用Syslog记录UNIX和Windows日志的方法Linux认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/586/2021_2022__E7_94_A8Syslog_E8_c103_586590.htm 在比较大规模的网络应用或者对安全有一定要求的应用中，通常需要对系统的日志进行记录分类并审核，默认情况下，每个系统会在本地硬盘上记录自己的日志，这样虽然也能有日志记录，但是有很多缺点：首先是管理不便，当服务器数量比较多的时候，登陆每台服务器去管理分析日志会十分不便，其次是安全问题，一旦有入侵者登陆系统，他可以轻松的删除所有日志，系统安全分析人员不能得到任何入侵信息。 因此，在网络中安排一台专用的日志服务器来记录系统日志是一个比较理想的方案。本文以FreeBSD下的syslog为例，介绍如何利用freebsd的syslogd来记录来自UNIX和windows的log信息。 一、记录UNIX类主机的log信息 首先需要对Freebsd的syslog进行配置，使它允许接收来自其他服务器的log信息。 在/etc/rc.conf中加入：syslogd_flags="-4 -a 0/0:*" 说明：freebsd的syslogd参数设置放在/etc/rc.conf文件的syslogd_flags变量中 Freebsd对syslogd的默认设置参数是syslogd_flags="-s"，(可以在/etc/defaults/rc.conf中看到) 默认的参数-s表示打开UDP端口监听，但是只监听本机的UDP端口，拒绝接收来自其他主机的log信息。如果是两个ss,即-ss，表示不打开任何UDP端口，只在本机用/dev/log设备来记录log. 修改后的参数说明： -4 只监听IPv4端口，如果你的网络是IPv6协议，可以换成-6 -a 0/0:* 接受来自所有网段所有端口发送过来的log信息。 如果只希望syslogd接收来自某特定网段的log信息可以这样写：-a 192.168.1.0/24:* -a

192.168.1.0/24:514或者-a 192.168.1.0/24表示仅接收来自该网段514端口的log信息，这也是freebsd的syslogd进程默认设置，也就是说freebsd 在接收来自其他主机的log信息的时候会判断对方发送信息的端口，如果对方不是用514端口发送的信息，那么freebsd的syslogd会拒绝接收信息。即，在默认情况下必须：远程IP的514端口 发送到本地IP的514， 在参数中加入*,表示允许接收来自任何端口的log信息。这点，在记录UNIX类主机信息的时候感觉不到加不加有什么区别，因为UNIX类主机都是用514端口发送和接收syslog信息的。但是在接收windows信息的时候就非常重要了。因为windows的syslog软件不用514端口发送信息，这会让默认配置的syslogd拒绝接收信息。笔者同样在linux系统下用linux的syslogd来配置log服务器，发现linux下的syslogd就没有那么多限制，只要给syslogd加上-r参数，就可以接收来自任何主机任何端口的syslog信息，在这方面来说freebsd的默认配置安全性要比linux稍微高一点。 修改好syslogd参数后，我们需要修改一下/etc/syslog.conf文件，指定log信息的存放路径， 比如你要记录其他系统的远程登陆登出信息并指定日志存放路径，则需要修改以下行：authpriv.* /var/log/testlog 这表示把系统的登入登出日志(包括本机系统登陆登出日志)存放到/var/log/testlog文件中。 当然，这是最简陋的做法，因为这样会把所有服务器的登陆登出信息存放在一个文件中，察看的时候很不方便，通常的做法是用一个脚本，对接收到的信息进行简单的分拣，再发送到不同的文件。 如下设置： authpriv.* |/var/log/filter_log.sh 在记录目标前面加上“ | ”表示把接收到的信息交给后面的程序处理，这个程序可以是一个专门的日志处理软件，也可以是一个自

己编写的小的脚本,举例： #!/bin/sh read stuff SERVER=`echo $stuff |awk ‘ {print $4} ’ ` echo $stuff gt. /var/log/login_log/$SERVER.log 这个简单的脚本以IP作为分类依据，先用read读取log信息，用awk取出第四字段(即IP地址或者主机名所在的字段)，以该字段为文件名存放该主机的日志。 这样一来，来自192.168.1.1的log会记录到192.168.1.1.log文件中,来自192.168.1.2的log会被记录在 192.168.1.2.log文件中，分析和归类就比较方便了。当然这是一个最简单的例子，读者可以根据自己的需求写出更好的脚本，甚至把log信息分类后插入数据库中，这样日志的管理和分析就更方便了。 最后重启一下syslogd服务，让配置生效: /etc/rc.d/syslogd restart OK,服务端的配置完成。现在配置一下客户端： 这里所说的客户端，就是发送自己的日志到远程日志服务器上的主机。修改/etc/syslog.conf文件： 我们举例你只要记录系统登入登出日志到远程日志服务器上，那么只需要修改以下一行: authpriv.* @192.168.10.100 这里的192.168.10.100就是log服务器的IP，“ @ ”符号表示发送到远程主机。 OK，重启一下syslog服务: Linux: /etc/init.d/syslogd restart BSD: /etc/rc.d/syslogd restart 用logger测试一下是否配置成功： logger p authpriv.notice “ Hello,this is a test ”到log服务器上去看看，“ Hello,this is a test ”应该已经被记录下了。最后在客户机上登陆登出几次，看看真实的authpriv信息是否也被成功的记录下。 二、Windows日志的记录 对于UNIX类主机之间记录日志，由于协议、软件和日志信息格式等都大同小异，因此实现起来比较简单，但是windows的系统日志格式不同，日志记录软件，方式等都不同。因此，我们需要第三方的软件来将windows的

日志转换成syslog类型的日志后，转发给syslog服务器。 介绍第三方软件evtsys (全称是evntlog to syslog) 文件才几十K大小，非常小巧，解压后是两个文件evtsys.dll和evtsys.exe 把这两个文件拷贝到 c:\windows\system32目录下。 打开Windows命令提示符(开始-gt.evtsys i h 192.168.10.100 -i 表示安装成系统服务 -h 指定log服务器的IP地址 如果要卸载evtsys,则： net stop evtsys evtsys -u 启动该服务: C:\gt.运行 输入 gpedit.msc) 在windows设置-gt. 本地策略 -&gt.审核策略中，打开你需要记录的windows日志。evtsys会实时的判断是否有新的windows日志产生，然后把新产生的日志转换成syslogd可识别的格式,通过UDP 3072端口发送给syslogd服务器。 OK,所有的配置windows端配置完成，现在配置一下syslogd的配置文件， 参数的配置和上面相同，所不同的是evtsys是以daemon设备的方式发送给 syslogd log信息的。因此，需要在/etc/syslog.conf中加入： daemon.notice |/var/log/filter_log.sh 关于syslog 记录设备和记录等级方面的知识可以参考syslog文档。 OK，所有配置设置完成。 Linux 、BSD和windows上的系统日志都可以统一记录到一台日志服务器上轻松管理了。 更多优质资料尽在百考试题论坛 百考试题在线题库 linux认证更多详细资料 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com