编者按: 伴随大量信息从计算机中获取, 其数据库应运而生。SQL SERVER 作为一种开放型的网络数据库, 其安全性十分重要。研究SQL SERVER 系统的安全保护机制, 可为该系统在农业上的广泛应用提供依据。

SQL SERVER 数据库系统安全保护机制研究

李华, 陈飞平, 李红 (1 . 江西农业大学职业技术师范学院, 江西南昌 330045 ;2 . 江西农业大学园林与艺术学院, 江西南昌 330045)

摘要　从应用角度出发, 介绍了SQL SERVER 数据库系统的安全要求、安全结构以及安全性实现方法。
关键词　数据库; SQL SERVER 数据库系统; 安全
中图分类号　TP311 .13　　文献标识码　A　　文章编号　0517 - 6611(2007) 19 - 05959 - 02

Research on Security Protection Mechanism of SQL SERVER Database System

LI Hua et al (Institute of Vocational Technology , Jiangxi Agricultural University , Nanchang , Jiangxi 330045)

Abstract　Starting with the application angle , the safe request , safety mechanism as well as the safe realization method of SQL SERVER database system were introduced in the article .
Key words　Database ; SQL SERVER database system; Safe

随着计算机、网络和通讯技术的飞速发展, 计算机技术日益深入到社会各个方面, 这为信息的传播提供了最广泛、快捷的途径。通过计算机可获得大量有用信息, 而这就需要大量的数据库管理工作, 网络和数据库技术的结合, 逐渐成为信息服务领域应用程序开发的一种重要手段。SQL SERVER 是一个网络数据库系列产品, 它被设计用来满足大型的数据处理系统和商业网站的存储需求。由于它是一个开放型的数据库系统, 因此在建立网络数据库时必须考虑其安全性问题。

1　SQL SERVER 数据库系统的安全要求

SQL SERVER 安全性主要是指允许具有相应数据访问权限的用户能够登录到SQL SERVER 并访问数据以及对数据库对象实施各种权限范围内的操作, 但是拒绝所有的非授权用户的非法操作。因此, 安全性管理与用户管理密不可分。SQL SERVER 提供了内置的安全性和数据保护, 并且这种管理简单、有效。

2　SQL SERVER 数据库安全结构

2 .1　用户分类

2 .1 .1　数据库登录权限类。具有数据库登录权限的用户能进入数据库管理系统, 使用数据库管理系统所提供的各类工具和实用程序。同时, 数据库客体的主人可以授予这类用户数据查询、建立视图等权限。这类用户只能查阅部分数据库信息, 而不能改动数据库中的任何数据。

2 .1 .2　资源管理权限类。具有资源管理权限的用户, 除了拥有数据库登录权限外, 还拥有创建数据库表、索引等数据库客体的权限, 可在权限允许的范围内修改、查询数据库, 将个人拥有的权限授予其他用户, 还可以申请审计。

2 .1 .3　数据库管理员权限类。具有数据库管理员权限的用户具有数据库管理的一切权限, 包括访问任何用户的所有数据, 授予(或回收) 用户的各种权限, 创建各种数据库客体, 完成数据库的整库备份、装入重组以及进行全系统的审计等工作。这类用户的工作是谨慎而具有全局性的, 只有极少数用户属于这种类型。

2 .2　数据分类

同一类权限的用户, 对数据库中数据管理和使用的范围可能是不同的。为此,SQL SERVER 提供了将数据分类的功能, 即建立视图。管理员把某用户可查询的数据逻辑上归并起来, 简称一个或多个视图, 并赋予名称, 再把该视图的查询权限授予该用户(也可以授予多个用户) 。这种数据分类可以进行得很细, 其最小粒度是数据库二维表中一个交叉的元素。

2 .3　审计功能

SQL SERVER 提供的审计功能是一个十分重要的安全措施, 它用来监视各用户对数据库施加的动作。审计方式分用户审计和系统审计2 种。用户启用审计功能时,SQL SERVER 的审计系统可记下所有对该数据库表或视图进行访问的企图(包括成功的和不成功的) 及每次操作的用户名、时间、操作代码等信息。这些信息一般都被记录在数据字典中, 用户可以利用这些信息进行审计分析。系统审计由系统管理员进行, 其审计内容主要是系统一级命令以及数据库客体的使用情况。

3　SQL SERVER 数据库系统安全性实现方法

3 .1　安装最新的服务包

为提高服务器安全性, 最有效的方法就是升级到 SQL SERVER 2000 SERVICE PACK 3a (SP3a) 。另外, 还应该安装所有已发布的安全更新。

3 .2　使用 MICROSOFT 基线安全性分析器(MBSA) 评估服务器的安全性

MBSA 是一个扫描多种 MICROSOFT 产品不安全配置的工具, 包括 SQL SERVER 和 MICROSOFT SQL SERVER 2000 DESKTOP ENGINE(MSDE 2000) 。它可以在本地运行, 也可以通过网络运行。该工具可对SQL SERVER 的以下安装问题进行检测: ①过多的sysadmin 固定服务器角色成员; ②授予sysadmin 以外的其他角色创建CmdExec 作业的权利; ③空的或简单的密码; ④脆弱的身份验证模式; ⑤授予管理员组过多的权利; ⑥SQL SERVER 数据目录中不正确的访问控制表(ACL) ; ⑦安装文件中使用纯文本的sa 密码; ⑧授予guest 帐户过多的权利; ⑨在同时是域控制器的系统中运行SQL SERVER; ⑩所有人(Everyone) 组的不正确配置, 提供对特定注册表键的访问; ⑪SQL SERVER 服务帐户的不正确

作者简介　李华(1979 -) , 女, 江西永新人, 硕士, 讲师, 从事数据库应用研究。
收稿日期　2006-11-15

配置;⑫没有安装必要的服务包和安全更新。

3.3 使用 WINDOWS 身份验证模式 在任何可能的时候,都应该对指向SQL SERVER 的连接要求 WINDOWS 身份验证模式。它通过限制对 MICROSOFT WINDOWS 用户和域用户账号的连接,保护SQL SERVER 免受大部分INTERNET 工具的侵害,而且,服务器也将从 WINDOWS 安全增强机制中获益,例如更强的身份验证协议以及强制的密码复杂性和过期时间。另外,凭证委派(在多台服务器间桥接凭证的能力)也只能在 WINDOWS 身份证验证模式中使用。在客户端,WINDOWS 身份验证模式不再需要存储密码。存储密码是使用标准SQL SERVER 登录的应用程序的主要漏洞之一。

3.4 隔离服务器,并定期备份 物理和逻辑上的隔离是SQL SERVER 安全性的基础。驻留数据库的机器应该处于一个从物理形式上受保护的地方,最好是一个上锁的机房,配备有洪水检测以及火灾检测 消防系统。数据库应该安装在企业内部网的安全区域中,不要直接连接到INTERNET 上。定期备份所有数据,并将副本保存在安全的站点。

3.5 分配一个强健的sa 密码 sa 帐户应该总拥有一个强健的密码,即使在配置为要求 WINDOWS 身份验证的服务器上也亦如此。这将保证在以后服务器被重新配置为混合模式身份验证时,不会出现空白或脆弱的sa。

3.6 限制 SQL SERVER 服务的权限 SQL SERVER 和SQL SERVER AGENT 是作为 WINDOWS 服务运行的。每个服务必须与一个 WINDOWS 帐户相关联,并从这个帐户中衍生出安全性上下文。SQL SERVER 允许sa 登录的用户(有时也包括其他用户)来访问操作系统特性。这些操作系统调用是由拥有服务器进程的帐户的安全性上下文来创建的。如果服务器被攻破,那么这些操作系统调用可能被用来向其他资源进行攻击。因此,限制SQL SERVER 的服务权限十分重要。

3.6.1 SQL SERVER ENGINE/ MSSQL SERVER。如果拥有指定实例,那么它们应该被命名为 MSSQL $InstanceName。作为具有一般用户权限的WINDOWS 域用户帐户运行。不要作为本地系统、本地管理员或域管理员帐户运行。

3.6.2 SQL SERVER AGENT SERVICE/ SQL SERVER AGENT。如果环境中不需要,则禁用该服务;否则应作为具有一般用户权限的WINDOWS 域用户帐户运行。不要作为本地系统、本地管理员或域管理员帐户运行。

3.7 在防火墙上禁用 SQL SERVER 端口 SQL SERVER 的默认安装将监视TCP 端口1433 以及UDP 端口1434。配置防火墙过滤到达这些端口的数据包,而且还应该在防火墙上阻止与指定实例相关联的其他端口。

3.8 使用最安全的文件系统 NTFS 是最适合安装SQL SERVER 的文件系统。它比FAT 文件系统更稳定且更容易恢复。同时它还包括一些安全选项,例如文件和目录ACL 以及文件加密(EFS)。在安装过程中,如果侦测到 NTFS,SQL SERVER 将在注册表键和文件上设置合适的ACL,所以不应该去更改这些权限。通过EFS,数据库文件将在运行SQL SERVER 的帐户身份下进行加密。只有这个帐户才能解密这些文件。

参考文献

[1] 苏亚娟. WEB 数据库安全性问题探讨[J]. 无锡南洋学院学报,2005(3):50-53.

[2] 赵渭泳,张小艳. 基于网络数据库应用系统的安全技术[J]. 信息化技术与创新管理,2006(4):60-64.

[3] 刘智璐,潘雪峰. 数据库安全性研究[J]. 武汉生物工程学院学报,2006(1):30-32.