马哥教育
IT人的高薪职业学院

DNS服务和BIND

讲师：王晓春

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

DNS服务

- DNS：Domain Name System 应用层协议
  C/S,53/udp, 53/tcp
- BIND：Bekerley Internat Name Domain
  ISC（www.isc.org）
- 本地名称解析配置文件：hosts
  /etc/hosts
  %WINDIR%/system32/drivers/etc/hosts
  122.10.117.2 www.magedu.com
  93.46.8.89 www.google.com

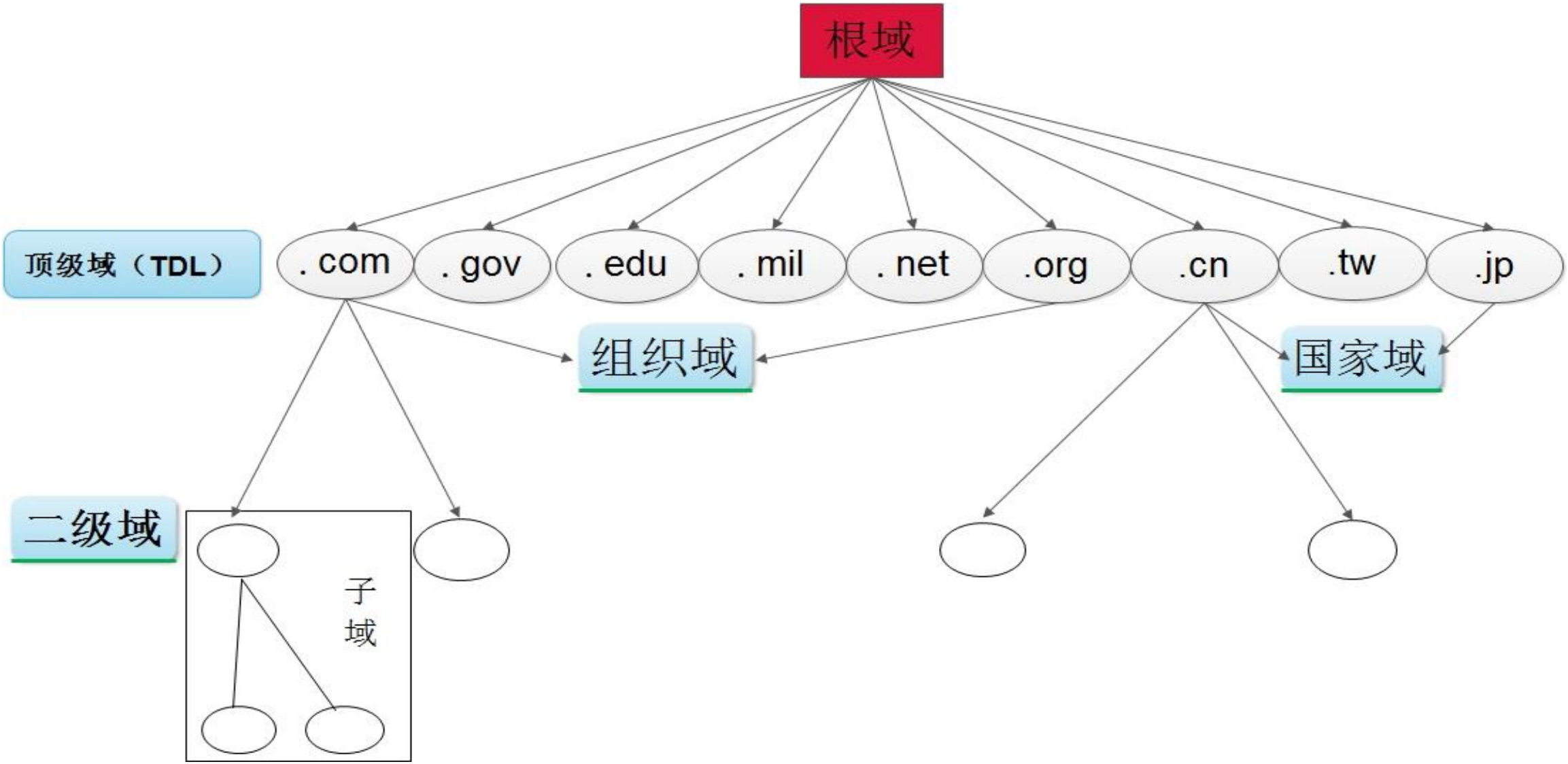
DNS域名

- 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
- 三级域名
- 最多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

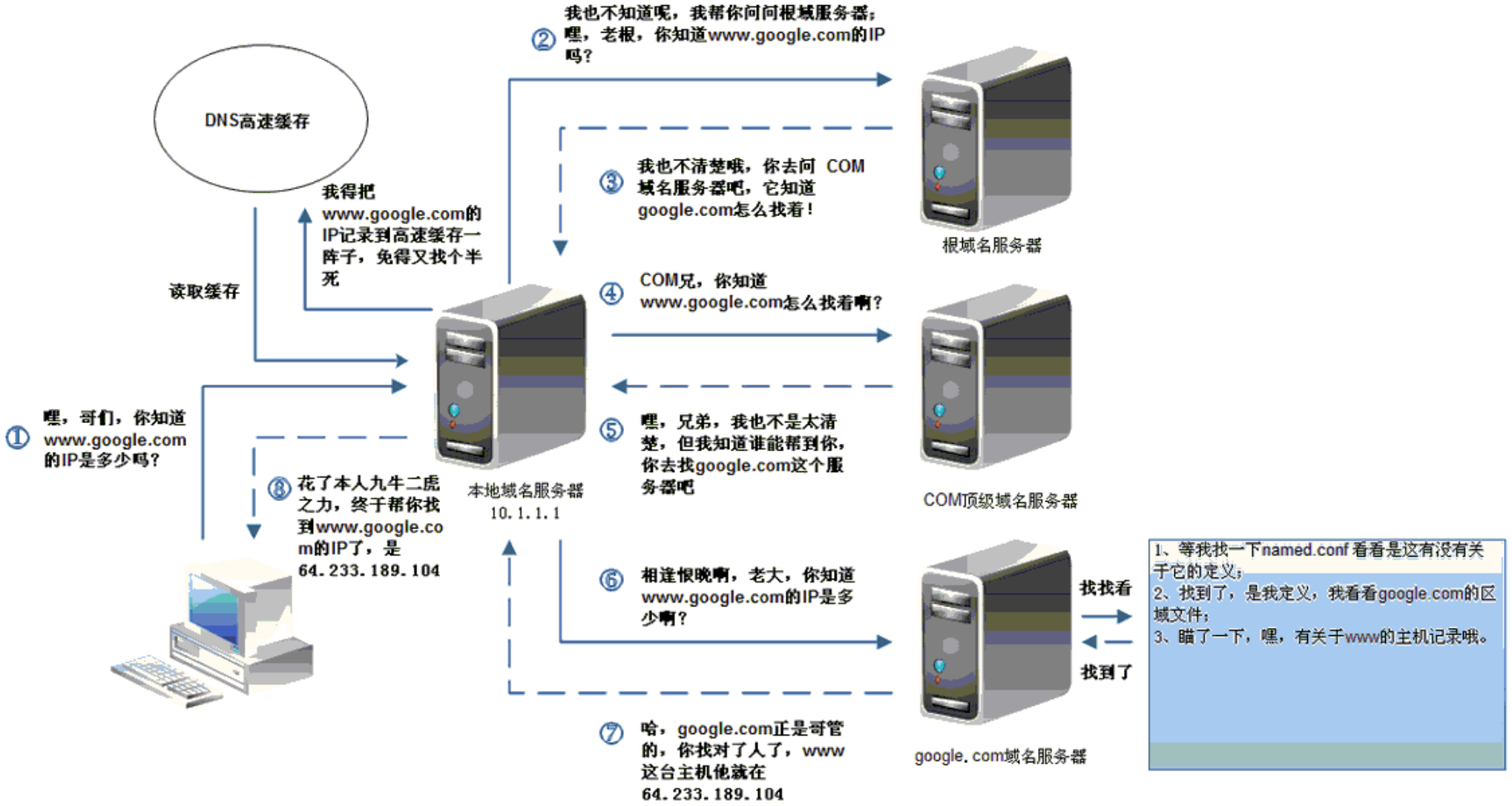
DNS域名结构



DNS解析

- DNS查询类型：
  - 递归查询
  - 迭代查询
- 名称服务器：域内负责解析本域内的名称的主机
  - 根服务器：13组服务器
- 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

DNS 域名解析过程



递归查询　　迭代查询

DNS服务器类型

- 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）
- 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
- 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

区域传输

- 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
- Domain: Fully Qualified Domain Name
  - 正向：FQDN --> IP
  - 反向: IP --> FQDN
- 负责本地域名的正向和反向解析库
  - 正向区域
  - 反向区域

DNS解析

- 一次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...

- 解析答案：

  肯定答案：

  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：

  非权威答案：

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
  示例：_dnsauth TXT 20120112000000051qgs69bwoh4h6nht4n1h0lr038x

资源记录

- 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) @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

SOA记录

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

```
magedu.com.          86400 IN      SOA    ns.magedu.com.
nsadmin.magedu.com.      (
            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
)
```

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.com.
- 注意：一个区域可以有多个NS记录

  例如：

  magedu.com.　　IN　　NS　　ns1.magedu.com.

  magedu.com.　　IN　　NS　　ns2.magedu.com.

- 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

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
- 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
- 例如：

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

- 注意：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

A记录

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

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

- 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

其它记录

- AAAA:

  name: FQDN

  value: IPv6

- PTR:

  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

- 例如：

  4.3.2.1.in-addr.arpa. IN PTR www.magedu.com.

  如1.2.3为网络地址，可简写成：

  4 IN PTR www.magedu.com.

- 注意：网络地址及后缀可省略；主机地址依然需要反着写

别名记录

- CNAME：
  - name: 别名的FQDN
  - value: 真正名字的FQDN
- 例如：

```
www.magedu.com.  IN  CNAME   websrv.magedu.com.
```

子域

- 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：

```
.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.com. 在.com的名称服务器上，解析库中添加资源记录

```
magedu.com.          IN      NS      ns1.magedu.com.
magedu.com.          IN      NS      ns2.magedu.com.
magedu.com.          IN      NS      ns3.magedu.com.
ns1.magedu.com.      IN      A       3.3.3.1
ns2.magedu.com.      IN      A       3.3.3.2
ns3.magedu.com.      IN      A       3.3.3.3
```

- glue record：粘合记录，父域授权子域的记录

互联网域名

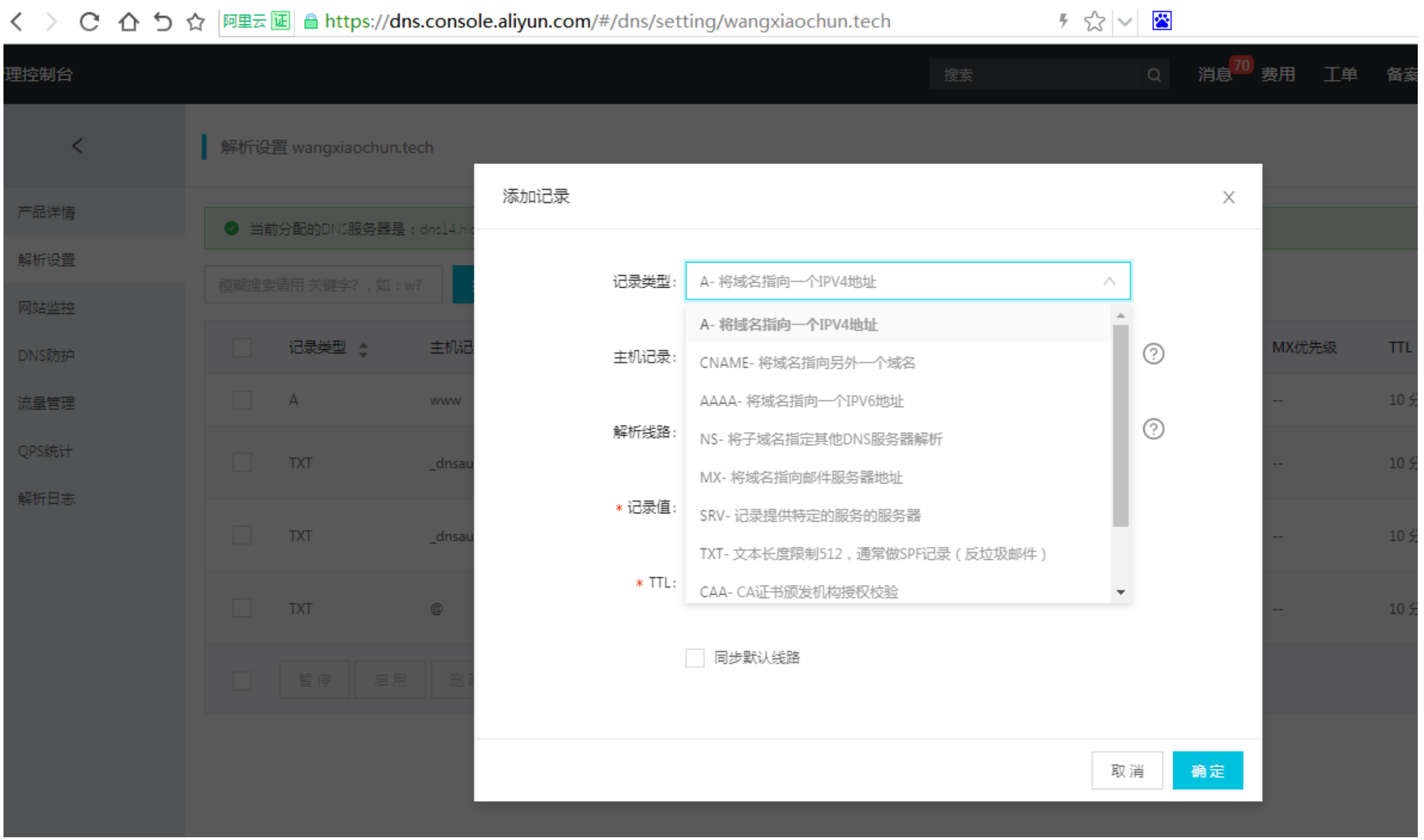
- 域名注册：

  代理商：万网, 新网, godaddy

- 注册完成以后，想自己用专用服务来解析

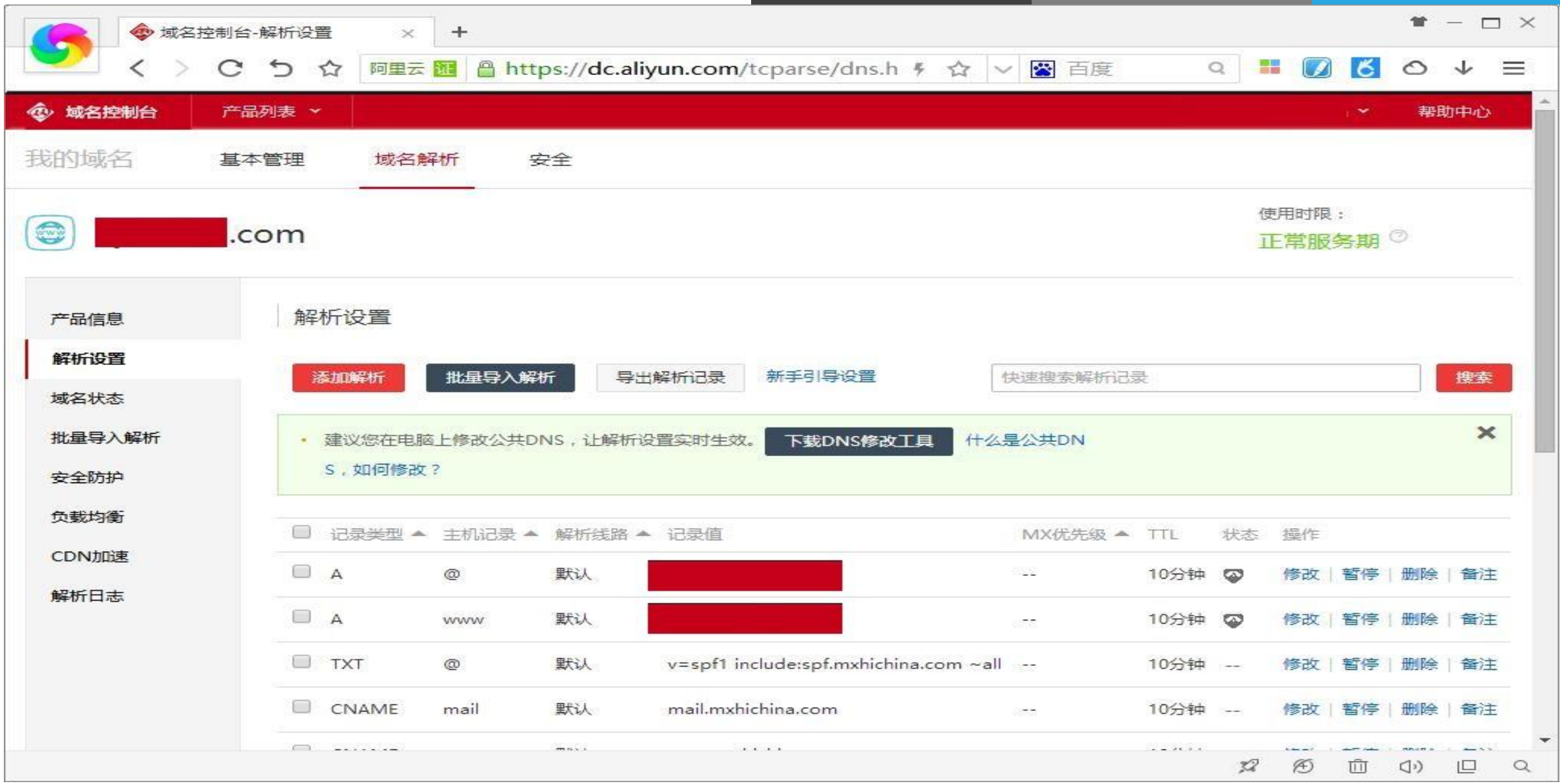
  管理后台：把NS记录指向的服务器名称，和A记录指向的服务器地址

阿里云DNS


https://dns.console.aliyun.com/#/dns/setting/wangxiaochun.tech
理控制台
搜索
消息 70
费用
工单
备案
解析设置 wangxiaochun.tech
产品详情
解析设置
网站监控
DNS防护
流量管理
QPS统计
解析日志
当前分配的DNS服务器是：dns14.hi
模糊搜索请用 关键字? ，如：w?
记录类型
主机记
MX优先级
TTL
A
www
TXT
_dnsau
TXT
_dnsau
TXT
@
暂停
启用
添加记录
记录类型：
A- 将域名指向一个IPV4地址
主机记录：
解析线路：
* 记录值：
* TTL：
A- 将域名指向一个IPV4地址
CNAME- 将域名指向另外一个域名
AAAA- 将域名指向一个IPV6地址
NS- 将子域名指定其他DNS服务器解析
MX- 将域名指向邮件服务器地址
SRV- 记录提供特定的服务的服务器
TXT- 文本长度限制512，通常做SPF记录（反垃圾邮件）
CAA- CA证书颁发机构授权校验
同步默认线路
取消
确定

阿里云DNS

马哥教育
IT人的高薪职业学院



阿里云DNS


https://dc.aliyun.com/tcparse/dns.htm?init=true&dtoken=YyUB7kmHuy
域名控制台
产品列表
帮助中心
我的域名
基本管理
域名解析
安全
[redacted]com
使用时限：
正常服务期
产品信息
解析设置
域名状态
批量导入解析
安全防护
负载均衡
CDN加速
解析日志
解析设置
添加解析
批量导入解析
导出解析记录
新手引导设置
快速搜索解析记录
搜索
建议您在电脑上修改公共DNS，让解析设置实时生效。
下载DNS修改工具
什么是公共DNS，如何修改？
记录类型
主机记录
解析线路
记录值
MX优先级
TTL
状态
操作
A
默认
--
10分钟
保存
取消
搭建网站：要将域名指向主机服务商提供的IP地址，请选择「A记录」；要将域名指向主机服务商提供的另一个域名，请选择「CNAME记录」。
建立邮箱：需要设置「MX记录」，根据邮箱服务商提供的MX记录填写。
A记录：将域名指向一个IPv4地址（例如：10.10.10.10），需要增加A记录
CNAME记录：如果将域名指向一个域名，实现与被指向域名相同的访问效果，需要增加CNAME记录
MX记录：建立电子邮箱服务，将指向邮件服务器地址，需要设置MX记录

BIND安装

- DNS服务器软件：bind，powerdns，unbound
- 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: /var/named/chroot/
- BIND程序名：named

bind服务器

- 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
- 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

- 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

配置文件

- 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

配置主DNS服务器

- 主DNS名称服务器：

  (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

- 主配置文件语法检查：

  named-checkconf

- 解析库文件语法检查：

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

- 配置生效：

  rndc reload 或 service named reload

主区域示例


```
$TTL 86400
$ORIGIN magedu.com.
        @       IN      SOA     ns1.magedu.com.  admin.magedu.com (
        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
```

测试命令dig

- dig [-t type] name [@SERVER] [query options]

  dig只用于测试dns系统，不会查询hosts文件进行解析

- 查询选项：

  +[no]trace：跟踪解析过程：dig +trace magedu.com

  +[no]recurse：进行递归解析

  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.com @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

测试命令

- host [-t type] name [SERVER]
  - host -t NS magedu.com 172.16.0.1
  - host -t soa magedu.com
  - host -t mx magedu.com
  - host -t axfr magedu.com
  - host 1.2.3.4
- nslookup命令： 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

反向区域

- 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

反向区域示例


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

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

定义从区域的方法：

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

rndc命令

- rndc：
  - rndc --> rndc (953/tcp)
  - 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

子域

- 子域授权：分布式数据库
- 正向解析区域子域方法
- 定义一个子区域：

```
ops.magedu.com.          IN    NS    ns1.ops.magedu.com.
ops.magedu.com.          IN    NS    ns2.ops.magedu.com.
ns1.ops.magedu.com.      IN    A     1.1.1.1
ns2.ops.magedu.com.      IN    A     1.1.1.2
fin.magedu.com.          IN    NS    ns1.fin.magedu.com.
fin.magedu.com.          IN    NS    ns2.fin.magedu.com.
ns1.fin.magedu.com.      IN    A     3.1.1.1
ns2.fin.magedu.com.      IN    A     3.1.1.2
```

转发服务器

- 注意：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
- (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

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

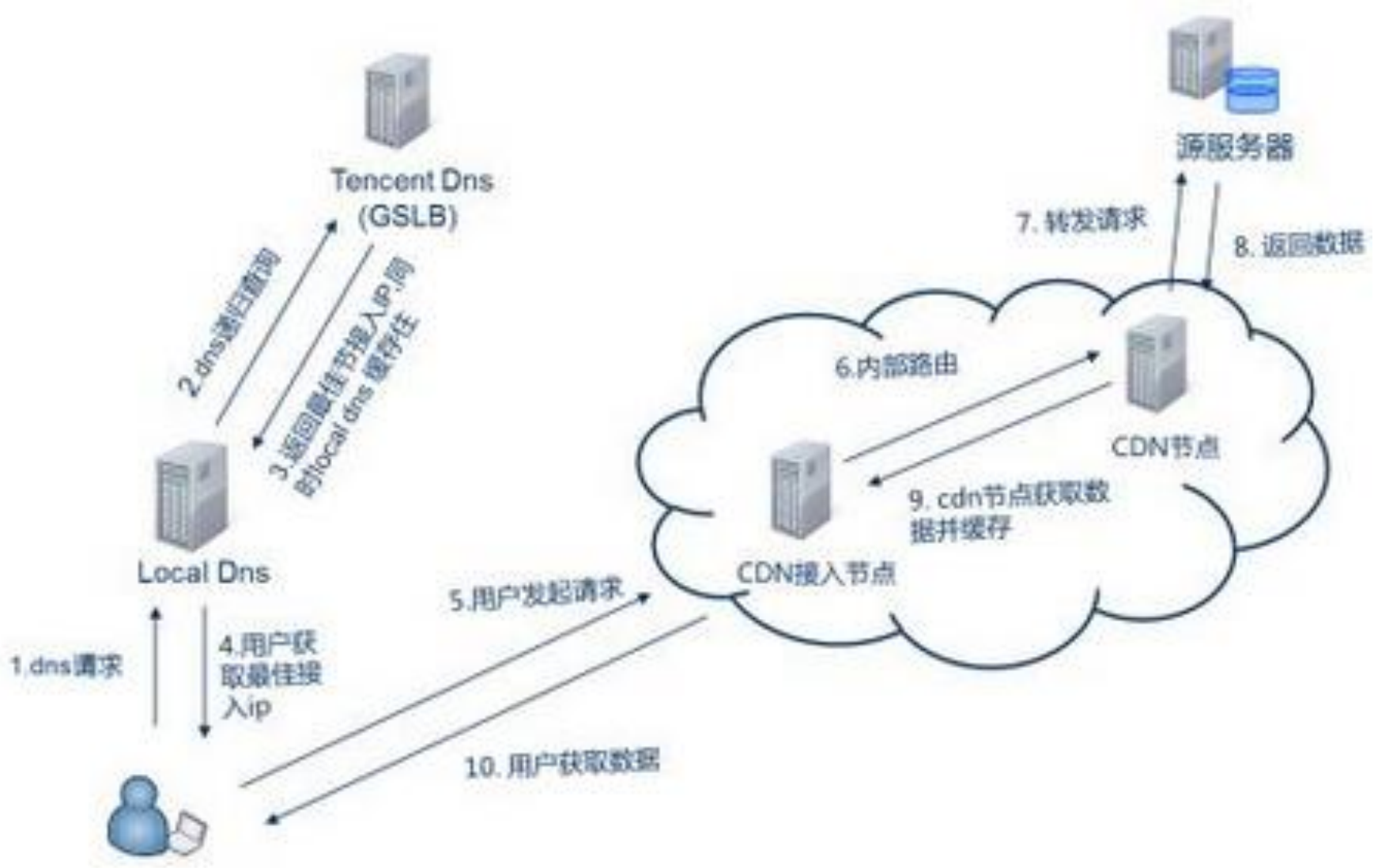
- (2) 特定区域转发：仅转发对特定的区域的请求，比全局转发优先级高

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

- 注意：关闭dnssec功能

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

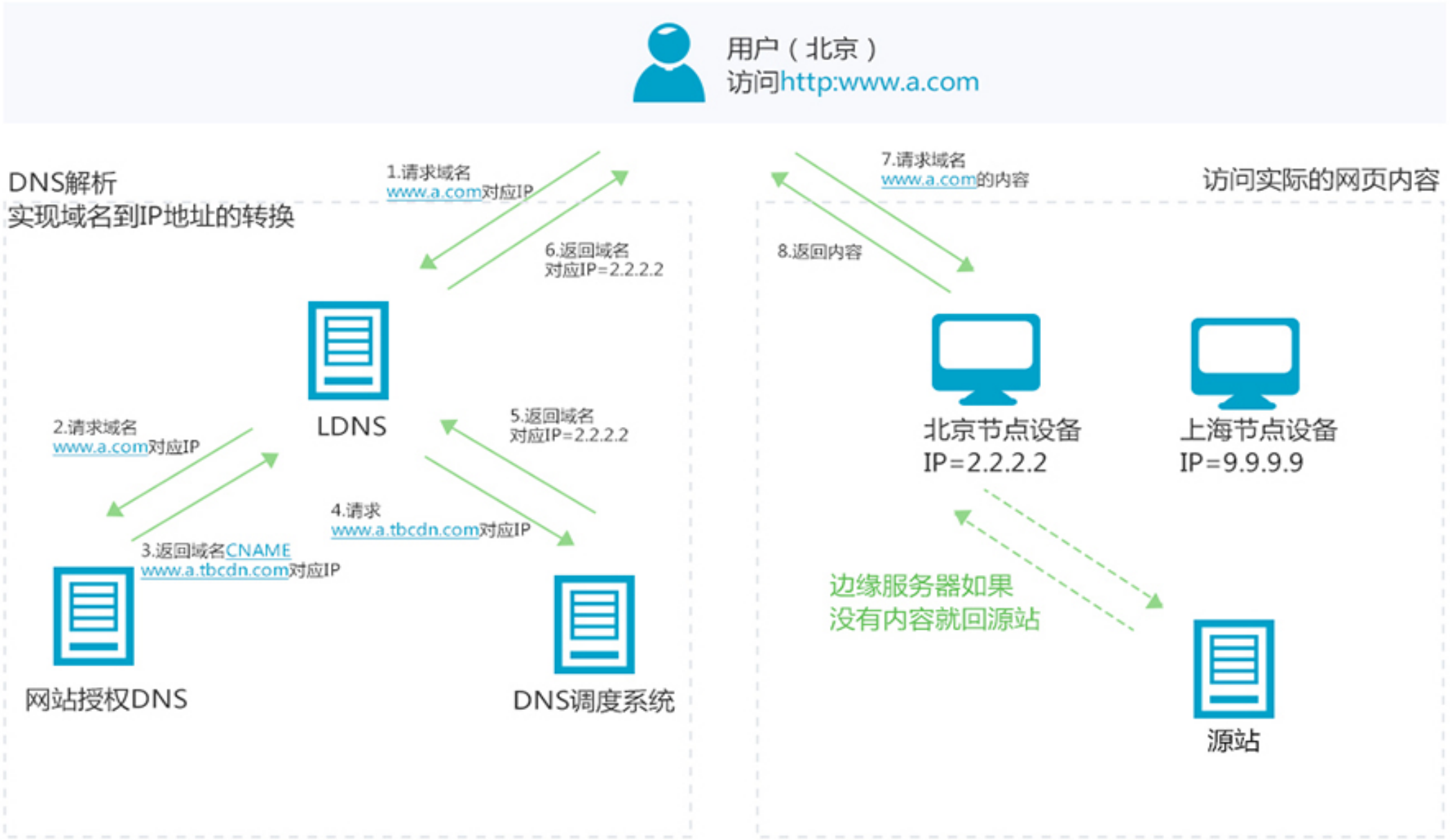
GSLB和CDN


Tencent Dns
(GSLB)
2.dns递归查询
3.返回最佳节接入IP,同时local dns 缓存住
Local Dns
1.dns请求
4.用户获取最佳接入ip
5.用户发起请求
10.用户获取数据
源服务器
7.转发请求
8.返回数据
6.内部路由
CDN节点
CDN接入节点
9.cdn节点获取数据并缓存

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

CDN（Content Delivery Network）



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

CDN

- CDN: Content Delivery Network 内容分发网络

  服务商：蓝汛，网宿，帝联等

- 智能DNS:

  dnspod

  dns.la

bind中ACL

- bind中基础的安全相关的配置：

  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

- 格式：

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

- 示例：

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

bind中ACL

- 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

- 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

bind view

- View：视图，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：
  (1) 一旦启用了view，所有的zone都只能定义在view中
  (2) 仅在允许递归请求的客户端所在view中定义根区域
  (3) 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

bind view

- 格式：

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

DNS排错

- #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

DNS排错

- NOERROR不代表没有问题，也可以是过时的记录
- 查看是否为权威记录，flags:aa标记判断
- 被删除的记录仍能返回结果，可能是因为*记录存在
- 如：*.example.com． IN A 172.25.254.254
- 注意“.”的使用
- 避免CNAME指向CNAME记录，可能产生回环
  - test.example.com. IN CNAME lab.example.com.
  - lab.example.com. IN CNAME test.example.com.
- 正确配置PTR记录，许多服务依赖PTR，如sshd,MTA
- 正确配置轮询round-robin记录

关于马哥教育

马哥教育
IT人的高薪职业学院

- 博客：http://mageedu.blog.51cto.com
- 主页：http://www.magedu.com
- QQ：1661815153, 113228115
- QQ群：203585050, 279599283

祝大家学业有成

谢　谢