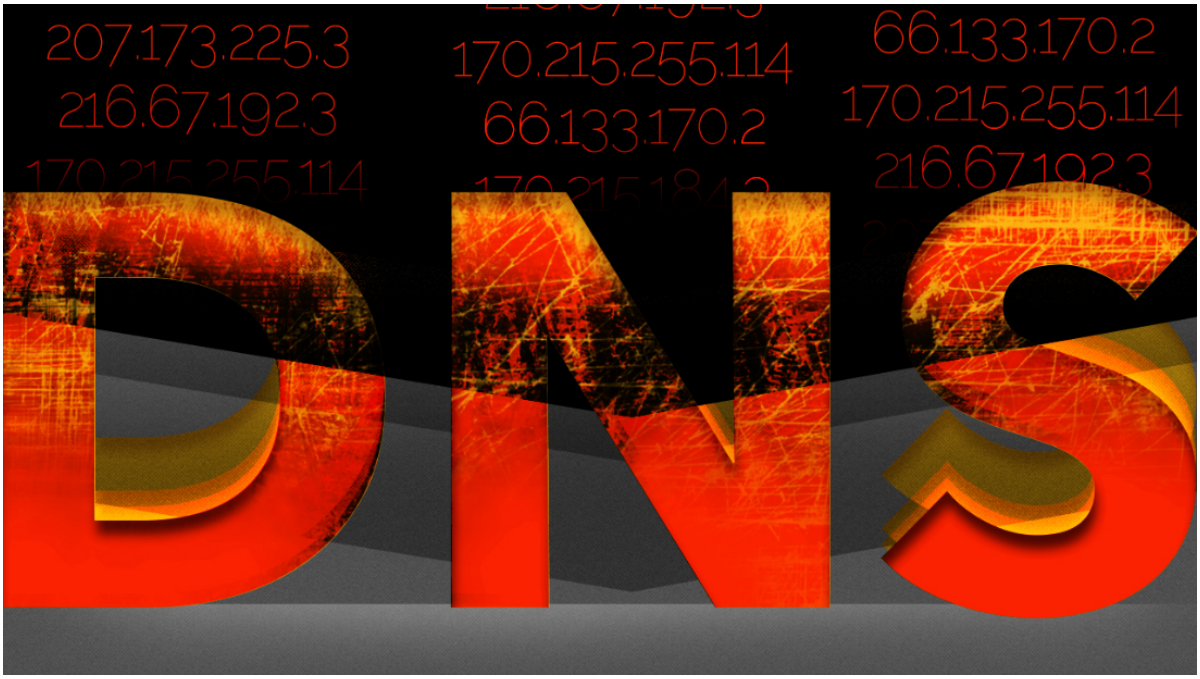

正/反向解析

> 以jinweiayy.com这个域名为例进行配置,DNS服务器IP为192.168.1.109，域名解析指向192.168.1.110

主配置文件：/etc/named.conf

```
vim /etc/named.conf

options {
  listen-on port 53 { any; };
  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-recursion { server_ip };
  allow-query { any; };
  recursion yes;
  allow-transfer { none; };
};

logging {
  channel default_debug {
    file "data/named.run";
```

```
    severity dynamic;
  };
};

zone "." IN {
  type hint;
  file "named.ca";
};

zone "jinweiayy.com." IN {
  type master;
  file "jinweiayy.com.zone";
};

zone "1.168.192.in-addr.arpa." IN {
  type master;
  file "192.168.1.zone"
};

include "/etc/named.rfc1912.zones";
```

正向解析区域文件：/var/named/jinweiayy.com.zone

```
vim /var/named/jinweiayy.com.zone

$TTL 600
@   IN  SOA dns.jinweiayy.com.  jinweiayy.gmail.com
(
            2017022601
            2H
            10M
            1W
            1D )
@   IN  NS  dns.jinweiayy.com.
dns IN  A   192.168.1.109
@       IN  MX  10  mail
mail    IN  A   192.168.1.110
www IN  A   192.168.1.110
```

```
15 ftp IN   CNAME    www
```

反向解析区域文件：/var/named/1.168.192.zone

```
1  vim /var/named/192.168.1.zone
2
3  $TTL 600
4  @    IN   SOA dns.jinweiayy.com.  jinweiayy.gmail.com
   (
5               2017022601
6               2H
7               10M
8               1W
9               1D )
10 @    IN   NS   dns.jinweiayy.com.
11 109  IN   PTR dns.jinweiayy.com.
12 110  IN   PTR www.jinweiayy.com.
13 110  IN   PTR mail.jinweiayy.com.
```

修改权限及属组

```
1 cd /var/named/
2 chown root:named jinweiayy.com.zone
3 chown root:named 192.168.1.zone
4 chmod 640 jinweiayy.com.zone
5 chmod 640 1.168.192.zone
```

检查主配置文件及区域文件

```
1 named-checkconf
2 named-checkconf -z /etc/named.conf  #显示详细的检查信息
3 named-checkzone "jinweiayy.com.zone"
  /var/named/jinweiayy.com.zone
4 named-checkzone "192.169.1.zone"
  /var/named/192.168.1.zone
```

启动并观测日志

```
systemctl start named.service
tail /var/log/messages
```

测试

```
#如果利用其他主机进行测试，需要开放53端口，设置开机自启
firewall-cmd --zone=public --add-port=53/tcp --permanent
firewall-cmd --zone=public --add-port=53/udp --permanent
systemctl reload firewalld.service
systemctl enable named.service
#测试
dig -t A www.jinweiayy.com @192.168.1.109
dig -t NS jinweiayy.com @192.168.1.109
dig -t MX jinweiayy.com @192.168.1.109
dig -x 192.168.1.110 @192.168.1.109
#继续观察日志信息，看是否报错信息
```

注意事项

1. 根据实际环境配置/etc/named.conf文件的options选项，尤其是安全控制选项
2. 反向解析区域的定义，zone-name为网络地址的逆写形式。例如：192.168.1.110，则zone-name写为1.168.192.in-addr.appa.

主从复制

> 以jinweiayy.com这个域名为例进行配置,Master DNS 服务器IP为192.168.1.107，Slave DNS 服务器IP为192.168.1.108。以上例为基础进行配置。

Master DNS 服务器配置

修改/etc/named.conf主配置文件

```
vim /etc/named.conf
```

```
2
3  options {
4    listen-on port 53 { any; };
5    directory "/var/named/";
6    dump-file "/var/named/data/cache_dump.db";
7    statistics-file "/var/named/data/named_stats.txt";
8    memstatistics-file
   "/var/named/data/named_mem_stats.txt";
9    //allow-recursion { server_ip };
10   allow-query { any; };
11   recursion yes;
12   //allow-transfer { none; };
13 };
14
15 logging {
16   channel default_debug {
17     file "data/named.run";
18     severity dynamic;
19   };
20 };
21
22 zone "." IN {
23   type hint;
24   file "named.ca";
25 };
26
27 zone "jinweiayy.com." IN {
28   type master;
29   file "jinweiayy.com.zone";
30   //增加Slave DNS 服务器的ip地址，即允许许谁传送
31   allow-transfer { 127.0.0.1; 192.168.1.108; };
32 };
33
34 zone "1.168.192.in-addr.arpa." IN {
35   type master;
36   file "192.168.1.zone"
37   //增加Slave DNS 服务器的ip地址，即允许许谁传送
38   allow-transfer { 127.0.0.1; 192.168.1.108; };
```

```
};

include "/etc/named.rfc1912.zones";
```

区域数据文件中增加资源记录

```
vim /var/named/jinweiayy.com.zone

$TTL 600
@   IN  SOA dns.jinweiayy.com.  jinweiayy.gmail.com
(
            2017022601
            2H
            10M
            1W
            1D )
@   IN  NS  dns.jinweiayy.com.
@   IN  NS  dns1.jinweiayy.com.
dns IN  A   192.168.1.107
dns1    IN  A   192.168.1.108
@       IN  MX  10  mail
mail    IN  A   192.168.1.110
www     IN  A   192.168.1.110
ftp IN  CNAME   www
```

```
vim /var/named/192.168.1.zone

$TTL 600
@   IN  SOA dns.jinweiayy.com.  jinweiayy.gmail.com
(
            2017022601
            2H
            10M
            1W
            1D )
@   IN  NS  dns.jinweiayy.com.
@   IN  NS  dns1.jinweiayy.com.
107 IN  PTR dns.jinweiayy.com.
```

```
108 IN  PTR dns.jinweiayy.com.
110 IN  PTR www.jinweiayy.com.
110 IN  PTR mail.jinweiayy.com.
```

Slave DNS 服务器配置

```
vim /etc/named.conf

options {
  listen-on port 53 { any; };
  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-recursion { server_ip };
  allow-query { any; };
  recursion yes;
  allow-transfer { none; };
};

logging {
  channel default_debug {
    file "data/named.run";
    severity dynamic;
  };
};

zone "." IN {
  type hint;
  file "named.ca";
};

zone "jinweiayy.com." IN {
  type slave;
  file "slaves/jinweiayy.com.zone";
  masters { 192.168.1.107; };
```

```
};

zone "1.168.192.in-addr.arpa." IN {
  type slave;
  file "slaves/192.169.1.zone";
  masters { 192.168.1.107; };
};

include "/etc/named.rfc1912.zones";
```

启动并观察日志

```
systemctl start named.service
tail /var/log/messages
#查看slave DNS 服务器是否有区域文件传送
ls -l /var/named/slaves
```

分别进行测试

```
dig -t A www.jinweiayy.com @192.168.1.107
dig -t NS jinweiayy.com @192.168.1.107
dig -t MX jinweiayy.com @192.168.1.107
dig -x 192.168.1.110 @192.168.1.107

dig -t A www.jinweiayy.com @192.168.1.108
dig -t NS jinweiayy.com @192.168.1.108
dig -t MX jinweiayy.com @192.168.1.108
dig -x 192.168.1.110 @192.168.1.108
```

注意事项

1. 一般而言，主DNS服务器的bind版本可以低于从服务器bind的版本，但如果高于从服务器bind版本，则可能会出现功能不支持的现象。
2. 从服务器和主服务器都需要获得上级授权，可以利用域名提供商的管理面板去修改DNS服务器IP从而获得授权。

子域授权

> jinweiayy.com.的子域xixi.jinweiayy.com.为例，以上例配置的Master/Slave DNS 服务器为基础。

在上层DNS服务器的区域文件中增加记录

只需要在上层DNS服务器的区域文件中增加一条NS记录和A记录。这个过程即是授权过程，将子域的解析职责授予下层DNS服务器进行管理。

```
xixi    IN  NS  dns.xixi.jinweiayy.com.
dns.xixi.jinweiayyy.com.    IN  A   192.168.1.109
```

请求转发

转发机制

当设置了转发机制后，当有查询请求时，如果不是本域负责的域名或者缓存中没有的查询都将转发到指定的DNS服务器，由这台指定的DNS服务器进行查询返回查询答复。

字段含义

> fordward：值可以是`first`和`only`。当值是first时，只转发，如果指定DNS服务器不应答也不去找根；当值是only时，先转发，如果DNS服务器不应答就去找根，由指定DNS服务器全权负责解析。

> forwarders：指定转发目的DNS服务器，这个字段也可以设置在zone内。

转发非本机负责解析的区域

```
opotions {
    forward only;
    forwarders { DNS_SERVER_ip; };
};
```

转发特定区域

```
zone "特定区域" IN {
    type forward;
    forwarders { DNS_SERVER_IP; };
    forwarders only;
};
```

view功能

> view：不同的客户端发来请求时答复给给不同的解析结果。

使用view功能的配置文件

```
options {
    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; };
    recursion yes;
    allow-transfer { none; };
};
//针对 intranet 给予的来源 IP 指定
acl external {
  192.168.1.109/24;
};
//加上惊叹号 (!) 代表反向选择的意思
acl internet {
  ! 192.168.100.109/24;
  any;
};
//每一个view要有一个名称
view "view1" {
    match-clients { "intranet"; };
    zone "." IN {
        type hint;
        file "named.ca";
```

```
    };
    zone "centos.vbird" IN {
        type master;
        file "named.centos.vbird";
        allow-transfer { 192.168.100.10; };
    };
    zone "100.168.192.in-addr.arpa" IN {
        type master;
        file "named.192.168.100";
        allow-transfer { 192.168.100.10; };
    };
};

view "view2" {
    match-clients { "internet"; };
    zone "." IN {
        type hint;
        file "named.ca";
    };
    zone "centos.vbird" IN {
        type master;
        file "named.centos.vbird.inter";
    };
};
```

注意事项

1. 如果使用 view 功能，则必须将所有的zone放入 view 中
2. view 将配置文件中规则从上往下匹配

性能测试

1. **下载bind源码包**

```
wget https://www.isc.org/downloads/file/bind-9-9-9-p6/?version=tar-gz
```

2. **编译测试工具**

```
cd bind-9.9.9-P6/contrib/queryperf
./configure
make
cp queryperf /usr/bin/
```

3. **测试**

```
#查看帮助信息
querypert -h

#创建测试查询文件。例如：
mail.xjwlinux.com       A
dns3.xjwlinux.com       NS
mail.xjwlinux.com       A
dns3.xjwlinux.com       NS
.
.
.

#测试
querypert -d test.DNS -s server_ip
```

ACL

1. ACL，访问控制列表
2. BIND的四个内置访问控制列表：any、none、local、localnet
3. ACL只有在定义之后才能使用
4. 示例

```
acl ACL_NAME {
    ip/24;
    ip/24;
};
```

RNDC

> rnds(Remote Name Domain Controller)，远程管理BIND的工具。可以在局域网或本地对DNS服务器进行方便快捷的管理。

rndc配置

```
#生成rndc.conf文件
rndc-confgen -r /dev/urandom > /etc/rndc.conf
```

```
#将key、controls项复制到/etc/named.conf文件中
cat /etc/rndc.conf

# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-md5;
        secret "0/aywg7w+6u/6Xo+35m4aA==";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-md5;
#       secret "0/aywg7w+6u/6Xo+35m4aA==";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#       allow { 127.0.0.1; } keys { "rndc-key"; };
# };
```

```
27 # End of named.conf
```

rndc命令

```
1  rndc status      #查看DNS服务器状态
2  rndc stats       #记录当前DNS服务器统计数据，并写入data/
   目录下
3  rndc dumpdb          #记录当前DNS服务器缓存数据，并写入
   data/目录下
4  rndc reload          #重新载入配置文件和区域文件
5  rndc reload zone_name    #重新载入指定区域文件
6  rndc stop        #停止服务器
7  rndc flush       #清空所有缓存
8  rndc retransfer z_name   #重新传送某个区域
9  rndc reconfig        #只重读配置文件并加载新增的区域
10 rndc querylog        #关闭或开启查询日志。客户端查询记录
   会在日志信息中显示
11 rndc trace       #打开debug模式
```

参考

/etc/named.comf：https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-bind-namedconf.html

DNS服务器类型及查询过程：http://www.178linux.com/67736

DNS 的 SOA 记录简介:http://www.sigma.me/2011/01/01/about_dns_soa.html

DNS and BIND 介绍及安装：http://www.178linux.com/16152

archlinuxBIND：https://wiki.archlinux.org/index.php/BIND_(%E7%AE%80%E4%BD%93%E4%B8%AD%E6%96%87)

IP地址详解：http://vod.sjtu.edu.cn/help/Article_Show.asp?ArticleID=631