# 内核参数调优

## 配置1

net.ipv4.ip\_forward

net.ipv4.tcp\_fin\_timeout

net.ipv4.tcp\_fastopen

net.ipv4.tcp\_keepalive\_time = 1200

net.ipv4.tcp\_max\_syn\_backlog = 8192

net.ipv4.tcp\_max\_tw\_buckets = 5000

net.core.netdev\_max\_backlog = 8192

net.core.somaxconn = 8192

net.core.rmem\_max = 12582912

net.core.rmem\_default = 6291456

net.core.wmem\_max = 12582912

net.core.wmem\_default = 6291456

updatedb\_optimum 取消

-------

#CTCDN 系统优化参数

#关闭 ipv6

net.ipv6.conf.all.disable\_ipv6 = 1

net.ipv6.conf.default.disable\_ipv6 = 1

#决定检查过期多久邻居条目

net.ipv4.neigh.default.gc\_stale\_time=120 ny

#使用 arp\_announce / arp\_ignore 解决 ARP 映射问题

net.ipv4.conf.default.arp\_announce = 2 ny

net.ipv4.conf.all.arp\_announce=2 ny

net.ipv4.conf.lo.arp\_announce=2 ny

# 避免放大攻击

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

# 开启恶意 icmp 错误消息保护

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1 ny

#关闭路由转发

net.ipv4.ip\_forward = 0

net.ipv4.conf.all.send\_redirects = 0 n

net.ipv4.conf.default.send\_redirects = 0 n

#开启反向路径过滤

net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.default.rp\_filter = 1

#处理无源路由的包

net.ipv4.conf.all.accept\_source\_route = 0

net.ipv4.conf.default.accept\_source\_route = 0

#关闭 sysrq 功能

kernel.sysrq = 0

#core 文件名中添加 pid 作为扩展名

kernel.core\_uses\_pid = 1

# 开启 SYN 洪水攻击保护

net.ipv4.tcp\_syncookies = 1

#修改消息队列长度

kernel.msgmnb = 65536

kernel.msgmax = 65536

#设置最大内存共享段大小 bytes

kernel.shmmax = 68719476736

kernel.shmall = 4294967296

#timewait 的数量，默认 180000

net.ipv4.tcp\_max\_tw\_buckets = 6000

net.ipv4.tcp\_sack = 1

net.ipv4.tcp\_window\_scaling = 1

net.ipv4.tcp\_rmem = 4096 87380 4194304

net.ipv4.tcp\_wmem = 4096 16384 4194304

net.core.wmem\_default = 8388608

net.core.rmem\_default = 8388608

net.core.rmem\_max = 16777216

net.core.wmem\_max = 16777216

#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.netdev\_max\_backlog = 262144 ~

#限制仅仅是为了防止简单的 DoS 攻击

net.ipv4.tcp\_max\_orphans = 3276800

#未收到客户端确认信息的连接请求的最大值

net.ipv4.tcp\_max\_syn\_backlog = 262144

net.ipv4.tcp\_timestamps = 0

#内核放弃建立连接之前发送 SYNACK 包的数量

net.ipv4.tcp\_synack\_retries = 1

#内核放弃建立连接之前发送 SYN 包的数量

net.ipv4.tcp\_syn\_retries = 1

#启用 timewait 快速回收

net.ipv4.tcp\_tw\_recycle = 1 ny

#开启重用。允许将 TIME-WAIT sockets 重新用于新的 TCP 连接

net.ipv4.tcp\_tw\_reuse = 1

net.ipv4.tcp\_mem = 94500000 915000000 927000000

net.ipv4.tcp\_fin\_timeout = 1 ~

#当 keepalive 起用的时候，TCP 发送 keepalive 消息的频度。缺省是 2 小时

net.ipv4.tcp\_keepalive\_time = 1800 ~

net.ipv4.tcp\_keepalive\_probes = 3

net.ipv4.tcp\_keepalive\_intvl = 15 ~

#允许系统打开的端口范围

net.ipv4.ip\_local\_port\_range = 1024 65000 ~

#修改防火墙表大小，默认 65536

net.netfilter.nf\_conntrack\_max=655350 ny

net.netfilter.nf\_conntrack\_tcp\_timeout\_established=1200 ny

# 确保无人能修改路由表

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.default.accept\_redirects = 0 ny

net.ipv4.conf.all.secure\_redirects = 0 ny

net.ipv4.conf.default.secure\_redirects = 0ny

EOF

n 表示配置2不存在未添加

ny表示配置2不存在已添加

~ 表示配置1，2设置的参数不一致

## 配置2

#决定检查过期多久邻居条目

net.ipv4.neigh.default.gc\_stale\_time=120

#使用 arp\_announce / arp\_ignore 解决 ARP 映射问题

net.ipv4.conf.default.arp\_announce = 2

net.ipv4.conf.all.arp\_announce=2

net.ipv4.conf.lo.arp\_announce=2

# 开启恶意 icmp 错误消息保护

net.ipv4.icmp\_ignore\_bogus\_error\_responses = 1

#启用 timewait 快速回收

net.ipv4.tcp\_tw\_recycle = 1

# Controls source route verification

#开启反向路径过滤

net.ipv4.conf.all.rp\_filter = 1

net.ipv4.conf.default.rp\_filter = 1

net.ipv4.ip\_nonlocal\_bind = 1

net.ipv4.ip\_forward = 1

# 确保无人能修改路由表

net.ipv4.conf.all.accept\_redirects = 0

net.ipv4.conf.default.accept\_redirects = 0

net.ipv4.conf.all.secure\_redirects = 0

net.ipv4.conf.default.secure\_redirects = 0

#处理无源路由的包

net.ipv4.conf.all.accept\_source\_route = 0

net.ipv4.conf.default.accept\_source\_route = 0

# 避免放大攻击

net.ipv4.icmp\_echo\_ignore\_broadcasts = 1

net.ipv4.conf.all.log\_martians = 1

net.ipv4.conf.default.log\_martians = 1

net.ipv4.conf.all.promote\_secondaries = 1

net.ipv4.conf.default.promote\_secondaries = 1

# Controls the use of TCP syncookies

#core 文件名中添加 pid 作为扩展名

kernel.core\_uses\_pid = 1

# Number of pid\_max

kernel.pid\_max = 1000000

# 开启 SYN 洪水攻击保护

net.ipv4.tcp\_syncookies = 1

# Controls the maximum size of a message, in bytes

# Controls the default maxmimum size of a mesage queue

# Controls the maximum shared segment size, in bytes

# Controls the maximum number of shared memory segments, in pages

#修改消息队列长度

kernel.msgmnb = 65536

kernel.msgmax = 65536

#设置最大内存共享段大小 bytes

kernel.shmmax = 68719476736

kernel.shmall = 4294967296

#关闭 sysrq 功能

kernel.sysrq = 1

kernel.softlockup\_panic = 1

kernel.printk = 5

# TCP kernel paramater

net.ipv4.tcp\_mem = 94500000 915000000 927000000

net.ipv4.tcp\_rmem = 4096 87380 4194304

net.ipv4.tcp\_wmem = 4096 16384 4194304

net.ipv4.tcp\_window\_scaling = 1

net.ipv4.tcp\_sack = 1

# Socket buffer

net.core.wmem\_default = 8388608

net.core.rmem\_default = 8388608

net.core.rmem\_max = 16777216

net.core.wmem\_max = 16777216

#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.netdev\_max\_backlog = 32768

net.core.somaxconn = 65535

net.core.optmem\_max = 81920

# TCP conn

#未收到客户端确认信息的连接请求的最大值

net.ipv4.tcp\_max\_syn\_backlog = 262144

#内核放弃建立连接之前发送 SYN 包的数量

net.ipv4.tcp\_syn\_retries = 1

net.ipv4.tcp\_retries1 = 3

net.ipv4.tcp\_retries2 = 15

# TCP conn reuse

net.ipv4.tcp\_timestamps = 0

#开启重用。允许将 TIME-WAIT sockets 重新用于新的 TCP 连接

net.ipv4.tcp\_tw\_reuse = 1

net.ipv4.tcp\_fin\_timeout = 5

net.ipv4.tcp\_max\_tw\_buckets = 7000

#限制仅仅是为了防止简单的 DoS 攻击

net.ipv4.tcp\_max\_orphans = 3276800

#内核放弃建立连接之前发送 SYNACK 包的数量

net.ipv4.tcp\_synack\_retries = 1

# keepalive conn

net.ipv4.tcp\_keepalive\_time = 300

net.ipv4.tcp\_keepalive\_intvl = 30

net.ipv4.tcp\_keepalive\_probes = 3

#允许系统打开的端口范围

net.ipv4.ip\_local\_port\_range = 1024 65535

net.ipv6.neigh.default.gc\_thresh3 = 4096

net.ipv4.neigh.default.gc\_thresh3 = 4096

#修改防火墙表大小，默认 65536

net.netfilter.nf\_conntrack\_max=655350

net.netfilter.nf\_conntrack\_tcp\_timeout\_established=1200