用路由器日志快速定位及排除故障 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/430/2021_2022__E7_94_A8_E8_B7_AF_E7_94_B1_E5_c101_430316.htm 日志对于网络安全来说非常重要，他记录了系统每天发生的各种各样的事情，你可以通过他来检查错误发生的原因，或者受到攻击时攻击者留下的痕迹。路由器是各种信息传输的枢纽，被广泛用于企事业单位的网络建设中，承担着局域网之间及局域网与广域网之间连接的重任。 Cisco是目前使用比较广泛的一种路由器，在许多行业系统中有非常普遍的应用。以下是笔者在日常工作中积累的一些对Cisco路由器日志设置方面的经验，这些实例都在实际应用中调试通过并投入使用，供大家参考。路由器的一些重要信息可以通过syslog机制在内部网络的Unix主机上作日志。在路由器运行过程中，路由器会向日志主机发送包括链路建立失败信息、包过滤信息等等日志信息，通过登录到日志主机，网络管理员可以了解日志事件，对日志文件进行分析，可以帮助管理员进行故障定位、故障排除和网络安全管理。 认识syslog设备 首先介绍一下syslog设备，它是标准Unix，的跟踪记录机制，syslog可以记录本地的一些事件或通过网络记录另外一个主机上的事件，然后将这些信息写到一个文件或设备中，或给用户发送一个信息。syslog机制主要依据两个重要的文件:/etc/syslogd(守护进程)和/etc/syslog.conf配置文件，syslogd的控制是由/etc/syslog.conf来做的。syslog.conf文件指明syslogd程序记录日志的行为，该程序在启动时查询syslog.conf配置文件。该文件由不同程序或消息分类的单个条目组成，每个占一行。对每类消息提供一

个选择域和一个动作域。这些域由tab隔开(注意:只能用tab键来分隔，不能用空格键)，其中选择域指明消息的类型和优先级.动作域指明sysloqd接收到一个与选择标准相匹配的消息时所执行的动作。每个选项是由设备和优先级组成。也就是说第一栏写"在什么情况下"及 "什么程度"。然后用TAB键跳到下一栏继续写 "符合条件以后要做什么"。当指明一个优先级时，syslogd将记录二个拥有相同或更高优先级的消息。每行的行动域指明当选择域选择了一个给定消息后应该把他发送到哪儿。 第一栏包含了何种情况与程度，中间用小数点分隔。详细的设定方式如下: 1.在什么情况下记录? 各种不同的情况以下面的宇串来决定: auth 关于系统安全与使用者认证； cron 关于系统自动排序执行(CronTable)； daemon 关于背景执行程序； ken 关于系统核心； Ipr 关于打印机； mai1 关于电子邮件； news 关于新闻讨论区； syslog 关于系统记录本身； user 关于使用者； uucp关于UNIX互拷(UUCP)。 2.什么程度才记录P 例如你要系统去记录info等级的事件，则notice、err、warning、Crit、alert、emerg等在info等级以上的也会被一并记录下来。把上面所写的1、2项以小数点组合起来就是完整的"要记录哪些东西"的写法。例如mail.info表示关于电子邮件传送系统的一般性信息。auth.emerg就是关于系统安全方面相当严重的信息。Ipr.none表示不要记录关于打印机的信息(通常用在有多个纪录条件时组合使用)。另外有三种特殊的符号可供应用: 星号(*):代表某一细项中所有项目。例如mail.*表示只要有关mail的，不管什么程度都要记录下来。而*.info会把所有程度为infn的事件给记录下来。 等号(=):表示只记录目前这一等级，其上的等级不要记录。例如上面的例子，平常写

下info等级时，也会把位于info等级上面的notice.err.warning、crit、alert、emerg等其他等级也记录下来。但若你写=info则就只有记录info这一等级了。 惊叹号(!):表示不要记录目前这一等级及其上的等级。 3、记录存放的位置 sysloqd提供下列方法供您记录系统发生的事件: 一般文件 这是最普遍的方式。你可以指定好文件路径与文件名称，但是必须以目录符号"/"开始，系统才会知道这是一个文件。例如/var/adm/maillog表示要记录到/var/adm下面一个称为maillog的文件。如果之前没有这个文件，系统会自动产生一个。 指定的终端机或其他设备 你也可以将系统记录写到一个终端机或是设备上。若将系统记录写到终端机，则目前正在使用该终端机的使用者就会直接在屏幕上看到系统信息(例如/dev/conso旧或是/dev/tty1，你可以拿一个屏幕专门来显示系统信息)。若将系统记录写到打印机(例如/dev/!p0)。，则你会有一长条印满系统记录的纸，这样网络入侵者就不能修改日志来隐藏入侵痕迹。 指定的远端主机 如果你不将系统信息记录在本地机器上，你可以写下网络中另一个主机的名称，然后在主机名称前面加上"@"符号(例如(@)ccunix1.variox.int，但被你指定的主机上必须要有sysloqd)。这可以防止由于硬盘错误等情况使日志文件丢失。 以上就是syslog各项记录程度及记录方式的写法，可以依照自己的需求记录下自己所需要的内容。但是这些记录都是一直追加上去的，除非将文件自行删除掉，否则这些文件就会越来越大。Syslog设备是一个网络攻击者的显著目标，通过修改日志来隐藏入侵痕迹，因此我们要特别注意。最好养成每周(或更短的时间)定期检查一次记录文件的习惯，并将过期的记录文件依照流水号或是日期

备份，以后查阅时也比较容易。千万不要记录下*.*，这样无论什么都被记录下来，结果会导致文件太大，要找资料时根本无法马上找出来。有人在记录网络日志时，连谁去ping他的主机都要记录，这样不仅降低系统效率而且增加了磁盘用量。 路由器日志功能的具体设置方法 首先在UNIX主机上做下列工作，以超级用户注册进入: 其中168.1.1.2为日志主机的IP地址。这样对路由器进行的一些操作将会记录在mail_debug和r2509_debug这两个文件中。 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