

Linux网管必须了解的系统目录_proc_sys_net_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_Linux_E7_BD_91_E7_AE_c103_586608.htm 在Linux的发行版本中，都存在一个/proc/目录，有的也称它为Proc文件系统。在这个目录中，包括了一些特殊的文件，不仅能用来反映内核的现行状态和查看硬件信息，而且，有些文件还允许用户来修改其中的内容，以调节内核的现行工作状态，例如/proc/sys/子目录下的文件。与/proc/目录中其它目录不相同的是，/proc/sys/目录下的文件不仅能提供系统的有关信息，而且还允许用户立即停止或开启内核的某些特性及功能。在/proc/sys/目录中的/proc/sys/net/子目录更是与网络息息相关，我们可以通过设置此目录下的某些文件来开启与网络应用相关的特殊功能，同时，也可以通过设置这个目录下的某些文件来保护我们的网络安全。因此，作为一名Linux下的网络管理员，就很有必要详细了解/proc/sys/net/目录下文件的各种功能和设置方法，让它能更好地为我们工作。

一、/proc/sys/net/目录说明。

/proc/sys/net/目录主要包括了许多网络相关的主题，例如：
：appletalk/,ethernet/,ipv4/,ipx/,及ipv6 /。通过改变这些目录中的文件，网络管理员能够在系统运行时调整相关网络参数。虽然在Linux中还有很多有关网络的配置方法，但熟悉此目录中的相关内容对网络应用是有很大的帮助的。

在/proc/sys/net/目录下有两个目录，与现在的IPV4网络的运行息息相关，调整这两个目录下的某些文件的参数，能为我们的网络应用带到意想不到的效果，这两个目录就是/proc/sys/net/core/目录和/proc/sys/net/ipv4/目录，下面笔者

将会对这两个目录中的重要文件分别作一个详细的说明。 1

、 /proc/sys/net/core/目录。 此目录中包括许多设置用来控制Linux内核与网络层的交互，即当网络有什么动作时，内核做出什么样的相应反应。 在其中有以下的一些重要文件：

（1）、 message_burst：设置每十秒写入多少次请求警告；此设置可以用来防止DOS攻击，缺省设置为50；（2）、 message_cost：设置每一个警告的度量值，缺省为5，当用来防止DOS攻击时设置为0；（3）、 netdev_max_backlog：设置当个别接口接收包的速度快于内核处理速度时允许的最大的包序列，缺省为300；（4）、 optmem_max:设置每个socket的最大辅助缓存大小；（5）、 rmem_default：设置接收socket的缺省缓存大小（字节）；（6）、 rmem_max：设置接收socket的最大缓存大小（字节）；（7）、 wmem_default:设置发送的socket缺省缓存大小（字节）；（8）、 wmem_max:设置发送的socket最大缓存大小（字节）。 2

、 /proc/sys/net/ipv4/目录。 此目录中的内容用来添加网络设置，在其中的许多设置，可以用来阻止对系统的攻击，或用来设置系统的路由功能。 其中有以下的这些重要的文件：

（1）、 icmp_destunreach_rate、 icmp_echoreply_rate、 icmp_paramprob_rate、 icmp_timeexceed_rate：设置发送和回应的最大icmp包的速率，最好不要为0；（2）

、 icmp_echo_ignore_all和icmp_echo_ignore_broadcasts：设置内核不应答icmp echo包，或指定的广播，值为0是允许回应，值为1是禁止；（3）、 ip_default_ttl：设置IP包的缺省生存时间（TTL），增加它的值能减少系统开销；（4）

、 ip_forward：设置接口是否可以转发包，缺省为0，设置为1

时允许网络进行包转发；（5）、ip_local_port_range：当本地需要端口时指定TCP或UDP端口范围。第一数为低端口，第二个数为高端口；（6）、tcp_syn_retries:提供限制在建立连接时重新发送回应的SYN包的次数；（7）、tcp_retries1：设置回应连入重送的次数，缺省为3；（8）、tcp_retries2:设置允许重送的TCP包的次数，缺省为15。二、/proc/sys/net/目录下文件的设置方法。

在了解了/proc/sys/net/core/目录和/proc/sys/net/ipv4/目录中一些重要文件的意义和作用后，下面说说如何设置这两个目录中的这些重要文件来为我们工作的。读者应该了解，在Linux系统中，要改变某种服务或设备的工作状态和功能，主要是通过使用命令方式和直接修改它的配置文件方式来达到目的，对于这两个目录下的文件，我们也可以通过这两种方式来修改这些文件内容中的值，使它们按照我们的意图工作。在进行设置之前，应当注意的是，当你确定要修改某个文件的当前值时，一定要保证输入的命令格式和值的内容都是正确的，因为任何的错误设置都会引起内核的不稳定，如果你不小心造成了这种问题，你就不得不重新引导系统了。在下面的说明中，笔者会将注意的地方特别说明出来的。首先来看看如何使用命令方式来修改这两个目录下文件的。我们可以通过echo和sysctl这两个命令来修改这两个目录中的文件，下面笔者将这两个命令的使用方法分别列出来。1、sysctl命令是为设置这两个目录中的文件而定制的,它被默认安装在/sbin/目录中，我们可以通过使用此命令来显示和设置/proc/sys/net/目录下的文件内容。例如

：/sbin/sysctl -a命令用来显示此目录下的所有文件配置内容

；/sbin/sysctl -w命令用来修改此目录下指定文件中的变量值，

如：`/sbin/sysctl -w net.ipv4.ip_forward="1"`用来设置允许IP包转发。其它的参数，读者可以通过输入`/sbin/sysctl h`命令来得到，在这里就不再具体全部列出了。要注意的是，这个命令的使用需要管理员权限的，如果用户不是以管理员身份登录的，在使用此命令前用`SU`命令得得管理权限后再操作。 2

、`/proc/sys/net/`目录下的文件内容也可以通过用`echo`命令来修改。例如：`echo 1 gt. /proc/sys/net/ipv4/icmp_echo_ignore_all`用来设置不回应ICMP ECHO包。在使用`echo`命令时，还应特别注意此命令的输入格式，即在`echo`命令和值之间，以及值与在于符号（`>`）之间，在于符号与要修改的文件路径之间都必需有一个空格。而且，在这两个目录中的有些文件有不上一个的值，所以，如果你想一次性传递多个值，那么，每一个值之间也应保证用空格隔开。同时也要注意的，用此方法修改`/proc/sys/net/`目录下文件中的内容在系统重新启动后，所设置的内容会全部变为默认值，因此，如果要想设置的值永久有效，可以直接把这个命令加入到`/etc/rc.d/rc.local`文件中，在这里，这个文件的路径是指Red Hat Linux发行版本中的，其它发行版本读者根据具体情况来定。如果命令项太多，也可以把这些命令项编写成一个脚本后，加上可执行权限，再放到这个文件中，这样当系统启动时，就会按`/etc/rc.d/rc.local`中的设置自动执行。如果你不想修改`/etc/rc.d/rc.local`文件，那么笔者推荐你使用`/sbin/sysctl`命令。使用命令方式设置`/proc/sys/net/`目录下的文件固然方便易行，但有一部分读者更喜欢直接修改它们的配置文件的方式，因为这种方式更加直观，但它比较适合对系统了解比较深的用户。与其它服务或设备不同的是，Linux系统只

为/proc/sys/net/目录提供了一个配置文件，那就是/etc/sysctl.conf，用户可以通过直接编辑/etc/sysctl.conf配置文件，来修改增加相应/proc/sys/net/目录下文件内容中的变量的值，这样当系统启动时就会读取此文件中的配置内容来设置相应的项。用vi来编辑此文件是非常简单的，此文件中内容格式也非常清晰易读，如其中有如下条目

：net.ipv4.ip_forward=0,把值修改为1后就打开IP包转发。其实，用/sbin/sysctl命令修改和直接编辑/etc/sysctl.conf文件内容具有相同的效果，因此，为了安全，推荐用户优先使用/sbin/sysctl命令方式。到这里，想必读者已经对/proc/sys/net/目录下的/proc/sys/net/core/和/proc/sys/net/ipv4/这两个目录，已经有了一定了解了。可是，这只是笔者为了突出/proc/目录与IPV4网络的作用而特别选出来说明，其实，在/proc/目录下，还有许多的文件，虽然不能被用户如上述的两个目录那样可以被设置，但是，可以通过这些文件来了解系统详细情况和现行的运行状态，读者可以从网络上找到这个目录的详细说明。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