Web 集群远程监控策略①

谭 鹏 黄红伟 (云南省科学技术情报研究院 云南 昆明 650051)

摘 要： 针对 Web 集群存在的网络流量监控问题，构建 MRTG 流量监控，根据 Web 服务的网络流量特点设置远程流量监控参数，使之能够监控集群中多台设备，通过 Apache 发布直观可靠的图形化网络流量和设备性能数据，研究 MRTG 在实际应用中的缺陷，提出合理可行的改进策略，使网络管理人员能够更加有效的通过远程监控网络流量和性能负载，判断网路或设备发生问题的可能原因，快速定位并加以处理。

关键词： MRTG；Linux；SNMP；Web 集群；网络流量

Web Cluster Remote Monitoring Strategy

TAN Peng, HUANG Hong-Wei

(Yunnan Academy of Scientific & Technical Information, Kunming 650051, China)

Abstract: With the difficulty of network traffic monitoring, this paper builds an MRTG traffic monitoring system. The long-distance network traffic flow monitoring parameters are set up according to Web services to enable them to monitor multiple devices in the cluster. Reliable data for graphical network traffic and equipment performance are released through Apache. MRTG's defects in practical applications are studied. Reasonable and feasible improvement on the strategy is made, so that network managers can remotely monitor network traffic load and its performance. In this way, can they determine the possible causes of problems in network or equipment, so as to find the problem out and address them in a short time.

Keywords: MRTG; Linux; SNMP; Web cluster; net traffic

1 引言

为提高 Web 服务器的高可用性，构建集群是一种较好的解决方式。目前我单位架设负载均衡的 Web 集群，由于应用的增加，将进行集群扩容建设，为全面衡量集群网络运行状况，对网络状态做更细致、更精确的测量，构建集群性能监测系统对于追踪 Web 集群服务的高可用性尤为重要。简单网络管理协议(SNMP: simple network management protocol)协议为互联网设备测量提供有力支持，而多路由数据绘图监控器(MRTG :MultiRouter Traffic Grapher)[1]就是基于 SNMP 协议的典型网络流量统计分析工具，它耗用的系统资源很小，可通过 SNMP 协议查询指定有 SNMP 协议的设备，定时统计其设备的流量或负载，再将统计结果绘制成统计图以非常直观的形式显示，是较为理想的 Web 集群性能监测工具。在此，首先介绍 MRTG 工作原理，并说明 Web 集群远程监控环境的实现，然后分析 MRTG 在对 Web 集群进行远程流量监控中存在的性能缺点，提出改进策略。

2 设备监测工作原理

MRTG 利用 SNMP 协议，侦测服务守护进程[2,3]。每隔几分钟采样并统计系统资源负载量、Server 流量和网络设备流量，将统计结果绘成统计图，最后生成 HTML 文件供 Web 发布。增加可以监控设备类型的描述。

① 收稿时间:2009-06-29

网络服务器的信息数据流量、CPU 使用率以及诸如 Squid 的代理服务等的封包传送率或数据流量是网络管理人员所必须注意的事项。因为当主机的 CPU 使用率过高时，系统将呈现不稳定的状态，这就需要注意是哪一个服务或者是由于什么原因而造成的。因此，网络管理方面，必须了解主机的流量状态，并视流量来调整网络带宽或预先介入处理可能出现的问题，以保证 Web 服务集群的稳定有效。

MRTG 功能实现主要由四部分完成，包括 SNMP 、日志文件、RateUp 模块和配置模块。

2.1 SNMP

MRTG 需要以 SNMP[4]或外挂程序的方式收集资料，通过 SNMP 通讯协议访问需要监测的网络设备，用 SNMP GET 获取需要的状态信息,产生即时统计图。

SNMP 管理模型中有三个基本功能，管理者(Manager)，被管代理(Agent)和管理信息库(MIB)。设备的所有需要被管理的信息被看作一个各种被管理对象的集合，这些被管理对象由 OSI 定义在一个被称作管理信息库(Management Information Base, MIB)的虚拟的信息库中。

管理者可以通过 SNMP 操作直接与管理代理通信,获得即时的设备信息,对网络设备进行远程配置管理或者操作；也可以通过对数据库的访问获得网络设备的历史信息,以决定网络配置变化等操作。MIB 是一个按照层次结构组织的树状结构(定义方式类似于域名系统)，管理对象定义为树中的相应叶子节点。管理对象是按照模块的形式组织，每个对象的父节点表示该种对象属于上层的哪一个模块。而且树中每一层的每个节点定义了唯一的一个数字标识，每层中的该数字标识从 1 开始递增，这样树中的每个节点都可以用从根开始到目的节点的相应的标识对应的一连串的数字来表示。每个对象的一连串数字表示被称为对象标识符 OID(Object In Dentifier)。SNMP 基本的标准 MIB 库是 MIB Ⅱ。

IP 网络测量工具大都利用 SNMP 协议来实现网络状态参数的测量。SNMP 事实上的普及、标准化的 MIB 以及规范的 OID 标识方法，使得基于 SNMP 的测量工具在 IP 网络上能够有效完成测量工作。

2.2 日志文件

MRTG 使用的日志文件采用 ASCII 文本形式记录采集到的流量数据,此日志文件具有常量大小的特征，能够支持长期的网络监测任务，为了避免长期监测时数据膨胀问题，MRTG 定期对数据进行整合,根据记录数据的的日期不同而以不同的粒度保存数据，随着时间的推移，相应数据的粒度逐渐变大，超过两年的数据不再保存。

2.3 RateUp 模块

RateUp 模块使用 C 语言实现，提供日志文件的更新和统计图形的生成。

2.4 配置模块

MRTG 提供了生成配置文件的工具，用于定义数据采集和图形定制时所需要的参数和规则。在配置文件中设置需要监测的目标变量、HTML 页面及图形的工作目录、图形显示方式、数据采集周期等信息，可以根据需要按照其规则进行修改。

工作原理图如图 1 所示：

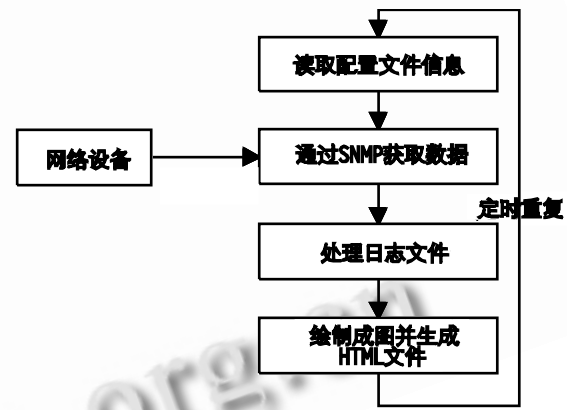

图 1　MRTG 工作原理图

3　MRTG应用部署

3.1 部署环境构成

在部署 MRTG 的 Web 集群中，包括堡垒主机一台[5]，Web 服务器两台，环境构成如图 2 所示：

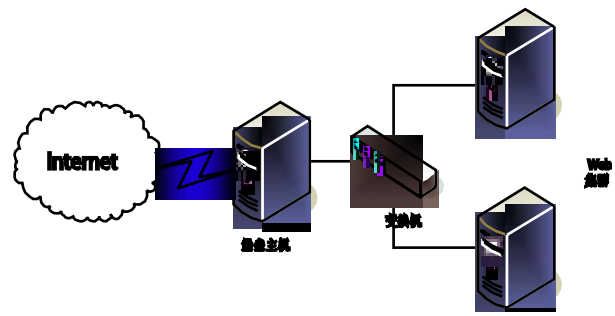

图 2　WEB 集群结构图

集群设备构成如表 1 所示：

表 1　监测环境表

设备名称	IP 地址	系统版本	用途
登录主机	192.168.1.1	Redhat 9.0	MRTG 管理工作站
Web 集群服务器	192.168.1.12	Windows 2000 Server	被监控的服务器(HTTP 和 FTP 服务)
Web 集群服务器	192.168.1.38	中软 Linux	被监控的服务器(HTTP 和 FTP 服务)

3.2 MRTG 设备状态监测

(1) 网卡设备监测

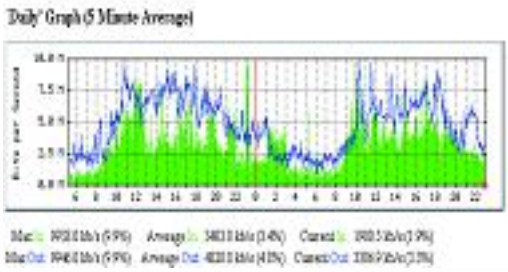

图 3　主机网卡流量监测

(2) 监测 CPU 负载量

监测 CPU 负载量[6]时，使用外挂程序 sysstat，可同时采集 CPU 系统负载和内存利用率，然后将两者放在一个 PNG 图形中。MRTG 要求其返回四行输出，第一、二行分别为两个变量当前的状态值，第三行以任一格式输出主机 uptime,第四行输出主机名和 IP 地址。软件包构成如下表所示：

表 2　Sysstat 软件包集成工具列表

工具名称	应用功能
iostat	提供CPU使用率及硬盘吞吐效率的数据；
mpstat	提供单个处理器或多个处理器相关数据；
sar	负责收集、报告并存储系统活跃的信息；
sal	负责收集并存储每天系统动态信息到一个二进制的文件中。通过计划任务工具cron来运行，是为sadc所设计的程序前端程序；
sa2	负责把每天的系统活跃性息写入总结性的报告中。它是为sar所设计的前端，要通过cron来调用；
sadc	是系统动态数据收集工具，收集的数据被写一个二进制的文件中，它被用作sar工具的后端；
sadf	显示被sar通过多种格式收集的数据；

(3) 主机 CPU 负载率与内存利用率如图 4 所示：

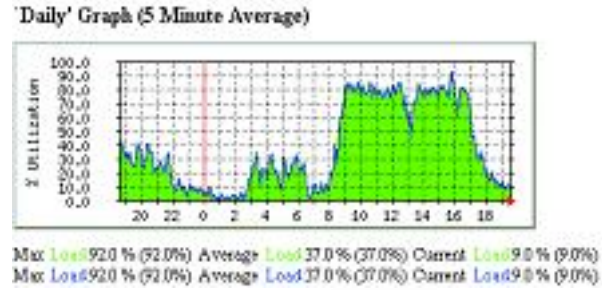

图 4　主机 CPU 负载率与内存利用率监测

4　MRTG性能缺陷及改进策略

4.1 MRTG 性能缺陷分析

(1) MRTG 采取以 ASCII 文本形式来记录采集到的流量数据，并保存到日志文件。MRTG 的日志不会变大，因为这里使用了独特的数据合并算法，使日志文件保持了常量大小。

但是在使用过程中发现，随时间的推移，相应数据的粒度会逐渐变大，所存储的数据粒度受到限制，而且文本式的监测数据会导致数据无法重复使用。新扫描的监测数据所产生的网页会覆盖上一次所生成的网页，比如，不能从中得到一个月前某天平均每半个小时的数据信息。

当需要对多个被监测对象在相同时刻相同时间单位图谱进行横向比较和对被监测对象在不同时刻相同时间单位图谱进行纵向比较时，发现 MRTG 无法提供此类对比，MRTG 所生成的网页只能查看被监测对象在某个时刻不同时间单位的图谱。

以上问题，会导致在监测 Web 集群性能时无法做到全面细致的分析与对比，不能够准确分析集群在某一时刻所发生的问题，影响对集群的管理和维护。经分析，发现这些问题的原因主要是由于 MRTG 的监测数据存储方式不能提供数据的重复使用，不够灵活。

(2) 根据对配置文件的设置，如：每 5 分钟 MRTG 会对设备进行一次监测，每次数据采集后，MRTG 都根据日志文件进行流量图生成，并以 HTML 格式呈现，而在实际应用中，由于管理人员需要管理大量网络设备，Web 集群中的服务器一个端口的流量统计分析图形被调用和查看的机率很低，而 MRTG 却周期性的生成大量不会被查看的图形，因此，耗费了大量用于生成图形的系统资源，如果当需要监测的端口数目增加较多时，就会产生性能瓶颈的影响，导致 MTRG

无法满足对集群的监测需要。

经分析发现周期性的自动生成图片与 HTML 文件，对监测集群性能没有实际意义，并且会耗费大量的系统开销，影响服务器性能。

4.2 MRTG 改进策略

根据 MRTG 存在的性能缺陷，可以引入改进的 MRTG 策略减少其自身性能缺陷所引起的 Web 集群性能监控问题。

(1) 针对 MRTG 采集的监测数据在存储方式上的缺陷，引入新的监测数据存储方案; MRTG 在从网络设备获取数据方面没有变动，但在按周期(如 5 分钟)获取监测数据后，将处理的日志文件存入新引进的数据模块中，分项目、分时间段存储，实现 Web 集群性能监测的数据长期保存，并能重复使用; 管理人员可以随时调用任意时间，任意设备的监测数据进行对比和分析。

(2) 针对周期性的自动生成监测图片与 HTML 文件所造成的系统开销增大问题，改进 MRTG 绘图策略，引入绘图触发模块，实现按需成图方式，绘制性能监测图并产生 HTML 文件。当管理人员在需要查看 Web 集群性能监测图时，通过绘图触发模块提交绘图请求，监测数据才从数据库中被提取出来，生成日志文件并调用绘图软件，将其绘制成图后一并生成 HTML 文件，再由 Apache 发布，最终提交至网络管理人员。

改进策略如图 5 所示:

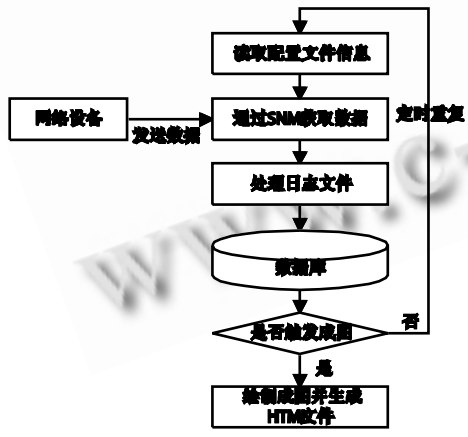

图 5　改进后的监控策略

4.3 策略分析

经过对 MRTG 监控策略的改进，更加有利于管理人员对 Web 集群有效的监控。

(1) 在实际工作中，我单位的具体情况是，系统管理人员需要处理的日常工作较为分散与多样，无法时刻监控日志数据，而在实际管理工作中通常需要随机调用某几个时段的监测数据进行分析比较，新策略中数据存储模式的改进，使得系统管理人员可以在任意时间调用所需时段、任意设备的监测数据。还可以通过调用不同日期，相同时段、相同设备的监控数据，可以帮助管理人员在任意时间做出客观准确的设备性能与运行状态分析。

(2) 在具体改进实现中，对监控数据的绘图和 HTML 内容的生成采用了触发控制的方式。触发控制是使用控制报文来实现的，控制报文是基于 TCP(传输控制协议) 的消息定义。当系统管理员需要查看某个时段的统计分析图形时，首先向成图控制模块发送控制报文，报文中指出了要调用哪个时段、设备及端口的图形，成图控制模块收到控制报文后根据日志文件进行图形生成，生成图形后向客户端发送控制反馈报文，客户端收到控制反馈报文后，即可调用新生成的流量分析统计图。

在实例应用中，MRTG 绘图策略改进后，MRTG 在客户端的响应上有了一定的延迟，但它大大减小了系统的开销，缩短了执行时间，当需要监控的设备和端口数量急剧增加后，设备监测最小执行周期可以显著缩小。

5　结语

Web 集群远程监控是网络安全与 Web 站点维护的重要环节。MRTG 本身既是一种灵活、高效的，较好的流量监控工具，但是在实际使用中针对 MRTG 自身的设计特点却成为 Web 集群监控中的缺陷，经过对 MRTG 的研究，修改定制了改进的性能监控策略，使 MRTG 在实际使用中的性能得到了显著提高，也方便了网络管理人员对 Web 集群性能的监测与管理，通过查看与分析 MRTG 所生成的性能监测图可以简单直观的看出在各个时段各个设备的网络流量与性能情况，这样较为容易发现各端口的异常情况，从而为排除网络故障、保证 Web 集群的高可用性提供了直接的帮助。

通过对 MRTG 和 Sysstat 工具的应用，为基于 Linux 操作系统的堡垒主机和 Web 集群性能的监测提供了一种灵活、高效的方法。由于生成的结果图形基于 Web，可以实现对 Web 集群的远程监控。

(下转第 44 页)

(上接第 86 页)

参考文献

1 MRTG web server configuration http://oss.oetiker.ch/mrtg/doc/mrtg-webserver.en.html

2 丛锁,吴甘沙,张伟,高传善.网络状态参数监测与MRTG的应用.微型电脑应用, 2000,16(4):51－53.

3 赵永胜.MRTG在网络管理中的应用.铁路通信信号工程技术, 2005,6:43－46.

4 Stallings W. SNMP, SNMPV2, Snmpv3, and RMON 1 and 2. Addison-Wesley/Pearson. 2005.

5 高建智.Linux 网络实际操作经典.北京:科学出版社, 2002.

6 姜大庆.Linux主机性能监测与MRTG的应用.计算机与现代化, 2004,2:64－66,88.