

DNS域名解释服务

1.DNS系统的作用及类型

2.DNS服务的查询模式及域名解析

3.DNS服务器的分布式结构

4.安装和控制DNS服务器

5.BIND服务的配置文件

6.构建缓存域名服务器

7.构建主域名服务器

8.构建从域名服务器

9、DNS解析综合学习案例

1.DNS系统的作用及类型

DNS（Domain Name System，域名系统）

手机号 - 通讯录 -- 名字

hosts文件

DNS系统

DNS协议使用53 端口，既用TCP， 又用UDP

FQDN--完整域名格式 常见域名后添加 “.” （根域） .com 顶级域
crushlinux.com --姓氏-域名 baidu.com. 中的第二个点叫根 www--名字

正向解析：根据域名查找IP地址

反向解析：根据IP查找域名----用的比较小 很多网站不配反向解析

每一台DNS服务器只管理一个有限的范围（一个或几个域），

特定的“zone”

紧急备用方案:

当主服务器出现问题，无法用域名登录网站，可以用IP登录

可以用备用，从服务器会定期下载主服务器的数据，备用的数量不受限，且可以提供服务
缓解主服务器的压力，负载量越大

区别: 记录维护在主服务器，从服务器无法修改，只是下载

主存域名服务器：权威

从存域名服务器：权威

主从的地位是相对的

缓存域名服务器：就近原则，在各地区起到加速的作用

转发器

2.DNS服务的查询模式及域名解析

面试题

域名解析过程 ——10步

1. 检查自身缓存
2. 浏览器缓存未命中，>找hosts文件，有，解析结束
hosts维护很重要，电脑被篡改过，只读，——域名劫持 安全性
3. 还未命中，本地域名服务器，LDNS解析。80%可以解决
4. 还未命中，（.）根
5. 根域名服务器返回LDNS一个主域名服务器地址
6. LDNS再发送请求给上一步返回的GTLD（类似于.com）
7. 接受请求的GTLD查找并返回这个域名对应的Name Server 的地址，这个Name Server就是网站注册的域名服务器（CrushLinux.com）
8. Name Server根据映射关系表找到目标ip, 返回给LDNS
9. LDNS 缓存这个域名和对应的ip
10. LDNS 把解析的结果返回给用户，用户根据TTL值缓存到本地系统缓存中，域名解析过程完毕。

浏览器缓存-->

hosts -->

LDNS -->

. 根域-->

.com 顶级域-->

.crushlinux.com 权威域服务器-->

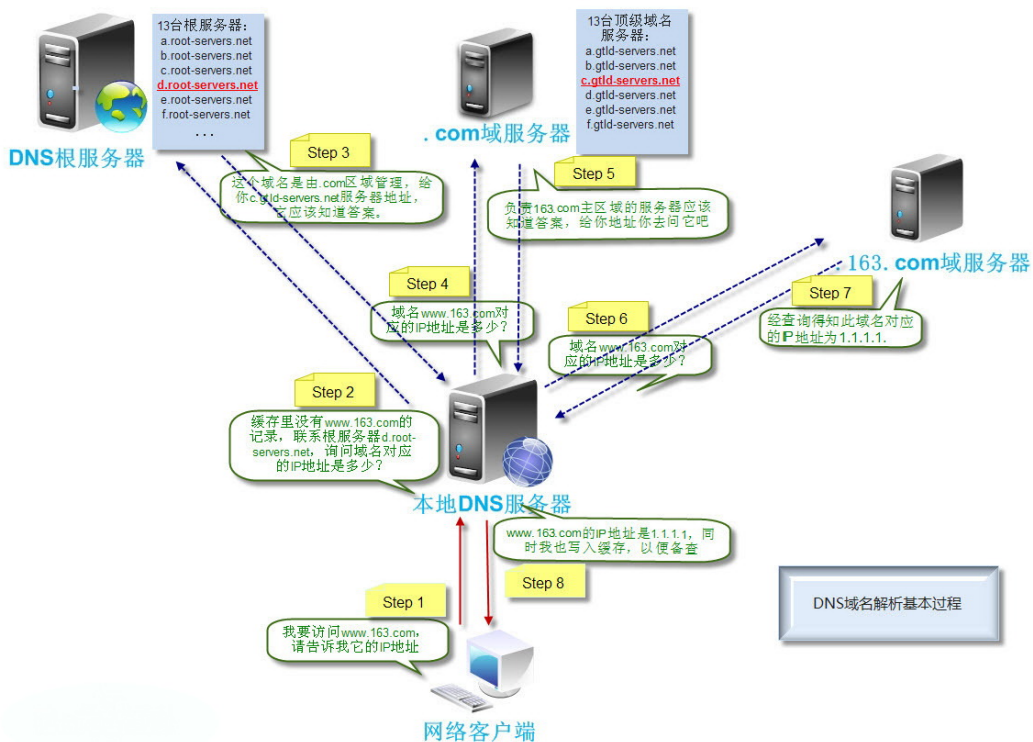
LDNS缓存 -->

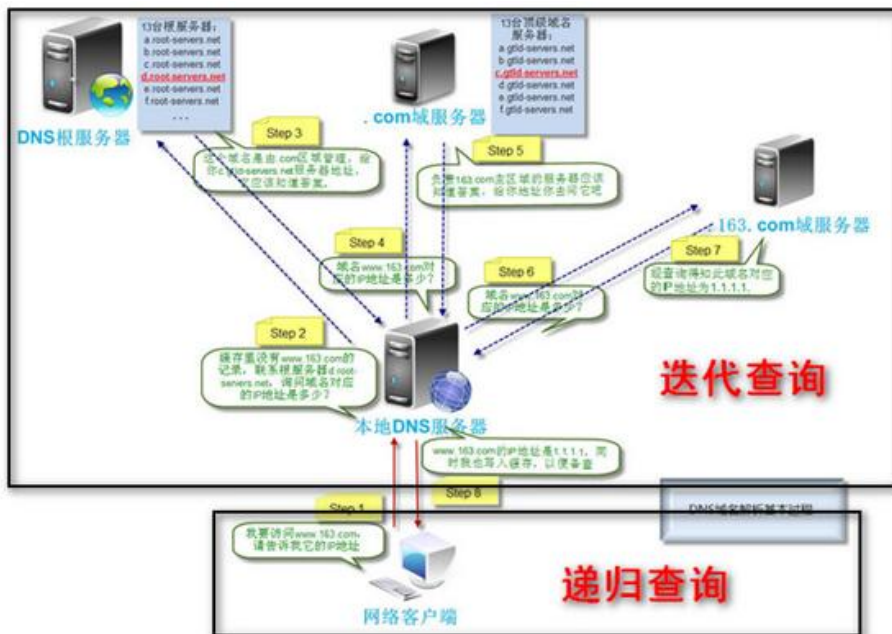
LDNS给客户端反馈结果 -->

客户端环境

递归查询

迭代查询





DNS解析测试工具

nslookup www.baidu.com

host www.tianmao.com

dig +trace www.abc.com

3.DNS服务器的分布式结构

根服务器主要用来管理互联网的主目录，全世界只有13台。

1个为主根服务器，放置在美国。其余12个均为辅根服务器，其中9个放置在美国，欧洲2个，位于英国和瑞典，亚洲1个，位于日本。

根域，顶级域，二级域，三级域

. com	公司企业
. cn	中国
. 中国	中国
. net	具有互联网标识
. org	各类组织机构（主要非盈利）
. gov. cn	中国政府机关单位

购买---备案（挺麻烦）-----一两周的时间

公司的话还要代表性的材料

越往后越贵，越用越贵，越火越贵
注册比较火的东西屯着，以后可以卖高价
后缀不好听的就特别便宜，还有免费的

4.安装和控制DNS服务器

chroot 修复文件系统 chroot /mnt/sysimage

BIND

安装及管理BIND软件

```
[root@ssh-server ~]# rpm -qa | grep ^bind
```

bind-9.9.4-37.el7.x86_64.rpm

bind-unilts-9.9.4-37.el7.x86_64.rpm

bind-libs-9.9.4-37.el7.x86_64.rpm

bind-chroot-9.9.4-37.el7.x86_64.rpm 可选软件包，为BIND服务提供一个伪装的根目录（将/var/named/chroot/文件夹作为BIND的根目录），以提高安全性，也称jail（监牢）机制。

```
/etc/named.conf > /var/named/chroot/etc/named.conf
```

BIND服务控制

5.BIND服务的配置文件

主配置文件 /etc/named.conf

用于设置named服务的全局选项、注册区域及访问控制等各种运行参数

区域数据文件

用于存放某个DNS区域的地址解析记录（正向或反向）

主配置文件：全局配置、区域配置

； 表示结束

、// 表示注释文字

/ * */ 表示大段注释

/var/named/crushlinux.zheng

/var/named/crushlinux.fan

全局配置部分

```
[root@ssh-server ~]# cd /etc/
[root@ssh-server etc]# vim named.conf

options {
    listen-on port 53 { 127.0.0.1; };
//监听地址和端口

    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
//区域数据文件的默认存放位置

    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";
    allow-query     { localhost; };
//允许使用本DNS服务的网段
}
```

区域配置（正、反）

```
zone "." IN {                                     //正向 "."区域
    type hint;                                    //类型为根区
    域 (master, slave, hint)
    file "named.ca";                             //区域数据文件为
};

/etc/named.conf  N个正向  1个反向
```

注意：

每个zone区域可选（根域，回环域，反向域），“IN”可省略
反向区域名称由倒序的网络地址与“in-addr.arpa”组成，例如：

192.168.200. 0/24 > 200.168.192. in-addr.arpa

file配置指定区域数据文件，文件名由管理员自行设置

allow-transfer 可以放全局配置里

语法检查

- 刚配完全局和区域，不要做语法检查，文件未配置，会报错file not found 是正常的
- 只检查语法，不会检查“值”，只检查括号，分号，空格

- 不要完全依赖语法检查

#检查主配置文件

named-checkconf

#检查域名配置文件

named-checkzone test.com /var/named/test.com.zone

区域数据配置文件

[root@ssh-server named]# vim named.localhost

\$TTL 1D #有效

解析记录的生存周期

@ IN SOA @ rname.invalid. (#SOA标记、域名、管理邮箱

0 ; serial #更新

序列号，10以内整数

3H ; refresh #刷新时

间，重新下载地址数据的间隔

1H ; retry #重试

延时。下载失败后的重试问题

1W ; expire #失效时

间，超过改时间仍无法下载则放弃

1D) ; minimum #无效解析记

录的生存周期

NS @

A 127.0.0.1

AAAA ::1

地址解析记录部分

MX 10 数字越大，优先级越低

CNAME 别名

第一列：主机部分

PTR ：指针记录，只能在反向里面用

泛域名解析

* A 192.168.200.111

基于域名解析的负载均衡，同一个域名对应到多个IP地址

正向解析文件

反向解析文件

拿一台服务器让它只负责一个区域的正反向解析来说，它一共有3个文件：
主配置文件、正向文件、反向文件

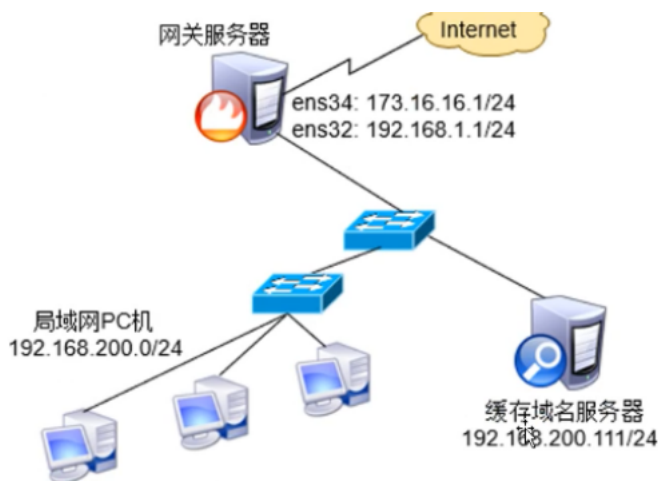
//、# :注释

MX? 邮件交换

6.构建缓存域名服务器

提高域名解析速度

缓存域名服务器能正常上



```
[root@localhost ~]# iptables -F
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# setenforce 0
```

```
[root@localhost ~]# ping www.baidu.com
```



```
[root@localhost ~]# yum -y install bind bind-libs bind-utils
[root@localhost ~]# rpm -qa | grep ^bind
bind-utils-9.9.4-61.el7.x86_64
bind-libs-9.9.4-61.el7.x86_64
bind-9.9.4-61.el7.x86_64

[root@localhost ~]# cp /etc/named.conf /etc/named.conf.bak
[root@localhost ~]# vim /etc/named.conf
options {
    listen-on port 53 { 192.168.200.111; };
    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";
    allow-query         { 192.168.200.0/24; };
    recursion yes;
    forwarders { 202.106.0.20; };
};
};

[root@localhost ~]# named-checkconf /etc/named.conf
[root@localhost ~]# systemctl start named
```

7.构建主域名服务器

```
[root@localhost ~]# iptables -F
[root@localhost ~]# systemctl stop firewalld
[root@localhost ~]# setenforce 0
[root@localhost ~]# yum -y install bind bind-libs bind-utils
[root@localhost ~]# cp /etc/named.conf /etc/named.conf.bak

[root@localhost ~]# vim /etc/hosts
192.168.200.111 ns1.crushlinux.com
192.168.200.112 ns2.crushlinux.com
```

```
[root@localhost ~]# vim /etc/resolv.conf
nameserver 192.168.200.111
nameserver 192.168.200.112
```

```
[root@localhost ~]# vim /etc/named.conf
options {
    directory      "/var/named";
};
```

```
zone "crushlinux.com" IN {
    type master;
    file "crushlinux.zheng";
};
```

```
zone "200.168.192.in-addr.arpa" IN {
    type master;
    file "crushlinux.fan";
};
```

```
[root@localhost ~]# cd /var/named/
[root@localhost named]# vim crushlinux.zheng
$TTL 86400
```

```
@      SOA      crushlinux.com.      admin.crushlinux.com.      (
                                20200312
                                3H
                                15M
                                1W
                                1D
)

      IN      NS      ns1.crushlinux.com.
      IN      MX 10    mail.crushlinux.com.
ns1    IN      A       192.168.200.111
www    IN      A       192.168.200.111
mail   IN      A       192.168.200.112
```

```
study    IN      A       192.168.200.113
*        IN      A       192.168.200.113
```

```
[root@localhost named]# vim crushlinux.fan
```

```
[root@localhost named]# cat crushlinux.fan
```

```
$TTL 86400
```

```
@        SOA      crushlinux.com.      admin.crushlinux.com.      (
                                20200312
                                3H
                                15M
                                1W
                                1D
)
```

```
                IN      NS      ns1.crushlinux.com.
                IN      MX 10    mail.crushlinux.com.
111          IN      PTR      ns1.crushlinux.com.
111          IN      PTR      www.crushlinux.com.
112          IN      PTR      mail.crushlinux.com.
113          IN      PTR      study.crushlinux.com.
```

```
[root@localhost named]# chgrp named crushlinux.*
```

```
[root@localhost named]# ll crushlinux.*
```

```
-rw-r--r-- 1 root named 278 3月 12 15:34 crushlinux.fan
-rw-r--r-- 1 root named 277 3月 12 15:32 crushlinux.zheng
```

```
[root@localhost named]# named-checkzone crushlinux.com crushlinux.zheng
```

```
[root@localhost named]# named-checkzone crushlinux.com crushlinux.fan
```

```
[root@localhost named]# systemctl restart named
```

```
C:\Users\Crushlinux>nslookup www.crushlinux.com
```

```
服务器: ns1.crushlinux.com
```

```
Address: 192.168.200.111
```

名称: www.crushlinux.com

Address: 192.168.200.111

C:\Users\Crushlinux>nslookup mail.crushlinux.com

服务器: ns1.crushlinux.com

Address: 192.168.200.111

名称: mail.crushlinux.com

Address: 192.168.200.112

C:\Users\Crushlinux>nslookup study.crushlinux.com

服务器: www.crushlinux.com

Address: 192.168.200.111

名称: study.crushlinux.com

Address: 192.168.200.113

C:\Users\Crushlinux>nslookup abc.crushlinux.com

服务器: www.crushlinux.com

Address: 192.168.200.111

名称: abc.crushlinux.com

Address: 192.168.200.113

C:\Users\Crushlinux>nslookup xyz.crushlinux.com

服务器: www.crushlinux.com

Address: 192.168.200.111

名称: xyz.crushlinux.com

Address: 192.168.200.113

```
C:\Users\Crushlinux>nslookup 192.168.200.112
```

```
服务器: ns1.crushlinux.com
```

```
Address: 192.168.200.111
```

```
名称: mail.crushlinux.com
```

```
Address: 192.168.200.112
```

```
C:\Users\Crushlinux>nslookup 192.168.200.113
```

```
服务器: ns1.crushlinux.com
```

```
Address: 192.168.200.111
```

```
名称: study.crushlinux.com
```

```
Address: 192.168.200.113
```

8.构建从域名服务器

```
[root@localhost ~]# iptables -F
```

```
[root@localhost ~]# systemctl stop firewalld
```

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

```
[root@localhost ~]# yum -y install bind bind-libs bind-utils
```

```
[root@localhost ~]# vim /etc/hosts
```

```
192.168.200.111 ns1.crushlinux.com
```

```
192.168.200.112 ns2.crushlinux.com
```

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

```
nameserver 192.168.200.111
```

```
nameserver 192.168.200.112
```

主:

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

```
options {
```

```

        directory      "/var/named";

};

zone "crushlinux.com" IN {
    type master;
    file "crushlinux.zheng";
    allow-transfer { 192.168.200.112; };
};

```

```

zone "200.168.192.in-addr.arpa" IN {
    type master;
    file "crushlinux.fan";
    allow-transfer { 192.168.200.112; };
};

```

```
[root@localhost ~]# vim /var/named/crushlinux.zheng
```

```
$TTL 86400
```

```

@      SOA      crushlinux.com.      admin.crushlinux.com.      (
                                20200312
                                3H
                                15M
                                1W
                                1D
)

```

```

                IN      NS      ns1.crushlinux.com.
                IN      NS      ns2.crushlinux.com.
                IN      MX 10    mail.crushlinux.com.
ns1      IN      A      192.168.200.111
ns2      IN      A      192.168.200.112
www      IN      A      192.168.200.111
mail     IN      A      192.168.200.112
study    IN      A      192.168.200.113
*        IN      A      192.168.200.113

```

```
[root@localhost ~]# vim /var/named/crushlinux.fan
```

```

$TTL 86400
@      SOA      crushlinux.com.      admin.crushlinux.com.      (
                                20200312
                                3H
                                15M
                                1W
                                1D
)

      IN      NS      ns1.crushlinux.com.
      IN      NS      ns2.crushlinux.com.
      IN      MX 10    mail.crushlinux.com.
111    IN      PTR     ns1.crushlinux.com.
112    IN      PTR     ns2.crushlinux.com.
111    IN      PTR     www.crushlinux.com.
112    IN      PTR     mail.crushlinux.com.
113    IN      PTR     study.crushlinux.com.
[root@localhost ~]# systemctl restart named

```

从:

```

[root@localhost ~]# cp /etc/named.conf /etc/named.conf.bak
[root@localhost ~]# vim /etc/named.conf
options {
    directory      "/var/named";
};

```

```

zone "crushlinux.com" IN {
    type slave;
    file "slaves/crushlinux.zheng";
    masters { 192.168.200.111; };
};

```

```

zone "200.168.192.in-addr.arpa" IN {
    type slave;
    file "slaves/crushlinux.fan";
};

```

```
masters { 192.168.200.111; };  
};
```

```
[root@localhost ~]# systemctl start named  
[root@localhost ~]# ls /var/named/slaves/  
crushlinux.fan  crushlinux.zheng
```

```
C:\Users\Crushlinux>nslookup  
默认服务器: ns2.crushlinux.c  
Address: 192.168.200.112
```

```
> www.crushlinux.com  
服务器: ns2.crushlinux.com  
Address: 192.168.200.112
```

```
名称: www.crushlinux.com  
Address: 192.168.200.111
```

```
> mail.crushlinux.com  
服务器: ns2.crushlinux.com  
Address: 192.168.200.112
```

```
名称: mail.crushlinux.com  
Address: 192.168.200.112
```

```
> 192.168.200.113  
服务器: ns2.crushlinux.com  
Address: 192.168.200.112
```

```
名称: study.crushlinux.com  
Address: 192.168.200.113
```

```
> 192.168.200.112  
服务器: ns2.crushlinux.com
```

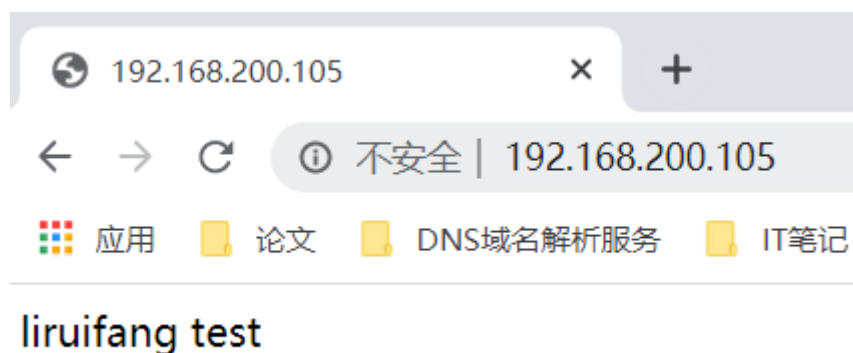

Address: 192.168.200.112

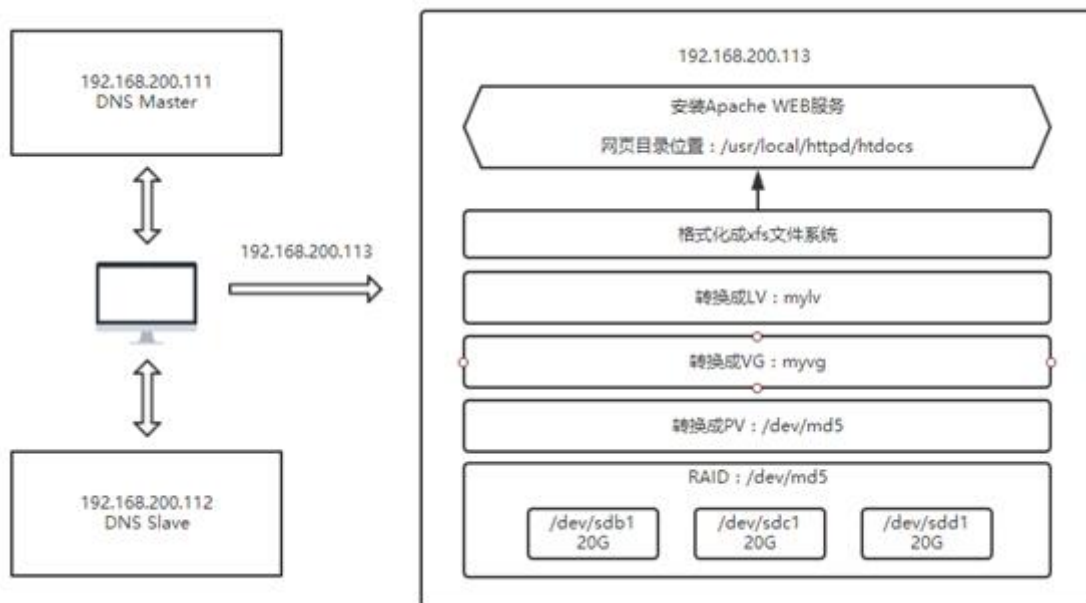
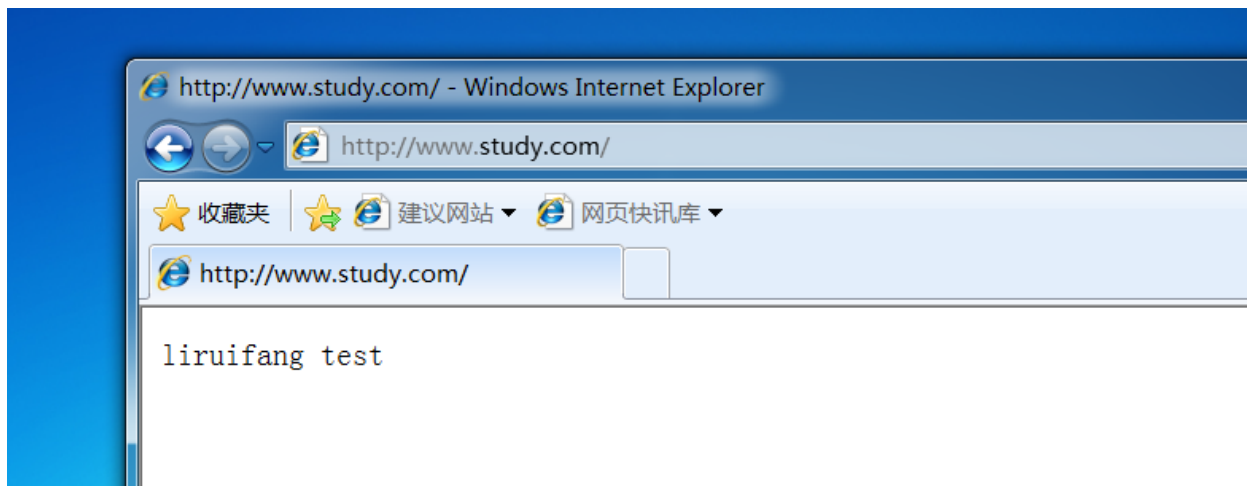
名称: mail.crushlinux.com

Address: 192.168.200.112

9、DNS解析综合学习案例

- 1、用户需把/dev/myvg/mylv逻辑卷以支持磁盘配额的方式挂载到网页目录下
- 2、在网页目录下创建测试文件index.html，内容为用户名称，通过浏览器访问测试
- 3、创建用户账户，对LVM配置磁盘配额限制用户磁盘容量为软限制80M；硬限制100M、文件数量软限制为80个；硬限制为100个。
- 4、构建主从DNS域名解析环境
- 5、主从DNS都可将
www.study.com域名解析为
192.168.200.113
- 6、客户机可通过浏览器访问
www.study.com得到WEB服务器相应内容
- 7、主域名服务器要同时担任缓存域名服务器功能
- 8、客户机通过nslookup域名测试工具可解析到
www.jd.com/www.taobao.com等网站的域名解析结果





- 1、缓存域名服务器
- 2、构建主从域名服务器
- 3、综合案例