优化Linux系统内核/etc/sysctl.conf

taokey_linux 关注

2016-08-01 19:20:46 1300人阅读 0人评论

```
vim /etc/sysctl.conf

net.ipv4.tcp_syncookies = 1
#表示开启SYN Cookies。当出现SYN等待队列溢出时，启用cookies来处理，可防范少量SYN攻击，默

net.ipv4.tcp_tw_reuse=1
#表示开启重用。运行将TIME-WAIT sockets重新用于新的TCP连接，默认为0，表示关闭。

net.ipv4.tcp_tw_recycle = 1
#表示开启TCP连接中TIME-WAIT sockets的快速回收，默认为0，表示关闭;

net.ipv4.tcp_fin_timeout
#修改系統默认的 TIMEOUT 时间。

net.ipv4.tcp_keepalive_time = 1200
#表示当keepalive起用的时候，TCP发送keepalive消息的频度。缺省是2小时，改为20分钟。

net.ipv4.ip_local_port_range = 10000 65000
#表示用于向外连接的端口范围。缺省情况下很小：32768到61000，改为10000到65000。（注意：这

net.ipv4.tcp_max_syn_backlog = 8192
#表示SYN队列的长度，默认为1024，加大队列长度为8192，可以容纳更多等待连接的网络连接数。

net.ipv4.tcp_max_tw_buckets = 5000
#表示系统同时保持TIME_WAIT的最大数量，如果超过这个数字，TIME_WAIT将立刻被清除并打印警

net.ipv4.tcp_max_syn_backlog = 65536
#记录的那些尚未收到客户端确认信息的连接请求的最大值。对于有128M内存的系统而言，缺省值是1

net.core.netdev_max_backlog = 32768
#每个网络接口接收数据包的速率比内核处理这些包的速率快时，允许送到队列的数据包的最大数目。

net.core.somaxconn = 32768
#net.core.somaxconn是linux中的一个kernel参数，表示socket监听（listen）的backlog上限。什么是b
```

```
net.core.rmem_max = 16777216
```
#最大socket读buffer,可参考的优化值:873200

```
net.core.wmem_max = 16777216
```
#最大socket写buffer,可参考的优化值:873200

```
net.ipv4.tcp_timestsmps = 0
```
#时间戳可以避免序列号的卷绕。一个1Gbps的链路肯定会遇到以前用过的序列号。时间戳能够让内核

```
net.ipv4.tcp_synack_retries = 2
```
#为了打开对端的连接，内核需要发送一个SYN并附带一个回应前面一个SYN的ACK。也就是所谓三次

```
net.ipv4.tcp_syn_retries = 2
```
#在内核放弃建立连接之前发送SYN包的数量。

```
net.ipv4.tcp_tw_reuse = 1
```
开启重用。允许将TIME-WAIT sockets重新用于新的TCP连接。

```
net.ipv4.tcp_wmem = 8192 436600 873200
```
TCP写buffer,可参考的优化值: 8192 436600 873200

```
net.ipv4.tcp_rmem  = 32768 436600 873200
```
TCP读buffer,可参考的优化值: 32768 436600 873200

```
net.ipv4.tcp_mem = 94500000 91500000 92700000
```
同样有3个值,意思是:

net.ipv4.tcp_mem[0]:低于此值，TCP没有内存压力。

net.ipv4.tcp_mem[1]:在此值下，进入内存压力阶段。

net.ipv4.tcp_mem[2]:高于此值，TCP拒绝分配socket。

上述内存单位是页，而不是字节。可参考的优化值是:786432 1048576 1572864

```
net.ipv4.tcp_max_orphans = 3276800
```
#系统中最多有多少个TCP套接字不被关联到任何一个用户文件句柄上。如果超过这个数字，连接将即

```
net.ipv4.tcp_fin_timeout = 30
```
#如果套接字由本端要求关闭，这个参数决定了它保持在FIN-WAIT-2状态的时间。对端可以出错并永远

修改完之后，需要执行sysctl -p，配置才能生效