



马哥教育  
最专业的Linux培训机构

# DNS服务

- ❖ 名字解析
- ❖ DNS服务
- ❖ 实现主从服务器
- ❖ 实现子域
- ❖ 实现view
- ❖ 编译安装
- ❖ 压力测试
- ❖ DNS排错

马哥教育

www.magedu.com

- ❖ DNS: Domain Name Service, 协议 (C/S, 53/udp, 53/tcp) 应用层协议
- ❖ BIND: Bekerley Internat Name Domain, ISC ([www.isc.org](http://www.isc.org))
- ❖ 本地名称解析配置文件: `hosts`

`/etc/hosts`

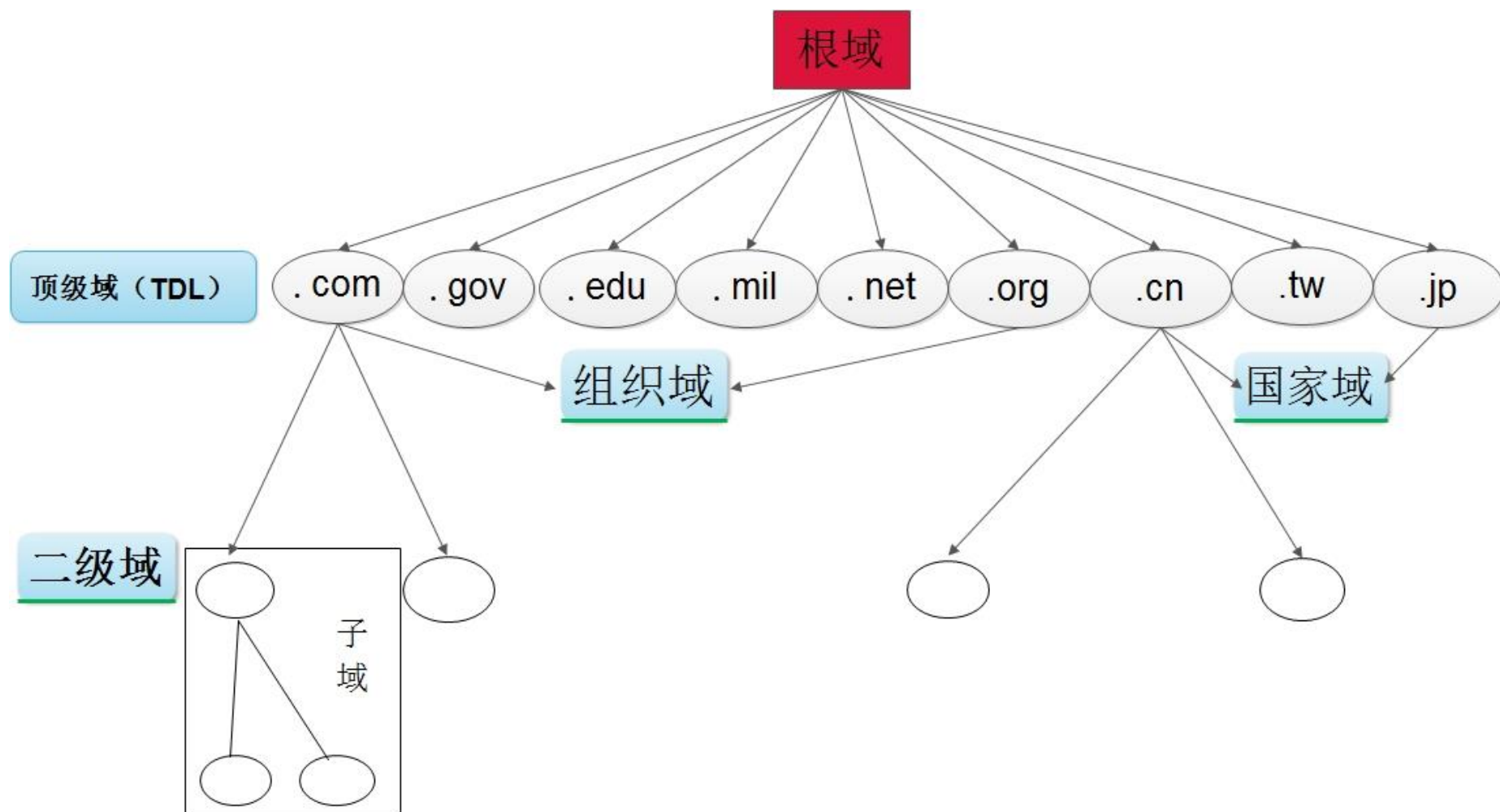
`%WINDIR%/system32/drivers/etc/hosts`

`1.1.1.1 www.magedu.com`

`2.2.2.2 www.apple.com`

`www.magedu.com`

- ❖ 根域
- ❖ 一级域名: Top Level Domain: tld  
com, edu, mil, gov, net, org, int,  
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:

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

马哥教育

www.magedu.com



❖ 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:

马哥教育

www.magedu.com

❖ 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

## ❖ 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

- ❖ **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linuxedu.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  
)
```

- ❖ **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

- ❖ **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**记录可有多条; 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:

(1) 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

- ❖ **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

- ❖ 注意:

*.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



## ❖ 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

简写成: 如1.2.3为网络地址, 可省

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

## ❖ CNAME:

**name:** 别名的FQDN

**value:** 真正名字的FQDN;

## ❖ 例如:

`www.magedu.com. IN CNAME webserv.magedu.com.`

马哥教育

www.magedu.com

❖ 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

## ❖ 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

马哥教育

www.magedu.com

域名控制台-解析设置

阿里云 <https://dc.aliyun.com/tcparse/dns.h> 百度

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

使用时长：  
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

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DN](#) [S，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	🛡️	<a href="#">修改</a> <a href="#">暂停</a> <a href="#">删除</a> <a href="#">备注</a>
A	www	默认		--	10分钟	🛡️	<a href="#">修改</a> <a href="#">暂停</a> <a href="#">删除</a> <a href="#">备注</a>
TXT	@	默认	v=spf1 include:spf.mxhichina.com ~all	--	10分钟	--	<a href="#">修改</a> <a href="#">暂停</a> <a href="#">删除</a> <a href="#">备注</a>
CNAME	mail	默认	mail.mxhichina.com	--	10分钟	--	<a href="#">修改</a> <a href="#">暂停</a> <a href="#">删除</a> <a href="#">备注</a>

域名控制台
 产品列表

我的域名
 基本管理
 域名解析
 安全

[redacted].com
 

使用期限：  
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](#)

[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	<input type="text"/>	默认	<input type="text"/>	--	10分钟		<a href="#">保存</a> <a href="#">取消</a>

**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

**NS记录：**域名解析服务器记录。如果要指定域名指定某个域名服务器来解析，需要设置NS记录



## ❖ BIND的安装配置:

dns服务程序包: bind, unbound

程序名: named, unbound

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/`

马哥教育  
[www.magedu.com](http://www.magedu.com)



- ❖ 服务脚本和名称: `/etc/rc.d/init.d/named`, `unbound.service`
- ❖ 主配置文件: `/etc/named.conf`, `/etc/named.rfc1912.zones`, `/etc/rndc.key`, `/etc/unbound/unbound.conf`
- ❖ 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;

马哥教育

## ❖ 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
```

```
rndc status|reload ;service named reload
```

\$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
```

❖ **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 @SERVER**

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**

❖ `host [-t type] name [SERVER]`

`host -t NS magedu.com @172.16.0.1`

❖ `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:

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.

- ❖ 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:

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

`rndc COMMAND`

## ❖ COMMAND:

**reload:** 重载主配置文件和区域解析库文件

**reload zone:** 重载区域解析库文件

**retransfer zone:** 手动启动区域传送过程，而不管序列号是否增加

**notify zone:** 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

- ❖ 注意：关闭dnssec功能：  
dnssec-enable no;  
dnssec-validation no;

- ❖ 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;

❖ 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/prefixlen;  
    .....  
};
```

❖ 示例:

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

❖ 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

马哥教育

www.magedu.com



## ❖ 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

马哥教育

www.magedu.com

- ❖ **view**:视图，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
- ❖ 格式：

```
view VIEW_NAME {  
    match-clients { };  
};
```

马哥教育  
www.magedu.com

## ❖ 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

## ❖ CDN: Content Delivery Network

## ❖ 智能DNS:

dnspod

dns.la

马哥教育

www.magedu.com

# 编译安装bind

## ❖ 下载bind:

isc.org:

bind-9.8

bind-9.9

bind-10

## ❖ 编译安装bind

```
# tar xvf bind-9.11.0a3.tar.gz
```

```
# cd bind-9.11.0a3/
```

```
# groupadd -r -g 53 named
```

```
# useradd -r -u 53 -g 53 named
```

```
# ./configure --prefix=/usr/local/bind9 --  
sysconfdir=/etc/named/ --disable-ipv6 --disable-chroot --enable-  
threads
```

```
# make
```

```
# make install
```

# 编译安装bind

## ❖ 环境变量:

- `vim /etc/profile.d/named.sh`  
`export PATH=/usr/local/bind9/bin:`  
`/usr/local/bind9/sbin/:$PATH`

## ❖ 库和头文件

- `vim /etc/ld.so.conf.d/named.conf`  
`/usr/local/bind9/lib`
- `ldconfig -v`
- `ls -sv /usr/local/bind9/include /usr/include/named`

## ❖ man帮助

- `vim /etc/man.config`  
`MANPATH /usr/local/bind9/share/man`
- `man named.conf`

```
❖ vim /etc/named/named.conf
    options {
        directory "/var/named/"
    };
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "localhost" IN {
        type master;
        file "named.localhost";
        allow-update {none;};
    };
    zone "1.0.0.127.in-addr.arpa" IN {
        type master;
        file "named.loopback";
        allow-update {none;};
    };
```

## ❖ 区域数据库

- `mkdir /var/named`
- `named-checkconf`
- `dig +nored @a.root-servers.net > /var/named/named.ca`
- `vim /var/named/named.localhost`

```
$TTL 1d
```

```
@ IN SOA localhost. admin.localhost. (
```

```
2016061801
```

```
1h
```

```
5m
```

```
7d
```

```
1d)
```

```
IN NS localhost.
```

```
localhost. IN A 127.0.0.1
```



```
❖ vim /var/named/named.local
    $TTL 1d
    @ IN SOA localhost. admin.localhost. (
        2016061801
        1h
        5m
        7d
        1d)
    IN NS localhost.
    IN PTR localhost.
```

## ❖ 设置权限

- `chmod 640 /var/named/*`
- `chmod 640 /etc/named/named.conf`
- `chown :named /var/named/*`
- `chown :named /etc/named/named.conf`

## ❖ 启动服务和测试

- `man named`
- `named -u named -f -g -d 3` 前端级别3方式运行
- `named -u named` 后台运行
- `killall named`
- `ss -uln`
- `tail /var/log/message`
- `named -u named`

## ❖ 支持rndc

- rndc reload 看报错提示
- rndc-confgen -r /dev/urandom > /etc/named/rndc.conf 生成key
- tail /etc/named/rndc.conf >> /etc/named/named.conf
- killall -SIGHUP named
- rndc status

马哥教育

www.magedu.com

- ❖ `/root/bind-xxx/contrib/scripts`
- ❖ 编译压力测试工具
  - `cd /root/bind-xxx/contrib/queryperf`
  - `./configure`
  - `make`
  - `cp queryperf /usr/local/bind9/bin`
  - `queryperf -h`

马哥教育

[www.magedu.com](http://www.magedu.com)

## ❖ 压力测试

- vim test.txt

www.magedu.com A

magedu.com NS

magedu.com MX

pop3.magedu.com A

web.magedu.com A

- queryperf -d test.txt -s 127.0.0.1

## ❖ 打开日志功能

马哥教育

- rndc querylog

www.magedu.com

- rndc status

- queryperf -d test.txt -s 127.0.0.1

- wc -l /var/log/message

## ❖ #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

- **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



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

马哥教育  
[www.magedu.com](http://www.magedu.com)



马哥教育  
最专业的Linux培训机构

# Thank You!