Linux操作系统及应用技术

DHCP服务器的搭建及应用

两台连接到互联网上的电脑相互之间通信，必须有各自的**IP地址**，由于IP地址**资源有限**，宽带接入运营商不能做到给每个报装宽带的用户都能分配一个固定的IP地址（所谓固定IP就是即使在你不上网的时候，别人也不能用这个IP地址，这个资源一直被你所独占），所以要采用**DHCP方式**对上网的用户进行临时的地址分配。也就是你的电脑连上网，**DHCP服务器**才从地址池里临时分配一个IP地址给你，每次上网分配的IP地址可能会不一样，这跟当时IP地址资源有关。当下线的时候，DHCP服务器可能就会把这个地址分配给之后上线的其他电脑。这样可以有效节约IP地址，既保证了网络通信，又提高IP地址的使用率，同时也方便维护和管理。

目录

本章要点

9.1.1 DHCP服务简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）通常被应用在**大型的局域网络**环境中，主要作用是集中地管理、分配IP地址，使网络环境中的主机动态地获得IP地址、Gateway地址、DNS服务器地址等信息，并能够提升地址的使用率。

DHCP协议采用**客户端/服务器模型**，主机地址的动态分配任务由**网络主机驱动。**当DHCP服务器接收到来自网络主机申请地址的信息时，才会向网络主机发送相关的地址配置等信息，以实现网络主机地址信息的动态配置。

DHCP的功能

① DHCP应当可以给用户分配永久固定的IP地址。

② DHCP应当可以给用户分配永久固定的IP地址。

③ DHCP应当可以同用其他方法获得IP地址的主机共存（如手工配置IP地址的主机）

④ DHCP服务器应当向现有的BOOTP客户端提供服务。

9.1.1 DHCP服务简介

DHCP服务器以地址租约的方式来为DHCP客户端提供服务。DHCP服务器分配给客户端的IP类型主要有以下两种。

- **固定IP（static IP）**：DHCP服务器根据MAC地址来分配固定的IP地址，客户机就能以一个固定的IP连接上Internet。
- **动态IP（dynamic IP）**：客户机每次连上DHCP服务器所取得的IP地址都不是固定的，而是由DHCP服务器从尚未被使用的IP地址中随机选取。

9.1.1 DHCP服务简介

DHCP的优点是“免客户端设定”，便于移动上网。它有三种机制分配IP地址：

自动分配方式（Automatic Allocation）

DHCP服务器为主机指定一个永久性的IP地址，一旦DHCP客户端第一次成功从DHCP服务器端租用到IP地址后，就可以永久性的使用该地址。

动态分配方式（Dynamic Allocation）

DHCP服务器给主机指定一个具有时间限制的IP地址，时间到期或主机明确表示放弃该地址时，该地址可以被其他主机使用。

手工分配方式（Manual Allocation）

客户端的IP地址是由网络管理员指定的，DHCP服务器只是将指定的IP地址告诉客户端主机。

9.1.2 DHCP工作原理

DHCP协议采用**UDP**作为传输协议，主机发送请求消息到DHCP服务器的67号端口，DHCP服务器应答消息给主机的68号端口，详细的交互过程如图9-1所示。

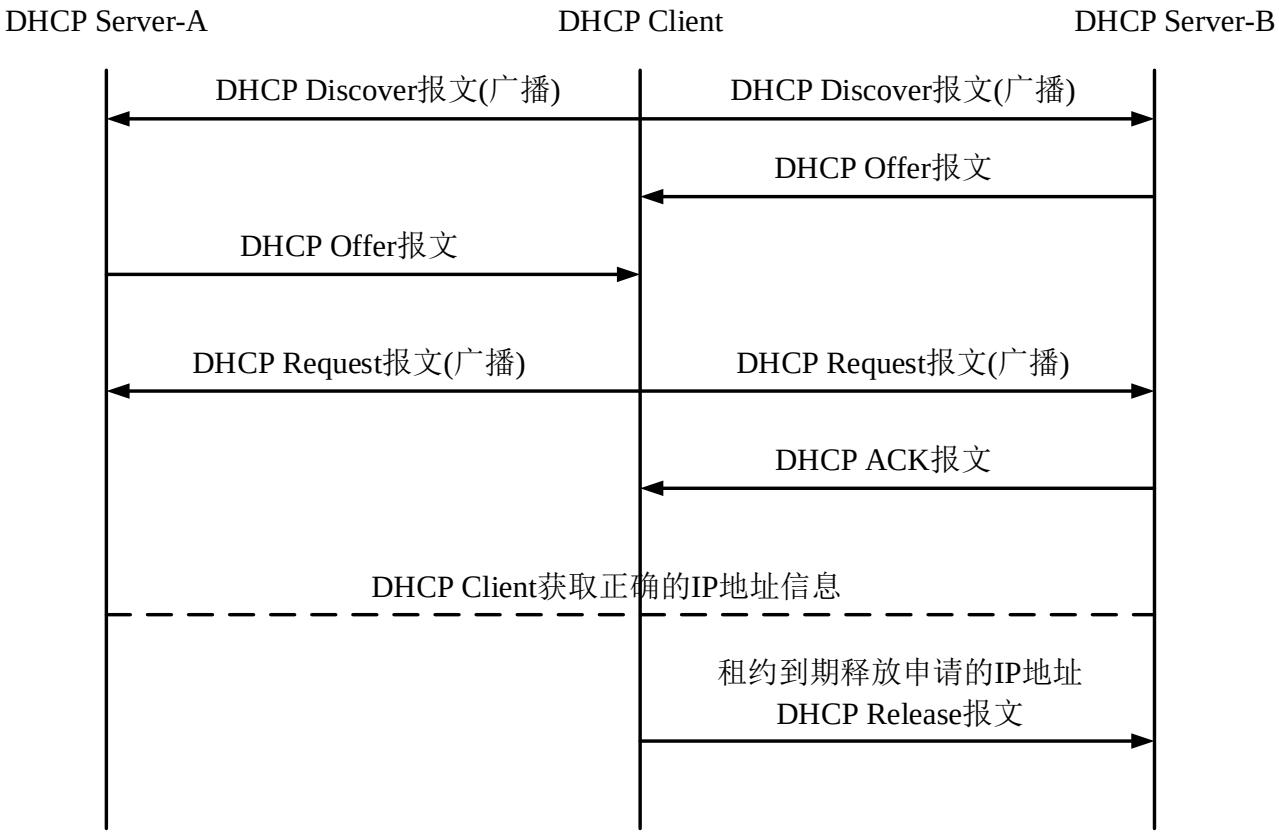


图9-1　DHCP工作原理

9.1.2 DHCP工作原理

具体实现过程如下：

1. DHCP Client**以广播的方式**发出DHCP Discover报文。

2. 所有的DHCP Server都能够接收到**DHCP Client**发送的DHCP Discover报文，所有的DHCP Server都会给出响应，向DHCP Client发送一个DHCP Offer报文。DHCP Offer报文中“Your(Client) IP Address”字段就是DHCP Server能够提供给DHCP Client使用的**IP地址**，且DHCP Server会将自己的IP地址放在“option”字段中以便DHCP Client区分不同的DHCP Server。DHCP Server在发出此报文后会存在一个已分配IP地址的记录。

9.1.2 DHCP工作原理

具体实现过程如下：

3

DHCP Client只能处理其中的一个**DHCP Offer报文**，一般的原则是DHCP Client处理**最先收到**的DHCP Offer报文。DHCP Client会发出一个广播的DHCP Request报文，在选项字段中会加入选中的DHCP Server的IP地址和需要的IP地址。

4

DHCP Server收到DHCP Request报文后，判断选项字段中的IP地址**是否与自己的地址相同**。如果不相同，DHCP Server不做任何处理只清除相应IP地址分配记录；如果相同，DHCP Server就会向DHCP Client响应一个DHCP ACK报文，并在选项字段中增加IP地址的使用租期信息。

9.1.2 DHCP工作原理

具体实现过程如下：

5

DHCP Client接收到DHCP ACK报文后，检查DHCP Server分配的IP地址是否能够使用。如果可以使用，则DHCP Client成功获得**IP地址**并根据IP地址使用租期自动启动续延过程；如果DHCP Client发现分配的IP地址已经被使用，则DHCP Client向DHCPServer发出DHCP Decline报文，通知DHCP Server禁用这个IP地址，然后DHCP Client开始新的地址申请过程。

6

DHCP Client在成功获取IP地址后，随时可以通过发送DHCP Release报文**释放自己的IP地址**，DHCP Server收到DHCP Release报文后，会回收相应的IP地址并**重新分配**。

9.1.2 DHCP工作原理

在使用租期**超过50%时刻**处，DHCP Client会**以单播形式**向DHCP Server发送DHCPRequest报文来**续租IP地址**。如果DHCP Client成功收到DHCP Server发送的DHCP ACK报文，则按相应时间延长IP地址租期；如果没有收到DHCP Server发送的DHCP ACK报文，则DHCP Client继续使用这个IP地址。

在使用租期**超过87.5%时刻**处，DHCP Client会**以广播形式**向DHCP Server发送DHCPRequest报文来续租IP地址。如果DHCP Client成功收到DHCP Server发送的DHCP ACK报文，则按相应时间延长IP地址租期；如果没有收到DHCP Server发送的DHCP ACK报文，则DHCP Client继续使用这个IP地址。直到IP地址使用租期到期时，DHCP Client才会向DHCP Server发送DHCP Release报文来释放这个IP地址，并开始新的IP地址申请过程。

9.1.2 DHCP工作原理

需要说明的是：DHCP客户端可以接收到多个DHCP服务器的DHCPOFFER数据包，然后可能接收任何一个DHCPOFFER数据包，但客户端通常只接受收到的第一个DHCPOFFER数据包。另外，DHCP服务器DHCPOFFER中指定的地址不一定为最终分配的地址，通常情况下，DHCP服务器会保留该地址直到客户端发出正式请求。

正式请求DHCP服务器分配地址

DHCPREQUEST采用广播包，是为了让其他所有发送DHCPOFFER数据包的DHCP服务器也能够接收到该数据包，然后释放已经OFFER（预分配）给客户端的IP地址。

如果发送给DHCP客户端的地址已经被其他DHCP客户端使用，客户端会向服务器发送DHCPDECLINE信息包拒绝接受已经分配的地址信息。

在协商过程中，如果DHCP客户端发送的REQUEST消息中的地址信息不正确，如客户端已经迁移到新的子网或者租约已经过期，DHCP服务器会发送DHCPNAK消息给DHCP客户端，让客户端重新发起地址请求过程。

目录

本章要点

1．获得DHCP软件包

RHEL7.2自带DHCP安装软件包，相关文件共有2个：

dhcp-4.2.5-42.el7.x86_64.rpm：DHCP主程序包，包括DHCP服务和中继代理程序，安装该软件包进行相应配置，即可以为客户机动态分配IP地址及其他TCP/IP信息。

dhcp-libs-4.2.5-42.el7.i686.rpm：DHCP服务器开发工具软件包，为DHCP开发提供库文件支持。

DHCP最新源代码软件包可访问http://www.isc.org网站获得

2．检查是否安装DHCP服务器

命令如下：

```
#rpm  -qa  dhcp
```

若无输出则表示未安装。

3．安装DHCP服务器软件包

将RHEL7的安装盘放入光驱，加载光驱后在光盘的Server目录下找到DHCP服务的RPM安装包文件dhcp-4.2.5-42.el7.x86_64.rpm，然后使用下面的命令安装DHCP服务：

```
# rpm -ivh   /Packages/dhcp-4.2.5-42.el7.x86_64.rpm
# rpm -q dhcp
dhcp-3.0.5-23.el5
```

4．DHCP服务器的运行管理

操作主要有：

- **启动：**# service dhcpd start
- **重新启动：**# service dhcpd restart
- **查询服务的启动状态：**# service dhcpd status
- **停止服务：**# service dhcpd stop

目录

本章要点

为学校其中一个机房架设一台DHCP服务器，其配置要求如下：

（1）动态分配的IP地址的范围为10.10.1.20～10.10.1.100，使用的子网掩码是255.255.255.0，默认网关地址为10.10.1.254。

（2）客户机使用的DNS服务器的IP地址为10.10.1.2，所在的网域名为abc.edu。

（3）为其中的一台教师机保留10.10.1.64地址，DNS的IP地址为222.246.129.80。

配置方法如下：

步骤 1 ▶

```
[root@localhost~]#vi /etc/dhcpd.conf
ddns-update-style interim;
ignore client-updates;
subnet 10.10.1.0 netmask 255.255.255.0{
                option router                   10.10.1.254;
                option subnet-mask 255.255.255.0;
                option domain-name "abc.edu";
                option domain-name-servers 10.10.1.2;
                range dynamic-bootp 10.10.1.20 10.10.1.100;
                default-lease-time 21600;
                max-lease-time 43200;
                host teacher{
                        hardware Ethernet 12:34:56:78:AB:CD;
                        fixed-address 10.10.1.64;
                        option domain-name-servers 222.246.129.80;
        }
}
```

配置方法如下：

步骤 2 ▶

```
[root@localhost ~]#service dhcpd start
启动dhcpd:                                [确定]
```

步骤 3 ▶ 测试。

▶ Linux用户客户端

1）修改Linux客户端的网卡配置文件

a) **# vim /etc/sysconfig/network-cripts/ifcfg-eth0**

b) 将BOOTPROTO=none修改为BOOTPROTO=dhcp，启用客户端DHCP功能。

2）重新启动网卡

 # ifdown eth0;ifup eth0

方法1

方法2

使用dhclient命令则重新发送广播申请IP地址

 # dhclient -d eth0

两种方法都使用ifconfig命令来查看动态分配的结果信息

 # ifconfig eth0

Windows用户客户端

1）在物理机上将IP地址设置为自动获得。

2）打开“运行”→输入“cmd”。

3）释放IP地址：**ipconfig /release。**

4）重新申请IP地址：**ipconfig /renew。**

5）执行：**ipconfig /all。**

6）此时若能看到所分配到的IP地址、默认网关和DNS服务器地址，则说明DHCP服务器工作正常，配置成功。

7）注意：Linux的DHCP是从IP地址池后面开始获取的，从高位开始分配的IP地址。

8）在服务器端看下日志：**cat /var/log/messages。**

9）查看**/var/lib/dhcpd/dhcpd.leases**这个文件，可以看到被租出去的IP地址和相关信息。

目录

本章要点

某学校有300台计算机，分别在两个机房里，每个机房分别提供不同的教学任务，为了避免互相干扰，需要设置不同的**IP网段**。这里要求采用DHCP服务器自动分配IP，提供网络内两个子网的用户主机**自动配置IP服务**。

根据需求可知，要提供动态IP地址分配的网段有2个，因此，在DHCP服务器中，需要定义2个DHCP作用域。对于各作用域都相同的域名服务器，可将其定义为默认域名服务器，在各作用域中就可不再单独配置了，如图9-2所示。

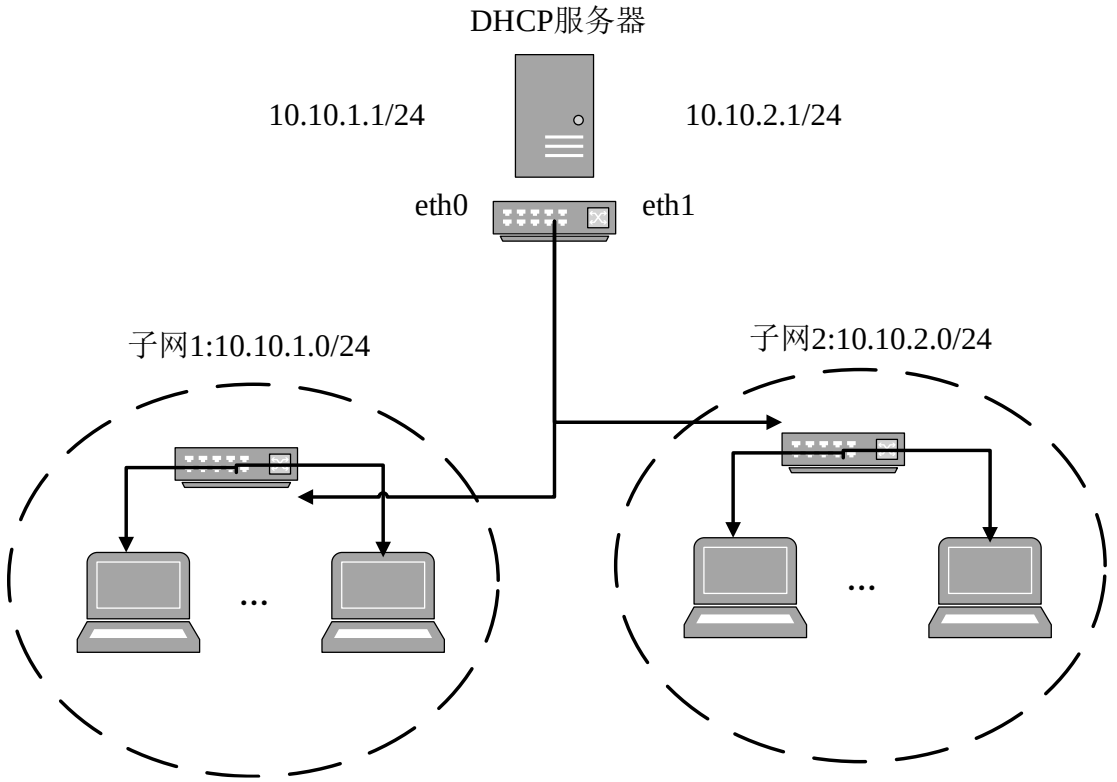


图9-2 配置多子网的DHCP服务

根据图9-2

10.10.1.0/24网段：

① 地址池范围为10.10.1.60-10.10.2.240。

② 默认网关（路由）为10.10.1.1。

③ 其余地址保留或用于静态分配。

④ 物理地址为00:0C:29:04:FB:E2的网卡，固定分配的IP地址为10.10.1.100；物理地址为00:0C:29:04:ED:35的网卡1，固定分配到的IP地址为10.10.1.101。

10.10.2.0/24网段：

① 地址池范围为10.10.2.20-10.10.2.100和10.10.2.140-192.168.3.240。

② 默认网关为10.10.2.254。

③ 各网段默认的域名服务器为61.128.192.68和61.128.128.68。

④ 物理地址为00:0C:29:1E:2F:4A的网卡，固定分配到的IP地址为10.10.2.100。

根据以上，配置步骤如下

步骤 1 ▶

为主机添加第二块网卡，然后启动。

注意：在虚拟机环境下：第一块网卡选择VMNET1，第二块网卡选择VMNET2

步骤 2 ▶

编辑dhcpd.conf主配置文件。

```
# vi /etc/dhcpd.conf                    #创建DHCP服务器配置文件
```

全局设置

```
ddns-update-style interim;      #设置DNS的动态更新方式（interim或ad-hoc）
```

步骤 2 ▶

以下设置是否允许动态更新DNS。若允许，则设置为：allow clienntupdates;

```
deny client-updates;                                    #不允许更新，或ignore client-updates;
default-lease-time 604800;                              #默认的IP租用期，以秒为单位
max-lease-time 864000;                                  #默认的最长租用期
option subnet-mask 255.255.255.0;                       #设置默认的子网掩码
#option domain-name "yourdomain.com";                   #设置默认DNS域名
option domain-name-servers 61.128.192.68，61.128.128.68;    #设置DNS服务器的IP
option time-offset -18000;                              #为客户端设定和格林威治时间的偏移时间
```

下面配置项用于设置默认的WINS服务器，用于主机名称解析，很少使用。

```
#option netbios-name-servers 10.10.0.253;
```

步骤 2 ▶

下面分别定义DHCP的作用域

```
subnet 10.10.1.0 netmask 255.255.255.0 {
 range 10.10.1.60  10.10.1.240;                  #指定可分配的IP地址范围
option broadcast-address 10.10.1.255;            #指定该网段的广播地址，可不设置
option routers 10.10.1.254;                              #指定该网段的默认网关
}
subnet 10.10.2.0 netmask 255.255.255.0 {
range 10.10.2.20   10.10.2.100;                  #指定第1段IP地址范围
range 10.10.2.140  10.10.2.240;                  #指定第2段IP地址范围
option broadcast-address 10.10.2.255;            #指定该网段的广播地址
option routers 10.10.2.254;                              #指定该网段的默认网关
}
```

步骤 2 ▶

以下对特殊的主机进行设置

```
group{
  default-lease-time 259200;                    #为该组的客户机单独设置租用期
  option routers 10.10.1.254;                   #为该组设置默认网关
  host staticiphost1 {
     hardware ethernet 00:0C:29:04:FB:E2;       #指定网卡的物理地址
     fixed-address 10.10.1.100;      }          #指定所固定分配到的IP地址
host staticiphost2 {
     hardware ethernet 00:0C:29:04:ED:35;
       fixed-address 10.10.2.101;    }
  host staticiphost3 {
     hardware ethernet 00:0C:29:1E:2F:4A;
     fixed-address 10.10.2.100;
     option routers 10.10.2.254;    } }          #为该主机特别指定默认网关
```

步骤 3 ▶

重启DHCP服务。

步骤 4 ▶

测试验证。

选择另一台虚拟机作为客户机，先后将其虚拟网卡设置为VMNET1和VMNET2，分别进行测试看是否能获得两个不同子网的分配。

若要使两个子网的客户机能通信，可将DHCP服务器上的路由开启。其方法是：

```
[root@localhost ~]# vim /etc/sysctl.conf
```

找到以下配置行：

```
net.ipv4.ip_forward=0
```

修改为：

```
net.ipv4.ip_forward=1
```

保存退出。

```
[root@localhost ~]# sysctl  -p /etc/sysctl.conf
```

使**sysctl.conf**的修改立即生效。

目录

本章要点

9.5.1 为什么需要DHCP中继代理

通过对于多作用域设置，使用多网卡的方式，虽然可以达到扩展可用IP地址范围的目的，但会增加网络拓扑的复杂性，并加大维护的难度。而如果想保持现有网络的结构，并实现网络扩容，可以选择采用超级作用域。

超级作用域是一个或多个作用域集合，用于支持同一物理网络上的多个逻辑IP子网。超级作用域包含子作用域的列表，对子作用域进行统一管理。

9.5.1 为什么需要DHCP中继代理

DHCP服务器启用**超级作用域**后，将会在其网络接口上根据超级作用域的设置，侦听并发送多个子网的信息。使用单块网卡就可以完成多个作用域的IP地址的分配工作。相比多网卡实现多作用域的设置，能够不改变当前网络拓扑结构，轻松完成IP地址的扩容。

但是，当超级作用域由多个作用域组成时，分配给客户机的IP地址也**不在同一个网段**，这个时候，不同子网的客户机互相访问就成了问题。为此，可以对网关配置**多个IP地址**，并在每个作用域中设置对应的网关IP地址，就可以使用客户机通过网关与其他不在同一网段的计算机进行通信。这就需要引入中继代理的技术。

9.5.2 配置DHCP中继代理方式

如果需要提供多个子网的IP自动分配，又要用单网卡而非多网卡来实现各子网间的通信效果，则需要配置DHCP中继代理服务。

配置DHCP中继代理方式：

- 在另一台Linux主机上安装、配置中继代理（实际中很少采用）。
- 通过路由器或三层交换机上设置DHCP中继代理实现跨网段的DHCP。

9.5.3 配置DHCP中继代理的步骤

在网关主机中构建DHCP服务器、DHCP中继服务器，为以下三个物理网段提供动态地址分配服务：

10.10.1.0/24、10.10.2.0/24、10.10.3.0/24

默认租约时间21600秒，最大租约时间43200秒。

客户机使用的DNS服务器地址如下：

202.106.0.20、202.106.148.1

用于动态分配的IP地址范围分别为：

10.10.1.20～10.10.1.200

10.10.2.20～10.10.2.200

9.5.3 配置DHCP中继代理的步骤

网关主机各接口的IP地址作为对应网段的默认网关。

应用需求描述，DHCP中继代理配置如图9-3所示。

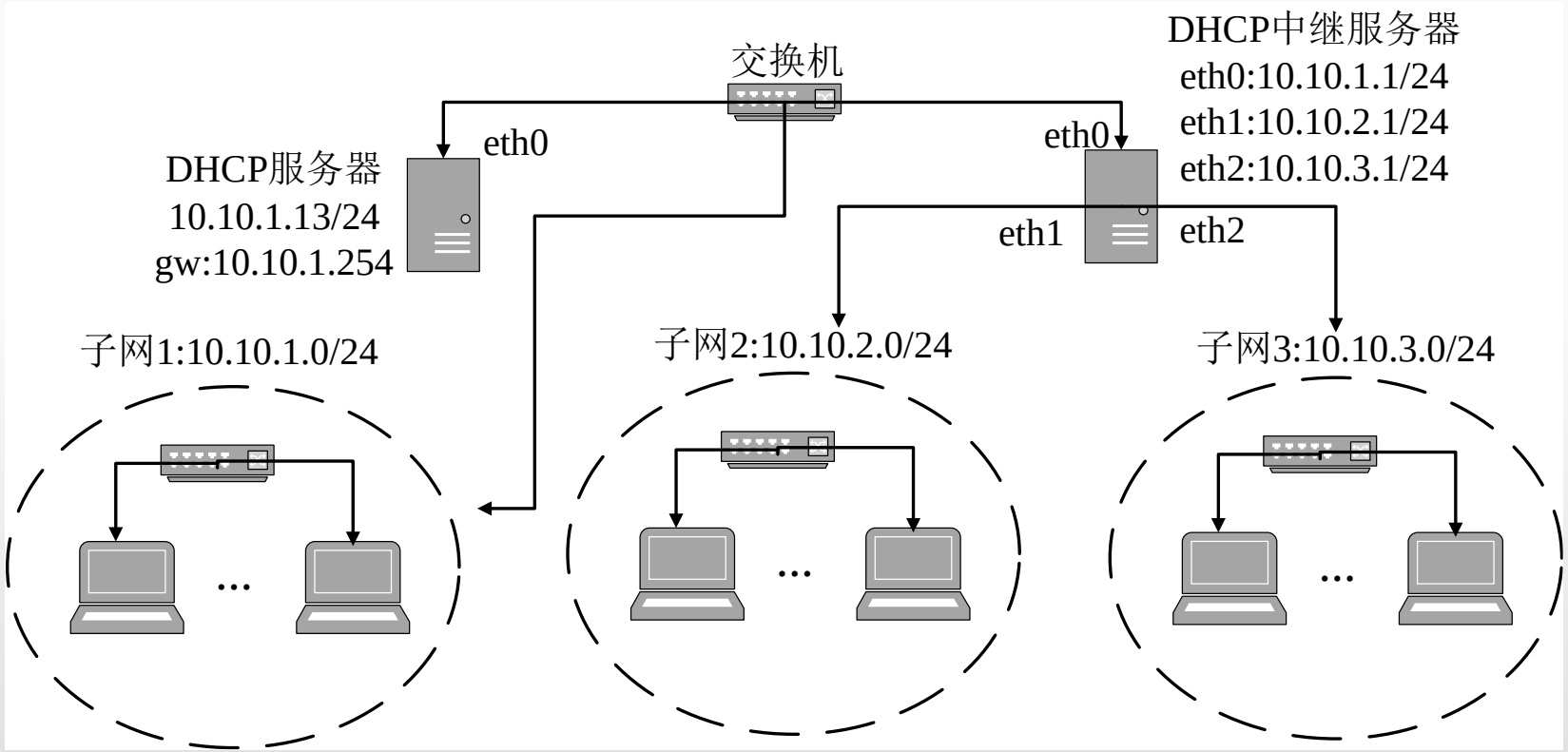


图9-3 配置DHCP中继代理

步骤 1 ▶

在一台Linux主机上安装、启动和配置DHCP服务器，配置每个作用域的IP地址池。需要定义超级作用域。

```
ddns-update-style interim:
default-lease-time 21600;
max-lease-time 43200;
option domain-name-servers 61.134.1.4,218.16.4.3;
subnet 192.168.1.0 netmansk 255.255.255.0 {
            # --- default gateway
                              option routers 192.168.1.1;
                              option subnet-mask 255.255.255.0;
        range dynamic-bootp 192.168.1.1 192.168.1.200;
}
```

步骤 1 ▶

```
subnet 192.168.2.0 netmansk 255.255.255.0 {
        # --- default gateway
                option routers 192.168.2.1;
                option subnet-mask 255.255.255.0;
    range dynamic-bootp 192.168.2.1 192.168.2.200;
}
subnet 192.168.3.0 netmansk 255.255.255.0 {
        # --- default gateway
                option routers 192.168.3.1;
                option subnet-mask 255.255.255.0;
    range dynamic-bootp 192.168.3.1 192.168.3.200;
}
"/etc/dhcpd.conf"  24L，774C
```

步骤 2 ▶

在另一台Linux主机上安装3块网卡，启动系统后再安装软件包：

dhcp- 4.2.5-42.el7.x86_64.rpm

步骤 3 ▶

配置3块网卡IP地址。　　根据网络拓扑图设置DHCP服务器网卡IP地址。

步骤 4 ▶

开启服务器的路由转发功能。

```
[root@localhost ~]# vi /etc/sysctl.conf
net.ipv4.ip_forward = 1
[root@localhost ~]# sysctl –p
```

步骤 5 ▶

设置中继接口及DHCP服务器的地址。

```
[root@localhost ~]# vi /etc/sysconfig/dhcrelay
INTERFACES="eth0 eth1 eth2"   //提供中继服务的子网接口
DHCPSERVERS="192.168.1.2"    //DHCP服务器IP地址
```

步骤 6 ▶

设置中继接口及DHCP服务器的地址。

```
service dhcrelay start
```

Linux操作系统及应用技术

vsftpd FTP服务器的搭建及应用

FTP是File Transfer Protocol（文件传输协议）的英文简称，而中文简称为**“文传协议”**。用于Internet上的控制文件的双向传输。同时，它也是一个**应用程序（Application）**。基于不同的操作系统有不同的FTP应用程序，而所有这些应用程序都遵守同一种协议以传输文件。

在FTP的使用当中，用户经常遇到两个概念：“下载”（Download）和“上传”（Upload）。下载文件就是从远程主机拷贝文件至自己的计算机上；上传文件就是将文件从自己的计算机中拷贝至远程主机上。用Internet语言来说，用户可通过**客户机程序**向（从）**远程主机**上传（下载）文件。

目录

本章要点

下面我们先来了解与FTP服务相关的一些基本概念。

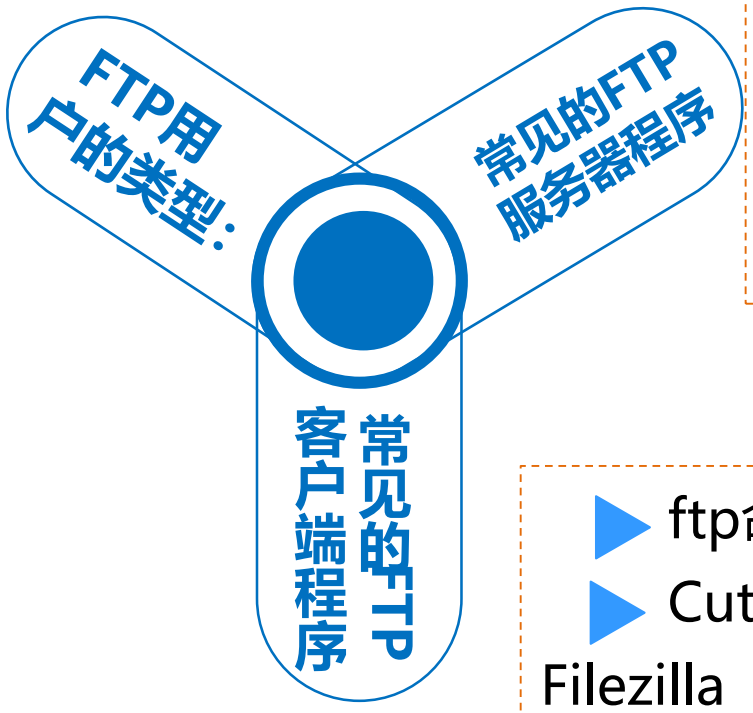
- 控制连接：标准端口为21，用于发送FTP命令信息；
- 数据连接：标准端口为20，用于上传、下载数据。

- 主动模式：服务端从20端口主动向客户端发起连接；
- 被动模式：服务端在指定范围内的某个端口被动等待客户端发起连接。

- 文本模式：ASCII模式，以文本序列传输数据；
- 二进制模式：Binary模式，以二进制序列传输数据

下面我们先来了解与FTP服务相关的一些基本概念。

- 匿名用户：anonymous或ftp；
- 本地用户：账号名称、密码等信息保存在passwd、shadow文件中；
- 虚拟用户：使用独立的账号/密码数据文件。



- IIS、Serv-U
- wu-ftpd、Proftpd
- vsftpd（Very Secure FTP Daemon）

- ftp命令
- CuteFTP、FlashFXP、LeapFTP、Filezilla
- gftp、kuftp

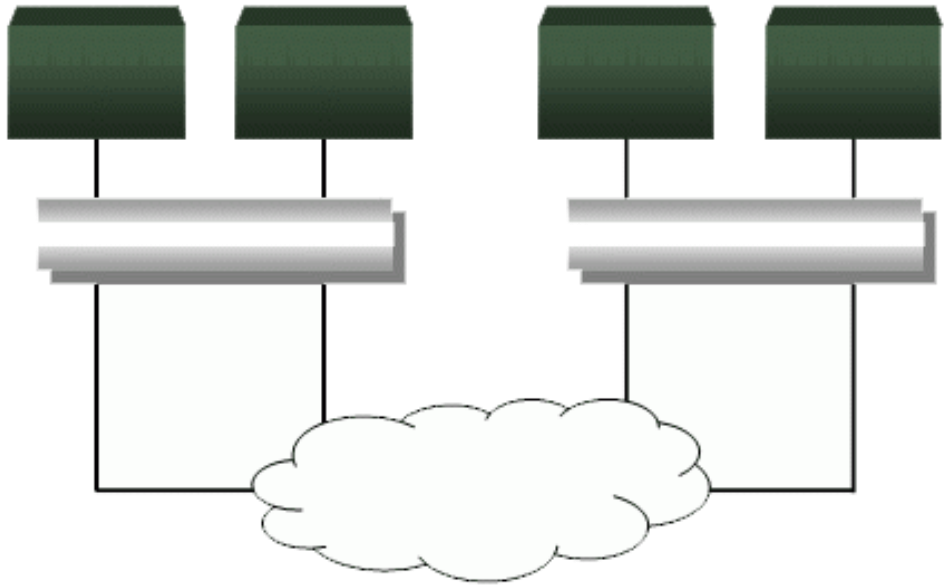
目录

本章要点

vsftp是一个基于**GPL发布**的类UNIX系统上使用的FTP服务器软件，目前已经被许多大型站点所采用，如ftp.redhat.com、ftp.kde.org和ftp.gnome.org.等。它的全称是Very Secure FTP，从此名称可以看出来，编制者的初衷是**代码的安全**。除了这与生俱来的安全特性以外，高速与高稳定性也是vsftp的两个重要特点。

在**速度**方面，使用ASCII代码的模式下载数据时，vsftp的速度是**Wu-FTP的两倍**，如果Linux主机使用2.4.*的内核，在千兆以太网上的下载速度可达86MB/S。

在**稳定**方面，vsftp就更加的出色，vsftp在单机（非集群）上支持4000个以上的并发用户同时连接，根据Red Hat的Ftp服务器（ftp.redhat.com）的数据，vsftp服务器可以支持15000个并发用户。



vsftpd是一款小巧易用**FTP服务器程序**，vsftpd在安全性、高性能及稳定性3个方面有上佳的表现。它提供的主要功能包括虚拟IP设置、虚拟用户、Standalone、inetd操作模式、强大的单用户设置能力及带宽限流等。在安全方面，它从原理上修补了大多数Wu-FTP、ProFTP，乃至BSD-FTP的安装缺陷，使用安全编码技术解决了缓冲溢出问题，并能有效避免“globbing”类型的拒绝服务攻击。目前正在使用vsftpd的官方网站有Red Hat、SuSE、Debian、GNU、GNOME、KDE、Gimp和OpenBSD等。它支持很多其他的FTP服务器不支持的特征。

vsftpd的实现有3种方式：

匿名用户形式：在默认安装的情况下，系统只提供匿名用户访问；

本地用户形式：以/etc/passwd中的用户名为认证方式；

虚拟用户形式：支持将用户名和口令保存在数据库文件或数据库服务器中。相对于FTP的本地用户形式来说，虚拟用户只是FTP服务器的专有用户，虚拟用户只能访问FTP服务器所提供的资源，这大大增强系统本身的安全性。相对于匿名用户而言，虚拟用户需要用户名和密码才能获取FTP服务器中的文件，增加了对用户和下载的可管理性。对于需要提供下载服务，但又不希望所有人都可以匿名下载；既需要对下载用户进行管理，又考虑到主机安全和管理方便的FTP站点来说，虚拟用户是一种极好的解决方案。

1 检查是否安装vsftpd软件

```
# rpm –qa |grep  vsftpd
```

若无任何显示，说明vsftpd未安装；若显示vsftpd-3.0.2-10.el7则说明当前系统已安装。

2 获得rpm安装包

在RHEL7.2中，系统自带了vsftpd，默认情况下，vsftpd未安装。

3 光驱挂载

```
# mount   /dev/cdrom   /mnt
```

4 安装vsftpd

```
# mount   /dev/cdrom   /mnt
```

5 vsftpd服务的运行管理

vsftpd服务器在/etc/rc.d/init.d目录下，有一个名为vsftpd的服务启动脚本，利用该脚本可启动、重启、状态查询、停止等操作。

service vsftpd start：启动vsftpd服务器

service vsftpd restare：重启vsftpd服务器

service vsftpd stop：停止vsftpd服务器

service vsftpd status：查询vsftpd服务器

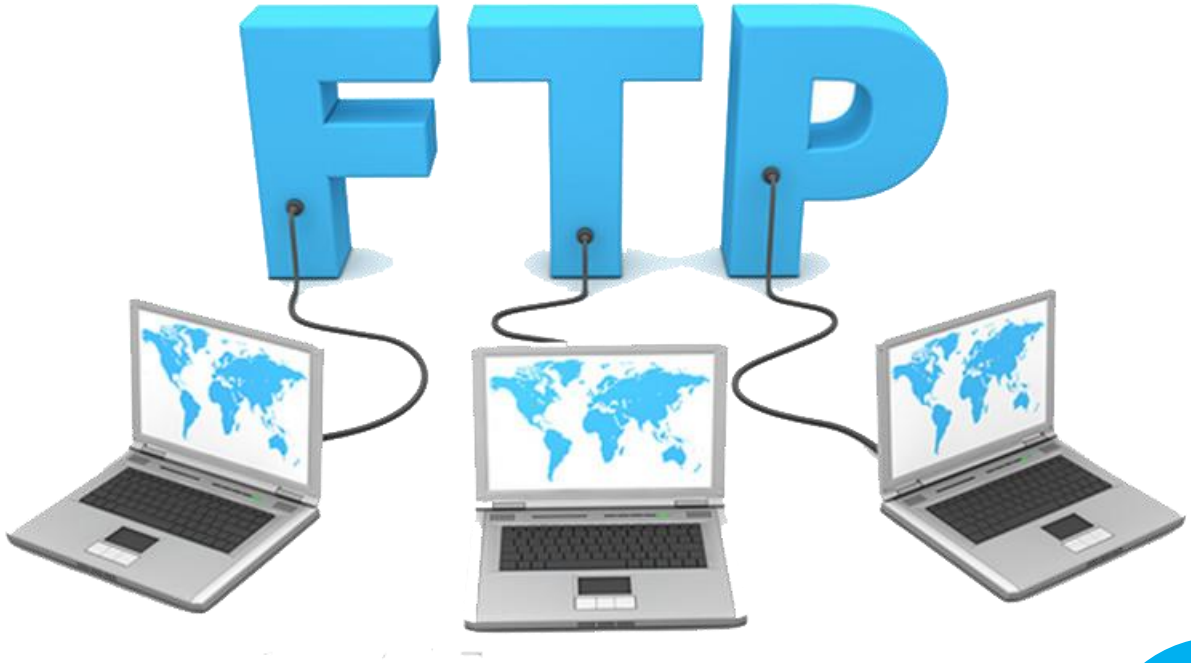
chkconfig–level 35 vsftpd on：设置vsftpd自启动，在执行等级3，5时，开启vsftpd系统服务

chkconfig-- listvsftpd ：vsftpd 0：off 1：off 2：off 3：on 4：off 5：on 6：off 显示系统服务列表，以及这些服务在运行级别0到6中已被启动还是停止。

6 匿名用户访问测试

启动服务后有关默认值如下：

- 匿名用户账户名称为：ftp或anonymous
- 匿名用户账户密码为：空或任意字符
- 登录后所在的FTP站点根目录为：/var/ftp
- 权限：可下载不可上传



7 在FTP服务器（本机）的测试过程

```
[root@server1 ~]# ftp 172.16.102.7
Connected to 172.16.102.7.
220 (vsFTPd 2.0.5)
530 Please login with USER and PASS.
530 Please login with USER and PASS.
KERBEROS_V4 rejected as an authentication type
Name (172.16.102.7:root): ftp          #输入登录者的用户名
331 Please specify the password.
Password:                              #输入用户密码
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
    227 Entering Passive Mode (172,16,102,7,174,72)
    150 Here comes the directory listing.
    drwxr-xr-x    2 0        0        4096 Nov 21 02:56 pub
    226 Directory send OK.
     ftp> quit
     221 Goodbye.
```

8 常用FTP命令

```
ftp  ip地址                                  //登录ftp服务器
dir、ls                                      //查询ftp站点的目录
cd                                           //改变当前工作目录
pwd                                          //显示远程主机当前工作目录
mkdir                                        //在远程主机上建立目录
get  远程文件名本地文件名                                  //下载
put/mput   本地文件名远程文件名          //上传
bye/quit                                     //退出ftp会话
```

表13-1 访问FTP服务器命令的返回值及含义

110	重新启动标记应答	221	服务的控制连接关闭，可以注销
120	服务在多久时间内ready	225	数据连结开启，但无传输动作
125	打开数据连接，传输开始	226	关闭数据连接端口，请求的文件操作成功
150	文件状态正常，开启数据连接端口	227	进入被动传输状态
200	命令被接受执行成功	230	使用者登入
202	命令执行失败	250	请求的文件操作完成
211	系统状态或是系统求助响应	257	显示目前的路径名称
212	目录的状态	331	用户名称正确，需要密码
213	文件的状态	332	登入时需要账号信息
214	求助的讯息	350	请求的操作需要进一部的命令
215	名称系统类型	421	无法提供服务，关闭控制连接
220	新的联机服务就绪	425	无法开启数据链路

表13-1 访问FTP服务器命令的返回值及含义

426	关闭联机，终止传输	504	命令所接的参数不正确
450	请求的操作未执行	530	登录不成功
451	命令终止：有本地的错误	532	储存文件需要账户登入
452	未执行命令：磁盘空间不足	550	未执行请求的操作
500	格式错误，无法识别命令	551	请求的命令终止，类型未知
501	参数语法错误	552	请求的文件终止，储存位溢出
502	命令执行失败	553	未执行请求的的命令，名称不正确
503	命令顺序错误		

目录

本章要点

vsftpd的配置文件如表13-2所示。

表13-2 vsftpd的配置文件

设置项	说明
/etc/vsftpd/vsftpd.conf	主配置文件
/etc/vsftpd/ftpusers	禁止使用vsftpd的本地用户帐号列表文件（黑名单）
/etc/vsftpd/user_list	禁止或允许使用vsftpd的用户列表文件
/etc/pam.d/vsftpd	PAM认证文件（其中file=/etc/vsftpd/ftpusers字段，指明阻止访问的用户来自/etc/vsftpd/ftpusers文件中的用户）
/var/ftp	匿名用户主目录
/var/ftp/pub	匿名用户的下载目录，此目录需赋权根chmod 1777 pub（1为特殊权限，使上载后无法删除）
/etc/logrotate.d/vsftpd.log	vsftpd的日志文件

主配置文件——/etc/vsftpd/vsftpd.conf，可设置用户登录控制、用户权限控制、超时设置、服务器功能选项、服务器性能选项、服务器响应消息等FTP服务器的配置。

 # vi　/etc/vsftpd/vsftpd.conf

以**#号开头**是注释行或是被关掉的具有某功能的配置行，所有有效配置行有相同的格式为：option=value，等号两边不能加空格。配置文件的详细帮助信息可查询手册页：# man vsftpd.conf。

在初始的样板文件中，并不包括所有想实现的功能，有些功能的实现要添加配置行。

1．匿名用户的有关设置

- **anonymous_enable =YES/NO**

  是否允许匿名用户登录FTP服务器，默认值为YES。

- **no_anon_password =YES/NO**

  控制匿名用户登入时是否需要密码，YES不需要，NO需要。默认值为NO。

- **anon_world_readable_only =YES/NO**

  匿名用户是否允许下载可阅读的文档。默认值为YES。

- **# anon_upload_enable =YES/NO**

  是否允许匿名用户上传文件，缺省为NO。

- **# anon_mkdir_write_enable =YES/NO**

  是否允许匿名用户有创建目录的写入权限，默认值为NO。

1．匿名用户的有关设置

anon_other_write_enable=YES/NO

是否允许匿名用户有其他的写入权限，如对文件改名、覆盖及删除文件。默认值为NO。

ftp_username=（自添）

匿名用户所使用的系统用户名。默认下，此参数在配置文件中不出现，默认值为ftp。

anon_root=/var/ftp （自添）

设置匿名用户登录后所在的目录（缺省为/var/ftp）。

anon_umask=022 （自添）

匿名用户所上传文件的默认权限掩码值。

anon_max_rate=200000

设置匿名用户的最大传输速度，单位为bytes/sec，值为0表示不限制。

2．本地用户的设置

- **local_enable=YES|NO**

  是否允许本地用户登录FTP服务器，默认值为YES。

- **local_umask=022**

  本地用户上传文件的默认权限掩码值。

- **local_max_rate=500000**

  设置本地用户的最大传输速度，单位为bytes/sec，值为0时表示不限制。

- **local_root=/var/ftp （自添）**

  设置本地用户登录后所在目录（缺省为为用户主目录）。

  如user1用户为：/home/user1

3．全局设置

write_enable=YES|NO

允许用户访问时，是否允许他们有写入的权限，默认值为YES。

banner_file =/etc/vsftpd/banner

设置vsftpd服务器是否以独立（standalone）模式运行，默认值为YES，建议不要更改。很多与服务器运行相关的配置命令，需要此运行模式才有效。若设置为NO，则vsftpd不是以独立的服务运行，要受xinetd服务的管理控制，功能上会受限制。

listen_port=21

设置FTP服务器建立连接所侦听的端口，默认值为21。

max_clients=0

设置FTP服务器所允许的最大客户端连接数，默认值为0，表示不限制。若设置为150时，则同时允许有150个连接，超出的将拒绝建立连接。只有在以standalone模式运行时才有效。

3．全局设置

max_per_ip=5

设置每个IP地址允许与FTP服务器同时建立连接的数目。默认为0，不受限制。通常可对此配置进行设置，防止同一个用户建立太多的连接。只有在以standalone模式运行时才有效。

xferlog_enable=YES

是否启用日志。

xferlog_file=var/log/vsftpd.log

设置日志文件名及路径，需启用xferlog_enable选项。

xferlog_std_format=YES

是否用标准格式存储日志。

pam_service_name=vsftpd

设置PAM认证服务的配置文件名，该文件位于/etc/pam.d目录下。

3．全局设置

ftpd_banner=Welcome blah FTP service

这边可定义欢迎话语的字符串，相较于banner_file是档案的形式，而ftpd_banner是字串的格式。预设为无。

banner_file =/etc/vsftpd/banner

当使用者登入时，会显示此设定所在的文件的内容，通常为欢迎话语或是说明。默认值为无。

dirmessage_enable =YES

如果启动这个选项，使用者第一次进入一个目录时，会检查该目录下是否有.message这个档案，若是有，则会出现此档案的内容，通常这个档案会放置欢迎话语，或是对该目录的说明。默认值为开启。

message_file=.message

设置目录消息文件。当使用者第一次进入一个目录时，是否显示该目录中的.message文件（需用编辑器手工创建）的内容，该文件通常放置欢迎话语或是对该目录的说明信息。

4．控制用户是否允许切换到上级目录

在默认配置下，用户可以使用“cd..”命名切换到上级目录。比如，若用户登录后所在的目录为/var/ftp，则在“ftp>”命令行下，执行“cd..”命令后，用户将切换到其上级目录/var，若继续执行该命令，则可进入Linux系统的根目录，从而可以对整个Linux的文件系统进行操作。

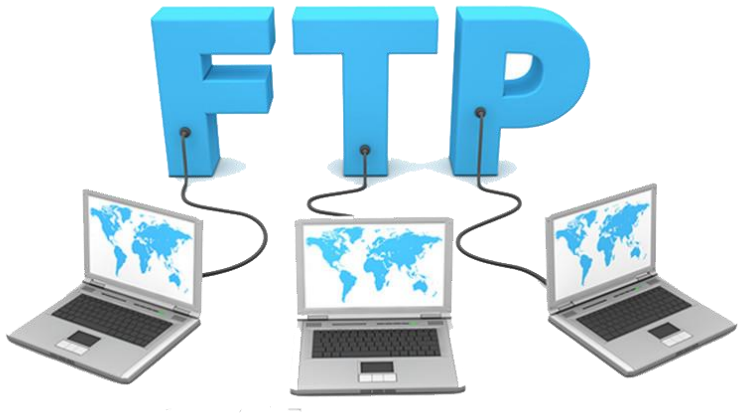
若设置了write_enable=YES，则用户还可对根目录下的文件进行改写操作，会给系统带来极大的安全隐患，因此，必须防止用户切换到Linux的根目录。相关的配置项如下：

1 配置所有登录不能改变自己的FTP根目录

本地用户是否锁定在宿主目录中：

chroot_local_user=YES|NO

要对**本地用户**查看效果，需先设置local_root=/var/ftp。



4．控制用户是否允许切换到上级目录

2 配置部分账户不允许改变自己的FTP根目录

是否启用chroot_list_file配置项指定的用户列表文件：

```
#chroot_list_enable=YES|NO
```

此文件需自己建立，被列入此文件的用户，在登录后将不能切换到自己目录以外的其他目录：

```
#chroot_list_file=/etc/vsftpd/chroot_list
```

chroot_list中的用户未锁定，chroot_list外的用户锁定：

```
chroot_list_enable=YES
chroot_local_user=YES
```

4．控制用户是否允许切换到上级目录

chroot_list中的用户锁定，chroot_list外的用户未锁定：

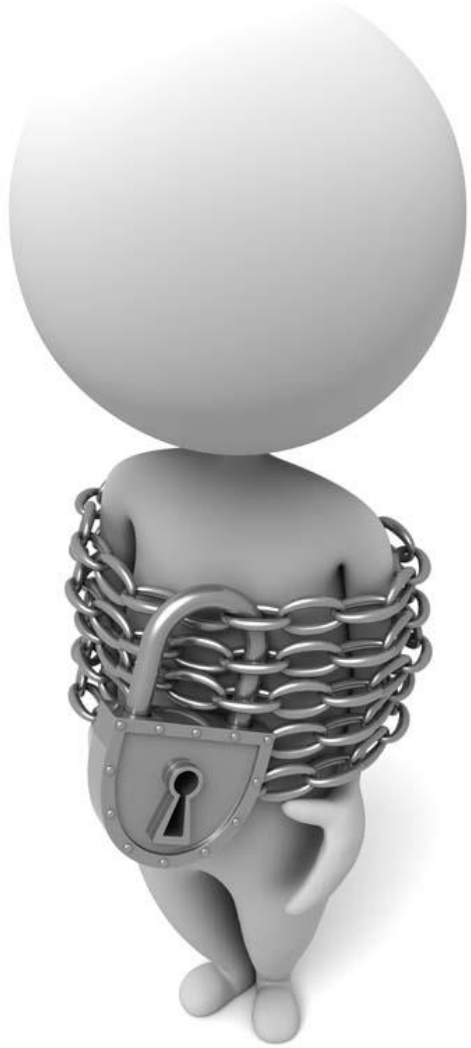
```
chroot_list_enable=YES
chroot_local_user=NO
```

所有用户锁定：

```
chroot_list_enable=NO
chroot_local_user=YES
```

所有用户未锁定：

```
chroot_list_enable=NO
chroot_local_user=NO
```



5．设置访问控制

（1）设置允许或不允许访问的主机

tcp_wrappers=YES

设置vsftpd服务器是否与tcp wrapper相结合，进行主机的访问控制。默认为YES，vsftpd服务器会检查/etc/hosts.allow和/etc/hosts.deny中的设置，以决定请求连接的主机是否允许访问该FTP服务器。这两个文件可以起到简易的防火墙功能。

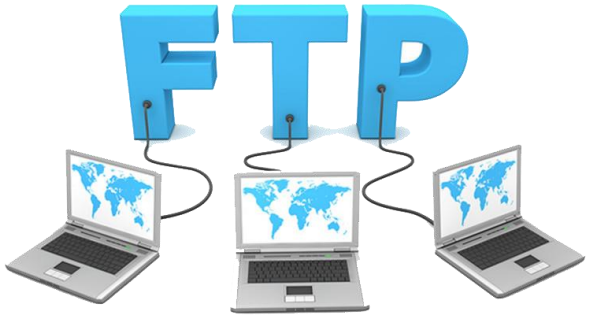
如：若仅允许192.168.168.1～192.168.168.254的用户，可以访问连接vsftpd服务器，则可在/etc/hosts.allow文件中添加以下内容：

vsftpd:192.168.168.0/255.255.255.0 :allow
all:all:deny

5．设置访问控制

（2）设置允许或不允许访问的用户

对用户的访问控制由/etc/vsftpd/user_list和/etc/vsftpd/ftpusers文件来控制实现。相关配置命令如下：



userlist_enable=YES | NO

设置/etc/vsftpd/user_list文件是否启用生效。YES则生效，NO不生效。

userlist_deny=YES | NO

设置/etc/vsftpd/user_list文件中的用户是允许访问还是不允许访问。

若设置为YES，则/etc/vsftpd/user_list文件中的用户将不允许访问FTP服务器；

若设置为NO，则只有vsftpd.user_list文件中的用户，才能访问FTP服务器。

5．设置访问控制

用户文件列表说明：

/etc/vsftpd/ftpusers

指定了不允许访问FTP服务器的本地用户账号（黑名单），如图13-1所示。这些账号不是普通用户账号，而是在系统中具有较高权限的账号，禁止这些账号进行FTP登录可提高系统的安全性。

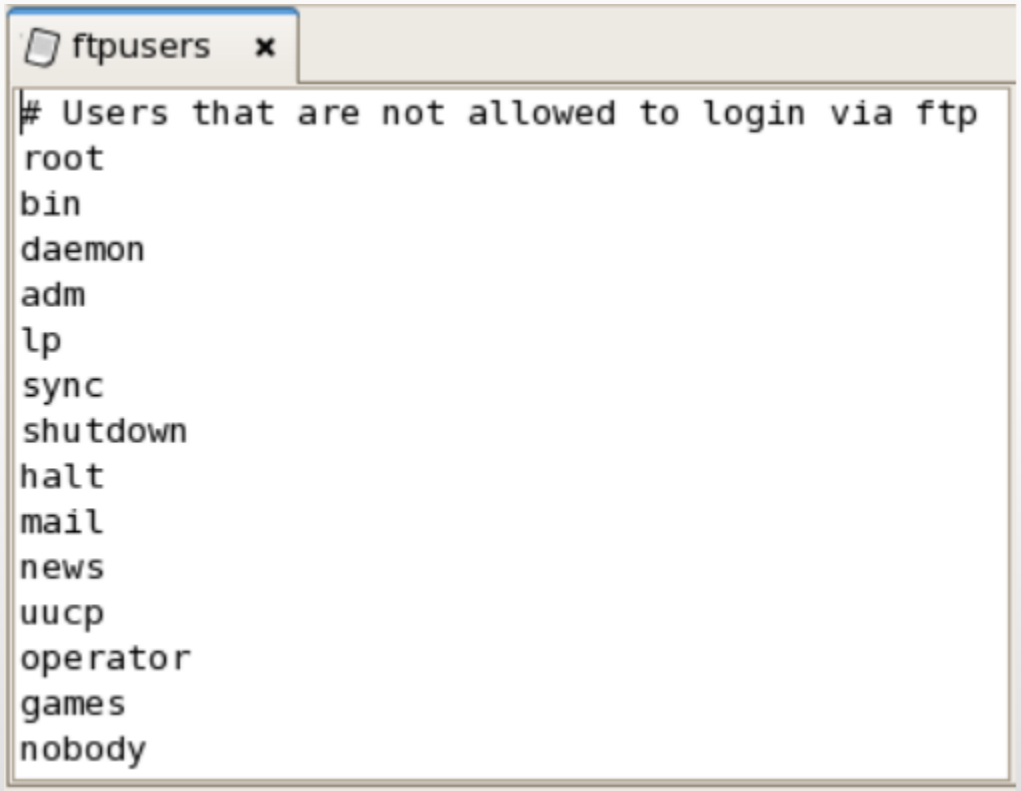


图13-1 ftpusers文件列表

5．设置访问控制

用户文件列表说明：

/etc/vsftpd/user_list

指定允许或不允许登录的用户列表，如图13-2所示。user_list文件需要与conf文件中的配置项结合来实现对user_list文件中指定用户账号的访问控制。

user_list

```
# vsftpd userlist
# If userlist_deny=NO, only allow users in
this file
# If userlist_deny=YES (default), never allow
users in this file, and
# do not even prompt for a password.
# Note that the default vsftpd pam config
also checks /etc/vsftpd/ftpusers
# for users that are denied.
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

图13-2 user_list文件列表

5．设置访问控制

1 设置禁止登录的用户账号

当conf配置文件中包括以下设置时，user_list文件中的用户账号被禁止进行FTP登录：

```
userlist_enable=YES
userlist_deny=YES
```

userlist_enable设置项设置使用user_list文件，userlist_deny设置为YES表示user_list文件用于设置禁止的用户账号。

2 设置只允许登录的用户账号

当conf配置文件中包括以下设置时，只有user_list文件中的用户账号能够进行FTP登录：

```
userlist_enable=YES
userlist_deny=NO
```

5．设置访问控制

userlist_enable设置项设置使用vsftpd.user_list文件，userlist_deny设置为NO表示vsftpd.usre_list文件用于设置只允许登录的用户账号，文件中未包括的用户账号被禁止FTP登录。

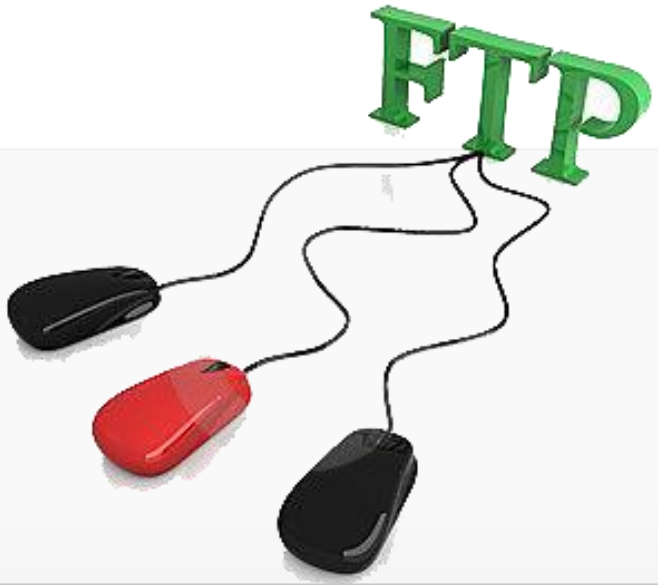
userlist_deny和userlist_enable选项限制**用户登录FTP服务器**（使用userlist_deny选项和user_list文件一起能有效阻止root、apache、www等系统用户登录FTP服务器，从而保证FTP服务器的分级安全性）。两个选项的具体表现形式和两种搭配使用方式的效果如表13-3所示。

5．设置访问控制

表13-2 vsftpd的配置文件

设置项	说明
userlist_enable=YES 且 userlist_deny=YES	ftpusers中用户禁止访问user_list中用户禁止访问（登录时不会出现密码提示，直接被服务器拒绝）
userlist_enable=YES 且 userlist_deny=NO	ftpusers中用户禁止访问user_list中用户允许访问
userlist_enable=YES	ftpusers中用户允许访问user_list中用户允许访问
userlist_enable=NO	ftpusers中用户禁止访问user_list中用户允许访问
userlist_deny=YES	ftpusers中用户禁止访问（登录时可以看到密码输入提示，但仍无法访问）user_list 中用户禁止访问
userlist_deny=NO	ftpusers中用户禁止访问user_list中用户允许访问

6．设置用户配置文件所在的目录



在vsftpd服务器中，不同用户还可使用不同的配置，这要通过用户配置文件来实现。

tcp_wrappers=YES

用于设置用户配置文件所在的目录。

设置了该配置项后，当用户登录FTP服务器时，系统就会到/etc/vsftpd/userconf目录下读取与当前用户名相同的文件，并根据文件中的配置命令，对当前用户进行更进一步的配置。比如，利用用户配置文件，可实现对不同用户进行访问的速度进行控制，在各用户配置文件中，定义local_max_rate配置，以决定该用户允许的访问速度

7．与连接相关的设置

listen_address=IP地址

设置在指定的IP地址上侦听用户的**FTP请求**。若不设置，则对服务器所绑定的所有IP地址进行侦听。只有在以standalone模式运行时才有效。对于只绑定了一个IP地址的服务器，不需要配置该项，默认情况下，配置文件中没有该配置项。若服务器同时绑定了多个IP地址，则应通过该配置项，指定在哪个IP地址上提供FTP服务，即指定FTP服务器所使用的IP地址。

注意

设置此值前后，可以通过netstat -tnl对比端口的监听情况。

7．与连接相关的设置

accept_timeout=60

设置建立**被动（PASV）数据连接**的超时时间，单位为秒，默认值为60。

connect_timeout=60

PORT方式下建立**数据连接**的超时时间，单位为秒。

data_connection_timeout=300

设置建立**FTP数据连接**的超时时间，默认为300秒。

idle_session_timeout=600

设置多长时间**不对FTP服务器进行任何操作**，则断开该FTP连接，单位为秒，默认为600秒。即设置发呆的逾时时间，在这个时间内，若没有数据传送或指令的输入，则会强行断开连接。

setproctitle_enable=NO|YES

设置**每个与FTP服务器的连接**，是否以不同的进程表现出来，默认值为NO，此时只有一个名为vsftpd的进程。若设置为YES，则每个连接都会有一个vsftpd进程，使用“ps-ef|grep ftp”命令可查看到详细的FTP连接信息。安全起见，建议关闭。

8．FTP工作方式与服务端口

connect_from_port_20＝YES|NO

指定FTP数据传输连接是否使用20端口，默认值为YES。若设置为NO，则进行数据连接时，所使用的端口由ftp_data_port指定。

ftp_data_port=20

设置PORT方式下FTP数据连接所使用的端口，默认值为20。

pasv_enable=YES|NO

若设置为YES，则使用PASV工作模式；若设置为NO，使用PORT模式。默认为YES，即使用PASV模式。

pasv_max_port=0

设置在PASV工作方式下，数据连接可以使用的端口范围的上界。默认值为0，表示任意端口。

pasv_mim_port=0

设置在PASV工作方式下，数据连接可以使用的端口范围的下界。默认值为0，表示任意端口。

9．设置传输模式

FTP在传输数据时，可使用二进制（Binary）方式，也可使用ASCII模式来上传或下载数据。

ascii_download_enable=YES

设置是否启用ASCII模式下载数据，默认为NO。

ascii_upload_enable=YES

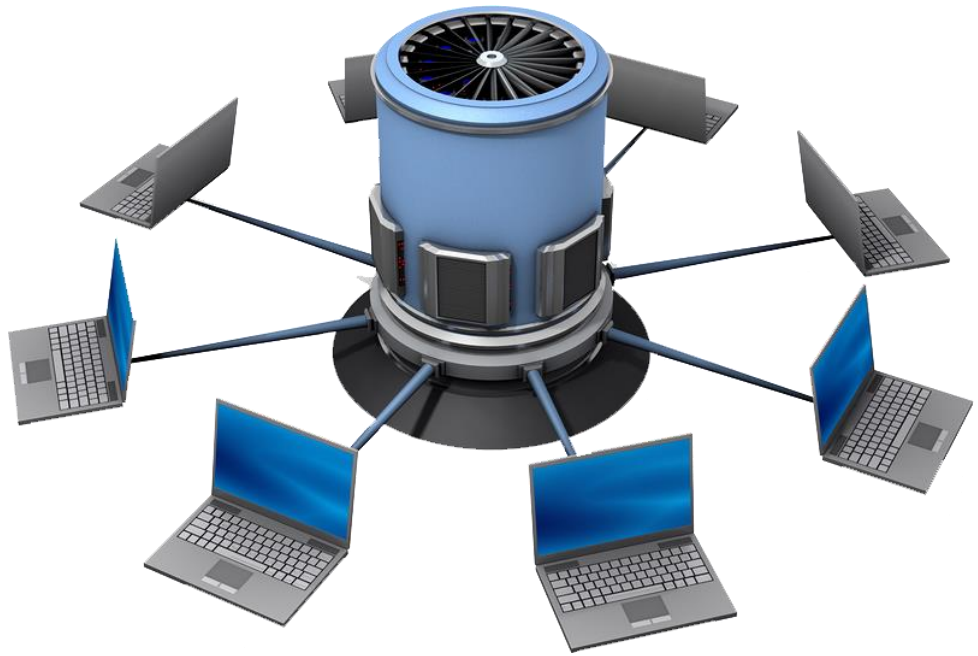
设置是否启用ASCII模式上传数据，默认为NO。

目录

本章要点

某学校需要搭建一台功能简单的**FTP服务器**，允许所有师生员工上传和下载文件，并允许创建用户自己的目录。

分析：允许所有师生员工上传和下载文件需要设置成允许匿名用户登录并且需要将允许匿名用户上传功能开启，最后anon_mkdir_write_enable字段可以控制是否允许匿名用户创建目录。



步骤 1 ▶

配置vsftpd.conf主配置文件。

按以下提示进行设置：

允许匿名用户访问 anonymous_enable=YES （所在位置12行）

匿名用户上传文件默认权限掩码值

anon_umask=022 （23行添加）

允许匿名用户上传文件 anon_upload_enable=YES （27行取消#号）

使允许匿名用户创建目录 anon_mkdir_write_enable=YES（31行取消#号）

修改完毕，保存退出。

步骤 2 ▶

修改上下文。

```
# mkdir  /var/ftp/mydata      //建立目录
# ll  -d   /var/ftp/mydata      //显示目录属性
drwxr-xr-x 2 root root 4096 11-22 10:25 /var/ftp/mydata
# chown   ftp  /var/ftp/mydata        //修改目录属性
# ll  -d   /var/ftp/mydata      //显示修改后目录属性
drwxr-xr-x 2 ftp root 4096 11-22 10:25 /var/ftp/mydata
```

步骤 3 ▶

修改seLinux，使seLinux支持匿名用户上传。

如下图所示，使用getsebool -a | grep ftp命令可以找到ftp的bool值，其中第二行：ftpd_anon_write的当前值为off，需改为on。

```
File  Edit  View  Search  Terminal  Help
[root@linuxprobe Desktop]# getsebool -a|grep ftp
ftp_home_dir --> off
ftpd_anon_write --> off
ftpd_connect_all_unreserved --> off
ftpd_connect_db --> off
ftpd_full_access --> off
ftpd_use_cifs --> off
ftpd_use_fusefs --> off
ftpd_use_nfs --> off
ftpd_use_passive_mode --> off
httpd_can_connect_ftp --> off
httpd_enable_ftp_server --> off
sftpd_anon_write --> off
sftpd_enable_homedirs --> off
sftpd_full_access --> off
sftpd_write_ssh_home --> off
tftp_anon_write --> off
tftp_home_dir --> off
[root@linuxprobe Desktop]#
```

步骤 4 ▶

修改上下文。

```
[root@server1 ~]# ll -Zd /var/ftp/mydata
drwxr-xr-x ftp root root:object_r:public_content_t /var/ftp/mydata
[root@server1 ~]# chcon -t public_content_rw_t /var/ftp/mydata
[root@server1 ~]# ll -Zd /var/ftp/mydata
drwxr-xr-x ftp root root:object_r:public_content_rw_t /var/ftp/mydata
```

步骤 5 ▶

使用reboot命令重新启动服务器。

```
[root@server1 ~]# reboot
```

步骤 6 ▶

修改上下文。

```
[root@server1 ~]# chkconfig   --list | grep vsftpd
vsftpd       0:关闭  1:关闭  2:关闭  3:关闭  4:关闭  5:关闭  6:关闭
[root@server1 ~]# chkconfig   --level   35  vsftpd on
[root@server1 ~]# chkconfig   --list | grep  vsftpd
vsftpd       0:关闭  1:关闭  2:关闭  3:启用  4:关闭  5:启用  6:关闭
```

步骤 7 ▶

启动vsftpd服务、开启21号端口。

```
# service   vsftpd   start
# iptables  -I  INPUT  -p  tcp   - -dport  21   -j  ACCEPT
```

在其他Windows主机测试（图形界面）。

步骤 8 ▶

打开IE的菜单“工具”→“Internet 选项”，单击“高级”标签卡，如图13-4所示，将“浏览”节点下的“使用被动FTP（为防火墙和DSL调制解调器兼容性）”前面的勾去掉。

图13-4 设置Internet 选项

步骤 9 ▶

在浏览器中输入ftp://172.16.102.61，出现如图13-5所示界面则测试成功。

图13-5 测试成功界面

目录

本章要点

某学校现有一台**FTP和Web服务器**，FTP的功能主要用于维护学校的Web网站内容，包括上传文件、创建目录、更新网页等。学校现有两个部门负责维护任务，并分别使用user1和user2账号进行管理。先要求仅允许user1和user2帐号登录FTP服务器，但不能登录本地系统，并将这两个账号的根目录限制为/var/www/html，不能进入该目录以外的任何目录。

在使用子进程处理HTTP请求的**Web服务器**上，由于要首先生成子进程才能处理客户的请求，因此反应时间就有一点延迟。但是，Apache服务器使用了一个特殊技术来摆脱这个问题，这就是预先生成多个空余的子进程驻留在系统中，一旦有请求出现，就立即使用这些空余的子进程进行处理，这样就不存在生成子进程造成的延迟了。

配置步骤如下：

步骤 1 ▶

建立维护网站内容的本地用户user1和user2并禁止本地登录，然后设置其密码。

```
[root@localhost ~]# useradd -s /sbin/nologin user1
[root@localhost ~]# useradd -s /sbin/nologin user2
[root@localhost ~]# passwd user1
[root@localhost ~]# passwd user2
```

步骤 2 ▶

创建上传根目录，并修改其权限。

```
[root@localhost ~]# # mkdir    -p    /var/www/html       //创建目录
[root@localhost ~]# ll  -d    /var/www/html              //显示目录属性
  drwxr-xr-x 2 root root 4096 11-14 18:46 /var/www/html
[root@localhost ~]# chmod   -R   o+w   /var/www/html//修改目录权限
[root@localhost ~]#  ll   -d    /var/www/html            //显示目录属性
drwxr-xrwx 2 root root 4096 11-14 18:46 /var/www/html
```

步骤 3 ▶

配置vsftpd.conf主配置文件并做相应修改。

anonymous_enable=NO （12行修改）

禁止匿名用户登录

local_enable=YES （15行）

允许本地用户登录

local_root=/var/www/html （16行添加）

设置本地用户的根目录为/var/www/html

chroot_list_enable=YES （96行去掉#号）

开启chroot功能

chroot_list_file=/etc/vsftpd/chroot_list（98行去掉#号）

设置锁定用户在根目录中的列表文件

步骤 4 ▶

建立/etc/vsftpd/chroot_list文件，添加user1和user2账号。

```
[root@localhost ~]# vim    /etc/vsftpd/chroot_list
user1
user2
```

步骤 5 ▶

开启禁用SELinux的FTP传输审核功能。

```
# getsebool -a | grep ftp
```

显示与ftp有关的所有seLinux的布尔值

```
# setsebool   -P  ftpd_disable_trans  on
```

on也可以换成1，off为0

注意

如果不禁用SELinux的FTP传输审核功能则会出现如下错误：“500 OOPS: 无法改变目录”。

步骤 6 ▶

重启vsftpd服务使配置生效。

```
# service  vsftpd  restart
```

步骤 7 ▶

测试。

测试1——在物理机的图形界面，登录界面如图13-6所示。登录后，鼠标拖拽窗口内的文件或文件夹进行下载和上传。

图13-6 登录界面

步骤 8 ▶

测试2——在物理机的字符界面，如图13-7所示。

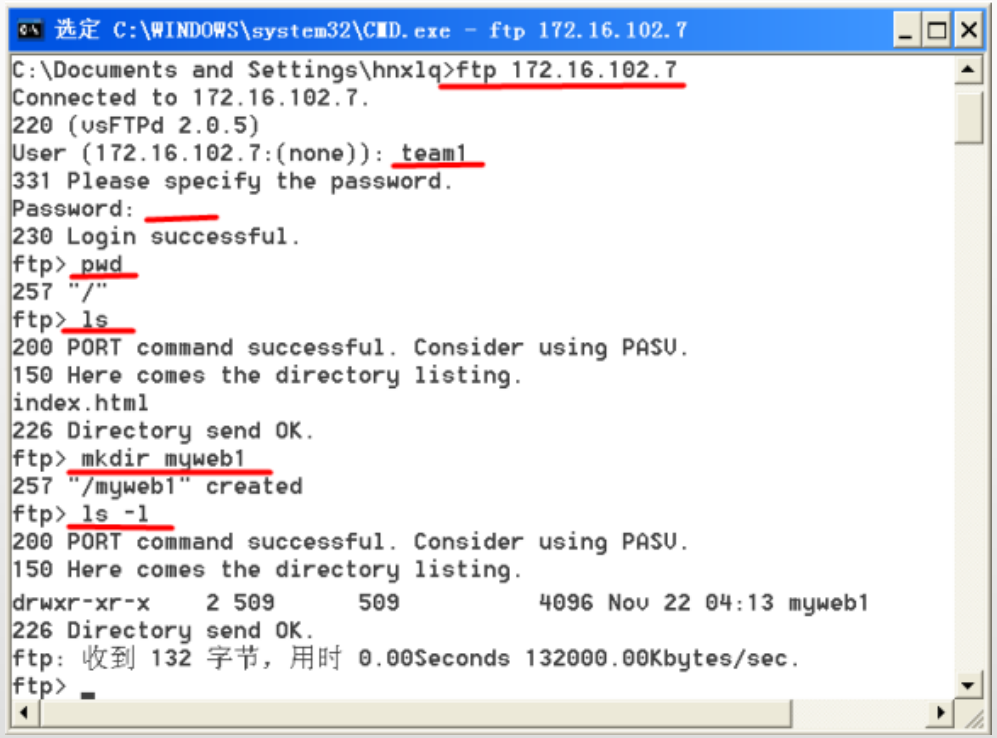


图13-7 字符界面

OK，需求目标全部达成，如图13-8所示。

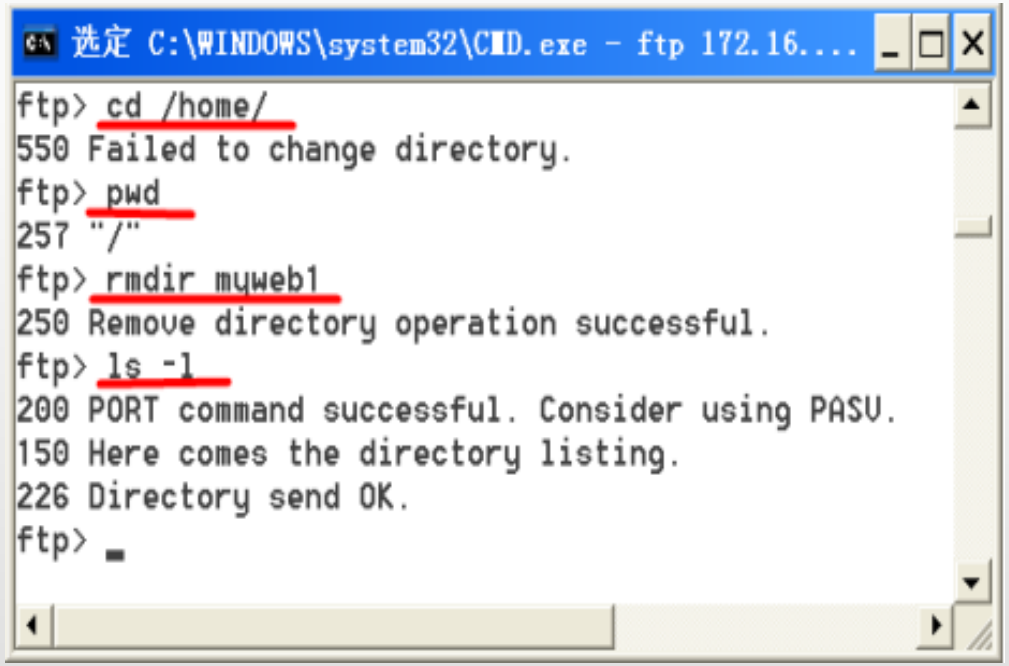


图13-8 测试成功

目录

本章要点

某学校为了便于师生员工的教学，计划搭建FTP服务器。对所有互联网用户开放共享目录，提供相关学习资料的下载，但禁止上传；学校内部的教师能够使用FTP服务器进行上传和下载，但不可以删除数据。为保证服务器的稳定性，要对**用户访问和下载/上传流量进行控制**。

根据学校的需求，对于不同用户进行不同的权限限制，FTP服务器需要实现用户的审核，考虑到服务器的安全性，关闭本地用户登录，使用虚拟用户验证机制，并对不同虚拟用户设置不同的权限。为了保证服务器的整体性能，还需要根据用户的等级，限制客户端的连接数及下载速度。

步骤 1 ▶

建立虚拟用户的用户名、密码列表的文本文件v_user.txt，添加公共账号ftp及教师账号teacher两个虚拟用户。

奇数行为账号名，偶数行为上一行中账号的密码。

```
[root@filesvr ~]# vi /etc/vsftpd/vusers.list
ftp
123
teacher
456
```

步骤 2 ▶

保存的v_user.txt文件无法被系统直接调用，需要使用db_load转换工具转化为Berkeley DB格式的数据库文件，为此需安装db4-utils-4.3.29-10.el5.i386.rpm软件包。

```
[root@localhost ~]# mount  /dev/cdrom  /mnt
[root@localhost ~]# rpm  -ivh  /mnt/Server/db4-utils-4.3.29-10.el5.i386.rpm
warning: /mnt/Server/db4-utils-4.3.29-10.el5.i386.rpm: Header V3 DSA signature: NOKEY, key ID
37017186
Preparing...          ########################################### [100%]
   1:db4-utils        ########################################### [100%]
```

步骤 3 ▶

使用db_load工具将列表文本文件转化为数据库文件。

```
[root@localhost ~]# cd /etc/vsftpd/
[root@localhost vsftpd]# db_load -T -t hash -f v_users.txt   v_users.db
```

步骤 4 ▶

修改数据库文件访问权限。

```
[root@localhost vsftpd]# chown 600 /etc/vsftpd/v_user.*
```

步骤 5 ▶

创建FTP根目录及虚拟用户映射的系统用户。

```
[root@localhost ~]# useradd  -d /var/ftp/share/  -s /sbin/nologin  ftpuser
[root@localhost ~]# useradd  -d /var/ftp/teacherdir/  -s /sbin/nologin  ftpteacher
[root@localhost ~]# chmod  -R 500  /var/ftp/share/
[root@localhost ~]# chmod  -R 700  /var/ftp/teacherdir/
```

步骤 6 ▶

建立支持虚拟用户的PAM认证文件。

```
[root@localhost ~]# vim /etc/pam.d/vuser.vu//配置文件的名称可以自行定义
#%PAM-1.0
auth       required     pam_userdb.so db=/etc/vsftpd/v_user
account    required     pam_userdb.so db=/etc/vsftpd/v_user
```

步骤 7 ▶

修改/etc/vsftpd/vsftpd.conf主配置文件。

```
anonymous_enable=NO
local_enable=YES                                    //使用虚拟用户一定要启用本地用户
chroot_local_user=YES                  //将所有本地用户限制在家目录中（需添加）
guest_enable=YES                                    //启用用户映射功能（需添加）
anon_world_readable_only=no //允许匿名用户浏览器整个服务器的文件系统（需添加）
pam_service_name=vuser.vu                                  //修改使用的PAM认证文件为vuser.vu
user_config_dir=/etc/vsftpd/vconfig      //指定虚拟用户的主目录位置（需添加）
max_clients=400                          //设置FTP服务器最大接入客户端数为400个（需添加）
max_per_ip=10                  //设置每个IP地址最大连接数为10个（需添加）
……
```

步骤 8 ▶

修改/etc/vsftpd/vsftpd.conf主配置文件。

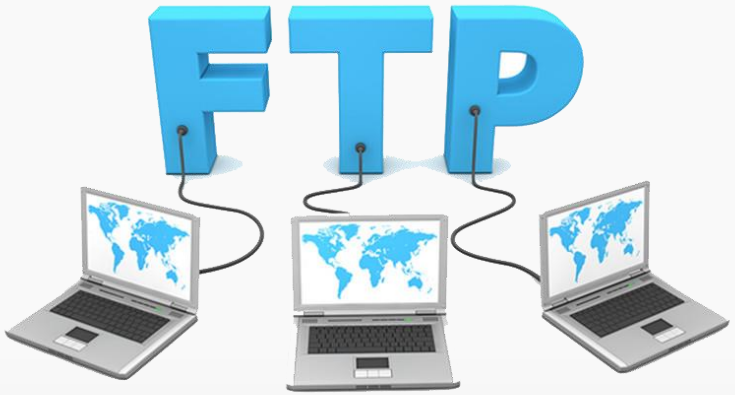
```
[root@localhost ~]# mkdir  /etc/vsftpd/vconfig/
[root@localhost ~]# vim  /etc/vsftpd/vconfig/ftp          //配置文件名与用户名同名
guest_username=ftpuser                                    //设置ftp对应的本地用户为
ftpuser
anon_max_rate=50000                                       //限定传输速率为50KB/s
[root@localhost ~]# vim /etc/vsftpd/vconfig/teacher       //配置文件名与用户名同名
guest_username=ftpteacher                                 //设置teacher对应的本地用户
为ftpteacher
write_enable=yes                                          //允许在文件系统写入权限
anon_mkdir_write_enable=yes                               //允许创建文件夹
anon_upload_enable=yes                                    //开启匿名帐号的上传功能
anon_max_rate=100000                                      //限定传输速度为100KB/s
……
```

步骤 9 ▶

修改seLinux设置，开启禁用SELinux

步骤 10 ▶

重新加载vsftpd配置。 `service vsftpd reload`



步骤 11 ▶

使用虚拟用户访问FTP的测试。

分别用ftp、teacher用户登录FTP服务器进行下载、上传测试，应得到以下结果：

- ftp用户可以登录，并可以浏览、下载文件（夹），但无法上传。
- teacher用户可以登录，并可以浏览、下载文件（夹），也可以上传文件（夹）。
- 匿名用户或其他系统用户不能登录vsftpd服务器。

Linux操作系统及应用技术

BIND域名解析服务器的搭建及应用

域名解析也叫**域名指向、服务器设置、域名配置以及反向IP登记**等。域名解析是把域名指向网站空间IP，让人们通过注册的域名可以方便地访问到网站的一种服务。IP地址是网络上标识站点的数字地址。为了方便记忆，采用域名来代替IP地址标识站点地址。域名解析就是域名到IP地址的转换过程。域名的解析工作由DNS服务器完成。

目录

本章要点

10.1.1 什么是DNS

DNS是计算机域名系统（Domain Name System或Domain Name Service）的缩写，它是由**解析器和域名服务器**组成的。

域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，而IP地址不一定有域名。域名系统采用类似目录树的等级结构。域名服务器为**客户机/服务器模式**中的服务器方，它主要有两种形式：主服务器和转发服务器。

10.1.1 什么是DNS

将域名映射为IP地址的过程就称为**“域名解析”**。在Internet上域名与IP地址之间是一对一（或者多对一）的，也可采用DNS轮循实现一对多，域名虽然便于人们记忆，但机器之间只认IP地址，它们之间的转换工作称为域名解析，域名解析需要由专门的域名解析服务器来完成，DNS就是进行**域名解析的服务器。**

DNS命名用于Internet等**TCP/IP网络**中，通过用户友好的名称查找计算机和服务。当用户在应用程序中输入DNS名称时，DNS服务可以将此名称解析为与之相关的其他信息，如IP地址。因为，你在上网时输入的网址，是通过域名解析系统解析找到了相对应的IP地址，这样才能上网。其实，域名的最终指向是**IP**。

10.1.1 什么是DNS

例如：对著名的**百度搜索引擎**来说，一般使用者在浏览这个网站时，都会输入网址http://www.baidu.com，很少有人会记住这台Server的IP是多少。所以http://www.baidu.com就是BAIDU站点的**Domain Name**。这正如我们在跟朋友打招呼时，一定是叫他的名字，几乎没有人是叫对方身份证号码来打招呼的。本质上在Internet上用于辨认机器的还是IP，所以当使用者在浏览器中输入Domain Name后，浏览器必须先到一台有Domain Name和IP对应信息的主机去查询这台电脑的IP，而这台被查询的主机，我们称它为Domain Name Server（域名服务器），简称DNS。

10.1.1 什么是DNS

当你输入http://www.baidu.com时，浏览器会将http://www.baidu.com这个名字传送到距离它最近的DNS Server上去做辨认，如果DNS Server查询出域名对应的IP，就会将这个IP值返回给这台主机，但如果没有查询到，就会出现警告信息。所以一旦你电脑的DNS Server设置不正确，就好比是路标错了，电脑也就不知道该将域名信息送到哪里去解析了。

10.1.2 DNS的结构

DNS是一个**分层级的分散式名称**，对应系统有点像电脑的目录树结构。在最顶端的是一个“.”（root），然后其下分为好几个基本类别名称如com、org、edu等，再下面是组织名称如cisco、Intel等，继而是主机名称如www、mail、ftp等。

因为当初Internet是从美国发起的，所以当时并没有国域名称，但随着后来Internet的蓬勃发展，DNS也加进了诸如cn、jp、au等国域名称。所以一个完整的DNS名称就好像是这样的www.xyz.com.cn，整个名称对应的就是一个IP地址了。

10.1.2 DNS的结构

root下面常用的6个组织类别，如表10-1所示。

表10-1 root下的组织类别

类别名称	代表意思
edu	教育学术单位
org	组织结构
net	网络通信单位
com	公司企业
gov	政府机关
mil	军事单位

说明

不过自从组织类别名称开放以后，各种各样五花八门的名称也相继现出来了。但无论如何，取名的规则最好是适合网站性质。除了原来的类别资料由美国的NIC（Network Information Center）管理之外，其他在国域以下的类别分别由该国的NIC管理。

10.1.3 理解DNS的工作方式

当DNS客户端需要查询程序中使用的名称时，它会通过查询DNS服务器来解析该名称。客户端发送的每条查询消息都包括3条信息，指定服务器回答的问题。

- 指定的DNS域名，规定为完全合格的域名（Fully Qualified Domain Name，FQDN）
- 指定的查询类型，可根据类型指定资源记录，或者指定查询操作的专用类型
- DNS域名的指定类别

例如，指定的名称可为计算机的FQDN，如www.baidu.com，并且指定的查询类型用于通过该名称搜索地址（A）资源记录。将DNS查询看作客户端向服务器询问由两部分组成的问题，如“您是否拥有名为‘www.baidu.com’的计算机的A资源记录？”当客户端收到来自服务器的应答时，它将读取并解释应答的A资源记录，获取根据名称询问的计算机的IP地址。

10.1.3 理解DNS的工作方式

DNS查询以各种不同的方式进行解析。有时，**客户端**也可使用从先前查询获得的缓存信息在本地应答查询。DNS服务器可使用其自身的资源记录信息缓存来应答查询。DNS服务器也可代表请求客户端查询或联系其他DNS服务器，以便完全解析该名称，并随后将应答返回至客户端。这个过程称为**递归（Recursion）**。

另外，客户端自己也可尝试联系其他的DNS服务器来解析名称。当客户端执行此操作时，它会根据来自服务器的参考答案，使用其他的独立查询。这个过程称为迭代。

10.1.3 理解DNS的工作方式

总之，DNS查询进程分两部分进行：

- 名称查询从客户端计算机开始，并传输至解析程序即DNS客户端服务程序进行解析；
- 不能在本地解析查询时，可根据需要查询DNS服务器来解析名称。

按照DNS搜索区域的类型，DNS的区域分为：

- **正向搜索**：是DNS服务器实现的主要功能，它根据域名解析出对应的IP地址；
- **反向搜索**：是根据IP地址解析出对应的域名。

10.1.4 DNS服务器的类型

DNS服务器主要有以下几种类型：

主域名服务器（Master DNS）：

是特定域所有信息的权威性信息源，对于某个指定域，主域名服务器是唯一存在的；主域名服务器中保存了指定域的区域文件。

辅助域名服务器（Slave DNS）：

不进行特定域信息（区域文件）的权威设置，而是从该域的主域名服务器中获取相应的文件并进行保存。当启动辅助域名服务器时，它会与它建立联系的所有主要域名服务器建立联系，并从中复制信息。它会定期地更改原有信息，以尽可能地保证副本与正本数据的一致性。辅助域名服务器主要有提供容错能力、加快查询速度和分担主域名服务器的负担等优点。

DNS服务器主要有以下几种类型：

缓存域名服务器：

或称为“惟高速缓存服务器”，主要功能是提供域名解析的缓存。

转发DNS服务器：

凡是可以向其他DNS服务器转发解析请求的DNS服务器都称为转发DNS服务器。

目录

本章要点

10.2.1 获得BIND软件包

BIND是一款开放源码的**DNS服务器软件**，BIND由美国加州大学伯克利分校开发和维护的，全名为Berkeley Internet Name Domain。它是目前世界上使用最为广泛的DNS服务器软件，支持各种Linux平台和Windows平台。

BIND软件包的安装方式有两种：

（1）利用**rpm格式**的安装包直接安装。

（2）利用**源代码**编译安装。

10.2.1 获得BIND软件包

RHEL7.2自带有版本号为9.9.4的BIND，主要有：

bind-9.9.4-29.el7.x86_64.rpm

DNS的主程序包

cachefilesd-0.10.5-6.el7.x86_64.rpm

高速缓冲DNS服务器的基本配置文件

bind-chroot-9.9.4-29.el7.x86_64.rpm

为BIND提供一个伪装的根目录以增强安全性工具。

说明

bind-chroot软件包最好最后一个安装，否则会报错。

10.2.1 获得BIND软件包

RHEL7.2自带有版本号为9.9.4的BIND，主要有：

bind-utils-9.9.4-29.el7.x86_64.rpm

提供对DNS服务器的测试工具程序，包括dig、host与nslookup等。（系统默认安装）

bind-libs-9.9.4-29.el7.x86_64.rpm

进行域名解析必备的库文件（系统默认安装）

10.2.2 检查是否已安装BIND软件包

执行命令：

```
#rpm -qa bind*
```

若只输出以下两行，说明没有安装BIND软件包

```
bind-libs-9.9.4-29.el7
bind-utils-9.9.4-29.el7
```

10.2.3 安装BIND软件包

RPM软件包安装——以RHEL7.2下自带的BIND为例。

```
# mount  /dev/cdrom   /mnt
# rpm -ivh /mnt/Packages /bind-9.9.4-29.el7.x86_64.rpm
# rpm  -ivh  /mnt/Packages/cachefilesd-0.10.5-6.el7.x86_64.rpm
# rpm  -ivh  /mnt/Packages /bind-chroot-9.9.4-29.el7.x86_64.rpm
```

10.2.4 DNS服务的运行管理

BIND软件包安装完毕以后，提供的主程序默认位于“/usr/sbin/named”，系统中会自动增加一个名为named的系统服务，通过脚本文件“/etc/init.d/named”或service命令都可以控制域名服务的运行。

service named start|stop|restart|status
启动/停止/重启/查询DNS服务

BIND配置文件如表10-2所示。

表10-2 BIND配置文件

样本文件的位置及名称	作用
全局配置文件：/var/named/chroot/etc/named.conf 样本文件：named.caching-nameserver.conf	设置一般的name参数，指向该服务器使用的域数据库的信息源
区域配置文件：/var/named/chroot/etc/named.rfc1912.zones	用于定义各解析区域特征的文件
正向解析数据库文件样本： /var/named/chroot/var/named/localdomain.zone	将域名映射为IP地址的文件
反向解析数据库文件样本： /var/named/chroot/var/named/named.local	将IP地址映射为域名的文件
根域地址数据库文件：/var/named/chroot/var/named/named.ca	记录了Internet中13台根域服务器的IP地址等相关信息
/etc/resolv.conf	指定本机DNS服务器的IP地址的配置文件

目录

本章要点

【例10-1】为某学校校园网搭建一台主DNS服务器，使得校园网内的用户能够通过域名访问校园网内的所有服务器，并通过DNS服务器的转发也能使用域名访问互联网中的服务器，DNS转发器设置为202.201.100.222。校园网内的服务器如表10-3所示。

表10-3 校园网内的服务器

服务器	完全合格域名	IP地址
主DNS服务器	dns1.abc.edu	172.10.1.11
辅助DNS服务器	dns2.abc.edu	172.10.1.13
缓存DNS服务器	dns3.abc.edu	172.10.1.15
Web服务器	www.abc.edu	172.10.1.12
FTP服务器	ftp.abc.edu	172.10.1.12
邮件服务器	mail.abc.edu	172.10.1.12
Samba服务器	smb.abc.edu	172.10.1.14

配置步骤：

步骤 1 ▶

配置DNS服务器网卡的IP地址为172.10.1.2，主机名为dns1.abc.edu。

步骤 2 ▶

全局配置文件/var/named/chroot/etc/named.caching-nameserver.conf。

```
# cd  /var/named/chroot/etc/
# cp  -p named.caching-nameserver.conf
named.conf
# vi    named.conf
```

步骤 2 ▶

修改其中4个地方（**红色字体处**）

```
options{
        listen-on port 53 {172.16.102.209;};
        listen-on-v6 port 53 {::1;};
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
                        statistics-file "/var/named/data/named_stats.txt";
                        memstatistics-file "/var/named/data/named_men_stats.txt";
        //Those options should be used carefully because the disable port
        //randomization
        //query-source port 53;
        //query-source-v6 port 53;
        allow-query  {any;};
        allow-query-cache {localhost;};};
```

步骤 2 ▶

修改其中4个地方（**红色字体处**）

```
logging{
        channel default_debug{
                file "data/named.run";
                severity dynamic;
};
};
view localhost_resolver{
        match-clients {any;};
        match-destinations {any;};
        recursion yes;
        include "/etc/named.rfc1912.zones";
};
```

◆ （1）options配置段常用配置项——用来说明全局属性

① listen-on port 53 { 172.10.1.1; };

设置named守护进程绑定的IP和监听的端口。若未指定，默认监听DNS服务器的所有IP地址的53号端口。

listen-on-v6 port 53{ ::1; };——设定监听进入服务器的ipv6请求的端口

② directory"/var/named";

指主配置文件的相对路径，其绝对路径为：/var/named/chroot/var/named

③ dump-file"/var/named/data/cache_dump.db";

指定域名缓存文件的保存位置和文件名。

statistics-file "/var/named/data/named_stats.txt";

当使用rndc stats命令的时候，服务器会将统计信息追加到的文件路径名。如果没有指定，默认为named.stats在服务器程序的当前目录中。

memstatistics-file "/var/named/data/named_mem_stats.txt";

服务器输出的内存使用统计文件的路径名，如果没有指定，默认值为named.memstats。

④ query-source port 53;

客户端在进行DNS查询时必须使用53作为源端口

query-source-v6 port 53;

⑤ allow-query { localhost ; };或allow-recursion{}

指定允许查询该DNS服务器的客户端IP地址或网络。在{}中可指定允许查询的客户机IP地址或网络地址列表，地址间用分号分隔。若不配置该项，则默认所有主机均可以查询。

比如：若仅允许127.0.0.1和192.168.168.0/24网段的主机查询该DNS服务器，则配置命令为：

memstatistics-file "/var/named/data/named_mem_stats.txt";

或表达为 **allow-query{127.0.0.1;192.168.168.0/24;};**

还可使用地址匹配符来表达允许的主机：

① any匹配所有IP地址；

② none不匹配任何IP地址；

③ localhost匹配本地主机；

④ localnets匹配本地网络。

若地址列表较多，通常可在options段之前，用acl定义一个访问控制列表，然后再在allow-query{}中引用该访问控制列表，其用法示例如下：

```
acl mylan {127.0.0.1;192.168.168.0/24;};
options{
    allow-query{mylan;};
};
```

◆ （2）Logging配置段——为域名服务器配置日志选项

```
channel default_debug {
file "data/named.run";
        severity dynamic;
};
```

channel短语对应于输出方式、格式选项和分类级别写入工作目录下的named.run文件；按照服务器当前的debug级别记录日志。

◆ （3）view配置段

view是BIND 9提出的新概念，可以根据域名查询请求的不同来源IP地址或目的IP地址，给客户提供不同的域名解析，从而实现策略（智能）DNS服务。

view用于定义一个view配置段（视区），对区域的定义，必须放在view视区中。

◆ （3）view配置段

① match-clients

{ localhost; };——客户端的源IP

② match-destinations

{ localhost; };——解析出的目标IP

①②中的参数中所有指定地址范围可以以下写法：

单个IP：	192.168.0.1;
网段：	192.168.0.0/24;或192.168.0.;
指定多个IP：	192.168.0.1;192.168.0.2;
none：	不匹配所有
any：	匹配所有
localhost：	DNS主机
localnet：	与DNS主机同网段

◆ （3）view配置段

③ recursion yes|no;

是否允许为客户机进行递归查询。如果客户端提交的FQDN本服务器没有，那么服务器会帮助客户端去查询。

view视区中的该项配置，将覆盖options中的该项全局设置。

④ include "/etc/named.rfc1912.zones";

定义将指定的区域配置文件包含进当前文件。

步骤 3 ▶

配置区域文件named.rfc1912.zones /var/named/chroot/etc和/etc下各有一个，后者是被链接的文件。

```
vim  named.rfc1912.zones
zone "." IN {
        type hint;
        file "named.ca";
};
zone "localdomain" IN{
        type master;
        file
"localdomain.zone";
        allow-update {none;};
};
```

```
zone "localhost" IN{
        type master;
        file "localhost.zone";
        allow-update {none;};
};
zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update {none;};
};
```

步骤 3 ▶

配置区域文件named.rfc1912.zones /var/named/chroot/etc和/etc下各有一个，后者是被链接的文件。

```
zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0." IN{
        type master;
        file "named.ip6.local";
        allow-update {none;};};
zone "255.in-addr.arpa" IN{
        type master;
        file "named.broadcast";
        allow-update {none;};};
zone "0.in-addr.arpa" IN{
        type master;
file "named.zero";
allow-udpate{none;};};
```

步骤 3 ▶

在文件named.rfc1912.zones尾部增加以下部分：

```
zone "abc.edu" IN {                    //指明要增加的DNS域的名称
type master;                           //指明增加的为DNS的主要区域
file "abc.edu.zone";      //设置该主要区域的区域配置文件名,该文件用于实现正向域名解析
allow-update { none; };                //设置该DNS不允许动态更新
};
zone "0.10.10.in-addr.arpa" IN {       //指明该区域为反向查找区域
type master;                           //指明该反向查找区域为主要区域
file "abc.edu.zero";                   //设置该反向查找区域的区域配置文件名
allow-update { none; };                //设置该DNS不允许动态更新
};
```

步骤 4 ▶

编辑正向解析数据库文件abc.edu.zone。

```
# cd  /var/named/chroot/var/named/
# cp  -p  localdomain.zone   abc.edu.zone
# vi    abc.edu.zone
          $TTL    86400
@ IN SOA    dns.abc.edu.  root.abc.edu.  (      //@表示当前的DNS域
   42       ; serial (d. adams)//序列号，要小于10位，一般定义为日期
            3H      ; refresh                    //更新时间，单位为秒
   15M      ; retry                              //更新失败重试时间
   1W       ; expiry                             //过期时间
   1D )     ; minimum                            //设置记录的缓存时间
@ IN       NS         dns.abc.edu.          /注意FQDN末尾的"."
  dns         IN       A         172.16.102.209
  www                  IN       A         172.16.102.210          //第一条主机记录
  ftp       IN       A         172.16.102.211                     //第二条主机记录
            mail       IN      CNAME     www.abc.edu.             //别名记录
   @        IN       MX      5   mail.abc.edu.                   //邮件记录
```

※（一）正向解析文件的格式和各部分的含义

数据库文件的每一行都由一条资源记录组成，每个资源记录通常包含5项，大多数情况下用ASCII文本显示，每条记录一行，格式如下：

Domain Time to live Record type Class Record data

各项的含义如下：

- **域名（Domain）：**该项给出要定义的资源记录的域名，该域通常用来作为域名查询时的关键字。
- **存活期（Time to live）：**在该存活期过后，该记录不再有效。
- **类别（Class）：**该项说明网络类型。目前大部分的资源记录都采用“IN”，表明Internet，该域的缺省值为“IN”。
- **记录数据（Record data）：**说明和该资源记录相关的信息，通常由资源记录类型来决定。
- **记录类型（Record type）：**该项说明资源记录的类型，常用的资源记录类型如下表所示。

※（二）各行的含义

$TTL 86400

从BIND 8.2开始，需要在区域文件的最前面加一条$TTL语句，用来设置域的默认生存时间TTL（Time To Live），时间单位为秒。86400秒即为1天，也可等价表达为$TTL 1D。

※（二）各行的含义

@　1D IN SOA@ root (

@——代表当前的域；也就是abc.edu.cn

1D——代表1天（day），3H代表3小时（hour），15M代表15分钟（minute），1W代表1周（week）；

IN——代表地址类别；

SOA——是授权起始（Start Of Authority）的缩写，是主域名服务器区域文件中一定要设置的，用于开始权威的域名信息记录，宣布该服务器具有权威性的名字空间。SOA之后应填写该域的名称，并且要在名称的最后附加上一个小数点“.”；域名之后，应填写域名服务器管理员的E-mail地址，E-mail地址中的“@”符号在此处用小数点代替，在E-mail地址的最后，也要附加一个小数点。

※（二）各行的含义

在该区域文件中，由于在前面使用了$ORIGIN语句进行定义，因此，此处的域名和域管理员E-mail就简约表达为了@ root，root名字不是以点结尾，系统会用$ORIGIN定义的域结尾，扩展后就变成了root.localhost.

接下来的括号中的值，其含义是：

1）**分号**为注释符；

2） **serial行前面的值：**代表该区域文件的版本号或序列号。用于辅域名服务器判断主域名服务的master file是否更新，所以如果有辅域名服务器，在每次修改master file后就应该修改这个序列号，以便辅域名服务器更新这个域的master file。

3） **refresh行前面的值：**代表更新的时间周期。此处设置为3H。

4） **retry行前面的值：**代表在更新出现通信故障时的重试时间。此处设置为15M，即15分钟。

接下来的括号中的值，其含义是：

5） **expire行前面的值：**代表重新执行更新动作后仍然无法完成更新任务而终止更新的时间。

6）**生存时间：**指定当域名服务器询问某个域名和其IP地址后，在域名服务器上放置的时间。

7） **minimum行前面的值：**代表客户域名查询的记录，在域名服务器上放置的时间，即设置记录的缓存时间。定义这个域在其他域名服务器的cache里的有效期，过了这个时间其他的域名服务器就会到这里来重新查询相关的信息。

※（三）常用的资源记录类型

表10-4 常用的资源记录类型

记录类型	说 明
SOA	每个区在区的开始处都包含了一个起始授权记录（Start of Authority Record），简称SOA记录。SOA定义了域的全局参数，进行整个域的管理设置。一个区域文件只允许存在唯一的SOA记录
NS	名称服务器（NS）资源记录表示该区的授权服务器，它们表示SOA资源记录中指定的该区的主和辅助服务器，也表示了任何授权区的服务器。每个区在区根处至少包含一个NS记录
A	将FQDN映射到IP地址
CNAME	指定标准主机的别名

※（三）常用的资源记录类型

表10-4 常用的资源记录类型

记录类型	说 明
MX	建立邮件服务器记录，此记录列出了负责接收发到域中的电子邮件的主机
PTR	将IP地址映射到FQDN
HINFO	主机描述，是以ASCII码表示的CPU和OS，该记录允许人们找出一个域内相应的机器和操作系统类型
TXT	定义一个zone，所有的定义只与该zone有关。该记录允许域以任意方式标识自身，HINFO和TXT两种记录类型都是为了用户的方便，其中任何一条都不是必要的

其中语句“IN MX 10 mail. abc.edu”用于为abc.edu域定义一条邮件地址交换记录（MX），10代表优先级，数字越小，优先级越高。当定义了两个或多个MX记录时，优先级高的服务器，将首先获得发来的邮件，只有定义了域的MX记录后，邮件服务器才能收到该域的邮件，以后域名mail.hnwy.edu就可作为邮件服务器的SMTP和POP3服务器的地址来使用。

1D IN NS @

用于添加一条NS（名称服务器）记录，用于指定权威的名称服务器。即该语句用于指定域名服务器，NS之后应放置当前域名服务器的名称。

1D IN A 127.0.0.1

用于添加一条A（Address）记录，即地址记录。用于指定一个名称所对应的IP地址。该条记录的含义就是将localhost解析为127.0.0.1

※（四）常用命令

1 named-checkconf

此命令可以发现/var/named.conf文件中的语法错误，命令如下：

```
# named-checkconf
```

如果有任何语法错误，会有消息告诉用户问题出在哪里，以及错误是什么等，否则没有任何输出显示。

2 named-checkzone

此命令用于检查创建的区域文件是否配置正确，过程如下：

```
#  named-checkzone edu.cn named.hosts
zone edu.cn/IN: loaded serial 1997022700
OK
```

其中，edu.cn是我们要检查的域名，named.hosts是我们创建的区域文件的名字。从此处显示的结果可以看出，没有语法错误。

3 dig

dig是另外一个功能强大的工具，作用和nslookup类似，使用方法如下：

```
# dig www.edu.cn
; <<>> DiG 9.2.1 <<>> www.edu.cn
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53208
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:0
;; QUESTION SECTION:
;www.edu.cn.                    IN      A
;; ANSWER SECTION:
www.edu.cn.         86400   IN      A       202.112.0.36
;; AUTHORITY SECTION:
edu.cn.             86400   IN      NS      sdedns.
;; Query time: 1 msec
;; SERVER: 202.194.224.3#53(202.194.224.3)
;; WHEN: Tue Mar 21 17:46:44 2006
;; MSG SIZE  rcvd: 68
```

更加详细的命令，大家可以通过使用man命令查看，例如

```
# man dig
```

步骤 5 ▶

编辑反向解析数据库文件localhost.com.zero。

```
# cd  /var/named/chroot/var/named/
# cp  -p  named.local    abc.edu.zero
# vi      abc.edu.zero
 $TTL    86400
@   IN   SOA  102.16.172 .in-addr.arpa.   root.localhost.com. (
                        1997022700 ; Serial
                        28800          ; Refresh
                        14400          ; Retry
                        3600000        ; Expire
                        86400 )        ; Minimum
@                  IN     NS                    dns.abc.edu.
209                IN     PTR                   dns.abc.edu.
210                IN     PTR                   www.abc.edu.
211                IN     PTR                   ftp.abc.edu.
```

说明

最后三句前面的209、210、211是指IP：172.16.102.209、172.16.102.210、172.16.102.211的最后一个数。

步骤 6 ▶

防火墙配置。如果不配置，就不能让其他人访问你的DNS服务器。

 # setup

在弹出的对话框中选择“防火墙配置”→“定制”选项，接着在所弹出对话框的“Other ports”项里输入：“53: tcp 53: udp”，如图10-1所示。

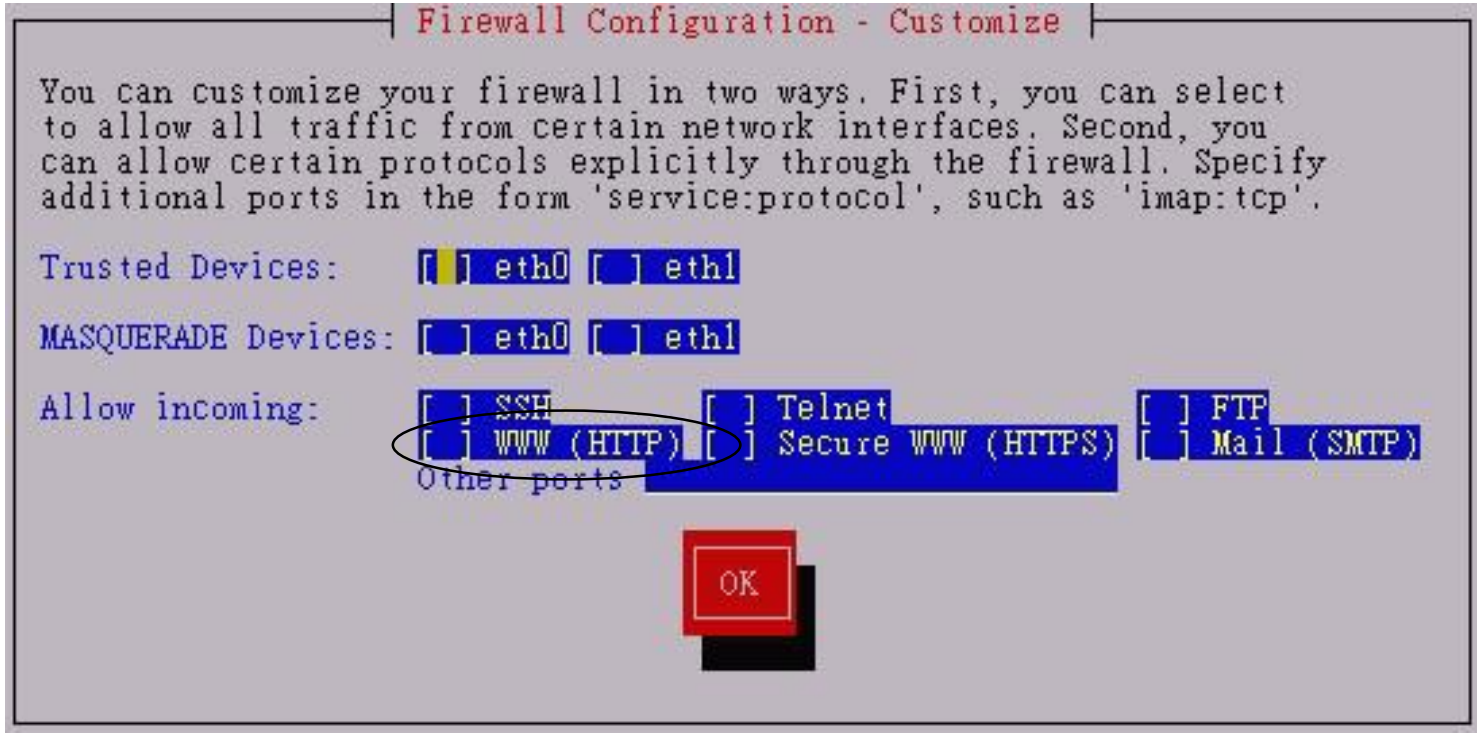


图10-1 防火墙配置

步骤 7 ▶

启动named守护进程，开始域名解析服务。

```
# service named start
```

步骤 8 ▶

测试。

在客户端修改/etc/resolv.conf文件，将DNS服务器指向域名服务器的IP地址。只有修改了这个文件才可以用自己的机器进行域名解析。

```
# vi   /etc/resolv.conf
```

只要加上一句：

```
nameserver 172.10.1.11
```

使用nslookup命令验证DNS查询结果。

目录

本章要点

基本配置步骤：

步骤 1 ▶

按照配置主DNS服务器的步骤完成主DNS服务器的搭建。

步骤 2 ▶

在主DNS服务器上编辑named.conf文件，在options选项中，添加设置允许进行区域传输的配置项allow-transfer。

```
[root@dns2 ~]# vim  named.conf
options {
    listen-on port 53 {172.10.1.12;};
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    allow-query { any; };
    allow-transfer { 172.10.1.12; }; //指定允许传输给的IP地址
……
```

步骤 3 ▶

按照DNS服务安装中的步骤，在IP地址为172.10.1.13的服务器上安装BIND软件包。

步骤 4 ▶

在named.conf配置文件中添加“localhost.deu”辅助区域。

```
[[root@ns2 ~]# vi /var/named/chroot/etc/named.conf
……
zone "abc.edu" IN {
        type slave;
        masters { 172.10.1.11; };     //指定主域名服务器的IP地址
        file "slaves/abc.edu.zone";
};
zone "0.10.10.in-addr.arpa" IN {
        type slave;
        masters { 172.10.1.11; };
        file "slaves/172.10.1.arpa";
};
```

步骤 5 ▶

启动从服务器中的named服务程序。

步骤 6 ▶

启验证从域名服务器。在客户机中将DNS服务器设为从域名服务器；使用nslookup测试域名解析是否正常。

目录

本章要点

步骤 1 ▶

在IP地址为172.10.1.15的服务器上安装BIND软件包。

步骤 2 ▶

创建纯缓存DNS服务器的主配置文件named.conf。

```
[root@dns3 ~]# vim  /var/named/chroot/etc/named.conf
options {
    listen-on port 53 {172.10.1.15;};
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";//设置域名缓存数据库文件位置
    statistics-file "/var/named/data/named_stats.txt";//设置状态统计文件位置
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    query-source  port 53;
    allow-query { any; };
    recursion  yes;
    forwarders {172.10.1.11;};//设置将DNS请求转发到主DNS服务器的IP地址
};
```

步骤 3 ▶

启动named服务。

```
service named start
```

步骤 4 ▶

在纯缓存DNS服务器上配置防火墙，开启53端口。

步骤 5 ▶

验证纯缓存DNS服务器。将客户机的DNS服务器的IP地址设为纯缓存DNS服务器的IP地址，然后使用nslookup命令测试正向解析和反向解析的效果。

目录

本章要点

例如：若要将上节中的纯缓存DNS服务器的解析请求转发给由ISP提供的IP地址为61.134.1.4和202.106.148.1的两个DNS服务器，则只要对named.conf作以下修改便可。

```
[root@dns3 ~]# vim  /var/named/chroot/etc/named.conf
options {
  listen-on port 53 {172.10.1.15;};
  directory "/var/named";
        dump-file  "/var/named/data/cache_dump.db";
        statistics-file  "/var/named/data/named_stats.txt";
        memstatistics-file  "/var/named/data/named_mem_stats.txt";
        query-source  port 53;
        allow-query { any; };
        recursion  yes;
        forwarders { 61.134.1.4; 202.106.148.1; };
        forward  only
};
```

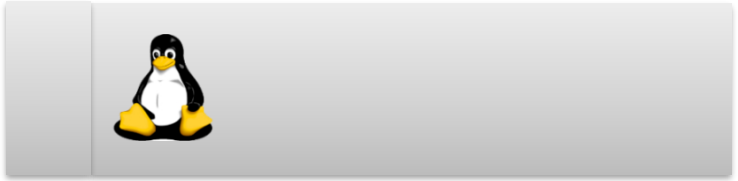
Linux操作系统及应用技术

Apache Web服务器的搭建及应用

万维网又称为**Web（World Wide Web，www）**，是在Internet上以**超文本**为基础形成的信息网。用户通过浏览器可以访问Web服务器上的信息资源，目前在Linux操作系统上最常用的Web服务器软件是**Apache**。Apache是世界使用排名第一的Web服务器软件。它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，是最流行的Web服务器端软件之一。它快速、可靠并且可通过简单的**API扩充**，将Perl/Python等解释器编译到服务器中。本节将简单介绍Web服务器的**历史**以及**工作原理**，并介绍Apache的**特点**以及它的**功能模块**。

目录

本章要点



11.1.1 Web服务的历史和工作原理

Internet上最热门的服务之一就是**万维网**，它是在因特网上以超文本为基础形成的信息网。用户通过它可以查阅Internet上的信息资源，例如，平时上网使用浏览器访问网站信息就是最常见的应用。Web在1989年起源于欧洲的一个**国际核能研究院**中，随着研究的深入和发展，研究院里的文件数量越来越多，而且人员流动也很大，要找到相关的最新的资料非常困难。于是一个科学家就提出了这样一个建议：在服务器上维护一个**目录**，目录的链接指向每个人的文件；每个人维护自己的文件，保证别人访问的时候总是**最新的文档**，这个建议得到采纳并被不断完善后，最终形成如今Internet上最常见的**WWW服务。**

11.1.1 Web服务的历史和工作原理

Web系统是**客户/服务器模式（C/S）**的，所以有服务器端和客户端程序两部分。常用的服务器有Apache、IIS等，常用的客户端浏览器有如IE、Netscape、Mozilla等，用户通过在浏览器的地址栏中输入统一资源定位地址（URL）来访问Web页面。

Web页面是**以超文本标记语言（HTML）**进行编写，它使得文本不再是传统的书页式文本，而是可以在浏览过程中从一个页面位置跳转到另一个页面。使用HTML语言编制的Web页面除文本信息外，还可以嵌入声音、图像、视频等多媒体信息。

11.1.1 Web服务的历史和工作原理

WWW服务遵循HTTP协议，默认的端口为80，Web客户端与Web服务器的通信过程如图11-1所示。

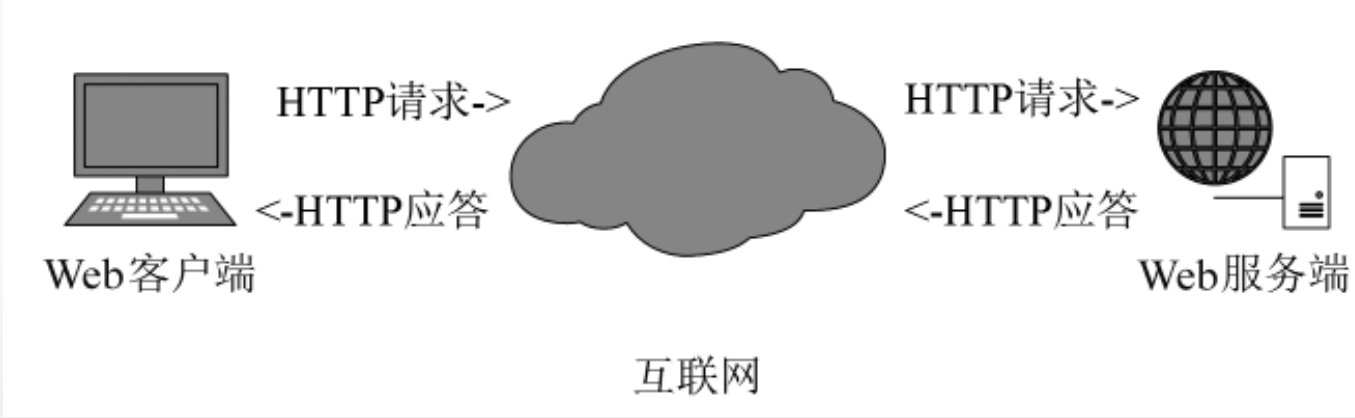


图11-1 Web工作原理

通信的过程分为以下3步：

（1）Web客户端通过浏览器根据用户输入的URL地址连接到相应的Web服务器上。

（2）从Web服务器上获得指定的Web文档。

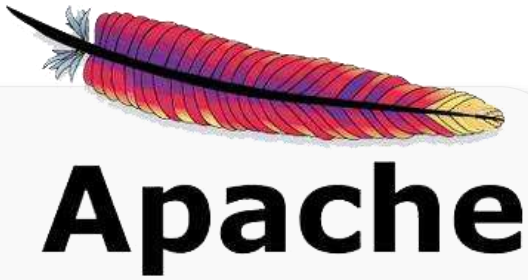
（3）断开与远程Web服务器的连接。用户每次浏览网站获取一个页面，都会重复上述的连接过程，周而复始。

11.1.2 Apache简介

Apache是一种开源的**HTTP服务器软件**，可以在包括UNIX、Linux以及Windows在内的大多数主流计算机操作系统中运行，由于其支持多平台和良好的安全性而被广泛使用。

Apache由伊利诺伊大学Urbana-Champaign的国家高级计算程序中心开发，它的名字取自a patchy server的读音，即充满补丁的服务器，可见在最初的时候该程序并不是非常完善。但由于Apache是开源软件，所以得到了开源社区的支持，不断开发出新的功能特性，并修补了原来的缺陷。经过多年来不断地完善，如今的Apache已是最流行的**Web服务器端软件**之一。

11.1.2 Apache简介



Apache拥有众多的特性，保证了它可以高效稳定地运行：

- 支持几乎所有的计算机平台。
- 简单有效的配置文件。
- 支持虚拟主机。
- 支持多种方式的HTTP认证。
- 集成Perl脚本语言。
- 集成代理服务器模块。
- 支持实时监视服务器状态和定制服务器日志。
- 支持服务器端包含指令（SSI）。
- 支持安全Socket层（SSL）。
- 提供用户会话过程的跟踪。
- 支持PHP。
- 支持FastCGI。
- 支持Java Servlets。
- 支持通用网关接口。
- 支持第三方软件开发商提供的功能模块。

目录

本章要点

11.2.1 Apache安装方法

Apache安装方法有以下两种：

- 利用源代码编译安装
- 利用RPM软件包安装

RHEL7.2自带httpd-2.4.6，Apache版本的更新一般要快于Linux内核的更新，要下载新的Apache版本，可到以下网站下载。

（1）http://updates.redhat.com

（2）http://www.apache.org

Apache网站下载画面如图11-2所示。

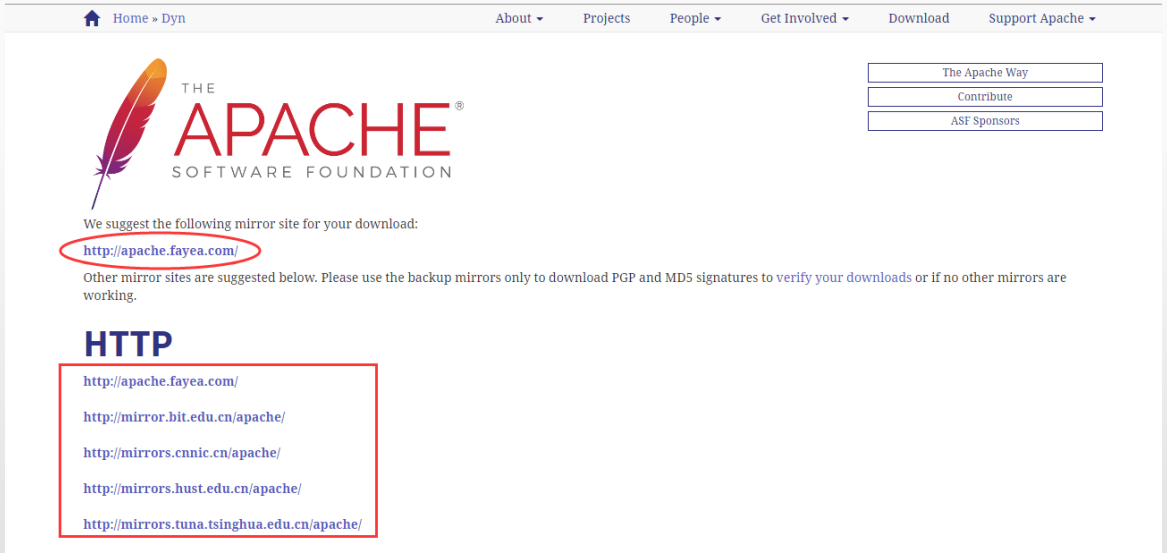


图11-2 Apache网站下载画面

11.2.1 Apache安装方法

安装步骤：

步骤 1 ▶

查询是否安装了Apache软件包 **# rpm –qa | grep httpd**

如果输出显示了Apache软件包名称“httpd-2.4.6-40.el7”，就说明已经安装了软件。

步骤 2 ▶

检查是否运行了httpd进程。 **#ps ax | grep httpd** **查看系统的进程**

11.2.1 Apache安装方法

步骤 3 ▶

安装Apache软件包（RHEL7.2）

```
# mount   /dev/cdrom   /mnt
# rpm  -ivh  /mnt/Packages/httpd-2.4.6-40.el7.x86_64.rpm
warning: /mnt/Packages/httpd-2.4.6-40.el7.x86_64.rpm: Header
V3 DSA signature:
NOKEY, key ID 37017186
error: Failed dependencies:
      libapr-1.so.0 is needed by httpd-2.4.6-40.el7.x86_64
      libaprutil-1.so.0 is needed by httpd-2.4.6-40.el7.x86_64
```

11.2.1 Apache安装方法

步骤 3 ▶

以上显示说明：httpd-2.4.6-40.el7.x86_64.rpm包的安装依赖于以下两个包：

apr-1.4.8-3.el7.x86_64.rpm
apr-util-1.5.2-6.el7.x86_64.rpm

而apr-util-1.5.2-6.el7.x86_64.rpm包的安装又依赖于：

postgresql-libs-9.2.13-1.el7_1.x86_64.rpm

为此，要先安装依赖关系的包，再安装被依赖的包，其安装顺序如下：

a) # rpm -ivh /mnt/Packages/apr-1.4.8-3.el7.x86_64.rpm
b) # rpm -ivh /mnt/Packages/postgresql-libs-9.2.13-1.el7_1.x86_64.rpm
c) # rpm -ivh /mnt/Packages/apr-util-1.5.2-6.el7.x86_64.rpm
d) # rpm -ivh /mnt/Packages/httpd-2.4.6-40.el7.x86_64.rpm
e) # rpm -qa | grep httpd
f) httpd-2.2.3-31.el5

11.2.1 Apache安装方法

安装步骤：

因为Web服务要通过**TCP协议**的80端口对外通信，如果安装了防火墙，请停止iptables服务或者用以下命令打开Web服务的默认端口80。

```
# iptables -I INPUT  -p tcp  --dport 80 -j  ACCEPT
```

步骤 4 ▶

（4）Apache软件包安装后的目录和文件位置

```
#rpm –ql httpd|more
```

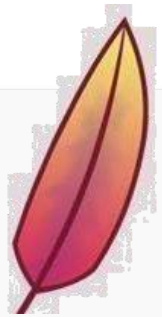
11.2.1 Apache安装方法

Apache软件包安装后的目录和文件位置如表11-1所示。

表11-1 目录表

描 述	目 录
主配置文件	/etc/httpd/conf/httpd.conf
启动脚本文件	/etc/rc.d/init.d/httpd（rpm安装时） /usr/sbin/apachectl（编译安装时）
网页目录	httpd.conf中DocumentRoot项设置设置： /var/www/html
访问日志文件	/var/httpd/logs/access_log
错误日志文件	/var/httpd/logs/error_log

11.2.1 Apache安装方法



步骤 5 ▶

启动和关闭Apache服务器

启动

```
service  httpd  start
```

重新启动

```
service  httpd  restart
```

重新装载httpd.conf配置文件的内容

```
service  httpd  reload
```

关闭

```
service  httpd  stop
```

设置自动启动

```
chkconfig  --level  35  httpd  on
```

11.2.1 Apache安装方法

当确认Apache服务启动后，可以在浏览器里输入以下地址，若可看到默认首页，则工作正常，如图11-3所示。

http://ip **或者** **http://127.0.0.1**

还可以自己建立一个网页测试Apahce。

```
#echo" Welcome to www.Linux.com!!
" >>/var/www/html/index.html
```

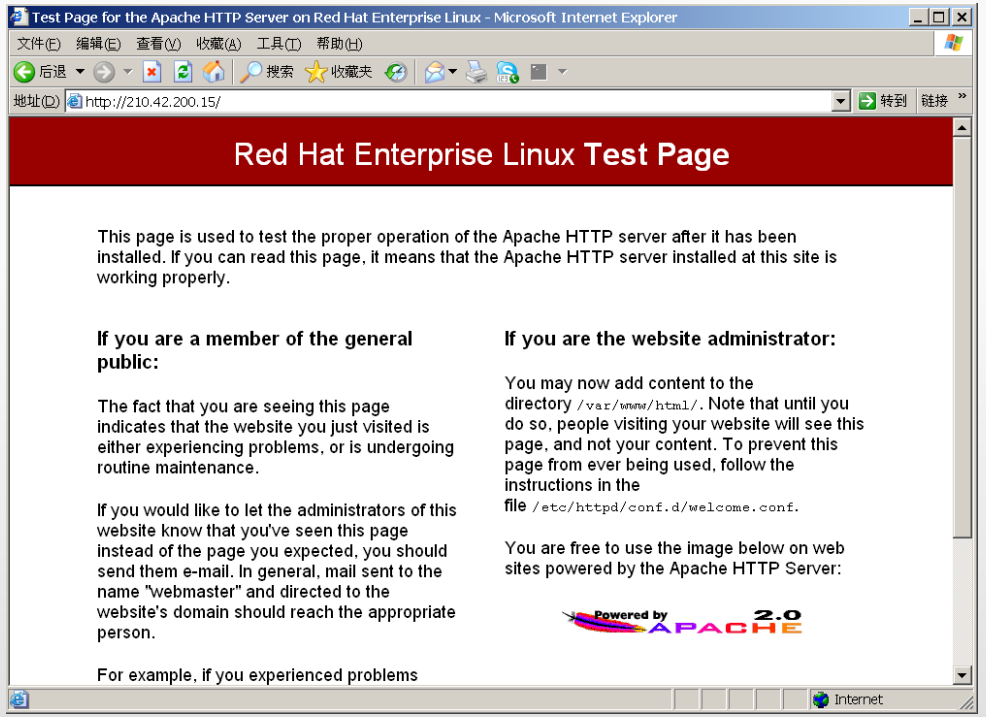


图11-3 测试结果图

11.2.2 认识Apache的目录和文件

1 Apache的主要目录和文件

Apache的主要目录和文件如表11-2所示。

表11-2 Apache的主要目录和文件用途

目录和文件	作用
/etc/httpd/	服务目录
/etc/httpd/conf/httpd.conf	主配置文件
/var/www/html/	网页目录
/var/log/httpd/access_log	访问日志
/var/log/httpd/error_log	错误日志
/etc/httpd/conf.d/welcome.conf	默认欢迎页面

11.2.2 认识Apache的目录和文件

2 主配置文件简介

配置文件是包含**若干指令的纯文本文件**。默认安装位于/etc/httpd/conf/httpd.conf目录，若安装tar.gz版本位于/usr/local/apache/conf目录。配置文件改变后，重启后生效。

每一行包含一个指令，在行尾使用**反斜杠“\”**可以表示续行，但是反斜杠与下一行之间不能有任何其他字符（包括空白字符）。

配置文件由三个部分组成：

- **全局环境设置：**主要作为一个整体来控制Apache服务器进程的标识。
- **主（默认）服务器设置：**响应虚拟主机不能处理的请求。
- **虚拟主机的设置：**配置不同IP地址、不同域名、不同端口号的多个站点。

11.2.2 认识Apache的目录和文件

Apache配置文件的格式如图11-4所示。

- 注释行——第一个字符为“#”符号的
- 指令行：与shell命令类似的命令
- 伪HTML标记

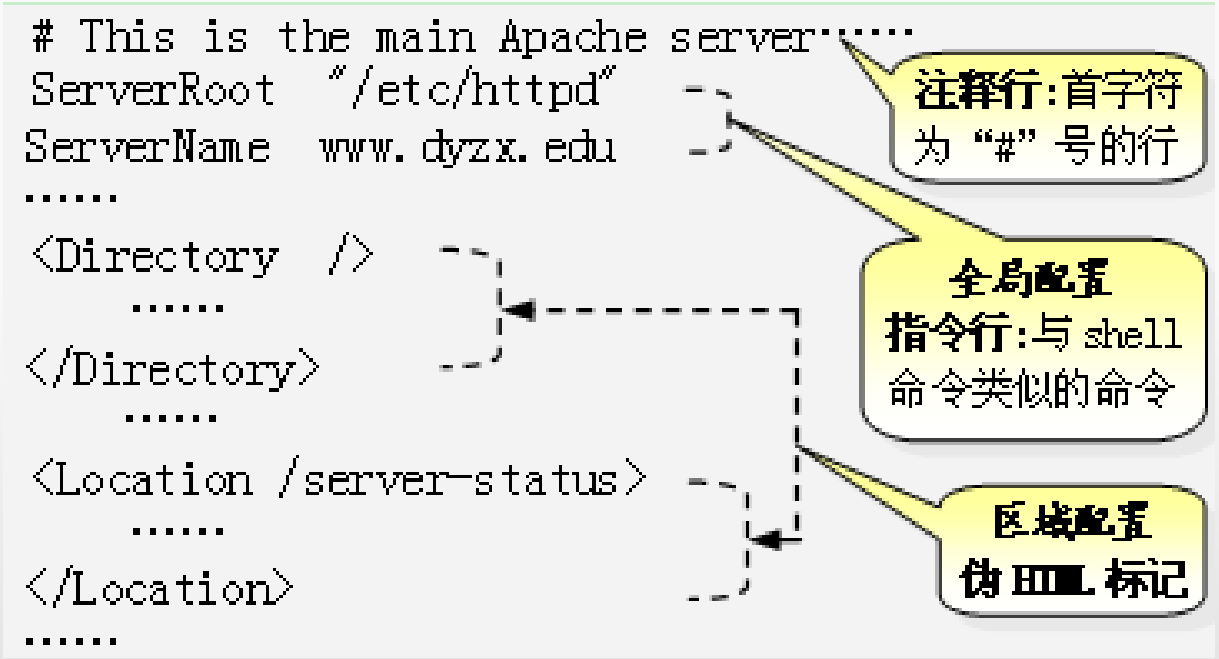


图11-4 Apache配置文件的格式

11.2.2 认识Apache的目录和文件

与HTML不同，伪HTML标记必须**各占一行**，我们可以像下面那样将命令组成一组放在某个伪HTML标记中。

```
<Directory / >
    Options FollowSymLinks
    AllowOverride All
</Directory >
```

在Apache配置文件中有很多类似这样的模块。

输入如下命令：可去掉所有注释行，只显示指令行

```
#grep  –v   "#"   /etc/httpd/conf/httpd.conf
```

输入如下命令可以计算并显示文件包含的行数：

```
# wc    –l      /etc/httpd/conf/httpd.conf
```

httpd.conf中的全局配置如表11-3所示。

11.2.2 认识Apache的目录和文件

表11-3 httpd.conf中的全局配置

设置项	说 明
ServerRoot	设置Apache服务器的根（Root）目录ServerRoot "/etc/httpd"
PidFile	设置保存httpd进程号（PID）的文件PidFile run/httpd.pid
Timeout	设置Web服务器与浏览器之间网络连接的超时秒数Timeout 120
KeepAlive	设置为Off时服务器不使用保持连接功能，传输的效率比较低；设置为On时，可以提高服务器传输文件的效率，建议设置保持连接功能有效KeepAlive Off
MaxKeepAliveRequests	每次连接最多请求文件数（当KeepAlive为On时，设置客户端每次连接允许请求响应的最大文件数，默认设置为100个文件）MaxKeepAliveRequests 100

11.2.2 认识Apache的目录和文件

表11-3 httpd.conf中的全局配置

设置项	说 明
KeepAliveTimeout	保持连接状态时的超时时间KeepAliveTimeout 15
Listen	设置服务器监听的IP地址、端口号Listen 80
Include	需要包含进来的其他配置文件Include conf.d/*.conf
User	运行服务的用户身份 User apache
Group	运行服务的组身份 Group apache

11.2.2 认识Apache的目录和文件

设置项	说 明
ServerAdmin	设置管理员的邮箱ServerAdmin root@localhost
ServerName	设置网站服务器的域名（完全合格域名）#ServerName www.example.com：80
DocumentRoot	设置网页文档的根目录DocumentRoot "/var/www/html"
DirectoryIndex	默认首页的网页的文件名DirectoryIndex index.html index.html.var
ErrorLog	错误日志文件的位置（路径和文件名）ErrorLog logs/error_log
CustomLog	访问日志文件的位置（路径和格式类型）#CustomLog logs/access_log common

11.2.2 认识Apache的目录和文件

说明

（1）**ServerRoot "/etc/httpd"**

用来设置服务器的根目录——Apache配置文件和日志文件的基础目录。也就是和Apache服务器相关的文件的基础目录。

（2）**#ServerName www.example.com:80**

用于设置服务器的FQDN，如果服务器的名字解析有问题（通常为反向解析不正确），或者没有正式的DNS名字，也可以在这里指定IP地址。

（3）**#Listen 12.34.56.78:80**

Listen 80

可以指定服务器除了监视标准的80端口之外，还监视其他端口的HTTP请求。

11.2.2 认识Apache的目录和文件

Apache启动时，会绑定本机上的某些**地址和端口**，并等待请求进入。缺省情况下，它会监听本机的所有地址。但是，要监听指定的地址和端口或者某种组合，尤其是在使用虚拟主机，对不同的IP、主机名和端口做出不同响应时，则必须明确指出。

Listen指令告诉服务器接受来自指定端口或者地址+端口的请求。如果Listen指令仅指定了端口，服务器会监听所有的地址；如果指定了**地址+端口**，则服务器只监听来自此地址和端口的请求。

多个Listen指令，可以指定多个地址和端口，例如：使服务器接受来自端口80和8000的请求，可以这样写：

```
Listen 80
Listen 8000
```

接受来自两个指定的地址+端口：

```
Listen 192.170.2.1:80
Listen 192.170.2.5:8000
```

11.2.2 认识Apache的目录和文件

（4）**ServerAdmin root@localhost**

用于配置Web服务器的管理员的**E-mail地址**。出现错误的条件下返回给**浏览器**，以便让Web使用者和管理员联系，报告错误。习惯上使用服务器上的webmaster作为WWW服务器的管理员，通过邮件服务器的别名机制，将发送到webmaster的电子邮件发送给真正的**Web管理员**。

（5）**DocumentRoot "/var/www/html"**

定义网页文档存放的路径，包括：

- 目录下的网页文件
- 子目录
- 符号连接文件和目录

11.2.2 认识Apache的目录和文件

（6）#ErrorDocument 错误号 所要显示的网页

用于定义当遇到错误时，服务器将给客户端什么样的回应，通常是显示预设置的一个错误页面。

ErrorDocument 400 /error / HTTP_BAD_REQUEST.html.var

（7）DirectoryIndex index.html index.html.var

用于设置站点主页文件的搜索顺序，各文件名间用空格分隔。排在前面的文件优先。

如：DirectoryIndex index.php index.html index.html.var

11.2.2 认识Apache的目录和文件

（8）User Apache和Group Apache

User和Group配置是Apache的**安全保证**，Apache在打开端口之后，就将其本身设置为这两个选项所设置的用户和组的权限然后进行运行，这样就降低了服务器的危险性。这个选项也只用于Standalone模式。缺省置为**nobody和nogroup**，这个用户和组在系统中不拥有文件，保证了服务器本身和由它启动的CGI进程没有权限更改文件系统。

（9）AddDefaultCharset　UTF-8

为发送出的所有页指定默认的**字符集**。简体中文使用的字符集为GB2312，所以可以设为：

AddDefaultCharse GB2312

11.2.2 认识Apache的目录和文件

（10）**ServerType standalone | inet**

定义服务器的启动方式：

standalone方式（独立方式，缺省值）：自身管理自己的启动进程，并驻留在主机中监视连接请求。启动文件/etc/rc.d/rc.local/init.d/apache中自动启动Web服务器，这种方式是推荐设置。

inet方式：使用超级服务器inetd监视连接请求并启动服务器。当需要使用inetd启动方式时，便需要更改为这个设置，并屏蔽/etc/rc.d/rc.local/init.d/apache文件，以及更改/etc/inetd.conf并重起inetd，那么Apache就能从inetd中启动了。

11.2.2 认识Apache的目录和文件

两种方式的区别：

- **独立方式**能立即启动服务器的多个副本，每个副本都驻留在内存中，一有连接请求不需要生成子进程就可以立即进行处理，对于客户浏览器的请求反应更快，性能较高。

- **inet方式**要由inetd发现有连接请求后才去启动http服务器，由于inetd要监听太多的端口，因此反应较慢、效率较低，但节约了没有连接请求时**Web服务器**占用的资源。只用于偶尔被访问并且不要求访问速度的服务器上，不适合http的突发和多连接的特性。因为一个页面可能包含多个图象，而每个图象都会引起一个连接请求，即使虽然访问人数较少，但瞬间的连接请求并不少，这就受到inetd性能的限制，甚至会影响由inetd启动的其他服务器程序。

11.2.2 认识Apache的目录和文件

3 性能配置命令

Timeout 300：

◆ （1）持续连接配置

定义客户程序请求连接服务器的超时间隔，超过这个时间间隔（秒）后服务器将断开与客户机的连接。

KeepAlive On|off：

启用或禁用持续的连接，设为On，以便提高访问性能。

MaxKeepAliveRequests 100：

用于在一次持续连接期间可以进行的HTTP请求的最大请求次数。将其值设为0，将支持在一次连接内进行无限次的传输请求。事实上没有客户程序在一次连接中请求太多的页面，通常达不到这个上限就完成连接了。

KeepAliveTimeout 15：

用于测试一次连接中的多次请求传输之间的时间（秒），如果服务器已经完成了一次请求，但一直没有接收到客户程序的下一次请求，在间隔超过了这个参数设置的值之后，服务器就断开连接。

11.2.2 认识Apache的目录和文件

3 性能配置命令

◆ （2）控制Apache进程

StartServers 5

用来设置httpd启动时启动的子进程副本数量。这个参数与MinSpareServers和MaxSpareServers参数相关，都是用于启动空闲子进程以提高服务器的反应速度的。它应该设置为前两个值之间的一个数值，小于MinSpareServers或大于MaxSpareServers都没有意义。

MinSpareServers 5

MinSpareServers最少的空余子进程数量。

MaxSpareServers 10

MaxSpareServers最多的空闲子进程数量，多余的服务器进程副本就会退出。

11.2.2 认识Apache的目录和文件

根据**服务器**的实际情况来进行设置，如果服务器性能较高，并且也被频繁访问，就应该增大这两个参数的设置。对于高负载的专业网站，这两个值应该大致相同，并且等同于系统支持的最多服务器副本数量，也减少了不必要的副本退出。

在使用子进程处理HTTP请求的**Web服务器**上，由于要首先生成子进程才能处理客户的请求，因此反应时间就有一点延迟。但是，Apache服务器使用了一个特殊技术来摆脱这个问题，这就是预先生成多个空余的子进程驻留在系统中，一旦有请求出现，就立即使用这些空余的子进程进行处理，这样就不存在生成子进程造成的延迟了。

11.2.2 认识Apache的目录和文件

在运行中随着客户**请求的增多**，启动的**子进程**会随之增多，但这些服务器副本在处理完一次HTTP请求之后并不立即退出，而是停留在计算机中等待下次请求。但是空余的子进程副本不能光增加不减少，太多的空余子进程没有处理任务，也占用服务器的处理能力，因此也要限制空余副本的数量，使其保持一个合适的数量，以便既能及时回应客户请求，又能减少不必要的进程数量。

MaxClients 150

服务器支持的**最多并发访问的客户数**。值设置得过大，系统在繁忙时不得不在过多的进程之间进行切换来为太多的客户进行服务，这样对每个客户的反应就会减慢，降低了整体的效率。值设置得较小，那么系统繁忙时就会拒绝一些客户的连接请求。当服务器性能较高时，可以适当增加这个值的设置。

11.2.2 认识Apache的目录和文件

对于**专业网站**，应该使用提高**服务器效率**的策略，因此这个参数不能超过硬件本身的限制，如果频繁出现拒绝访问现象，就说明需要升级服务器硬件了。

对于**非专业网站**，不太在意客户浏览器的反应速度，或者认为反应速度较慢也比拒绝连接好，也就可以略微超过硬件条件来设置这个参数。

MaxRequestsPerChild 30

定义每个子进程处理服务请求的次数。缺省的设置值为30，这个值对于具备高稳定性特点的Linux系统来讲是过于保守的设置，实际上可以设置为1000甚至更高，设置为0时支持每个副本进行无限次的服务处理

11.2.2 认识Apache的目录和文件

使用子进程的方式提供服务的**Web服务**，常用的方式是一个子进程为一次连接服务，这样造成的问题就是每次连接都需要生成、退出子进程的**系统操作**，使得这些额外的处理过程占据了计算机的大量处理能力。因此，最好的方式是**一个子进程可以为多次连接请求服务**，这样就不需要这些生成、退出进程的系统消耗。Apache就采用了这样的方式，一次连接结束后，子进程并不退出，而是停留在系统中等待下一次服务请求，这样就极大地提高了性能。

由于在处理过程中子进程要不断地申请和释放内存，次数多了就会造成一些内存垃圾，会影响系统的稳定性，并且影响系统资源的有效利用。因此在一个副本处理过一定次数的请求之后，就可以让这个子进程副本退出，再从原始的httpd进程中重新复制一个干净的副本，这样就能提高系统的稳定性。

11.2.2 认识Apache的目录和文件

4 日志配置命令

（1）ErrorLog logs/error_log

用来指定服务器存放错误日志文件的位置和文件名

（2）LogLevel warn

用于设置记录错误日志中的详细程度，其级别和含义如表11-4所示

表11-4 错误日志的级别与含义（降序排列）

级别名称	含义
emerg	紧急，系统将无法使用
alert	必须立即采取措施
crit	致命情况
error	错误情况
warn	紧告情况
motice	一般重要情况
info	普通信息
debug	出错级别信息

11.2.2 认识Apache的目录和文件

（3）LogFormat、CustomLog

LogFormat用于定义日志文件的记录格式，有以下4种格式：

- LogFormat "%h %l %u %t \"%r \" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
- LogFormat "%h %l %u %t \"%r \" %>s %b" common
- LogFormat "%{Referer}i -> %U" referer
- LogFormat “%{User-agent}i” agent

日志格式主要用于指定要记录的信息以及彼此之间的排列顺序。

 # CustomLog logs/access_log common

用于指定access_log日志文件的位置和日志记录的格式，access_log日志文件用于记录服务器处理的所有请求。

11.2.2 认识Apache的目录和文件

5 容器与访问控制命令

可以在容器指令内配置不同对象的各种访问控制。

容器指令的语法：

包括在<>……</>括号内

常用的容器指令有：

(1) <Directory>……</Directory>
(2) <Files>……</Files>
(3) <Location>……</Location>
(4) <VirtualHost>……</VirtualHost>

11.2.2 认识Apache的目录和文件

6 其他配置命令

（1）**htaccess文件：**该文件中可放置一些配置命令，以作用于该文件所在的目录及其下的所有子目录；该文件可位于多个目录中，以分别对这些目录进行控制。

（2）**Options命令：**用于控制在特定目录中将使用哪些服务器特性，通常用在<Directory>容器中。Options指令后可以附加指定多种服务器特性，特性选项之间以空格分隔。可以附加的特性选项的具体作用及含义如表11-5所示。

表11-5 功能选项列表

选项	功能描述
None	不启用任何额外特性，所有的目录特性都无效
All	所有的目录特性都有效，这是缺省状态
ExecCGI	允许执行CGI程序
FollowSymLinks	允许在此目录中使用符号连接。在<Location>段中无效
Indexes	允许浏览器可以生成这个目录下所有文件的索引，使得在这个目录下没有index.html（或其他索引文件）时，能向浏览器发送这个目录下的文件列表

11.2.2 认识Apache的目录和文件

【例11-1】学校内部搭建一台**Web主服务器**，采用的IP地址为172.16.102.61，端口号为80，首页采用index.html文件，管理员E-mail地址为root@localhost.edu，网页的编码类型采用UTF-8，所有网站资源都存放在/var/www/html目录下，并将Apache的根目录设置为/etc/httpd目录。

11.2.2 认识Apache的目录和文件

步骤 1 ▶

修改主配置文件httpd.conf。

```
[root@localhost ~]# vim /etc/httpd/conf/httpd.conf
ServerRoot "/etc/httpd"              //设置Apache的根目录为/etc/httpd
Timeout 120                          //设置客户端访问超时时间为120秒
Listen 80                            //设置httpd监听端口80
ServerAdmin  root@localhost                  //设置管理员E-mail地址为
root@localhost.com
ServerName  172.16.102.61:80       //设置Web服务器的主机名和监听端口
DocumentRoot  "/var/www/html" //设置网页文档的主目录为/var/www/html
DirectoryIndex  index.html         //设置主页文件为index.html
AddDefaultCharset  UTF-8         //设置服务器的默认编码为UTF-8
```

11.2.2 认识Apache的目录和文件

步骤 2 ▶

将制作好的网页文档存放在目录/var/www/html中，测试用首页建立如下：

```
[root@localhost ~]# echo "Welcome to德雅职业学校网站"
>/var/www/html/index.html
```

步骤 3 ▶

重新启动httpd服务。

```
[root@localhost ~]# service httpd restart
```

步骤 4 ▶

测试。在浏览器地址栏中输入“http://172.16.102.61”，便可访问首页。

目录

本章要点

拟目录有以下优点：

（1）便于访问。

（2）便于移动站点中的目录。

（3）能灵活加大磁盘空间。

（4）安全性好。

使用Alias选项可以创建虚拟目录。

【例11-2】在创建的Web网站的基础上，通过虚拟目录为“信息工程系”建立子站点，配置参数如表11-6所示。

名称	虚拟目录别名	物理路径	IP地址
学校网站		/var/www/html/	172.16.102.61
信息工程系	/xxgcx	/localhost/xxgc/	

步骤 1 ▶

创建物理目录路径及虚拟目录默认首页文件。

```
[root@localhost ~]# mkdir  -p /localhost/xxgc
[root@localhost ~]# echo  "Welcome to信息工程系主页" > /localhost/xxgc/index.html
```

步骤 2 ▶

重新启动httpd服务。

```
[root@localhost ~]# vim  /etc/httpd/conf/httpd.conf
```

//在文件末尾添加以下行

```
Alias  /xxgcx  "/localhost/xxgc"
```

步骤 3 ▶

若开启SELinux，则临时禁用。

```
[root@localhost ~]# setenforce 0
```

步骤 4 ▶

重新启动httpd服务。

```
[root@localhost ~]# service  httpd  restart
```

步骤 5 ▶

测试。在浏览器地址栏中输入“http://172.16.102.61/xxgcx”便可访问，结果如图11-5所示。

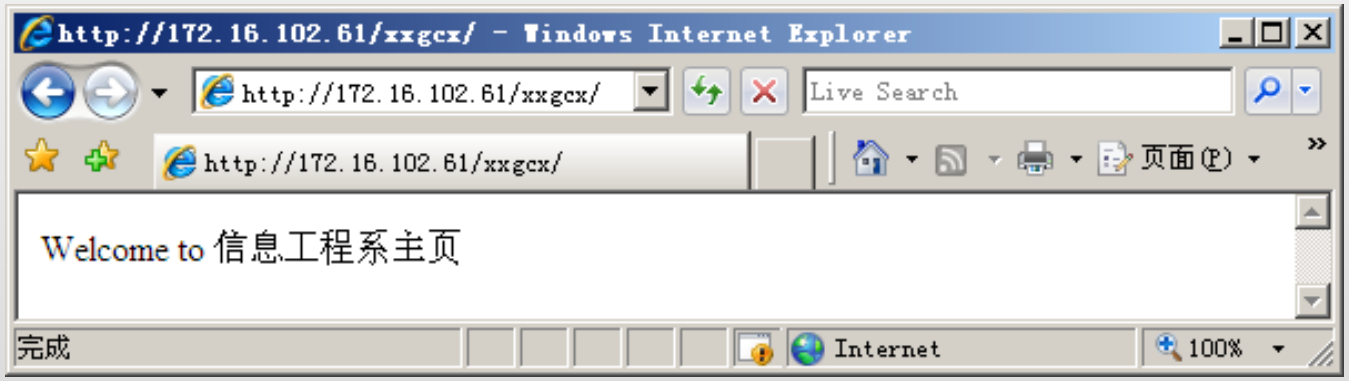


图11-5 访问结果

目录

本章要点

虚拟主机是在一台服务器上运行多个**Web站点**。设定虚拟主机的方式有以下3种：

基于名称的虚拟主机

只需服务器有一个IP地址即可，所有的虚拟主机共享同一个IP，各虚拟主机之间通过域名进行区分。但需要新版本的HTTP 1.1浏览器支持。这种方式已经成为建立虚拟主机的标准方式。

基于IP的虚拟主机

需要在服务器上绑定多个IP地址，然后配置Apache，将多个网站绑定在不同的IP地址上，访问服务器上不同的IP地址，就可以看到不同的网站。

基于端口号的虚拟主机

只需服务器有一个IP地址即可，所有的虚拟主机共享同一个IP，各虚拟主机之间通过不同的端口号进行区分。在设置基于端口号的虚拟主机的配置时，需要利用Listen语句设置所监听的端口。

1 配置基于域名虚拟主机

根据表11-6所示的配置参数，搭建域名不同的两个虚拟主机。

服务器IP地址：**172.16.102.61**

两个虚拟主机的域名分别为：**www.web1.com**
www.web2.com

站点根目录：**/var/www/myweb1/**
/var/www/myweb2/

日志文件分别存放在：**/var/vhlogs/myweb1**
/var/vhlogs/myweb2

创建步骤：

1. 注册虚拟主机所要使用的域名。

实现域名解析可以有两种方法：

在客户机上通过修改/etc/hosts文件实现

这是一种比较简单的方法，只需在/etc/hosts文件中加入下面两行：

172.16.102.61　www. web1.com
172.16.102.61　www. web2.com

在DNS服务器上通过配置DNS实现

需要给每台虚拟主机创建一个CNAME，在var/named/named.hosts文件中加入下面两行：

www. web1.com　IN　CNAME　a100.redflag.com.
www. web2.com　IN　CNAME　a100.redflag.com

1 注册虚拟主机所要使用的域名。

重启DNS后，可以用nslookup和ping命令来测试，命令如下：

```
#nslookup
>set type=cname
>hosta.redflag.com
#ping www. web1.com
#ping www. web2.com
```

2 创建所需的目录和默认首页文件。

在/usr目录下创建4个目录，分别用来存放两主机的网页和日志文件。

```
# mkdir   -p   /var/www/myweb1
# mkdir   -p  /var/www/myweb2
```

-p——快速建立目录结构中指定的每个目录。

```
echo  " this is www.web1.com's web!!">> /var/www/myweb1/index.html
echo  “ this is www.web2.com ‘s web!!”  >> /var/www/myweb2/index.html
```

3 编辑/etc/httpd/conf/httpd.conf配置文件，设置Listen侦听端口。

Listen 80

4 在httpd.conf文件最后添加虚拟主机的定义。

NameVirtualHost 172.16.102.209

5 编辑/etc/httpd/conf/httpd.conf配置文件，设置Listen侦听端口。

```
<VirtualHost 172.16.102.61 >
ServerAdmin     webmaster@web1.com
DocumentRoot    /var/www/myweb1
ServerName      www. web1.com
ErrorLog logs  logs/myweb1 /error_log
CustomLog       logs/myweb1 /access_log  common
</VirtualHost>

<VirtualHost 172.16.102.61 >
ServerAdmin     webmaster@web1.com
DocumentRoot    /var/www/myweb1
ServerName      www. web2.com
ErrorLog logs  logs/myweb2 /error_log
CustomLog    logs/myweb2 /access_log  common
</VirtualHost>
```

6 重新启动httpd服务。

```
service  httpd  restart
```

7 切换到图形界面，启动浏览器，在地址栏键入各自的域名，观察各自的页面能否显示在客户端看到的访问界面。

2 配置基于IP地址的虚拟主机

① 为一块网卡绑定多个IP地址

```
# cd   /etc/sysconfig/network-scripts
# cp  ifcfg-eth0   ifcfg-eth0:0
# vi   ifcfg-eth0:0
DEVICE=eth0:0
IPADDR=172.16.102.121
# ifdown eth0      //禁用网卡
# ifup eth0:0      //启用网卡
# ifup eth0
```

② 注册虚拟主机所使用的域名

```
#vi  /etc/hosts
```

增加两行：

```
172.16.102.61
www.myLinux1.com
172.16.102.121
www.myLinux2.com.
```

③ 创建web站点根目录和默认首页文件

在/usr目录下创建两个目录，分别用来存放两主机的网页：

```
# mkdir   -p   /var/www/ip2     /var/www/ip3
#echo " this is 172.16.102.61's web!!">>/var/www/ip2 /index.html
# echo " this is 172.16.102.121's web!!">>/var/www/ip3/index.html
```

④ 编辑/etc/httpd/conf/httpd.conf配置文件，保证有以下Listen指令

```
Listen 80
```

⑤ 配置虚拟主机

```
<VirtualHost  172.16.102.61>
ServerName    www.myLinux1.com
DocumentRoot  /var/www/ip2
</VirtualHost>

<VirtualHost 172.16.102.121>
ServerName    www.myLinux2.com
DocumentRoot   /var/www/ip3
</VirtualHost>
```

⑥ 测试

重新启动httpd服务，切换到图形界面，启动浏览器，在地址栏键入各自的域名，然后观察各自的页面能否显示。

3 配置基于端口号的虚拟主机

举例：

假设服务器IP地址为172.16.102.61，创建基于8000和8800两个不同端口号的虚拟主机，要求不同的虚拟主机对应的主目录不同，默认文档的内容也不同。

① 分别创建两个主目录和两个默认文件。

```
# mkdir   /var/www/port1                /var/www/port2
#echo "this is port8000's      web!!">>/var/www/port1 /index.html
# echo  “this is port8800  ‘s web!!”  >>/var/www/port2/index.html
```

② 在httpd.conf文件中，设置基于端口号的虚拟主机，配置内容如下。

```
Listen   8000
Linten   8800
<VirtualHost  172.16.102.61:8000 >
ServerName    www.myLinux1.com
DocumentRoot  /var/www//port8000
</VirtualHost>

<VirtualHost 172.16.102.61: 8800 >
ServerName    www.myLinux2.com
DocumentRoot   /var/www//port8800
</VirtualHost>
```

③ 重新启动httpd服务。

④ 在客户端访问。

目录

本章要点

1 基于用户的访问控制

建立**Web服务器**，并根据以下要求配置Web服务器。

（1）设置主目录的路径为/var/www/web。

（2）添加index.jsp文件作为默认文档。

（3）设置Apache监听的端口号为8888。

（4）设置默认字符集为GB2312。

（5）建立一个名为temp的**虚拟目录**，其对应的物理路径是/usr/local/temp，并配置Web服务器允许该虚拟目录具备目录浏览和允许内容协商的多重视图特性。仅允许来自网络172.16.102.0/24客户机的访问。

（6）建立一个名为private的虚拟目录，其对应的物理路径是/usr/local/private，并配置Web服务器对该虚拟目录启用用户认证，只允许用户名为abc和xyz的用户访问。

```
[root@localhost ~]# mkdir  /var/www/web
[root@localhost ~]# mkdir  /usr/local/temp
[root@localhost ~]# mkdir  /usr/local/private
[root@localhost ~]# htpasswd  -c /etc/httpd/mycreatpwd abc
[root@localhost ~]# htpasswd  /etc/httpd/mycreatpwd xyz
```

注意

mycreatpwd的文件的权限，只需要设置成apaceh用户能访问就OK，而且尽可能不要放在网站的目录下，防止被下载。

配置httpd.conf：

```
root@localhost ~]# vim /etc/httpd/conf/httpd.conf
DocumentRoot "/var/www/web"
DirectoryIndex index.jsp
Litsen 8888
AddDefaultCharset GB2312
Alias /temp "/usr/local/temp/"
<Directory "/usr/local/tmp">
        Options Indexes MultiViews
        Order allow,deny
        Allow from 10.0.0.0/8
</Directory>
```

配置httpd.conf：

```
Alias /private "/usr/local/private/"
<Directory "/usr/local/private">
        AuthType Basic
        AuthUserFile /etc/httpd/mycreatpwd
        AuthName "this is private directory,please Login:"
        Require user abc xyz
        AllowOverride None
        Order allow,deny
         Allow from all
</Directory>
```

2 基于客户端地址的访问控制

Order配置项，用于定义控制顺序。

- 先允许后拒绝，默认拒绝所有：Order allow,deny
- 先拒绝后允许，默认允许所有：Order deny,allow

例如：

```
Deny from address1 address2 ...
Allow from address1 address2 ...
<Directory  /usr/local/apache2/htdocs>
    Order allow,deny
    Allow from 192.168.0.0/24
    Deny from 192.168.0.100
</Directory>
```

目录

本章要点

在**Apache服务器**中，为系统用户wang5设置个人主页空间。该用户的家目录为/home/wang5，个人主页空间所在的目录为public_html。

步骤 1 ▶

创建wang5系统用户，修改其家目录权限，使其他用户具有读和执行的权限文件。

```
[root@localhost ~]# useradd  wang5
[root@localhost ~]# passwd  wang5
[root@localhost ~]# chmod o+x /home/wang5/     //添加权限
```

步骤 2 ▶

创建wang5系统用户，修改其家目录权限，使其他用户具有读和执行的权限文件。

```
[root@localhost ~]# mkdir  /home/wang5/public_html/
[root@localhost ~]# echo  "this is wang5’ s web!">/home/wang5/public_html/index.html
```

步骤 3 ▶

修改httpd.conf文件，启用个人主页功能。

```
[root@localhost ~]# vim  /etc/httpd/conf/httpd.conf
......
#UserDir  disable                          //若存在此行，应注释掉以开启个人主页功能
......
UserDir  public_html                                  //设置用户的主页存放的目录
<Directory  "/home/*/public_html">                    //确认目录区域设置
    AllowOverride none
    Options none
    Order allow,deny
    Allow from all
</Directory>
```

步骤 4 ▶

重启httpd服务，在客户端的浏览器中输入："http://172.16.102.61/~wang5"

Linux操作系统及应用技术

MySQL数据库服务器的搭建及应用

MySQL是一个**关系型数据库管理系统**，由瑞典MySQL AB公司开发，目前属于Oracle旗下公司。MySQL最流行的关系型数据库管理系统，在Web应用方面MySQL是最好的RDBMS（Relational Database Management System，关系数据库管理系统）应用软件之一。

MySQL所使用的**SQL语言**是用于访问数据库的最常用标准化语言，由于其体积小、速度快、总体拥有成本低，尤其是开放源码这一特点，一般中小型网站的开发都选择MySQL作为网站数据库。MySQL软件采用了**双授权政策**，它分为社区版和商业版，其社区版的性能卓越，搭配PHP和Apache可组成良好的开发环境。

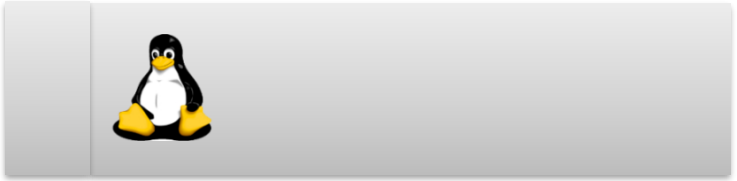
目录

本章要点

12.1.1 数据库服务器的基本概念

下面我们先来了解几个与服务器有关的基本概念：

- **数据库（DataBase）**：是依照某种数据模型组织起来并存放二级存储器中的数据集合。这种数据集合具有如下特点：尽可能**不重复**，以最优方式为某个特定组织的多种应用服务，其数据结构独立于使用它的应用程序，对数据的增、删、改、查由统一软件进行管理和控制。



12.1.1 数据库服务器的基本概念

数据库管理系统（DataBase Management System）：是一种操纵和管理数据库的大型软件，用于建立、使用和维护数据库，简称DBMS。它对数据库进行统一的管理和控制，以保证数据库的安全性和完整性。用户通过DBMS访问数据库中的数据，数据库管理员也通过dbms进行数据库的维护工作。它可使多个应用程序和用户用不同的方法在同时或不同时刻去建立，修改和询问数据库。大部分DBMS提供**数据定义语言DDL（Data Definition Language）**和**数据操作语言DML（Data Manipulation Language）**，供用户定义数据库的模式结构与权限约束，实现对数据的追加、删除等操作。

12.1.1 数据库服务器的基本概念

- **数据库系统（DataBase System）**：通常由软件、数据库和数据管理员组成。其软件主要包括操作系统、各种宿主语言、实用程序以及数据库管理系统。数据库由数据库管理系统统一管理，数据的插入、修改和检索均要通过数据库管理系统进行。
- **数据库服务器（DataBase Server）**：数据库服务器建立在数据库系统基础上，具有数据库系统的特性，且有其独特的一面。

12.1.1 数据库服务器的基本概念

本章我们主要学习的就是**数据库服务器的搭建及应用**，其主要功能如下：

数据库管理功能，包括系统配置与管理、数据存取与更新管理、数据完整性管理和数据安全性管理。

数据库的查询和操纵功能，该功能包括数据库检索和修改。

本章我们主要学习的就是**数据库服务器的搭建及应用**，其主要功能如下：

数据库维护功能，包括数据导入/导出管理，数据库结构维护、数据恢复功能和性能监测。

- 数据库**并行运行**，由于在同一时间，访问数据库的用户不止一个，所以数据库服务器必须支持并行运行机制，处理多个事件的同时发生。

12.1.1 数据库服务器的基本概念

数据库分为3种基本形式：关系型数据库、层次型数据库、网状型数据库。运行在Linux系统上的关系型数据库管理系统主要产品：企业级服务器Oracle、Sybase、DB2；中小型服务器MySQL、PostgreSQL。

12.1.2 MySQL简介

总体来说，MySQL数据库管理系统具有以下主要特点：

可以运行在不同平台上，支持多用户、多线程和多CPU，没有内存溢出漏洞；

提供多种数据类型，支持ODBC、SSL、支持多种语言利用MySQL的API进行开发；

是目前市场上现有产品中运行速度最快的数据库系统；

同时访问数据库的用户数量不受限制；

可以保存超过50,000,000条记录；

用户权限设置简单、有效。

目录

本章要点

1．认识MySQL的rpm安装包

MySQL的rpm安装包文件名和功能如表12-1所示。

表12-1 MySQL的rpm安装包文件名和功能

rpm安装包文件名	功能描述
mysql-server-5.7.13-1.el7.x86_64.rpm	MySQL服务器需要的相关程序
mysql-5.7.13-1.el7.x86_64.rpm	MySQL客户端程序和共享库
mysql-devel-5.7.13-1.el7.x86_64.rpm	MySQL头文件和库文件，若数据库服务器需要提供给第三方程序（如PHP网页）读取则需安装
mysql-connector-odbc-5.2.5-6.el7.x86_64.rpm	MySQL的ODBC驱动程序。若在PHP网页中要使用ODBC方式来存取MySQL数据库则需安装
mysql-test-5.7.13-1.el7.x86_64.rpm	MySQL客户端测试实用程序
Mysql-python-1.2.3-11.el7.x86_64.rpm	用于使用MySQL数据库的PHP程序的模块

2．使用rpm包安装MySQL

使用rpm包安装MySQL的步骤如下：

步骤 1 ▶

以root身份登录到RHEL7.2系统的字符界面。

步骤 2 ▶

查看系统中是否已安装MySQL软件，若无任何显示表明未安装。

```
[root@localhost ~]# rpm -qa  *mysql*
```

步骤 3 ▶

将DVD安装光盘放入光驱，并将光驱挂载到/mnt目录中。

```
[root@localhost ~]# mount  /dev/cdrom  /mnt
mount: block device /dev/cdrom is write-protected,       mounting read-only
[root@localhost ~]# cd  /mnt/Server
```

步骤 4 ▶

由于此主机既作为服务器端又作为客户端，这里先安装MySQL的客户端安装包，该安装包的依赖软件包是perl-DBI。MySQL的服务端安装包还要依赖perl-DBD-MySQL软件包。

目录

本章要点

1 MySQL服务的启动、停止、重启和查询启动状态

命令如下：

```
service mysqld start|stop|restart|status
```

或

```
/etc/rcd/init.d/mysqld start| stop|restart|status
```

2 设置开机自动启动的功能

命令如下：

```
[root@localhost Server]# chkconfig  --list|grep mysqld
```

3 登录及退出MySQL环境

登录命令：

```
mysql -h 主机名或IP地址  -u 用户名  -p 用户密码
```

退出MySQL服务器，可在MySQL提示符后输入exit或quit命令：

```
mysql> exit
```

4 设置MySQL数据库root账号的密码

root用户默认的空口令，更改命令的格式为：

```
# mysqladmin -u root -p password 新口令
```

目录

本章要点

1．数据库管理

数据库管理中常用的命令和功能如表12-2所示。

表12-2 数据库管理中常用的命令

MySQL命令	功能
show databases;	查看服务器中当前有哪些数据库
use数据库名;	选择所使用的数据库
create database数据库名;	创建数据库
drop database数据库名;	删除指定的数据库

1．数据库管理

MySQL安装后默认会创建3个数据库**information_schema**、**mysql**和**test**，其中名为“mysql”的数据库很重要，它里面保存有MySQL的系统信息，用户修改密码和新增用户，实际上就是针对该数据库中的有关数据表进行操作的。

新建一个student的学生库，并选择该数据库作为当前数据库。

```
mysql> CREATE DATABASE student;
Query OK, 1 row affected (0.00 sec)
mysql> USE student;
Database changed
```

2．数据表结构管理

常用于数据表结构管理的命令和功能如表12-3所示。

表12-3 常用数据表结构管理的命令和功能

MySQL命令	功能
create table表名（字段设定列表）	在当前数据库中创建数据表
show tables;	显示当前数据库中有哪些数据表
describe[数据库名.]表名;	显示当前或指定数据库中指定数据表的结构（字段）信息
drop table[数据库名.]表名;	删除当前或指定数据库中指定的数据表

3．记录的查看、插入、修改与删除

常用于记录的查看、插入、修改与删除的命令和功能如表12-4所示。

表12-4 常用记录操作的命令和功能

MySQL命令	功能
insert into 表名（字段1，字段2，……）values（字段1的值，字段2的值，……）；	向数据表中插入新的记录
update表名set字段名1=字段值1[，字段名2=字段值2] where条件表达式；	修改、更新数据表中的记录
select字段名1，字段名2……from表名where条件表达式；	从数据表中查找符合条件的记录
select * from表名；	显示当前数据库的表中的记录
delete from表名where条件表达式；	在数据表中删除指定的记录
delete from表名；	将当前数据库表中记录清空

目录

本章要点

1 授予用户权限

grant 权限列表 on 数据库名.表名 to 用户名@来源地址 [identified by '密码']

权限列表：是以逗号分隔的权限符号，主要用户权限如表12-5所示。

表12-5 主要用户权限

权限符号	权限	权限符号	权限
select	读取表的数据	insert	向表中插入数据
update	更新表中的数据	delete	删除表中的数据
index	创建或删除表的索引	create	创建新的数据库和表
alter	修改表的结构	grant	将自己拥有的某些权限授予其他用户
drop	删除现存的数据库和表	file	在数据库服务器上读取和写入文件
reload	重新装载授权表	process	查看当前执行的查询
shutdown	停止或关闭mysql服务	all	具有全部权限

1 授予用户权限

数据库名.表名：

可使用通配符“*”，例如“*.*”表示任意数据库中的任意表。

用户名@来源地址：

用于设置谁能登录，能从哪里登录。用户名不能使用通配符，但可使用连续的两个单引号“''”来表示空字符串，可用于匹配任何用户；来源地址可使用“%”作为通配符，匹配某个域内的所有地址（如%.hnwy.com），或使用带掩码标记的网络地址（如172.16.1.0/16）；省略来源地址时相当于“%”。

省略“identified by”部分时，新用户的密码将为空。

2 查看用户的权限

查看用户权限命令：

```
select命令
show grants for 用户名@域名或IP地址;
```

3 撤销用户的权限

```
revoke 权限列表 on 数据库名.表名 from 用户名@域名或IP地址
```

目录

本章要点

1 直接备份数据库所在的目录

使用cp、tar等命令直接备份数据库所存放的目录。

2 使用mysqldump命令备份和恢复

》备份（导出）数据

mysqldump -u 用户名 -p [密码] [选项] [数据库名] [表名] > /备份路径/备份文件名

常用以下两个选项：

① **all-databases**：备份服务器中的所有数据库内容；

② **opt**：对备份过程进行优化，此项为默认选项。

》恢复（导入）数据

mysql -u root -p [数据库名] < /备份路径/备份文件名

Linux操作系统及应用技术

Samba跨平台资源共享的管理及应用

Samba是在Linux和UNIX系统上**实现SMB协议**的一个免费软件，由服务器及客户端程序构成。SMB（Server Messages Block，信息服务块）是在局域网上共享文件和打印机的一种**通信协议**，它为局域网内的不同计算机之间提供文件及打印机等资源的共享服务。SMB协议是**客户机/服务器型协议**，客户机通过该协议可以访问服务器上的共享文件系统、打印机及其他资源。通过设置“NetBIOS over TCP/IP”使得Samba不但能与局域网络主机分享资源，还能与全世界的电脑分享资源。

目录

本章要点

1．SMB/CIFS协议

SMB协议是Microsoft和Intel在1987年开发的，通过该协议使得客户端应用程序可以在各种网络环境下访问服务器端的文件和打印机等资源，从而实现不同Windows系统主机之间的资源共享。

Samba是在Linux系统上对**SMB/CIFS**的具体实现，通过Samba服务器的搭建和Samba客户机软件的安装，就可以实现Linux系统主机和Windows主机之间的双向文件和打印机的共享，如图8-1所示（见下页）。

1．SMB/CIFS协议

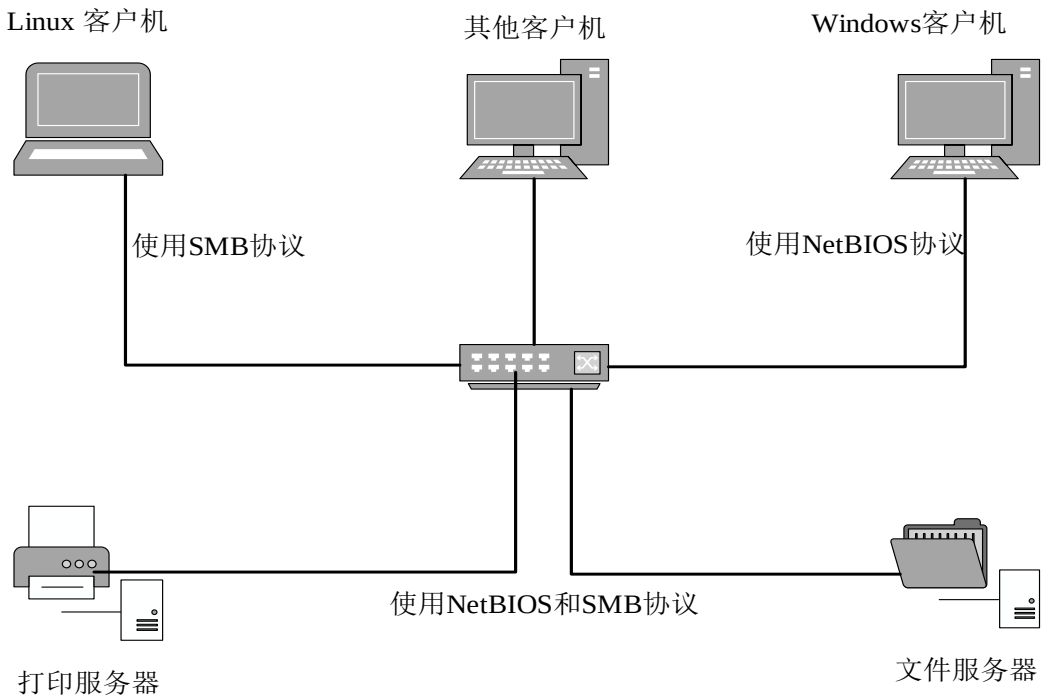


图8-1 通过Samba实现Linux与Windows主机之间的双向文件和打印机共享

2．Samba的主要功能

01 用于Linux与Windows系统直接的文件共享和打印共享

02 解析NetBIOS名字

03 支持跨平台访问的身份验证和权限设置，支持SSL（Secure Socket Layer，安全套接字层）

04 Samba服务器可作为网络中的WINS服务器，甚至作为Windows Server 2003/2008域中的域控制器的一些功能

05 网络浏览服务

06 满足CIFS协议的UNIX共享

3．Samba服务的工作过程

组成Samba运行的有两个服务，一个是**SMB**，另一个是**NMB**。SMB是Samba的**核心启动服务**，主要负责建立Linux Samba服务器与Samba客户机之间的对话，验证用户身份并提供对文件和打印系统的访问，只有SMB服务启动，才能实现文件的共享，监听139 TCP端口；而NMB服务是**负责解析**用的，类似于DNS实现的功能，NMB可以将Linux系统共享的工作组名称与其IP对应起来，如果NMB服务没有启动，就只能通过IP来访问共享文件，监听137和138 UDP端口。

通过Samba服务，Windows用户可以通过**“网上邻居”**窗口查看到Linux服务器中共享的资源，同时Linux用户也能够查看到服务器上的共享资源。

3．Samba服务的工作过程

Samba服务的具体工作过程如图8-2所示。

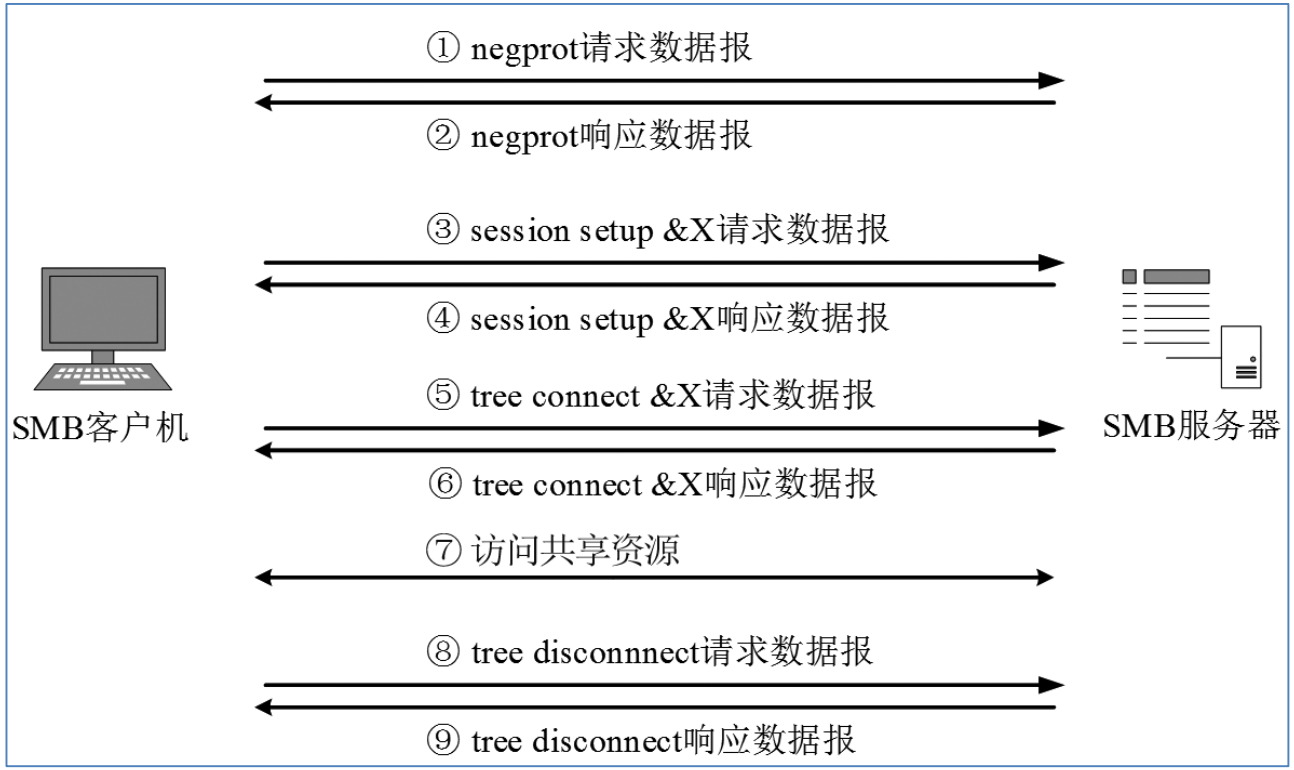


图8-2 Samba服务的工作过程

3．Samba服务的工作过程

具体步骤如下：

客户端在访问Samba服务器时，首先由客户端发送一个SMB negprot请求数据报，并列出它所支持的所有SMB协议版本。服务器在接收到请求信息后开始响应请求，并列出希望使用的协议版本。如果没有可使用的协议版本则返回oXFFFFH信息，结束通信。

当SMB协议版本确定后，客户端进程向服务器发起一个用户或共享的认证，这个过程是通过发送Session setup &X请求数据报实现的。客户端发送一对用户名和密码或一个简单密码到服务器，然后服务器通过发送一个Session setup&X请应答数据报来允许或拒绝本次连接。

具体步骤如下：

- 当客户端和服务器完成了协商和认证之后，它会发送一个Tree connect或SMB Tree connect&X数据报并列出它想访问网络资源的名称，之后服务器会发送一个SMB Tree connect&X应答数据报以表示此次连接是否被接受或拒绝。
- 连接到相应资源，SMB客户端就能够open SMB打开一个文件，通过read SMB读取文件，通过write SMB写入文件，通过close SMB关闭文件。

目录

本章要点

1．Samba软件包的组成

samba-common-tools-4.2.3-10.el7.x86_64.rpm

该包是服务器和Linux客户端均必须要安装的通用工具。

samba-libs-4.2.3-10.el7.x86_64.rpm

该包是Samba服务的库文件。

samba-client-libs-4.2.3-10.el7.x86_64.rpm

该包是Linux客户端连接Samba服务器的库文件，Linux客户机上必须安装。

1．Samba软件包的组成

samba-common-4.2.3-10.el7.noarch.rpm

该包是服务器和Linux客户端均必须要安装的公共文件。

samba-4.2.3-10.el7.x86_64.rpm

该包是Samba服务的主程序包。服务器必须安装该软件包。

samba-common-libs-4.2.3-10.el7.x86_64.rpm

该包是服务器和Linux客户端均必须要安装的通用库文件。

2．检查是否安装了Samba服务器

输入命令

```
# rpm -qa |grep samba
samba-common-tools-4.2.3-10.el7.x86_64
samba-libs-4.2.3-10.el7.x86_64
samba-client-libs-4.2.3-10.el7.x86_64
samba-common-4.2.3-10.el7.noarch
samba-4.2.3-10.el7.x86_64
samba-common-libs-4.2.3-10.el7.x86_64
```

若上述6行字体为红色，则未安装。

RHEL7.2系统中默认未安装Samba的主程序包。

注意

如果某个目录本身便是NFS导出或者挂载的NFS文件系统，请勿使用Samba来共享此目录。这可能导致文件损坏、文件锁过时或共享方面的其他文件访问问题。

3．安装Samba软件包

```
# mount /dev/cdrom /mnt
# rpm -ivh /mnt/Packages/samba-common-tools-4.2.3-10.el7.x86_64.rpm
# rpm -ivh /mnt/Packages/samba-libs-4.2.3-10.el7.x86_64.rpm
# rpm -ivh /mnt/Packages/samba-client-libs-4.2.3-10.el7.x86_64.rpm
# rpm -ivh /mnt/Packages/samba-common-4.2.3-10.el7.noarch.rpm
# rpm -ivh /mnt/Packages/samba-4.2.3-10.el7.x86_64.rpm
# rpm -ivh /mnt/Packages/samba-common-libs-4.2.3-10.el7.x86_64
```

出现相关性错误，原因是缺少perl类的有关软件包。为此先安装perl，再安装Samba主程序。

```
# rpm -ivh /mnt/Packages/perl-Convert-ASN1-0.26-4.el7.noarch.rpm
# rpm -ivh /mnt/Packages/samba-4.2.3-10.el7.x86_64.rpm
```

4．Samba服务的运行控制

启动、停止、重新启动和重新加载Samba服务：

```
service smb start|stop|restart|reload
或/etc/rc.d/init.d/smb start|stop|restart|reload
```

出现相关性错误，原因是缺少perl类的有关软件包。为此先安装perl，再安装Samba主程序。

```
chkconfig --level 345  smb on|off
```

还可以使用ntsysv工具配置开机自动启动。

目录

本章要点

1．Samba服务的配置文件

Samba服务的配置文件如表8-1所示。

表8-1 配置文件

文件	说明
/etc/samba/smb.conf	是Samba中最重要的一个**配置文件**，类似于Windows系统中的*.ini文件，可以配置服务器的权限、共享目录、打印机和计算机所属的工作组等各种选项
/etc/samba/lmhosts	**主机配置文件**，用于本地解析NetBIOS名与对应的IP，功能同/etc/hosts类似。在启动Samba服务进程时能自动捕捉到网络中相关IP地址对应的NetBIOS名，并自动在lmhosts文件中添加这些映射关系所以通常不需专门配置该文件
/var/log/samba/	该目录用于存放Samba的**日志文件**

1．Samba服务的配置文件

smb.conf主配置文件的主要组成部分如表8-2所示。

表8-2 smb.conf主配置文件的主要组成部分

部分	节/段落	说明
全局设置 (Global Settings)	[global]	用于定义Samba服务器的**总体特性**，其配置项对所有共享资源生效，是smb.conf配置文件中最重要的部分
共享定义 (Share Definitions)	[homes]	用于设置**用户宿主目录**的共享属性
	[printes]	用于设置**打印机共享资源**的属性
	[myshare]	用于用户自定义的共享目录的**共享属性**的设置（需自己添加，每个共享目录对应一节）

1．Samba服务的配置文件

smb.conf文件中全局参数的设置如表8-3所示。

表8-3 smb.conf全局设置主要配置项

类型	配置项及默认值	说明
基本	workgroup=MYGROUP	设置Samba服务器要加入的**工作组**的名称，也即出现在Windows操作系统中“网上邻居”里面的名称
	server string=Samba Server Version %v	设定Samba服务器的**文字说明**，默认为 “Version %v”表示显示Samba版本号
	netbios name=MYSERVER	设定本机在“网上邻居”中显示的**计算机名**
	interfaces=lo eth0 192.168.12.2/24 192.168.13.2/24	指定Samba服务器监听哪些**网卡**，若服务器上有多块网卡应配置此项。可以写网卡名或该网卡的IP地址

2．smb.conf文件中全局参数的设置

表8-3 smb.conf全局设置主要配置项

类型	配置项及默认值	说明
日志	log file=/var/log/samba/%m.log	指定日志文件的**存放位置**，并为每个登录服务器的用户建立不同的日志文件，“%m”变量表示客户端的主机名或IP地址
	max log size=50	指定日志文件的**最大容量**，单位为KB，“0”代表无限制
安全	security=user	设置Samba服务器的**安全级别**
	Password server=<NT-Server-Name>	当Samba服务器的安全级别不是share或user时，用于指定验证Samba用户和口令的**服务器名**
	hosts allow=127. 192.168.12. 192.168.13.	设置可访问Samba服务器的主机、子网或网域，可以EXCEP排除某些IP地址。默认是全部允许
	username map=/etc/samba/smbusers	设置Linux用户到Windows的**用户映射**

1．Samba服务的配置文件

表8-3 smb.conf全局设置主要配置项

类型	配置项及默认值	说明
打印	load printers=yes	是否允许**加载打印配置文件中的所有打印机**，在开机时自动加载浏览列表，以支持客户端的浏览功能
	cups option=raw	指定打印机系统的**工作模式**
	printcap name=/etc/printcap	设置开机时自动加载的打印机配置**文件名称和路径**
	printing=cpus	**设置打印机的类型**。标准类型包括bsd、sysv、plp、lprng、aix hpux、qnx、cups

2．smb.conf文件中全局参数的设置

Samba服务器的安全级别，按照安全性由低到高为以下4种取值：

share

没有安全性的级别，客户端不需要输入Samba用户名和密码就可访问Samba服务器的共享资源。适用于公共的共享资源，安全性差，需要配合其他权限设置来保证samba服务器的安全性。

user

是Samba服务器的默认安全级别。Samba服务器要求用户在访问共享资源之前资源必须先提供用户名和密码进行验证。

server

和user安全级别类似，但用户名和密码是递交到另外一个Samba服务器或Windows服务器去验证，此时必须指定负责验证的那个服务器名称。如果递交失败，就退到user安全级。

domain

该安全级别要求网络上存在一台Windows的域控制器，samba将用户名和密码递交给它去验证，此时必须指定域控制服务器的NetBIOS名称。

3．smb.conf文件中共享定义的设置

要发布共享资源，需要对**共享定义部分（Share Definitions）**进行配置。共享定义通过[Homes][Printers]和[自定义目录名]等节来说明共享资源的属性。

[homes]为特殊共享目录，其名字不能改变。[homes]共享目录并不特指某个具体共享目录，而是表示Samba用户的宿主目录，即Samba用户登录后可以访问同名Linux系统用户的宿主目录中的内容。默认情况下，用户宿主目录位于/home目录下，每个用户有一个以用户名命名的子目录。

[printers]表示共享打印机。[printers]行也是特殊的行，不能修改其名字。若定义了[printers]段，用户就可以连接在printcap文件里指定的打印机。要注意的是，若是设置共享打印机，则必须设置printable关键字语句为yes，否则用户无法打印。

3．smb.conf文件中共享定义的设置

smb.conf共享定义常用配置项如表8-4所示。

表8-4 smb.conf共享定义常用配置项

配置项	说明
[用户自定义的共享名]	用户访问时通过此共享名来识别。也就是【网上邻居】里面看见的文件夹的名字，可以与原目录名不同。
comment=备注信息	设置共享目录或打印机的说明信息
path=绝对地址路径	指定共享目录在Samba服务器中的绝对路径
public=yes|no	是否允许匿名用户访问共享的文件夹或打印机资源
guest ok = yes|no	连接共享资源时是否需要密码

3．smb.conf文件中共享定义的设置

表8-4 smb.conf共享定义常用配置项

配置项	说明
valid users=用户名或组名清单	设置允许访问的**用户或组成员**，组名前面带@，多个用户名或组名以空格或逗号分隔
readonly=yes|no	设置共享目录**只读还是可读写**
writable=yes|no	指定共享目录有**写入权限还是只读权限**（目录本身是否可写是前提），与readonly的作用相反
write list=用户名或组名清单	设置对共享目录具有可读写权限的**用户名或组名**。组名前面带@，多个用户名或组名以空格或逗号分隔，write list要生效的话，writeable设置成no

3．smb.conf文件中共享定义的设置

表8-4 smb.conf共享定义常用配置项

配置项	说明
browseable=yes|no	设置共享目录在“网上邻居”中是否可见（默认为no即隐藏共享目录）
printable=yes|no	是否允许打印
create mask=文件权限值	设置用户在共享目录下创建的文件的**默认访问权限**。通常是以数字表示的，如0664，代表的是文件所有者对新创建的文件具有可读可写权限，其他用户具有可读权限，而所属主要组成员不具有任何访问权限
directory mask=子目录权限值	设置用户在共享目录下创建的子目录的默认访问权限

4．smb.conf文件的测试

在完成smb.conf文件所有配置后，可使用**testparm命令**测试配置文件中的语法是否正确。若显示“Loaded services file OK.”信息表示配置文件的语法是正确的，再按**【Enter】键**，会显示主配置文件当前有效的配置清单。

注意

指令read only=no与writable=yes相同，这可能会产生混淆。

目录

本章要点

在share安全级别下的Samba服务器允许**匿名访问**（不需要客户端提供用户名和密码）其共享资源，对于安全性要求不高的小型网络，是一种方便实用的可选方案。

配置步骤如下：

步骤 1 ▶

网先关闭防火墙，确保服务器防火墙开放TCP139端口和UDP137、138端口。

步骤 2 ▶

创建文件共享目录/user/share/mydoc，并设置其访问权限。

```
#mkdir -p /user/share/mydoc
#chmod 2775 /user/share/mydoc
```

步骤 3 ▶

修改samba主配置文件smb.conf。

```
#vim /etc/samba/smb.conf
......
[global]
security=user
map to guest=Bad User
[public]
    comment=Public share directory
    path=/user/share/mydoc
    writable=yes
    guest ok=yes
......
```

步骤 4 ▶

重新加载配置，使修改后的配置文件生效。

步骤 5 ▶

修改SELinux。

```
#setsebool -P samba_export_all_rw=1
```

步骤 6 ▶

测试

目录

本章要点

对于重要文件的目录，为了保证系统安全性及资料保密性，就必须对用户进行**筛选**，允许或禁止相应的用户访问**指定目录**。实现用户身份验证的途径可以通过将安全级别配置为user、server和domain来实现。

配置步骤如下：

步骤 1 ▶

按部门创建Linux系统用户、组。

步骤 2 ▶

建立相应的Samba用户账号。

步骤 3 ▶

创建各部门相应的目录并规划其权限。

步骤 4 ▶

重新加载配置，使修改后的配置文件生效。

步骤 5 ▶

测试

目录

本章要点

1．虚拟用户的配置

隐藏系统真实用户，减少密码穷举攻击的风险。真实用户与虚拟用户的映射关系通过“/etc/samba/smbusers”文件来定义和保存。

配置步骤如下：

步骤 1 ▶

编辑主配置文件，开启用户账号映射功能。

```
[root@localhost ~]# vim  /etc/samba/smb.conf
//在[global]中添加以下配置行:
username map = /etc/samba/smbusers     //开启用户账号映射功能
```

步骤 2 ▶

编辑/etc/samba/smbusers，smbusers文件中定义账号映射关系的格式为：

samba用户 = 虚拟用户[,虚拟用户...]

步骤 3 ▶

重启Samba服务。

步骤 4 ▶

验证。

2．隐藏共享目录的配置

使用browseable字段可实现隐藏共享的功能。共享目录隐藏了并不是说不共享了，只要知道共享名，并且有相应权限，在Windows客户端可以在地址栏中输入“\\IP地址\共享名”来访问隐藏共享。

```
[root@localhost ~]# vim
/etc/samba/smb.conf
.....................
[sales_doc]
comment = sales data
path = /usr/share/sales
valid users = ceo @sales
browseable = no
                    //设置隐藏sales目录
[root@localhost ~]# service smb restart
```

3．搭建基于用户或用户组的独立配置文件

配置步骤如下：

步骤 1 ▶

建立独立的配置文件。

```
[root@localhost ~]# cd  /etc/samba/
[root@localhost ~]# cp  smb.conf  smb.conf.ceo
```

步骤 2 ▶

编辑smb.conf主配置文件。

```
[root@localhost ~]# vim  /etc/samba/smb.conf
[global]
config file = /etc/samba/smb.conf.%U
                                        //添加此行
.............
```

配置步骤如下：

步骤 3 ▶

编辑smb.conf.ceo独立配置文件。

编辑ceo账号的独立配置文件smb.conf.ceo，将定义[sales_doc]共享目录里面的browseable = no删除，其余配置不变。

步骤 4 ▶

重新启动samba服务。

目录

本章要点

1．在Linux客户端访问共享目录

Linux客户端的安装

在Linux客户端登录访问Samba服务器或Windows主机时，首先要确保该Linux客户端已经安装了samba-client软件包。

8.7 Linux与Windows资源互访

Linux客户端访问samba服务器

（1）使用smbclient工具登录到共享目录所在主机，其使用的形式有如下几种情况：

① 查看服务器中的共享资源

smbclient -L 目标IP地址或主机名 -U 登录用户名%密码

② 浏览、上传下载服务器中的共享资源

smbclient //目标IP地址或主机名/共享目录 -U 用户名%密码

（2）利用mount命令将共享目录挂载到本地使用。

mount //目标IP或主机名/共享目录名挂载点
-o username=用户名%密码

2．Windows客户端访问Samba服务器中的共享目录

在Windows客户端上，不需要另外安装任何软件，并且访问Samba服务器中的共享目录与访问其他Windows主机提供的共享目录，使用方法完全相同。可以在**【运行】对话框**、资源管理器的地址栏、IE浏览器的地址栏中直接输入**UNC路径**实现访问Samba服务器中的共享目录，也可通过**【网上邻居】**浏览的方式找到Samba服务器，然后再访问共享资源。

目录

本章要点

8.8 配置Samba打印共享

默认情况下，Samba的打印服务是开放的，所以只要将打印机安装好后客户端的用户就可以使用打印机了。

安装完打印机后必须重新启动Samba服务，否则客户端可能无法看到共享的打印机。

1．设置global配置项

修改smb.conf全局配置，开启打印共享功能。命令如下：

```
[root@localhost ~]# vim  /etc/samba/smb.conf
[global]
.............
    load printers = yes
    cups options = raw
    printcap name = /etc/printcap
    printing = cups
```

8.8 配置Samba打印共享

2．设置printers配置项

修改smb.conf打印配置，将browseable、gust ok、writable、printable、public改为yes。命令如下：

```
    [root@localhost ~]# vim /etc/samba/smb.conf
    [printers]
        comment = All Printers
        path = /var/spool/samba
        browseable = yes
        guest ok = yes
        writable = yes
        printable = yes
        public = yes
```

3．重启cups和samba

命令如下：

```
#service cups restart
#service smb restart
```


谢谢观看