马哥教育
IT人的高薪职业学院

DNS服务和BIND

讲师：王晓春

域名系统 DNS

本章内容

- **名字解析介绍**
- **DNS服务工作原理**
- **实现主服务器**
- **实现反向解析区域**
- **实现从服务器**
- **实现子域**
- **实现转发**

- **实现智能DNS**
- **DNS排错**

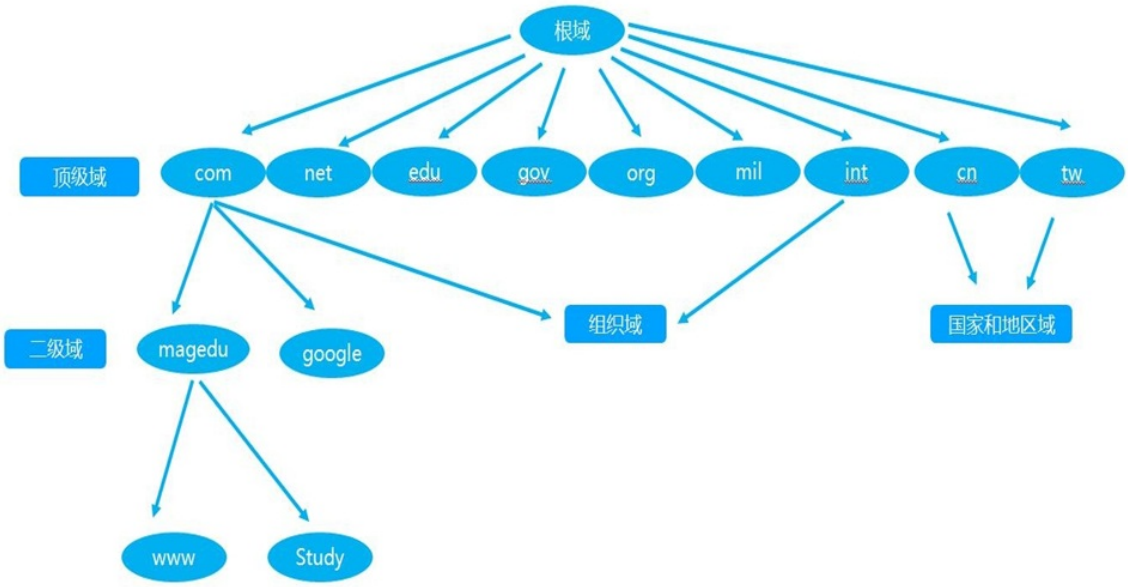
1 名字解析介绍和DNS

当前TCP/IP网络中的设备之间进行通信，是利用和依赖于IP地址实现的。但数字形式的IP地址是很难记忆的。当网络设备众多，想要记住每个设备的IP地址，可以说是"不可能完成的任务"。那么如何解决这一难题呢？我们可以给每个网络设备起一个友好的名称，如：www.magedu.org，这种由文字组成的名称，显而易见要更容易记忆。但是计算机不会理解这种名称的，我们可以利用一种名字解析服务将名称转化成（解析）成IP地址。从而我们就可以利用名称来直接访问网络中设备了。而实现此服务的方法是多样的。如下面所述：

本地名称解析配置文件：hosts Linux: /etc/hosts windows: %WINDIR%/system32/drivers/etc/hosts 122.10.117.2 www.magedu.org 93.46.8.89 www.google.com

DNS：Domain Name System 域名系统,应用层协议,是互联网的一项服务。它作为将域名和IP地址相互映射的一个分布式数据库，能够使人更方便地访问互联网 C/S,53/udp, 53/tcp BIND：Bekerley Internat Name Domain,由ISC（www.isc.org）提供的DNS软件实现

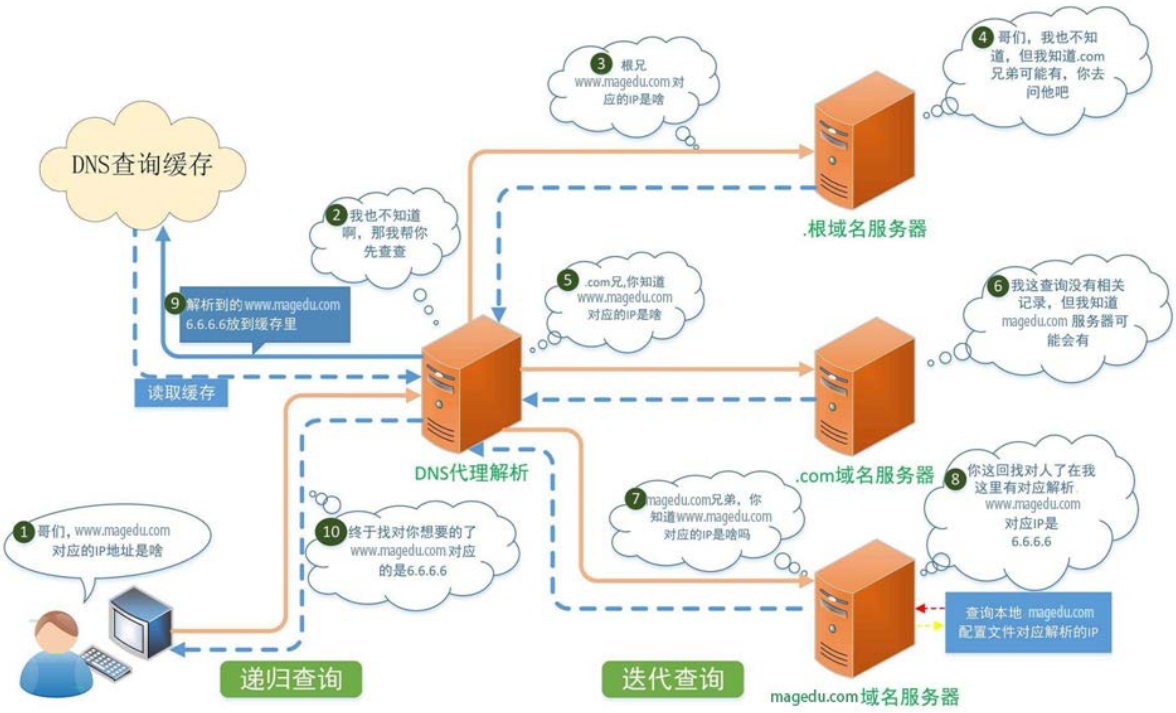
1.1 DNS域名结构



- 根域
- 一级域名：Top Level Domain: tld com, edu, mil, gov, net, org, int,arpa 三类：组织域、国家域(.cn, .ca, .hk, .tw)、反向域
- 二级域名：magedu.com
- 三级域名：study.magedu.com
- 最多可达到127级域名

ICANN（The Internet Corporation for Assigned Names and Numbers）互联网名称与数字地址分配机构，负责在全球范围内对互联网通用顶级域名（gTLD）以及国家和地区顶级域名（ccTLD）系统的管理、以及根服务器系统的管理

1.2 DNS服务工作原理



1.3 DNS查询类型：

- 递归查询
- 迭代查询

1.4 名称服务器

Name Server,域内负责解析本域内的名称的DNS服务器

根名称服务器：13组负责解析根域的DNS服务器

1.5 解析类型

- FQDN --> IP
- IP --> FQDN

  注意：正反向解析是两个不同的名称空间，是两棵不同的解析树

1.6 完整的查询请求经过的流程

```
Client -->hosts文件 -->DNS Service Local Cache --> DNS Server (recursion) -->
Server Cache --```>iteration(迭代) --> 根--> 顶级域名DNS-->二级域名DNS…
```

2 DNS 服务相关概念和技术

2.1 DNS服务器的类型

- 主DNS服务器
- 从DNS服务器
- 缓存DNS服务器（转发器）

  #### 2.1.1 主DNS服务器：

  管理和维护所负责解析的域内解析库的服务器

2.1.2 从DNS服务器：

从主服务器或从服务器"复制"（区域传输）解析库副本

序列号：解析库版本号，主服务器解析库变化时，其序列递增 刷新时间间隔：从服务器从主服务器请求同步解析的时间间隔 重试时间间隔：从服务器请求同步失败时，再次尝试时间间隔 过期时长：从服务器联系不到主服务器时，多久后停止服务 "通知"机制：主服务器解析库发生变化时，会主动通知从服务器

2.2 区域传输

完全传输：传送整个解析库 增量传输：传递解析库变化的那部分内容

2.3 解析形式

正向：FQDN（ Fully Qualified Domain Name ） --> IP 反向: IP --> FQDN

2.4 负责本地域名的正向和反向解析库

正向区域 反向区域

2.5 解析答案

肯定答案：存在对应的查询结果

否定答案：请求的条目不存在等原因导致无法返回结果

权威答案：直接由存有此查询结果的DNS服务器（权威服务器）返回的答案

非权威答案：由其它非权威服务器返回的查询答案

2.6 各种资源记录

区域解析库：由众多RR组成： 资源记录：Resource Record, RR 记录类型：A, AAAA, PTR, SOA, NS, CNAME, MX

- SOA：Start Of Authority，起始授权记录；一个区域解析库有且仅能有一个SOA记录，必须位于解析库的第一条记录
- A：internet Address，作用，FQDN --> IP
- AAAA：FQDN --> IPv6
- PTR：PoinTeR，IP --> FQDN
- NS：Name Server，专用于标明当前区域的DNS服务器
- CNAME ： Canonical Name，别名记录
- MX：Mail eXchanger，邮件交换器
- TXT：对域名进行标识和说明的一种方式，一般做验证记录时会使用此项，如：SPF（反垃圾邮件）记录，https验证等，如下示例：

```
_dnsauth TXT  20120112000000051qgs69bwoh4h6nht4n1h0lr038x
```

2.6.1 资源记录定义的格式

```
语法：name     [TTL]   IN  rr_type     value
```

注意：

1. TTL可从全局继承

2. 使用 “@” 符号可用于引用当前区域的名字
3. 同一个名字可以通过多条记录定义多个不同的值；此时DNS服务器会以轮询方式响应
4. 同一个值也可能有多个不同的定义名字；通过多个不同的名字指向同一个值进行定义；此仅表示通过多个不同的名字可以找到同一个主机

2.6.2 SOA记录

name: 当前区域的名字，例如“magedu.org.” value: 有多部分组成

注意：

1. 当前区域的主DNS服务器的FQDN，也可以使用当前区域的名字
2. 当前区域管理员的邮箱地址；但地址中不能使用@符号，一般用.替换 例如：admin.magedu.org
3. 主从服务区域传输相关定义以及否定的答案的统一的TTL

范例：

```
magedu.org.     86400   IN  SOA     ns.magedu.org.  nsadmin.magedu.org.     (
        2015042201  ;序列号
        2H              ;刷新时间
        10M     ;重试时间
        1W      ;过期时间
        1D      ;否定答案的TTL值
        )
```

2.6.3 NS记录

name: 当前区域的名字 value: 当前区域的某DNS服务器的名字，例如ns.magedu.org.

注意：

1. 相邻的两个资源记录的name相同时，后续的可省略
2. 对NS记录而言，任何一个ns记录后面的服务器名字，都应该在后续有一个A记录
3. 一个区域可以有多个NS记录

范例：

```
magedu.org. IN  NS      ns1.magedu.org.
magedu.org. IN  NS      ns2.magedu.org.
```

2.6.4 MX记录

name: 当前区域的名字 value: 当前区域的某邮件服务器(smtp服务器)的主机名

注意：

1. 一个区域内，MX记录可有多个；但每个记录的value之前应该有一个数字(0-99)，表示此服务器的优先级；数字越小优先级越高
2. 对MX记录而言，任何一个MX记录后面的服务器名字，都应该在后续有一个A记录

范例：

```
magedu.org. IN      MX  10  mx1.magedu.org.
            IN      MX  20  mx2.magedu.org.
```

2.6.5 A记录

name: 某主机的FQDN，例如：www.magedu.org. value: 主机名对应主机的IP地址

避免用户写错名称时给错误答案，可通过泛域名解析进行解析至某特定地址

范例：

```
www.magedu.org.          IN      A   1.1.1.1
www.magedu.org.          IN      A   2.2.2.2
mx1.magedu.org.          IN      A   3.3.3.3
mx2.magedu.org.          IN      A   4.4.4.4
$GENERATE 1-254 HOST$    IN      A   1.2.3.$
*.magedu.org.            IN      A   5.5.5.5
magedu.org.              IN      A   6.6.6.6
```

2.6 6 AAAA记录

name: FQDN value: IPv6

2.6.7 PTR记录

name: IP，有特定格式，把IP地址反过来写，1.2.3.4，要写作4.3.2.1；而有特定后缀：in-addr.arpa.，所以完整写法为：4.3.2.1.in-addr.arpa. value: FQDN

注意：网络地址及后缀可省略；主机地址依然需要反着写

例如：

```
4.3.2.1.in-addr.arpa. IN PTR www.magedu.org.
#如1.2.3为网络地址，可简写成：
4   IN  PTR     www.magedu.org.
```

2.6.8 CNAME别名记录

name: 别名的FQDN value: 真正名字的FQDN 例如：

```
www.magedu.org.  IN  CNAME   websrv.magedu.org.
```

2.7 子域授权

每个域的名称服务器，都是通过其上级名称服务器在解析库进行授权,类似根域授权tld

glue record：粘合记录，父域授权子域的记录

范例：

```
.com.       IN      NS      ns1.com.
.com.       IN          NS  ns2.com.
ns1.com.    IN      A   2.2.2.1
ns2.com.    IN      A   2.2.2.2
#magedu.org. 在.com的名称服务器上，解析库中添加资源记录
magedu.org.         IN  NS  ns1.magedu.org.
magedu.org.         IN  NS  ns2.magedu.org.
magedu.org.         IN  NS  ns3.magedu.org.
ns1.magedu.org.     IN  A   3.3.3.1
ns2.magedu.org.     IN  A   3.3.3.2
ns3.magedu.org.     IN  A   3.3.3.3
```

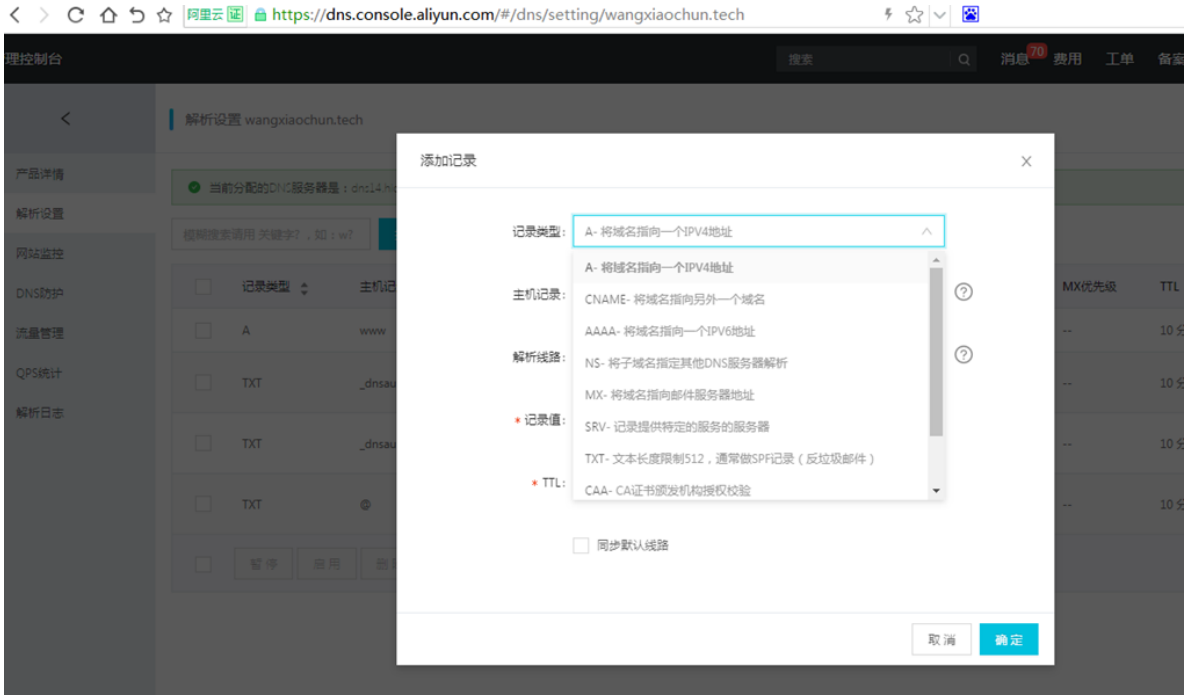
2.8 互联网域名

1. **域名注册**

   代理商：万网, 新网, godaddy

2. **注册完成以后，想自己用专用服务来解析**

管理后台：把NS记录指向的服务器名称，和A记录指向的服务器地址



3 DNS软件bind

DNS服务器软件：bind，powerdns，unbound

3.1 BIND相关程序包：

yum list all bind*

- bind：服务器
- bind-libs：相关库
- bind-utils: 客户端
- bind-chroot: 安全包，/var/named/chroot/

3.2 BIND包相关文件

- BIND程序名：/usr/sbin/named
- 服务脚本和名称：/etc/rc.d/init.d/named /usr/lib/systemd/system/named.service
- 主配置文件：/etc/named.conf, /etc/named.rfc1912.zones, /etc/rndc.key
- 管理工具：/usr/sbin/rndc：remote name domain controller， 默认与bind安装在同一主机，且只能通过127.0.0.1连接named进程 提供辅助性的管理功能；953/tcp
- 解析库文件：/var/named/ZONE_NAME.ZONE

  注意：(1) 一台物理服务器可同时为多个区域提供解析 (2) 必须要有根区域文件；named.ca (3) 应该有两个（如果包括ipv6的，应该更多）实现localhost和本地回环地址的解析库

3.3 主配置文件

- 全局配置：options {};
- 日志子系统配置：logging {};
- 区域定义：本机能够为哪些zone进行解析，就要定义哪些zone zone "ZONE_NAME" IN {};

注意：

- 任何服务程序如果期望其能够通过网络被其它主机访问，至少应该监听在一个能与外部主机通信的IP地址上
- 缓存名称服务器的配置：监听外部地址即可
- dnssec: 建议关闭dnssec，设为no

4 实现主DNS服务器

4.1 主DNS服务器配置：

1. 在主配置文件中定义区域

```
zone "ZONE_NAME" IN {
    type {master|slave|hint|forward};
file "ZONE_NAME.zone";
};
```

2. 定义区域解析库文件 出现的内容 宏定义 资源记录

   范例

```
$TTL 86400
$ORIGIN magedu.org.
@   IN  SOA ns1.magedu.org. admin.magedu.org (
        2015042201
        1H
        5M
        7D
        1D )
    IN  NS  ns1
    IN  NS  ns2
    IN  MX 10   mx1
    IN  MX 20   mx2
    ns1 IN  A   172.16.100.11
    ns2 IN  A   172.16.100.12
    mx1 IN  A   172.16.100.13
    mx2 IN  A   172.16.100.14
    websrv  IN  A   172.16.100.11
    websrv  IN  A   172.16.100.12
    www IN  CNAME   websrv
```

4.2 主配置文件语法检查：

named-checkconf

4.3 解析库文件语法检查：

named-checkzone "magedu.org" /var/named/magedu.org.zone

4.4 配置生效：

rndc reload 或 service named reload

4.5 测试命令

dig命令：

dig只用于测试dns系统，不会查询hosts文件进行解析

命令格式：

```
dig [-t type] name [@SERVER] [query options]
query options:
    +[no]trace：跟踪解析过程 ： dig +trace magedu.org
    +[no]recurse：进行递归解析
```

范例：

```
#测试反向解析：
dig -x IP = dig –t ptr reverseip.in-addr.arpa
#模拟区域传送：
dig -t axfr ZONE_NAME  @SERVER
dig -t axfr magedu.org  @10.10.10.11
dig –t axfr 100.1.10.in-addr.arpa  @172.16.1.1
dig -t NS . @114.114.114.114
dig -t NS  .  @a.root-servers.net
```

host命令

命令格式：

```
host [-t type] name [SERVER]
```

范例

```
host -t NS magedu.org  172.16.0.1
host -t soa magedu.org
host -t mx magedu.org
host -t axfr magedu.org
host  1.2.3.4
```

nslookup命令：

全令格式：

```
nslookup [-option] [name | -] [server]
```

交互式模式： nslookup> server IP: 指明使用哪个DNS server进行查询 set q=RR_TYPE: 指明查询的资源记录类型 NAME: 要查询的名称

4.6 实战案例：实现DNS正向主服务器

4.6.1 实验目的

搭建DNS正向主服务器，实现web服务器基于FQDN的访问

4.6.2 环境要求

需要三台主机
DNS服务端：192.168.8.8
web服务器：192.168.8.7
DNS客户端：192.168.8.6

4.6.3 前提准备

关闭SElinux
关闭防火墙
时间同步

4.6.4 实现步骤

4.6.4.1 在DNS服务端安装bind

```
yum install bind -y
```

4.6.4.2 修改bind 配置文件

```
vim /etc/named.conf
#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

vim /etc/named.rfc1912.zones
#加上这段
zone "magedu.org" {
    type master;
    file  "magedu.org.zone";
};
```

4.6.4.3 DNS区域数据库文件

```
cp -p /var/named/named.localhost /var/named/magedu.org.zone
#如果没有加-p选项，需要修改所有者或权限。chgrp named magedu.org.zone

vim /var/named/magedu.org.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    2019042210  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master      A    192.168.8.8
www         A    192.168.8.7
```

4.6.4.4 检查配置文件和数据库文件格式，并启动服务

```
named-checkconf
named-checkzone  magedu.org /var/named/magedu.org.zone

systemctl start named           #第一次启动服务
rndc reload                     #不是第一次启动服务
```

4.6.4.5 实现WEB服务

```
#安装http服务
yum install httpd
#配置主页面
echo www.magedu.org  > /var/www/html/index.html
#启动服务
systemctl start httpd
```

4.6.4.6 在客户端实现测试

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
    DNS1=192.168.8.8
service network restart
#有以下记录，算是成功
cat /etc/resolv.conf
    # Generated by NetworkManager
    nameserver 192.168.23.129

#测试网页,能显示就是成功
curl www.magedu.org
www.magedu.org
```

4.7 允许动态更新

动态更新：可以通过远程更新区域数据库的资源记录

实现动态更新，需要在指定的zone语句块中：

```
Allow-update {any;};
```

范例：

```
chmod 770 /var/named
setsebool  -P named_write_master_zones on
nsupdate
>server 127.0.0.1
>zone magedu.org
>update add ftp.magedu.org 88888 IN A 8.8.8.8
>send
>update delete www.magedu.org A
>send
#测试
dig ftp.magedu.org @127.0.0.1
ls -l /var/named/magedu.org.zone.jnl
cat /var/named/magedu.org.zone
```

5 实现反向解析区域

反向区域： 区域名称：网络地址反写.in-addr.arpa. 172.16.100. --> 100.16.172.in-addr.arpa. (1) 定义区域 zone "ZONE_NAME" IN { type {master|slave|forward}； file "网络地址.zone" }; (2) 定义区域解析库文件 注意：不需要MX,以PTR记录为主

范例：

```
$TTL 86400
$ORIGIN 100.16.172.in-addr.arpa.
@   IN  SOA ns1.magedu.org. admin.magedu.org. (
            2015042201
            1H
            5M
            7D
            1D )
    IN  NS  ns1.magedu.org.
    IN  NS  ns2.magedu.org.
11  IN  PTR ns1.magedu.org.
11  IN  PTR www.magedu.org.
12  IN  PTR mx1.magedu.org.
12  IN  PTR www.magedu.org.
13  IN  PTR mx2.magedu.org.
```

6 实现从服务器

6.1 DNS从服务器

1. 应该为一台独立的名称服务器
2. 主服务器的区域解析库文件中必须有一条NS记录指向从服务器
3. 从服务器只需要定义区域，而无须提供解析库文件；解析库文件应该放置于/var/named/slaves/目录中
4. 主服务器得允许从服务器作区域传送
5. 主从服务器时间应该同步，可通过ntp进行
6. bind程序的版本应该保持一致；否则，应该从高，主低

6.2 定义从区域

格式:

```
    zone "ZONE_NAME" IN {
        type slave;
        masters { MASTER_IP; };
        file "slaves/ZONE_NAME.zone";
    };
```

6.3 rndc 工具

利用rndc工具可以实现管理DNS功能

rndc 监听端口: 953/tcp

命令格式:

```
rndc COMMAND
COMMAND:
    reload: 重载主配置文件和区域解析库文件
    reload zonename: 重载区域解析库文件
    retransfer zonename: 手动启动区域传送，而不管序列号是否增加
    notify zonename: 重新对区域传送发通知
    reconfig: 重载主配置文件
    querylog: 开启或关闭查询日志文件/var/log/message
    trace: 递增debug一个级别
    trace LEVEL: 指定使用的级别
    notrace：将调试级别设置为 0
    flush：清空DNS服务器的所有缓存记录
```

6.4 实战案例：实现DNS从服务器

6.4.1 实验目的

```
搭建DNS主从服务器架构，实现DNS服务冗余
```

6.4.2 环境要求

```
需要四台主机
DNS主服务器：192.168.8.8
DNS从服务器:192.168.8.18
web服务器：192.168.8.7
DNS客户端：192.168.8.6
```

6.4.3 前提准备

```
关闭SElinux
关闭防火墙
时间同步
```

6.4.4 实现步骤

6.4.4.1 主DNS服务端配置(参看前面案例)

```
yum install bind -y

vim /etc/named.conf
#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

#只允许从服务器进行区域传输
allow-transfer { 从服务器IP;};

vim /etc/named.rfc1912.zones
#加上这段
zone "magedu.org" {
    type master;
    file  "magedu.org.zone";
};
```

```
cp -p /var/named/named.localhost /var/named/magedu.org.zone
#如果没有-p，需要改权限。chgrp named magedu.org.zone

vim /var/named/magedu.org.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    1   ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
            NS   slave
master      A    192.168.8.8
slave       A    192.168.8.18


systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

6.4.4.2 从DNS服务器配置

```
yum install bind -y

vim /etc/named.conf
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };
#不允许其它主机进行区域传输
allow-transfer { none;};

vim /etc/named.rfc1912.zones
zone "magedu.org" {
    type slave;
    masters { 主服务器IP;};

    file "slaves/magedu.org.slave";
};

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
ls  /var/named/slaves/magedu.org.slave #查看区域数据库文件是否生成
```

6.4.4.3 客户端测试主从DNS服务架构

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
DNS1=主服务器
DNS2=从服务器

#验证从DNS服务器是否可以查询
dig www.magedu.org
curl www.magedu.org

#在主服务器上停止DNS服务
systemctl stop named

#验证从DNS服务器仍然可以查询
```

```
dig www.magedu.org
curl www.magedu.org
```

---

7 实现子域

7.1 子域授权

将子域委派给其它主机管理，实现分布式DNS数据库

正向解析区域子域方法

范例：定义两个子域区域

```
shanghai.magedu.org.        IN  NS  ns1.ops.magedu.org.
shanghai.magedu.org.        IN  NS  ns2.ops.magedu.org.
shenzhen.magedu.org.        IN  NS  ns1.shenzhen.magedu.org.
shenzhen.magedu.org.        IN  NS  ns2.shenzhen.magedu.org.
ns1.shanghai.magedu.org.    IN  A  1.1.1.1
ns2.shanghai.magedu.org.    IN  A  1.1.1.2
ns1.shenzhen.magedu.org.    IN  A  1.1.1.3
ns2.shenzhen.magedu.org.    IN  A  1.1.1.4
```

7.2 范例：实现DNS父域和子域服务

7.2.1 实验目的

```
搭建DNS父域子域服务器。
```

7.2.2 环境要求

```
需要五台主机
DNS父服务器：192.168.8.8
DNS子域服务器:192.168.8.18
父域的web服务器：192.168.8.7
子域的web服务器：192.168.8.17
DNS客户端：192.168.8.6
```

7.2.3 前提准备

```
关闭SElinux
关闭防火墙
时间同步
```

7.2.3 实现步骤

7.2.3.1 在父域DNS服务器上实现主magedu.org域的主DNS服务

```
yum install bind -y

vim /etc/named.conf
```

```
#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

#只允许从服务器进行区域传输
allow-transfer { 从服务器IP;};

vim /etc/named.rfc1912.zones
#加上这段
zone "magedu.org" {
    type master;
    file  "magedu.org.zone";
};

cp -p /var/named/named.localhost /var/named/magedu.org.zone
#如果没有-p，需要改权限。chgrp named magedu.org.zone

vim /var/named/magedu.org.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    1   ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
shanghai    NS   shanghains
master      A    192.168.8.8
shanghains  A    192.168.8.18
websrv      A    192.168.8.7
www         CNAME  websrv


systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

7.2.3.2 实现子域的DNS服务器

```
yum install bind -y

vim /etc/named.conf
#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };
allow-transfer { none;};

vim /etc/named.rfc1912.zones

zone "chengdu.magedu.org" {
    type master;
    file "shanghai.magedu.org.zone";
};

cp -p /var/named/named.localhost /var/named/shanghai.magedu.org.zone
#如果没有-p，需要改权限。chgrp named magedu.org.zone

vim /var/named/shanghai.magedu.org.zone
```

```
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    2019042214  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master     A    192.168.8.18
websrv     A    192.168.8.7
www       CNAME  websrv

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

7.2.3.4 在父域和子域的web服务器上安装httpd服务

```
#父域的web服务器利用上面案例（略）
#在子域的web服务器上安装http服务
yum install httpd
#配置主页面
echo www.shanghai.magedu.org  > /var/www/html/index.html
#启动服务
systemctl start httpd
```

7.2.3.4 客户端测试

```
dig www.shanghai.magedu.org
www.shanghai.magedu.org
```

8 实现DNS转发（缓存）服务器

8.1 DNS转发

利用DNS转发，可以将用户的DNS请求，转发至指定的DNS服务，而非默认的根DNS服务器，并将指定服务器查询的返回结果进行缓存，提高效率。

注意：

1. 被转发的服务器需要能够为请求者做递归，否则转发请求不予进行
2. 在全局配置块中，关闭dnssec功能

```
dnssec-enable no;
dnssec-validation no;
```

8.2 转发方式

8.2.1 全局转发:

对非本机所负责解析区域的请求，全转发给指定的服务器 在全局配置块中实现：

```
Options {
        forward  first|only;
        forwarders { ip;};
};
```

8.2.2 特定区域转发

仅转发对特定的区域的请求，比全局转发优先级高

```
zone "ZONE_NAME" IN {
    type forward;
    forward  first|only;
    forwarders { ip;};
};
```

first：先转发至指定DNS服务器，如果无法解析查询请求，则本服务器再去根服务器查询

only: 先转发至指定DNS服务器，如果无法解析查询请求，则本服务器将不再去根服务器查询

8.3 实战案例：实现DNS forward（缓存）服务器

8.3.1 实验目的

```
搭建DNS转发（缓存）服务器
```

8.3.2 环境要求

```
需要四台主机
DNS只缓存服务器：192.168.8.8
DNS主服务器:192.168.8.18
web服务器：192.168.8.7
DNS客户端：192.168.8.6
```

8.3.3 前提准备

```
关闭SElinux
关闭防火墙
时间同步
```

8.3.4 实现步骤

8.3.4.1 实现转发（只缓存）DNS服务器

```
yum install bind -y

vim /etc/named.conf
#注释掉两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

forward first;
forwarders { 192.168.8.18;};
```

```
#关闭dnsec功能
dnssec-enable no;
dnssec-validation no;

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

8.3.4.2 实现主DNS服务器

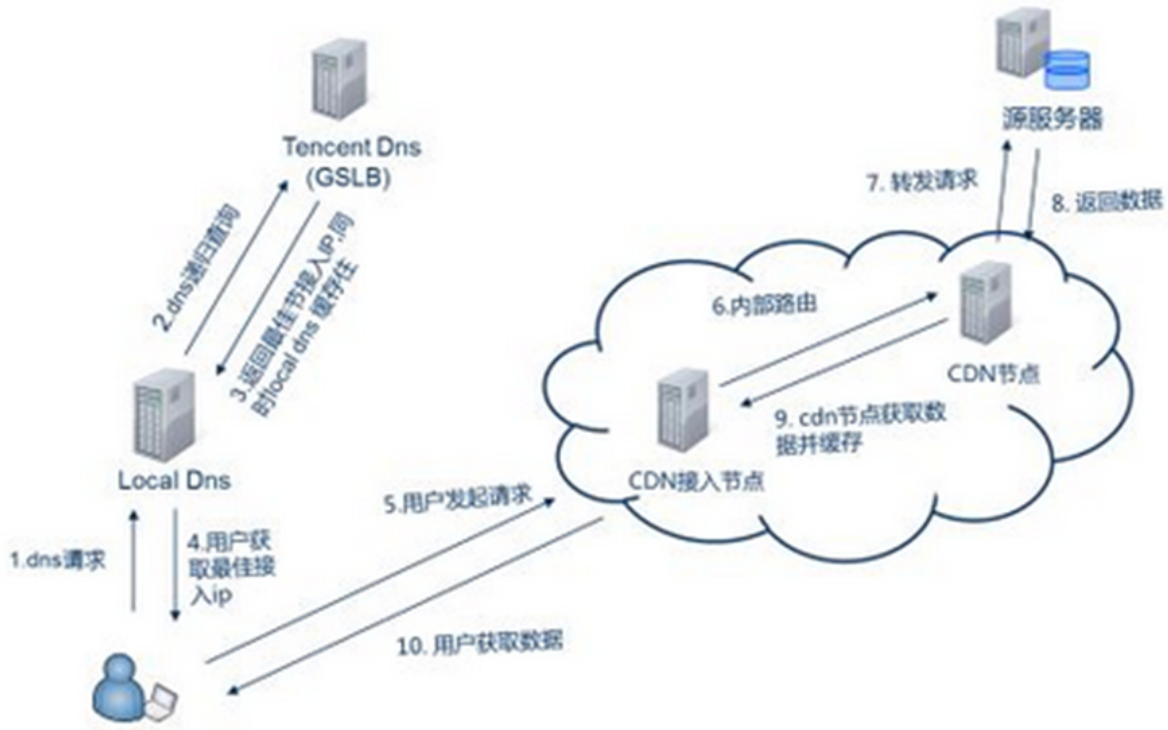
```
yum install bind -y

vim /etc/named.conf
#注释掉两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

vim /etc/named.rfc1912.zones
#加上下面这段
zone "magedu.org" {
    type master;
    file  "magedu.org.zone";
};

cp -p /var/named/named.localhost /var/named/magedu.org.zone
#如果没有-p，需要改权限。chgrp named magedu.org.zone

vim /var/named/magedu.org.zone

$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    2019042214  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master      A    192.168.8.18
websrv      A    192.168.8.7
www       CNAME  websrv


systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

8.3.4.3 web服务器配置（参看前面案例，略）

8.3.4.4 在客户端测试

```
#客户端配置（参看前面案例，略）
dig www.magedu.org
curl www.magedu.org
```

9 实现智能DNS



9.1 GSLB

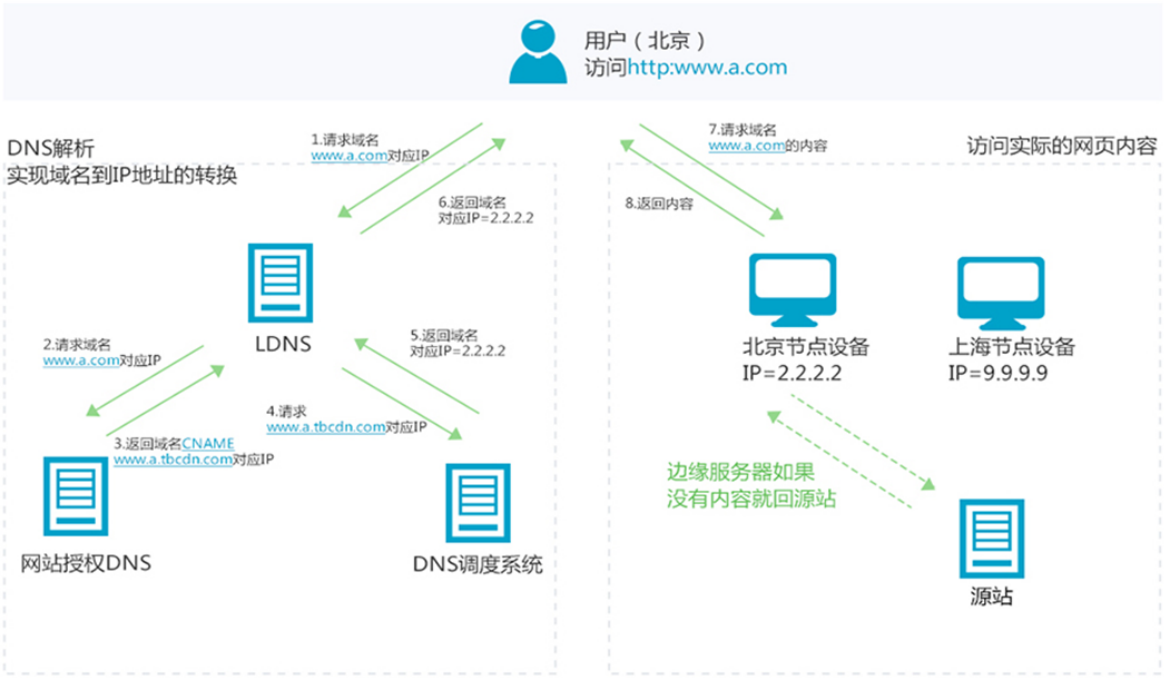
GSLB：Global Server Load Balance全局负载均衡

GSLB是对服务器和链路进行综合判断来决定由哪个地点的服务器来提供服务，实现异地服务器群服务质量的保证

GSLB主要的目的是在整个网络范围内将用户的请求定向到最近的节点（或者区域）

GSLB分为基于DNS实现、基于重定向实现、基于路由协议实现，其中最通用的是基于DNS解析方式

9.2 CDN （Content Delivery Network）内容分发网络



9.2.1 CDN工作原理

1. 用户向浏览器输入www.a.com这个域名，浏览器第一次发现本地没有dns缓存，则向网站的DNS服务器请求
2. 网站的DNS域名解析器设置了CNAME，指向了www.a.tbcdn.com,请求指向了CDN网络中的智能DNS负载均衡系统
3. 智能DNS负载均衡系统解析域名，把对用户响应速度最快的IP节点返回给用户；
4. 用户向该IP节点（CDN服务器）发出请求
5. 由于是第一次访问，CDN服务器会通过Cache内部专用DNS解析得到此域名的原web站点IP，向原站点服务器发起请求，并在CDN服务器上缓存内容
6. 请求结果发给用户

9.2.2 CDN服务商

- 服务商：蓝汛，网宿，帝联等
- 智能DNS: dnspod dns.la

9.3 智能DNS相关技术

9.3.1 bind中ACL

acl: 把一个或多个地址归并为一个集合，并通过一个统一的名称调用

注意：只能先定义后使用；因此一般定义在配置文件中，处于options的前面

格式：

```
acl acl_name {
    ip;
    net/prelen;
    ……
};
```

范例：

```
acl mynet {
    172.16.0.0/16;
    10.10.10.10;
};
```

9.3.2 bind有四个内置的acl

- none 没有一个主机
- any 任意主机
- localhost 本机
- localnet 本机的IP同掩码运算后得到的网络地址

9.3.3 访问控制的指令：

- allow-query {}： 允许查询的主机；白名单
- allow-transfer {}：允许区域传送的主机；白名单
- allow-recursion {}: 允许递归的主机,建议全局使用
- allow-update {}: 允许更新区域数据库中的内容

9.3.4 view 视图

9.3.4.1 View：视图，将ACL和区域数据库实现对应关系，以实现智能DNS

- 一个bind服务器可定义多个view，每个view中可定义一个或多个zone

- 每个view用来匹配一组客户端
- 多个view内可能需要对同一个区域进行解析，但使用不同的区域解析库文件

注意：

- 一旦启用了view，所有的zone都只能定义在view中
- 仅在允许递归请求的客户端所在view中定义根区域
- 客户端请求到达时，是自上而下检查每个view所服务的客户端列表

9.3.4.2 view 格式

```
view VIEW_NAME {
        match-clients { testacl;  };
        zone “magedu.org” {
            type master;
            file “magedu.org.zone”;
        };
        include “/etc/named.rfc1912.zones”;
};
```

9.4 实战案例：利用view实现智能DNS

9.4.1 实验目的

```
搭建DNS主从服务器架构，实现DNS服务冗余
```

9.4.2 环境要求

```
需要五台主机
DNS主服务器和web服务器1：192.168.8.8/24，172.16.0.8/16
web服务器2：192.168.8.7/24
web服务器3：172.16.0.7/16
DNS客户端1：192.168.8.6/24
DNS客户端2：172.16.0.6/16
```

9.4.3 前提准备

```
关闭SElinux
关闭防火墙
时间同步
```

9.4.4 实现步骤

9.4.4.1 DNS 服务器的网卡配置

```
#配置两个IP地址
#eth0：192.168.8.8/24
#eth1:172.16.0.8/16
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
```

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:0c:29:f9:8d:90 brd ff:ff:ff:ff:ff:ff
    inet 192.168.8.8/24 brd 192.168.8.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fef9:8d90/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group
default qlen 1000
    link/ether 00:0c:29:f9:8d:11 brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.8/16 brd 172.16.0.255 scope global noprefixroute eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe11:8d90/64 scope link
       valid_lft forever preferred_lft forever
```

9.4.4.2 主DNS服务端配置文件实现view

```
yum install bind -y

vim /etc/named.conf
#在文件最前面加下面行
acl beijingnet {
    192.168.8.0/24;
};
acl shanghainet {
    172.16.0.0/16;
};
acl othernet {
    any;
};

#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

#其它略

# 创建view
view  beijingview {
    match-clients  { beijingnet;};
    include "/etc/named.rfc1912.zones.bj";
};
view  shanghaiview {
    match-clients  { shanghainet;};
    include "/etc/named.rfc1912.zones.sh";
};
view  otherview {
    match-clients  { othernet;};
    include "/etc/named.rfc1912.zones.other";
};
include "/etc/named.root.key";
```

9.4.4.3 实现区域配置文件

```
vim /etc/named.rfc1912.zones.bj
zone "." IN {
    type hint;
    file "named.ca";
};
zone "magedu.org" {
    type master;
    file "magedu.org.zone.bj";
};

vim /etc/named.rfc1912.zones.sh
zone "." IN {
    type hint;
    file "named.ca";
};
zone "magedu.org" {
    type master;
    file "magedu.org.zone.sh";
};

vim /etc/named.rfc1912.zones.bj
zone "." IN {
    type hint;
    file "named.ca";
};
zone "magedu.org" {
    type master;
    file "magedu.org.zone.other";
};

chgrp named /etc/named.rfc1912.zones.bj
chgrp named /etc/named.rfc1912.zones.sh
chgrp named /etc/named.rfc1912.zones.other
```

9.4.4.4 创建区域数据库文件

```
vim /var/named/magedu.org.zone.bj
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    2019042214  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master      A    192.168.8.8
websrv      A    192.168.8.7
www        CNAME  websrv

vim /var/named/magedu.org.zone.sh
$TTL 1D
@   IN SOA  master admin.magedu.org. (
```

```
                    2019042214  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master      A    192.168.8.8
websrv      A    172.16.0.7
www        CNAME  websrv

vim /var/named/magedu.org.zone.other
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    2019042214  ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
master      A    192.168.8.8
websrv      A    127.0.0.1
www        CNAME  websrv

chgrp named /var/named/magedu.org.zone.bj
chgrp named /var/named/magedu.org.zone.sh
chgrp named /var/named/magedu.org.zone.other


systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

9.4.4.5 实现位于不同区域的三个WEB服务器

```
#分别在三台主机上安装http服务
#在web服务器1：192.168.8.8/24实现
yum install httpd
echo www.magedu.org in Other  > /var/www/html/index.html
systemctl start httpd
#在web服务器2：192.168.8.7/16
echo www.magedu.org in Beijing  > /var/www/html/index.html
systemctl start httpd
#在web服务器3：172.16.0.7/16
yum install httpd
echo www.magedu.org in Shanghai  > /var/www/html/index.html
systemctl start httpd
```

9.4.4.6 客户端测试

```
#分别在三台主机上访问
#DNS客户端1：192.168.8.6/24 实现，确保DNS指向192.168.8.8
curl www.magedu.org
www.magedu.org in Beijing
#DNS客户端2：172.16.0.6/16  实现，确保DNS指向172.16.0.8
curl www.magedu.org
www.magedu.org in Shanghai
#DNS客户端3：192.168.8.8  实现，，确保DNS指向127.0.0.1
curl www.magedu.org
www.magedu.org in Other
```

10 DNS排错

范例：

```
dig A example.com

; <<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> A example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30523
...
```

SERVFAIL:The nameserver encountered a problem while processing the query. 可使用dig +trace排错，可能是网络和防火墙导致 NXDOMAIN：The queried name does not exist in the zone. 可能是CNAME对应的A记录不存在导致 REFUSED：The nameserver refused the client's DNS request due to policy restrictions. 可能是DNS策略导致

范例：

```
dig A example.com
; <<>> DiG 9.9.4-RedHat-9.9.4-14.el7 <<>> A example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30523
...
SERVFAIL:The nameserver encountered a problem while processing the query.
```

可使用dig +trace排错，可能是网络和防火墙导致 NXDOMAIN：The queried name does not exist in the zone. 可能是CNAME对应的A记录不存在导致 REFUSED：The nameserver refused the client's DNS request due to policy restrictions. 可能是DNS策略导致

11 实战案例：综合案例，实现Intenet 的DNS 服务架构

11.1 实验目的

```
搭建DNS实现internet dns架构。
```

11.2 环境要求

```
需要8台主机
DNS客户端：192.168.8.6/24
本地DNS服务器（只缓存）：192.168.8.8/24
转发目标DNS服务器：192.168.8.18/24
根DNS服务器：192.168.8.28/24
org域DNS服务器：192.168.8.38/24
magedu.org域主DNS服务器：192.168.8.48/24
magedu.org域从DNS服务器：192.168.8.58/24
www.magedu.org的WEB服务器：192.168.8.68/24
```

11.3 前提准备

```
关闭SElinux
关闭防火墙
时间同步
```

11.4 实现步骤

11.4.1 各种主机的网络配置（参看上面的环境要求）

```
#在客户端配置DNS服务器地址
vim /etc/sysconfig/network-scripts/ifcfg-ens33
NAME=eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=192.168.8.6
NETMASK=255.255.255.0
DNS1=192.168.8.8
ONBOOT=yes

service network restart
```

11.4.2 实现WEB服务

```
#在web服务器192.168.8.68/24上实现
yum install httpd
echo www.magedu.org  > /var/www/html/index.html
systemctl start httpd
```

11.4.3 实现magedu.org域的主DNS服务器

```
#在magedu.org域主DNS服务器192.168.8.48/24上实现
yum install bind -y

vim /etc/named.conf
#注释掉下面两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

#只允许从服务器进行区域传输
allow-transfer { 从服务器IP;};

vim /etc/named.rfc1912.zones
#加上这段
zone "magedu.org" {
```

```
    type master;
    file  "magedu.org.zone";
};

vim /var/named/magedu.org.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. (
                    1   ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
            NS   master
            NS   slave
master      A    192.168.8.48
slave       A    192.168.8.58

chgrp named  /var/named/magedu.org.zone

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

11.4.4 实现magedu.org域的从DNS服务器配置

```
#在magedu.org域从DNS服务器192.168.8.58/24上实现
yum install bind -y

vim /etc/named.conf
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };
#不允许其它主机进行区域传输
allow-transfer { none;};

vim /etc/named.rfc1912.zones
zone "magedu.org" {
    type slave;
    masters { 主服务器IP;};

    file "slaves/magedu.org.slave";
};

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
ls  /var/named/slaves/magedu.org.slave #查看区域数据库文件是否生成
```

11.4.5 实现org域的主DNS服务器

```
#在org域的主DNS服务器192.168.8.38/24上实现
yum install bind -y

vim /etc/named.conf
#注释掉两行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };
```

```
vim /etc/named.rfc1912.zones
#加上这段
zone "org" {
    type master;
    file  "org.zone";
};

vim /var/named/org.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. ( 1 1D 1H 1W 3D )
            NS   master
magedu      NS mageduns1
magedu      NS mageduns2
master      A 192.168.8.38
mageduns1 A 192.168.8.48
mageduns2 A 192.168.8.58

chgrp named  /var/named/org.zone

systemctl start named          #第一次启动服务
rndc reload                    #不是第一次启动服务
```

11.4.6 实现根域的主DNS服务器

```
#在根域的主DNS服务器192.168.8.28/24上实现
yum install bind -y
vim /etc/named.conf
#注释掉两行，第13行和第21行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };
#将下面行改为：
zone "." IN {
        type master;
        file "root.zone";
};

vim /var/named/root.zone
$TTL 1D
@   IN SOA  master admin.magedu.org. ( 1 1D 1H 1W 3D )
            NS   master
com         NS   comns
master      A 192.168.8.28
comns       A 192.168.8.38

#安全加固
chgrp named /var/named/root.zone
chmod 640 /var/named/root.zone

systemctl start named   #第一次启动
rndc reload             #不是第一次启动
```

11.4.6 实现转发目标的DNS服务器

```
#在转发目标的DNS服务器192.168.8.18/24上实现
yum install bind -y
```

```
vim /etc/named.conf
#注释掉两行，第13行和第21行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };


vim /var/named/named.ca
.                       518400  IN      NS      a.root-servers.net.
a.root-servers.net.     3600000 IN      A       192.168.8.28

systemctl start named   #第一次启动
rndc reload             #不是第一次启动
```

11.4.7 实现本地只缓存DNS服务器

```
#在转发目标的DNS服务器192.168.8.8/24上实现
yum install bind -y

vim /etc/named.conf
#注释掉两行，第13行和第21行
//  listen-on port 53 { 127.0.0.1; };
//  allow-query     { localhost; };

forward only;
forwarders { 192.168.8.18;};

dnssec-enable no;
dnssec-validation no


systemctl start named   #第一次启动
rndc reload             #不是第一次启动
```

11.4.8 客户端测试

```
cat /etc/resolv.conf
nameserver 192.168.8.8

dig www.magedu.org

; <<>> DiG 9.9.4-RedHat-9.9.4-61.el7 <<>> www.magedu.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40755
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.magedu.org.                IN  A

;; ANSWER SECTION:
www.magedu.org.     86181   IN  A   192.168.8.68
```

```
;; AUTHORITY SECTION:
magedu.org.     86181   IN  NS  ns2.magedu.org.
magedu.org.     86181   IN  NS  ns1.magedu.org.

;; ADDITIONAL SECTION:
ns2.magedu.org.     86181   IN  A   192.168.8.48
ns1.magedu.org.     86181   IN  A   192.168.8.58

;; Query time: 1 msec
;; SERVER: 192.168.8.8#53(192.168.8.8)
;; WHEN: Fri May 10 17:28:39 CST 2019
;; MSG SIZE  rcvd: 127        成功

curl www.magedu.org
www.magedu.org
```