[系统优化 3](#_Toc143535872)

[SELinux 3](#_Toc1781865234)

[永久关闭需要修改selinux的配置文件 3](#_Toc1753256331)

[修改配置文件： 3](#_Toc1244683749)

[临时关闭SELinux 4](#_Toc406180691)

[Runlevel 5](#_Toc1773879645)

[查看runlevel 的运行级别 5](#_Toc806943643)

[切换运行级别 5](#_Toc1005506681)

[精简系统开机启动 6](#_Toc1405553085)

[必须启动的五个服务介绍 6](#_Toc1709824888)

[查看系统启动项 6](#_Toc1864152511)

[关掉除sshd rsyslog netowrk crond sysstat的其它服务 6](#_Toc487630868)

[关闭 iptables 防火墙 7](#_Toc840823954)

[查看防火墙 7](#_Toc1037567421)

[关闭防火墙 8](#_Toc682427699)

[查看状态 8](#_Toc908151644)

[最小化原理 8](#_Toc1321174148)

[SSH Secure Shell 9](#_Toc33173657)

[SSH介绍 9](#_Toc1605431242)

[安装SSH 9](#_Toc819968379)

[查看SSHD的进程以及端口号 9](#_Toc533167946)

[客户端 11](#_Toc2092967184)

[用户管理 11](#_Toc1491737311)

[用户账户的管理 12](#_Toc874058760)

[系统字符集 12](#_Toc673242883)

[设置Linux 服务器时间同步 13](#_Toc2117836880)

[文件描述符 14](#_Toc1568250376)

[系统内核 14](#_Toc947456493)

[Linux版本信息及修改 16](#_Toc1554741772)

[目录结构 17](#_Toc597249797)

[总结 17](#_Toc1439892073)

# 系统优化

## SELinux

SELinux(Security-Enhanced Linux) 是美国国家安全局（NSA）对于强制访问控制的实现，是 Linux历史上最杰出的新安全子系统。因为控制太严格，生产环境不用它，使用其他的安全手段（永久关闭需要重启系统）

### 永久关闭需要修改selinux的配置文件

# cat /etc/selinux/config

# This file controls the state of SELinux on the system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - No SELinux policy is loaded.

SELINUX=enforcing

# SELINUXTYPE= can take one of these two values:

# targeted - Targeted processes are protected,

# mls - Multi Level Security protection.

SELINUXTYPE=targeted

### 修改配置文件：

Selinux 有三个值，enforcing, permissive, disabled.

* Permissive 就是selinux 有效，但是即使你违反了策略的话率让你继续操作，但是把你违反的内容记录下来。
* Enforcing 就是你违反了策略，你就无法继续操作下去。
* Disabled 就是不启用selinux

SELINUXTYPE 主要有两大娄

* Targeted 是红帽开始的，它只是对于主要的网络服务进行保护，比如apache, sendmail, bind,等，不属于那些domain的都让他们在unconfined\_t里，可导入性高，可用性好但不能对整体进行保护
* Mls

关闭SELinux 需要把SELINUX=enforcing改为SELINUX= disabled

1. 在修改之前先备份文件

$cp /etc/selinux/config /etc/selinux/config,bak

1. 之后可以用VIM修改也可以用其它方法修改

$sed 's#SELINUX=enforcing #SELINUX=disabled #g' /etc/selinux/config

# This file controls the state of SELinux on the system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - No SELinux policy is loaded.

SELINUX=disabled

# SELINUXTYPE= can take one of these two values:

# targeted - Targeted processes are protected,

# mls - Multi Level Security protection.

SELINUXTYPE=targeted

查看是否修改对，然后加上 –i 修改文件

1. 修改后查看

$grep disabled /etc/selinux/config

# disabled - No SELinux policy is loaded.

SELINUX=disabled

### 临时关闭SELinux

getenforce - get the current mode of SELinux 首先查看当前selinux状态

$ getenforce

Enforcing

setenforce - modify the mode SELinux is running in. 修改selinux 运行状态

setenforce [ Enforcing | Permissive | 1 | 0 ] 1为enforcing; 0为permissive

$ setenforce 0

$getenforce

Permissive

## Runlevel

linux操作系统自从开始启动至启动完毕需要经历几个不同的阶段（用数字表示），这几个阶段就叫做runlevel，同样，当linux操作系统关闭时也要经历另外几个不同的runlevel，

### 查看runlevel 的运行级别

$cat /etc/inittab

# Default runlevel. The runlevels used are:

# 0 - halt (Do NOT set initdefault to this)

# 1 - Single user mode

# 2 - Multiuser, without NFS (The same as 3, if you do not have networking)

# 3 - Full multiuser mode

# 4 - unused

# 5 - X11

# 6 - reboot (Do NOT set initdefault to this)

id:3:initdefault:

单用户用来找回root密码，3多用户文本模式，(工作模式)

### 切换运行级别

$ init 6

## 精简系统开机启动

精简系统开机启动：节省开机时间，加快启动速度；节省资源开销； 减少安全隐患。

需要开机启动的服务有：sshd rsyslog netowrk crond sysstat

在centos里也可以用setup 选第四项system services来选择修改系统启动项。或者类似windows下的msconfig 输入ntsysv 也可以进入system services来个性系统启动项下面主要介绍用chkconfig来关闭开机启动服务

### 必须启动的五个服务介绍

sshd 远程连接服务

rsyslog 是操作系统提供的一种机制，系统的守护程序通常会使用rsyrlog将各种信息写到各个系统日志文件中

network网络服务

crond 闹钟服务 周期性的处理一些重复的问题。

sysstat 监测系统性能及效率的一组工具

### 查看系统启动项

$ chkconfig

abrt-ccpp 0:off 1:off 2:off 3:on 4:off 5:on 6:off

abrtd 0:off 1:off 2:off 3:on 4:off 5:on 6:off

acpid 0:off 1:off 2:on 3:on 4:on 5:on 6:off

atd 0:off 1:off 2:off 3:on 4:on 5:on 6:off

auditd 0:off 1:off 2:on 3:on 4:on 5:on 6:off

…

### 关掉除sshd rsyslog netowrk crond sysstat的其它服务

也可以用grep 来过滤，runlevel为3的启动项

$ chkconfig --list|grep 3:on|awk '{print $1,$5}' >runlevel3on.txt

abrt-ccpp 3:on

abrtd 3:on

acpid 3:on

atd 3:on

auditd 3:on

把sshd rsyslog netowrk crond sysstat这五个服务过滤掉

$ chkconfig --list|grep 3:on|awk '{print $1}'|grep -Ev "sshd|rsyslog|network|crond|sysstat" >runlevel3on.txt

现在就可以把这些服关掉了下面有多种方法来实现

$ for name in `cat runlevel3on.txt`;do chkconfig $name --level 3 off;done

$ cat runlevel3on.txt | awk '{print "chkconfig " $1 " --level 3 off"}'| bash

$ awk '{print "chkconfig " $1 " --level 3 off"}' runlevel3on.txt | bash

$ cat runlevel3on.txt |sed 's#\(.\*\)#chkconfig –-level 3 \1 off#g'| bash

$ sed 's#\(.\*\)#chkconfig –-level 3 \1 off#g' runlevel3on.txt| bash

$ sed –r 's#(.\*)#chkconfig –-level 3 \1 off#g' runlevel3on.txt| bash

现在为止已经把除那必要的服务之外的其它服务都关闭了

## 关闭 iptables 防火墙

关闭防火墙是为了初学者学习更方便。

### 查看防火墙

$ iptables -L -n

Chain INPUT (policy ACCEPT)

target prot opt source destination

ACCEPT all -- 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED

ACCEPT icmp -- 0.0.0.0/0 0.0.0.0/0

ACCEPT all -- 0.0.0.0/0 0.0.0.0/0

ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22

REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain FORWARD (policy ACCEPT)

target prot opt source destination

REJECT all -- 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited

Chain OUTPUT (policy ACCEPT)

target prot opt source destination

### 关闭防火墙

$ /etc/init.d/iptables stop

iptables: Setting chains to policy ACCEPT: filter [ OK ]

iptables: Flushing firewall rules: [ OK ]

iptables: Unloading modules: [ OK ]

$ service iptables stop %无法用tab补全，不常用的命令

### 查看状态

$ /etc/init.d/iptables status

iptables: Firewall is not running.

## 最小化原理

安装linux系统最小化，即选包最小化，yum安装最小化

开机自启动服务最小化，操作命令最小化

登录用户最小化，尽量用普通用户登录，特殊需求切到root

普通用户授权权限最小化。

Linux系统文件及目录权限设置最小化，禁止随意创建，更改，删除文件。

## SSH Secure Shell

### SSH介绍

SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。SSH最初是UNIX系统上的一个程序，后来又迅速扩展到其他操作平台。SSH在正确使用时可弥补网络中的漏洞。SSH客户端适用于多种平台。几乎所有UNIX平台—包括HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix，以及其他平台，都可运行SSH。

### 安装SSH

$ rpm –aq openssh openssl

Openssh主要负责的是实现远程连接这个功能，openssl主要负责连接的加密传输。

Linux远程管理端口是22 管理端口的范围可以是0-5535， windows 类似ssh远程桌面的端口号是3389，

在linux里运行着的服务都会有一个控制服务行为的文件，配置文件。而ssh 的配置文件是 /etc/ssh/sshd\_config在SSH服务端里，有一个SSHD守护进程，D的意思是后台运行。

# /etc/init.d/sshd status

openssh-daemon (pid 1240) is running...

### 查看SSHD的进程以及端口号

$ ps -ef |grep sshd

root 1552 1 0 Sep25 ? 00:00:00 /usr/sbin/sshd

root 41537 1552 0 07:35 ? 00:00:00 sshd: root@pts/0

root 41716 1552 0 07:42 ? 00:00:00 sshd: root@pts/1

root 41796 41721 0 07:58 pts/1 00:00:00 grep sshd

$ netstat -lntup |grep sshd

tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 1552/sshd

tcp 0 0 :::22 :::\* LISTEN 1552/sshd

# ss -lntup|grep ssh

tcp LISTEN 0 128 :::52113 :::\* users:(("sshd",1240,4))

tcp LISTEN 0 1 \*:52113 \*:\* users:(("sshd",1240,3))

在修改sshd\_config之前先备份

# cp /etc/ssh/sshd\_config /etc/ssh/sshd\_config.bak\_10.05

我们再起需要配置的sshd\_config有下面几个：

Port 52113 修改默认端口

UseDNS no 不使用DNS

PermitRootLogin no 禁止root 登录

ListenAddress 192.168.1.101 只允许这个IP访问

PermitEmptyPasswords no

GSSAPIAuthentication no

GSSAPIAuthentication这个是解决linux之间使用SSH远程连接慢的问题

UseDNS，指定SSHD是否应该对远程主机名进行反向解析，以检查此主机名是否与其IP地址真实对应，默认值为yes建议改成no,否则可能会导致ssh连接很慢

PermitRootLogin是否允许root登录，yes表示允许； without passwords表示禁止使用密码认证登录；foreced commands only表示只有指定了command选项的情况下才允许使用公钥登录，同时其认证方法全部被禁止。

sed –ir ’13 iPort 52113\nPermitRootLogin no\nPermitEmptyPasswords no\nUseDNS no\nGSSAPIAuthentication no' sshd\_config

现在我们知道有很多种方法修改比如 VI或者用echo追加后。

使之生效。

$ /etc/init.d/sshd reload

### 客户端

客户端常用的软件有CRT XSHELL PUTTY。连接方法在这里便不多介绍，仅介绍下故障排查思路

连接服务端故障排查思路：

1: Ping 主机，

2:telnet 主机（在linux里可以用yum install telnet nmap 来安装telnet和nmap）

3:查看防火墙

Connection refused 的主要原因可能是防火墙，或者是ssh没开。

No route to host 主要原因是防火墙，查看[关闭防火墙方法](#_关闭防火墙)

## 用户管理

Linux是个多用户多任务的分时操作系统，所有一个要使用系统资源的用户都必须先向系统管理员申请一个账号，然后以这个账号的身份进入系统。用户的账号一方面能帮助系统管理员对使用系统的用户进行跟踪，并控制他们对系统资源的访问；另一方面也能帮助用户组织文件，并为用户提供安全性保护。每个用户账号都拥有一个惟一的用户名和用户口令。用户在登录时键入正确的用户名和口令后，才能进入系统和自己的主目录。  
实现用户账号的管理，要完成的工作主要有如下几个方面：  
a.用户账号的添加、删除和修改。  
b.用户口令的管理。  
c.用户组的管理。

Root 超级管理员 ====》皇帝

普通用户====》公民（root就会任命一部分用户管理 linux）

虚拟用户 ====》 傀儡(没有实际用途，为了程序服务启动要求)

### 用户账户的管理

用户账号的管理主要涉及到用户账号的添加、删除和修改。  
添加用户账号就是在系统中创建一个新账号，然后为新账号分配用户号、用户组、主目录和登录Shell等资源。刚添加的账号是被锁定的，无法使用。

useradd用来建立用户帐号。帐号建好之后，再用passwd设定帐号的密码．而可用userdel删除帐号。使用useradd指令所建立的帐号，实际上是保存在/etc/passwd文本文件中。可以用usermod来修改用户信息，其参数与useradd相同。可以用id username 来查看username 的id。 group username显示用户username所在的组,缺省为当前用户所在的组信息

$ useradd -d /usr/oldboy -m oldboy

$ passwd oldboy

使用userdel删除账号时

$ userdel -r oldboy

如果需要修改当前用户信息，需要使用usermod

$ usermod -s /bin/ksh -d /home/z -g developer sam

此命令将用户sam的登录Shell修改为ksh，主目录改为/home/z，用户组改为developer。

$ Useradd oldgirl && echo "123456" |passwd –stdin oldgirl

可以用id username 或者在 /etc/passwd里查看用户信息

可以用su - username 来切换用户。然后用whoami来查看当前用户

普通用户的提示符为$。 root用户提示符为#

$ set|grep -i ps1  
PS1='[\u@\h \W]\$ '

$ PS1='[\u@\h \W\t]\$'

## 系统字符集

查看系统字符集,以及修改字符集

$ cat /etc/sysconfig/i18n

LANG="en\_US.UTF-8"

SYSFONT="latarcyrheb-sun16"

$ cp /etc/sysconfig/i18n /etc/sysconfig/i18n.bak\_10.05

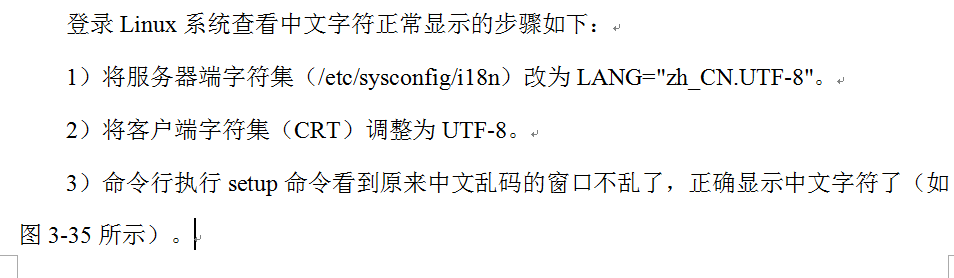
$ sed –I ‘s#LANG=”en\_US.UTF-8”#LANG=”zh\_CN.UTF-8”#g’ /etc/sysconfig/i18n

$cat /etc/sysconfig/i18n

$ . /etc/sysconfig/i18n

$ echo $LANG

调整客户端，属性，外观，



## 设置Linux 服务器时间同步

date 用来查看时间。 cal 时查看日历

uptime 查看时间，系统负载，

同步网络服务器

$ /usr/sbin/ntpdate time.nist.gov

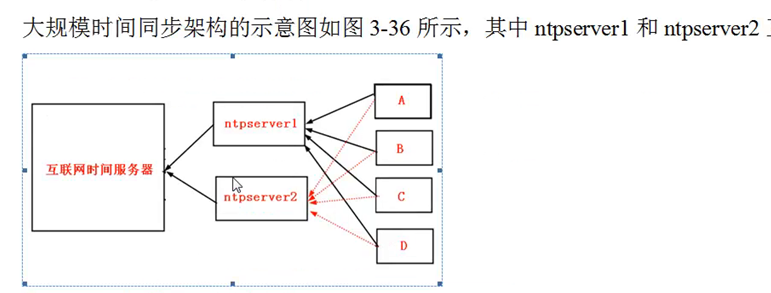
下面介绍一个定时任务crond 让时间第隔五分钟更新一次

$ echo "\*/5 \* \* \* \* /usr/sbin/ntpdate time.nist.gov >/dev/null 2>&1 " >> /var/spool/cron/root

五个星的意思是： 分 时 日 月 星期

>/dev/null 2>&1 标准输出与错误输出都输到/etc/null 也可以这样写 1>/dev/null 2>/dev/null 或 &>/dev/null

如果公司有多台服务器，多台服务器都与网络时间服务器同步时间时宽带开销便会增大。可以用以下方法



## 文件描述符

就是数字，当运行某个程序时，用文件描述符来标识该运行程序打开的文件。如果无文件描述符，程序便会运行异常。

[root@oldboy ~]# ulimit -n  
1024

Echo '\* - nofile 65535 ' >>/etc/security/limits.conf

$ulimit –SHn 65535

## 系统内核

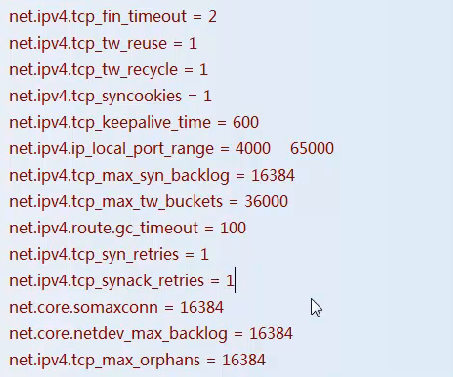
内核配置文件在 /etc/sysctl.conf 修改后可以用 sysctl –p 生效

Please note that modules loaded after sysctl is run may override the settings (example: sunrpc.\* settings are overridden hen the sunrpc module is loaded). This may cause some confusion during boot when the settings in sysctl.conf may be overriden. to prevent such a situation, sysctl must be run after the particular module is loaded

net.ipv4.tcp\_fin\_timeout = 2  
net.ipv4.tcp\_tw\_reuse = 1  
net.ipv4.tcp\_tw\_recycle = 1  
net.ipv4.tcp\_syncookies = 1  
net.ipv4.tcp\_keepalive\_time = 600  
net.ipv4.ip\_local\_port\_range = 4000    65000  
net.ipv4.tcp\_max\_syn\_backlog = 16384  
net.ipv4.tcp\_max\_tw\_buckets = 36000  
net.ipv4.route.gc\_timeout = 100  
net.ipv4.tcp\_syn\_retries = 1  
net.ipv4.tcp\_synack\_retries = 1  
net.core.somaxconn = 16384  
net.core.netdev\_max\_backlog = 16384  
net.ipv4.tcp\_max\_orphans = 16384  
#以下参数是对iptables防火墙的优化，防火墙不开会提示，可以忽略不理。  
net.nf\_conntrack\_max = 25000000  
net.netfilter.nf\_conntrack\_max = 25000000  
net.netfilter.nf\_conntrack\_tcp\_timeout\_established = 180  
net.netfilter.nf\_conntrack\_tcp\_timeout\_time\_wait = 120  
net.netfilter.nf\_conntrack\_tcp\_timeout\_close\_wait = 60  
net.netfilter.nf\_conntrack\_tcp\_timeout\_fin\_wait = 120

网络状态说明及优化命令和优化细节参考资料请看：  
http://yangrong.blog.51cto.com/6945369/1321594 ç老男孩教育的优秀学生博文  
http://oldboy.blog.51cto.com/2561410/1336488

echo 0 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all  [root@www ~]# echo "net.ipv4.icmp\_echo\_ignore\_all=1" >> /etc/sysctl.conf  
[root@www ~]# tail -1 /etc/sysctl.conf   
net.ipv4.icmp\_echo\_ignore\_all=1  
[root@www ~]# sysctl -p  
生效：  
[root@www ~]# echo "net.ipv4.icmp\_echo\_ignore\_all=1" >> /etc/sysctl.conf  
[root@www ~]# tail -1 /etc/sysctl.conf   
net.ipv4.icmp\_echo\_ignore\_all=1  
[root@www ~]# sysctl -p  
  
还原：  
echo 0 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all



## Linux版本信息及修改

版本信息放在/etc/issue /etc/issue.net里面，只需要清空便在启动时不会显示版本信息

自定义启动时的信息可以修改/etc/motd

# 目录结构

FILES

/etc/group

Group account information.

/etc/login.defs

Shadow password suite configuration.

/etc/passwd

User account information.

/etc/shadow

Secure user account information.

# 总结

1）不用root管理,以普通用户的名义通过sudo授权管理。  
2) 更改默认的远程连接SSH服务端口，禁止root用户远程连接，  
甚至要更改为只监听内网IP。  
  
3）定时自动更新服务器时间，使其和互联网时间同步。  
  
4）配置yum更新源,从国内更新源下载安装软件包。  
  
5）关闭seLinux及iptables（在工作场景中，如果有外部IP一般要打开iptables，高并发除外）。  
6）调整文件描述符的数量，进程及文件的打开都会消耗文件描述符。  
  
7）定时自动清理邮件目录垃圾文件，防止inodes节点被占满  
（注意Centos6和Centos5的目录不同）。  
  
8）精简并保留必要的开机自启动服务（如crond、sshd、network、rsyslog、sysstat）。  
  
9）Linux内核参数优化/etc/sysctl.conf，执行sysctl -p生效。  
  
10）更改字符集，使其支持中文，但建议还是用英文字符集，防止出现乱码问题。  
  
11）锁定关键系统文件如（/etc/passwd /etc/shadow /etc/group /etc/gshadow /etc/inittab）  
处理以上内容后把chattr、lsattr改名为oldboy，这样就安全多了。  
  
12）清空/etc/issue、/etc/issue.net，去除系统及内核版本登录前的屏幕显示。  
  
13）清除多余的系统虚拟账号。  
  
14）为grub菜单加密码。  
  
15)禁止被PING

16）升级漏洞软件

优化系统总结 定时清理邮件邮务临时文件，配置防火墙，清除多余的账户，grub加密， sudo管理，linux内核优化