



链滴

DNS 服务 bind 配置说明

作者: [nianxingyan](#)

原文链接: <https://ld246.com/article/1509012910017>

来源网站: 链滴

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

官网: <https://www.isc.org/downloads/bind/>

安装:

```
yum install bind
```

```
yum install bind-utils # 包含了dig/nslookup/host等工具
```

```
yum install bind-chroot # 说是可以出于安全原因, 改变配置文件的根路径, 但不知道怎么用, 感不装也行
```

安装完成后, 默认配置文件位于:

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

```
/var/named/
```

注意, /var/named/目录下的解析文件权限必须是0640, 且必须在named用户组, 否则解析文件会载失败, 导致解析相应域名时出现SERVFAIL错误

/etc/named.conf内容:

```
// 全局配置
options {
    listen-on port 53 { 127.0.0.1; 192.168.10.8; };
    // 配置文件根目录
    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 { localhost; 192.168.10.0/24; };
    recursion yes;
    // 外部的DNS服务器, 这里可以配置成ISP的DNS服务器
    forwarders { 211.167.230.100; 211.167.230.200; };
    // 这里定义了一个特殊的zone, 实际我们用这个zone来定义哪些域名被禁止解析
    response-policy { zone "badlist"; };
};
// 日志
logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};
// 一个zone就相当于DNS解析中的一个域名
// 比如 "zhilehuo.com"
// 然后在zone的file指定的文件中, 配置该域名下所有的解析记录
zone "bjoffice1.zhilehuo.com" IN {
    type master;
    file "named.bjoffice1.zhilehuo.com.zone";
};
// 这是一个特殊的zone, 被定义在options中的response-policy中
// 作用是可以定义一个特殊的zone文件, 不过我有点描述不清楚.....
zone "badlist" {
    type master;
    file "named.badlist.zone";
    allow-query { none; };
};
```

```
};  
// 这是bind安装后默认生成的一个文件, 定义了类似localhost, 127.0.0.1等  
include "/etc/named.rfc1912.zones";
```

/var/named/named.bjoffice1.zhilehuo.com.zone 内容:

```
$TTL 60  
@ IN SOA @ rname.invalid. (  
    0 ; serial  
    1D ; refresh  
    1H ; retry  
    1W ; expire  
    3H ) ; minimum  
NS @  
@ IN A 192.168.10.8  
* IN A 192.168.10.8
```

/var/named/named.badlist.zone 内容:

```
$TTL 1H  
@ SOA LOCALHOST. named-mgr.example.com (1 1h 15m 30d 2h)  
NS LOCALHOST.
```

```
bjoffice1-proxy.zhilehuo.com CNAME .  
*.bjoffice1-proxy.zhilehuo.com CNAME .
```

维护命令:

bind的进程名称是**named**, 在Centos6下安装后, 会创建/etc/init.d/named脚本, 可以手动通过**chkconfig**加到系统启动列表中; 同时, 应该也被安装在service服务中

在CentOS7下, bind安装后以**systemctl**服务存在, 需要通过systemctl启动:

```
systemctl enable named  
systemctl start named
```

配置修改后, 可以重启named, 或者通过**rndc reload**重新加载配置