服务器知识手册（四）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

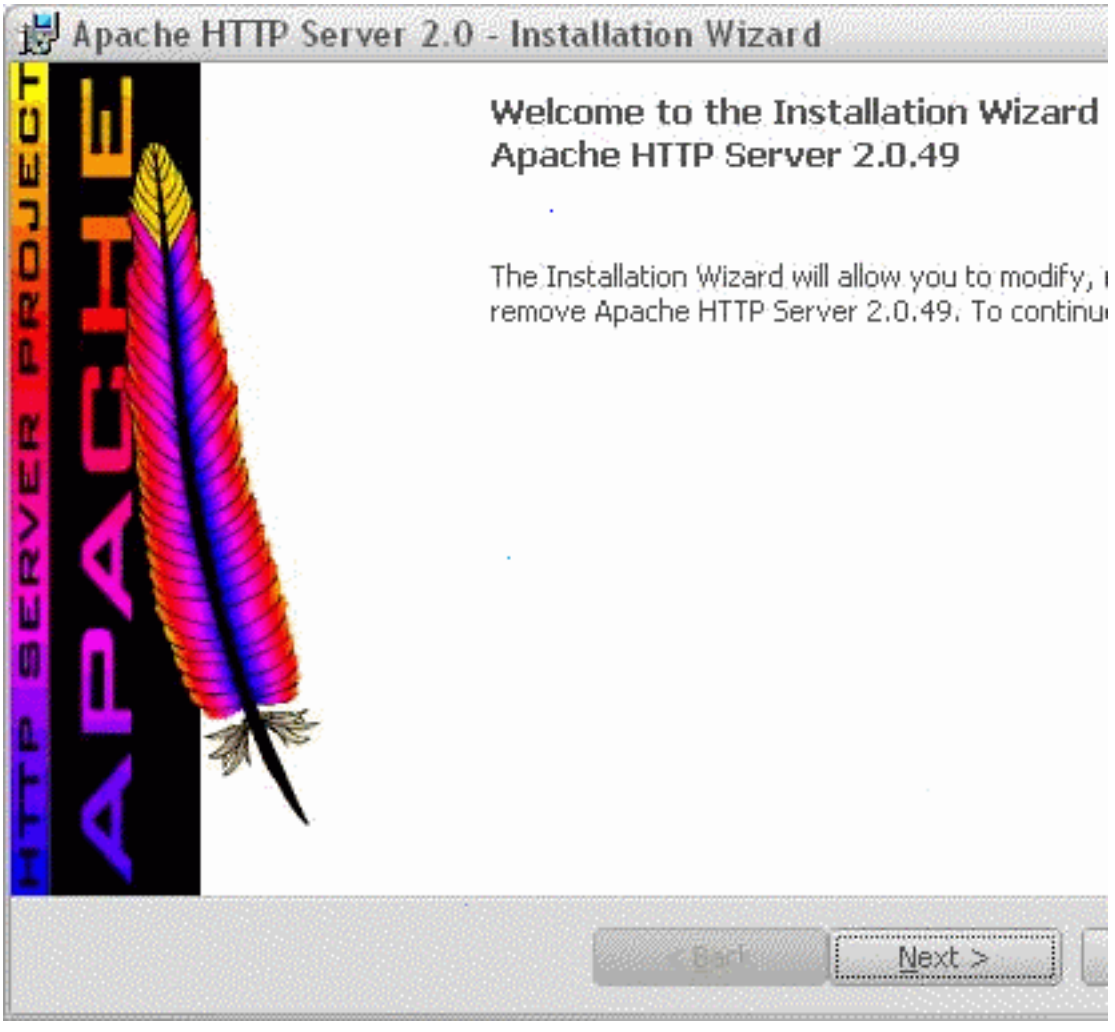
Web 服务器.....1
Apache 服务器的安装教程 1
配置一个安全的 chrootDNS 10
让 DNS 服务器支持泛域名解析 28
基于 Jave 的 Web 服务工作机制 30
解析 Web 接口描述语言 WSDL 47
Web 服务器记录中查找黑客踪迹 64
建立安全的 Web 站点 70
Apache 服务器的安全性及实现 80
基于 Web 的电子商务解决方案 90
用 Win2000 打造内部 Web 站点 97
让 Web 服务走向门户网站 101
在局域网中实现 Web 共享 113
Apache 服务器配置技巧 116
一个安全 WEB 服务器的安装 121

Web 服务器

Apache 服务器的安装教程

为什么选择 Apache？首先，Apache 是免费的，你无需为它交纳任何费用；其次，Apache 是开放源代码的，也许你感觉不到它的好处，但我可以告诉你，一个开放源代码的软件往往能够等到更广泛的支持，可以说，全世界的程序员都在为你服务。而且，它更灵活，使你能够根据自己的需要选用包含特定功能的模块。再给你提供一条消息，现在全世界超过 60%的 HTTP 服务器在使用 Apache。那么你要不要也加入其中呢？

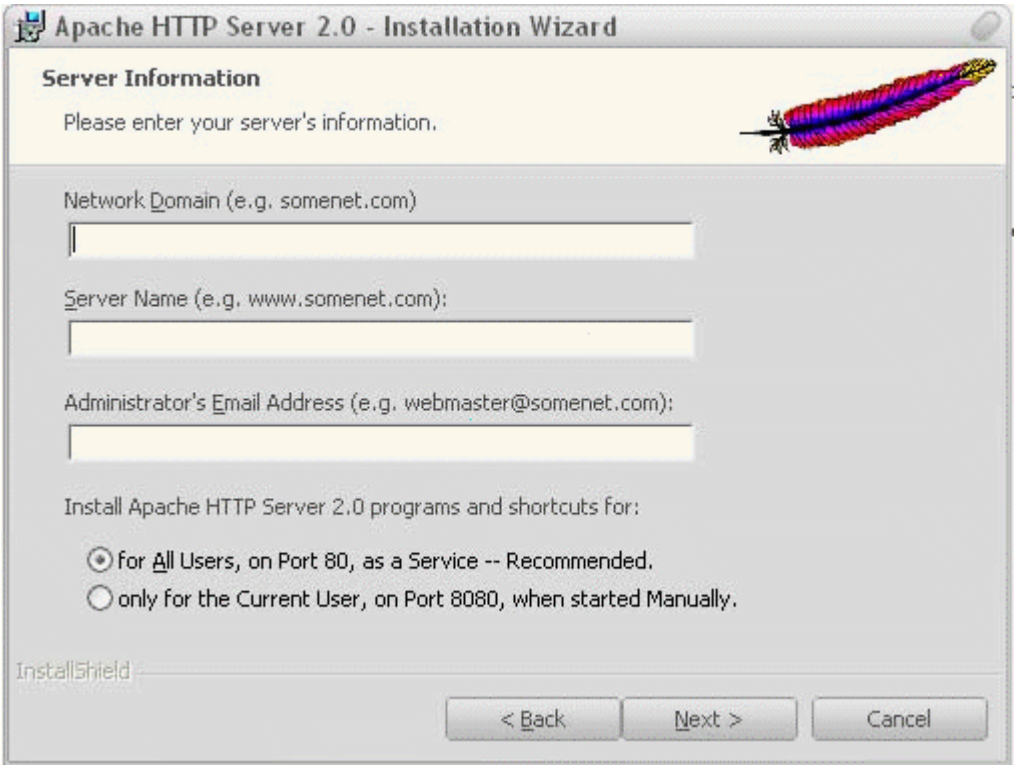
你可以从 Apache 的网站 http://httpd.apache.org/download.cgi 下载 Apache 的安装文件，或者在其他镜像网站获得。现在的最新版本是 2.0.49。



图一：Apache 的安装界面

Apache **的安装非常简单，选择接受许可协议后进入服务器信息配置界面，如下图。第一栏**"NetworkDomain" **域名信息，在这里填入你的服务器的域名，如果你已经申请到域名的话填入你申请的域名，（注意这里要填的是域名，只是你申请到的完整域名的后半部分，不包括**"www"**。如果你申请的是二级域名的话，就是第一个**"."

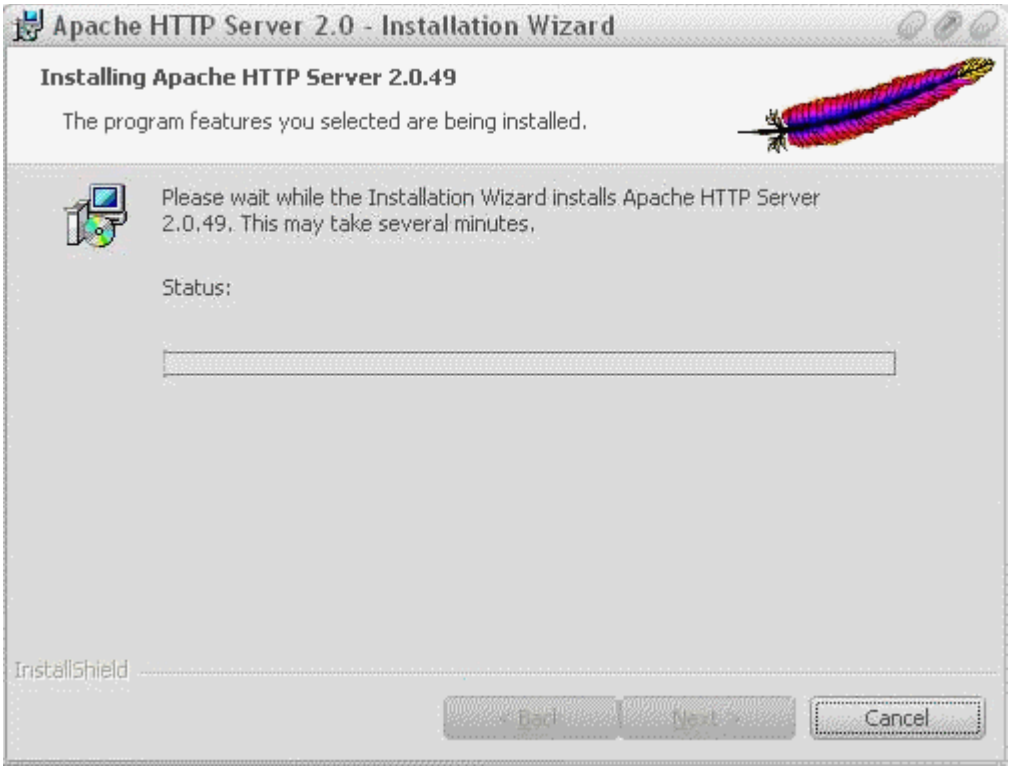
之后的部分）如果还没有的话，把本机的 IP 填上去就行了。下一行是服务器名，填入完整的域名或 IP 地址。再下一栏是管理员 Email 地址。这三项在安装是就必须填写，但是在安装完成后你还可以随时进行修改，所以你不必担心填错了会出问题。最后的选项不用改就可以了。



图二：服务器信息配置界面

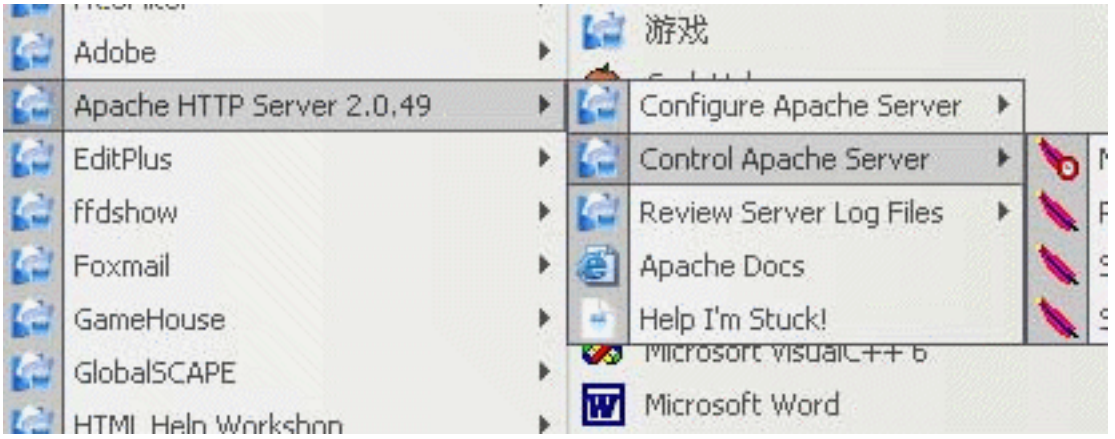
点击"Next"进入下一步。选择"Typical"典型安装，下一步选择安装目录，默认安装目录是系统盘的 ProgramFiles/ApacheGroup 目录。点击"Next"再单击"Install"进行安装。

需要全本请访问 www.ertongbook.com



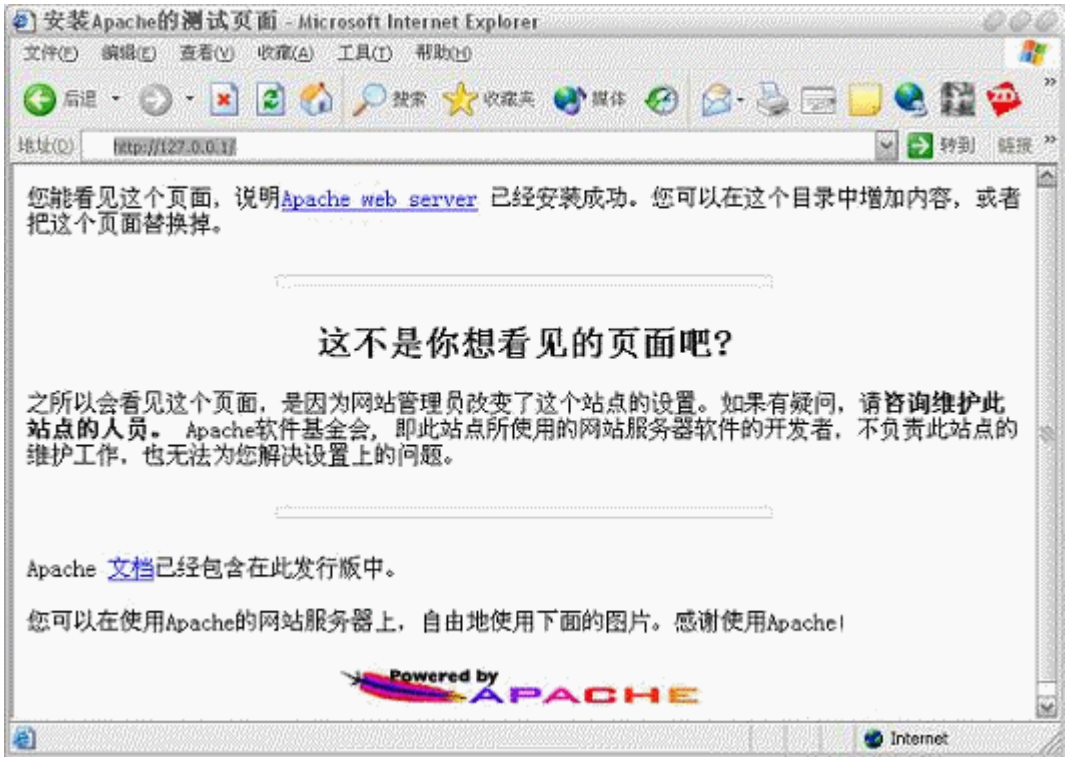
图三：Apache 的安装界面

安装完成后，在开始菜单的 ApacheHTTPServer2.0.49 **菜单中可以看到五个选项，现在点击**"ControlApacheServer"**目录下的**"Start"**启动服务器。可以看到系统状态栏里出现** Apache **的羽毛状图标并带有绿色箭头，说明服务器启动成功。**



图四：Apache 菜单

现在看看我们的成绩吧。打开浏览器，输入 localhost **或者** 127.0.0.1（**这两个都指向本机地址），回车，如果安装正确的话你就能看到** Apache **的测试页面了。（如图五）简单吧，从此，你的电脑也是一台** HTTP **服务器了！**



图五：Apache 的测试页面

也许你会问，这不是我的网站啊，我的网站在哪里呢？别着急，通过下面几步，你就能把你自己精心制作的网站展示给全世界了。

首先单击开始菜单中 Apache **目录下的** "ConfigureApacheServer" **中的** "EdittheApachehttpd.confConfigurationFile"，**打开** Apache **的配置文件。看到了文件是不是有点吓人啊，九百多行的全英文文件。但是不用紧张，我们关心的只是其中的某几行而已。**

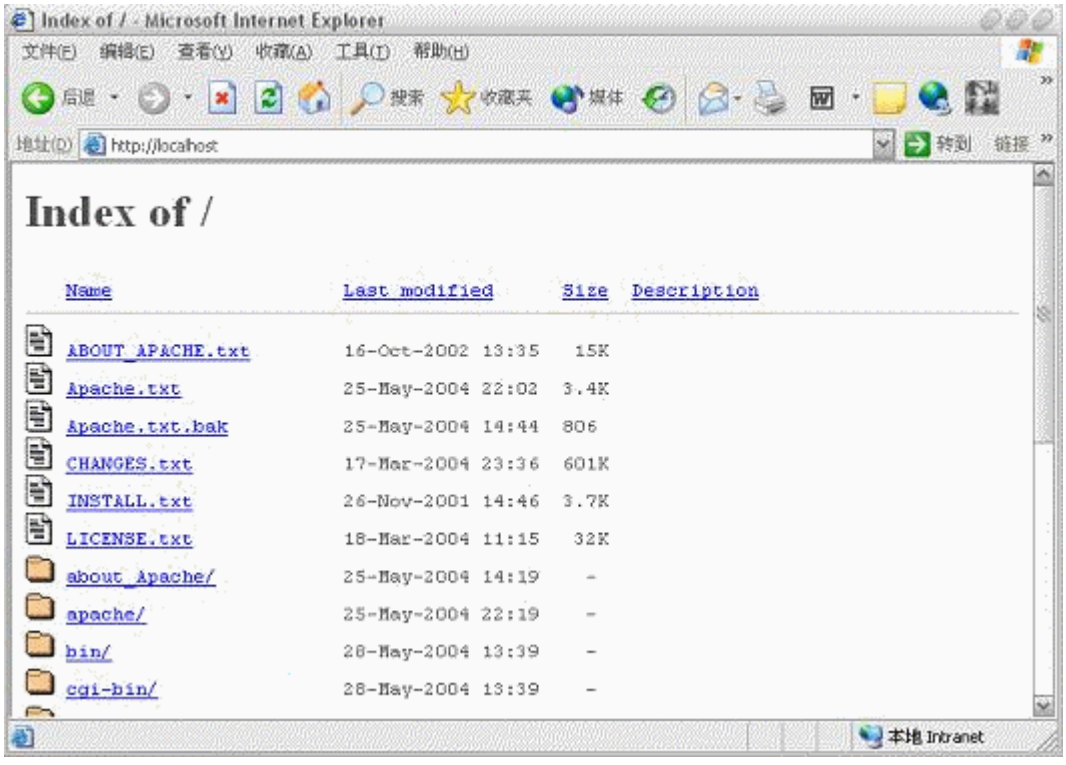
首先，我们要让服务器显示我们自己的内容。找到 "Section1:GlobalEnvironment" **的位置，这一部分是**

Apache 的全局设置。注意到文件的大部分都是以#开头的，程序将略过这些内容，所以，我们也没有必要去研究它们。好了，找到从此开始的没有#的第一行，"ServerRoot……",后面的一部分就是你服务器的根目录了，把它改成你想要的目录就行了，这里建议你使用绝对地址，这样避免一些不必要的问题。需要说明的一点是这里的地址要用斜杠'/'而不是 Windows 文件系统习惯的反斜杠'\'在地址的最后不要加斜杠。

OK，这一部分就这样了，其余的都不用修改。向下继续找到"Section2:'Main'serverconfiguration"如果你觉得这样找起来太麻烦的话，记事本中的查找功能也许能帮你一些忙。（在记事本窗口，按 Ctrl＋F，会弹出查找对话框，将上面的内容复制进去，单击"查找下一个"，记事本将为你找到它所在的那一行）还是只看没有#的行，下面的"ServerAdmin","ServerName"是有关服务器的一些信息，可以暂时不理会。继续向下，找到"DocumentRoot"一行，这后面的地址就是你服务器的文档的地址了，所有对你服务器的访问都将从此地址开始，将这个地址替换成你的网站的文件夹地址，同样注意要用斜杠'/'。

下面是<Directory/>和</Directory>括起来的内容，用于设置你服务器根目录的权限，这里第一个尖括号内的'/'就代表服务器的根目录，无需改动。在向下还是一个尖括号，这是对你刚才设置的文档文件夹的权限设置。将 Directory 后的路径改为你刚才设置的文档文件夹的路径，好了，存盘，单击开始菜单 Apache 文件夹"ControlApacheServer"目录下的"Restart"。再打开浏览器，输入 localhost，回车，是不是有变化了？没变化？

试一下刷新，有了没有？



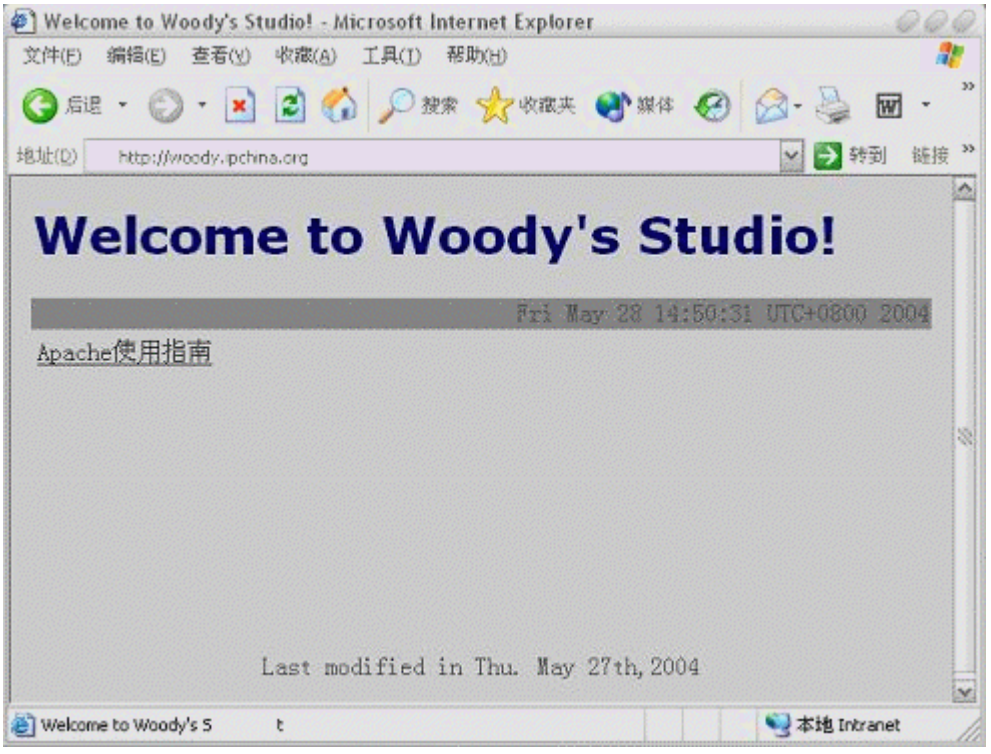
图六：改变设置后服务器的内容

到此为止，你的 HTTP 服务器就可以算是建立起来了。

不过，如果还没有你想要的网页显示出来，也不要着急，我们再回到刚才编辑的文件，找到刚才最后改动的位置，就是<Directory...>，向下看，有一行 options, 应该是"OptionsIndexesFollowSymLinks",在 Indexes 前面加一个减号，这样可以禁止显示目录。现在应该是"Options-IndexesFollowSymLinks"。再下面几行，有一个 DirectoryIndex，后面是服务器默认的主页名称，服务器

将按顺序依次在目录中查找这些文件，并将最先找到的显示出来。你可以把你的网站的默认页面的名字写在这后面。（一般要加一个 index.htm）存盘，Restart。还有什么不满意的吗？

等等，有点不对劲，怎么中文是乱码？这是 Apache 将默认语言设成了西欧语言的原因，还是打开刚才编辑过的文件，找到"AddDefaultCharset"一行，（强烈建议使用记事本的查找工具）将它后面的内容改为 GB2312。存盘，重启服务器。也许你的浏览器这时候看到的还是乱码，那是因为浏览器记住了这个页面的设置，清空浏览器的历史记录和缓存，一切搞定！



图七：完成设置后显示主页

需要全本请访问 www.ertongbook.com

好了，你现在的任务就是申请一个域名，将它指向你主机的 IP，记得上面提到过的"ServerName"吗,改成你申请的域名就可以了。

现在，只要你开着计算机，连着网，你就是因特网上一个 HTTP 服务器的管理员了！

配置一个安全的 chrootDNS

由于天缘最近使用的比较多的是 RedHat 操作系统，而且自己也是在一台 RedHat9 下面配置好 Bind9 的，因此在下面的例子中就以 RedHatAS3 为配置平台进行介绍。天缘所在单位的服务 DNS 是 solaris 操作系统，因此写 shell 的时候，我争取做到对 Solaris 也通用。由于各种因素，我没能亲自在 Solaris 上进行测试。下面的安装过程对 RedHat 和其他 unix 操作系统都没问题，最后附上的自动安装的 shell 脚本我只在 RedHat 下测试成功，对 Solaris 大概也基本上顾及到了，如果大家在实际使用那个脚本的时候发现在 Solaris 下使用存在问题，请及时反馈到此文的留言中，以使我及时更正，方便其他读者朋友。

首先，在开始以前，让我们解释一下标题中出现的 chroot 和 bind 这两个词。先是 chroot，事实上，在很多英文文章中，称它为"jail"（监牢,拘留所,监狱）。那么什么是"Jail"呢？简单来说，就是把一个事物限制到某个范围。大家都知道，有时候由于一个应用程序的 bug、漏洞等问题，会导致该程序被攻击者控制，取得相应用户的权限，进而取得系统管理员级别的权限。例如 Windows 用户对一些 iis 漏洞导致系统最高权限落入攻击者之手

的事情肯定时有耳闻。不管什么程序，都可能有 bug/漏洞，为了防止这样系统中某程序的漏洞导致系统最高权限被攻击者窃取的事件发生，就需要限制该程序的权限。

所谓的限制，并不是不让该程序运行，而是对程序运行时候可以使用的系统资源、用户权限、所在目录进行严格控制。这样，在该程序被他人非法控制后，能具有的权限也相当有限，对系统也不会造成更大的危害。举个形象的例子，架过 ftp 服务器的朋友都知道，用户凭借自己的用户名/密码可以进入到自己的空间内进行上传/下载/添加删除目录等操作权限，而对其他用户的目录和系统的其他目录无法进行任何操作（当然，这些权限是管理者合法授权的），这个就可以看做是一个 Jail，把 ftp 用户限制在自己的目录里。在计算机界术语中，我们把这种对程序的 Jail，特称为”chroot”。因此题目中的 chrootbind,大家可以理解成“权限受严格限制的 bind”。

值得一提的是，chroot 的程序并不能说是程序本身更安全了，它跟没有 chroot 的程序比较，依然有着同样多的 bug/漏洞，依然会被攻击者利用这些 bug/漏洞进行攻击并得逞。那么我们辛苦 chroot 是为了什么呢？是为了把损失降低到最小。打个比方，购买人生保险并不能保你一生平安，但是可以在你遇到麻烦的时候让损失少一些。我们的 chroot 程序也是同样的道理，当攻击者取得了该程序的权限的时候，由于程序本身的权限被严格限制了，因此攻击者无法造成更大的破坏，也无法夺取操作系统的最高权限。DNS 服务器由于是作域名解析之用，需要应付来自各地的很多访问，且一般不限制来访 ip，因此安全隐患和被攻击的可能性相当大。做一个 DNS

服务器的资料网络上到处可寻，而作为网络管理员，我们需要的除了域名解析，还有“安全”（天缘在以前的网管笔记中提到过，“安全是一种意识”，在做任何事情的时候都提醒自己注意安全，是一个称职的网络管理者所应该具备的）！

好了，接下来是第二个名词“Bind”。Bind 是 ISC 公司的软件，而它也是目前世界上使用最普遍、最通用的 DNS 软件，如果说 Apache 和 IIS 是两分 WebServer 天下的话，那么 Bind 不折不扣是 DNSServer 事实上的标准了。

接下来开始步入正题，开始我们的 Bind 安装之旅。chroot 方式安装软件，事实上是把一个软件整体限制到根目录下的一个子目录中。即该软件只在此目录内具有权限，而一旦跳出该目录就无任何权限了。在 Bind8 的时候，想要把 Bind 的全部文件放到一个目录下是一件很麻烦的事，而到了 Bind9 开发公司 ISC 终于顺应民心，不光让 Bind 软件能方便地安装到同一目录下进行权限限制作业，而且连远程控制软件也加上了，真是超值奉送（稍安勿燥，后面会详细介绍）。

向耐心看到这里的朋友致敬，下面我们立即开始正题：

1、安装 Bind9

虽然我所用的 RedHatAS3 中有 rpm 包，但是为了方便其他操作系统的朋友，我们还是从源代码包方式安装。首先从 ISC 公司的主页(http://www.isc.org/products/BIND/)下 Bind9 软件包。

wgetftp://ftp.isc.org/isc/bind9/9.2.3/bind-9.2.3.tar.gz

(我没下最新的，下的是稳定版，您可以根据自己的

需要选取)

接着开始解压缩（为描述简单，以下操作如无特殊声明，都是以 root 权限进行）

tarvzxfbind-9.2.3.tar.gz

卸载 RedHat 中原有的 Bind，一共有三个 rpm 包

rpm-ebindbind-utilscaching-nameserver

进入该目录开始编译安装

./configure--prefix=/usr/local--disable-ipv6--disable-threads

#因为 ipv6 和线程方式我用不到就去掉了，把 Bind9 安装到/usr/local 下

make;makeinstall

到此 Bind9 已经安装完成了，普通的 DNSServer 到此就安装结束了，而对我们的 chroot 而言才刚开始呢。

2、构建 chroot 目录环境

a.创建 Bind 工作目录/chroot/named 及下属工作目录

rm-rf/chroot/named#删除原来的旧目录，之所以加这句是我写 shell 的时候调试方便

mkdir-p/chroot/named

cd/chroot/named

mkdirdev（虚拟/dev）

mkdiretc（虚拟/etc）

mkdirlogs（存放日志）

mkdir-pvar/run（将来会在这下面放一个 named.pid 文件）

b.建立 Bind 的组和用户 named

groupaddnamed

useradd-gnamed-d/chroot/named-s/bin/truenamed

pASswd-lnamed#-l,Lock,表示锁定用户

c.创建虚拟设备（dev），日志记录的时候有的选项可能用到它们。在默认情况下，是使用/dev 目录下的文件，但是由于我们需要把 DNS 限制到一个目录，所以必须完全把/dev 下用到的文件（或者说设备）模拟过来才可以。

ls-lL/dev/zero/dev/null/dev/random

看到类似

crw-rw-rw-1rootroot1,32003-09-15/dev/null

crw-r--r--1rootroot1,82003-09-15/dev/random

crw-rw-rw-1rootroot1,52003-09-15/dev/zero

这样的，将其中的 1,3 这样的数字记录下来，这表示主设备号和次设备号（一般来说主设备号用来区分设备的种类；次设备号则是为了作唯一性区分，标明不同属性——注意，在 unix 系统中是把设备也当作文件来对待的），在 redhat9 下，ls 加不加-L 参数都无所谓，但是在 Solaris 下则一定要加上才可以显示。

mknoddev/nullc13

mknoddev/zeroc15

mknoddev/randomc18

d.复制时钟文件到我们 chroot 的 etc 下，Linux 的时钟设置文件为：/etc/localtime，实际上这个文件是/usr/share/zoneinfo 目录下对应文件的符号连接。（假设我们所处的地区位于上海，那么只要运行以下的命令就可以设置时区了。

ln-sf/usr/share/zoneinfo/ASia/Shanghai/etc/localtime；注意在天缘用的 solaris2.6 中并没有此文件，而是该用/usr/share/lib/zoneinfo/GB）

cp/etc/localtimeetc/

3、创建和设置 BIND9 配置文件

默认情形下，bind 以/etc/named.conf 文件为配置文件。但由于我们这里是要做 chroot 的 DNS，因此需要把 named.conf 放到/chroot/named/conf 下去，然后再做一个符号连接到/etc/named.conf。首先创建并编辑 named.conf 文件（由于介绍 DNS 的文章大多对 named.conf 的配置解释得相当详细，因此我就不一句句解释了，大家结合注释，参考其他文章看看，很容易理解的）

```
vi/chroot/named/etc/named.conf，输入以下内容(由于每个人的配置都不同，所以天缘在这里只列出一个做 cacheonly 的 DNS 的设置)

options{

//注意，由于是 chroot 方式，所以以下的/conf、/var 并不是系统中真正的/conf 和/var 目录，而是指/chroot/named 下的同名目录，此配置文件中所有地方都如此

directory"/conf";//配置文件所在目录

pid-file"/var/run/named.pid";//进程守护文件

statistics-file"/var/run/named.stats";//状态输出文件；在 rndc 中用到

dump-file"/var/run/named.db";//输出数据库文件，在 rndc 中用到

//隐藏真实版本号,我这里写个 4.0 作刻意误导

version"[4.0]";
```

需要全本请访问 www.ertongbook.com