张晖，李雅静，赵颖，2012．SQL Server 数据库中数据的安全监控．震灾防御技术，**7**（2）：208—213.

SQL Server数据库中数据的安全监控 [1]

张 晖 李雅静 赵 颖

（天津市地震局，天津 300201）

摘要 本文主要阐述了作者在工作中遇到的 SQL Server 数据库中一些重要数据泄漏或是异常变动现象，随后通过各种技术手段追踪数据异常变更的根源的学习研究过程。从而达到了对日常工作中的重要数据进行安全监控、跟踪相关操作的目的，同时，也为各类数据的安全性、准确性提供了坚实的保障。

关键词：SQL Server 关系数据库 存储过程 追踪

前言

数据库的安全性是指保护数据库以防止不合法的使用造成数据泄漏、更改或破坏。数据库和计算机系统的安全性，以及操作系统和网络系统的安全性是紧密联系、相互支持的（王岳斌等，2009）。

当前，对数据库安全的威胁主要分为物理上的和逻辑上的。物理上的威胁主要是指由计算机软硬件故障、错误导致的数据丢失等，为了消除物理上的威胁，通常采用备份和恢复的策略。逻辑上的威胁主要是指对信息未被授权的存取，可以分为 3 类：①信息泄漏，包括直接和非直接（通过推理）地对保护数据的存取；②非法数据修改，由操作人员的失误或非法用户的故意修改引起；③拒绝服务，通过独占系统资源导致其他用户不能访问数据库（Li Yanyuan，2005；徐龙琴等，2009）。

本文中所要追踪的是使用超级管理员的高级权限登录数据库对数据进行查询、更改甚至删除等操作的现象。

1 研究过程

目前，SQL Server 数据库已被广泛应用于各个领域，而地震行业中的信息网络、测震台网、前兆台网、应急指挥、震害防御等学科也或多或少地应用到该数据库系统。天津地震应急指挥系统使用了基于 SQL Server 数据库的检索系统，在系统的开发和使用中发现一些重要数据的异常变动，这些数据的变更并非通过相应的程序正常操作而发生的。为了保障数据的安全，开始研究重要数据读写的追踪（王建国等，2006）。

1 基金项目 本文由“天津地震灾害损失初评估快速查询应急资料箱建设”资助
［**收稿日期**］ 2011-12-27
［**作者简介**］ 张晖，女，生于 1979 年。硕士，工程师。主要从事地震应急工作。E-mail: 15375539@qq.com

1.1　初步研究

面对上述情况，首先对日志文件进行查询。日志文件能够显示出数据被查询或是被篡改的 SQL 语句和执行时间等信息，但日志文件里只记录了登陆数据库的用户名，即超级管理员用户名，无法定位到执行该指令的计算机，更无法定位到具体人员。日志文件如图 1 所示。

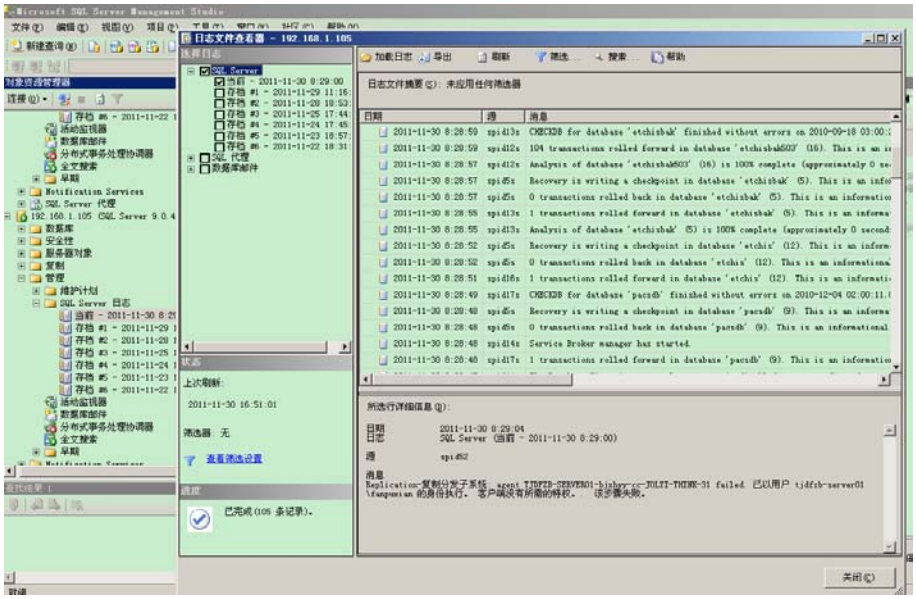

图 1　SQL Server 日志文件

Fig. 1　SQL Server log files

经研究我们发现，可通过 DBCC INPUTBUFFER 语句来获取客户端发送到 SQL Server 的最后一条 SQL 语句。这个方法需要提供 session_id，而这个 session_id 可以通过 master 库（系统库）中的系统视图 sys.sysprocesses 来获得，而这个系统视图中有这样几个字段：hostname（客户端机器名）、program_name（应用程序名称）、net_address（最初认为 net_address 是客户机的 MAC 地址，但经过多次试验发现有的机器确实是 MAC 地址，有的却不是）。这样，如果局域网内有通过域来管理所有机器，那么客户机的机器名是不能随意变动的，即可通过查询 hostname 来锁定执行相关指令的客户端。

通过写一个.net 程序（c/s 架构），其中设一个定时器（timer），每间隔一秒钟刷新一次，每次刷新都通过 DBCC INPUTBUFFER 语句来获取客户端发送到 SQL Server 的最后一条 SQL 语句，当然这里面的 session_id（即 spid）要通过 sys.sysprocesses 来循环获取，然后将获取的语句以及相关信息写入建好的记录表中。定时器程序执行存储过程的流程如图 2 所示。

图 2 是程序中刷新监控记录的存储过程，可以实时监控，也可以将这些记录再写入一个历史记录表中以便存证。如果局域网未通过域来管理，即客户端可随意更改本机的机器名，这样就必须找出执行相关指令的客户端的 IP 地址。客户端的 IP 地址可以用 exec master..xp_cmdshell ping host_name 方法获得。但是此方法仅限于客户端机器开启 ping 功能的情况下，一旦其关闭该功能则无法取得对方客户端的 IP 地址。

经过不断测试，我们发现该方法仍然存在以下几个问题：

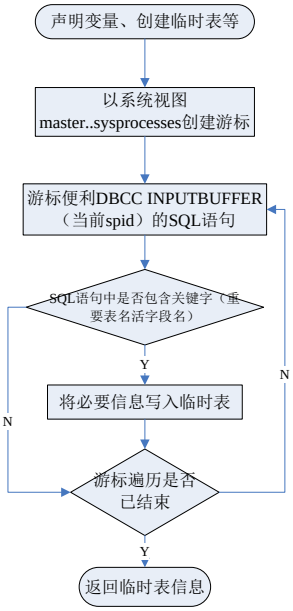

图 2 存储过程流程图

Fig. 2 Flowchart of storage procedure

①无法追踪到客户端通过存储过程访问数据库的具体 SQL 语句。

②监控是通过定时器的循环指令执行，如定时器间隔时间设置过长，则会遗漏一些重要信息；如定时器时间间隔设置过短，则会占用服务器较多资源，从而影响服务器的正常运行。

③记录中存在 hostname 为空的 SQL 语句执行记录，这样便无法追踪到执行该指令的客户端（上文所述获取客户端 IP 地址的方法也是通过 hostname 来实现的）。

1.2 深入研究

在进一步研究的过程中，还需要将测试中发现的问题一一解决。

首先，通过遍历 sys.object 系统表来发现可疑的存储过程，即通过 sp_helptext 来读出该存储过程的内容，同时遍历其语句，看看有无访问数据表。

其次，通过 SQL Server 自带的 SQL Server Profiler 功能查找遗漏的重要信息，如图 3 所示。

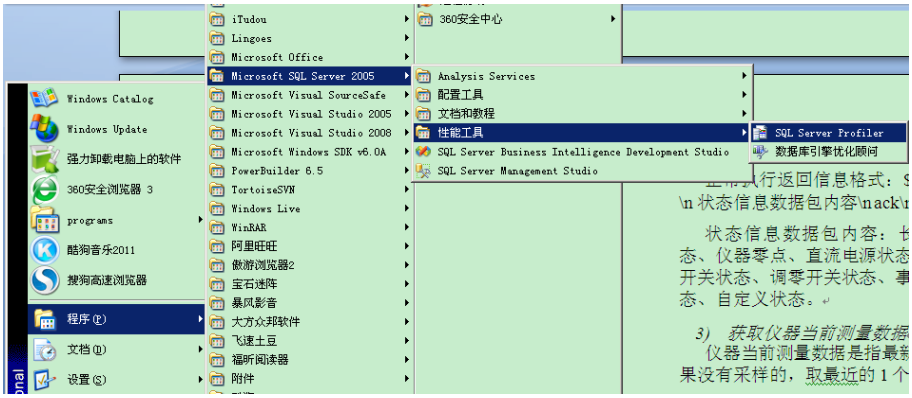

图 3 SQL Profiler 菜单

Fig. 3 Main menu of SQL Profiler

在初步研究的方案中是通过 DBCC INPUTBUFFER 语句来获取客户端发送到 SQL Server 的最后一条 SQL 语句。如果一次性提交多条 SQL 语句，该方法只能够捕捉到最后一条 SQL 语句，而忽略前面的若干条。经测试，通过 SQL Server Profiler 功能来跟踪语句则不会出现类似的状况，SQL Server Profiler 功能可以跟踪出所有的 SQL 语句，避免了重要信息的遗漏。

经过一段时间的研究及测试，发现安装 PowerBuilder 开发环境的客户端可以通过开发环境连接 SQL Server 数据，并查看或更改数据，这样通过 DBCC INPUTBUFFER 方法无法获取其主要的 SQL 语句，只能捕捉到最后一句，通常是提交或回滚数据库事务的语句，而通过 SQL Server Profiler 功能来跟踪语句则能够跟踪到所有语句。

当 hostname 为空时，如何找到该记录对应的客户端机器，则需要通过 SQL Server Profiler

功能跟踪表中的 SPID 与当时的关系库中的系统视图 sys.dm_exec_connections 中的 session_id 关联，就可以从系统视图 sys.dm_exec_connections 中的 client_net_adress 字段中获取执行指令的客户端的 IP 地址了。为什么是“当时”呢？因为 SPID 即 session_id 在数据库中是又系统分配的，只能保证在一段时间内唯一。因此我们在跟踪到相关语句时，必须尽快联表查询到对应 IP，并写入一个记录表中，才能达到准确存证的目的。

2　实现过程

上文已经将遇到的技术难点一一解决，接下来是记录实现的过程：

（1）SQL Server Profiler 设置

第一步需要设置 SQL Server Profiler 跟踪，下面列出几个关键的操作步骤：

①设置跟踪记录表

打开 SQL Server Profiler 后，点击菜单中“文件”——“新建跟踪”，然后选择需要跟踪的数据库并通过超级管理员用户登录。在弹出的跟踪属性对话框中勾选“保存到表”，并将该表保存到我们需要存证的那个数据库。也可以根据需要设置一个跟踪停止时间，因为这个跟踪表不能无限增大，最好定期更换。需要注意的是，跟踪表不能保存在被跟踪的数据库实例中，否则会产生大量的冗余跟踪数据。

②设置关键字

在跟踪属性对话框内选择“事件选择”标签页，这里可以根据实际需求来勾选需要跟踪的事件以及所显示列等，如图 4 所示。

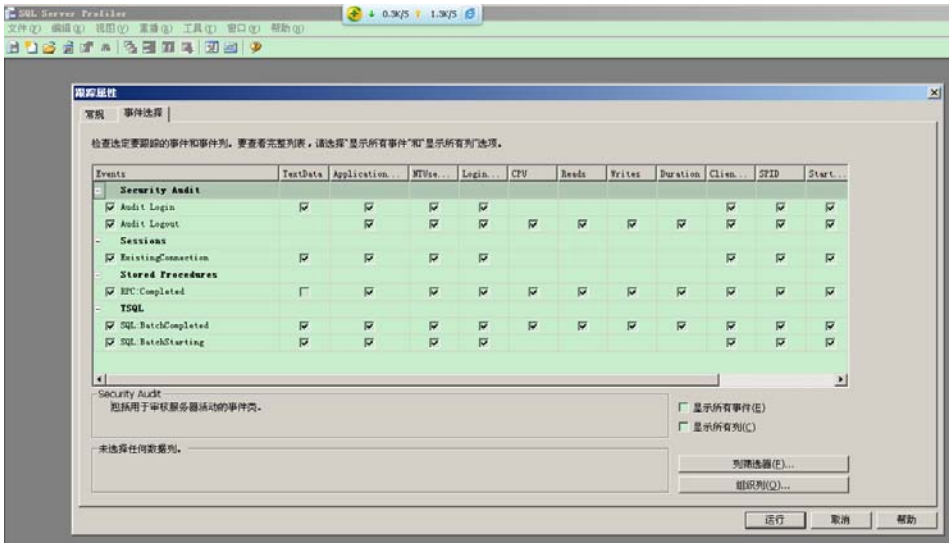

图 4　SQL Profiler 跟踪属性——事件选择

Fig. 4　SQL Profiler track attribute — events selection

必须要在 TextData 字段上设置关键字，例如数据表名、字段名等。在关键字前后加上“%”，便于在跟踪到的 SQL 语句中模糊查询。

参数设置完成，即可运行，开始跟踪数据库。还需要注意两点：一是可以将该跟踪存为

一个模板，便于重复使用；二是该跟踪程可以运行在任何一台可以连接被跟踪数据库的计算机上。

（2）实时获取 IP

SQL Server Profiler 跟踪运行好后，我们就需要实时（或近似实时）将跟踪数据联表得到对应的 IP 地址，然后将这个记录写入我们的存证表中。

为此需要设计一个服务，每秒或每间隔几秒读取一下跟踪数据表数据，并将关联系统视图 sys.dm_exec_connections 中得到的 IP 地址一起写入历史存证表中即可。这里需要注意的是，可以根据跟踪表中的 RowNumber 字段来区分将每次多出的数据联表插入到历史存证表中。如跟踪重启后，跟踪表会重新计数，这时程序内需要将两个表中的 RowNumber 做对比判断，将新增的数据插入历史存证表中。当然也可以根据历史记录表中的最后一条记录时间来进行判断。

（3）跟踪数据查询分析

经过前面两个步骤，已经将需要的数据实时写入历史存证表中，然后我们只需要设计一个查询历史记录的页面即可，这个页面上方为查询条件，例如：时间、应用名称等；下方列表中为记录的一些关键字段，如图 5 所示。

图 5 重要数据访问查询

Fig. 5 Important data access and query

点击每条记录后的“查看”可以看到具体的 SQL 语句，如图 6 所示。

图 6 数据访问查询明细

Fig. 6 The detailed record of important data access and query

3　结语

数据库系统作为信息的聚集体，其安全性至关重要。文中叙述了作者追踪 SQL Server 数据库数据被篡改的研究过程。作者经过多次的尝试和研究，最终实现了对读写数据库指令的追踪。当然，所有追踪的作用也只是亡羊补牢，只能作为监控数据安全的辅助手段，而有效的防窃取、防篡改才是建设数据库至关重要的任务，才能保证数据的保密性、完整性和有效性。

参考文献

王建国，崔晓峰，陈化然等，2006. Microsoft SQL Server 2000 在天津市地震前兆台网中心的应用. 华北地震科学，**24**（3）：56—60.

王岳斌，阳国贵，邝祝芳等，2009. 基于 HMM 的数据库异常检测系统设计与实现. 计算机应用与软件，**26**（1）：15—16.

徐龙琴，刘双印，沈玉利等，2009. 数据库安全性控制的研究. 计算机应用与软件，**26**（5）：31—35.

Li Yanyuan, 2005. The Documentation of Logic SQL. Alberta Univemity，Canada.

Data Security Monitoring of SQL Server Database

Zhang Hui, Li Yajing and Zhao Ying

（Earthquake Administration of Tianjin Municipality, Tianjin 300201, China）

Abstract　Since database system is information aggregation, the security of database is very important. In this paper we discuss some problems in daily data management such as data leakage and abnormal variation, and track back the sources that cause such problems. By doing so we may monitor the important data in daily work to ensure the safety and accuracy of database.

Key words: SQL Server; Relation database; Storage process; Track

更正：本刊 2012 年 1 期 83 页页下注“西藏地震现场工作队，2011.9. 2011 年 9 月 18 日印度锡金邦 6.8 级地震中国西藏灾区灾害直接损失评估报告.”更正为“孙柏涛，姚新强，周强等，2010. 西藏自治区农牧民安居工程抗震加固试验与分析技术报告，121—122.”