

一种服务器操作系统资源监控工具的设计和实现

陈磊,李征宇,简炜,高炽扬

(中国软件评测中心,北京 100048)

摘要:随着我国信息技术的高速发展,国产服务器操作系统得到了快速的发展,但是针对国产服务器操作系统的测试技术却没有同步发展。文中介绍的服务器操作系统性能监控工具主要是以服务于国产服务器操作系统测试过程为基础,兼顾对行业内主流操作系统的性能监控技术。本工具经过实际环境检验,能够基本满足服务器操作系统测试的要求。该工具主要通过 SSH 协议连接 Linux/Unix 服务器、WMI 服务连接 Windows 服务器,通过特定的方式和命令,监控相应的操作系统,返回服务器性能值。

关键词:SSH;WMI;服务器操作系统;性能监控

中图分类号:TP31

文献标识码:A

文章编号:1673-629X(2013)04-0104-03

doi:10.3969/j.issn.1673-629X.2013.04.025

Design and Realization of a Server Operation System Resource Monitoring Tool

CHEN Lei, LI Zheng-yu, JIAN Wei, GAO Chi-yang

(China Software Test Center, Beijing 100048, China)

Abstract: With the national information technology developing, the national server operation system also was developed quickly, but the software testing aimed at national server operation system was not developed. In this paper, the server operating system performance monitoring tools are mainly in the service of domestic server operating system test process as the foundation, pay attention to the performance monitoring technology in the industry of the mainstream operating system. After the actual environmental inspection, this tool can basically meet the server operating system test requirements. This tool is mainly through the SSH protocol connecting Unix/Linux server, WMI service connecting Windows server, through the specific ways and command, monitor the corresponding operating system to return the server performance value.

Key words: SSH; WMI; server operation system; performance monitoring

0 引言

近年来随着国家支持力度的日益加大,我国的国产基础软件得到了快速发展,同时也对国产基础软件关键测试技术的发展提出了迫切的需求。文中基于此需求,详细介绍了一款服务器操作系统监控工具的设计过程和实现方法,该工具以监控国产服务器操作系统资源监控为根本出发点,兼顾对行业内主流服务器操作系统的性能监控技术。

该工具通过 SSH 协议或者 WMI 服务远程连接到

服务器操作系统上,获取服务器资源快照,既满足对服务器操作系统资源监控的需求,又实现了监控服务对服务器资源消耗的最小化。本工具通过远程连接服务直接获取被监控服务器操作系统资源,能够将采样间隔时间缩小到最小 1 秒钟,大大提高了采样精度^[1]。

1 关键技术

1.1 SSH

SSH 的英文全称为 Secure Shell,由 IETF 的网络工作小组(Network Working Group)所制定;SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠,专为远程登录会话和其他网络服务提供安全性的协议^[2]。其目的是在普通的网络上提供安全的远程访问控制的协议^[3]。SSH 协议包括口令、二进制文件和管理命令的加密,取代 rlogin、rsh 和 telnet 等网络服

收稿日期:2012-07-31;修回日期:2012-11-01

基金项目:“核高基”科技重大专项(2009ZX01045-004,2009ZX01045-005)

作者简介:陈磊(1982-),男,河北唐山人,工程师,研究方向为软件和信息测试及优化技术、协议一致性测试、自动化测试框架。

务管理维护远程服务器^[4]。

1.2 WMI

WMI 是以 CIMOM 为基础的单元对象库^[5],是 WBEM 模型的一种实现。通过 WMI 软件和脚本程序可以方便快捷地访问操作系统不同的访问接口^[6]。WBEM(Web-Based Enterprise Management)是由 DMTF(Distributed Management Task Force,分布式管理任务组)创建的网络管理环境^[7]。

1.3 多线程与委托

线程是组成进程的唯一单位元素,是进程中的一个执行流^[8]。在多线程中每个线程都独自享有寄存器和共享代码区的特点^[9]。在一个程序中可以同时运行多个线程执行不同的或者相同的任务^[10]。委托是一种程序中引用对象的方法,通过委托可以将被委托对象传递给可调用返回值的程序。委托能够通过静态方法和实例方法调用,通过封装委托对象调用被封装的方法^[11]。

2 面向性能测试的服务器操作系统资源监控工具

2.1 Linux/Unix 服务器操作系统监控技术

Linux/Unix 服务器性能数据要通过采集和网络传输才能在客户端显示,因此对应的数据采集应该分为 SSH 建立连接、数据采集和资源结果传输三部分,首先通过 SSH 连接服务器操作系统,然后通过 Linux/Unix 的 SHELL 命令,sar 和 iostat 实现资源数据的采集^[12],最后将结果以文本形式传回监控机客户端。SSH 远程连接国产服务器操作系统监控资源算法如下:

```
_conn = SSHConnection.Connect(f, reader, s); //通过 SSH 连接服务器
```

```
reader._conn = _conn;  
ch = _conn.OpenShell(reader);  
b[0] = (byte)input;  
.....  
reader._pf.Transmit(b);  
b = System.Text.Encoding.Default.GetBytes("sar -n DEV 1  
1;iostat -m;free -m -t -o;sar 1 1");  
//一次输入所有监控命令  
reader._pf.Transmit(b);
```

通过上述算法就可以在客户端获取到 sar 命令和 iostat 命令执行的结果,并通过 SSH 协议以文本的方式传给客户端。

在配置测试环境的时候,Linux 服务器操作系统中有些是不安装 sar 和 iostat 命令的,因此该工具通过主动探寻,自动安装的方式实现了监控环境的自配置功能。

首先通过加载被监控 Linux 服务器操作系统的 IP

地址、用户名(有 root 用户权限)和密码通过 SSH 协议远程连接被监控服务器,通过运行 iostat 和 sar 命令查看其是否已经包含了这两个命令。如果被监控操作系统无上述两个命令,该工具通过开启 ftp 服务,上传 sar 和 iostat 命令依赖的 sysstat.rpm 文件到服务器操作系统的 home 下,然后使用命令 rpm -ivh sysstat.rpm 安装完成自配置监控功能。

图 1 是自配置监控环境流程图。

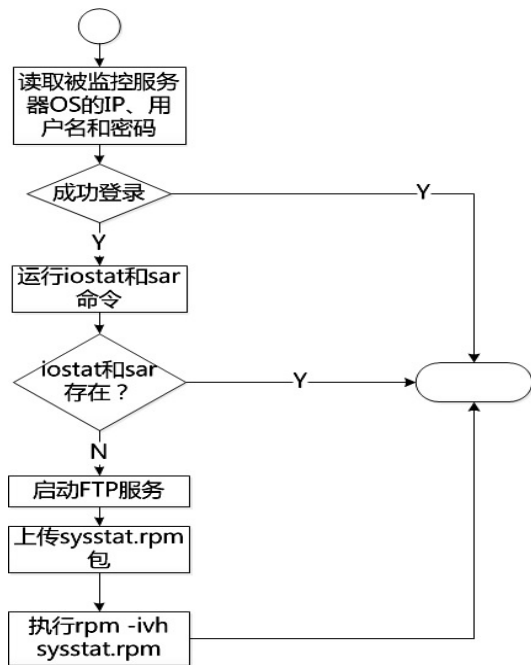


图 1 自配置监控环境流程图

2.2 Windows 服务器操作系统监控技术

对于 Windows 服务器操作系统的性能监控技术主要是通过 WMI 体系结构实现的,WMI 从 Windows 服务器操作系统中拿到感兴趣的性能数据,并将这些数据取出后通过 SNMP 协议返回给监控机客户端。但是一些性能值例如空闲内存数等并不能直接通过 WMI 取得,要通过一定的计算得到。WMI 获取资源的算法如下:

```
//获取 CPU 利用率  
private PerformanceCounter pcCpuLoad; //定义 CPU 计数器  
.....  
pcCpuLoad = new PerformanceCounter("Processor", "% Processor Time", "_Total");  
pcCpuLoad.NextValue(); //初始化 CPU 计数器,并获取当前 CPU 利用率  
//可用内存  
ObjectQuery query = new ObjectQuery("select FreePhysicalMemory FROM Win32_OperatingSystem");  
.....  
free_mem = long.Parse(Return["FreePhysicalMemory"].ToString()) / 1024; //计算获得当前可用内存,单位为兆  
//获取网络吞吐量
```

```
query = new ObjectQuery ( " select BytesTotalPerSec, Times-
tamp_PerfTime, Frequency_PerfTime FROM Win32_PerfRawData_
Tcpip_NetworkInterface" );
.....
newByte += long. Parse ( Return [ " BytesTotalPerSec" ]. ToS-
tring ( ) );
newTimeStamp = long. Parse ( Return [ " Timestamp _ Per-
fTime" ]. ToString ( ) );
frequency = long. Parse ( Return [ " Frequency_PerfTime" ]. To-
String ( ) );
.....
byteMTotal = 1.0f * ( newByte - oldNetPerSec ) * frequency
/ ( newTimeStamp - oldNetTimeStamp );//计算获得当前网络吞
吐量
//计算磁盘 I/O
query = new ObjectQuery ( " select DiskBytesPerSec, Timestamp
_PerfTime, Frequency_PerfTime FROM Win32_PerfRawData_Per-
fDisk_PhysicalDisk" );
//WQL 语句, 设定的 WMI 查询内容和 WMI 的操作范围, 检
索 WMI 对象集合
searcher = new ManagementObjectSearcher ( management-
Scope, query ); //异步调用 WMI 查询
.....
ioByte = 1.0f * ( newByte - oldIOPerSec ) * frequency /
( ( newTimeStamp - oldIOTimeStamp ) * 1024 );
//其中 newBytes 新获得的磁盘 I/O, oldIOPerSec 上一次获
取的磁盘 I/O
// frequency 采样频率 newTimeStamp 获得 newBytes 值的时
间戳
//oldIOTimeStamp 获得 oldIOPerSec 值的时间戳。这样就计
算了这一个时间价格内的磁盘 I/O
```

通过 WMI 服务进行测试, 获取被监控服务器的原始数据, 经过上述算法得到被监控服务器 CPU 利用率、可用内存、网络吞吐量和磁盘 IO。如果被监控服务器中未开启 WMI 服务, 可以通过在被监控服务器上运行 net start winmgmt 对服务 WMI 启动。

通过 WMI 服务监控 Windows 服务器资源主要是通过读取配置文件中被监控服务器系统的 IP 地址、用户名和密码建立连接, 应用 PerformanceCount 和 WQL 获取被监控服务器的 CPU、内存、网络 and 磁盘的原始数据, 最后根据获取的原始数据取得被监控服务器的 CPU 利用率、可用内存、网络吞吐量和磁盘 IO。

2.3 服务器操作系统资源监控工具的实现

服务器操作系统资源监控工具采用了 SSH 协议和 WMI 远程连接被监控服务器操作系统, 通过对应服务器类型的监控线程进行数据采集, 通过多线程方式实现了同时监控多台服务器操作系统, 并应用委托的方式将多线程监控结果回传给 UI 显示服务器操作系统。资源监控工具总体流程图如图 2, 图 3 所示。

图 2 为获取 Windows 服务器资源流程图。

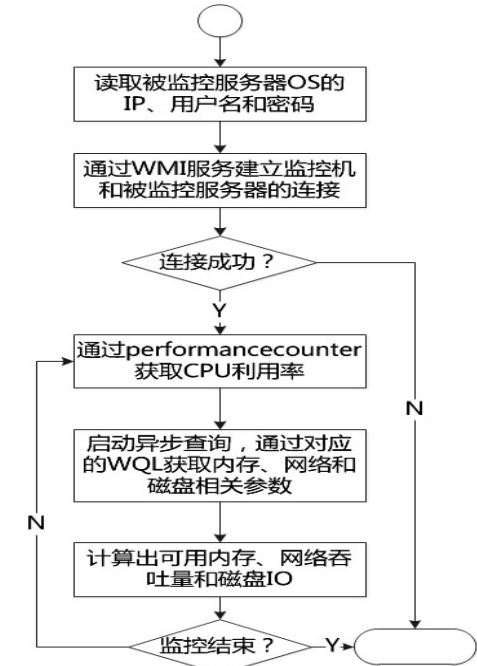


图 2 获取 Windows 服务器资源流程图

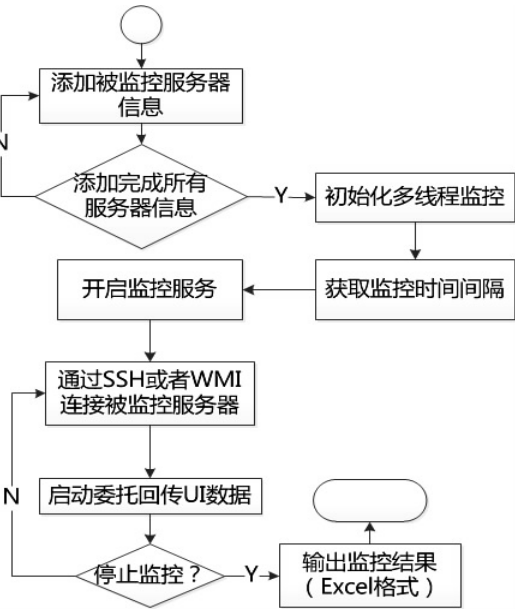


图 3 服务器操作系统资源监控工具流程图

服务器操作系统资源监控工具依据上述算法, 通过维护被监控服务器系统列表, 建立多线程监控算法。同时通过委托将数据传递给 ZedGraph 控件动态地展现各个指标的实时曲线。

3 结束语

文中对服务器操作系统资源监控工具进行了简单介绍, 同时介绍了该工具应用的多线程技术进行多服务器同时监控, 通过 SSH 远程连接算法或者 WMI 服务获取服务器资源, 通过委托展现监控结果, 但是本工具

6 结束语

各种网络脆弱性分析方法从不同的角度入手,在解决特定问题时各有优点,例如:基于扫描分析更适于查找已知漏洞;攻击图更适于系统安全性分析、入侵行为分析。在分析实际网络安全时,应根据实际情况和安全要求选择合适的模型或者对现有模型进行改进,将实际网络中与安全有关的局部信息一步一步地加入模型,使得模型具有更强的解决实际问题的能力。

脆弱性评估方法的发展经历了人工分析到自动分析的阶段,现在正在由局部分析向整体分析发展,由基于扫描分析方法向基于模型的分析方法发展,由静态分析向动态分析发展,由单机分析向分布式分析发展。

参考文献:

- [1] Bishop M, Bailey D. A critical analysis of vulnerability taxonomies[R]. Davis: University of California at Davis, 1996.
- [2] 刘海燕, 杨洪路, 王 岫. 一个基于网络的脆弱性扫描系统[J]. 计算机应用, 2003, 23(7): 98-99.
- [3] 林 闯, 汪 洋, 李泉林. 网络安全的随机模型方法与评价技术[J]. 计算机学报, 2005, 28(12): 1943-1956.
- [4] Noel S, Jacobs S, Jacobs M. Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs[C]//Proc of the 19th Annual Computer Security Applications Conference. Las Vegas, Nevada; [s. n.], 2003: 86-95.
- [5] Ilgun K. USTAT: A real-time intrusion detection system for UNIX[C]//Proc of IEEE Symposium on Research in Security and Privacy. Oakland, CA; [s. n.], 1993.
- [6] Swiler L P, Phillips C, Gaylor T. A graph-based network-vulnerability analysis system[R]. Sandia: Sandia National Labo-

ratories, 1997.

- [7] Li W. An Approach to Graph-based Modeling of Network Exploitations[D]. Mississippi State: Mississippi State University, 2005.
- [8] Noel S, Jajodia S, Berry B, et al. Efficient Minimum-cost Network Hardening via Exploit Dependency Graphs[C]//Proceedings of the 19th Annual Computer Security Applications Conference. Las Vegas, Nevada; [s. n.], 2003: 1-10.
- [9] 张维明, 毛捍东, 陈 锋. 一种基于图论的网络安全分析方法研究[J]. 国防科技大学学报, 2008, 30(2): 97-101.
- [10] Liu Yu, Man Hong. Network Vulnerability Assessment Using Bayesian Networks[C]//The International Society for Optical Engineering. San Diego, CA: SPIE Press, 2005: 61-71.
- [11] Girault C, Valk R. Petri Nets for Systems Engineering: A Guide to Modeling, Verification, and Application[M]. Berlin Heidelberg: Springer-Verlag, 2003: 1-14.
- [12] 林 闯. 随机 Petri 网和网络系统性能评价[M]. 第 2 版. 北京: 清华大学出版社, 2000: 5-21.
- [13] 王桢珍, 姜 欣. 信息安全风险概率计算的贝叶斯网络模型[J]. 电子学报, 2010(BO2): 18-22.
- [14] 张金槐, 刘 琦, 冯 静. Bayes 试验分析方法[M]. 长沙: 国防科大出版社, 2007.
- [15] 毛捍东. 基于逻辑渗透图模型的网络安全风险评估方法研究[D]. 长沙: 国防科学技术大学, 2008.
- [16] 冯萍慧, 连一峰, 戴英侠, 等. 基于可靠性理论的分布式系统脆弱性模型[J]. 软件学报, 2006(7): 1633-1640.
- [17] 王纯子, 黄光球. 基于脆弱性关联模型的网络威胁分析[J]. 计算机应用, 2010, 30(11): 3047-3050.
- [18] 邢栩嘉, 林 闯, 蒋屹新. 计算机系统脆弱性评估研究[J]. 计算机学报, 2004, 27(1): 1-11.

(上接第 106 页)

还处于测试阶段,对于采样时间戳的控制等功能的完善还需要进一步推进。

参考文献:

- [1] Chen Lei, Jian Wei, Li Yanbo, et al. Research of Performance Monitoring for Spatial Information System[C]//2010 International Conference on Future Information Technology and Management Engineering. [s. l.]: [s. n.], 2010.
- [2] Merkel R. Secure Shell[EB/OL]. 2005 [2009-09-12]. http://en.wikipedia.org/wiki/Secure_Shell.
- [3] 余永洪. 用 SSH 技术远程管理 Linux 服务器[J]. 计算机与现代化, 2007(7): 96-98.
- [4] 马昕炜. Linux 系统管理员手册[M]. 北京: 北京希望电子出版社, 2005.
- [5] 陈永建, 朱 娟, 黎桂林. 基于 WMI 的实时监控系统设计 with 实现[J]. 微计算机信息, 2005(21): 47-49.

- [6] Iverson T. Windows Management Instrumentation[EB/OL]. 2004 [2012-09-04]. http://en.wikipedia.org/wiki/Windows_Management_Instrumentation.
- [7] Polichat M. WMI 技术指南[M]. 北京: 机械工业出版社, 2003: 5-40.
- [8] 卜春芬. C#后台处理与多线程技术的应用[J]. 昆明学院学报, 2010(3): 88-91.
- [9] 陈少强. VC++中基于 MFC 的多线程应用程序设计[J]. 三明高等专科学校学报, 2002(2): 49-55.
- [10] 多线程[EB/OL]. 2012-09-01. <http://baike.baidu.com/view/65706.htm>.
- [11] Nagel C, Evjen B, Glynn J. C#高级编程[M]. 李敏波译. 第 4 版. 北京: 清华大学出版社, 2006: 153-163.
- [12] Dmerrill. Linux[EB/OL]. 2001 [2012-09-08]. <http://en.wikipedia.org/wiki/Linux>.

一种服务器操作系统资源监控工具的设计和实现

作者: [陈磊](#), [李征宇](#), [简炜](#), [高炽扬](#)
作者单位: [中国软件评测中心, 北京 100048](#)
刊名: [计算机技术与发展](#)
英文刊名: [Computer Technology and Development](#)
年, 卷(期): 2013(4)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjfz201304027.aspx