# 二.DNS服务器搭建

## 1.DNS工作原理

### 1.1DNS服务器的功能

– **正向解析**:根据注册的域名查找其对应的IP地址

– **反向解析**:根据IP地址查找对应的注册域名,不常用

### 1.2DNS的分布结构

所有完整的域名都会以 **.** 结尾

根域 .

**一级DNS服务器**

.com .cn .us .tw .kr .hk .......

**二级DNS服务器**

.com.cn .net.cn .org.cn .edu.cn

**三级DNS服务器**

.tedu.com.cn .haha.com.cn .xixi.com.cn

**完整的主机名**

web1.tedu.com.cn tts.tedu.com.cn

• Full Qualified Domain Name (FQDN),完全合格主机名

– = **站点名.域名后缀**

– = **站点名. .. .. .二级域.一级域**

比如,www.pku.edu.cn

• 常见的顶级/一级域名

**– 国家/地区域: .cn、.us、.kr、.hk、.tw、.. ..**

**– 组织域:.com、.net、.edu、.org、.gov、.mil、.. ..**

## 2.BIND服务分析

### 2.1BIND域名服务

• BIND(Berkeley Internet Name Daemon)

– 伯克利 Internet 域名服务

– 官方站点:https://www.isc.org/

bind-9.9.4-29.el7.x86\_64 //域名服务包

bind-chroot-9.9.4-29.el7.x86\_64 //提供虚拟根支持

.BIND服务器端程序

**– 主要执行程序:/usr/sbin/named**

**– 系统服务:named**

**– 默认端口:TCP/UDP 53**

**– 运行时的虚拟根环境:/var/named/chroot/**

**• 主配置文件: /etc/named.conf #设置本机负责解析的域名是什么**

**• 地址库文件: /var/named/ #主机名与ip地址的对应关系**

## 3.单区域DNS服务

搭建基本的DNS服务

服务端：**虚拟机A**

### 3.1安装软件包(bind bind-chroot)

[root@svr7 ~]# **yum -y install bind bind-chroot**

### 3.2修改配置文件/etc/named.conf

[root@svr7 ~]# **vim /etc/named.conf**

options {

directory "/var/named"; #指定地址库文件存放路径

};

zone "tedu.cn" IN { #指定本机负责解析的域名

type master; #指定本机为权威主DNS服务器

file "tedu.cn.zone"; #指定地址库文件为tedu.cn.zone

};

### 3.3检查配置语法

**格式：**

**named-checkconf [配置文件]**

[root@svr7 ~]# named-checkconf **[若配置正确，无任何输出]**

### 3.4建立地址库文件tedu.cn.zone

[root@svr7 ~]# cd /var/named/

[root@svr7 named]# **cp -p named.localhost tedu.cn.zone**

#**权限属性不变拷贝**

[root@svr7 named]# ls -l tedu.cn.zone

-rw-r----- 1 root named 152 6月 21 2007 tedu.cn.zone

[root@svr7 named]# vim tedu.cn.zone

[root@svr7 named]# tail -4 tedu.cn.zone

tedu.cn. NS  **ns1.tedu.cn.** #域名可以随便定义

#**声明tedu.cn.域名的DNS服务器为svr7.tedu.cn.**

svr7 A 192.168.4.7 #**指定svr7.tedu.cn.的ip地址为192.168.4.7**

ns1 A 192.168.4.7

**www** A 1.1.1.1 **#前面不允许有空格**

ftp A 2.2.2.2

### 3.5重起named，设置开机自启动

[root@svr7 named]# systemctl restart named

[root@svr7 named]# systemctl enable named

### 3.6客户端检查

客户端：**虚拟机B**

方法1（**临时配置**）

[root@pc207 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@pc207 ~]# nslookup www.tedu.cn

方法2（**永久配置**）

[root@pc207 ~]# nmcli connection modify eth0 ipv4.dns 192.168.4.7

[root@pc207 ~]# nslookup svr7.tedu.cn

## 4.多区域DNS服务

**虚拟机A**

### 4.1修改配置文件/etc/named.conf

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

### 4.2建立地址库文件

[root@svr7 /]# cd /var/named/

[root@svr7 named]# cp -p tedu.cn.zone qq.com.zone

[root@svr7 named]# vim qq.com.zone

[root@svr7 named]# tail -4 qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 3.3.3.3

ftp A 4.4.4.4

### 4.3重起named服务

[root@svr7 named]# systemctl restart named

# 三.特殊的解析记录

## 1.基于DNS域名的负载均衡

[root@svr7 named]# vim qq.com.zone

[root@svr7 named]# tail -6 qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.11

www A 192.168.4.12

www A 192.168.4.13

ftp A 4.4.4.4

## 2.泛域名解析

**虚拟机A**

[root@svr7 /]# cd /var/named/

[root@svr7 named]# vim qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.11

ftp A 4.4.4.4

\* A 1.2.3.4

[root@svr7 /]# systemctl restart named

**虚拟机B**

[root@pc207 /]# nslookup www.qq.com

[root@pc207 /]# nslookup hahaxixi.qq.com

## 3.有规律的泛域名解析

web1.qq.com------》192.168.10.1

web2.qq.com------》192.168.10.2

web3.qq.com------》192.168.10.3

web4.qq.com------》192.168.10.4

......

web50.qq.com------》192.168.10.50

**函数： $GENERATE 生成连续范围的数字**

**虚拟机A**

[root@svr7 /]# cd /var/named/

[root@svr7 named]# vim qq.com.zone

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.11

ftp A 4.4.4.4

\* A 1.2.3.4

$GENERATE 1-50 web$ A 192.168.10.$

[root@svr7 named]# systemctl restart named

# 四.DNS的子域授权

父域 www.tedu.cn 总公司

子域 www.bj.tedu.cn 北京分公司

tedu.cn域名由 svr7 服务器192.168.4.7

bj.tedu.cn域名由 pc207 服务器 192.168.4.207

虚拟机B：搭建DNS负责解析bj.tedu.cn域名

1.安装软件包

[root@pc207 ~]# yum -y install bind bind-chroot

2.修改配置文件/etc/named.conf

options {

directory "/var/named";

};

zone "bj.tedu.cn" IN {

type master;

file "bj.tedu.cn.zone";

};

3.建立地址库文件bj.tedu.cn.zone

[root@pc207 ~]# cd /var/named/

[root@pc207 named]# cp -p named.localhost bj.tedu.cn.zone

[root@pc207 named]# vim bj.tedu.cn.zone

bj.tedu.cn. NS pc207

pc207 A 192.168.4.207

www A 11.12.13.14

4.重起named，设置开机自启动

[root@pc207 named]# systemctl restart named

[root@pc207 named]# systemctl enable named

[root@pc207 named]# nslookup www.bj.tedu.cn 192.168.4.207

实现目标1：询问svr7虚拟机A www.bj.tedu.cn 能够得到结果

虚拟机A：子域授权

[root@svr7 named]# cd /var/named

[root@svr7 named]# vim tedu.cn.zone #指定子域的DNS服务器

tedu.cn. NS svr7

bj.tedu.cn. NS pc207.bj

svr7 A 192.168.4.7

pc207.bj A 192.168.4.207

www A 1.1.1.1

ftp A 2.2.2.2

[root@svr7 named]# systemctl restart named

[root@svr7 named]# nslookup www.bj.tedu.cn 192.168.4.7

Server: 192.168.4.7

Address: 192.168.4.7#53

Non-authoritative answer: #非权威解答

Name: www.bj.tedu.cn

Address: 11.12.13.14

递归解析： 首选DNS服务器，跑到相应其他DNS服务器上，询问最终将结果带回来过程（客户端与首选DNS服务器交互）

迭代查询： 首选DNS服务器 与 其他DNS服务器交互

• 递归查询是默认开启的

– 也可以设置 recursion yes; 来明确启用

• 若要禁止递归

– 需要设置 recursion no;

缓存DNS

作用：加速解析过程，让客户端最快得到结果

• 方式1:全局转发

– 将请求转发给指定的公共DNS(其他缓存DNS),请求递归服务

• 方式2:根域迭代

– 依次向根、一级、二级......域的DNS服务器迭代

思路：真机作为缓存DNS服务器，虚拟机A作为客户端，真正的DNS为172.40.1.10

1.查看真机DNS服务器地址

[root@room9pc01 ~]# cat /etc/resolv.conf

nameserver 172.40.1.10

2.真机搭建Yum仓库

[root@room9pc01 ~]# mount /iso/CentOS-7-x86\_64-DVD-1708.iso /dvd

mount: /dev/loop2 写保护，将以只读方式挂载

[root@room9pc01 ~]# ls /dvd

[root@room9pc01 ~]# vim /etc/yum.repos.d/nsd.repo

[CentOS]

name=CentOS 7.4

baseurl=file:///dvd

enabled=1

gpgcheck=0

[root@room9pc01 ~]# yum repolist

[root@room9pc01 ~]# yum -y install bind bind-chroot

[root@room9pc01 ~]# vim /etc/named.conf

options {

directory "/var/named";

forwarders { 172.40.1.10; };

};

[root@room9pc01 ~]# systemctl restart named

客户端：虚拟机A

[root@svr7 /]# nslookup www.360.com 192.168.4.254

# DAY3

检查两台虚拟机的Yum仓库

[root@svr7 ~]# yum clean all #清空缓存

[root@svr7 ~]# yum repolist #查看仓库信息

Split分离解析

什么是分离解析

• 当收到客户机的DNS查询请求的时候

– 能够区分客户机的来源地址

– 为不同类别的客户机提供不同的解析结果(IP地址)

– 当不同类别的客户机请求解析同一个域名时，得到的解析结果不同

– 意义：让客户端访问网络中最近的服务器

BIND的view视图

• 根据源地址集合将客户机分类

– 不同客户机获得不同结果(待遇有差别)

– 注意：客户机分类得当（所有的客户端都要找到对应的分类）

– 注意：由上到下匹配，匹配即停止

– 注意：所有的zone都必须在view字段里面

view "nsd" {

match-clients { 192.168.4.207; } #匹配客户端的地址

zone "tedu.cn" {

...... 地址库1;

}; };

view "abc" {

match-clients { any; }

zone "tedu.cn" {

...... 地址库2;

}; };

环境及需求

– 权威DNS:svr7.tedu.cn 192.168.4.7

– 负责区域:tedu.cn

– A记录分离解析 —— 以 www.tedu.cn 为例

客户机来自 解析结果

192.168.4.207---------》 192.168.4.100

其他地址 ---------》 1.2.3.4

虚拟机A：

1.修改配置文件/etc/named.conf

view "nsd" {

match-clients { 192.168.4.207; };

zone "tedu.cn" {

type master;

file "tedu.cn.nsd";

};

};

view "abc" {

match-clients { any; };

zone "tedu.cn" {

type master;

file "tedu.cn.abc";

};

};

2.建立地址库文件

[root@svr7 /]# tail -3 /var/named/tedu.cn.nsd

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.100

[root@svr7 /]# tail -3 /var/named/tedu.cn.abc

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 1.2.3.4

3.重起named服务

4.在虚拟机A与虚拟机B，分别测试解析

##########################################################################

options {

directory "/var/named";

};

acl myip { 192.168.4.207; 192.168.4.10;

192.168.4.1; 192.168.4.123; };

view "nsd" {

match-clients { myip; };

zone "tedu.cn" {

type master;

file "tedu.cn.nsd";

};

};

view "abc" {

match-clients { any; };

zone "tedu.cn" {

type master;

file "tedu.cn.abc";

};

};

## 配置转发dns服务器

vim /etc/named.conf

options{

forwarders { 176.19.0.26; };

};