Linux搭建DNS服务

参考 ： http://blog.csdn.net/charlsecharlse/article/details/17955119

DNS服务器分为 ： 主域名服务器、从域名服务器、缓存域名服务器
提供的服务分为 ： 正向解析、反向解析

一、单一域名服务器
DNS是域名系统（Domain Name System）的缩写，是因特网的一项核心服务，它能提供域名与IP地址之间对应关系的转换服务。这样我们就可以更方便地去访问互联网了，不用去记住那一串IP数字。本文档主要是说明如何把一台CentOS主机配置成一个DNS服务器，以便能提供域名解析服务。

(1) DNS服务器端配置

操作系统：CentOS 6.4
IP地址：172.16.1.4
DNS软件：Bind 9.8
测试域名：realhostip.com
作用：主要提供解析realhostip.com域名的服务

1. 安装**bind**
yum install bind

2. 修改**/etc/named.conf**配置文件
vi /etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { any; }; //开启监听端口53，接受任意IP连接
        listen-on-v6 port 53 { ::1; };  //支持IP V6
        directory       "/var/named";  //所有的正向反向区域文件都在这个目录下创建
        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     { 0.0.0.0/0; }; //允许任意IP查询
        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};
```

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

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

include "/etc/named.rfc1912.zones"; //主要配置文件
include "/etc/named.root.key";
```

3. 修改**/etc/named.rfc1912.zones**文件，添加**realhostip.com**的正向和反向区域

```
# vi /etc/ named.rfc1912.zones
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "named.localhost";
        allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
        type master;
        file "named.loopback";
        allow-update { none; };
};



        type master;
        file "named.loopback";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.empty";
        allow-update { none; };
};
```

```
//realhostip.com的正向区域
zone "realhostip.com" IN {
        type master;
        file "named.realhostip.com";
        allow-update { none; };
};
//realhostip.com的反向区域
zone "1.16.172.in-addr.arpa" IN {
        type master;
        file "172.16.1.arpa";
        allow-update { none; };
};
```

这里需要注意的是，添加反向区域时，网络号要反过来写（网络号是IP地址与子网掩码进行与操作后的结果）。

例如，我现在配置的网络号172.16.1这个网段，那么它的反向区域是1.16.172.in-addr.arpa。区域里面的file字段表明解析时的数据来源文件，接下来我们去创建named.realhostip.com和172.16.1.arpa文件。

4. 创建正向和反向区域资源文件

在配置named.conf时，指明的资源文件目录是/var/named，故先进入该目录。

```
# cd /var/named
# vi named.realhostip.com
$TTL 1D
@       IN SOA  realhostip.com. rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
172-16-1-50 IN A 172.16.1.50
172-16-1-51 IN A 172.16.1.51
```

以上我添加了两条记录，其中172-16-1-50 IN A 172.16.1.50表明域名172-16-1-50.realhostip.com对应的IP地址为172.16.1.50。

如果需要添加多条，按此类似添加，留意realhostip.com后面的那个不起眼的点（.）。

```
# vi 172.16.1.arpa
$TTL 1D
@       IN SOA  realhostip.com. rname.invalid. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        AAAA    ::1
50      PTR     172-16-1-50.realhostip.com.
51      PTR     172-16-1-51.realhostip.com.
```

以上我也添加了两条记录，其中50 PTR 172-16-1-50.realhostip.com表明IP地址172.16.1.50对应的域名为172-16-1-50.realhostip.com。如果要添加多条，按此类似添加，留意realhostip.com后面的那个不起眼的点（.）。

5. 启动**named**服务

```
#service named start
```

至此，DNS服务器端的配置已完成，下面我们稍微配置一下客户端来测试我们的DNS服务器是否正常工作。

(2) 客户端配置

操作系统：windows和linux都可以，我这里是CentOS 6.4

IP地址：能够ping通DNS服务器的IP（172.16.1.4）都可以，我这里是172.16.1.104

作用：测试DNS服务器是否正常工作。

1. 安装**bind-utils**包，以便能使用**nslookup**、**dig**和**host**工具

yum install bind-utils

2. 修改**DNS**配置使用我们的**DNS**服务器

vi /etc/resolv.conf

nameserver 172.16.1.4
nameserver 192.168.13.31
nameserver 172.16.1.1

resolv.conf文件中可能会有多个nameserver，必须把我们的DNS服务器放在所有nameserver的最前面，
这样当需要解析域名时，第一个使用的就是我们配置的DNS服务器，其它的都是候选项。

3. 正向解析测试，使用**nslookup**命令

#nslookup

> 172-16-1-50.realhostip.com
Server: 172.16.1.4
Address: 172.16.1.4#53

Name: 172-16-1-50.realhostip.com
Address: 172.16.1.50

>
> 172-16-1-51.realhostip.com
Server: 172.16.1.4
Address: 172.16.1.4#53

Name: 172-16-1-51.realhostip.com
Address: 172.16.1.51
>

从结果可以看到，我们配置的两个域名都能成功解析，并且DNS服务器就是我们配置的那个服务器。

4. 反向解析，使用**nslookup**命令

#nslookup

>
> 172.16.1.51
Server: 172.16.1.4
Address: 172.16.1.4#53

51.1.16.172.in-addr.arpa name = 172-16-1-51.realhostip.com.
>
>
> 172.16.1.50
Server: 172.16.1.4
Address: 172.16.1.4#53

50.1.16.172.in-addr.arpa name = 172-16-1-50.realhostip.com.
>
>

从结果来看，可以正确解析我们的IP地址，并且DNS服务器就是我们配置的那个服务器。

5. 查看**realhostip.com**这个域名是哪个**DNS**服务器管理的，使用**dig**命令

```
# dig -t ns realhostip.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6 <<>> -t ns realhostip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37964
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;realhostip.com.                IN      NS

;; ANSWER SECTION:
realhostip.com.         86400   IN      NS      realhostip.com.

;; ADDITIONAL SECTION:
realhostip.com.         86400   IN      A       172.16.1.4
realhostip.com.         86400   IN      AAAA    ::1

;; Query time: 1 msec
;; SERVER: 172.16.1.4#53(172.16.1.4)
;; WHEN: Wed Oct 23 14:15:22 2013
;; MSG SIZE  rcvd: 90
```

6. 使用**dig**命令进行正向解析

```
# dig 172-16-1-50.realhostip.com

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.17.rc1.el6_4.6 <<>> 172-16-1-50.realhostip.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21109
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;172-16-1-50.realhostip.com.    IN      A

;; ANSWER SECTION:
172-16-1-50.realhostip.com. 86400 IN    A       172.16.1.50

;; AUTHORITY SECTION:
realhostip.com.         86400   IN      NS      realhostip.com.

;; ADDITIONAL SECTION:
realhostip.com.         86400   IN      A       172.16.1.4
realhostip.com.         86400   IN      AAAA    ::1

;; Query time: 1 msec
;; SERVER: 172.16.1.4#53(172.16.1.4)
;; WHEN: Wed Oct 23 14:17:57 2013
;; MSG SIZE  rcvd: 118
```

注意：

windows客户端上只有nslookup工具

二、主从域名服务器

环境 ： 192.168.2.7 dns1 ： 主DNS服务

192.168.2.8　dns2 : 从DNS服务

软件 ：

bind包 ： 提供主程序

bind-libs : 提供库文件

bind-utils : 提供常用命令工具包

bind-chroot : 将服务器根转换到dns目录下，提高服务器安全性

安装配置软件 ：

yum install bind bind-libs bind-utils