基于 MS SQL Server 分布式数据库的安全性设计

姜芳芃　范力军　刘方鑫　（徐州中国矿业大学计算机系　221008）

摘要：数据库的安全性设计是数据库管理系统开发过程中的一个关键环节。笔者对基于 Microsoft SQL Server 6.5 分布式数据库的安全性进行了分析和研究，提出了一套有效的安全性设计方法。

关键词：Microsoft SQL Server 6.5　数据库的安全性　集成安全模式

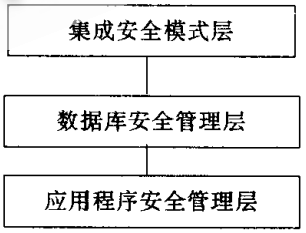
一、引言

良好的数据库的安全性设计，可以有效地保护数据库，防止不合法的访问和破坏。具体地说：可以防止数据向未授权用户泄露，甚至被未授权用户更改；防止一些合法用户得到了权限以外的信息；防止由于一些具有合法权限的用户的误操作，破坏了数据库中的数据；防止由于一些故障引起数据库中的数据丢失或破坏。在一个复杂的分布式数据库中，数据是分布的，用户是分布的，用户较多且权限不同，安全性设计更是开发者不可回避的重要环节。

我们在开发分布式数据库系统时，在服务器端采用了 Microsoft SQL Server 6.5，这种产品是 Microsoft 面向分布式客户机/服务器计算的关系数据库系统，是为支持分布式计算环境而设计的。同时，操作系统使用的是 Windows NT Server 4.0，其具有可扩充性、可移植性、可靠性、兼容性等性能；在客户机端采用 Access 7.0，依靠 ODBC 驱动程序与 SQL Server 相联接。本文对该数据库系统的安全性做了如下设计和研究。

二、安全性设计与研究

通常分布式数据库系统的安全由操作系统、数据库系统、应用程序三方面独立完成，我们则将操作系统和数据库系统有机结合，提出了集成安全模式层、数据库安全管理层、应用程序安全管理层三层结构，采用逐层推进的方式，完善系统的安全机制。图示如下：



1. 集成安全模式层

集成安全模式是操作系统和数据库系统的有机结合。集成安全模式允许一个 SQL 服务器用 Windows NT 的认证机制，证实 SQL 服务器的所有连接的登录。一方面，使 SQL 服务器采用了 Windows NT 安全特性的优点，包括加密口令、口令期限、域范围的用户帐户以及基于 Windows NT 的用户管理。另一方面，不必为每个用户都建立登录 ID 号，由 SQL 服务器提供的"SQL Security Manager"实用程序将基于 NT 的用户名映射为 SQL 服务器登录 ID 号，用户对 NT 和 SQL 服务器只维护单一的登录号和口令。

2. 数据库安全管理层

(1)多层次的访问管理

①SQL 服务器登录管理。将 NT 用户登录号增加到服务器，这些用户才能获得对服务器的访问。

②数据库用户管理。增加用户到数据库，才可访问数据库。

③数据库对象许可管理。数据库对象包括表、视图、列、存储过程等，数据库拥有者对数据库对象拥有全部权限，数据库拥有者可以使用 GRANT 语句，将某些对象的访问权限授予某用户，该用户才可在此权限范围内访问数据库对象。

权限	数据库对象
select	表、视图、列
update	表、视图、列
insert	表、视图
delete	表、视图
reference	表
execute	存储过程

④语句许可管理。授予用户语句许可，用户才可使用这些语句。语句包括：

Create DB，Create Table，Create View，Create SP，Create Default，Create Rule，Dump DB，Dump Trans。

(2) 简单而有效的安全机制——视图、存储过程、触发器。视图是虚表，它是一个或一个以上的表中的行和列的一个子集。用户可被授予对一视图的许可权，使用户不直接对基表操作，而是通过视图间接对其中的可见部分操作，提高了数据库数据的安全性。通过定义不同的视图，和有选择地授予它们的许可权，可以限制用户对数据特定子集的访问。可能限制用户的访问为：

·基表的行子集(一个值依赖的子集)；

·基表的列子集(一个值依赖的子集)；

·基表的行列子集 * 限定多个基表的连接的行；

·基表中数据的统计总结信息；

·另一个视图或几个视图和基表的组合的子集。

存储过程(触发器是一种特殊的存储过程)也可用来增强数据库的安全性。执行存储过程许可权独立于可能存在的对由该存储过程所参考的数据库对象的任何访问特权。用户特权可被限于执行存储过程的特权，因为该过程本身拥有更新基表的特权，故该用户不需要明显地被授予该特权，这同时限定了用户对基表的其他操作。

(3) 完整性控制

①语义完整性约束：SQL Server 6.5 提供了完整性描述手段，便于建立语义完整性约束(唯一性、引用约束、检验约束、缺省约束)，这些约束对添加、修改、删除的记录进行完整性检查，不符合约束的记录被拒绝。

②并发控制：SQL Server 6.5 提供了良好的自动并发控制机制，用户也可以自己设计如何加锁。

③恢复：对数据库及其事务日志进行定期备份，以便由于以意外事故对数据库造成破坏时，及时对数据库进行恢复。

3.应用程序安全管理层

(1) 对客户端应用程序加密码。

(2) 将 Access 开发的客户端应用程序制作成 MDE 文件，即可将系统中模块的代码部分进行编译，使窗体、报表、模块均不可修改。

(3) 将表、查询、宏的属性定义为隐藏，再利用菜单中"工具"的"选项"的不显示隐藏对象，使它们成为不可见，以减少一般用户对应用程序的修改和删除。

三、安全设计实现

1.设置服务器为集成安全模式

(1) 从"Microsoft SQL Server 6.5"程序组中启动"SQL Enterprise Manager"应用程序。

(2)从"Server Manager"窗口中打开一个服务器并选择要管理的服务器。

(3)从"Server"菜单中选择"Configurations"。

(4)从"Server Configuration"对话框中选择"Security Options"选项卡。

(5)设置安全模式、缺省域、审计级、特殊字符映射等。

2.创建有权访问服务器的 Windows NT 小组

(1)使用 NT 的"User Manager"创建一个名为"SQL Users"的本地小组，只有用户级特权；创建另一个小组"SQL Adimins"，有系统管理员特权。然后分别加入单个用户。

(2)使用"SQL Security Manager"应用程序授权 NT 小组和用户可访问 SQL 服务器。

3.增加小组、用户到一个数据库中去

使用"SQL Enterprise Manager"应用程序增加小组、用户到一个数据库中去。小组提供了一个便利的方法，可以同时给多个用户授予和撤消特权许可。另外，常用别名建立共同的用户身份，别名允许将多个人看做数据库中的同一用户，给他们同样的许可。例如，要给"SQL Users"组中的"user1 user2 user3"三个用户建立一个别名，只需在该组添加"userx"并选择"available Logins"为"user1 user2 user3"。

4.创建数据库和日志设备

5.使用创建语 CREATE，创建表(增加语义完整性约束)、视图、存储过程、触发器；使用授权语句 GRANT，分别授予数据库用户和小组对数据库对象的许可和语句的许可。

6.创建备份设备，设置备份内容和周期

7.在客户端设置数据库密码、生成 MDE 文件、隐藏一些数据库的表、查询、宏。

四、结束语

本系统已开发完成，试运行情况良好，尤其是在安全性方面，充分考虑了影响数据库的各种不安全因素，尽可能地采取了一些必要措施，达到了保护数据库的目的。

参考文献

[1] 《Microsoft SQL Server 6.5 管理员指南》Microsoft 著

[2] 《Microsoft SQL Server 6.5 程序员指南》Microsoft 著

[3] 《Microsoft SQL Server 6.5 参考手册》Microsoft 著

[4] 《关系数据库原理与应用》刘方鑫 曲云尧 孟凡荣

(来稿时间：1998 年 8 月)