

数据库系统安全代价测试工具的设计^{*})

叶晓俊 王建民

(清华大学软件学院信息系统与工程所信息安全教育部重点实验室 北京 100084)

摘要 安全和可靠是数据库系统两个重要的可信指标,它们的策略配置与系统的高效运行是有冲突的。本文分析了安全、可靠等可信指标及其相关测试工具,提出了可信性能基准程序性能测试特点,以指导用户制定、评价、选择数据库安全可靠策略的实施。最后介绍了基于 TPC 性能基准改进的数据库系统安全代价测试工具功能及其实施方法。

关键词 可信,性能基准,安全代价

Design of Database System Dependability Benchmarking Tools

YE Xiao-jun WANG Jian-min

(Key Laboratory for Information System Security, Ministry of Education School of Software, Tsinghua University, Beijing 100084, China)

Abstract Both security and performance targets are treated as two important nonfunctional requirements. Dependability protection configurations can highly affect the throughput of systems. This paper first discusses basic security, dependability concepts and the correlative evaluation criteria. Then the dependability benchmarking characteristics are concluded, in order to guide the user to implement their dependability protection measure. Finally, we give the design of security cost testing tool based on TPC performance benchmarking and its implementation method.

Keywords Dependability, Performance benchmarking, Security cost

1 引言

数据库系统的性能一直是用户和 IT 厂家关注的核心问题^[1]。为证明产品的高效性,IT 厂家都会按照性能基准进行测试。稳定可靠和安全运行也是系统的重要特性,这是从可信软件角度考察产品各组件可用性。因此性能和可靠/可信是应用系统两个重要的非功能评测指标^[5]。一般来讲,这两个指标是与底层的数据库管理系统(DBMS)、应用服务器(AP)等系统软件的解决方案相关的,综合起来进行评测更能说明数据库系统的实际可用性。

DBMS 是信息系统最重要的基础设施。如何在复杂异构的网络环境下配置数据库服务器的安全服务体系结构、如何在 DBMS 固有的脆弱性、操作失误和管理缺陷以及网络攻击和人为破坏客观存在的状况下,选择 DBMS 的各种可信策略,都是用户必须综合考虑的问题^[6]。在信息系统规划、运行与升级的过程中,企业必须考虑在可以容忍的风险级别和可以接受的系统运行效率之间配置服务 DBMS 的可信策略,制定并实施 DBMS 的安全/可靠控制机制。这就要求我们提供可信代价分析比较工具,定量分析系统提供的各种保护机制及其效率,有效地指导用户正确地选择可信策略的实施方案。

传统的安全测试工具只是从功能上静态地确认 DBMS 的安全机制,基准性能测试只考虑最佳配置下的系统吞吐量,还没有通用的可信代价测试基准指导 DBMS 各种可信保护策略下的系统性能测试。本文提出安全代价测试工具既可以帮助数据库最终用户、安全咨询组织、数据库产品厂商制定、评价、选择 DBMS 可信策略提供定量的指标依据,其评测和度量指标也可以帮助数据库研究人员设计、开发高效的可信信息系统。

2 数据库安全评测

测试分为手工测试和自动测试。DBMS 可信功能手工测试主要通过其提供的图形界面和接口做确认测试(当然也采用一些脚本程序)。目前比较认可的安全测试标准是国际通用准则(CC)^[2]。所以在评测 DBMS 安全等级之前,一般都会按照用户安全需求建立一组安全保护轮廓,再针对被测系统建立安全目标,以作为指定的信息产品评估基础的一组安全要求和规范,最后按照评估指南及其步骤对被测系统进行确认测试。

涉及 DBMS 安全自动测试工具分成安全等级测试工具、安全漏洞扫描工具、SQL 注入安全漏洞测试工具、拒绝服务攻击测试工具、缓存溢出测试工具等。现在商品化比较好的面向企业用户的安全工具主要是安全漏洞扫描工具,例如针对数据库安全漏洞扫描包括 ISS 公司的安全数据库扫描工具、下一代公司的智能安全评估工具套件、Application Security 公司的 Web 应用安全测试工具等。分析这些工具,可以发现它们的主要技术原理包括:

- 1)建立了安全漏洞数据库,这样用户可以及时更新相关产品发布的最新漏洞;
- 2)提供了一个通用的测试框架,给出了必要的模拟恶意攻击及其接口,以便集成发现产品的安全漏洞;
- 3)提供一些分析模型以便对系统使用的安全策略进行建模分析,发现其不一致性、不完备性等;
- 4)制定了安全测试用例,供用户参照。

这些工具都忽略了安全/可靠等可信策略对系统性能的影响,没有与被测系统的业务模型和运行特征动态地结合起来,特别是在特定应用环境中如何配置这些安全策略,在保证

^{*})国家 863 项目(2007AA01Z156)、国家自然科学基金项目(60673140)、北京市基金项目(Z07000100730702)。叶晓俊 博士,副教授,主要研究方向为数据组织与管理、数据库技术、隐私保护;王建民 教授,主要研究方向为信息系统、 workflow 技术、数据库技术。

系统安全运行的同时减少其对系统性能的影响。另外,这些工具都是面向企业最终用户的,对于指导企业数据库管理员的可信策略配置来说还不够。因为安全策略除了要满足安全功能需求外,还应该满足系统的可用性的要求。再者,如何建立安全攻击模型及其评价指标,如何定制这些测试环境,满足不同的测试目的,减少测试成本,都是有待解决的问题。

因此文献[5]提出了一个面向 DBMS 的安全性能基准^[4]:依据 TPC 性能基准的工作负载模型,通过引入故障负载(模拟恶意攻击)研究 DBMS 在不同安全等级策略下的安全代价。可惜的是,作者只考虑了安全控制对性能的影响,没有将 DBMS 系统的其它可信属性(如可靠性、可用性)解决方案结合起来考虑可信策略保护的代价。

3 数据库性能基准评测

性能基准测试是指根据性能基准设计检测程序,搭建检测环境,进行性能测试,并把检测结果与相同检测程序在相同系统或另外系统上的运行结果相比较的整个过程。目前比较认可的性能基准分为事务处理性能理事会(TPC)性能基准和标准性能评估公司 SPEC 性能基准。这两个基准的测试目的是不一样的:TPC 是面向最终用户的,是测试系统的整体性能指标的;SPEC 更专业些,可以测试被测系统的某些特殊指标。

使用基准测试有很多优点,因为利用测试结果我们可以对不同的系统做一个定量比较。当然基准测试也具有局限性:

1) 基准测试通常是测试系统可能达到的最佳性能;系统硬件、数据库实例及其数据存储等配置在测试前都经过了优化。实际的应用系统是达不到这样的配置水平的,需要根据企业应用的安全性、完整性、可用性等需求和企业的实际基础设施设置对应的配置 DBMS 运行参数(例如检查点、日志多路复用、数据加密),这些 DBMS 可信策略的配置将影响应用系统的实际性能。

2) 基准测试在最大工作负载下测试系统的性能。在不同负荷和安全策略保护下,DBMS 提供了不同的配置参数,以适应不同的应用需求。因此性能测试应该考虑系统的健壮性、可靠性、可用性、可维护性、安全性等可信需求。换句话说,基准测试不仅要考虑工作负载,还应该考虑系统测试过程中可信保护机制和故障负载解决方案对性能的影响。

3) 数据库性能基准测试只是检测 DBMS 服务器性能,并不需要把应用运行环境(如网络基础设施)考虑在内。而在真实应用环境中需要考虑人和硬件环境的因素,例如人为错误导致系统可用性及其安全与性能代价等,从而给出更加实用的性能指标。

考虑上述因素对系统性能的影响需要用测试数据来说话,所以需要安全等可信策略对系统的性能影响的评价基准、方法及其工具,这样才能够以数据的方式准确地、定量地给出系统的可靠性、可用性、安全保护、安全性等代价。

4 可信赖性能评测

性能基准是在最优的测试环境和最佳的数据库配置下测试系统的整体性能,没有考虑系统在不同的可信保护策略下面对系统的不同故障负荷(包括各种攻击)下系统的性能和可用性。因此基于 TPC 性能测试的 DBMS 系统的性能指标受到数据库最终用户的怀疑。因为随着人们对信息系统的依赖性的不断增强,构成信息系统核心的 DBMS 可信赖性研究变得越来越重要。因为可信赖性不但是度量各种系统服务质量

的重要指标,而且它与安全性策略极大地影响着系统的整体性能。

过去的研究以追求高效行为为目标,而今天信息系统需要建立高可信的服务。可信赖性必须成为可以衡量和验证的指标,因为终端用户更关心应用系统的可用性、可管理性、可靠性、可伸缩性、安全性等可信指标。经典的性能基准程序实际上只能评测反映系统处理能力方面的性能指标,不能评测可信赖性指标。可信赖性能基准程序应具备以下测试特性^[4,5,7]:

1) 可再现性:它保证当另一方执行同一个基准程序时能够获得等价性的结果;

2) 代表性:不同的应用领域具有不同的工作负载和故障负载,从而可能需要不同的基准程序;

3) 可移植性:可运行在多个不同的目标系统上,以便比较它们的性能;

4) 容侵性:由于基准程序一般要求对目标系统做一定的修改,因此如何把这种侵入(如物理侵入)降低到一个可以接受的程度是基准程序设计时需要考虑的一个重要因素;

5) 抗干扰性:必须尽量降低由基准程序所引起的对目标系统的非期望的干扰;

6) 可扩展性:这样可以使它能够适用于不同规模的目标系统;

7) 可观测性:希望所采用的插装机制能够探测到更多的系统状态;

8) 执行开销:必须在执行开销与完整的、高精度的评估结果之间进行权衡。

2001 年底,欧共体在 1992 年开始的可信计算系统研究的基础上启动了 DBench 项目^[4]。这个项目从概念框架、威胁标识和评估使能技术、基准定义、测试和验证及其测试评估程序等方面进行了深入的研究,提供了以下问题的解决方法:

1) 描述和评估一个组件/系统的可信赖性;

2) 识别系统的弱点;

3) 比较可选解决方案的可信赖性。

DBench 目标是提供可信赖性基准评测的概念、规格说明和指导规则,开发可信赖性基准评测的原型工具。例如针对 DBMS,DBench 给出了一个包括工作负载、故障负载及其度量的可信赖性能基准组件结构。基于 Oracle 和 TPC-C 性能基准,并按照图 1 所示的测试步骤,Madeira 教授通过增加故障负荷,从数据库恢复、人为故障等方面研究了在线交易事务系统的数据库可信赖性能测试指标,并进行了实验验证^[4]。

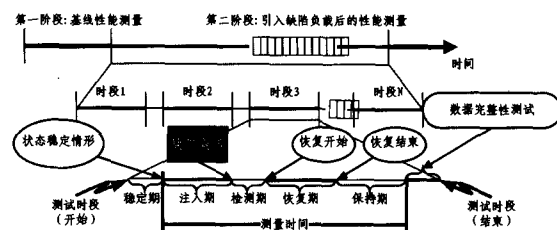


图1 可信赖性测试流程

从图1看出可信赖性基准程序是运行于需要确定可信赖性度量的系统之上的一组工作负载和故障负载,或者是一组指示系统处理内部故障和外部故障能力的程序。故障负载由一组模拟系统在现场将要遭遇到的真实异常情况的各种威胁及其应用条件所组成。

传统的安全性包括机密性、完整性和可用性,可信赖性包

括可靠性、可用性、防危性、安全性等。因此两者的指标在子概念上存在交叉,存在整合的可能。从方法论的角度来考虑,系统失效无论起因是外界的攻击还是系统内部的故障,所采取的解决方法是一致的。因此,我们可以在性能基准测试工具基础上集成这些可信测试指标。Jonsson 教授从被测系统与环境交互的角度,将两者整合在一个 security/dependability 概念模型中,提出可以用完整性、正确性和可信性三个属性来统一描述可信性和安全性,并给出了图 2 所示的按照防护和行为属性重新划分的可信性/安全性概念模型^[3]。

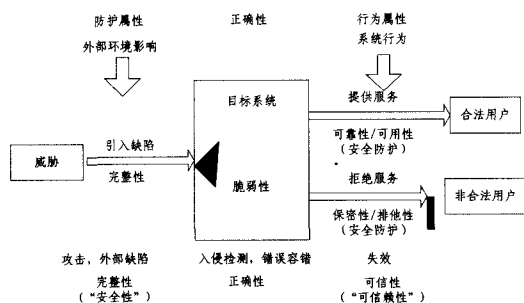


图2 可信性/安全性概念模型

5 安全代价测试工具的设计

基于可信性和安全性的概念及其上述集成框架,通过在 TPC 性能基准中引入故障负载,建立一些可信度量指标,并增加测试系统的业务模型和数据比例的定制性,我们设计一个数据库可信代价评测工具。该工具具备下列功能:

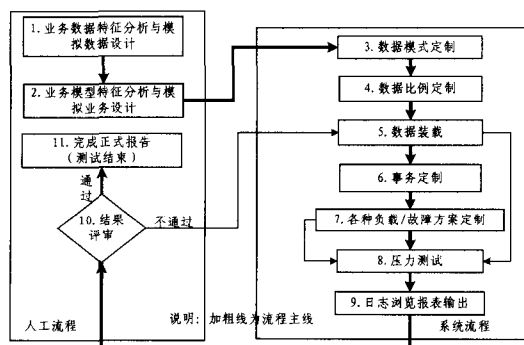


图3 安全代价(性能)测试的流程

1) 根据应用数据分布规律,能够生成可变规模的应用数据,包括数据规模、数据比例关系等,以满足不同应用的负载特征;

2) 根据应用负载特点和 TPC 事务模型允许定制事务并发比例和工作负载,提供自定义事务能力;

3) 根据数据库应用故障特点,基于 DBMS 安全控制机制、可恢复机制等特点分析 DBMS 的威胁和脆弱性,以便定制 DBMS 的故障类型和故障负载;

4) 能够根据应用数据处理过程,定制一些数据访问控制的脚本,实现故障负载的自动加载(注入);

5) 根据可信性指标和等级安全性要求、搭建测试环境,根据若干测试结果,预测安全策略的性能影响。

设计工具采用 XML 对测试对象的数据模式(包括字段属性、取值及字段间的主外键关系、表之间数据规模、比例关系等)、测试事务及其比例等进行动态配置,系统能针对此配置自动向被测数据库初始化一定规模的模拟数据,并按照设定的事务特点和压力特征、可信解决方案进行测试。系统测

试基本流程如图 3 所示。

系统的开发采用面向接口开发的动态链接库(DLL)技术对事务模式进行动态配置。测试终端事务调度引擎如图 4 所示,我们采用 IOCP 等技术构建的高性能测试终端事务调度引擎,保证了测试系统的可伸缩性和减少了被测系统的配置成本。

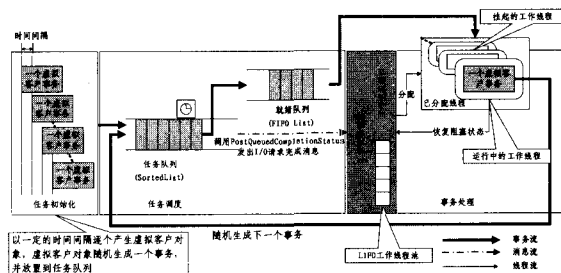


图4 测试终端事务调度引擎工作模型图

系统提供了各种图形用户界面,用于配置测试环境、业务模型、数据规模及其比例等(如图 5)。安全策略设置和可靠性配置主要借助于 DBMS 提供的管理工具。

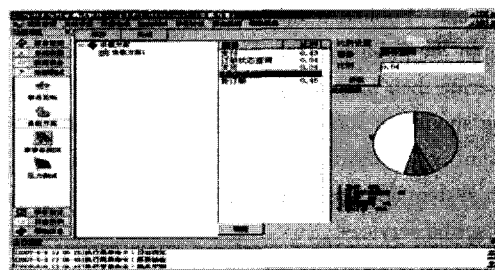


图5 工具图形管理界面

结束语 随着数据库技术广泛应用,安全与性能测试在信息系统开发、调优、选型中成了不可或缺的一环。可信性性能测试有助于优化可信系统的结构,还有助于开发新的数据库安全测试技术、可测试性设计方法和可信性设计方法。

本文介绍了一种将安全、可靠与性能结合起来进行统一评测的性能测试工具的思想及其所开发的工具。该测试工具框架具有占用系统资源少、可扩展性好、易用性强,能够模拟大规模的用户,能模拟真实的应用环境等优点,并已在国家某安全评测中心得到验证。

参考文献

- [1] Brown A. Availability Benchmarking of a Database System. UC Berkeley, CA, December 2000
- [2] Criteria C. Database Management System Protection Profile (D-BMS PP), May 2000
- [3] Jonsson E. Towards an Integrated Conceptual Model of Security and Dependability// Proc. of the 1st International Conf. on Availability, Reliability and Security. 2006
- [4] Madeira H, Kanoun K, et al. Towards a Framework for Dependability Benchmarking// Proc. of EDCC 2004
- [5] Vieira M, Madeira H. Towards a security benchmark for database management systems// IEEE/IFIP International Proc. of DSN. 2005
- [6] 孟小峰,周龙骧,王珊. 数据库技术发展趋. 软件学报, 2004, 15 (12)
- [7] 段云所,刘欣,陈钟. 信息系统组合安全强度和脆弱性分析. 北京大学学报, 2005 (3)