

版本：V1.0

计算机终端安全配置手册 (For Linux)



信息规划与管理部

发布日期：2012 年 6 月 29 日

NEUSOFT CONFIDENTIAL

Neusoft

前 言

随着公司业务发展需要，很多计算机终端安装 Linux 操作系统，为加强计算机终端安全的管理，降低计算机受到各种威胁和攻击的风险，保障计算机安全稳定运行，现针对 Linux 操作系统的安全设置，编制本手册。

手册通过帐户设置、特权文件权限管理、网络安全相关设置、日志文件开启设置 4 个部分阐述 Linux 操作系统安全设置方法。员工应依据部门的业务需要，进行合理地设置。

手册中描述的各项设置要求适用于 Linux 2.2.x/2.4.x /2.6.x 内核版本系统，并在 Red Hat Enterprise Linux 4.2、CentOS5.4、Ubuntu11.04 环境下测试通过。

本手册中部分服务（如 NTP、SSH 等）在某些操作系统版本中缺省没有安装，所以部分文件或命令无法运行，需要手动安装后进行相关设置。

如果您发现手册有任何问题，或者对于本手册有任何意见或建议，请通过以下方式反馈给信息规划与管理部：

电话：024-83665512、924-65512

邮箱：ipm@neusoft.com

目 录

1. 帐户设置	1
1.1 设置密码策略	1
1.2 设置屏幕保护程序	2
1.3 删除无用的特殊账户	3
2. 特权文件权限管理	4
2.1 用户名密码文件权限控制	4
2.2 /etc/services文件权限控制	5
2.3 /etc/rc.d/init.d下script文件权限控制	5
3. 网络安全相关设置	6
3.1 限制超级管理员直接远程登录	6
3.2 修改SSH端口	6
3.3 隐藏系统信息	7
3.4 关闭系统不必要的服务	7
3.5 设置时钟同步	8
4. 日志文件开启设置	9
附录：Linux操作系统终端安全CheckList	11

1. 帐户设置

1.1 设置密码策略

公司对于密码的设置有着严格的规定，Linux 操作系统同 Windows 操作系统一样，也应该遵循相应的强密码策略的要求，通过修改密码策略的最长使用期限、密码最小长度可以起到部分强制密码策略的作用。

密码策略修改以后，需要重新启动系统，并使用 passwd 命令重新设置密码，同时确认使用强密码，以确保系统中不存在空口令、弱口令。

设置要求：必须

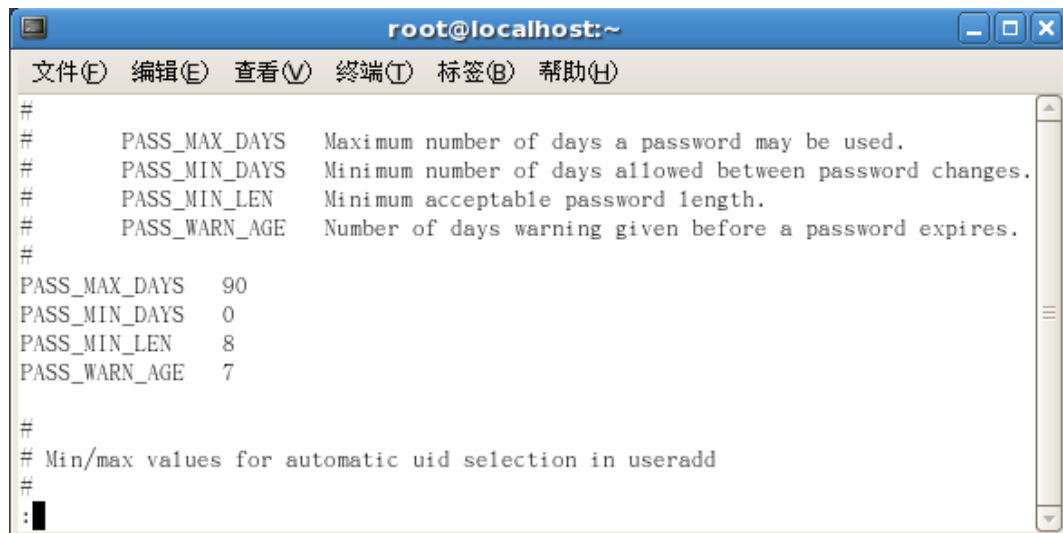
设置方法：

1、CentOS、Red Hat 设置方法：

```
[root@localhost]#vi /etc/login.defs
```

打开 login.defs 文件后，修改如下参数值：

PASS_MAX_DAYS	90	#口令最长保留期限 90 天
PASS_MIN_DAYS	0	#口令最短保留期限 0 天
PASS_MIN_LEN	8	#口令最小 8 个字符
PASS_WARN_AGE	7	#口令到期前 7 天提醒



2、Ubuntu 设置方法：

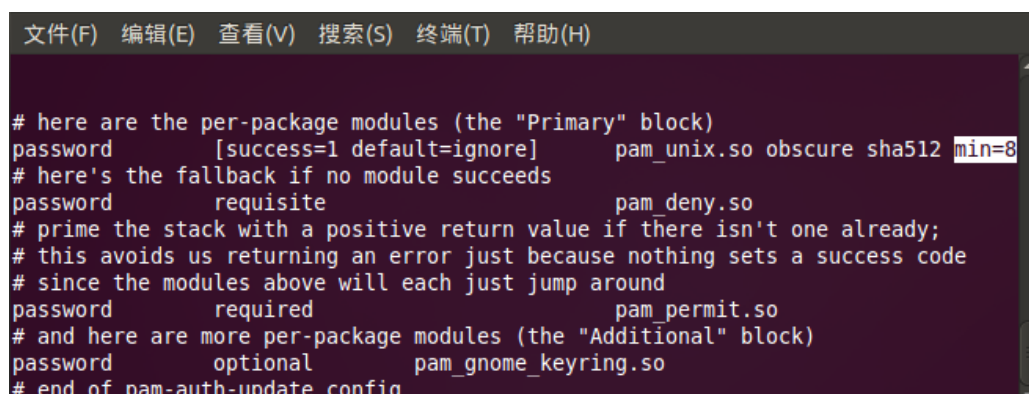
1) 设置最短密码为 8 位

```
[root@localhost]#vi /etc/pam.d/common-password
```

在 password [success=1 default=ignore] pam_unix.so obscure sha512 后

添加：min=8。

如下图所示：



```
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)

# here are the per-package modules (the "Primary" block)
password      [success=1 default=ignore]      pam_unix.so obscure sha512 min=8
# here's the fallback if no module succeeds
password      requisite                        pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password      required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
password      optional                        pam_gnome_keyring.so
# end of pam-auth-update config
```

2) 修改密码有效期为 90 天

chage -M 90 username(即需要修改密码的用户名，如 root)

1.2 设置屏幕保护程序

员工离开座位时，如果忘记注销 root 账户，将会带来很大的安全隐患，应设置屏幕保护程序开启时长，使系统自动注销。

设置要求：必须

设置方法：

1、CentOS、Red Hat 设置方法：

[root@localhost /]#vi /etc/profile

编辑 profile 文件，在“ HISTSIZE ”一行的后面增加一行：TMOUT=300，如下图所示，保存退出。数字 300 表示 300 秒，也就是 5 分钟，如果系统中登陆的用户在 5 分钟内都没有动作，系统将自动注销，从而实现账户保护。



```
root@localhost:/etc

文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)

# No core files by default
ulimit -S -c 0 > /dev/null 2>&1

if [ -x /usr/bin/id ]; then
    USER=`id -un`
    LOGNAME=$USER
    MAIL="/var/spool/mail/$USER"
fi

HOSTNAME=`/bin/hostname`
HISTSIZE=1000
TMOUT=300

— INSERT —
```

2、Ubuntu 设置方法：

在任务栏上选择【系统】--》【首选项】--》【屏幕保护程序】，设置屏保密码为 5 分钟，同时勾选“计算机空闲时激活屏幕保护程序”、“屏幕保护程序激活时锁定屏幕”两项，如下图所示。



1.3 删除无用的特殊账户

在 Linux 操作系统安装后，系统会自动增加很多的特殊帐户，分别应用于不同的用途，如 Sendmail、Ftp 等。

员工应该根据业务需要，删除所有无用的缺省用户（比如 lp, sync, shutdown, halt, news, uucp, operator, games, gopher 等）。以下以 CentOS5.4 的缺省用户名举例，在不同版本中会略有不同。

设置要求：建议

设置方法：

在终端中输入如下命令删掉相应帐户（/etc/passwd）：

```
[root@localhost ~]#userdel adm
```

```
[root@localhost ~]#userdel lp
```

```
[root@localhost ~]#userdel sync
```

```
[root@localhost ~]#userdel shutdown
```

```
[root@localhost ~]#userdel halt
```

```
[root@localhost ~]#userdel mail（用于 sendmail、procmail.mailx 帐户）
```

```
[root@localhost ~]# userdel news
```

```
[root@localhost ~]# userdel uucp
```

```
[root@localhost ~]# userdel operator
```

```
[root@localhost ~]# userdel games (用于 X windows 帐户)
```

```
[root@localhost ~]# userdel gopher
```

```
[root@localhost ~]# userdel ftp (用于匿名 FTP 服务)
```



```
root@localhost:~  
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)  
[root@localhost ~]# userdel adm  
[root@localhost ~]# userdel lp  
[root@localhost ~]# userdel sync  
[root@localhost ~]# userdel shutdown  
[root@localhost ~]# userdel halt  
[root@localhost ~]# userdel mail  
[root@localhost ~]# userdel news  
[root@localhost ~]# userdel uucp  
[root@localhost ~]# userdel operator  
[root@localhost ~]# userdel gopher  
[root@localhost ~]# userdel ftp  
[root@localhost ~]#
```

2. 特权文件权限管理

2.1 用户名密码文件权限控制

Linux 系统将用户名存放在 `/etc/passwd` 文件中，密码以加密的形式存放在 `/etc/shadow` 文件中，通过设置这两个文件的属性，可以防止他人使用口令破解工具得到加密前的口令，但经过此项设置后，将会影响到用户修改密码，增加、删除或修改用户等操作。

`/etc/passwd` 记录当前用户列表

`/etc/shadow` 记录当前密码配置

设置要求：必须

设置方法：

```
[root@localhost ~]# chmod +i /etc/passwd
```

```
[root@localhost ~]# chmod +i /etc/shadow
```

使用 `lsattr` 命令可以查看文件属性：

```
[root@localhost ~]# lsattr /etc/passwd
```

```
[root@localhost ~]# lsattr /etc/shadow
```

注：`chmod` 是改变文件属性的命令，参数 `i` 代表不得任意更改文件或目录，此处的 `i`

为不可修改位（下同）。

2.2 /etc/services 文件权限控制

Linux 操作系统中/etc/services 是等同于 windows 下的服务进程，使/etc/services 文件免疫，可以有效防止未经许可的删除或添加服务。

该项设置将会影响到服务的增加、删除等操作。

设置要求：必须

设置方法：

```
[root@localhost /]#chattr +i /etc/services
```



只有 root 账户才能解锁，用命令：

```
[root@localhost /]#chattr -i /etc/services
```

使用 lsattr 命令可以查看文件属性：

```
[root@localhost /]#lsattr /etc/ services
```



2.3 /etc/rc.d/init.d 下 script 文件权限控制

Linux 操作系统中/etc/rc.d/init.d 目录下放的是服务启动脚本文件，用以决定启动时需要运行的所有正常进程的开启和停止。通过此项设置，只允许 root 用户在该目录下使用 Read、Write、Execute 脚本文件的权限。

设置要求：必须

设置方法：

```
[root@localhost /]#chmod -R 700 /etc/rc.d/init.d/*
```




```
root@localhost:/etc/rc.d/init.d
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
[root@localhost init.d]# chmod -r /etc/rc.d/init.d/*
[root@localhost init.d]# ls -l
总计 836
-rwx--x--x 1 root root 1566 2009-09-09 acpid
-rwx--x--x 1 root root 1441 2007-03-28 anacron
-rwx--x--x 1 root root 1429 2007-03-14 apmd
-rwx--x--x 1 root root 1176 2007-01-06 atd
-rwx--x--x 1 root root 3328 2009-09-04 auditd
-rwx--x--x 1 root root 3059 2009-09-04 autofs
-rwx--x--x 1 root root 1848 2009-09-20 avahi-daemon
-rwx--x--x 1 root root 1789 2009-09-20 avahi-dnscfgd
```

3. 网络安全相关设置

3.1 限制超级管理员直接远程登录

使用超级管理员权限直接远程登录，会使计算机终端存在较大的安全风险。远程执行超级管理员权限操作时，必须以普通权限用户远程登录后，再切换到超级管理员权限账户。这样，即使他人获取到计算机的 root 用户权限，也无法远程操控计算机。

设置要求：建议

设置方法：

```
[root@localhost /]#vi /etc/ssh/sshd_config
```

把 PermitRootLogin yes 改为 PermitRootLogin no



```
root@localhost:/etc/ssh
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
PermitRootLogin no
— INSERT —
```

修改后，需要重新启动 sshd 服务：

```
[root@localhost /]#service sshd restart
```



```
root@localhost:/etc/ssh
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
[root@localhost ssh]# service sshd restart
停止 sshd: ok yes [确定]
启动 sshd: ve yes [确定]
[root@localhost ssh]#
```

3.2 修改 SSH 端口

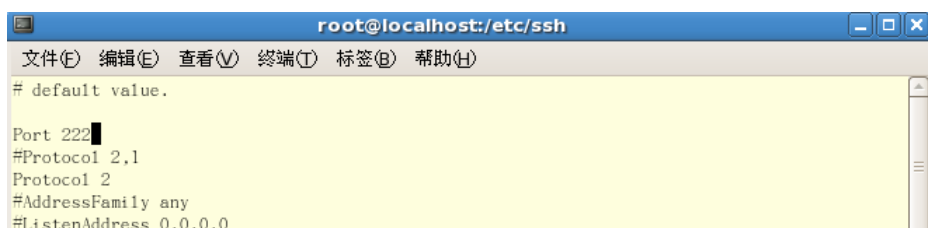
修改 SSH 端口号，可以在不影响到业务应用的情况下，降低计算机的安全隐患，防止他人利用黑客工具远程恶意破解登录密码。

设置要求：建议

设置方法：

```
[root@localhost /]#vi /etc/ssh/sshd_config
```

修改 port 22 为其它端口，以迷惑非法窃探者，如：将 SSH 的端口改为 222



保存修改后，需要重新启动 sshd 服务：

```
[root@localhost /]#service sshd restart
```



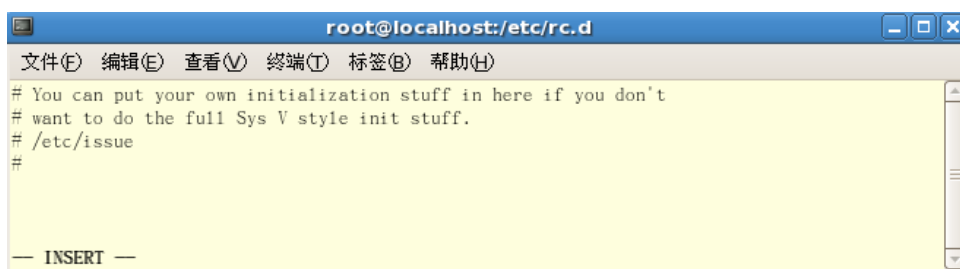
3.3 隐藏系统信息

在缺省情况下,当试图远程登录到 linux 操作系统时,系统缺省会显示该 linux 的名称、版本、内核、计算机名称等信息。删除这些系统提示信息，可以确保他人无法直接获取计算机相关信息，从而进行密码破解和漏洞攻击。

设置要求：建议

设置方法：

编辑/etc/rc.d/rc.local 文件，在下面显示的这些行前加一个#，把输出信息的命令注释掉。



3.4 关闭系统不必要的服务

Linux 操作系统开启时，默认启动了很多的服务，但有许多服务是工作中不需要的，很容易引起安全风险，需要将不必要的服务关闭。/etc/init.d 是操作系统下的进程启动目录，可以使用 chkconfig 命令来关闭系统启动的服务。

查看所有服务启动情况

```
chkconfig --list
```

设置要求：建议

设置方法：

关闭不必要的服务命令：

```
[root@localhost ~]#cd /etc/init.d
[root@localhost init.d]#chkconfig --level 35 apmd off
[root@localhost init.d]#chkconfig --level 35 netfs off
[root@localhost init.d]#chkconfig --level 35 yppasswdd off
[root@localhost init.d]#chkconfig --level 35 ypserv off
[root@localhost init.d]#chkconfig --level 35 dhcpd off
[root@localhost init.d]#chkconfig --level 35 portmap off
[root@localhost init.d]#chkconfig --level 35 lpd off
[root@localhost init.d]#chkconfig --level 35 nfs off
[root@localhost init.d]#chkconfig --level 35 sendmail off
[root@localhost init.d]#chkconfig --level 35 snmpd off
[root@localhost init.d]#chkconfig --level 35 rstatd off
[root@localhost init.d]#chkconfig --level 35 atd off
```

注：等级 0 表示关机；等级 1 表示单用户模式；等级 2 表示无网络连接的多用户命令行模式；等级 3 表示有网络连接的多用户命令行模式；等级 4 表示不可用；等级 5 表示带图形界面的多用户模式；等级 6 表示重新启动。

3.5 设置时钟同步

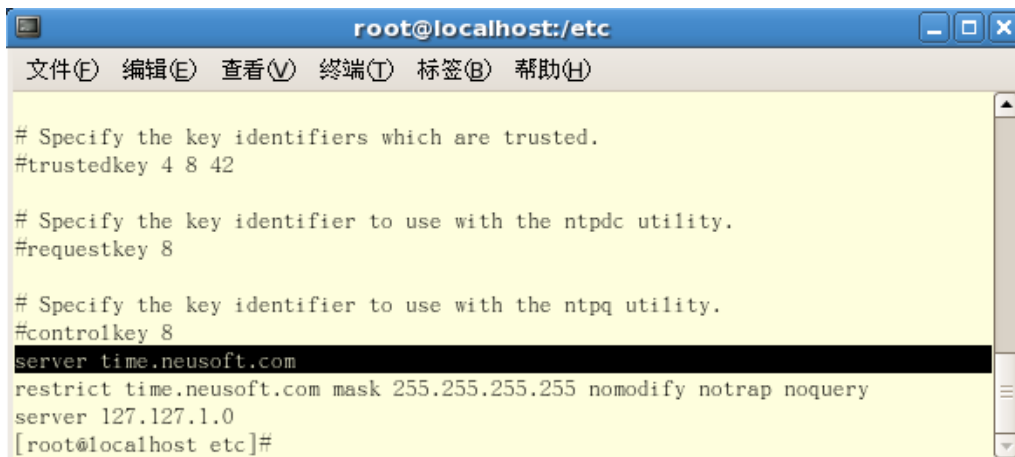
设置时钟同步可以准确记录计算机安全事件发生的时间，从而实现对安全事件进行有效追踪。NTP 的设置文件是/etc/ntp.conf。

设置要求：必须

设置方法：

```
#vi /etc/ntp.conf
```

增加一行：server time.neusoft.com



```
root@localhost:/etc
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)

# Specify the key identifiers which are trusted.
#trustedkey 4 8 42

# Specify the key identifier to use with the ntpdc utility.
#requestkey 8

# Specify the key identifier to use with the ntpq utility.
#controlkey 8
server time.neusoft.com
restrict time.neusoft.com mask 255.255.255.255 nomodify notrap noquery
server 127.127.1.0
[root@localhost etc]#
```

编辑保存后，启动 NTP Server，并且设置其在开机后自动运行

```
#/etc/init.d/ntpd/start
```

```
#chkconfig --level 35 ntpd on
```

4. 日志文件开启设置

确认计算机是否已经开启日志，可以通过查看/etc/syslog.conf 文件中是否存在 authpriv.*，参数进行确认。


设置要求：必须

设置方法：

1、在 CentOS、Red Hat 下的设置方法如下：

```
[root@localhost /]#cat syslog.conf
```

查看 authpriv.*参数，如果不存在或被注释，则增加该参数。



```
root@localhost:/var/log
文件(F) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)

# Don't log private authentication messages!
*.info;mail.none;news.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg *
```

增加后对参数值 secure 文件进行授权：

修改文件为当前时间：

```
[root@localhost /]#touch /var/log/secure
```

将日志文件用户属性设置为 root

```
[root@localhost /]#chown root:root /var/log/secure
```

修改日志文件使用权限

```
[root@localhost /]#chmod 600 /var/log/secure
```



```
root@localhost:/var/log
文件(E) 编辑(E) 查看(V) 终端(T) 标签(B) 帮助(H)
[root@localhost log]# touch secure
[root@localhost log]# chown root:root secure
[root@localhost log]# chmod 600 secure
[root@localhost log]# ls secure -l
-rw----- 1 root root 676 06-11 11:13 secure
[root@localhost log]#
```

2、在 Ubuntu 下的日志缺省即开启状态，并记录在/var/log 目录下，可以通过【系统】-->【系统管理】-->【系统日志查看器】进行查看。

附录：Linux 操作系统终端安全 CheckList

章	节	检查项	关键字	设置要求	检查结果
1. 帐户设置	1.1	设置密码策略	CentOS、Red Hat: /etc/login.defs Ubuntu : /etc/pam.d/common -password	必须	
	1.2	设置屏幕保护程序	CentOS、Red Hat: /etc/profile Ubuntu : 系统--》首选项--》屏幕 保护程序	必须	
	1.3	删除不用的特殊 账户	/etc/passwd userdel	建议	
2. 特权文件 权限管理	2.1	用户名密码文件 权限控制	chattr +i /etc/passwd chattr +i /etc/shadow	必须	
	2.2	/etc/services 文件权限控制	Chattr +i /etc/services	必须	
	2.3	/etc/rc.d/init.d 下 script 文件权 限控制	chmod -R 700 /etc/rc.d/init.d/*	必须	
3. 网络 安全 相关 设置	3.1	限制超级管理员 直接远程登录	/etc/ssh/sshd_config PermitRootLogin no	建议	
	3.2	修改 ssh 端口	port 222	建议	
	3.3	隐藏系统信息	/etc/rc.d/rc.local	建议	
	3.4	关闭系统不必要 的服务	/etc/init.d chkconfig	建议	
	3.5	设置时钟同步	/etc/ntp.conf server time.neusoft.com	必须	
4. 日志 文件	4	日志文件开启设 置	/etc/syslog.conf authpriv.*	必须	