NSTL综合运维管理系统应用实践

张婧，韩旸
（中国科学技术信息研究所，北京 100038）

摘要：随着信息技术的发展，各单位信息系统建设规模和复杂度日益提升，确保信息系统安全和业务连续性成为运维工作关注的核心。如何改变分散的、低水平监控和运维现状，借助高水平、安全、高效的统一运维技术实现信息系统高可靠运行，成为当前监控和运维建设的发展方向。本文介绍了国家科技图书文献中心（NSTL）信息系统综合运维平台的建设实例和使用效果。

关键词：监控；运维；信息系统；网络安全
中图分类号：TP3
DOI：10.3772/j.issn.1673-2286.2016.7.012

1 引言

信息技术的飞速发展使各个行业的信息服务系统已经深入社会的方方面面，重要信息系统的安全风险越来越高，中断或停运导致的不良影响和损失不断加大。各国政府和标准化机构为提高信息系统的服务管理水平，陆续出台了一些规范标准。但是，这些标准多面向流程管理，不能代替信息系统运维的技术解决方案，在使用环境上也有诸多客观限制。同时，由于信息系统的规模越来越大，设备数量猛增，从基础设施到应用架构的系统复杂度也越来越高，使安全风险不断加剧，给运维人员带来严峻的挑战。

国家科技图书文献中心（National Science and Technology Library，NSTL）承担着国家科技文献的在线文献信息服务工作。NSTL网络服务系统目前包括文献服务、回溯分析、引文、数据加工、长期保存、集成揭示等应用系统，网络覆盖了中心主站、9 个成员单位和分布在全国的 39 个服务站及 24 个用户管理平台。十多年来，从网络基础设施、业务系统到文献数据资源的规模都在持续增加，给运维人员带来巨大的工作压力，迫切需要改变传统低效的人工运维模式。为此，自2013年开始，NSTL启动IT综合运维管理系统建设，系统覆盖网络、设备、主机、虚拟化平台、数据库和中间件以及NSTL网络服务系统等业务，实现对日常运维管理网络、设备、业务的实时监测和预警。其设计思想和技术体系改变了在众多信息系统运维中存在的分散、低水平、低效率的人工监控运维状况，形成集中高效、安全可靠的统一运维中心，提高运维工作效率，缩短故障处理时间，成效显著。本文着重介绍NSTL综合运维管理系统的特点和使用效果。

2 设计思想

2.1 一体化管理

一体化管理是要建立一套集中、统一的立体监控和智能分析平台，以跟踪各类核心业务的运行情况和IT故障的处理状况，使信息孤岛间建立起关联关系，对各类IT信息进行集中采集、集中处理、集中展现。

集中采集，即实现对基础资源监控、环境监控、应用监控、上层业务等各层次被管理对象的集中采集，实现对物理环境、应用、业务各层面系统的集中接入和运行状态的管理，将原本孤立的IT运行监控手段纳入统一的应用监控平台管理架构。

集中处理，即通过对各类被管对象产生的大量事件进行集中监控处理，实现对各类状态、风险的快速定

位和分析处理。通过甄别源头和成因，还原事件的发生过程，预计风险的影响范围，为IT运行监控运维管理提供可靠的技术手段。

集中展现，即将各类处理信息在统一平台上进行集中呈现，通过业务影响视图展示IT与业务的承载关系，通过性能视图集中呈现各类异构平台和环境的关键性能指标，帮助运维人员一目了然地掌握关键系统健康状况。

2.2 规范化管理

从NSTL整个业务状况来看，系统监控的维度涵盖从应用层到业务层的各类指标，需要和各监控系统、业务系统进行集成接口开发、业务指标梳理、业务模型建立、上层展示功能梳理等多项工作。因此，要定制一套应用监控接入规范，内容需涵盖通信协议规范、接口数据文件内容规范、监控详细指标规范等，以便不同系统或功能模块的整合与衔接，从而提升运维系统的可扩充性。

2.3 精细化管理

为更好地展示核心业务系统关键指标的运行状态，采用基于业务数据仪表盘的展示方式，将核心业务关键业务点以及相关关键绩效指标（Key Performance Indicator）组织在一起集中分析和展示，同时结合各个维度、各个细粒度的统计分析报表，包括业务指标实时性能、业务占比、业务流量、访问量、检索量等，使维护人员能一目了然地查看业务系统的当前运转情况和关键业务指标的当前值和历史性能趋势图，实现对核心业务系统的精细化管理。

3 系统架构设计

3.1 系统架构

综合运维管理系统是一个整合网管、服务器监控和应用监控并且兼容SNMP、ICMP、syslog等多种标准协议的统一运维平台[1]，其服务层面采用B/S结构，配置有 5 台物理服务器，其中 2 台高性能服务器部署控制中心，3 台服务器存放告警和日志收集信息。

综合运维管理系统采用统一的操作界面进行维护管理，统一操作台既可以高兼容性地维护系统的文件、进程和服务，还可显示不同设备的监控曲线、拓扑图、监控规则逻辑图、各类服务器系统的综合状态等。除安装主机代理端和插件外，系统全部为图形配置界面，日常配置管理和监控都是通过Web方式实现。

综合运维管理系统内部由若干控制引擎组成（见图1），对应管理认证、加密、协议、监测、通告、配置、数据、文件等不同应用，实现对监测对象的信息采集、分析和告警。

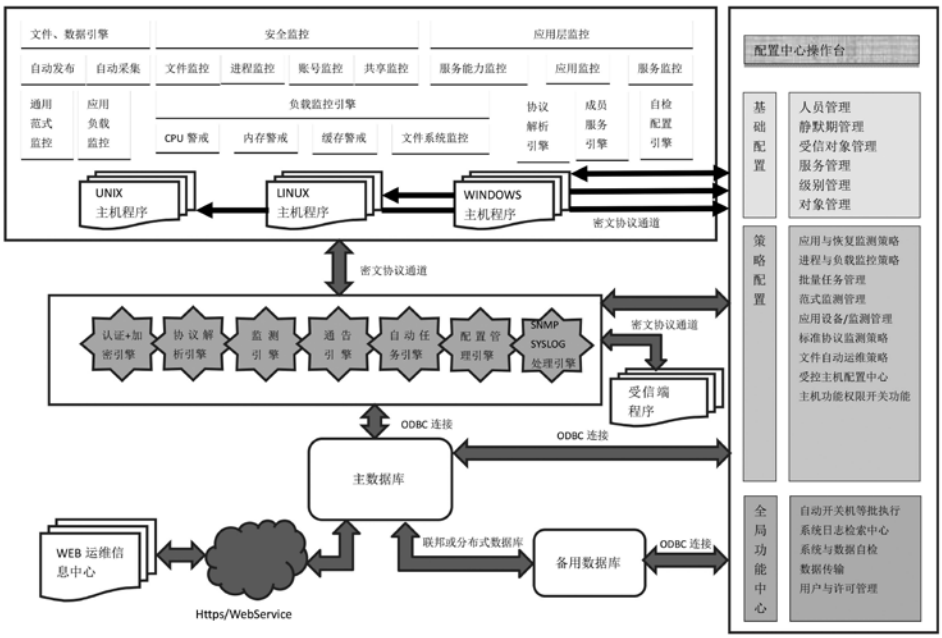

图 1 综合运维管理系统结构示意图

3.2 监测指标体系

综合运维管理系统的监测指标包含被监测设备的硬件、操作系统、资源、进程、负载、端口等关键性参数，通过预先设定临界值和规则，当监测指标高于或低于设定值时，系统就会根据预先设定的规则触发告警。运维工作中，通过协议监测和仿真监测相结合，做到设备与服务分别监测。例如，在对全国几十个服务站的网络和服务监测过程中，系统通过获取每次访问的联通性、响应时间及错误响应代码，精准地实现了由网络、线路、防火墙等原因导致的规模性访问中断的故障定位。网络具体监控指标体系见表1。

表 1 网络具体监控指标体系

序 号	系统监控项目	描 述	监控对象	监控技术与方法
1	CPU	平均CPU负载	服务器OS:AIX、Linux、Windows 数据库:Oracle 服务、Trip服务器	时间区域 临界监控
2	内存	内存使用率Free、Buff等		
3	缓存	缓存使用率，包括Free、Cache、Paging rate、Si、so等参数		
3	磁盘	磁盘空间使用率、磁盘I/O		
4	网络流量	网络I/O		
5	系统连通性及响应时间	包括探测次数、连通次数、最小响应时间、最大响应时间、平均响应时间、超时次数、平均超时时间、可用率等参数；失败原因统计；不同站点/系统的横向比较分析（平均值的数据对比报表及统计图表）	NSTL全系统	连续仿真监控
6	网站流量统计	包括独立IP、独立访客、访问量、人均页面访问量等参数	门户网站	日志分析
7	Web服务	应用服务器的监控包括吞吐率（服务器每秒处理请求数）和并发连接数统计，如等待连接数、关闭连接数、发送响应内容、持久连接数、读取请求等	WebLogic、Tomcat	时间区域 临界监控
8	独立访客行为统计	包括停留时间、跳出率、访问深度等参数	门户网站	日志分析
9	独立访客浏览方式统计	包括上网设备类型、浏览器名称和版本、电脑分辨率显示模式、操作系统、地理分布等参数	门户网站	日志分析

4 系统功能

4.1 故障监测

运维工作中最常遇见的就是设备发生故障，故障监测是网络管理最基本的功能，也是不可或缺的内容，具体包括故障检测、隔离和纠正。它通过检查错误日志，跟踪、辨认错误信息，执行诊断测试，纠正错误等环节实现故障监测和定位，具体通过对网络组成部件的状态监测来实现。简单问题通常被记录在错误日志中并不作特别处理；严重故障则需要通知网络管理器，即所谓的“警报”，传送告警给运维人员，并且还会直观地反应在监控对象的页面上。告警通过警报引擎完成[3]，具有限时、延时、防波动、自动跟踪、取消警报、自动越级上报、自动节假日警报特别处置、自动区分对象差异警报等功能。

4.2 运行监测

运行监测指性能监测和管理，评估系统资源运行状况、通信效率等系统性能，包括监视和分析被管网络及所提供的各种服务。性能分析结果可能会触发某个诊断测试过程或重新配置网络以维持网络的性能。性能管理，指收集分析有关被管网络当前状况的数据信息，并维持和分析性能日志，典型功能如收集统计信息、维护并检查系统状态日志、确定自然和人工状态下系统的性能、改变系统操作模式以进行系统性能管理的操作等。此外，这些性能都采用独有的防波动算法，能有效防止给用户发无用或已失效的警报。

4.3 业务监测

因为业务系统自身的特殊性，业务系统监测相对硬

件故障监测要复杂得多。在NSTL业务监测中，其关注点主要包括业务系统的安全稳定性，覆盖全国的服务站和用户管理平台的网络连通性，用户检索量、文献浏览量、全文订单量、注册用户数、在线用户数等业务统计数据以及相关网络、设备、中间件、数据库间逻辑关系和实时运行状态等。业务监测不仅需在综合运维平台展示这些指标，还要反映实时的系统运行状态、相关设备连接关系、业务逻辑和重要配置管理信息。

4.4 其他功能

除监测功能外，综合运维管理系统还具有一些辅助功能。例如，设备巡检、资产管理、ITSM运维流程管理、值班记录等。另外，对虚拟化平台设备的监测也能提供较好地支持，可以动态呈现每台虚拟机的运行状态。

5 应用特点

（1）基于策略的监控。基于策略的监控把常规网络监测提升到网元级的深度[4-5]，使得设备、线路、路由、拓扑、流量、配置等环节的任一变化都能达到短信实时警报且具有高精度水平，其维护操作方式简便，只需通过点击界面选项完成，工作量显著降低。这些简单策略直接覆盖主机、虚拟化、数据库、中间件、存储及所有应用监控环节，实现全监控系统的动态跟踪。同时，集监控、运维、基础管理的统一监管平台彻底消除了信息孤岛，实现机构、人员、权限、资产、策略、档案、配置、展示、警报、故障等全部元素的有机整合，覆盖了信息系统各元素的全程。

（2）多种操作系统统一运维技术。在主机层面对CPU、内存、缓存、文件系统、裸设备和进程等元素的监管，直接以统一图形界面展现，兼容于UNIX、Linux、Windows等不同操作系统，也无需第三方平台支持和代码开发工作，从而实现对众多品牌和不同操作系统的集成监管，具有较高的安全性和可靠性。

（3）Agent模式。Agent是在被监测服务器上安装的客户端软件，利用Agent可以对服务器内存、缓存、CPU、磁盘空间等进行深度监测，当这些重要指标超过所设阈值，系统便会触发报警。此外，进程并发数量、进程存活、数据库连接数、Sessions数、事务总数、DB名称、高速缓冲区大小、共享池、表空间、管理员账号等也可利用Agent模式监测。

（4）层次化通告技术。为确保故障发生时，各层级管理员能及时收到事故通报告警信息，综合运维管理系统采用三级延时通报技术。当故障发生时，系统会发送通告给设定的管理员，20 分钟后若问题未能解决，通告将会发送到上一级管理员；再过 30 分钟问题仍未能处理解决，则会上报至更高级管理员或信息主管。警报延时发送的时间间隔可由管理员根据自身需要任意设定。另外，综合运维管理系统还可为不同类别的用户提供不同的定制通报信息。实践中，这种通报机制可以避免告警信息漏报情况的发生，从而确保问题和故障能够及时得到处理。

（5）安全设计。综合运维管理系统在系统级采用C/S结构，除Windows版需要.Net支撑环境外，不依赖于任何第三方服务软件；完全采用加密协议通道通信；同时还对服务器提供特别保护，当系统配置文件或账号发生变动时可触发告警。

6 应用效果

6.1 网络管理由分散转变为集中

以前NSTL网络服务系统的各个业务系统都是分散的，业务架构、业务流程比较复杂，多种软件分布在一个或多个硬件上运行，无法统一运维管理。通过综合运维管理系统，使所有业务系统都能实现可视化、自动化管理；网络拓扑、设备自动发现；业务逻辑关系、关键技术指标、故障位置清晰可见。可与各业务系统接口对接，自动实现业务数据的实时同步更新，用户访问量、文献检索量、全文订单量、下载量、用户数等重要业务数据实时显示，实现集中统一的自动化运维管理，工作效率明显提高。

6.2 业务监测由人工转变为智能

对于提供文献检索服务的系统，网站二级或三级页面与首页同等重要，以往检索结果报错不易被发现且响应时间严重滞后[2]，现在利用综合运维管理系统直接对二级、三级或特定页面进行监测，当监测到检索系统出现403或404一类的故障信息时，系统会在 10 分钟内通知管理员处理，缩短故障处理时间。

NSTL分布在全国的服务站和用户管理平台大都

采用公网连接，拓扑结构复杂。以往几乎很难做到对服务站、管理平台网络和系统运行情况的实时监控，但实施综合运维管理系统后，通过展示中心能够全面直观地监测所有服务站的运行情况，并详细记录和统计每个服务站点的联通率、超时连接时间、累计应答超时次数等。这些数据对分析某一阶段用户访问量、原文订购量、原文传递时间变化提供参考依据，进而可对NSTL整体网络运行平稳度和文献服务质量作出评价。从近6个月的监测统计数据看，已开通的39个服务站平均联通率为94.61%，17个用户管理平台平均联通率为91.96%，网络版期刊数据库平均联通率为94.00%，数据显示网络和服务系统运行情况良好，而这在以前是无法做到的。

应用自动部署主要用于NSTL主站与全国服务站间的系统同步，通过综合运维管理系统文件自动发布和批量处理功能，使得所有服务站应用升级工作可以自动、有序地完成，改变以往人工远程登录对端系统来更新文件的模式，减轻工作量。

6.3 安全防护由被动转变为主动

以往网络安全基本处于被动地应对，现在NSTL已经建立了统一的日志存放中心，积累了大量珍贵的网络设备、安全设备等各类日志信息，这些日志信息还在持续增长。这些对于分析诊断故障和进行安全风险评估，起着极其重要的作用。综合运维管理系统能够获取这些日志并与所收集的告警信息进行事件关联分析[6]，目前这项工作还在不断探索，尝试运用大数据分析能力和智能学习能力开展数据关联分析，从而形成态势感知和主动预警，若仅靠人工力量是难以实现的。

7 结语

综合运维管理系统投入使用以来，监测网络、设备、业务系统等节点数量已达200多个，监测用户服务站和用户管理平台节点63个、全国开通现刊数据库节点51个、虚拟主机100余台。实现NSTL网络内设备故障精确定位和运行状态准确监测及告警，形成网络、主机、应用统一的动态监测和展示中心。监测预警效果显著，故障告警明显减少，通过设定系统预警阈值，使系统发生故障的情况逐渐减少，有效地提升运维工作效率，保证网络和系统的安全稳定运行。但系统仍存在一些问题和不足，如当某些复杂原因引起多台设备同时告警时，会造成系统负载过大而无法正常发送告警信息；系统还不能做到智能化关联分析等。针对存在的问题和不足，下一步将对系统实施进一步升级改造。

参考文献

[1] 吕德奎,崔艳军.自动化综合运维监管平台设计与实现[J].软件导刊,2015,14(6):91-94.

[2] 徐亮,邹鑫灏.信息系统安全运维管理平台建设研究[J].科技传播,2015,7(21):123-124.

[3] 朱伟.数据中心机房环境监控系统的研究和应用[J].金融电子化,2008(4):53-55.

[4] 杨达达.IP网监控管理系统的设计及实践研究[J].信息与电脑(理论版),2015(12):100-101.

[5] 沙永刚,张婧.基于状态的应用监控与恢复算法与模型[J].信息安全与技术,2013,4(7):93-96.

[6] 张先哲.信息系统安全运维管理平台建设研究[J].软件工程师,2015(5):38-39.

作者简介

张婧，女，高级工程师，研究方向：网络信息安全，E-mail：zhangj@istic.ac.cn。
韩旸，男，学士，助理工程师，研究方向：网络管理，E-mail：hany@istic.ac.cn。

NSTL Integrated Operational Management System Application Practice

ZHANG Jing, HAN Yang
（Institute of Science and Technology Information of China, Beijing 100038, China）

Abstract: With the development of information technology, the scale and complexity of information system are continuously growing. The way to ensure the information system security and business continuity becomes the core of the operation management. How to change the scattered and low levels of monitoring and operational status, and use the unification of a high level, safe and efficient operations technology to make information system running with high reliability, becomes the development direction of the current construction of monitoring and operation. This paper introduces the construction of the National Science and Technology Library information system integrated operational platform and its using effect.

Keywords: Monitoring; Operation and Maintenance; Information System; Network Security

（收稿日期：2016-07-05）