1. **Iptables模块reload问题(解决iptables服务重启导致TCP长连接断开)**

2016年03月17日 [Linux运维](http://www.coooz.com/archives/category/basic/os/linux), [安全基础](http://www.coooz.com/archives/category/basic/security), [系统管理](http://www.coooz.com/archives/category/basic/os), [运维基础](http://www.coooz.com/archives/category/basic) [暂无评论](http://www.coooz.com/archives/690#respond) 阅读 1,936 views 次

    在最近的Linux内核里，默认情况下，Iptables重启动的时候，iptables模块会被卸载(unload)，然后加载重启。

    这种配置下 iptables如果重启，对于那些tcp发起端window scale option有效的的连接会产生以下影响：

     1，重启后 window size会不能被正确识别；

     2，已经建立的tcp会话状态会从ESTABLISHED →　INVALID 导致会话中断；

以上问题对于有重传机制的应用或许问题不大，但是如果一个应用不支持重传，当底层tcp会话中断后 就会发生异常问题。

  如果应用环境中，这种类型会话偏多，而且iptabls的配置又因为安全问题要经常变动，就有必要探讨是否配置强制iptable模块在重启时不被unlod。

以下描述整个配置的修改过程：

1 确认配置情况

① window scale option 的配置确认  
# cat /proc/sys/net/ipv4/tcp\_window\_scaling  
1  
↑ window scale option有效  
0：无效

② iptables的配置  
# grep UNLOAD /etc/sysconfig/iptables-config  
IPTABLES\_MODULES\_UNLOAD="yes"  
↑ iptables模块在重启是会被unload  
"no" ：不会被unload

2 修改配置

1. 系统环境  
   $ uname -a  
   Linux test01 2.6.18-164.el5 #1 SMP Thu Sep 3 03:28:30 EDT 2009 x86\_64 x86\_64 x86\_64 GNU/Linux  
     
   ② 配置修改成重启iptables  
   # /etc/init.d/iptables restart  
   Flushing firewall rules: [ OK ]  
   Setting chains to policy ACCEPT: nat filter [ OK ]  
   Unloading iptables modules: [ OK ] ←　被卸载了  
   Applying iptables firewall rules: [ OK ]  
   Loading additional iptables modules: ip\_conntrack\_netbios\_n[ OK ] ←　重新加载  
   ③　修改配置  
   # vi /etc/sysconfig/iptables-config  
   IPTABLES\_MODULES\_UNLOAD="no"  
     
   ④　配置后重启iptables的结果如下：  
   # /etc/init.d/iptables restart  
   Flushing firewall rules: [ OK ]  
   Setting chains to policy ACCEPT: nat filter [ OK ]  
   Applying iptables firewall rules: [ OK ]  
   Loading additional iptables modules: ip\_conntrack\_netbios\_n[ OK ] ←　模块加载

sed -i '/TABLES\_MODULES\_UNLOAD/s#yes#no#g' /etc/sysconfig/{iptables-config,ip6tables-config}

grep 'UNLOAD' -R /etc/sysconfig