服务器知识手册（七）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

Web 服务器.....1
Apache 服务器高级设置指南 1
BSD 上 Apache 性能的调整 7
学用 Lotus 办公——DominoWeb 服务器应用 12
Web 服务器的安全和攻击防范 15
基于 Apache 的 Web 页面访问权限控制 30
构建安全的 e-commerce 服务器 32
加固 NT 和 IIS 的安全 40
面向对象的 Web 服务器 Zope 53
WEB 服务器配置全攻略 62
Office 和 Web 的整合 70
Web 的公文发布系统 76
Web 数据库技术介绍 84
FTP 服务器.....91
内网 FTP 服务器架设不完全解析 91
Linux 下 FTP 的配置与应用 95
用 tar 包配置高可用性 vsftp 105
架设 FTP 服务器 116
使用 CesarFTP 架设 FTP 服务器 121
快速架设基于宽带的 FTP 服务器 128
ISA 下 FTP 的解决办法 132

Web 服务器

Apache 服务器高级设置指南

目前 WWWServer 软件有许多，能运行在 linux 下的也不少，有 NCSAHTTPdServer、CERNHTTPdServer、pache、NetscapeFastTrackServer、ZeusServer 等。这些软件各有特色：NCSA（美国伊利诺斯大学的国家超级计算应用中心）是 WWWBrowserMosaic 发迹之地，也是 Netscape 公司的安德森成名的地方；CERN（欧洲原子核研究中心）是 WWW 的起源地，1989 年蒂姆·贝纳斯-李正是在这开发成功了世界上第一个 Web 服务器和客户机。这两家推出的 WWWServer 功能齐全，成为同类软件的标准，再加上它们都是 Freeware，因此刚一推出就大受欢迎。前几年，在 linux 下 WWWServer 软件使用最多的是 NCSA 和 CERN，但这一两年来，后起之秀 Apache 却独领风骚，号称"WWWServer 之王"。在最新的 RedHat、Slackware 和 OpenLinux 各版本中都包含了 Apache。

Apache 是在 NCSA 的基础上发展起来的，因此这二者的配置文件十分相似。

一、安装

Apache 的安装十分简单。最好在安装 RedHat 时，选择安装 WebServer，这样即使你对编译操作不熟的话，也能轻轻松松把服务器架设起来。

如果你想亲自编译源文件，那么你已经不是一个初学者，建议你直接去看 How-To 文档或其他资料。打开机器，进入 X-Window 系统后，启动 NetscapeNavigator，敲入本机的 IP 地址，如果出现"Itworked"的欢迎页面，那说明服务器程序工作正常。你可以进行下一步配置工作。在不同的版本下，服务器默认的工作根目录也不一样。RedHat 默认的是/etc/httpd，配置文件在/etc/httpd/conf 目录下，页面文件在/home/httpd 目录下。

二、设置 httpd.conf、srm.conf、access.conf 文件

Apache 安装成功后，在 conf 子目录下有四个文件：httpd.conf、srm.conf、access.conf、magic（请注意：在 www-howto 文档中，说第四个文件是 mime.types，但在实际安装中，在 conf 子目录下是 magic 文件）。httpd.conf 是 Apache 设置文件中的主文件，httpd 程序启动时会先读取 httpd.conf。srm.conf 是数据配置文件，在这个文件中主要设置 WWWServer 读取文件的目录、目录索引时的画面、CGI 执行时的目录等等。access.conf 是负责基本的读取文件控制，限制目录所能执行的功能及访问目录的权限设置。

下面将简单对这三个数据设置文件进行说明。

httpd.conf 文件

TransferLog：

如果你想知道你的网站上哪个页面最受来访者的欢迎，在一段时间内有多少人访问你的站点，你当然可以设置一个计数器，但每页都设计数器，太繁琐而且得到的结果不太可靠。最好的办法是查看相应 log 文件，TransferLog 命令就是指定当浏览器要求服务器传送文件时记录到所设置的文件，可以根据此文件查看有哪些用户

看过哪些 HTML 文件。可用一些程序分析这个文件的数据，得出监测各种有用的数据。默认的访问 log 文件是 logs/access_log。

ErrorLog：

这个命令是指定当 WWWServer 运转过程中发生问题时错误信息存放到哪个文件。默认是 logs/error_log。

VirtualHost：

这个命令是用来设置虚拟主机，即用一台主机执行多个域名的 WWWServer。详细命令使用将在第三部分详细解释。

srm.conf

DocumentRoot：

指定 WWWServer 存放 html 文件的根目录。WWW Server 从硬盘中读取 html 文件传送给浏览器，并不是可从任一个目录中读取文件，而是从一个特定目录中开始读取文件，这个特定的目录就是由 DocumentRoot 命令来指定。redhat5.2 中默认的目录是/home/httpd/html。

如果用户访问 http://www.swm.com.cn/netlife/index.html，此时 WWWServer 并不是从系统的根目录下的 net life 目录中读取 index.html，而是从/home/httpd/html/netlife 目录中读取 index.html 文件。

UserDir：

如果要在 WWWServer 上给一些用户开设空间，搁放个人主页，最好不要把每个人的 html 文件都放到 Doc umentRoot 目录中，用 UserDir 命令可让每个人的页面放置在自己的 home 目录中。默认的目录是 public_html。

如果 UserDir 设置的目录是 public_html，而 Userna me 是 yan，而该 user 的 home 目录是/home/yan，那你访

需要全本请访问 www.ertongbook.com

问 http://www.swm.com.cn/~yan/intr.html 时所看到的 intr.html 文件存放在/home/yan/public_html 中，而不是/home/httpd/html。

access.conf

如果你有些目录只想让某些人访问，或者只允许在特定的目录下允许 CGI 程序，这时就要对 access.conf 进行修改。

Apache 的存取控制方式有两种：一是"整体存取控制"，只通过 access.conf 来控制文件的设置，来限定目录所能执行的功能及存取目录的权限设置。二是"特定目录存取控制"，在特定目录中建立存取设置文件，这个文件名在 srm.conf 中的 AcessFileName 来决定，默认是.htaccess。例如某些目录中的文件只允许某些人访问，那可在该目录下建立.htaccess 文件，当 WWWServer 读取该目录时便会自动读取.htaccess 来决定是否读取执行或要求口令验证。这两种方式所使用的命令几乎相同，而且设置的格式也相同。

Directory：

说明要设置的目录，然后再用命令来设置目录的功能和权限。

Options：

设置目录可以执行哪些功能。有 None、All、ExecCGI、Includes、Indexs、IncludesNoExec、FollowSymlink、SymlinksOwnerMatch 等选项。如果想让某个目录可以执行 CGI 程序，那么应在 Options 命令中加上 ExecCGI 选项。

Require：

设置可以对所指定目录以指定方式来存取的 Users

和 Group。该命令执行后，当读取该目录数据时，系统会要求输入 Username 和 Password。

忠告：修改完设置文件后，不要像在 Windows 工作那样，重启机器使其生效。要记住，你现在 linux 下，使用 linux 的好处之一就是不用再见到 Windows98 那死机时的蓝屏以及不必对配置文件做了一点点修改就无聊而又频繁地重启机器。你的 WWW 服务器任何时候都有很多人在访问，频繁地重启机器将把你的客人赶跑。要学会不重启机器，而是重新启动一个正执行的程序（Process，严格一点应叫做进程、作业）。可以用 kill 命令来使程序重新启动。具体 kill 的使用参见有关文档。

先用 ps 命令查看 httpd 的 pid 号，然后用 kill 命令杀死它，重新启动 httpd。具体命令如下：

```
linux>ps-x
linux>kill-HUP13668
```

（13668 是假设 httpd 的 pid 号，在实际使用中，不同的情况值也不同）

这样就可将 httpd 重新启动，使修改的配置文件生效。看完上面一大堆命令，是不是有些烦，其实你不了解这些命令也无所谓，用系统默认设置也能正常工作。

三、虚拟主机（VirtualHost）的设置

作为系统管理员，若你只有一个 IP 地址，却有好几个域名，又要求访问每个域名都要看到不同的内容，那怎么办？总不至于为每个域名都配上一台服务器吧。这就要采用虚拟主机（VirtualHost）技术，幸好 Apache 就支持这种功能。虚拟主机有两种方式：IP－Based（基于 IP 式）、Name-based（基于域名式）。IP－Based 指的是一个域名对应一个 IP 地址，而 Name-based 指的是多个

域名对应一个 IP 地址。

虚拟主机的设置并不复杂，只要在 httpd.conf 文件中加入相应的命令就行。

下面是一个 Name-based（基于域名式）虚拟主机的 httpd.conf 例子（编者注：因篇幅原因，我们这只给出了相关部分，全文见 www.swm.com.cn）。IP 为：192.168.188.20，两个域名分别是 long.com.cn、short.com.cn。

```
httpd.conf:
NameVirtualHost192.168.188.20
ServerAdminwebmaster@long.com
ServerNamewww.long.com
DocumentRoot/home/httpd/long/html
ErrorLoglogs/error_log
TransferLoglogs/access_log
ServerAdminwebmaster@short.com
ServerNamewww.short.com
DocumentRoot/home/httpd/short/html
ErrorLoglogs/short.com-error_log
TransferLoglogs/short.com-access_log
```

NameVirtualHost 命令指定在哪个 IP 上设置虚拟主机

在 VirtualHost 命令中进行各个主机的具体设置。

ServerAdmin 命令是设定当 WWWServer 执行有问题时，会将 ServerAdmin 所设置的 E-mail 传送到浏览器，让使用者用该 E-mail 与系统管理员联系。

ServerName 命令是设置 WWWServer 的域名。

四、提供个人主页空间、用户 homepage 的设定

经常见到某些网站提供个人主页，显得很神气，其

实你也可以开放你机器上的空间给别人，这很简单就能实现。只要你按照下面的提示对你的 WWW 服务器配置文件进行修改。

给用户开放个人主页空间，一是要确定用户主页的存放目录，二是开放用户主页目录的读取权限。

方法一

你以 root 的身份给用户 chen 开个帐号，系统自动会给 chen 分配一空间/home/user，而后在/home/chen 的目录下建一 public_html 的子目录，子目录的属性要设成 other 可读和可执行的。

接着修改 access.conf。在文件的最后加上以下一段：

```
AllowOverrideNone
orderallow,deny
allowfromall
```

而后，重新运行 httpd，用户就可以通过 http://www.swm.com.cn/~chen/访问 chen 的个人主页。

这种方法的优点是方便，缺点是安全性太差。

方法二

另一种办法是在/home/httpd 目录下为用户 chen 建个目录 chen。修改 srm.conf 中的 UserDir 为/home/httpd/*/html，接着重新运行 httpd 便可以了。

BSD 上 Apache 性能的调整

FreeBSD 是一个性能稳定的免费操作系统，当前很多的商业网站使用在 FreeBSD 上的 Apache 来搭建 Web 服务器平台。在 FreeBSD 上，Apache 的运行性能受到很多因素的影响，本文将介绍如何调整 Apache 的性能，

使你的 Web 服务器运行的更好。

和其他操作系统一样，监听队列（listenqueue）是首要限制条件。下面是 AaronGifford 对 BSDI1.x，2.x 和 FreeBSD2.0（包括旧版本）上的建议。

编辑下面两个文件：

/usr/include/sys/socket.h

/usr/src/sys/sys/socket.h

在每个文件中，搜寻：

/*

*Maximumqueuelengthspecifiablebylisten.

*/

#defineSOMAXCONN5

将 5 修改为任何可以工作的值即可。经测试调整到 32 是不会有什么问题的。修改后，重新编译 kernel 和 ApacheServer 然后重新启动。FreeBSD2.1 在 SOMAXCONN 设置为 32 时工作的非常好。

如果正运行着一个非常繁忙的 BSDApache 服务器并且系统的反应很慢，那么如下工作将很有用处：

运行 vmstat 检查内存使用情况、page/swap 利用率等；

运行 netstat-m 检查 mbuf 使用情况；

运行 fstat 检查文件描述符使用情况；

这些应用提供给你该如何调整 kernel 的信息以及是否应该增加一些内存。下面是一个有很重负载的 BSD 服务器的 kernel 配置参数（实际是 BSDI 服务器，但是与 FreeBSD 和 4.4-Lite 相关）,系统其他参数没有变化。

maxusers256

maxusers 对其他 kernel 参数产生影响：

进程的最大数目

每个用户进程的最大数目

系统打开文件数目限制

每个用户打开文件数目限制

mbufclusters 最大数目

Proc/pgrphash 表大小

这些引申参数的定义公式在/usr/src/sys/conf/param.c 中。这些计算出来的参数部分会被 kernel 配置文建里自己定义的值覆盖：

#Networkoptions.NMBCLUSTERSdefinesthenumberofmbufclustersand

#defaultsto256.Thismachineisaserverthathandleslotsoftraffic,

#sowecrankthatvalue.

optionsNMBCLUSTERS=4096#mbufclustersat4096

#

#Misc.options

#

optionsCHILD_MAX=512#maximumnumberofchildprocesses

optionsOPEN_MAX=512#maximumfds(breaksRPCsvcs)

在许多情况下，NMBCLUSTERS 应该设置的比第一眼看上去需要设置的值大的多。这是因为如果浏览器在传输中中断了连接，与特定连接相关的 socketfd 要在 TIME_WAIT 状态等几分钟才释放，在等待时 mbuf 并没有释放。另外，在服务器的 timeouts 中，一些连接会停留在 FIN_WAIT_2 状态，这个状态不会超时，浏览器又不

需要全本请访问 www.ertongbook.com

会发出最终的 FIN 信号。

关于 mbufclusters 更多的信息（Fromsys/mubf.h）

```
/*
*Mbufsareofasinglesize,MSIZE(machine/machparam.h),which
*includesoverhead.Anmbufmayaddasingle"mbufcluster"ofsize
*MCLBYTES(alsoinmachine/machparam.h),whichhasnoadditionaloverhead
*andisusedinsteadoftheinternaldataarea;thisisdonewhen
*atleastMINCLSIZEofdatamustbestored.
*/
```

CHILD_MAX 和 OPEN_MAX 设置成允许 512 个子进程（与每用户最大进程数不同）和文件描述符。这个值可以根据你的特殊配置进行修改（如果你的模块或 CGI 要打开许多文件时，就设置一个较大的 OPEN_MAX）。如果在同一机器上除 httpd 外还有其他许多工作，就需要设置较大的 NPROC。该例中 NPROC 的值来源于 maxusers。

增大 listen()queue 的大小，需要调整 SOMAXCONN 的值。SOMAXCONN 不是来自于 maxusers 的。所以需要自己增大这个值。目前，这个值在 sys/socket.h 中设置。调整这个参数最好的方式时 run-time（运行时更改），这要比在头文件中修改要好。要在运行时更改，编辑/etc/rc.local，增加：

```
/usr/sbin/sysctl-wkern.somaxconn=256
```

这里使用 256，可以进行更改以适合你的需要。许

多情况下，设置成 128 就可以了。

如果配置的 kernel 使用的资源超过了你可使用的系统 RAM 的数量，系统可能不能启动。保证任何时候有一个可以启动系统的 kernel。使用一些系统工具了解一下你是否需要增加一些内存。

当 OPEN_MAX 大于 256 时，RPC 服务会失败。这是由于原始的 RPC 库的一个函数使用 1byte 保存文件描述符导致的。BSDIrelease2.1 解决了部分问题，但最终的解决需要等待重新设计 RPC。

最后还有一个在 Apache 中对子进程配置的硬限制。对 Apache1.0.5 以后的版本，需要改变 httpd.h 中 HARD _SERVER_LIMIT 的定义并重新编译才能运行超过 150 个 httpd 进程。在 conf/httpd.conf-dist 中：

#Limitontotalnumberofserversrunning,i.e.,limitonthenumber

#ofclientswhocansimultaneouslyconnect---ifthislimitisever

#reached,clientswillbeLOCKEDOUT,soitshouldNOTBESETTOOLOW.

#Itisintendedmainlyasabraketokeeparunawayserverfromtaking

#Unixwithitasitspiralsdown...

MaxClients150

在增大这个值之前，要检查一下你的系统，RAM 扩展，并调整 kernel。

M.Teterin"写到:

对 kernel 和经常使用的应用程序进行优化非常有用。在 AMD-133（486 类 CPU）上重新编译 FreeBSDke

rnel 时加上-m486-fexpensive-optimizations-fomit-frame-pointer-O2 可以减少"unable"errors。

学用 Lotus 办公——DominoWeb 服务器应用

学过 Do-mino 邮件服务配置后，大家对 Domino 服务应该有了更深刻的认识体会。本篇继续介绍 Domino Web 服务器的配置，结合一个 Web 方式办公 BBS 系统的创建要点介绍 DominoWeb 服务器应用。

一、DominoWeb 服务器配置

DominoWeb 服务器的工作方式是：DominoWeb 服务器检查外来请求中的 URL，确定该请求是针对 Domino 数据库中的条目还是文件系统中的 HTML 文件。如果是 HTML 文件，Domino 服务器将同其他 Web 服务器一样，为 Web 客户机提供文件服务。如果请求的是 Domino 数据库中的内容，Domino 将与数据库交互作用，为 Web 客户机处理消息，或者将信息从 Web 客户机存入数据库。

Domino 支持 URL 扩展，该扩展使得 Web 客户机能够使用 Domino 功能。例如：Http·//www．kingstone．com/hello．nsf ？OpenDatabase 可以用于打开 Kingstone．com 站点上的数据库等。

配置 DominoWeb 服务器步骤如下：

1．首先启动 DominoAdministrator，在 DominoAdministrator 中，单击“配置”附签，选择“服务器”，然后打开“服务器”文档。

2．选择“端口·Internet 端口·Web 附签”，然后填入 TCP/IP 端口号，如果你的 NT 装有 IIS，建议选择端口

号不要和 IIS 相同，如 8081 等。

3．选择“Internet 协议·HTTP 附签”，然后在 DNS 查询项中选择“禁用”，这样可以改善 Domino 服务器性能。接着启用“联编到主机名”，在“主机名”中输入别名，这样可允许用户使用不同于 Domino 服务器名的别名来访问 Web 服务器。最后在“允许 HTTP 客户浏览数据库”一栏中选择“是”，允许 Web 用户使用“？OpenServer”命令显示服务器上的数据库列表。

4．选择“Internet 协议·DominoWeb 引擎”，然后选择“启用”，使搜索站点者可以访问本站点。

5．最后在 NT 控制台中输入命令“tell httprestart”，重新启动 http 服务，使得修改得以生效。

6．其它 DominoWeb 服务器控制操作：

(1)手动启动 Web 服务器，在控制台中输入“loadhttp”。

(2)启动 Domino 时自动启动 Web 服务器，只需在 NOTES．INI 中编辑 ServerTasks，使其包括 http 命令。

(3)关闭 Web 服务器可以在控制台中输入“tellhttpquit”。

二、DominoWeb 服务器应用

DominoWeb 服务器较之 IIS 系统的优点在于：DominoWeb 服务器包含了数据库、页面、应用程序，同时提供了众多的模板，使得用户可以迅速完成一个含数据库功能复杂站点的建设。以下结合一个 Web 方式 BBS 系统的创建要点介绍 DominoWeb 服务器的应用构建要点。

1．建立 BBS 组件

(1)数据库：向 HTTP 服务器显示一个 Notes 数据库来组织、保存数据和设计元素以供 Web 用户查看。

(2)表单：为用户提供向数据库中输入新信息和查看现有信息的框架。

(3)文档：保存数据库数据的单个 W-eb 页面。

(4)域：文档中的域包含了一部分信息，例如人名、注释、号码、日期或计算结果。

(5)导航器：作为图像映像出现在 W-eb 页面上，导航器提供了图形化的方式来让用户查找文档或在打开的数据库中执行操作而不用打开视图。

(6)主页面：可使用 AboutDatabase 文档或表单、导航器制作，也可直接用 HTML 文件。

(7)链接：Domino 支持数据库链接、文档链接、视图链接以及 URL 链接。

(8)公式与 LotusScript：大部分公式、@函数和 Scri pt 都可在 Web 上应用。

(9)代理和动作：代理通常由动作触发或在表单提交时被触发，动作用于链接 Notes 对象和触发代理建立。

2．规划 BBS 站点

Web 站点是组织起来的信息集合，这些信息保存在 Domino 服务器上的一个或多个数据库中。规划 Web 站点时，要考虑到构建站点的数据库、视图、表单和导航器的类型和存取级别(使用读者、作者、编辑者、管理者四种权限等级)。

3．实现 BBS 站点

Domino 自动地将所有的设计元素和文档转换成 We b 页面。因此，创建了带有视图、导航器、表单和文档的数据库，就相当于创建了 Web 页面。

(1)主页数据库：站点主页文档，包括站点介绍以及其他有关数据库视图、文档或导航器的链接。

(2)注册区数据库：注册表单，更改个人信息表单。

(3)讨论区数据库：主文档表单，答复文档表单，答复的答复文档表单，以及按作者、按日期、按主题的视图各一张，按作者、按日期、按主题的导航器各一个。

(4)精华区数据库：主文档表单，按作者、按日期、按主题的视图各一张，按作者、按日期、按主题的导航器各一个。

Web 服务器的安全和攻击防范

分析一下最近几个月信用卡号码被盗和网站被黑所显示的种种安全问题，可以很清楚地看出，许多 Web 应用都是凑合着运行，很少有人关注其安全问题或作出安全规划。那么，造成服务器缺乏安全保障的常见原因有哪些？如何防范这些不安全因素？作为客户或者最终用户，如何才能信任某个服务器符合了基本的安全需求？

对于以往安全事故的分析表明，大多数安全问题都属于下面三种类型之一：

服务器向公众提供了不应该提供的服务。

服务器把本应私有的数据放到了可公开访问的区域。

服务器信赖了来自不可信赖数据源的数据。

提供不应该提供的服务

显然，许多服务器管理员从来没有从另一个角度来看看他们的服务器，例如使用端口扫描程序。如果他们曾经这样做了，就不会在自己的系统上运行那么多的服务，而这些服务原本无需在正式提供 Web 服务的机器上运行，或者这些服务原本无需面向公众开放。

需要全本请访问 www.ertongbook.com