日志服务器的构建及自动化存储

张艳超

(温州大学现代教育技术中心，浙江温州 325035)

摘 要：从系统安全管理和服务器日志的特点着手，分析了构建日志服务器的重要性．依据不同的操作系统平台，讨论并设计了日志自动化存储的方法．

关键词：服务器；日志；脚本；计划任务

中图分类号：TP399 **文献标识码**：A **文章编号**：1006-0375(2007)05-0052-05

随着计算机技术的广泛应用，绝大部分企事业机构都构建了自己的局域网，同时架设了一定数量的服务器．操作平台一般有 windows 和 linux 两种形式．这些服务器每天会产生大量的系统日志．日志对于系统的安全来说非常重要，它记录了系统每天发生的各种各样的事情，用户可以通过它来检查错误发生的原因，或者寻找受到攻击时攻击者留下的痕迹．日志主要的功能是审计和监测，可以实时地监测系统状态，监测和追踪侵入者．所以如何维护系统日志是服务器日常管理的重要内容．构建日志服务器则是一个行之有效的方法．我们可以定期自动备份所有服务器的系统日志到我们的日志服务器上．通过日志查看器，就可以在日志服务器上查看所有服务器的系统日志，即使应用服务器本身出了重大问题，不能启动了，在日志服务器上也可以查到该服务器上以前的日志．

1 如何构建日志服务器

对于 Windows 操作系统，在开始菜单的运行对话框中输入“eventvwr”，点击确定后，就会看到一个名叫“事件查看器”的窗口．从事件查看器中可以看到系统日志中的事件分为三类：应用程序、安全性、系统．其中“应用程序”事件描述的是应用程序错误记录，“安全性”事件描述的是安全审核记录，“系统”事件描述的是系统错误记录．对应的日志文件则是应用程序日志（AppEvent.Evt）、安全日志（SecEvent.Evt）、系统日志（SysEvent.Ev）．

对于 Linux 系统而言，所有的日志文件都在/var/log 下．Linux 系统一般有 3 个主要的日志子系统：连接时间日志、进程统计日志和错误日志．其中连接时间日志是由多个程序执行，把记录写入到/var/log/wtmp、/var/run/utmp 和 login 等程序，更新 wtmp 和 utmp 文件，使系统管理员能够跟踪谁在何时登录到系统．进程统计日志是由系统内核执行，当一个进程终止时，为每个进程在进程统计文件（pacct 或 acct）中写一个记录．进程统计的目的是为系统中的基本服务提供命令使用统计．错误日志是由 syslogd 执行，各种系统守护进程、用户进程和内核通过 syslog 向文件/var/log/messages 报告值得注意的事件[1].

收稿日期：2006-12-10

作者简介：张艳超(1979-)，男，吉林长春人，助教，研究方向：办公自动化

对于网络服务器而言，网络服务器日志主要有 WWW 日志、FTP 日志和邮件服务器日志．一旦服务器的服务，像虚拟主机、FTP、Email 等出现不正常工作，或者是服务器的系统出现硬件故障等，这些信息都会记录在服务器的日志里．要解决这些问题，首先要检查系统日志，看日志里都记录了些什么，从而找到解决问题的办法，而不能简单地把服务器及其服务重启或者重装，否则问题还会不断地发生，给企事业机构带来很大的损失．有时服务器出现故障，系统的日志也会丢失或者是不能获取，这时，可以通过查看日志服务器上的日志备份来解决问题．我们采用 Windows 2003 操作系统来构建日志服务器，在日志服务器上安装 Serv-U 作为 ftp 服务器，在日志服务器上指定一段 ftp 空间作为日志的存放空间．

2 日志的自动备份实现

在实现系统日志的自动备份上，要考虑服务器的安全问题．服务器一般都是放在防火墙的后面．防火墙默认所有的端口都是关闭的，服务器需要什么端口，在防火墙上就开启什么端口．一般来说，我们只是打开 80、20、21 等几个端口．端口开启的越少系统则越安全．从安全性方面考虑，利用文件夹共享等方式来实现系统日志的自动备份会用到 139 等端口，这样会存在很严重的安全隐患．因为开启 139 端口虽然可以提供共享服务，但是常常被攻击者所利用进行攻击，比如使用流光、SuperScan 等端口扫描工具，就可以扫描目标计算机的 139 端口，如果发现有漏洞，可以试图获取用户名和密码，这是非常危险的．21 端口是用来实现 FTP 文件传输的默认端口，所以可以通过 FTP 方式来远程备份日志．

2.1 Windows 系统日志备份

对于采用 Windows 操作系统的服务器，通过 FTP 传输来实现系统日志的自动定期备份，需要利用 WSH（Windows Script Host）进行脚本编程．WSH 是 Microsoft 公司提供的脚本宿主软件，包含在 WScript.exe 和 Cscript.exe 文件中．目前采用 Wscript.exe 作为脚本宿主居多．微软公司提供了两种语言，VBScript 和 Jscript（JavaScript 的微软版本）用来作为脚本引擎．所谓脚本其实就是纯文本文件，文件扩展名为 VBS 或 JS．Wscript.exe 会使用不同的脚本引擎来执行相应的脚本文件．WSH 包含 SCRRUN.DLL 和 WSHOM.OCX 两个文件．WSH 提供的 COM（Component Object Model）对象如表 1 所示．

表 1　WSH 所提供的 COM 对象[2]

对象名	描述
Scripting.FileSystemObject	提供一套文件系统操作函数
Scripting.Dictionary	返回存放键值对的字典对象
Wscript.Shell	提供一套读取系统信息的函数: 读写注册表、查找文件夹路径、读取链接中的设置, 读取环境变量
Wscript.NetWork	提供网络连接和远程打印机管理的函数: 查找当前登记用户名

操作系统的日志文件是不能直接进行拷贝的，必须在事件查看器中手动给事件日志打包或者用专门的软件工具打包．我们在每一台服务器上安装一个名叫 Microsoft Product Support Reporting Tool 的工具，这个软件每次运行后都会记录下很多操作系统的信息．其中包括系统的日志．系统日志是以*.evt 文件格式保存．这个软件安装后有一个名叫 MPSRpt.cmd 的文件，把它放到计划任务中，考虑到日志的传送会影响到服务器的性能，假定把它设置为每天凌晨 2:00 执行，到这个时间系统的事件日志就被自动备份到本机上了，然后编写一个把系统日志上传到指定的 ftp 空间的

脚本 ftpbak.txt，代码如下：

```
open 10.10.2.23      ‘登录到指定的 FTP 服务器
syslog               ‘FTP 用户名
putlog               ‘FTP 密码
binary
lcd C:\WINDOWS\MPSReports\Setup\Reports      ‘指定本地上传目录
put WZDX-CMET_Application.evt                ‘上传“应用程序”事件
put WZDX-CMET_System.evt                     ‘上传“系统”事件
bye                  ‘退出 FTP
```

把 ftpbak.txt 这个脚本放在 c:\ 目录下，同时再编写一个用来启动 FTP 命令、调用 ftpbak.txt 文件的批处理脚本 startup-ftp.bat．代码如下：

```
C:\WINDOWS\system32\ftp.exe -s:c:\ftpbak.txt
```

把 start-ftp.bat 这个脚本加到计划任务中，设置在 2:30 执行．这样就使生成的日志文件自动地传到指定的 FTP 空间里．

2.2 Linux 系统日志备份

对于采用 Linux 操作系统的服务器，也可通过 FTP 传输来实现系统日志的自动定期备份．Linux 系统的各种日志通常都放在/var/log 这个目录下．这里要用到 Linux 的计划任务来实现日志文件的自动传输．在 Linux 系统中，计划任务一般是由 cron 承担，可以把 cron 设置为开机时自动启动．cron 启动后，它会读取它的所有配置文件（全局性配置文件/etc/crontab，以及每个用户的计划任务配置文件），然后 cron 会根据命令和执行时间来按时调用工作任务．利用 vi 打开 crontab 后可以看到如下信息：

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
01 * * * * root run-parts /etc/cron.hourly
30 15 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

据此可以知道在/etc/下还有四个目录：cron.hourly、cron.daily、cron.weekly 和 cron.monthly，只要把需要按计划每小时、每天、每周、每月执行的脚本放在相应的目录下就可以了．cron 配置计划任务的书写格式是：分钟 小时 日 月 周 ［用户名］ 命令[3].

其中第一字段应该定义的是：分钟，表示每个小时的第几分钟来执行，范围是 0-59；第二字段应该定义的是：小时，表示从第几个小时来执行，范围是 0-23；第三字段应该定义的是：日期，表示从每个月的第几天执行，范围 1-31；第四字段应该定义的是：月，表示每年的第几个月来执行，范围 1-12；第五字段应该定义的是：周，表示每周的第几天执行，范围从是 0-6，其中 0 表示星期日；每六字段应该定义的是：用户名，也就是执行程序要通过哪个用户来执行，这个可省

略；第七字段应该定义的是：执行的命令和参数[3].

例如设定系统日志的传送时间是每天的 15 点 30 分，把传送日志的脚本 ftpbak.sh 放在/etc/cron.daily/目录下．Ftpbak.sh 的代码如下：

```
#!/bin/sh
echo " open 10.10.2.23                    /*用 open 连接日志服务器 */
user syslog   putlog                      /*输入用户名和密码*/
binary                                    /*以二进制传输*/
hash                                      /*当有数据传输时，显示#号*/
lcd /var/log                              /*更换到日志所在目录*/
put messages.1                            /*上传日志信息*/
bye " | ftp –n                            /*执行 ftp 命令*/
```

这样在规定的时间，Linux 服务器也会自动把自己的日志传到日志服务器上．这时，还有一个问题，按照我们编写的脚本程序，每天上传的日志文件名字都是相同的．这样在日志服务器里今天上传的日志就会把昨天上传的日志覆盖掉．所以还需编写一个脚本 rename.vbs，重新命名日志服务器中的日志文件．代码如下：

```
dim time
‘把今天的日期转化成字符串
time = CStr(Date())
Set objFSO = CreateObject("Scripting.FileSystemObject")
‘给应用程序事件文件名前加上日期
objFSO.MoveFile "e:\log\WZDX-CMET_Application.evt", time & "-" & "WZDX-CMET_Application" & ".evt"
‘给系统事件文件名前加上日期
objFSO.MoveFile "e:\log\WZDX-CMET_System.evt" ， time & "-" & "WZDX-CMET_System" & ".evt"
‘给 Linux 系统日志加上日期
objFSO.MoveFile "e:\log\messages.1" ， time & "-" & “messages.1”
```

把 rename.vbs 这个脚本加到日志服务器的计划任务中，设置为每天 3:00 自动执行．这样就完成了通过 21 端口来远程自动备份系统的日志．

3 结束语

如果日志文件比较大，可以在本地先给日志打包压缩，这时只需要再做一个压缩日志文件的简单脚本就可以了，然后再上传给日志服务器．依据上面的方法，就可以构建一个简易的日志服务器了．存储在日志服务器上的日志信息极其珍贵，对于我们日常服务器的管理和维护是相当有帮助的．

参考文献

[1] 黄海隆, 陈赛娉. 计算机日志分析与管理方法的研究[J]. 大众科技, 2006, (7): 67-68.

[2] Tobias W (抖斗书屋译). Windows 脚本编程核心技术精解[M]. 北京: 中国水利水电出版社, 2001. 94-95.

[3] 北南南北. 计划任务工具 Cron 的配置和说明[EB/OL]. http://www.linuxsir.org/main/?q=node/209, 2006-05-09.

On Construction and Automated Memory of Log Server

ZHANG Yanchao

(The Center of Modern Educational Technology, Wenzhou University, Wenzhou, China 325035)

Abstract: From the aspects of safe system management and the characteristics of log server, the author analyses the importance of log server construction and discusses the methods of log automated memory in the different operating systems.

Key words: Server; Log; Script; Scheduled task

（编辑：王一芳）