面向业务的IT管理系统设计与实现

甘春明，刘连忠
（北京航空航天大学 计算机学院，北京 100083）

摘 要：业务对应于信息系统，业务的正常运行是由支持信息系统的各种软硬件资源的正常运行来保障。但目前对业务的运行环境的管理主要从IT元素出发，存在“管理孤岛”现象，为解决该现象，设计并实现了面向业务的IT管理系统。该系统基于安全审计与监控机制，采用事件描述语言(EDL)将审计和监控得到的大量告警、故障信息进行整合分析，并最终映射到相应业务系统的可用性和可靠性，可以从业务角度把握整个系统的实时运行状况，方便了系统管理人员的工作。

关键词：面向业务；监控；日志；告警；事件；故障
中图分类号：TP311.52 **文献标识码**：A **文章编号**：1673-629X(2008)06-0156-04

Design and Implementation of Business-Oriented IT Management System

GAN Chun-ming, LIU Lian-zhong
(School of Computer Science, Beihang University, Beijing 100083, China)

Abstract: Business is corresponding to information system. The operation of the business is supported by the operation on the resources of the corresponding information system. However, there are so many managements of the support environment are based on the respective IT elements. To resolve the problems of islands of management in the traditional IT management area, presents a business-oriented IT management system which based on the technology of security audit and monitor. It used the event description language to analyse so many scattered alarms and faults in an unified way. The analysed results was mapped to the usability and reliability of the relative business system at last. In that the system administrator will know the state of the whole system from the business perspective while it is running in real-time.

Key words: business-oriented; monitor; log; alarm; event; fault

0 引 言

近年来，随着信息技术的迅速发展，各种网络应用系统的建设也以很快的速度逐年递增。各行业IT维护和管理成本与日俱增，对安全性能的要求越来越高，IT基础建设的可用性和可靠性越来越让人担忧。

现有各行业采用的IT管理工具大都是从传统的IT网元监测出发，基于各自独立的派系模式，管理自动化程度低，维护人员疲于应对多套管理工具，出现了多种形式的告警、分离的故障和投诉。IT环境作为一个整体应处于为企业业务服务的角色，急需摆脱IT管理的高成本低效率，摆脱IT管理与业务管理相脱离的现状，渴望一个从业务视角出发的、完整易行的管理工具，从被动分散的维护转变为主动集中的控制和管理。此外，传统的IT管理监控基本上都仅限于网络管理、应用管理等方面，而很少涉及安全审计这一信息安全领域。安全审计作为CC标准[1]中的一部分，在信息化飞速发展的今天扮演着越来越重要的角色。鉴于此，设计并实现了结合安全审计与监控技术、面向业务的IT管理系统。

收稿日期：2007-09-01
基金项目：国家“863”计划资助项目(2005AA113040)
作者简介：甘春明(1983-)，男，硕士研究生，研究方向为信息安全、网络管理；刘连忠，硕士，教授，研究方向为网络安全、数据库技术。

1 面向业务管理的内容

新一代的企业IT架构管理需要将IT作为企业业务服务的整体框架来统一管理，面向客户和业务，将通常被分割管理的网络、系统、应用软件，直至企业内外依赖于IT网络的各项业务及服务，都整合于一个综合支撑管理平台，实现集中集成管理，还原其原本就不可分割的相互依赖性和统一性。

图1是某部委干部管理业务的简单拓扑图。如果从传统的IT管理产品出发，管理这个业务系统，需要分别管理文件服务器、数据库服务器和WEB服务器，

这会导致IT管理和业务管理脱节的问题。当网络管理员发现数据库服务器出现问题时,IT网络管理员可能只认为数据库有些常规问题,但此时整个网络办公系统已陷入瘫痪。

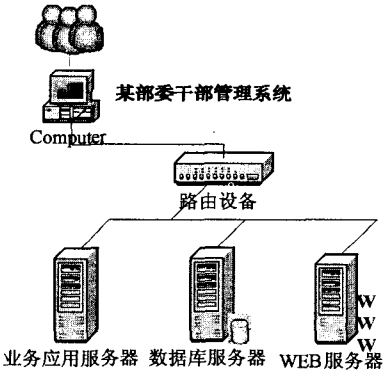

图1　从业务角度管理IT

这个问题从业务角度出发进行管理,网络管理员只要监控办公系统的整体业务视图就可以,当办公系统中的任意一台服务器出现问题时,首先管理员和业务员都可以看到整个办公系统视图在报警,而且能够通过视图迅速直观地定位故障。

以业务为主线的管理方式就是要消除传统管理机制下的IT管理孤岛现象。将各种管理信息整合起来,将网络的联通性、应用服务器的内存负载率、数据库的连接数、操作系统的违规事件等状态信息和审计信息与业务的响应时间、可用性关联起来。

2　面向业务的IT管理系统总体架构

面向业务的IT管理系统(Business－Oriented IT Management System, BOITM)主要由资源管理、安全审计、性能监测、性能报告、故障管理、拓扑管理以及自身的安全管理等几部分组成,其总体结构如图2所示。

3　系统实现

3.1　面向业务的资源管理

在BOITM系统中,基础设施资源多种多样,如操作系统、数据库、应用服务器、邮件服务器、EJB组件和COBAR组件等软件资源以及路由器、交换机、主机等硬件设备。一个业务依赖于很多资源,而一个资源也可能支撑多个业务,因此业务和资源之间的关系是错综复杂的,设计一个良好的资源模型很重要。

根据CIM(Common Information Model[2])提供的定义,BOITM系统设计的资源模型主要包括:

(1)数据收集:资源监测模型通过轮询的方式周期性地收集数据,对数据加时间戳,标识数据的时序关系。

(2)周期:对收集数据的时间间隔值。

(3)门限值:对可接受资源性能参数的限制,该值可能是定值也可能是区间值。

(4)事件:当一个资源状态达到门限值时产生,触发系统进行相应处理的提示。

(5)属性:通过字符串或数值对资源某一方面的描述。

(6)动作:对触发的事件采取的处理。

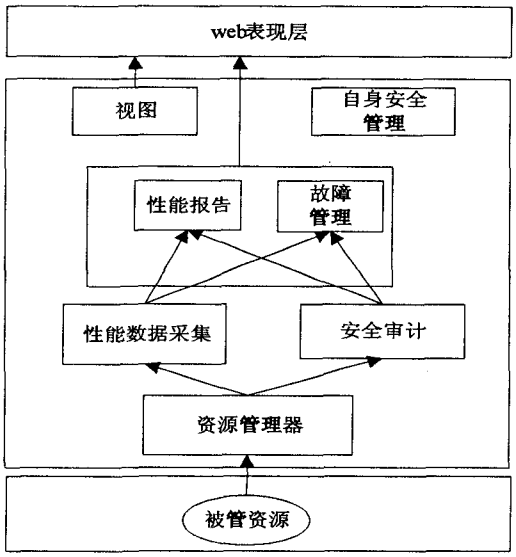

图2　BOITM系统的总体架构图

文中尝试采取自动发现和手动修改相结合的方式来实现资源的定义管理。通过SNMP和内部Agent接口自动发现开放了SNMP接口或者安装了BOITM Agent的网络节点(如路由器,交换机,服务器等)。通过图形的方式自动生成业务拓扑视图;根据发现的设备类型,使用SMNP Get方式采集被监测网络节点的配置信息,系统管理人员可以通过手动的方式来修改资源的一些基本信息和参数。

3.2　安全审计

各种网络设备、操作系统、应用服务器等都可产生大量的日志数据。这些日志数据详实地记录了系统和网络的运行事件,是安全审计的重要数据[3]。将这些彼此孤立的日志信息以面向业务的角度来整合审计是本系统的目标之一。安全审计模块由日志采集器、日志格式转换器、日志分析器三部分组成。

日志采集器负责收集主机所产生的操作系统的内核日志、应用程序日志、网络设备(如路由器、防火墙)日志、IDS日志、重要文件以及用户活动的状态与行为等。日志格式转换器将采集的各类日志转换为统一的、规范化的审计数据格式。日志分析器采用高效的模式匹配算法,对已规范化的日志进行筛选和分类处理:将确认为对入侵检测和评审无关的信息丢弃;将已

经检测到的攻击行为送报警器;将不能确定的信息送往中心服务器进行关联分析。

处理流程如图 3 所示。

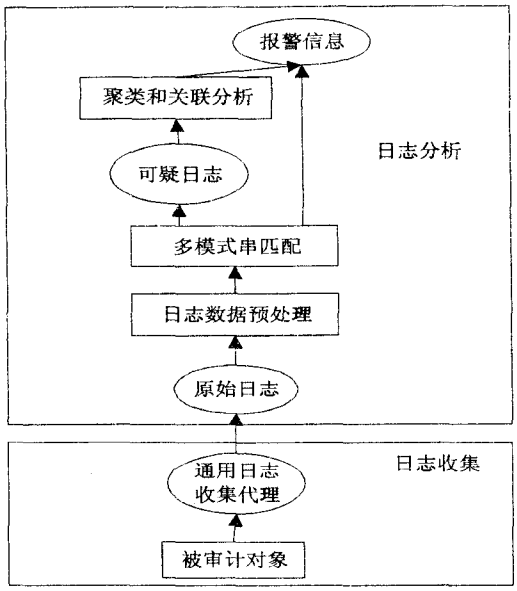

图 3 安全审计模块

3.3 基于探测器的资源性能监测

网络中每个节点、每个应用的性能好坏都直接影响到网络和业务的正常运行[4],对每个资源的性能数据采集是进行监控的前提。

基于监测器的面向对象的数据采集可以将每一种监测器都作为一个相对独立的小插件,本系统采用 JMX 技术,将网络设备、主机、数据库、操作系统及其它可达的软硬件资源封装成 MBean[5],从这些资源中采集状态和性能数据,并向 BOITM 的功能组件(如故障管理和性能管理等)提供最新的监测数据。这样的监测体系旨在适应复杂异构的网络环境、不断发展的网络技术和 IT 基础架构的频繁升级改造。

监测器的主要监测手段是基于 SNMP 协议实现的。同时也充分考虑到实际网络中复杂异构的设备类型和用户业务的不同要求,对于不支持或者不开放 SNMP 协议的被管理对象,提供基于 SSH 和 Agent(代理模块)的监测方式。

3.4 性能报告和故障管理

在获取日志审计信息和资源性能数据后,BOITM 系统对这些数据进行综合处理,以业务为主线进行性能统计和分析报表,并基于业务视图计算业务的服务水平(SLA,Service Level Agreements)报告,包括故障时间、有效率等,为此研究中采用计算量小、适合于联机建模的线性回归模型,其一般形式是:$y = b_0 + b_1x_1 + b_2x_2 + \cdots + b_mx_m$,该模型通过模型参数 $b_i(1 \leqslant i \leqslant m)$ 把解释变量 $x_i(1 \leqslant i \leqslant m)$ 与响应变量 y 联系起来。对于线性回归,知道了说明变量 $x_i(1 \leqslant i \leqslant m)$ 以及相应的样本数据,很容易用最小二乘法求得相关的模型参数 $b_i(1 \leqslant i \leqslant m)$。文中采用多元线性回归分析法[6]和逐步回归的选元法作为联机算法来计算 SLA 值。

BOITM 系统提供强大的故障管理功能,对用户网络及系统发出的预警信息和故障信息进行及时的整合和自动处理。本系统采用的方法是:利用日志分析后的结果生成相应的告警事件;利用不同类型的监测器采集系统级和应用级可用性信息,并在监测器指标测量失败时发送告警事件;利用 Syslog 接收器获取相关设备转发的 Syslog 信息;利用 SNMP Trap 接收器获取设备或第三方管理工具的事件告警信息,并实现过滤和相关性分析的处理。最后将上述告警信息进行格式化后实现集中统一的监测和管理。

由于面向业务系统将会产生大量重复的告警事件,因而需要有很好的压缩机制。

3.4.1 合并重复告警和告警屏蔽

BOITM 将根据内部的相同事件判定条件(告警标识符唯一标识一个告警)将重复告警自动合并成一条告警,只标识告警发生的次数,并在告警的详细信息中记录各次发生的时间,从而减少告警信息的数量,有效防止告警风暴。

故障管理的告警屏蔽功能是通过预定义的过滤规则,将不需关心的告警事件予以滤除。使管理员将精力集中在重要的告警事件的监视和处理上,屏蔽干扰信息。

3.4.2 事件相关性分析

在充分采集网络环境中各种事件的同时具备智能化的事件相关性分析机制,能有效地屏蔽各种衍生事件、干扰事件和误告警。网络环境中来自不同信息源的告警和事件信息(无论是来自网络节点、主机系统、还是应用软件)必然是相互依赖不可分割的。经常发生由于网络端口不通,导致服务器失去联系、业务无法访问等连锁反映,这种情况下如果将 IT 分割为不同层次分别管理,管理员将会看到多个管理工具同时出现大量告警,很难在短时间内定位真正的故障根源。因此需要提供一种根源原因相关性分析方法,使得管理员能够合理建立从 IT 元素到业务的、跨层次的任何事件依赖关系,当有依赖关系的多个告警在指定的时间窗口内出现的时候,管理员只在告警浏览器中看到一个根源告警。

BOITM 系统提出了一套灵活并且表达能力丰富的规则语言 EDL(Event Description Language),允许程序员在规则中指定复杂的事件模式,并设计了一个基

于EDL语言的事件流分析引擎。EDL提供原始事件、与、或、非、时序和时间观测器6种表达式。该语言跟其他事件描述语言相比有如下特点:

(1)提供了与时间相关的运算符,为管理人员提供了定时的提醒和任务运行的功能。

(2)增加了控制运算符every,用来控制事件模式的产生和结束。

(3)针对GEM[7]等语言的not运算符的不足,改进了该运算符的语义,增强了not运算符的灵活性。

事件流分析引擎采用基于状态分析树的事件检测算法实现从事件流中找出匹配事件模式表达式的事件序列,语言解析需要经过以下几个阶段,首先是词法分析,然后是语法分析,语法分析之后生成抽象语法树,接下来再进行语义分析,最后将分析结果生成抽象事件树。

基于状态分析树的检测机制如图4所示。

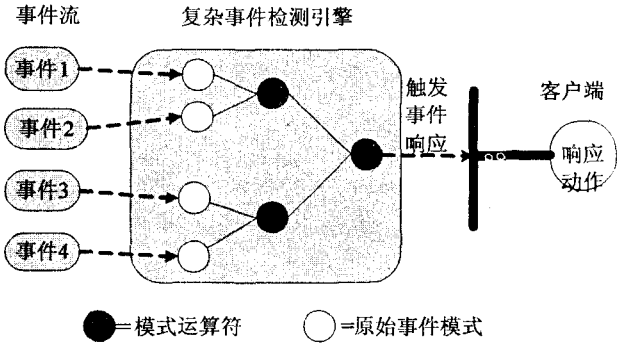

图4　基于状态分析树的检测机制

该检测算法的步骤如下:

第1步:接收事件流E;

第2步:读入复杂事件模式;

第3步:生成抽象事件树;

第4步:生成状态分析树SAT,并且生成当前的原始事件模式匹配路径attributePath。

(1)从事件流E中得到事件e,首先调用原始事件检测算法判断事件e是否符合原始事件模式,如果匹配没有成功,返回到(1);

(2)改变SAT树的状态,变换SAT树的结构,如果SAT树到达Root根节点,并且该树的状态值为真,那么通知监听该SAT树的监听程序;

(3)如果SAT树没有到达Root根节点,得到新的原始事件模式匹配路径,处理下一个事件,转到(1)。

3.5　视图管理

从不同角度不同层次提供多种表现形式的网络拓扑显示对于提高系统的友好性和交互性很重要,特别是对于面向业务的网络应用管理系统。BOITM系统提供以下几种视图:IP拓扑视图、设备视图、业务视图和自定义视图。业务视图是为运营商和企业从业务划分的角度提供IT资源管理的视图,建立从业务(或客户)到IT资源及性能之间的依赖关系。即以业务为主线,将每项业务所依赖的网络资源、系统资源、应用软件贯穿起来,形成绑定业务的拓扑视图,实现面向业务的监测和管理。当业务所依赖的某个IT资源出现告警和故障时,代表此项业务的图标将在拓扑图中呈现不同的报警颜色。

4　结束语

提出了一种面向业务的基于安全审计与监控的IT管理系统,并给出了其设计方案与实现方法,该方法较好地解决了传统网络系统管理中的IT管理孤岛问题,实现了真正面向系统管理人员的IT管理系统,减轻了工作负担,为改善企业IT管理现状提供了比较实用的解决方案,将为企业业务的持续发展提供有效的支撑。

目前该系统已成功应用于某部委的干部管理信息系统中。

参考文献:

[1] Bishop M. 计算机安全学导论[M]. 北京:电子工业出版社,2005.

[2] DMTF. Common information model (CIM) specification version2.2[EB/OL]. 1999-06-01[2003-04-20]. http://www.dmtf.org/standards/cim.spec.v22/.

[3] Schaen S I, McKenney B W. Network auditing: issues and recommendations[C]//In Proceedings of 7th Computer Security Applications Conference. San Antonio, TX: [s.n.], 1991: 66-79.

[4] Lewis L, Ray P. Service level management definition, architecture, and research challenges[C]//In Proceedings of Global Telecommunications Conference, 1999. Rio de Janeireo: [s.n.], 1999: 1974-1978.

[5] Mcmanus E. JSR-255 Java Management Extensions[M]. US: Sun Microsystems Inc., 2004.

[6] 张小蒂. 应用回归分析[M]. 杭州:浙江大学出版社,1991: 67-72.

[7] Mansouri-Samaniyx M, Slomanzk M. GEM: a generalized event monitoring language for distributed systems[J]. IEE/IOP/BCS Distributed System Engineering Journal, 1997, 4(2): 96-108.