

应用系统运行状态监管的设计与开发^①

阎 伟, 刘 瑜, 郝达睿

(天津市市政公路信息中心, 天津 300050)

摘 要: 通过实际需求分析及相关技术的分析, 提出了“以应用系统为主体的监管技术设计思路”, 并采用 WMI、Windows API 技术、数据库技术, 通过构建分布式的运行监控模式, 实现了监控系统对应用系统运行状态的全面监控。经过机房的实际运行, 获取了真实的监控数据, 并可以直观的用于应用系统运行问题的解决及预测判断。
关键词: 系统化; 应用系统; 监控; 管理; WMI

Application System Running Status Supervision Design and Development

YAN Wei, LIU Yu, HAO Da-Rui

(Road and municipal information center of Tianjing, Tianjing 300050, China)

Abstract: Through the energy demand analysis and correlation technique's analysis, proposed “take the application system as the main body supervision technical design mentality”, and uses WMI, Windows the API technology, the data bank technology, through constructs the distributional movement monitoring pattern, has realized the supervisory system to the application system running status comprehensive monitoring. After the Computer room actual movement, gained the real monitoring data, and may direct-viewing use in the application system operational problems the solution and the forecast judgment.

Key words: systematization; Application system; monitoring; manage; WMI

1 前言

随着国内信息化技术对生产经营、管理的支撑比重越来越大, 信息化系统越来越复杂、越来越庞大情况的发展, 对应用系统的维护和监控要求也越来越高。

以天津市市政公路局信息化建设为例, 在信息中心机房已经部署了“网格化系统”、“Gis 综合应用系统”、“高速 ETC 收费系统”、“局网站”等一系列重要系统。在维护过程, 发现经常出现某进程死掉、服务器荡机、系统服务响应缓慢等突发性问题。虽然, 这些问题, 原因各有不同, 但是, 及时发现, 提早预防, 及时提醒, 统一管理成了急需解决的问题。

经过前期调研和比较, 发现市面上很多现有机房监管系统, 都存在一些缺陷: 如有些偏重网络环境监控; 有些偏重硬件及操作系统的监控; 有些功能庞杂, 但是不好用^[1]。尤其缺少以应用系统为主要监控对象

的监管系统。

2 应用系统运行过程存在问题及分析

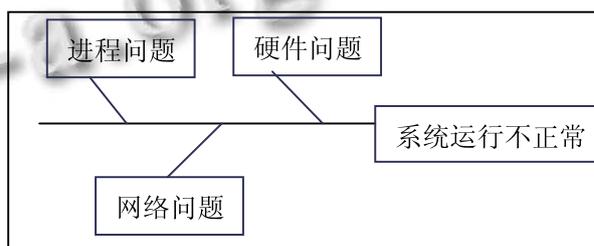


图 1 应用系统运行不正常主要问题鱼刺分析图

图 1, 为信息中心 2 年多来主要问题源累计、分析的结果。该图所示问题, 主要局限于机房内部运行过程发生的问题, 不涉及外部其他因素。进程问题、

① 基金项目: 安徽省教育厅自然科学基金(2005KJ004ZD)

收稿时间: 2011-08-29; 收到修改稿时间: 2011-09-16

硬件问题、网络问题是应用系统运行不正常的主要原因。

进程问题，主要为 arcGis、oracle、Office 等应用系统支持进程的不稳定式死掉。

硬件问题，主要为应用系统运行的服务器硬件环境情况，包括 CPU、内存、硬盘的使用情况。上述任意一个硬件实际使用资源不够，都会导致应用系统运行变慢，甚至无法运行。

网络问题，主要从服务器端口进出数据流量，了解应用系统运行情况。在硬件设备正常运行的前提下，需要考虑应用系统的某一网络路段是否存在网络流量过大现象。为维护人员调整系统部署，或优化硬件资源提供判断依据。

考虑到应用系统的复杂性，如“网格化系统”涉及 11 台服务器，10 多个子系统，又涉及 arcGis、Oracle、报表中间件等后台支撑软件。为了管理方便，也为了针对性的解决问题。在系统设计时，强调了“以应用系统为关注主体，重点监控相关问题源的设计思路”。

3 网络管理技术比选

在 Windows 网络环境下，目前比较流行的网络管理技术有 SNMP、WMI、API+Socket 等技术^[2-4]。

表 1 网络管理技术比较

比较项	WMI	SNMP	API+Socket
远程控制能力	100	100	100
适用监控范围	90	40	100
中间件是否受限制	90	40	60
实际需求验证	90	20	80
技术容易度	100	70	30
Windows 版本适应性	90	70	60
平均值:	93.3%	56.7%	71.7%

表 1 的数据主要采用相关资料验证+实际测试结果+主观评价，综合得出。通过该表可以看出 WMI 技术更有利系统设计的实现。

WMI 缺陷及应对措施:

表 1 中“适用监控范围”得 90 分的原因是，极少数监控功能缺失，如网络流量监控功能，根据实际测试结果，竟然没有实现！同理 WMI 在“实际需求验证”上也只能得“90 分”。该方面的技术问题，可以通过

API 技术得到弥补。在“Windows 版本适应性”方面，WMI 技术在 Windows2000 后才支持，所以也只能得“90 分”，不过该问题可以通过安装 WMI 中间件来弥补。最后评价结果采用 WMI 技术可以完全实现项目的需求。

4 主要功能实现过程

4.1 应用功能框架的实现

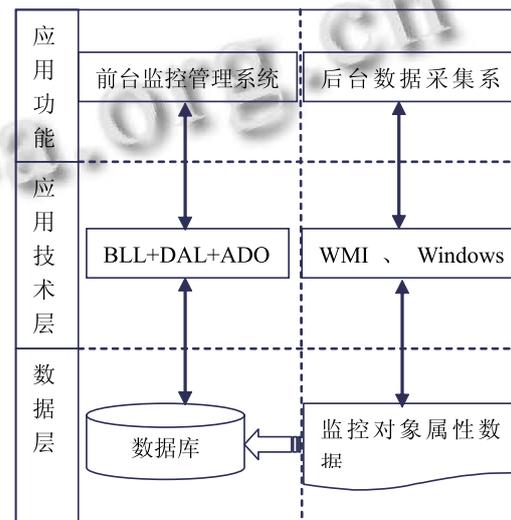


图 2 监控系统框架

图 2，主要分两部分实现监控过程。后台数据采集系统，分布于各受控服务器端，独立实现每台服务器端的数据采集，在规定的实现所监控对象数据的采集，然后，各自汇总于数据库中。而前台主监控管理系统，可以任意安装于一台监控电脑中，实现系统数据的统一提取和分析，并统一实现对各后台数据采集时间点的设置。

目前对于监管系统，监控方式主要有两种：一种是单点式监控，通过一台电脑实现远程监控所有设备；另外一种分布式监控，也就是受控设备上装监控后台，另外有前台进行独立数据提取、分析及控制操作。^[5]这两种方式各有优缺点。本项目从以下几方面的因素考虑，采用的是分布式的运行方式。

① 提高系统操作效率，减少系统资源占用。由于单点式，在受控对象数量级增大的情况下，如几台，几十台，几百台之间产生的监控数据流量区别是比较大的。因此带来的系统响应时间延迟、大数据流等，容易对正常运行的应用系统产生干扰。而分布式的，

由于在本地执行数据采集命令，网络流量会小得多。

② 保证数据采集质量，减少开发难度。由于应用系统出现运行迟缓等现象时，往往关心的是某一时刻，某几台相关设备的运行状态，所以，要求采集数据尽量能同步采集。分布式监控方式，后台各自运行，互不干扰，能在统一时间点上同时采集数据，实现比较容易。

③ 分布式缺点及应对措施。当然，跟单点式监控比较，分布式监控，在系统安装、维护等方面似乎更麻烦。为此，项目设计时充分考虑了该方面的问题。尽量做到一次安装，无须干扰的效果。如系统自重启功能、后台托盘运行功能、出错强制自起功能、晚上监控参数自更新更能，都做了充分的考虑，保证的系统操作简单、方便。

4.2 主要功能模块设计

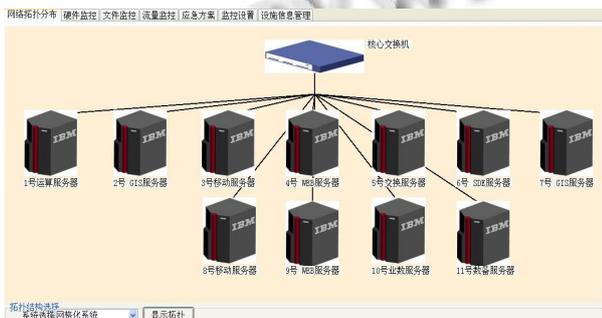


图 3 前台监控系统主要功能界面(网格化系统拓扑图)

1.前台监控功能。图 3 为前台监控主界面，主要功能为“网络拓扑分布”、“硬件监控”、“文件监控”、“流量监控”、“应急方案”、“监控设置”、“设施信息管理”、“警报信息”、“维修日志”等。所设计的监控主体及相关问题源的分析，体现了图 1 及“应用系统为主体对象”的监管思想。以应用系统为独立单位的网络拓扑图，直观、方便的展现于维护管理者，有利管理人员系统的、全面的针对系统不同问题，进行判断和解决。该系统可以通过选择项显示不同的应用系统网络拓扑图。图 3 显示的是“网格化系统分布拓扑图”。“硬件监控”主要提取分析 CPU、内存、硬盘等的运行情况；“文件监控”主要监控并记录，重要文件的变化状态，如修改、删除、建立等情况；“流量监控”主要提并分析取受控服务器上传、下载的数据流量；“应急方案”主要对应用系统相关的应急方案进行统一管理；“监控设置”主要设置后台监控系统的数据采

集时间点，管理者可以根据关心的时间点灵活统一设置，后台自动执行；“设施信息管理”主要处理受控设备的相关辅助信息，如 IP 地址、保修期等；“警报信息”主要提示受控对象异常信息，如进程死掉、服务器荡机等；“维修日志”主要记录维护人员问题的解决过程。

2.后台监控功能

后台监控主要功能为各种受控对象相关参数信息的采集，包括硬件的，CPU、硬盘、内存；网络的，网卡端口流量；文件夹下，文件；IIS 服务内的网站地址；服务器进程内的，arcGis、Oracle 等进程进行定点数据采集。实现主要技术采用 WMI，对于部分功能辅以 Windows API 技术。

3.核心功能模块实现原理

以“硬件监控”模块实现过程为例：

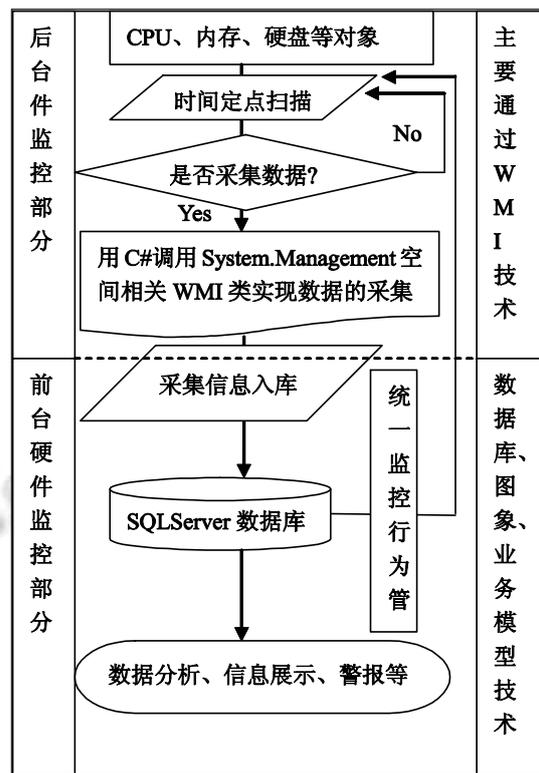


图 4 硬件监控模块功能实现主要原理

图 4 主要采用 WMI、数据库、图象、业务模型分析等相关技术，实现了硬件对象监控过程。该实现过程除了要掌握上述技术外，还应注意数据采集扫描方式的选择，特别是时间扫描点的确认。该处考虑到数据流量、及实际工作需要，采用了人工经验式定点

设置, 定点获取监控对象数据的方式, 在获取过程也考虑了样本数据量的问题, 以及样本可代表性问题。

4. 数据分析效果

对应用系统相关的问题源监控对象数据的分析, 大量采用二维折线图。为了直观、真实的体现受监控对象的实际状态及趋势, 在画出实际运行状态线外, 还增加了极大值线, 使维护人员判断更加容易。另外充分考虑了多同类监控对象的问题, 如图 5 所示:



图 5 服务器硬盘资源使用情况分析

图 5 右边的“图例说明”下, 除了硬盘 C:、D:、E: 三个逻辑分盘外, 还增加了三个逻辑分盘的最大值图示 (带 M 者), 这样维护者可以根据实际使用状态线和极大值线进行直观的比较, 并很容易判断出存在的问题。如图 4 存在 C: 盘空间不足现象 (见左红线圈内), 如发现应用系统反应变慢, C 盘空间是很受怀疑的, 然后维护人员可以针对性的进行系统运行环境优

化, 再进行问题评价, 最后把问题解决过程进行记录。

5 运行结论

经过几个月机房环境下实际运行, 该系统采集了大量的有价值的监控数据。主要使用特点为:

① 操作简单, 一天只需观察前台监控系统 1, 2 次就行, 每次大概 5 到 10 分钟。有效的解决了原有人工管理模式, 低效的管理方式。

② 能直观、及时发现系统运行环境中存在的问题, 特别是应用系统响应速度变慢、个别进程死机等隐蔽问题, 能及时判断。

③ 能直观判断潜在问题的发展趋势, 对系统运行环境的优化, 提供了辅助决策依据。

④ 体现了系统化管理理念, 以应用系统为主体的管理方式, 有利维护人员系统、周全的考虑问题和解决问题。

⑤ 系统扩展性好, 能满足大范围的监控要求。

参考文献

- 1 翁凌宇, 柳阳, 韩志伟. 远程软件运行监测的设计与实现. 舰船电子工程, 2008, 28(6): 149-153.
- 2 吴江川, 饶一梅. Windows 下基于 WMI 的数据和程序. 计算机系统应用, 2010, 19(7): 126-129.
- 3 唐忠, 何慧敏, 苏飞. 基于 WMI 技术服务器网管软件设计和实现. 桂林电子科技大学学报, 2008, 28(6): 461-465.
- 4 赵志定. 基于 SNMP 的开放式网管软件系统的研究和设计 [硕士学位论文]. 浙江工业大学, 2010: 23-15.
- 5 万洪斌. 基于 WMI 的 Windows 客户端安全集中控制管理系统设计与实现 [硕士学位论文]. 四川电子科技大学, 2010: 35.