文章编号：1005-8451（2011）01-0026-04

信息系统运行安全综合管理监控平台的设计与实现

刘继全
（北京铁路局 信息技术处，北京 100860）

摘 要：本文围绕信息系统运行安全，提出将日志分析、网络管理、环境监控和视频监控等模块集成为一个综合监控平台，实现对全局网络拓扑结构的实时监测、对各类关键设备的日志实时采集分析、短信报警和对机房环境的综合实时监测。最终实现对机房信息系统安全的全方位监测，为信息系统维护人员预先发现问题、解决问题提供科学依据。

关键词：信息安全；综合监控平台；网络管理；日志监测
中图分类号：U291-39 文献标识码：A

Design and implementation of integrated management monitoring platform for running safety of Information System

LIU Ji-quan
(Department of Information Technology, Beijing Railway Administration, Beijing 100860, China)

Abstract: In this paper, it was discussed that log analyzing, network management, environment monitoring and video model and so on, were integrated to be an integrated monitoring platform for the running safety of Information System, it could monitor the entire administration' s network topology real time, collect and analyzed log of all key devices, given alarms through sending short messages to mobile telephones and it could monitor computer room environment real time also. The platform could monitor Information System safety in computer room full-scale, provide scientific basis for Information System maintenance personnel to find and solve problems eventually.

Key words: information safety; integrated monitoring platform; network management; log monitoring

随着信息技术日益发展，信息系统已经成铁路运输、管理和经营等方面不可缺少的辅助手段。特别是近几年来，随着高速铁路的陆续开通运行和调度系统的不断整合，对信息系统运行安全、运行质量提出了更高的要求。以客票系统为例，随着京津城际的开通，列车运行间隔缩短到10 min左右。这就意味着如果客票系统故障延时超过10 min，就可能影响到车站的售票和乘车秩序。同样，随着列车的不断提速，调度系统、施工命令等项目对信息运行安全也提出了更高的要求。信息系统安全运行成为我们的首要任务。

近年来，为了提高运行维护质量，确保信息系统安全，我们陆续采用了一些监测技术，对机房综合环境、计算机生产任务运行状态等进行监控。目前存在的问题主要有：

（1）监测范围不足。信息系统运行主要由4个部分组成：硬件设备、通信网络、应用软件和机房环境，既有的监测系统大都集中在对机房环境、应用系统进程等进行监测，监测范围不足。

（2）监测信息不全。硬件设备故障占系统故障的比例较大，以往在发生设备故障时，我们以及时恢复应用为目标，采取的一些应急措施例如设备重启，致使“现场”被破坏，信息丢失，不利于事后故障分析。

（3）监测平台不同。2009年，北京铁路局信息系统进行整合，信息处有包括原3个铁路分局电子所机房在内的5个机房，采用的监测系统各自不同，没有统一部署，运行值班人员不便维护和管理。

在应用项目实时性越来越高、机房设备越来越多和安全问题各级领导越来越重视的情况下，为了保证信息系统稳定运行，我们提出了建立“大运维”体系，实行“状态修”标准，以信息系统运维安全为出发点和落脚点，建立信息系统运行安全综合管理监控平台，在与传统监测系统有机融合的基础上，采用先进的技术手段，补强原有功能，拓展监测范围，提高监测水平，加大故障发生

收稿日期：2010-10-24
作者简介：刘继全，高级工程师。

前的预警预报比例，对系统设备、网络、应用软件、机房环境实施综合监控和管理。

1 系统设计

在信息系统运行安全综合管理监控平台上运用后台实时数据库和前台展示技术，对生产用计算机的网络联通状态、系统日志情况、机房综合环境、计算机生产任务运行状态实施自动监测，对各类异常情况第1时间报警通知值班人员，替代传统的人工巡视和被动响应的管理模式，实现计算机设备、网络和生产任务的稳定运行。

1.1 建立计算机网络监测

网络设备是计算机设备的重要组成部分，网络设备运行的正常与否关系到运营生产信息的传递，所以对计算机网络的监测非常重要。网络监测运用WWW和Java技术，以及面向对象的编程技术，实现对所辖多种类型网络设备的性能和故障的监控管理。实现对多种类型主机设备的性能和故障的监控管理；实现对所辖的安全设备的性能和故障的监控管理。实现对网络流量及网络链路质量的监控；实现对网络主机及网络设备的日志进行管理。根据监测到的性能原始数据，对信息系统运行状况，运行趋势等进行分析。

1.2 实现设备运行日志实时监测

能够实时对核心生产网络设备、客票相关设备和应用服务器小型机进行监控，减少技术人员的工作强度。可以设置不同的用户组分配权限，便于管理和考核。能够在设备发生重大故障时，通过短信方式通知机房值班人员及相应的技术人员，提高应急响应时间，最大限度缩小故障的影响范围。能够将收集到的日志信息长期保存，以便日后的故障分析并产生相应的分析报表。

1.3 完善计算机运行环境监测和应用项目监测

计算机运行环境包含电力环境、周边环境和安全环境等几部分，对计算机运行环境的监测就是通过采用各种传感器和变送器等设备将模拟信号转换为数字信号，将信号接入到计算机，然后对各种信息进行综合处理。采用数字信息处理和模拟信号集成技术对大中型计算机机房温度、湿度、电源输入频率、电压和电流等物理状态实施监测。

为实现对计算机生产任务实施监测，采用控制机轮询方式或代理机制，对计算机各应用项目的状态参数进行对比，超出比较阈值的限度，系统作出判断，按照用户参数要求，将故障现象、原因和解决方法及时通过声响、屏幕显示等方式通知到值班员或项目管理员。

1.4 视频监控

对主机房、各设备间进行环境安全视频图像的监控。

2 系统功能

2.1 综合网络管理模块功能

（1）自动发现：能自动发现路由器、交换机、服务器和其它网络设备。通过参照ARP表创建可能活动的设备列表，能够加快发现进程，但同时又执行一次彻底的ping扫描，以避免忽略某些设备。还能发现设备上运行的服务(如HTTP等)。通常在2 min之内就能发现一个C级的网络。

（2）映射设备：能自动为服务器、路由器、打印机、交换机和防火墙创建基础架构视图。用户根据业务要求创建业务视图来分组设备。

（3）实时网络监控，及时告警：只要检测到问题，就会通过e-mail或SMS通知管理员。综合网络管理系统的网络监控功能还包括运行外部程序、系统命令或播放音频文件。

（4）网络流量分析：对WAN和LAN深入流量分析。能够收集和分析诸如NetFlow、JFlow和SFlow等流量。深入分析网络流量接口明细，例如应用、资源、目的地、会话以及QoS。除增强网络监控和排除故障外，可以提供带宽趋势信息，便于规划容量。可以生成丰富的网络级或设备级的报表，以便分析可用性、应答时间、网络流量、接口利用率或应用应答时间。

（5）网络链路质量监控：不良的WAN链路会影响业务，网络管理软件有助于基本的WAN监控并对发现WAN问题大有用处，使用WAN视图帮助可视化WAN链路。当链路失败时，视图会反映出来，根据严重性以红色，橙色或粉色显示。

（6）丰富的报表：可以生成丰富的网络级或设备级的报表，以便分析可用性、应答时间、网络流量、接口利用率或应用应答时间。

2.2 日志分析模块功能

（1）采用BS方式，支持H3C、CISCO网络设备，LINUX、SOLARIS、HPUIX、AIX操作系统，Windows操作系统。不用安装代理，只需在其中的Syslog中加入1条日志转发语句即可，Windows系统采取主动添加，提供主机的用户名和密码。通过集中管理各种设备的日志，省略了每次都要登陆不同设备查看日志的繁重工作。

（2）可以通过数据库过滤功能，设置1台或1组相同设备的日志级别或关键词过滤，以节省日志服务器存储空间和日志级别较高的信息的快速过滤。

（3）可以设置告警级别提示，把1台设备或1组设备，根据日志安全级别或事件ID或日志文件中的关键词设置告警消息提示，在前台显示，并通过电子邮件或短信方式发给相应的管理员。

（4）可在Evenlog主页显示所有添加的设备，可通过自定义时间间隔查看相应时间段设备的日志情况。

（5）可以通过归档文件管理，设置文件归档时间间隔，并设置归档文件采用ZIP格式进行压缩时间间隔，可以及时存储备份日志文件，将已经备份的日志文件删除，节省空间。可以将归档的文件自动加载到数据库中进行浏览，将已经归档的日志根据日志级别和日期进行浏览。

（6）可以针对某1台设备或1组设备产生自定义的报表，使该设备设置的过滤条件产生的错误信息以图表的形式显示。直观地发现自定义时间段中哪种级别日志出现频率较高，及时发现问题。

（7）可以在evenlog主页查看和搜索相应的设备信息，并按照设备主机名和主机组进行排列。

（8）创建自定义报表配置之后，可以设置计划，在指定的时间间隔自动生成报表。

（9）可以根据日志级别和相应事件产生4种规范报表，在以后的工作中使用，产生法律效力。

（10）可以产生基于事件级别、事件分类和告警趋势的报表，及时发现相应设备或设备组的问题和漏洞。

（11）日志服务器发生问题，可以通过电子邮件方式通知管理员。

（12）可以通过用户管理，实现管理员、操作员和访客的权限。

（13）支持短信告警平台。

（14）管理员分组管理，可以根据自己的权限管理本组的设备。

（15）可以查看管理员登陆的记录，可以根据登陆情况确定是否查看日志。

（16）完善告警信息内容，在原有的日志源进程、主机名和告警名称基础上，增加危机程度、发生次数、信息内容和相同信息内容限制发送次数等参数内容。

3 系统实现

3.1 网络管理模块

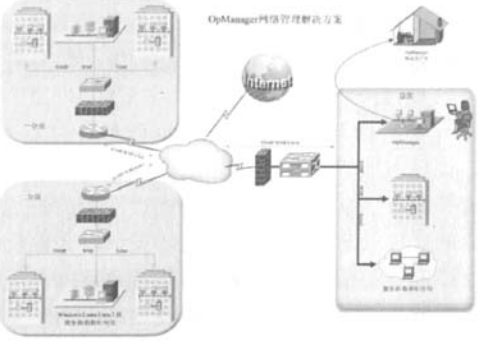

图1 网络管理解决方案示意图

将综合网络管理系统部署在企业网络中，可以通过SNMP（简单网络管理协议）管理整个网络环境中的所有支持该协议的设备。图1为网络管理解决方案示意图，图2为网络管理处理流程。

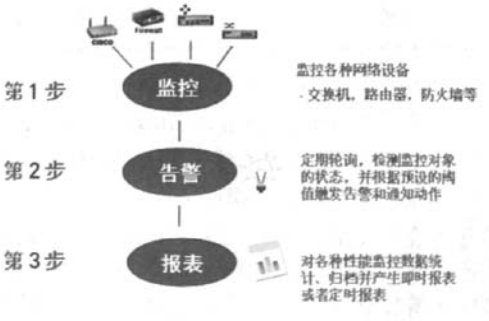

图2 网络管理处理流程

3.2 日志监控模块

将日志分析系统部署在企业网络中，通过

Syslog方式获取并统计整个网络环境的日志。图3为日志分析系统架构示意图，图4为日志分析处理流程。

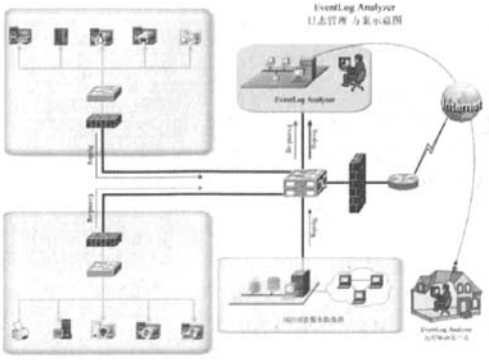

图3　日志分析系统架构示意图

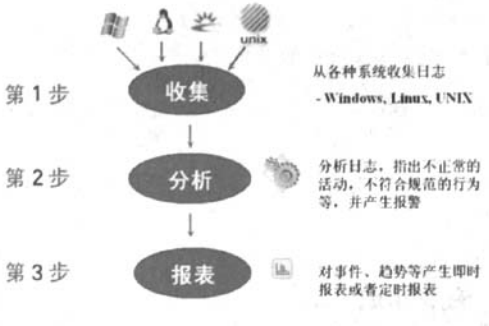

图4　日志分析处理流程

4　关键技术

4.1　网络监测模块

综合网络监测系统对WAN，服务器，应用程序等所有IT设施提供全面的故障和性能管理。实现网络和数据中心监控能力，从而使复杂的IT管理简单易行。它通过3种不同的方法执行网络监控：SNMP、WMI或Telnet/SSH不间断监控重要的设备健康参数，并支持阈值，另外也可以监听设备的SNMP陷阱。

4.2　日志分析模块

日志分析系统是一套基于Web的日志分析工具，采用Syslog机制，不用安装代理，通过网络设备和服务器开启Syslog服务来接收日志。它能全天候监视网络设备和服务器的日志，并收集、分析和汇总整个企业范围内网络设备和服务器的日志。并在网络设备和服务器产生严重的事件的时候通过短信或邮件方式立即通知管理员。

上述2个模块的主程序均采用Java开发，具有良好的跨平台性。采用Apache作为Web服务器，实现B/S架构，用户只需浏览器即可使用，大大简便了用户操作。数据库采用MySql，MySql是一个快速、多线程和多用户的SQL数据库服务器。MySql的核心程序采用完全的多线程编程。线程是轻量级的进程，它可以灵活地为用户提供服务，而不占用过多的系统资源。MySql拥有一个非常快速而稳定的基于线程的内存分配系统，可以持续使用而不必担心其稳定性。另外，日志采集器采用C语言编写，大大加快处理速度，提高吞吐量。

5　结束语

信息系统运行安全综合管理监控平台将日志分析、网络管理、综合监控和视频等功能集成为一个综合监控平台，实现对全局网络拓扑结构的实时监测、对各类关键设备的日志实时采集分析、短信报警和对机房环境的综合实时监测，最终实现对机房信息系统安全的全方位监测，2009年6月开始试运行，收到良好效果。以日志分析系统为例，采用传统的人工监测方式，每台设备登陆查看日志需要5 min左右，所有的设备都要登陆查看一遍需要3 h～4 h，使用该系统后，现在查看20-30个设备日志只需要5 min左右。自2010年1月1日正式投入使用以来，截止到2010年5月，预警、主动发现故障所占比例由年初的21%上升到目前的82%左右。在信息系统安全生产中发挥了重要的作用，在确保计算机安全稳定运行及机房管理方面上了一个新台阶。

参考文献：

[1]（美）Bhai Ji,Y. 网络安全技术与解决方案[M]. 北京：人民邮电出版社，2009，3.

[2] 蒋建春.计算机网络管理理论与实践教程[M]. 北京：北京邮电出版社，2009，1.

[3] 殷兆麟，张永平，姜淑娟.java网络高级编程[M]. 北京：清华大学出版社，2005，9.