CentOS 系统安全配置

目　录

任务一 系统安全配置

假如你想要搭建一个 Linux 服务器，并且希望可以长期维护的话，就需要考虑安全性能与速度等众多因素。一份正确的 linux 基本安全配置手册就显得格外重要。

1.删除系统特殊的的用户帐号：

禁止所有默认的被操作系统本身启动的且不需要的帐号，当你第一次装上系统时就应该做此检查，Linux 提供了各种帐号，你可能不需要，如果你不需要这个帐号，就移走它，你有的帐号越多，就越容易受到攻击。

#为删除你系统上的用户，用下面的命令：

```
[root@c1gstudio]# userdel username
```

#批量删除方式

#这里删除"adm lp sync shutdown halt mail news uucp operator games gopher ftp "账号

#如果你开着 ftp 等服务可以把 ftp 账号保留下来。

```
for i in adm lp sync shutdown halt mail news uucp ope
rator games gopher ftp ;do userdel $i ;done
```

2.删除系统特殊的组帐号

```
[root@c1gstudio]# groupdel groupname
```

#批量删除方式

```
for i in adm lp mail news uucp games dip pppusers pop
users slipusers ;do groupdel $i ;done
```

3.用户密码设置

安装 linux 时默认的密码最小长度是 5 个字节,但这并不够,要把它设为 8 个字节。修改最短密码长度需要编辑 login.defs 文件#vi /etc/login.defs

```
PASS_MAX_DAYS   99999     ##密码设置最长有效期（默认值）

PASS_MIN_DAYS   0         ##密码设置最短有效期

PASS_MIN_LEN    5         ##设置密码最小长度，将 5 改为 8

PASS_WARN_AGE   7         ##提前多少天警告用户密码即将过期。
```

然后修改 Root 密码

```
#passwd root
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

4.修改自动注销帐号时间

自动注销帐号的登录，在 Linux 系统中 root 账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销 root 账户，那将会带来很大的安全隐患，应该让系统会自动注销。通过修改账户中“TMOUT”参数，可以实现此功能。TMOUT 按秒计算。编辑你的 profile 文件（vi /etc/profile）,在"HISTSIZE="后面加入下面这行：

TMOUT=300

300，表示 300 秒，也就是表示 5 分钟。这样，如果系统中登陆的用户在 5 分钟内都没有动作，那么系统会自动注销这个账户。

5.限制 Shell 命令记录大小

默认情况下，bash shell 会在文件$HOME/.bash_history 中存放多达 500 条命令记录(根据具体的系统不同，默认记录条数不同)。系统中每个用户的主目录下都有一个这样的文件。在此笔者强烈建议限制该文件的大小。

您可以编辑/etc/profile 文件，修改其中的选项如下:

HISTFILESIZE=30 或 HISTSIZE=30

```
#vi /etc/profile
HISTSIZE=30
```

6.注销时删除命令记录

编辑/etc/skel/.bash_logout 文件，增加如下行:

rm -f $HOME/.bash_history

这样，系统中的所有用户在注销时都会删除其命令记录。

如果只需要针对某个特定用户，如 root 用户进行设置，则可只在该用户的主目录下修改/$HOME/.bash_history 文件，增加相同的一行即可。

7.用下面的命令加需要的用户组和用户帐号

```
[root@c1gstudio]# groupadd
```

例如：增加 website 用户组，groupadd website

然后调用 vigr 命令查看已添加的用户组

用下面的命令加需要的用户帐号

[root@c1gstudio]# useradd username -g website //添加用户到 website 组（作为 webserver 的普通管理员，而非 root 管理员）

然后调用 vipw 命令查看已添加的用户

用下面的命令改变用户口令（至少输入 8 位字母和数字组合的密码，并将密码记录于本地机的专门文档中，以防遗忘）

```
[root@c1gstudio]# passwd username
```

8.阻止任何人 su 作为 root

如果你不想任何人能够 su 作为 root,你能编辑/etc/pam.d/su 加下面的行：

```
#vi /etc/pam.d/su
auth sufficient /lib/security/$ISA/pam_rootok.so debug
auth required /lib/security/$ISA/pam_wheel.so group=website
```

意味着仅仅 website 组的用户可以 su 作为 root.

9.修改 ssh 服务的 root 登录权限

修改 ssh 服务配置文件，使的 ssh 服务不允许直接使用 root 用户来登录，这样减少系统被恶意登录攻击的机会。

```
#vi /etc/ssh/sshd_config
PermitRootLogin yes
```

将这行前的＃去掉后，修改为：

```
PermitRootLogin no
```

10.关闭系统不使用的服务：

cd /etc/init.d #进入到系统 init 进程启动目录
在这里有两个方法，可以关闭 init 目录下的服务，

一、将 init 目录下的文件名 mv 成*.old 类的文件名，即修改文件名，作用就是在系统启动的时候找不到这个服务的启动文件。

二、使用 chkconfig 系统命令来关闭系统启动等级的服务。

注：在使用以下任何一种方法时，请先检查需要关闭的服务是否是本服务器特别需要启动支持的服务，以防关闭正常使用的服务。

使用 chkcofig 命令来关闭不使用的系统服务 (level 前面为 2 个减号)要想在修改启动脚本前了解有多少服务正在运行，输入：

```
ps aux | wc -l
```

然后修改启动脚本后，重启系统，再次输入上面的命令，就可计算出减少了多少项服务。越少服务在运行，安全性就越好。另外运行以下命令可以了解还有多少服务在运行：

```
netstat -na --ip
```

以下为手动方式及解释,执行批量方式后不需再执行了

```
chkconfig --level 345 apmd off ##笔记本需要
```

```
chkconfig --level 345 netfs off ## nfs 客户端
```

```
chkconfig --level 345 yppasswdd off ## NIS 服务器，此服务漏洞很多
```

```
chkconfig --level 345 ypserv off ## NIS 服务器，此服务漏洞很多
```

```
chkconfig --level 345 dhcpd off ## dhcp 服务
```

```
chkconfig --level 345 portmap off ##运行 rpc(111 端口)服务必需
```

chkconfig --level 345 lpd off ##打印服务

chkconfig --level 345 nfs off ## NFS 服务器，漏洞极多

chkconfig --level 345 sendmail off ##邮件服务，漏洞极多

chkconfig --level 345 snmpd off ## SNMP，远程用户能从中获得许多系统信息

chkconfig --level 345 rstatd off ##避免运行 r 服务，远程用户可以从中获取很多信息

chkconfig --level 345 atd off ##和 cron 很相似的定时运行程序的服务

注：以上 chkcofig 命令中的 3 和 5 是系统启动的类型，以下为数字代表意思

0:开机(请不要切换到此等级)

1:单人使用者模式的文字界面

2:多人使用者模式的文字界面,不具有网络档案系统(NFS)功能

3:多人使用者模式的文字界面,具有网络档案系统(NFS)功能

4:某些发行版的 linux 使用此等级进入 x windows system

5:某些发行版的 linux 使用此等级进入 x windows system

6:重新启动

如果不指定--level 单用 on 和 off 开关，系统默认只对运行级 3，4，5 有效

chkconfig cups off #打印机

chkconfig bluetooth off # 蓝牙

chkconfig hidd off # 蓝牙

chkconfig ip6tables off # ipv6

chkconfig ipsec off # vpn

chkconfig auditd off #用户空间监控程序

chkconfig autofs off #光盘软盘硬盘等自动加载服务

chkconfig avahi-daemon off #主要用于 Zero Configuration Networking ，一般没什么用建议关闭

chkconfig avahi-dnsconfd off #主要用于 Zero Configuration Networking ,同上,建议关闭

chkconfig cpuspeed off #动态调整 CPU 频率的进程，在服务器系统中这个进程建议关闭

chkconfig isdn off #isdn

chkconfig kudzu off #硬件自动监测服务

chkconfig nfslock off #NFS 文档锁定功能。文档共享支持，无需的能够关了

chkconfig nscd off #负责密码和组的查询，在有 NIS 服务时需要

chkconfig pcscd off #智能卡支持，,如果没有可以关了

chkconfig yum-updatesd off #yum 更新

```
chkconfig acpid off

chkconfig autofs off

chkconfig firstboot off

chkconfig mcstrans off #selinux

chkconfig microcode_ctl off

chkconfig rpcgssd off

chkconfig rpcidmapd off

chkconfig setroubleshoot off

chkconfig xfs off

chkconfig xinetd off

chkconfig messagebus off

chkconfig gpm off #鼠标

chkconfig restorecond off #selinux

chkconfig haldaemon off

chkconfig sysstat off

chkconfig readahead_early off

chkconfig anacron off
```

需要保留的服务

```
crond , irqbalance , microcode_ctl ,network , sshd ,syslog
```

因为有些服务已运行，所以设置完后需重启

```
chkconfig

/*
```

语法：chkconfig [--add][--del][--list][系统服务] 或 chkconfig [--level <等级代号>][系统服务][on/off/reset]

补充说明：这是 Red Hat 公司遵循 GPL 规则所开发的程序，它可查询操作系统在每一个执行等级中会执行哪些系统服务，其中包括各类常驻服务。

参数：

--add　增加所指定的系统服务，让 chkconfig 指令得以管理它，并同时在系统启动的叙述文件内增加相关数据。

--del　删除所指定的系统服务，不再由 chkconfig 指令管理，并同时在系统启动的叙述文件内删除相关数据。

--level<等级代号>　指定读系统服务要在哪一个执行等级中开启或关闭

*/

11.阻止系统响应任何从外部/内部来的 ping 请求

既然没有人能 ping 通你的机器并收到响应，你可以大大增强你的站点的安全性。你可以加下面的一行命令到/etc/rc.d/rc.local，以使每次启动后自动运行。

```
echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all
```

12.修改“/etc/host.conf”文件

“/etc/host.conf”说明了如何解析地址。编辑“/etc/host.conf”文件（vi /etc/host.conf），加入下面这行：

```
# Lookup names via DNS first then fall back to /etc/hosts.
order hosts,bind
# We have machines with multiple IP addresses.
multi on
# Check for IP address spoofing.
nospoof on
```

第一项设置首先通过 DNS 解析 IP 地址，然后通过 hosts 文件解析。第二项设置检测是否“/etc/hosts”文件中的主机是否拥有多个 IP 地址（比如有多个以太口网卡）。第三项设置说明要注意对本机未经许可的电子欺骗。

13.不允许从不同的控制台进行 root 登陆

"/etc/securetty"文件允许你定义 root 用户可以从那个 TTY 设备登陆。你可以编辑"/etc/securetty"文件，再不需要登陆的 TTY 设备前添加“#”标志，来禁止从该 TTY 设备进行 root 登陆。

在/etc/inittab 文件中有如下一段话：

```
# Run gettys in standard runlevels

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty2

#3:2345:respawn:/sbin/mingetty tty3

#4:2345:respawn:/sbin/mingetty tty4

#5:2345:respawn:/sbin/mingetty tty5

#6:2345:respawn:/sbin/mingetty tty6
```

系统默认的可以使用 6 个控制台，即 Alt+F1,Alt+F2...，这里在 3，4，5，6 前面加上“#”，注释该句话，这样现在只有两个控制台可供使用，最好保留两个。然后重新启动 init 进程，改动即可生效！

14.禁止 Control-Alt-Delete 键盘关闭命令

在"/etc/inittab" 文件中注释掉下面这行（使用#）：

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

改为：

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

为了使这项改动起作用，输入下面这个命令：

```
# /sbin/init q
```

15.用 chattr 命令给下面的文件加上不可更改属性。

```
[root@c1gstudio]# chattr +i /etc/passwd

[root@c1gstudio]# chattr +i /etc/shadow

[root@c1gstudio]# chattr +i /etc/group

[root@c1gstudio]# chattr +i /etc/gshadow
```

【注：chattr 是改变文件属性的命令，参数 i 代表不得任意更动文件或目录,此处的 i 为不可修改位(immutable)。查看方法：lsattr /etc/passwd，撤销为 chattr –i /etc/group】

补充说明：这项指令可改变存放在 ext2 文件系统上的文件或目录属性，这些属性共有以下 8 种模式：

a：让文件或目录仅供附加用途。

b：不更新文件或目录的最后存取时间。

c：将文件或目录压缩后存放。

d：将文件或目录排除在倾倒操作之外。

i：不得任意更动文件或目录。

s：保密性删除文件或目录。

S：即时更新文件或目录。

u：预防以外删除。

参数：

-R 递归处理，将指定目录下的所有文件及子目录一并处理。

-v<版本编号> 设置文件或目录版本。

-V 显示指令执行过程。

+<属性> 开启文件或目录的该项属性。

-<属性> 关闭文件或目录的该项属性。

=<属性> 指定文件或目录的该项属性。

16.给系统服务端口列表文件加锁

主要作用：防止未经许可的删除或添加服务

```
chattr +i /etc/services
```

【查看方法：lsattr /etc/ services，撤销为 chattr -i /etc/ services】

17.系统文件权限修改

Linux 文件系统的安全主要是通过设置文件的权限来实现的。每一个 Linux 的文件或目录，都有 3 组属性，分别定义文件或目录的所有者，用户组和其他人的使用权限（只读、可写、可执行、允许 SUID、允许 SGID 等）。特别注意，权限为 SUID 和 SGID 的可执行文件，在程序运行过程中，会给进程赋予所有者的权限，如果被黑客发现并利用就会给系统造成危害。

(1)修改 init 目录文件执行权限：

chmod -R 700 /etc/init.d/* （递归处理，owner 具有 rwx，group 无，others 无）

(2)修改部分系统文件的 SUID 和 SGID 的权限：

```
chmod a-s /usr/bin/chage
chmod a-s /usr/bin/gpasswd
chmod a-s /usr/bin/wall
chmod a-s /usr/bin/chfn
chmod a-s /usr/bin/chsh
chmod a-s /usr/bin/newgrp
chmod a-s /usr/bin/write
chmod a-s /usr/sbin/usernetctl
chmod a-s /usr/sbin/traceroute
chmod a-s /bin/mount
chmod a-s /bin/umount
chmod a-s /sbin/netreport
```

(3)修改系统引导文件

```
chmod 600 /etc/grub.conf
chattr +i /etc/grub.conf
```

【查看方法：lsattr /etc/grub.conf，撤销为 chattr –i /etc/grub.conf】

18.增加 dns

```
#vi /etc/resolv.conf
nameserver 8.8.8.8 #google dns
nameserver 8.8.4.4
```

19.hostname 修改

#注意需先把 mysql、postfix 等服务停了

1.hostname servername

2.vi /etc/sysconfig/network

service network restart

3.vi /etc/hosts

20.selinux 修改

开启 selinux 可以增加安全性，但装软件时可能会遇到一些奇怪问题以下是关闭方法

#vi /etc/selinux/config

改成 disabled

21.关闭 ipv6

```
echo "alias net-pf-10 off" >> /etc/modprobe.conf
echo "alias ipv6 off" >> /etc/modprobe.conf
#vi /etc/sysconfig/network
NETWORKING_IPV6=no
```

重启服务

Service ip6tables stop

Service network restart

关闭自动启动

chkconfig --level 235 ip6tables off

22.linux 调整系统时区/时间的方法

把/usr/share/zoneinfo 里相应的时区与/etc/localtime 做个软 link.比如使用上海时区的时间:ln -s /usr/share/zoneinfo/Asia/Shanghai /etc/localtime 如果要使用 UTC 计时方式,则应在/etc/sysconfig/clock 文件里改 UTC=TRUE 时间的设置:使用 date 命令加 s 参数修改，注意 linux 的时间格式为"月日时分年",也可以只修改时间 date -s 22:30:20,如果修改的是年月日和时间，格式为"月日时分年.秒",2007-03-18 11:01:56 则应写为"date -s 031811012007.56 硬件时间与当前时间更新: hwclock --systohc 如果硬件记时用 UTC,则为 hwclock --systohc --utc

linux 调整系统时区/时间的方法

1) 找到相应的时区文件

```
/usr/share/zoneinfo/Asia/Shanghai
```

用这个文件替换当前的/etc/localtime 文件。
步骤： cp –i /usr/share/zoneinfo/Asia/Shanghai /etc/localtime

选择覆盖

2) 修改/etc/sysconfig/clock 文件，修改为：

```
ZONE="Asia/Shanghai"
UTC=false
ARC=false
```

3)时间设定成 2005 年 8 月 30 日的命令如下：

```
#date -s 08/30/2005
```

将系统时间设定成下午 6 点 40 分 0 秒的命令如下：

```
#date -s 18:40:00
```

4)同步 BIOS 时钟，强制把系统时间写入 CMOS，命令如下：

```
#clock -w
```

23.设置语言

英文语言，中文支持

```
#vi /etc/sysconfig/i18n
LANG="en_US.UTF-8"
SUPPORTED="zh_CN.UTF-8:zh_CN:zh"
SYSFONT="latarcyrheb-sun16"
```

24.tmpwatch 定时清除

假设服务器自定义了 php 的 session 和 upload 目录

```
#vi /etc/cron.daily/tmpwatch
```

在 240 /tmp 前增加

```
-x /tmp/session -x /tmp/upload
#mkdir /tmp/session
#mkdir /tmp/upload
#chown nobody:nobody /tmp/upload
#chmod 0770 /tmp/upload
```

任务二　Web 服务器安全配置

1. 勤打补丁

在 www.apache.org 上的 changelog 中都写着 bug fix 、security bug 的字样。所以，Linux 管理员要经常关注相关网站的缺陷，及时升级系统或者打补丁。使用最高的和最新的安全版本对于加强 Apache 服务器的安全是至关重要的。将你的 openssl 升级打牌 0.9.6e 或更高的版本，伪造的密钥将起不了任何作用，也不能渗透到系统中。一些反病毒程序能够发现并杀死 ssl 病毒，但是蠕虫病毒可能产生变体，从而逃脱反病毒软件的追捕。重启 Apache 可以杀死这样的病毒，但是对于防止将来的感染没有什么积极的作用。

隐藏和伪装 Apache 的版本

通常，软件的漏洞和特定的版本是相关的，因此，版本号对黑客来说是最有价值的东西。

默认情况下，系统会把 Apache 版本模块都显示出来（在 HTTP 返回头中）。如果列举目录的话，会显示域名信息（文件列表正文），去除 Apache 的版本号的方法是修改配置文件 http.conf。找打一下关键字：serversignature 并将其设定为：

Serversignature off

Servertokens prod

然后重启服务器。

通过分析 web 服务器的类型，可以大致推测出操作系统的类型，比如，windows 使用 IIS，而 Linux 下最常见的是 Apache。

默认的 Apache 配置里没有任何信息保护机制，并且允许目录浏览。通过目录浏览，通常可以获得类似“Apache/1.3.27 server at apache.linuxforum.net port 80”或者“apache/2.0.49(unix)PHP/4.38”这类的信息。

通过修改配置文件的 servertokens 参数，可以将 Apache 的相关信息隐藏起来。但是，Red Hat Linux 运行的 Apache 是编译好的程序，提示信息被编译在程序里，要隐藏这些信息需要改动 Apache 的源代码，然后，重新编译安装程序，以替换里面的提示内容。

以 Apache 2.0.50 为例，编辑 ap_release.h 文件，修改“#define AP_SERVER_BASEPRODUCT\"Apache"\为“#define AP_SERVER_BASEPRODUCT\"micosoft-IIS 6.0" \”. 修改完后，重新编译，安装 Apache。

Apache 安装按成后，修改 httpd.conf 配置文件，将“servertokens full”改成“servertokens prod”；将“Serversignature on”改成“Serversignature off”，然后存盘退出。重启服务器后，用工具进行扫面就会发现提示信息中显示的操作系统为 windows。

2. 建立一个安全的目录结构

Apache 服务器包括以下四个目录

- serverroot 保存配置文件（conf 子目录）、二进制文件和其他服务器配置文件。
- documentroot 保存 web 站点内容，包括 HTML 文件和图片等。
- scripalias 保存 CGI 脚本文件。

• customlog 和 errorlog 保存访问日志和错误日志。

建立设定这样一个目录，以上四个主要目录互相独立且不存在父子逻辑关系。

要求：serverroot 目录应该配置成为只能由 root 用户访问，documentroot 应该只能被管理 web 站点内容的用户访问和使用 Apache 服务器的 Apache 用户的 Apache 用户组访问。Scripalias 目录只能由 CGI 开发人员和 Apache 用户访问。只有 root 用户可以访问日志目录。

3. 为 Apache 使用专门的用户和用户组

按照最小特权原则（是保证系统安全的最基本原则之一，它限制了使用者对系统及数据进行存取所需的最小权限，这样，即保证了用户能完成所需的操作，同时也确保非法用户或者异常操作所造成的损失最小化），需要 Apache 分配一个合适的权限，某个目录的权限错误不会影响到其他目录。

必须保证 Apache 使用一个专门的用户和用户组，不要使用系统预置的账号，比如 nobody 用户和 nogroup 用户组。因为只有 root 用户可以运行 Apache，documentroot 应该能够被管理 web 站点内容的用户访问和使用 Apache 服务器的 Apache 用户和用户组访问。所以，如果希望“A”用户在 web 站点发布内容，并且可以以 httpd 身份运行 Apache 服务器，通常可以这样：

```
Groupadd webteam
    Usermod  –G webteam A
    Chown  -R http.webteam  /www/html
    Chmod –R 2570 /www/htdocs
```

有 root 用户访问日志目录，这个目录的权限应设为：

```
Chown –R root .root /etc/logs
Chmod –R 700 /etc/htdcs
```

4. Web 目录的访问策略

对于可以访问的 web 目录，要使用相对保守的途径进行访问，不要让用户查看任何目录索引列表。

（1）禁止使用目录索引

Apache 服务器在接收到用户对一个目录的访问时，会查找 directoryindex 指令指定的目录索引文件，默认情况下该文件是 index.html。如果该文件不存在，那么 Apache 会创建一个动态列表为用户显示该目录的内容。通常这样的设置会暴露 web 站点结构，因此需要修改配置文件来禁止显示动态目录索引。

修改配置文件 httpd.conf：

Options –indexes followsymlinks

Options 指令通知 Apache 禁止使用目录索引。Followsymlinks 表示不允许使用符号链接。

（2）禁止默认访问

一个好的安全策略是要禁止默认访问的存在，只对指定的目录开启访问权限，如果允许访问/var/www/html 目录，则需要以下设置：

Order deny,allow

Allow from all

（3）禁止用户重载

为了禁止用户对目录配置文件（.htaccess）进行重载（修改）可以这样设置：

Allowoverride None

Apache 服务访问控制方法

Apache 的 access.conf 文件负责文件的访问设置，可以实现互联网域名和 IP 地址的访问控制。它包含一些指令，控制允许什么用户访问 Apache 目录，应该把 deny from all 设置成初始化指令，再使用 allow from 指令打开访问权限。如果允许 192.168.1.1 到 192.168.1.254 的主机访问，可以这样设置：

Order deny，allow

Deny from all

Allow　from pair 192.168.1.0/255.255.255.0

5. 配置 Apache 服务器访问日志

（1）相关配置文件说明

一个好的 Linux 管理员会密切关注服务器的日志系统，这些日志可以提供异常访问的线索。Apache 可以记录所有的访问请求，同样，错误的请求也会记录。Apache 配置文件中，需要关系和日志相关的配置文件有两个：

$ customLog /www/logs/access_log common #　记录对 web 站点的每个进入请求#

$ errorLog /www/logs/error_log common #记录产生错误状态的请求

Customlog 用来指示 Apache 的访问日志存放的位置和格式。Errorlog 用来指示 Apache 的错误日志存放的位置。对于不配置虚拟主机的服务器来说，只要直接在 httpd.conf 中查找 customlog 配置进行修改即可。而对于具有多个虚拟服务器的 web 服务器来说，需要分离各个虚拟服务器的访问日志，以便对各个虚拟服务器进行访问统计和分析，因此，需要在虚拟服务器配置中进行独立的日志配置。

（2）Web 服务器日志轮循

Web 服务器日志轮循比较好的方式有三种，第一种是利用 Linux 系统自身的日志文件轮循机制 logrotate。第二种是利用 Apache 自带的日志轮循程序 cronolog。对于大型 web 服务器来说，往往使用负载均衡技术提高 web 站点的服务能力，这样后台有多个服务器提供 web 服务，大大方便了服务器的分布规划和扩展。如果有多个服务器，需要对日志进行合并，统一进行统计分析。因此为了保证统计的精确性，需要严格按照每天的时段来自动生成日志。

（3）使用 logrotate 实现日志轮循

Linux 系统自带的 logrotate 是专门对各种日志文件（syslog、mail）进行轮循的程序。该程序是由运行程序的服务 crond 每天凌晨 4：02 运行的。在/etc/cron.daily 目录下可以看到 logrotate 文件：

#　!/bin/sh/

$　user/sbin/logrotate/etc/logrotate.conf

每天凌晨 crond 都会启动/etc/cron.daily 目录下的 logrotate 脚本来进行日志轮循。

• 使用 rotatelogs 实现日志轮循

Apache 提供一个不把日志直接写入文件，而是通过管道发送给另外一个程序的能力。这样就大大加强了对日志文件的处理能力。这个通过管道得到的程序可以是任意程序，如日志分析器、压缩日志器等。要实现将日志写到管道的操作，只需要将配置文件中日志文件部分的内容替换成“|程序名”即可，例如：

#compressed　logs

$ custmonlog “|/user/bin/gzip –c >>/var/log/access_log.gz” common

这样就可以使用 Apache 服务自带的轮循工具来对日志文件进行轮循。Rotatelogs 基本是按照时间或者大小来控制日志的。

6. Apache 服务器的密码保护

.htaccess 文件是 Apache 服务器上一个配置文件。它是一个文本文件，可以使用任何文本编辑器来进行编写。.htaccess 文件提供了针对目录改变配置的方法，即通过在一个特定的文档目录中放置一个包含一个或多个指令的文件（.htaccess），以作用于此目录及其所有子目录。.htaccess 的功能包括设置网页密码、设置发生错误时出现的文件、改变首页的文件名、禁止读取文件名、重新导向文件、加上 MIME 类别、禁止；列出目录下的文件等。注意，.htaccess 文件是一个完整的文件名。而不是**.htaccess 或者其他格式。另外，上传.htaccess 文件时，必须使用 ASCII 文件格式，并使用 chmod 命令改变权限为 644（RW_R_R_）每一个放置.htaccess 文件的目录和其子目录都会被.htaccess 影响。例如，在/abc/目录下放置了一个.htaccess 文件，那么/abc/和/abc/def 内所有的文件都会被它所影响，这一点是很重要的。

（1）建立.htaccess 文件

首先在设置存取控制的目录（如 htdocs）下建立一个文件，文件名可以自定。一般服务器都会设置成.htpasswd，该文件是不能由 HTTP 读取的。.htpasswd 文件中的每一行代表一个使用者，使用者的名字及经过加密的密码以冒号：分隔。

（2）.htaccess 文件的保护

.htaccess 文件内容如下：

Authtype basic

Authuserfile /usr/home/***/htdocs/.acname1

Authgroupfile /usr/home/***/htdocs/.abcname2

Authname information

<limit get post>

require valid-user

</limit>

其中第二三行的***可以改成个人的 ftp 登录名。.abcname1 和.abcname2 可以是任意文件名，如.htpasswd，但不可以是.htaccess。将.htaccess 上传到要进行木马保护的目录中，.htaccess 文件最后的“require”告诉服务器哪些用户可以进入。Requre valid-user 是指只要是.htpassword 中的任何一个都可以进入。也可以指定名单上某人或者某几个人可以通过。

（3）增加新的许可用户

进入 htdocs 目录，在命令行状态下输入以下命令：

Echo > .abcname1

/var/www/bin/htpasswd.abcname1 abc

这样就可以生成.abcname1 文件

Abc 代表要增加的用户名。输入此命令后，系统会提示输入此用户的密码，这样该用户名就生效了。以后要是再增加用户，运行第二行的命令时换一个用户名即可。如果这个用户存在，则会提示更换密码。

（4）建立允许访问的组

组的设置方法是建立一个名为.htgroup 的文本文件，内容如下：

Groupname1: username1 username2 username3

Groupname2: username1 username3 username4

并在.htaccess 文件中加上“authgroupfile/absolute/path/.htgroup”以 ASCII 模式上传所有文件后，该目录下的文件都会被保护起来。

（5）禁止读取文件

如果将某些内容如密码，存在一个文件中，那么别人只要知道该文件相对应的位置，就可以一目了然。这样很不安全，其实只要在.htaccess 文件中加入以下几行即可：

<file filename.ext>

Order allow ,deny

Deny from all

</files>

总之，通过.htaccess 文件来保护网站更为安全和方便。因为它不像利用程序来实现密码保护时，有可能通过猜测的方法来获得密码。利用.htaccess 文件实现密码保护，一般是很难被破解的。

7. 减少 CGI 和 SSI 风险

CGI 脚本的漏洞已经成为 web 服务器的首要安全隐患，通常是程序编写 CGI 脚本中产生了许多漏洞。控制 CGI 脚本的漏洞除了在编写时要注意输入数据的合法性检查、对系统调用的谨慎使用等因素外，首先使用 CGI 脚本所有者的 uid 是怎样的。这些 CGI 程序即使存在一些漏洞，那么其危害也只是限于该 uid 所能够访问的文件，也就是说，，这样只能伤害用户的文件而不会对整个系统带来危害。

通过安装使用 suEXEC 的应用程序，可以为 Apache 服务提供 CGI 程序的控制支持，可以把 suEXEC 看做一个包装器，在 Apache 接到对 CGI 程序的调用请求后，它将这个嗲用请求交给 suEXEC 来负责完成具体的调用，并且其从 suEXEC 获得返回结果。

suEXEC 能解决一些安全问题，但也会降低服务性能，因为它只能运行在 CGI 版本的 PHP 上，而 CGI 版本比模块版本运行速度慢。原因是模块版本使用了线程，而 CGI 使用的进程。

因此，建议在安全性能要求比较高的时候使用 suEXEC，为此要以牺牲速度为代价，

要减少 SSI 脚本风险，如果使用 EXEC 等 SSI 命令运行外部程序，也会存在类似 CGI 脚本程序的危险，除了内部调试程序时都应当可以使用 option 命令来禁止其使用。

让 Apache 在“监狱”中运行

所谓监狱，是指通过 chroot 机制来更改某个软件运行时所看到的根目录的权限。即将某软件运行限制在指定目录中，保证该软件只能对该目录或其子目录文件有所动作，从而保证整个服务器的安全。这样即使被破坏或入侵，损失也不会很大。

Chroot 是内核中一个系统调用，软件可以通过调用库函数 chroot，来更改某个进程所能看到的根目录，比如，Apache 软件安装在/usr/local/httpd 目录下，以 root 用户启动 Apache，这个 root 权限的父进程会派生多个以 nobody 权限运行的子进程。这样，父进程监听 80 端口的 TCP 数据流，然后根据内部算法将这个请求分配给某个子进程来处理，这样 Apache 子进程所处的目录继承父进程。但是一旦目录权限设定失误，被攻击的 Apache 子进程可以访问/usr/local、/usr 、/tmp 甚至整个系统。因为 Apache 进程所处的根目录仍为整个文件系统的根，如果能使用 chroot 将 Apache 限制在/usr/local/httpd，那么，Apache 所能够存取的文件都是/usr/local/httpd 下的文件，创建 chroot 监狱的作用就是将进程权限限制在文件系统目录树中的某一子树。

8. 使用 SSL 加固 Apache

使用具有 SSL 功能的 web 服务器，可以提高网站的安全性能，SSL 协议工作在 Linux 的 TCP/IP 协议和 HTTP 协议之间。

SSL 使用加密方法来保护 web 服务器和浏览器之间的信息流。SSL 不仅用于加密在互联网上传输的数据流，而且还能提供双方的身份验证，这样就可以安全的在线购物而不必担心别人窃取信用卡的信息。这种特性使得 SSL 适用于那些交换重要信息的地方。

Apache 服务器使用 SSL 通常有两种选择，即主服务器和虚拟 web 站点。

如果使用 Linux 在 3.0~4.0 时，那么可以直接使用命令“rpm –qa|grep mod_ssl”检查，如果没有安装，那么可以以 root 的身份登录，输入命令：

System-config-packages

利用 GUI 套件管理工具的网页服务器，点击“详细信息”，然后勾选“mod_ssl”，提示放入适当的光盘，便可以完成安装工作。

之后，就可以以 https 开头的 URL 来访问安全的页面了。

9. Apache 服务器防范 DoS 攻击

可同通过编辑 httpd.conf 文件的具体参数来防范拒绝服务攻击，或减少伤害程度。

- Timeout 值：设置成 300 或更少
- KeepAlive：设置成 KeepAlive ON
- KeepAliveTimeout 值：设置为 15 或更少
- StartServers：介于 5 和 10 之间
- MinSpareServers 值：介于 5 和 10
- MaxSpareServers 值：为 10 或以下
- MaxKeepAliveRequests 的值：不等于 0
- MaxSpareServers 值：为 10 或以下
- MaxClients 值：256 或更少