基于Linux的网站解决方案

那景芳 (中国矿业大学北京校区 100083)

摘要：本文提出了一种基于Linux的网站建设方案，利用Red Hat Linux建设Internet/Intranet服务器和防火墙，并说明了设置防火墙和各种服务器的主要配置文件，同时详细解释了配置文件中的重要参数和命令。

关键词：Linux操作系统 服务器 防火墙 局域网 互联网

1 引言

由于计算机的发展趋势及Linux操作系统的诸多优点，使其成为我们所建网站的首选服务器操作系统。在建站过程中我们逐渐体会到Linux系统的强大和健壮。根据建站的体会，在此提出一种全面基于Linux的网站解决方案。网站的示意图如图1所示，图中的服务器是指软件，所提到的各种服务器可在一台计算机上配置，也可分别配置于多台计算机上；终端指以Windows或Linux为操作系统的工作站，现以WIN98工作站为例进行讨论。该方案中，防火墙及各种服务器均由Linux系统来实现。

内部局域网是基于以太网(Ethernet)的Intranet。每台服务器和终端上都安装有以太网卡，由网线连接到交换机的端口。而作为防火墙的计算机上应至少有两块网卡，一块通过网线与路由器相连，另一块通过网线与交换机相连。局域网通过路由器连接到Internet上。

2 linux的安装

以Red Hat Linux 6.2为例。Linux有多种安装方法：从CD-ROM安装，从NFS安装，从FTP安装，从硬盘安装等。可以在一台计算机上安装单一的Linux系统，也可以采取多操作系统的安装方法，它可与Windows 98或95、Windows 2000、Windows NT等操作系统同存于一台机器上。

具体的安装过程在这里不详细说明，只讨论两个问题。在安装过程中，系统会检测到网卡，可以进行网络设置，如主机名称、域名、主机IP地址、子网掩码等。当要求选择安装组件时，可以选择所要安装的各种服务器组件，若以后需增加其他服务，可以手工安装相关组件；或者，选择安装全部组件，在安装完毕后，手工设置服务器，停止不需要的服务。现假定Red Hat Linux系统已经安装在机器上。

3 内部局域网的建设

3.1 配置TCP/IP

服务器网卡参数的设置在安装过程中已经完成。需要确定WIN98工作站上是否安装了TCP/IP协议，其安装过程是，打开控制面板→网络→配置→添加→协议，这时会出现"选择网络协议"选择框，找到TCP/IP协议并安装。然后进行属性设置，如IP地址、DNS参数(参数的设置要参考上述服务器的网络参数)。

3.2 /etc/hosts文件

/etc/hosts中定义了主机IP地址与主机名称之间的映像信息。如果局域网中没有配置DNS服务器就必须在/etc/hosts中明确指定主机IP地址与名称之间的对应关系。实际上，在比较小型的局域网中，完全可以不设置DNS服务器，而直接使用/etc/hosts文件进行域名解析。

/etc/hosts文件一般以"localhost"定义开始，然后是本机的IP地址和主机名称。

下面是一个示例：

```
127.0.0.1 localhost.localdomain localhost
10.1.18.1 e8s.com e8s
```

其中，e8s.com为域名，e8s为主机名称。

3.3 Samba服务器

Samba程序让Linux服务器懂得SMB (Server Messages Block)协议，从而实现在Linux服务器和Windows 98工作站之间的打印共享和文件共享。

配置Samba服务器所需的文件是/etc/smb.conf，文件中设定了系统与其他机器共享的资源以及访问权限。文件由若干部分组成，每部分定义一项服务，其中包括一些属性。下面是一个简单的smb.conf例子：

```
[global]
printcap name = /etc/printcap
load printers = yes
printing = bsd
security = share
[homes]
comment = Home Directories
browseable = no
writable = yes
[printers]
```

Website solution base on Linux

comment = All Printers

path = /var/spool/samba

browseable = no

guest ok = yes

writable = no

printable = yes

[globle] 部分定义可用于其他配置部分的Samba参数；[homes] 部分允许设置供从Windows系统访问的主目录；[printers] 部分定义了打印服务。

4 构建Internet服务器

4.1 Web服务器

Apache是Red Hat Linux默认安装的Web服务器。Apache服务器软件的配置文件主要有：/etc/httpd/conf目录下的access.conf、httpd.conf、srm.conf及/etc/mime.types(记录Apache服务器所能识别的MIME格式)。

(1) 设置httpd.conf。httpd.conf主要用来设置与服务器有关的系统及基本信息。可修改其中的一些配置，以使其适合你的站点。一般情况下，httpd.conf中的大部分缺省值可保留：

只需改动以下几项内容：

· ServerType

该命令指定Web服务器运行的方法。可以使用单机(standalone)或者inetd方法运行服务器。单机方式在性能上更高效。

· User&Group

当主要的Web服务器进程为了完成一个请求而装入一个子服务器进程的时候，它根据这些命令设置的值改变子服务器进程的用户ID (UID)和组ID (GID)。缺省值均为nobody，这是出于安全性的选择。应参考/etc/group和/etc/passwd文件来决定这些设定。

· ServerAdmin

该命令设置Web管理员的地址，地址形式如webmaster@domain.com。

· ServerName

该命令设置服务器的主机名，可以输入类似www.yourcompany.com的主机名称。

(2) 设置srm.conf。srm.conf是资源配置文件，主要用于文件资源的设定，用来说明服务器应提供什么样的资源，以及在什么地方和提供方法。主要设置命令如下：

· DocumentRoot

该命令设置所有Apache文档的根目录，可将被访问的文档文件存放在该命令后的目录中。

· UserDir

该命令使Apache知道哪个目录作为系统上用户的个人目录。它是相对本地用户主目录的一个目录。若不希望使用用户支持的目录则需指定：UserDir DISABLED。

· DirectoryIndex

此命令指定当URL中没有明确指出文档名称时，服务器将返回目录中的哪个文档，其参数可为多个文件名，按先后顺序排定优先级。

(3) 设置access.conf。access.conf是全局的访问控制文件，用于设置系统中的存取方式和环境，用该文件对Web网站上的对象例如文件、目录和脚本设置访问权限。文件结构比较严紧，内容被包括在<Directory></Directory>这两个标记之间。

4.2 动态网页的实现

为了实现动态网页，选用了PHP脚本语言，并安装了Mysql数据库，利用PHP应用程序访问Mysql数据库。PHP作为一种服务器端HTML嵌入式脚本描述语言，其特色在于能够很方便的实现在互联网网页上对数据库的操作，而且它是免费软件。Mysql是一个多用户、多线程的SQL数据库管理系统，它支持Linux、Unix等多种操作系统，其特点是速度快、健壮和容易使用。Apache + PHP + Mysql是非常好的组合，具有安装简单，使用方便，性能稳定，速度快，成本低的特点。

4.3 DNS服务器

域名服务(DNS)是Internet的核心，简单地说，它是把Internet主机名称解析为IP地址的系统。Linux内置了DNS服务器，启动Linux，看到named启动就说明DNS服务器已经开始工作。现在假定要建立一个名为e8s.com的域。

所需配置文件有：/etc/named.conf；/etc/hosts；/etc/resolv.conf；/var/named/e8s.db；/var/named/db.e8s。

(1) /etc/named.conf是主配置文件，定义了域数据库信息的基本参数和源点。该文件中包含若干个域，文件示例如下：

options {


```
directory "/var/named";
#定义了named要读写文件的路径
};
zone "." {
type hint;
#表明在启动时被用来初始化域名服务器的文件
file "named.ca";
#指定所要读取的文件名
};
zone "0.0.127.in-addr.arpa" {
type master;
#表明服务器是主域名服务器
file "named.local";
};
zone "18.1.10.in-addr.arpa" {
# 定义被解释网段
type master;
file "db.e8s";
};
zone "e8s.com.cn" {
# 定义被解释的域名
type master;
file "e8s.db";
};
```

其中第三个区域声明把域名服务器设置为10.1.18.0网络的主要名字服务器，即所有对该网络的IP到主机名的翻译都由该名字服务器处理。第四个区域(zone)声明把域名服务器设置为e8s.com域的主要授权域名服务器，即所有对e8s.com的主机名到IP的翻译都由该域名服务器处理。

(2) 其他文件的说明：

/var/named/e8s.db：正向解析配置文件，即实现域名到IP的对应。

/var/named/db.e8s：DNS反向解析配置文件，即实现IP地址到域名的映射。

/etc/hosts：实现网上其他主要计算机的映射，它通常被当作DNS的备份。

/etc/resolv.conf：指定域名服务器的IP和搜索顺序。

4.4 E-mail服务器

Sendmail是Red Hat Linux默认安装的邮件服务器。客户和服务器间的通信协议是邮局协议(POP)和简单邮件传输协议(SMTP)。

(1) 配置邮件服务器的第一步，加入邮件交换(MX)记录，它是用来标明SMTP邮件服务器资源的，该资源在域的DNS配置文件上设置，其格式为：

IN MX preference-value mail-server-hostname.

preference-value (优先级) 是正整数，mail-server-hostname为邮件服务器的名称。

(2) 对配置文件进行设置，这些文件为/etc/sendmail.cf、/etc/sendmail.cw和/etc/mail/*。

/etc/sendmail.cf是主配置文件，控制sendmail运行时的配置。完整的sendmail配置应该包括7部分：Local Info (本地信息)、Options (选项)、Message Precedence (消息的优先级)、Trusted Users (信任用户)、Format of Headers (头格式)、Rewriting Rules (改写规则)、Mailer Definition (邮寄者说明)。上述内容可根据文件中的注释，进行设置。管理员需要执行touch命令来创建库文件，然后重新启动sendmail。sendmail是根据这些库文件运行的。

/etc/sendmail.cw中必须列出接收mail所有主机名或域名。配置文件中的FEATURE指出了sendmail从/etc/sendmail.cw可读取的所有主机名或域名。

在/etc/mail/目录下，有若干配置文件：利用access限制访问sendmail服务器；利用aliases产生用户的别名；利用domaintable映射域；利用mailtable改变域的邮件路由；利用relay-domains建立邮件中继。

(3) POP服务器设置。在/etc/services文件中必须进行如下设置：

pop-3　110/tcp

在/etc/inetd.conf文件中有如下设置：

pop-3 stream　tcp　nowait　root /usr/sbin/tcpdipop3d

4.5 FTP服务器

FTP(文件传送协议)提供了文件传送的基本服务，FTP可以减少甚至消除在不同操作系统之间处理文件的不兼容性。一个FTP服务器进程可以同时为多个客户进程提供服务。

配置文件包括/etc目录下的services、inetd.conf、ftpaccess、ftpconversions、ftphosts和ftpusers。

(1) 在/etc/services文件中必须进行如下设置：

ftp-data 20/tcp

ftp　21/tcp

在/etc/inetd.conf文件中有如下设置：

ftp stream　tcp　nowait　root　/usr/sbin/tcpd in.ftpd -l -a

(2) /etc/ftpaccess是FTP服务器的主要配置文件。该文件在下列格式中包括配置信息。

keyword　[one or more options]

该文件包含如下几类属性：guestuser(FTP用户)、class(用户类别)、loginfails(允许输错密码次数)、message(执行指定指令时的显示信息)、shutdown(设置关闭时间文件)、passwd-check(设定匿名用户密码使用方式)、limit(允许连接人数上限)、alias(目录别名)。

(3) /etc/ftpconversions：保存FTP服务器的转换数据库。

/etc/ftphosts：用来控制来自各种主机的特定账号对FTP的访问。

/etc/ftpusers：FTP用户黑名单，为了安全考虑，需要禁止某些用户使用FTP。

5 包过滤防火墙

在Red Hat Linux中使用ipchains来实现数据包过滤的功能。网络中数据都是以数据包形式存在，每个数据包都有标头(header)和数据(body)两部分，标头部分指明了该数据包的源地址、目的地址和数据包类型。Ipchains是运行于主机中的数据包过滤软件，负责检查通过该主机的数据包标头，并决定对数据包进行何种处理。它主要定义了对数据包进行过滤的一些规则，其他功能还包括数据包伪装和透明代理。

系统中有四种chains：IP input chains(接收的外部数据包)；IP output chains(发送到外部的数据包)；IP forward chains(经过本地主机的数据包)；用户自定义的chains。

每种chains都有自己的规则集合，它们定义了对各种数据包所进行的操作。每个规则都需要指定对数据包的处理方法，被称为"策略"，包括ACCEPT(允许通过)、DENY(拒绝通过)、REJECT(不接受且返回通知信息)、MASQ(IP伪装)和REDIRECT(重新导向)，以下是几条ipchains的命令示例：

/sbin/ipchains -F forward

#-F：刷新，该命令实现了forward chains的刷新

/sbin/ipchains -P input ACCEPT

#-P：修改策略，该命令将input chains的策略改为接收

/sbin/ipchains -A output -j DENY -i eth0 -s 127.0.0.0/8

#－A：向某个chains中添加一个规则

#－j：指明对数据包的操作方式

#－i：指明主机的特定端口，可以是一个网络接口

#－s：指明源IP地址

#该命令禁止源地址为loopback接口的输出数据包

/sbin/ipchains -A forward -j MASQ -i eth0 -s 192.168.0.0/24

#该命令实现了IP伪装，它将从网络192.168.0.0/24中输出的数据包标头部分的源地址重写为外部网络接口的IP地址，即eth0的IP地址；当eth0接收到外部数据包时，再次重写数据包标头目的地址部分，把目的地址修改为192.168.0.*，再将数据包发送给目的主机。

配置防火墙需要做以下几步：在/etc/rc.d/目录下用touch命令建立firewall文件；执行chmod u+x firewll以更改文件属性；编辑/etc/rc.d/rc.local文件，在末尾加上/etc/rc.d/firewall以确保开机时能自动执行该脚本；使用vi或其他编辑器对文件firewall进行编辑，在该文件中写入对各种数据包的过滤方法，其命令行的格式如上述示例所示。

参考文献

1 [美] Mohammed J. Kabir. Red Hat Linux 6服务器使用指南，北京电子工业出版社，2000。

2 裴植、肖薇，红旗Red Hat Linux开发及网络应用，人民邮电出版社，2001。

3 网胜工作室，PHP4.0程序设计，北京希望电子出版社，2000。

4 夏阳、刘广钟，Apache在Red Hat Linux上建立与运行的关键技术，计算机工程，2000，26(10)。