

# 设计分析书

## 一. 基本服务器的配置:

### (一) DNS 服务器的构建:

#### 1. DNS 简介:

域名服务 (DNS) 是一种重要的网络服务, 是一种组织成域层次结构的计算机和网络服务命名系统。通过 DNS 服务可以将域名解析为 IP 地址, 从而使得人们能通过简单好记的域名来代替 IP 地址访问网络。通过建立 DNS 数据库, 记录主机名称与 IP 地址的对应关系, 驻留在服务器端, 为客户端的主机提供 IP 地址解析服务。整个 DNS 域名系统由 DNS 域名空间 (指定用于组织名称的域的层次结构)、资源记录 (将域名映射到特定的资源信息, 以便在名称注册和解析时使用)、DNS 服务器 (提供存储和应答资源记录的名称查询服务) 和 DNS 客户端 (查询 DNS 服务器, 将域名称解析为查询中指定的资源记录类型) 四个部分组成。

#### 2. DNS 查询工作原理:

两种查询方式:

(1) .本地解析: 使用本地缓存信息进行解析。本地解析程序的缓存包括两种名称信息, 分别是本地配置的主机文件和从以前的 DNS 查询应答的响应中获取的资源记录。

(2) .查询 DNS 服务器:

#### 3. 相关配置文件:

(1) .DNS 主要配置文件:

/etc/hosts 主机的一个列表文件。包含简单的主机名解析 (系统的 IP 不是动态生成)。

/etc/host.conf 转换程序控制文件。告诉网络域名服务器如何查找主机名。

/etc/resolv.conf 转换程序配置文件。在配置程序请求 BIND 域名查询服务查询主机名称时, 告诉程序使用哪个域名服务器和 IP 地址来完成这个任务。

(2) .named 配置文件族:

/etc/named.conf 主文件。设置一般的 name 参数。

/var/named/named.ca 根域名配置服务器指向文件。指向根域名配置服务器, 用于告诉缓存服务器初始化。

/var/named/localhost.zone Localhost 区正向域名解析文件。将本地 IP 转换为回送方名字。

#### 4. 配置操作:

(1) 配置 Cache-only Server:

/etc/named.conf:

forwarders(168.95.1.1);

forward only;

命令:

#service named reload

(2) 配置 Primary Name Server

区声明: /etc/named.conf

配置正向解析数据库文件: /etc/named/xxx.net.hosts

配置反向解析数据库文件: /etc/named/192.168.1.rev

重新启动 DNS 服务器

(3)配置辅助域名服务器:

从主域名服务器中复制配置文件:

修改配置文件: master 改为 slave, 指定主域名服务器的 IP 地址

## 5. 故障排除:

(1) 利用 `dlint` 工具帮助分析 DNS 配置文件中的问题。

(2) 使用 `dnstop`, `nslookup`, `dig`, `named_checkzone`, `named_checkconf`, `whois`, `traceroute`, `host`, `ping` 等工具或命令来对 DNS 服务器的工作状态检查。

## (二) Apache 服务器的配置

### 1. 简介:

Apache 作为在 Internet 上最流行的 web 服务器之一, 实现了信息发布、资料查询、数据处理、视频点播等诸多应用, 并透过超级链接 (hypertext) 的方式, 将信息透过 Internet 传递到世界各处。由于 Apache 能运行在多种操作系统平台上, 且有开放源代码的优势, 得到全世界许多程序员的支持, 为其提供了许多功能模块, 使其具有无限扩展功能的优点, 工作性能和稳定性远远领先于其他同类产品。

### 2. 工作原理:

使用超文本传输协议 HTTP (一个在 TCP/IP 协议基础上的应用程序级协议), 在客户端和服务器端建立连接。

### 3. 相关配置文件:

/etc/httpd/conf/httpd.conf(旧版本还包括/etc/httpd/conf/目录下的 access.conf 和 srm.conf)

### 4. 配置操作:

(1)配置服务器在整个运行过程中的环境变量。如服务器的根目录、运行服务器时使用 PidFile 的路径、服务器响应 header 信息时显示的版本和操作系统的名称、服务器启动时运行的进程数等。

(2)配置主服务器或默认服务器运行时的详细接口参数。如运行服务器的用户和组、管理员的 EMAIL、根文档路径、根的访问权限、日志存放位置、记录日志的格式根据文件类型进行与之相应的操作、设置默认字符集、设置错误输出页面、设置浏览器匹配等。

(3)虚拟服务器设置。设置虚拟服务器, 使得在同一台 Apache 服务器上可以完成不同 IP 地址或主机名的 web 请求。可配制基于相同 IP 不同端口的虚拟主机或基于相同端口不同 IP 的虚拟主机或基于域名的虚拟主机。

### 5. Apache 服务器的访问控制、认证和授权:

使用 `order`, `deny`, `allow` 配置访问控制, 通过建立口令文件实现用户认证。

### （三）Vsftpd 服务器的配置：

#### 1. 简介：

FTP 服务是最基本的网络服务之一，具有管理简单性和双向传输功能。FTP 协议就是文件传输控制协议，使得文件通过网络从一台主机传送到同一网络的另一台主机上，而不受计算机类型和操作系统类型的限制。Vsftpd 是一个安全、高速且稳定的 FTP 服务器，可以设定多个基于 IP 的虚拟服务器。由于不执行任何外部程序，从而减少了安全隐患。其基本功能是上传下载，支持虚拟用户，支持 PAM 或 xinetd/tcp\_wrappers 的认证方式，支持带宽限制。

#### 2. 工作原理：

采用客户/服务器模式，客户端和服务端使用 TCP 建立连接，在服务器端预分配两个端口号，而客户端则动态分配其端口号，二者之间进行数据传输。

#### 3. 相关配置文件：

/etc/sbin/vsftpd Vsftpd 的主程序  
/etc/rc.d/init.d/vsftpd 启动脚本  
/etc/vsftpd/vsftpd.conf 主配置文件  
/etc/pam.d/vsftpd PAM 认证文件  
/etc/vsftpd.ftputers 禁止使用的用户列表文件  
/etc/vsftpd.user\_list 禁止或允许使用的用户列表文件  
/var/ftp 匿名用户主目录  
/var/ftp/pub 匿名用户的下载目录  
/etc/logrotate.d/vsftpd.log 日志文件

#### 4. 配置操作：

- （1）连接选项：设置与控制端口，FTP 模式与数据端口及 ASCII 模式。
- （2）性能与负载控制：设置超时选项，负载控制等。
- （3）用户选项：分别对匿名用户、本地用户、及虚拟用户设置相关信息。
- （4）安全措施：设置用户登录控制、目录访问控制、文件操作控制来提高服务器安全。
- （5）提示信息：设置登录时显示的欢迎语、某文件的内容，是否启用目录提示信息功能等。
- （6）日志设置：设置是否启用日志文件，文件名称，使用格式等。
- （7）其他设置：显示会话状态、显示时间、PAM 配置文件名等其他相关信息。

### （四）电子邮件服务器的配置：

#### 1. 简介：

电子邮件服务是 Internet 上最基本的服务之一，用户可以通过它与远程用户进行交流。电子邮件服务基于客户/服务器模式。对于一个完整的电子邮件系统而言，它主要由用户代理（UA，用户与电子邮件系统的接口）、邮件服务器（发送和接收邮件）、使用协议（SMTP / POP3 / IMAP4）组成。目前主流邮件服务器有 Sendmail、Postfix 和 Qmail。

#### 2. 工作原理：

MUA 将邮件提交给 MTA，MTA 决定如何处理邮件，发送到本地用户或转发给其他 MTA。接收者使用 MUA 获取邮件并阅读。

### 3. Sendmail 服务器的配置:

- (1) 修改 Sendmail 的设定文件/etc/mail/sendmail.mc
- (2) 制作 Sendmail 设定文件: #m4 sendmail.mc > sendmail.cf
- (3) 修改开机执行文件: 添加/etc/rc.d/saslauthd -a shadow
- (4) 手动启动 saslauthd 服务
- (5) 启动 Sendmail
- (6) 启动 POP3: 修改/etc/dovecot.conf,添加 protocols=pop3,启动 dovecot
- (7) 检查服务启动状态和防火墙
- (8) 设定主机名称/etc/mail/local-host-names

### 4. 优化 Sendmail

- (1)提高防垃圾邮件的能力:关闭 Sendmail 的 Relay 功能、添加 RBL 功能、使用 SpamAssassin.
- (2)限制“拒绝服务”攻击: 设置/etc/mail/sendmail.mc 的 confCONNECTION\_RATE\_THROTTLE confMAX\_DAEMON\_CHILDREN confMIN\_FREE\_BLOCKS confMAX\_HEADERS\_LENGTH confMAX\_MESSAGE\_SIZE 等目录的限度限制攻击的有效性。
- (3) 配置基于 Sendmail 的 Webmail, 使得使用者直接通过浏览器连接到 Web 服务器。
- (4) 通过过滤日志文件、使用 Telnet 解决常见故障。

## (五) NFS 服务器的配置:

### 1. 简介:

NFS 即网络文件系统, 使不同计算机之间能通过网络进行文件共享。采用客户/服务器模的工作模式。由客户端操作系统代表用户进程完成客户端调用, 服务器则在服务器操作系统中实现。

### 2. 工作原理:

使用远程过程调用 (RPC) 的服务来通过网络进行交互通信。RPC 指定 NFS 功能的端口号并回报给客户。

### 3. 配置操作:

- (1) 编辑/etc/exports 文件, 设定读写权限、判定使用者身份、设定资料同步写入等。
- (2) 使用 exportfs 命令重新扫描一次/etc/exports 文件
- (3) 激活服务 portmap 和 nfsd
- (4) 查看目录/var/lib/nfs/xtab 检验共享的目录内容
- (5) showmount 命令扫描主机提供的 NFS 共享目录
- (6) 使用 netstat 命令观察激活的端口号

## (六) DHCP 服务器的配置:

### 1. 简介:

动态主机配置协议 DHCP 是一个简化主机 IP 地址分配管理的 TCP/IP 协议, 负责接入网络中计算机的所有入网的必要参数, 如 IP 地址、子网掩码、默认网关、DNS 服务器的地址等。DHCP 协议的使用不仅减轻网络管理员管理和维护的负担, 还可以解决 IP 地址不够用的问题。

### 2. 工作原理:

使用客户/服务器模式, 客户端启动时自动与服务器通信, 服务器为客户端自动分配新的 IP 地址, 或者更新 IP 地址租约。

### 3. 配置操作:

(1) 编辑/etc/dhcpd.conf 文件, 设置其中的参数、声明与选项, 以完成子网的配置信息和全局配置信息。

(2) 建立名为 dhcpd.leases 的客户端租约文件, 其中保存所有已经分发的 IP 地址。

(3) 设置 DHCP 转发代理, 将无 DHCP 服务器子网的 DHCP 和 BOOTP 请求转发给其他子网内的 DHCP 服务器。

## (七) Samba 服务器的配置:

### 1. 简介:

服务信息块 SMB 是局域网上的共享文件夹和打印机的一种协议。通过 SMB 协议, 客户端应用程序可以在各种网络环境下读写服务器上的文件, 以及对服务器程序提出服务请求, 访问远程服务器端的文件和打印机等资源。

### 2. 工作原理:

Samba 程序让 NetBIOS 和 SMB 这两个协议运行于 TCP/IP 通信协议之上, 使用 Windows 的 NetBEUI 协议让 linux 可以在“网上邻居”中被 Windows 用户看到, 同时也使 linux 客户端可以使用服务器上的资源。

### 3. 配置操作:

(1) 编辑配置文件/etc/samba/smb.conf, 设置关于服务器主机的相关信息、访问服务器的主机信息、允许共享的文件和打印机的信息、日志文件信息、用户权限信息及网络信息等。

(2) 设置 Samba 密码文件/etc/samba/smbpasswd 添加账户: 使用 linux 命令组合将/etc/passwd 里所有用户批量添加到 smbpasswd 里, 或使用带参数的 smbpasswd 命令添加单个的账户并设置口令(被添加的账户的本地系统用户账号必须已经存在)。

## (八) Squid 代理服务器的配置:

### 1. 简介:

代理服务器提供文件缓存、复制和地址过滤等服务, 充分利用有限出口带宽, 加快内部主机访问速度, 解决多用户同时访问外网但公有 IP 不足的问题。同时作为一个防火墙, 隔离内网与外网, 提供监控网路和记录传输信息的功能。

## 2. 工作原理:

代表其他计算机传递网页、电子邮件、多媒体文件及其他网络应用程序等数据包或信息, 通过它的文件缓存和访问控制等功能, 实现快速浏览和对用户访问的有效管理。

## 3. 相关配置文件:

配置文件:

/etc/squid/squid.conf 主配置文件

/etc/squid/errors 错误报告

/etc/squid/mib.txt SQUID-MIB 定义文件

/etc/squid/mime.conf 定义 MIME TYPE

/etc/squid/msntauth.conf MSTN 认证配置文件

文档目录:

/usr/share/doc/squid 文档目录的根

缓存目录:

/var/spool/squid 缓存目录的根

错误提示:

/usr/share/squid/errors 错误语言文件的根目录

应用程序和库文件:

/usr/sbin/squid 主应用文件

/usr/sbin/squidclient 统计客户端程序

/usr/lib/\*\_auth 认证库文件

/usr/lib/squid/cachemgr.cgi 监控 squid 的 CGI 脚本

日志文件:

/var/log/squid/access.log 访问日志文件

/var/log/squid/store.log 缓存中存储对象的日志文件

/var/log/squid/cache.log 服务进程的日志文件

/etc/logrotate/squid 日志滚动文件

## 4. 配置操作:

(1) 编辑配置文件/etc/squid/squid.conf, 设置监听的 IP 地址和端口、内存缓冲大小、硬盘缓冲大小、使用缓存的有效用户及用户组、日志文件、主机名称、访问控制列表等信息。

(2) 建立使用硬盘缓冲区的目录结构

(3) 设置错误提示信息

(4) 配置主配置文件结合 NAT 和代理, 实现透明代理。

(5) 通过配置 squid.conf 文件、建立账户文件来实现用户的身份认证。

## (九) NTP 服务器的配置:

### 1. 简介:

Network Time Protocol (NTP) 是用来使计算机时间同步化的一种协议, 它可以使计算机对其服务器或时钟源 (如石英钟, GPS 等等) 做同步化, 它可以提供高精度度的时间校正 (LAN 上与标准间差小于 1 毫秒, WAN 上几十毫秒), 且可介由加密确认的方式来防止恶

毒的协议攻击。

## 2. 工作原理：

NTP 通过从原子钟、天文台、卫星或 Internet 获取国际标准时间 UTC。时间按 NTP 服务器的等级传播。按照离外部 UTC 源的远近将所有服务器归入不同的 Stratum（层）中。计算机主机一般同多个时间服务器连接，利用统计学的算法过滤来自不同服务器的时间，以选择最佳的路径和来源来校正主机时间。

## 3. 配置文件：

/etc/ntp.conf 主配置文件

/usr/share/zoneinfo 规定各主要时区的时间设定文件

/etc/sysconfig/clock 主要时区设定文件

/etc/localtime 本地系统的时间设定文件

## 4. 配置操作：

(1) 设置文件/etc/ntp.conf：使用 restrict 参数来设定权限，设定时间服务器的时钟，打开 iptables 防火墙 123 端口等。

(2) netstat 查看服务器工作情况，ntpq 监视 ntpd 操作

# 二．防火墙的构建：

## 1. 简介：

防火墙是设置在不同网络或网络安全域之间的一系列不见的组合，增强机构内部网络的安全性。类型包括包过滤防火墙、代理服务型防火墙。Iptables 组成 linux 下的包过滤防火墙，完成封包过滤、封包重定向、和网络地址转化 NAT 等功能。由 netfilter 组件和 iptables 组件构成。

## 2. 工作原理：

包过滤防火墙通过包检查模块在操作系统或路由器转发包以前拦截所有的数据包，并对其进行验证，查看是否满足过滤规则。代理服务型防火墙则在应用层上实现防火墙功能，提供部分与传输有关的状态，处理和管理信息。

## 3. 配置操作：

(1) 关闭系统防火墙

(2) 定义默认策略 iptables -P

(3) 查看规则 iptables -L

(4) 增加、插入、删除和替换规则 iptables -A-I-D-R，设置 Web 服务器、DNS、Sendmail，设置不回应 ICMP 封包、防止 IP Spoofing，防止网络扫描等。

(5) 清除原有旧的规则和计数器 iptables -F-Z

(6) 使用 SYN 阻止未经授权的访问

(7) 使用 iptables 命令防范病毒和假冒的 IP 地址

### 三. LVM 的应用:

#### (一) 简介:

LVM, 逻辑盘卷管理 (Logical Volume Manager), 是 Linux 环境下对磁盘分区进行管理的机制, LVM 是建立在硬盘和分区之上的一个逻辑层, 来提高磁盘分区管理的灵活性。LVM 是在磁盘分区和文件系统之间添加的逻辑层, 为文件系统屏蔽下层磁盘分区布局, 提供一个抽象的盘卷, 在盘卷上建立文件系统。

#### (二) 配置操作:

##### 1. 安装 LVM:

- (1) 安装 LVM 软件包
- (2) 配置内核支持 LVM, 并重新编译内核
- (3) 编辑系统启动脚本, 使用 `vgscan` 和 `vgchange-ay` 等命令确保在系统启动时激活 LVM

##### 2. 创建、管理 LVM:

- (1) 创建 LVM 分区, 分区类型为 `8e`
- (2) 使用 `pvcreeate` 命令创建物理卷
- (3) 使用 `vgcreate` 命令创建卷组
- (4) 使用 `vgchange` 命令激活卷组
- (5) 使用 `vgextend` `vgreduce` 在卷组中添加或删除物理卷
- (6) 使用 `lvcreate` 创建逻辑卷
- (7) 创建文件系统, 加载并使用
- (8) 使用 `lvextend` `lvreduce` `lvremove` 扩展、减少逻辑卷的大小或删除逻辑卷, 之前需要卸载该逻辑卷

### 四. 其他组件的添加与删除:

1. 删除了 `/lib/modules` 下不必要的模块
2. 压缩 `/bin` 目录、`/etc` 目录、`/home` 目录、`/lib` 目录、`/opt` 目录、`/root` 目录、`/usr` 目录  
为了节省一定空间及资源, 将这些目录压缩成为 `*.lzm` 格式。当光盘启动时有选择地进行解压。
3. `passwd -d root` 取消 `root` 密码  
由于此系统面向大众, 为了方便广大用户登录, 取消 `root` 密码。

### 五. Live CD 技术的应用:



1. 升级内核 for live 模式:

```
rpm -ivh kernel-2.6.24.4.rpm --nodeps --force
```

2. 修改 grub 默认登陆 live 核心

编辑/etc/grub.conf 文件, 使用以下语句控制 grub 登录方式:

```
root (cd)
```

```
kernel /boot/vmlinuz root=/dev/VolGroup00 ro
```

制作 CD 时通过执行脚本文件将其改为: root=/dev/ram0 rw

3. 安装 mkisofs 组件:

mkisofs, make iso file system, 建立 ISO 9660 映像文件, 即光盘文件。安装 mkisofs 软件包即可。

4. 封装:

将系统正常安装在主机或虚拟机上, 组件大小控制在 2000M 左右, 优化后打包封装即可。

## 六. 总结:

通过对 Asianux 3 workstation 的一系列服务器功能添加, 使得此系统囊括小型服务器的基本功能; 通过防火墙的设置, 优化网络环境, 使其更加安全有效; 修改内核及其他部件使其适用于 live 模式, 有选择地进行加载和使用; 删除旧的、无用的、可能产生安全问题的一些冗余模块, 压缩目录, 使其在精简的同时不失实用性和有效性。经过一系列修改, 在 CD 中的整个系统约 500M 左右。