# BIND提供域名解析服务

1 DNS域名解析服务

2 正向解析实验

3 反向解析实验

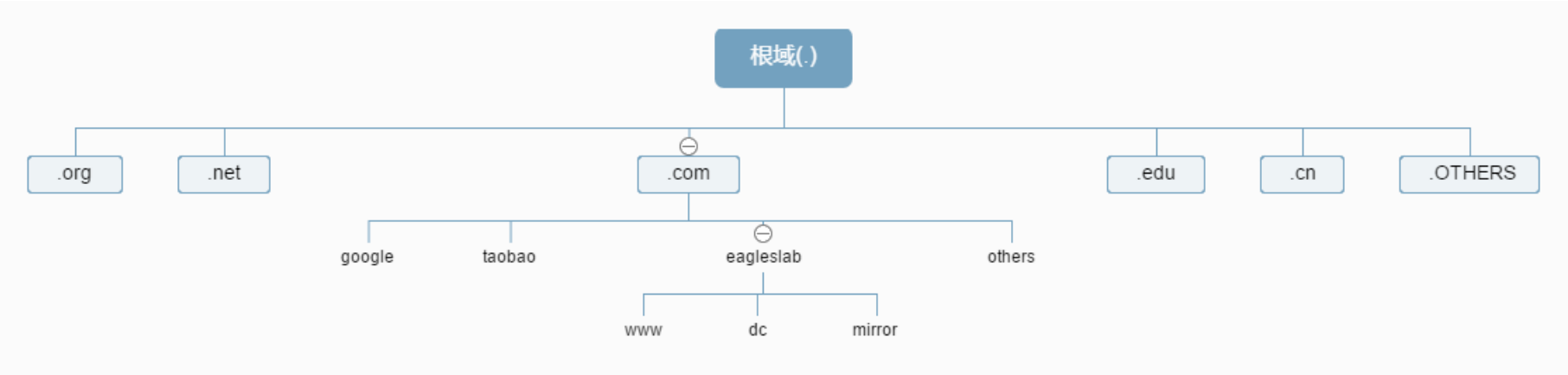
4 部署从服务器

5 安全的加密传输

# DNS域名解析服务

# DNS域名解析服务

DNS域名解析服务采用的目录树层次结构



# DNS域名解析服务

13台根DNS服务器的具体信息

| 名称 | 管理单位 | 地理位置 | IP地址 |
|---|---|---|---|
| A | INTERNIC.NET | 美国弗吉尼亚州 | 198.41.0.4 |
| B | 美国信息科学研究所 | 美国加利福尼亚州 | 128.9.0.107 |
| C | PSINet公司 | 美国弗吉尼亚州 | 192.33.4.12 |
| D | 马里兰大学 | 美国马里兰州 | 128.8.10.90 |
| E | 美国航空航天管理局 | 美国加利福尼亚州 | 192.203.230.10 |
| F | 因特网软件联盟 | 美国加利福尼亚州 | 192.5.5.241 |
| G | 美国国防部网络信息中心 | 美国弗吉尼亚州 | 192.112.36.4 |
| H | 美国陆军研究所 | 美国马里兰州 | 128.63.2.53 |
| I | Autonomica公司 | 瑞典斯德哥尔摩 | 192.36.148.17 |
| J | VeriSign公司 | 美国弗吉尼亚州 | 192.58.128.30 |
| K | RIPE NCC | 英国伦敦 | 193.0.14.129 |
| L | IANA | 美国弗吉尼亚州 | 199.7.83.42 |
| M | WIDE Project | 日本东京 | 202.12.27.33 |

# DNS域名解析服务

安装bind服务程序

```
[root@server ~]# yum install bind bind-chroot bind-utils
```

在bind服务程序中有下面这三个比较关键的文件。

- 主配置文件（/etc/named.conf）：只有58行，而且在去除注释信息和空行之后，实际有效的参数仅有30行左右，这些参数用来定义bind服务程序的运行。
- 区域配置文件（/etc/named.rfc1912.zones）：用来保存域名和IP地址对应关系的所在位置。类似于图书的目录，对应着每个域和相应IP地址所在的具体位置，当需要查看或修改时，可根据这个位置找到相关文件。
- 数据配置文件目录（/var/named）：该目录用来保存域名和IP地址真实对应关系的数据配置文件。

# DNS域名解析服务

首先需要在/etc目录中找到该服务程序的主配置文件，
然后把第13行和第19行的地址均修改为any，

- 分别表示服务器上的所有IP地址均可提供DNS域名解析服务，
- 以及允许所有人对本服务器发送DNS查询请求。这两个地方一定要修改准确。

```
[root@localhost ~]# vi /etc/named.conf
------------省略部分内容------------------
options {
         listen-on port 53 { any; };
         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_mem_stats.txt";
         allow-query     { any; };
------------省略部分内容------------------
```

# DNS域名解析服务

bind服务程序的区域配置文件（/etc/named.rfc1912.zones）用来保存域名和IP地址对应关系的所在位置。

在这个文件中，定义了域名与IP地址解析规则保存的文件位置以及服务类型等内容，而没有包含具体的域名、IP地址对应关系等信息。

服务类型有三种，分别为hint（根区域）、master（主区域）、slave（辅助区域），其中常用的master和slave指的就是主服务器和从服务器。

```
[root@localhost ~]# vi /etc/named.rfc1912.zones
------------省略部分内容-----------------
 zone "localhost.localdomain" IN {
            type master;
            file "named.localhost";
            //服务类型，域名与IP地址解析规则保存的文件位置
            allow-update { none; };
            //允许哪些客户机动更新解析信息
};

zone "localhost" IN {
            type master;
            file "named.localhost";
            allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
            type master;
            file "named.loopback";
            allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
    //表示127.0.0.1的反向解析区域
            type master;
            file "named.loopback";
            allow-update { none; };
};

zone "0.in-addr.arpa" IN {
            type master;
            file "named.empty";
            allow-update { none; };
};
```

# DNS域名解析服务

可以执行named-checkconf命令和named-checkzone命令，分别检查主配置文件与数据配置文件中语法或参数的错误。

# 正向解析实验

正向解析是指根据域名（主机名）查找到对应的IP地址。也就是说，当用户输入了一个域名后，bind服务程序会自动进行查找，并将匹配到的IP地址返给用户。这也是最常用的DNS工作模式。

# 编辑区域配置文件

```
[root@localhost ~]# vi /etc/named.rfc1912.zones
----------省略部分内容-----------
zone "test.com" IN {
        type master;
        file "test.com.zone";
        allow-update { none; };
};
```

# 编辑数据配置文件

```
[root@localhost ~]# cd /var/named
[root@localhost named]# ls -al named.localhost
-rw-r-----. 1 root named 152 6月  21 2007 named.localhost
[root@localhost named]# cp -a named.localhost test.com.zone
[root@localhost named]# vi test.com.zone
[root@localhost named]# cat test.com.zone
$TTL 1D
@       IN SOA    test.com. admin.test.com. (
                                               0         ; serial
                                               1D        ; refresh
                                               1H        ; retry
                                               1W        ; expire
                                               3H )      ; minimum
        NS        ns.test.com.
ns      IN A      192.168.9.101
        IN MX 10  mail.test.com.
mail    IN A      192.168.9.101
www     IN A      192.168.9.101
bbs     IN A      192.168.9.101
        IN AAAA   ::1
[root@localhost named]# systemctl restart named
```

# 编辑数据配置文件

| | | | | | |
|---|---|---|---|---|---|
| $TTL 1D | #生存周期为1天 | | | | |
| @ | IN SOA | test.com. | root.test.com. | ( | |
| | #授权信息开始 | #DNS区域的地址 | #域名管理员的邮箱（不要用@符号） | | |
| | | | | 0;serial | #更新序列号 |
| | | | | 1D;refresh | #更新时间 |
| | | | | 1H;retry | #重试延时 |
| | | | | 1W;expire | #失效时间 |
| | | | | 3H);minimum | #无效解析记录的缓存时间 |
| | NS | ns.test.com. | | #域名服务器记录 | |
| ns | IN A | 192.168.9.101 | | #地址记录（ns.test.com.） | |
| | IN MX 10 | mail.test.com. | | #邮箱交换记录 | |
| mail | IN A | 192.168.9.101 | | #地址记录（mail.test.com.） | |
| www | IN A | 192.168.9.101 | | #地址记录（www.test.com.） | |
| bbs | IN A | 192.168.9.101 | | #地址记录（bbs.test.com.） | |

# 更改本地DNS解析服务器

```
[root@localhost ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search localdomain
nameserver 192.168.9.101
[root@localhost ~]# nslookup
> bbs.test.com
Server:            192.168.9.101
Address: 192.168.9.101#53

Name:    bbs.test.com
Address: 192.168.9.101
```

# 反向解析实验

# 编辑区域配置文件

```
[root@localhost ~]# vi /etc/named.rfc1912.zones
--------省略部分内容------------
zone "9.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.9.arpa";
};
```

# 编辑数据配置文件

```
[root@localhost named]# cd /var/named/
[root@localhost named]# cp -a named.loopback 192.168.9.arpa
[root@localhost named]# vi 192.168.9.arpa
$TTL 1D
@       IN SOA  test.com. admin.test.com. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      test.com.
ns      A       192.168.9.101
        AAAA    ::1
101      PTR     ns.test.com.
101      PTR     mail.test.com.
102      PTR     www.test.com.
101      PTR     bbs.test.com.
[root@localhost named]# nslookup
> 192.168.9.101
Server:               192.168.9.101
Address:   192.168.9.101#53

142.179.168.192.in-addr.arpa     name = mail.test.com.
142.179.168.192.in-addr.arpa     name = bbs.test.com.
142.179.168.192.in-addr.arpa     name = ns.test.com.
142.179.168.192.in-addr.arpa     name = www.test.com.
>
```

# 编辑数据配置文件

| | | | | |
|---|---|---|---|---|
| $TTL 1D | | | | |
| @ | IN SOA | test.com. | admin.test.com. | ( |
| | | | | 0;serial |
| | | | | 1D;refresh |
| | | | | 1H;retry |
| | | | | 1W;expire |
| | | | | 3H);minimum |
| | NS | ns.test.com. | | |
| ns | A | 192.168.9.101 | | |
| 10 | PTR | ns.test.com. | #PTR为指针记录，仅用于反向解析 | |
| 10 | PTR | mail.test.com. | | |
| 10 | PTR | www.test.com. | | |
| 20 | PTR | bbs.test.com. | | |