DNS 服务基础、特殊解析、DNS 子域授权、缓存 DNS

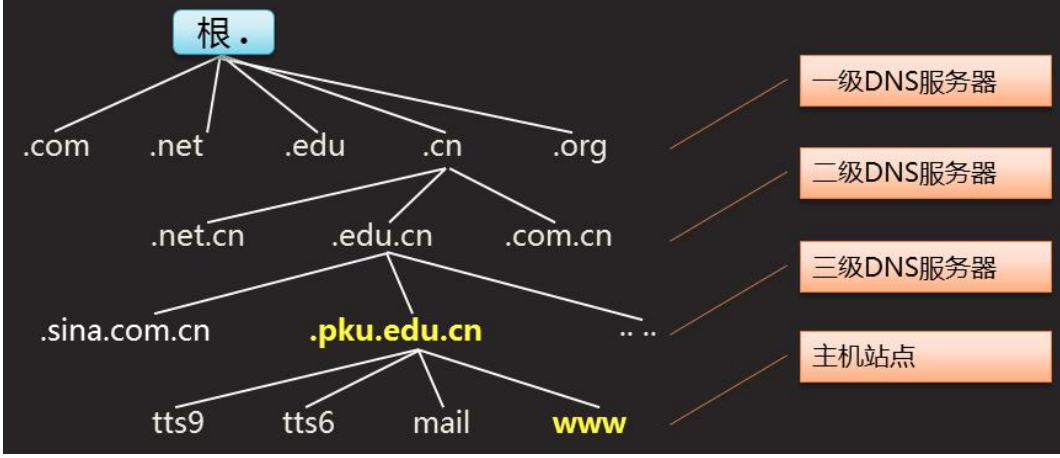
DNS服务器的功能

DNS 解析的作用

- 正向解析：根据注册的域名查找其对应的IP地址
- 反向解析：根据IP地址查找对应的注册域名，不常用

• 大型、分布式的互联网DNS解析库

DNS 的分布式结构



Full Qualified Domain Name，完全合格主机名

- = 站点名.域名后缀
- = 站点名. .. .. .二级域.一级域

比如，www.pku.edu.cn

常见的顶级/一级域名

- 国家/地区域：.cn、.us、.kr、.hk、.tw、.. ..
- 组织域：.com、.net、.edu、.org、.gov、.mil、.. ..

搭建 DNS 服务器

BIND（Berkeley Internet Name Daemon）

- 伯克利 Internet 域名服务
- 官方站点：https://www.isc.org/

```
[root@svr7 ~]# yum -y install bind-chroot bind
[root@svr7 ~]# rpm -qa bind*
bind-9.9.4-29.el7.x86_64                  //域名服务包
bind-chroot-9.9.4-29.el7.x86_64           //提供虚拟根支持（牢笼政策）
```

BIND服务器端程序

– 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 设置本机负责解析的域名（解析哪些域名）

地址库文件：/var/named/.. .. 主机名与 IP 地址对应关系

1 安装软件包

```
[root@svr7 ~]# yum -y install bind-chroot bind
已加载插件：langpacks, product-id, search-disabled-repos, subscription-m
anager
```

```
[root@svr7 ~]# rpm -q bind
bind-9.9.4-29.el7.x86_64
[root@svr7 ~]# rpm -q bind-chroot
bind-chroot-9.9.4-29.el7.x86_64
```

2 修改配置文件 /etc/named.conf

```
[root@svr7 ~]# vim /etc/named.conf
```

```
options {
        directory       "/var/named";#指定地址库文件位置
};
zone "tedu.cn" IN {       #指定本机解析的域名
        type master;   #指定本机为主 DNS 服务器
        file "tedu.cn.zone";#指定域名解析的地址库文件的名字
};
```

3 创建地址库文件 /var/named/tedu.cn.zone

```
[root@svr7 ~]# cd /var/named
[root@svr7 named]# cp -p named.localhost tedu.cn.zone
[root@svr7 named]# ls -l tedu.cn.zone
-rw-r-----. 1 root named 152 6月  21 2007 tedu.cn.zone
```

```
[root@svr7 named]# vim tedu.cn.zone
```

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
tedu.cn.        NS      svr7    #声明域名的服务器名称
svr7            A       192.168.4.7  #解析 DNS 主机名对应 IP
www             A       1.1.1.1      #主机名解析记录
ftp             A       2.2.2.2      #主机名解析记录
```

4 重启 named 服务，设置开机自启

```
[root@svr7 named]# systemctl restart named
[root@svr7 named]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.s
ervice to /usr/lib/systemd/system/named.service.
```

5 客户端

```
[root@pc207 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf
[root@pc207 ~]# nslookup www.tedu.cn
Server:         192.168.4.7
Address:        192.168.4.7#53

Name:   www.tedu.cn
Address: 1.1.1.1
```

泛域名解析

```
[root@svr7 named]# vim 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       192.168.4.7
www             A       1.1.1.1
ftp             A       2.2.2.2
*               A       10.11.12.13
tedu.cn.        A       100.110.120.130
```

```
[root@svr7 named]# systemctl restart named
```

```
[root@pc207 ~]# nslookup tedu.cn
Server:         192.168.4.7
Address:        192.168.4.7#53

Name:   tedu.cn
Address: 100.110.120.130
```

```
[root@pc207 ~]# nslookup haha.tedu.cn
Server:         192.168.4.7
Address:        192.168.4.7#53

Name:   haha.tedu.cn
Address: 10.11.12.13
```

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

```
[root@svr7 ~]# vim  /var/named/tedu.cn.zone
.. ..
*               IN      A       192.168.4.100       //最后一条记录
                                                    //正向区域文件
```

有规律的泛域名解析

$GENERATE 生成连续范围的数字

```
[root@svr7 named]# vim 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       192.168.4.7
www             A       1.1.1.1
ftp             A       2.2.2.2
*               A       10.11.12.13
tedu.cn.        A       100.110.120.130
$GENERATE 1-50 pc$ A 192.168.10.$
```

```
[root@svr7 named]# systemctl restart named
```

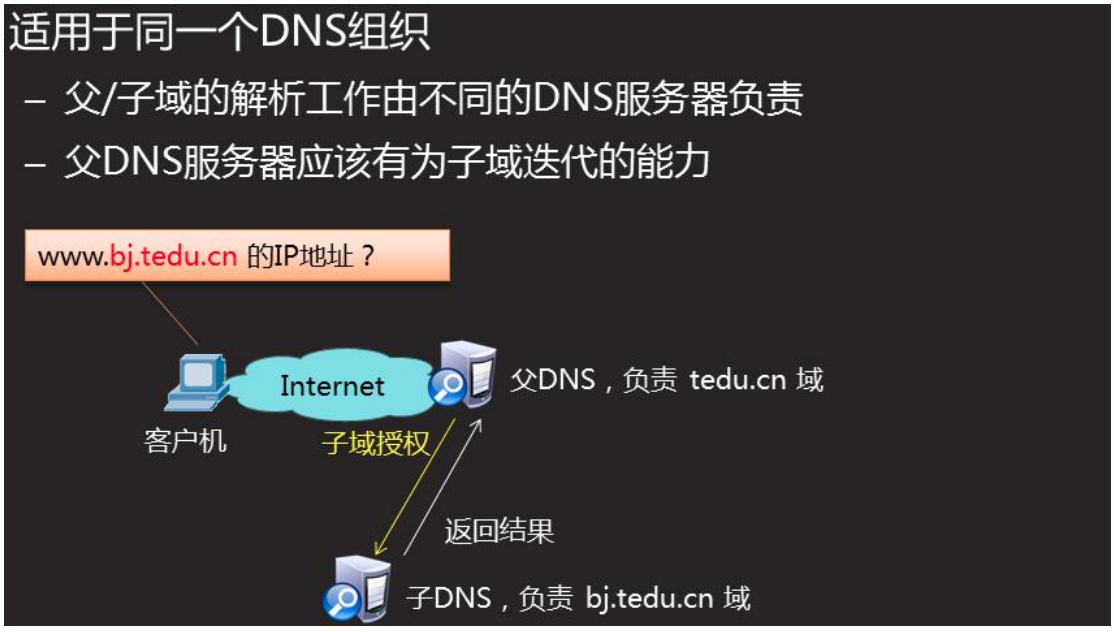
```
[root@pc207 ~]# nslookup pc1.tedu.cn
Server:         192.168.4.7
Address:        192.168.4.7#53

Name:   pc1.tedu.cn
Address: 192.168.10.1

[root@pc207 ~]# nslookup pc10.tedu.cn
Server:         192.168.4.7
Address:        192.168.4.7#53

Name:   pc10.tedu.cn
Address: 192.168.10.10
```

DNS 子域授权



父域：www.tedu.cn

子域：www.bj.tedu.cn

虚拟机 A 能够解析父域的域名：tedu.cn

虚拟机 B 能够解析子域的域名：bj.tedu.cn

子域授权：

客户端解析 www.bj.tedu.cn---->192.168.4.7 能得到虚拟机 B 的解析

虚拟机 B：

```
[root@pc207 ~]# yum -y install bind-chroot bind
```

```
[root@pc207 ~]# vim /etc/named.conf
```

```
options {
        directory       "/var/named";
};
zone "bj.tedu.cn" IN {
        type master;
        file "bj.tedu.cn.zone";
};
```

```
[root@pc207 ~]# cd /var/named
[root@pc207 named]# cp -p named.localhost bj.tedu.cn.zone
```

```
[root@pc207 named]# vim bj.tedu.cn.zone
```

```
$TTL 1D
@       IN SOA  @ rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
bj.tedu.cn.     NS          pc207
pc207           A           192.168.4.207
www             A           4.4.5.5
```

```
[root@pc207 named]# systemctl restart named
```

虚拟机 A：

```
[root@svr7 named]# 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
bj.tedu.cn.     NS      pc207
svr7            A       192.168.4.7
pc207           A       192.168.4.207
www             A       1.1.1.1
ftp             A       2.2.2.2
*               A       10.11.12.13
tedu.cn.        A       100.110.120.130
$GENERATE 1-50 pc$ A 192.168.10.$
```

```
[root@svr7 named]# systemctl restart named
[root@svr7 named]# nslookup www.bj.tedu.cn 192.168.4.7
Server:         192.168.4.7
Address:        192.168.4.7#53

Non-authoritative answer:
Name:   www.bj.tedu.cn
Address: 4.4.5.5
```

递归查询：主 DNS 服务器，与其他 DNS 交互，最后将解析结果返回给客户端

迭代查询

##
客户端解析 www.bj.tedu.cn---->192.168.4.7 能得到虚拟机 B 的解析
子域转发：
虚拟机 B

```
[root@pc207 named]# vim /etc/named.conf
```

```
options {
        directory       "/var/named";
};
zone "bj.tedu.cn" IN {
        type master;
        file "bj.tedu.cn.zone";
};
zone "tedu.cn" IN {
        type forward;
        forwarders  {   192.168.4.7;        };
};
```

```
[root@pc207 named]# systemctl restart named
[root@pc207 named]# nslookup www.tedu.cn 192.168.4.207
Server:         192.168.4.207
Address:        192.168.4.207#53

Non-authoritative answer:
Name:   www.tedu.cn
Address: 1.1.1.1
```

##
缓存 DNS 服务器

权威/官方DNS

- 至少管理一个DNS区域，，需要IANA等官方机构授权
- 典型应用：根域DNS、一级域DNS、.. ..

缓存DNS

- 不需要管理任何DNS区域，但是能够替客户机查询，而且通过缓存、复用查询结果来加快速度
- 典型应用：ISP服务商、企业局域网

方式1：全局转发

- 将请求转发给指定的公共DNS（其他缓存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