

DNS 服务 使用 BIND

装包

```
yum -y install bind-chroot bind
```

bind-chroot #牢笼政策 为了安全

查看安装的包

```
rpm -qa bind*
```

BIND 服务端程序

主要执行程序

/usr/sbin/named

系统服务: named

默认端口: TCP/UDP 53

运行时的虚拟根环境 /var/named/chroot/

主配置文件: /etc/named.conf #主要负责 指定负责解析的域名是什么

地址库文件: /var/named/.. #主机名和IP地址的对应关系

主配置文件和地址库文件 都配置完成, 才能正常启动使用

正常解析: UDP 53

主从同步: TCP 53

开始操作修改主配置文件, 指定负责解析的域名为tedu.cn

修改主配置文件

```
vim /etc/named.conf
```

```
options {  
    listen-on port 53 { any ; };    # 把127.0.0.1 改为 any 或者这行直接删除
```

最终保留的内容为:

```
options {  
    directory    "/var/named";
```

```
zone "." IN {
    type hint;
    file "named.ca";
};
```

需要修改的内容:

```
options {
    directory      "/var/named";    #指定地址库的存放位置
```

```
zone "tedu.cn" IN {
    type master;                # hint 代表根域    ,    master 代表本区域的主
, slave 代表 从
    file "tedu.cn.zone";        #指定地址库文件
};
```

创建 /var/named 地址库文件 tedu.cn.zone"

手写太复杂, 去找模板

```
vim /var/named/named.localhost    #查看
```

复制这个文件起名 tedu.cn.zone

```
cp -p named.localhost tedu.cn.zone    # -p 参数 保留原始的文件所属组
```

修改库文件 tedu.cn.zone

```
vim /var/named/tedu.cn.zone
```

添加内容:

tedu.cn. NS svr7 # 也可以用@, @=tedu.cn. 域名, 仅在本文件中。取决于主配置文件。 NS=Name Server 域名服务

svr7.tedu.cn. A 192.168.239.144 #A 是IP解析 仅用于正向解析区域

www A 192.168.239.144

FTP A 192.168.239.144

重启服务

```
systemctl restart named
```

验证:

desktop虚拟机

修改DNS文件

```
vim /etc/resolv.conf
```

```
nameserver 192.168.239.144
```

验证DNS服务器

```
nslookup www.tedu.cn
```

```
nslookup ftp.tedu.cn
```

多区域的DNS服务器

修改/etc/named.conf

追加写入

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

添加qq.com.zone 库文件

```
cp -p /var/edu.cn.zone /var/qq.com.zone
```

修改配置文件

添加如下内容:

```
qq.com NS svr7
```

```
svr7 A 192.168.239.144 #A 是IP解析,仅用于正向解析区域
```

```
www A 1.1.1.1
```

```
FTP A 2.2.2.2
```

desktop 测试

```
nslookup www.qq.com
```

DNS的负载均衡, 解析结果的轮询

- 一个域名 多个不同IP地址
- 每个IP提供镜像服务内容

- 后期是用调度服务器来实现这个功能

```
minimum
8  tedu.cn.      NS  svr7
9  svr7          A   192.168.4.7
10 www          A   192.168.4.100
11 www          A   192.168.4.200
12 www          A   192.168.4.210
13 ftp          A   2.2.2.2
14
15
16
17
18 ■
```

泛域名解析

匹配本域内未定义的任何主机地址

- 直接以*条目匹配
- 一般只用在正向区域文件中

```
vim /var/named/qq.com.zone
```

```
qq.com  NS  svr7
```

```
svr7    A   192.168.239.144
```

```
www     A   1.1.1.1
```

```
FTP     A   2.2.2.2
```

```
      *           A 2.2.2.2    #用* 来定义泛域名，代表任意
```

有规律的泛域名解析

举例

```
stu1.tedu.cn-----> 192.168.10.1
```

```
stu2.tedu.cn-----> 192.168.10.2
```

```
stu3.tedu.cn-----> 192.168.10.3
```

```
stu4.tedu.cn-----> 192.168.10.4
```

```
stu5.tedu.cn-----> 192.168.10.5
```

```
stu6.tedu.cn-----> 192.168.10.6
```

可以生成连续范围的数字

\$GENERATE 生成连续范围的数字 必须大写 这是个函数

```
$GENERATE 1-60 stu$.tedu.cn. A 192.168.10.$
```

```
vim /var/named/tedu.cn.zone
```

```
$TTL 1D
```

```
@      IN SOA  @ rname.invalid. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum
```

```
tedu.cn.      NS      svr7
svr7           A       192.168.239.144
www           A       1.1.1.1
ftp           A       2.2.2.2
*             A       10.10.10.10
$GENERATE 1-60 stu$.tedu.cn. A 192.168.10.$
```

DNS子域授权

父域: www.tedu.cn #父域的DNS, 负责tedu.cn

子域: www.bj.tedu.cn #子域的DNS, 负责bj.tedu.cn

在虚拟机desktop上进行子域的搭建和测试

装包: yum -y install chroot-bind bind

修改主配置文件

```
vim /etc/named.conf
```

```
options {
    listen-on port 53 { any; };
    directory    "/var/named";
```

```
logging {
```

```

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

```

```

zone "bj.tedu.cn" IN {
    type master;
    file "bj.tedu.cn.zone";
};

```

保存退出

复制并修改库文件

```
cp -p /var/named/named.localhost /var/named/bj.tedu.cn.zone
```

\$TTL 1D

```

@      IN SOA  @ rname.invalid. (
                                0      ; serial
                                1D     ; refresh
                                1H     ; retry
                                1W     ; expire
                                3H )   ; minimum

```

```

bj.tedu.cn.      NS      bogon
bogon  A          192.168.239.145
www    A          1.2.3.4

```

重启DNS服务

```
systemctl restart named
```

验证:

```
nslookup www.bj.tedu.cn 192.168.239.145 # 指定DNS的IP地址为 192.168.239.145
```

输出结果:

```
[root@bogon named]# nslookup www.bj.tedu.cn 192.168.239.145
```

Server: 192.168.239.145
Address: 192.168.239.145#53

Name: www.bj.tedu.cn

Address: 1.2.3.4

父域的DNS服务器，能够解析tedu.cn结尾的主机名（父域的解析名）

子域的DNS服务器，能够解析bj.tedu.cn结尾的主机名（子域的解析名）

最终实现

父域的DNS服务器，能够解析bj.tedu.cn结尾的主机名（子域的解析名）

使用的方式：

子域名授权

需要在父域的库配置文件中添加如下内容

bj.tedu.cn. NS bogon.bj.tedu.cn. 或者bogon #bogon 是主机名

bogon.bj.tedu.cn. 或者bogon A 192.168.239.145

递归解析：DNS服务器，与其他DNS服务器交互，最终将解析结果带回来的过程

禁止递归

方法如下：

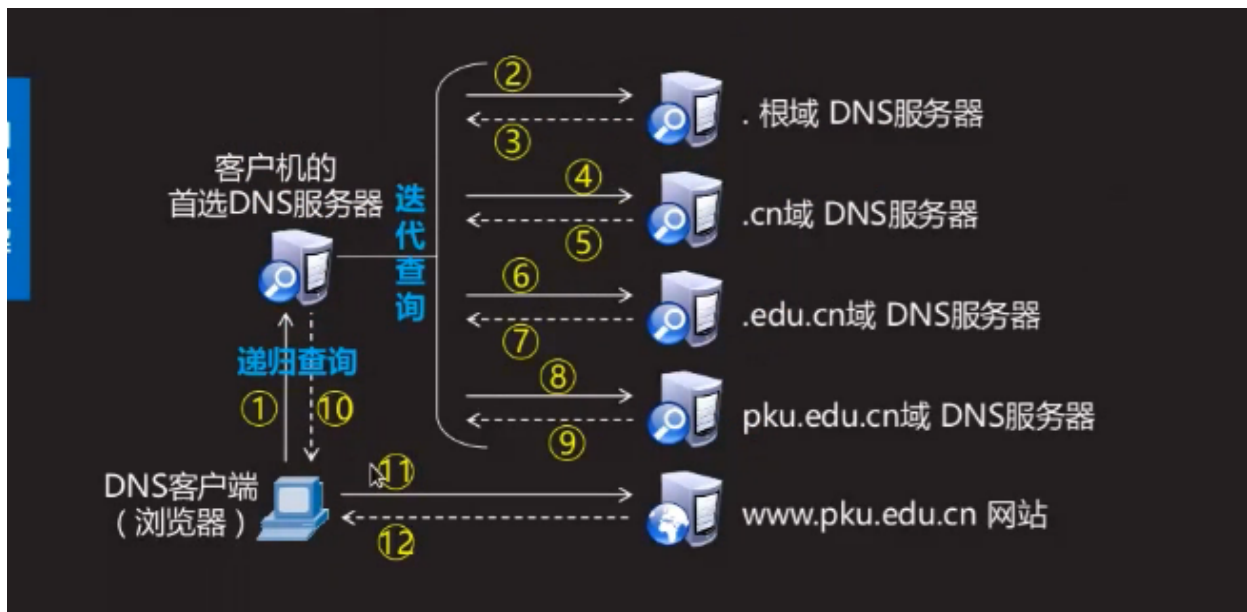
vim /etc/named.conf

```
options {  
    listen-on port 53 { any; };  
    directory "/var/named";  
    recursion no;    #禁止递归  
};
```

```
zone "tedu.cn" IN {  
    type master;  
    file "tedu.cn.zone";  
};
```

迭代解析

从 根域 . 一级一级的往下查你要的网址



子域转发

子域的DNS，能够解析父域的tedu.cn

desktop上更改主配置文件

```
vim /etc/named.conf
```

```
4yy p
```

```
zone "tedu.cn" IN {
    type forward;
    forwarders { 192.168.239.144; };
};
```

保存退出

重启

```
systemctl restart named
```

验证

```
[root@bogon named]# nslookup www.tedu.cn 192.168.239.145
```

```
Server:          192.168.239.145
```

```
Address:         192.168.239.145#53
```

Non-authoritative answer:

Name: www.tedu.cn

Address: 1.1.1.1

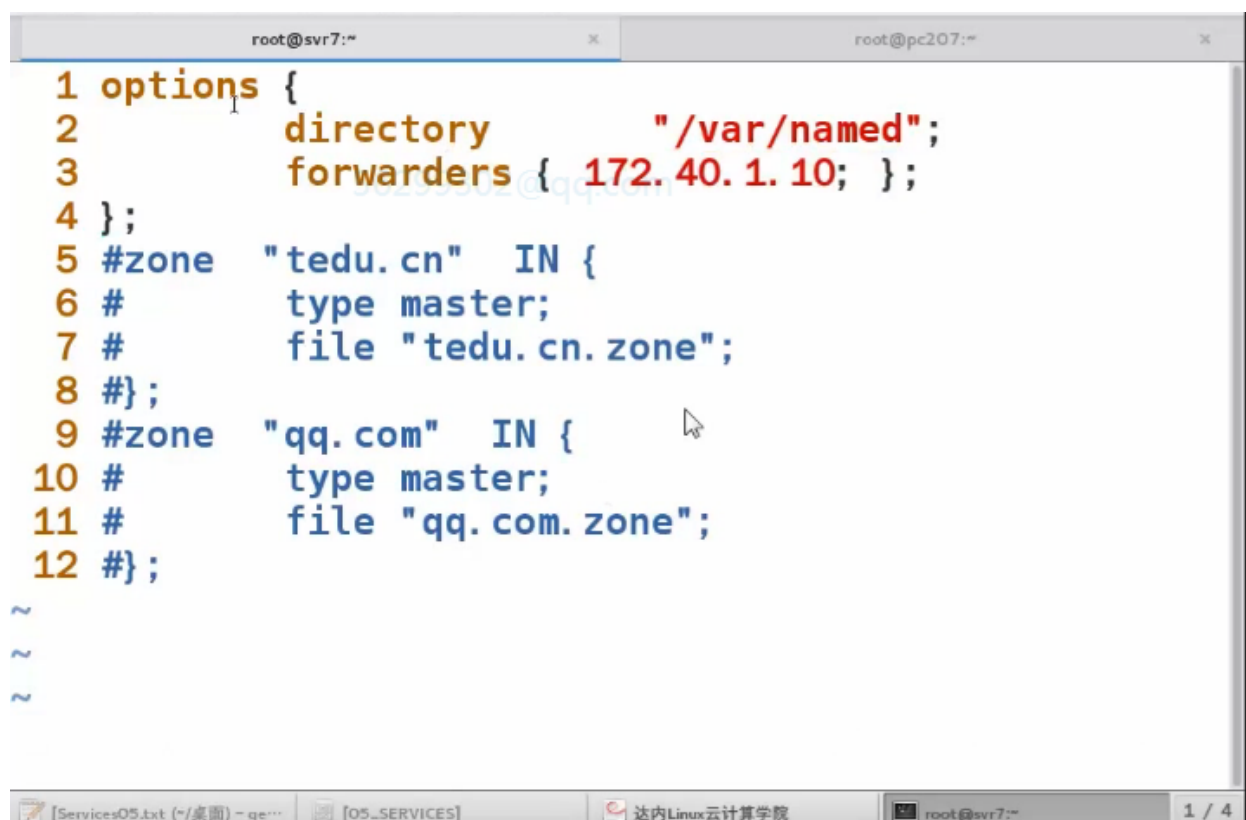
缓存DNS

方式1: 全局转发

-讲所有请求发给指定的公共DNS, 请求递归服务

方式2: 根域迭代

依次向根, 一级, 二级.....域的DNS服务器迭代



```
1 options {
2     directory "/var/named";
3     forwarders { 172.40.1.10; };
4 };
5 #zone "tedu.cn" IN {
6 #     type master;
7 #     file "tedu.cn.zone";
8 #};
9 #zone "qq.com" IN {
10 #     type master;
11 #     file "qq.com.zone";
12 #};
~
~
~
```

只需要一条

```
forwarders { 202.106.196.115; };
```

保存退出并重启验证

