8 个步骤把 Linux 优化好

一、最小化原则

（1）安装最小化

（2）开机启动服务最小化

（3）操作最小化

（4）权限最小化

（5）配置参数合理，不要最大化

二、端口优化

远程登录的端口默认是 22 号端口，这是大家都知道的。所以为了安全着想，我们要修改服务器远程连接端口，这样黑客就不好破解你的 linux 服务器。同时，默认登录的用户名为 root，我们可以修改配置，使远程不能使用 root 登录。方法，更改 ssh 服务远程登录的配置。

```
vim /etc/ssh/sshd_config #更改前先备份
Port 22  #修改端口（随便改为其他的，自己记住）
PermitRootLogin yes   #yes 改为 no，不允许 root 登录
PermitEmptyPasswords no #静止空密码登录
UseDns no #不使用 DNS
service sshd restart 重启 ssh 服务
```

临时关闭防火墙

```
service iptables stop
```

永久关闭防火墙

```
chkconfig --level 35 iptables off
```

三、sudo 让普通用户可以拥有定制的 root 权限功能

sudo + 命令 普通用户使用 root 授予普通用户的特定权限

普通用户模式下 sudo-l 查看你拥有什么权限

visudo 修改 sudo 权限（本质是修改 / etc/sudoers)

四、内核的优化

```
net.ipv4.tcp_fin_timeout=2
net.ipv4.tcp_tw_reuse=1
net.ipv4.tcp_tw_recycle=1
net.ipv4.tcp_syncookiies=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
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
```

将以上的配置信息加入文件的最后即可。

五、防火墙的优化

也是以上的文件内，加入以下代码

```
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
```

sysctl -p 使上面加入的代码生效。

六、增加系统安全

隐藏系统版本：

```
[root@cai ~]# >/etc/issue
[root@cai ~]# cat /dev/null
```

锁定关键文件系统：

```
[root@cai ~]# chattr +i /etc/passwd /etc/gshadow /etc/inittab
```

七、linux 优化总结

1）不用 root，添加普通用户，通过 sudo 授权管理（visudo）

2）更改默认的远程连接 ssh 端口及静止 root 远程登录

3）定时更新服务器时间

4）配置 yum 更新源，从国内更新源下载安装 rpm 包（阿里云比 163 要好一点）

5）关闭 selinux 及 iptables（iptables 工作场景如果 wan ip 一般要打开，高开发除外）

6）调整文件描述符数量

7）定时清理 / var/spool/clientmqene / 目录垃圾文件，防止 inodes 节点被沾满（centos6.5 有默认清理不需要设置）

8）精简开机自启动服务（crond，ssh，network，syslog）

9）以上有

八 Linux 系统安装包安装方式

以安装 apache 为例

1）源码编译安装 apache：比较灵活，只编译你想要的参数（中小公司常用）

2）yum 或 rpm 安装：简单，但是不够灵活

3）高级安装结合了编译和 yum、rpm 的双重优点：通过源码（根据自己业务需求）制作符合自己的 rpm 放入自己的 yum 仓库中，然后在全网服务端通过 yum 实现批量部署、管理、升级。