

proc文件系统中网络参数详解(2)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\\_ti2020/645/2021\\_2022\\_proc\\_E6\\_96\\_87\\_E4\\_BB\\_B6\\_c103\\_645269.htm](https://www.100test.com/kao_ti2020/645/2021_2022_proc_E6_96_87_E4_BB_B6_c103_645269.htm)

`tcp_max_orphans` : INTEGER  
缺省值是8192 系统所能处理不属于任何进程的TCP sockets最大数量。假如超过这个数量那么不属于任何进程的连接会被立即reset，并同时显示警告信息。之所以要设定这个限制纯粹为了抵御那些简单的 DoS 攻击千万不要依赖这个或是人为的降低这个限制(这个值Redhat AS版本中设置为32768,但是很多防火墙修改的时候,建议该值修改为2000)

`tcp_abort_on_overflow` : BOOLEAN 缺省值是0 当守护进程太忙而不能接受新的连接，就象对方发送reset消息，默认值是false。这意味着当溢出的原因是因为一个偶然的猝发，那么连接将恢复状态。只有在你确信守护进程真的不能完成连接请求时才打开该选项，该选项会影响客户的使用。(对待已经满载的sendmail,apache这类服务的时候,这个可以很快让客户端终止连接,可以给予服务程序处理已有连接的缓冲机会,所以很多防火墙上推荐打开它) `tcp_syncookies` : BOOLEAN 默认值是0 只有在内核编译时选择了CONFIG\_SYNCOOKIES时才会发生作用。当出现syn等候队列出现溢出时象对方发送syncookies。目的是为了防止syn flood攻击。注意：该选项千万不能用于那些没有收到攻击的高负载服务器，如果在日志中出现synflood消息，但是调查发现没有收到synflood攻击，而是合法用户的连接负载过高的原因，你应该调整其它参数来提高服务器性能。参考: `tcp_max_syn_backlog`

`tcp_synack_retries` `tcp_abort_on_overflow` `syncookie`严重的违

背TCP协议，不允许使用TCP扩展，可能对某些服务导致严重的性能影响(如SMTP转发)。(注意,该实现与BSD上面使用的tcp proxy一样,是违反了RFC中关于tcp连接的三次握手实现的,但是对于防御syn-flood的确很有用.) tcp\_stdurg

: BOOLEAN 默认值为0 使用 TCP urg pointer 字段中的主机请求解释功能。大部份的主机都使用老旧的 BSD解释，因此如果您在 Linux 打开它或会导致不能和它们正确沟通。

tcp\_max\_syn\_backlog : INTEGER 对于那些依然还未获得客户端确认的连接请求需要保存在队列中最大数目。对于超过 128Mb 内存的系统默认值是 1024 低于 128Mb 的则为 128。如果服务器经常出现过载可以尝试增加这个数字。警告假如您将此值设为大于 1024最好修改 include/net/tcp.h 里面的 TCP\_SYNQ\_HSIZE 以保持 TCP\_SYNQ\_HSIZE\*16 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](http://www.100test.com)