员分为数据库管理员DBA，数据库安全管理员SSO，数据库审计员Auditor三类。DBA负责自主存取控制及系统维护与管理方面的工作，SSO负责强制存取控制，Auditor负

责系统的审计。这种管理体制真正做到三权分立，各行其责，相互制约，可靠地保证了数据库的安全性。 自主访问与强制访问控制 自主访问控制就是对主体(用户)访问客体(数据库对象) 的操作权限实施控制，目的就是要保证用户只能存取他有权存取的数据，当用户拥有数据库对象上的某些操作权限及相应的转授权时，可以自由地把这些操作权限部分或全部转授给其他用户，从而使得其他用户也获得在这些数据库对象上的使用权限。DM3系统根据用户的权限执行自主访问控制。规定用户权限要考虑三个因素：用户、数据对象和操作。所有的用户权限都要记录在系统表(数据字典)中，对用户存取权限的定义称为授权，当用户提出操作请求时，DM3根据授权情况进行检查，以决定是执行操作还是拒绝执行，从而保证用户能够存取他有权存取的数据。 所谓强制访问控制是通过给主体(用户)和客体(数据对象) 指定安全级，并根据安全级匹配规则来确定某主体是否被准许访问某客体。DM3系统根据用户的操作请求、安全级和客体的安全级执行强制访问控制，保证用户只能访问与其安全级相匹配的数据。强制访问控制必须事先定义主体和客体的安全级，所有主体和客体的安全级都要记录在系统中。当用户提出操作请求时，DM3首先检查用户对所操作的数据对象是否具有相应的操作权限，然后检查该用户的操作请求及安全级与所操作的数据对象的安全级是否匹配，当两个条件都满足时，DM3才执行用户的操作请求，否则拒绝执行。 