

□□CentOS 6.5安全加固及性能优化

□□

经常玩Linux系统的朋友多多少少也知道些系统参数优化和怎样增强系统安全性, 系统默认的一些参数都是比较保守的, 所以我们可以通过调整系统参数来提高系统内存、CPU、内核资源的占用, 通过禁用不必要的服务、端口, 来提高系统的安全性, 更好的发挥系统的可用性。通过自己对Linux了解, 对系统调优做了如下小结:

□□操作系统:CentOS 6.5_x64最小化安装 1、主机名设置

□□1. [root@localhost~]# vi /etc/sysconfig/network

□□2. HOSTNAME=test.com

□□3.[root@localhost~]# hostname test.com #临时生效

□□2、关闭SELinux

□□1. [root@localhost~]# vi /etc/selinux/config

□□2. SELINUX=disabled

□□3. [root@localhost~]# setenforce #临时生效

□□4.[root@localhost~]# getenforce #查看selinux状态

□□3、清空防火墙并设置规则

□□1. [root@localhost~]# iptables -F #清楚防火墙规则

□□2. [root@localhost~]# iptables -L #查看防火墙规则

□□3. [root@localhost~]# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

□□4. [root@localhost~]# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

□□5. [root@localhost~]# iptables -A INPUT -p tcp --dport 53 -j ACCEPT

□□6. [root@localhost~]# iptables -A INPUT -p udp --dport 53 -j ACCEPT

□□7. [root@localhost~]# iptables -A INPUT -p udp --dport 123 -j ACCEPT

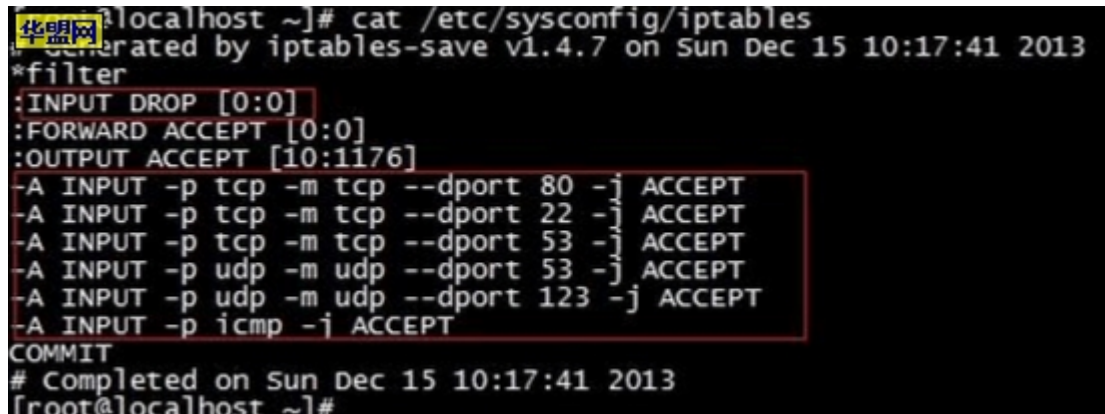
□□8. [root@localhost~]# iptables -A INPUT -p icmp -j ACCEPT

□□9. [root@localhost~]# iptables -P INPUT DROP

□□10.[root@localhost~]# /etc/init.d/iptables save

□□#根据需求开启相应端口

□□

A terminal window showing the contents of the /etc/sysconfig/iptables file. The output is as follows:

```
[root@localhost ~]# cat /etc/sysconfig/iptables
Generated by iptables-save v1.4.7 on Sun Dec 15 10:17:41 2013
*filter
:INPUT DROP [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [10:1176]
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 123 -j ACCEPT
-A INPUT -p icmp -j ACCEPT
COMMIT
# Completed on Sun Dec 15 10:17:41 2013
[root@localhost ~]#
```

□□4、添加普通用户并进行sudo授权管理

□□1. [root@localhost~]# useradd user

□□2. [root@localhost~]# echo "123456" | passwd --stdin user #设置密码

□□3.[root@localhost~]# vi /etc/sudoers #或visudo打开，添加user用户所有权限

□□4. root ALL=(ALL) ALL

□□5.user ALL=(ALL) ALL

□□5、禁用root远程登录

□□1. [root@localhost~]# vi /etc/ssh/sshd_config

□□2. PermitRootLoginno

□□3. PermitEmptyPasswords no #禁止空密码登录

□□4.UseDN Sno #关闭DNS查询

□□6、关闭不必要开机自启动服务

□□

```
华盟网 [root@localhost ~]# chkconfig --list | grep 3:on
blk-availability 0:off 1:off 2:on 3:on 4:on 5:on 6:off 6:off
crond 0:off 1:off 2:on 3:on 4:on 5:on 6:off
ip6tables 0:off 1:off 2:on 3:on 4:on 5:on 6:off
lvm2-monitor 0:off 1:on 2:on 3:on 4:on 5:on 6:off
netfs 0:off 1:off 2:off 3:on 4:on 5:on 6:off
network 0:off 1:off 2:on 3:on 4:on 5:on 6:off
postfix 0:off 1:off 2:on 3:on 4:on 5:on 6:off
rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
udev-post 0:off 1:on 2:on 3:on 4:on 5:on 6:off
[root@localhost ~]# chkconfig auditd off
[root@localhost ~]# chkconfig blk-availability off
[root@localhost ~]# chkconfig ip6tables off
[root@localhost ~]# chkconfig lvm2-monitor off
[root@localhost ~]# chkconfig netfs off
[root@localhost ~]# chkconfig udev-post off
[root@localhost ~]# chkconfig --list | grep 3:on
crond 0:off 1:off 2:on 3:on 4:on 5:on 6:off
network 0:off 1:off 2:on 3:on 4:on 5:on 6:off
postfix 0:off 1:off 2:on 3:on 4:on 5:on 6:off
rsyslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off
sshd 0:off 1:off 2:on 3:on 4:on 5:on 6:off
[root@localhost ~]#
```

□□7、删除不必要的系统用户

□□

```
华盟网 [root@localhost ~]# awk -F ":" '{print $1}' /etc/passwd
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
uucp
operator
games
gopher
ftp
nobody
vcsa
saslauth
postfix
sshd
ntp
[root@localhost ~]# userdel adm
[root@localhost ~]# userdel lp
[root@localhost ~]# userdel shutdown
[root@localhost ~]# userdel halt
[root@localhost ~]# userdel uucp
[root@localhost ~]# userdel operator
[root@localhost ~]# userdel games
[root@localhost ~]# userdel gopher
```

□□8、关闭重启ctl-alt-delete组合键

□□1. [root@localhost ~]# vi /etc/init/control-alt-delete.conf

□□2. #exec /sbin/shutdown -r now "Control-Alt-Deletepressed" #注释掉

□□9、调整文件描述符大小

□□1. [root@localhost ~]# ulimit -n #默认是1024 2. 1024

□□3.[root@localhost ~]# echo "ulimit -SHn 102400">> /etc/rc.local #设置

□□开机自动生效

□□10、去除系统相关信息

□□1. [root@localhost ~]# echo "Welcome to Server" >/etc/issue

□□2.[root@localhost ~]# echo "Welcome to Server" >/etc/redhat-release

□□11、修改history记录

□□1. [root@localhost ~]# vi /etc/profile #修改记录10个

□□2.HISTSIZE=10

□□12、同步系统时间

□□1.[root@localhost ~]# cp /usr/share/zoneinfo/Asia/Shanghai/etc/localtime

□□#设置Shanghai时区

□□2.[root@localhost ~]# ntpdate cn.pool.ntp.org ;hwclock-w #同步时间并写入blos硬件时间

□□3. [root@localhost ~]# crontab -e #设置任务计划每天零点同步一次

□□4.0 * * * * /usr/sbin/ntpdate cn.pool.ntp.org hwclock -w

□□13、内核参数优化

□□1. [root@localhost ~]# vi /etc/sysctl.conf #末尾添加如下参数

□□2.net.ipv4.tcp_syncookies = 1 #1是开启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, 默认是0
关闭

□□3.net.ipv4.tcp_tw_reuse = 1 #1是开启重用, 允许讲TIME_WAIT
sockets重新用于新的TCP连接, 默认是0关闭

□□4.net.ipv4.tcp_tw_recycle = 1 #TCP失败重传次数, 默认是15, 减少次数可释放内核资源

□□5.net.ipv4.ip_local_port_range = 4096 65000 #应用程序可使用的端口范围

□□6. net.ipv4.tcp_max_tw_buckets = 5000
#系统同时保持TIME_WAIT套接字的最大数量, 如果超出这个数字, TIME_WAIT套接字将立刻被清除并打印警告信息, 默认180000

□□7.net.ipv4.tcp_max_syn_backlog = 4096 #进入SYN宝的最大请求队列, 默认是1024

□□8.net.core.netdev_max_backlog = 10240 #允许送到队列的数据包最大设备队列, 默认300

□□9.net.core.somaxconn = 2048 #listen挂起请求的最大数量, 默认128

□□10. net.core.wmem_default = 8388608 #发送缓存区大小的缺省值

□□11.net.core.rmem_default = 8388608 #接受套接字缓冲区大小的缺省值(以字节为单位)

□□12. net.core.rmem_max = 16777216 #最大接收缓冲区大小的最大值

□□13. net.core.wmem_max = 16777216 #发送缓冲区大小的最大值

□□14.net.ipv4.tcp_synack_retries = 2 #SYN-ACK握手状态重试次数, 默认5

□□15. net.ipv4.tcp_syn_retries = 2 #向外SYN握手重试次数, 默认4

□□16.net.ipv4.tcp_tw_recycle = 1 #开启TCP连接中TIME_WAIT sockets的快速回收, 默认是0关闭

□□17.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, 如果超出这个数字, 孤儿连接将立即复位并打印警告信息

□□18. net.ipv4.tcp_mem = 94500000 915000000 927000000

□□19. net.ipv4.tcp_mem[0]:低于此值, TCP没有内存压力;

□□20. net.ipv4.tcp_mem[1]:在此值下, 进入内存压力阶段;

□□

21.net.ipv4.tcp_mem[2]:高于此值, TCP拒绝分配socket。内存单位是页, 可根据物理内存大小进行调整, 如果内存足够大的话, 可适当往上调。上述内存单位是页, 而不是字节。

至此CentOS 6.5_x64最小化安装系统基本优化调整完毕, 需要重启下系统。