**3\_Services03管理NDS服务基础**

**一 DNS 服务基础**

**1.1 DNS解析的作用**

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]

**1.2 域名结构:树型结构**

1.2.1所有的域名都必须以点结尾

[www.qq.com](http://www.qq.com) ---> [www.qq.com](http://www.qq.com). 浏览器自动补齐最后的点

最后一个点称为**根域名**,对其进行解析的服务器称为根域名服务器.

1.2.2 DNS服务器分级

一级DNS服务器

二级DNS服务器

三级DNS服务器

1.2.3 域名分级

一级域名[国家域名]: .cn .us .kr .tw .hk .jp .com[代表全球的组织]...

二级域名[商业域名]: .com.cn .tedu.cn .net.cn .org.cn ...

三级域名[示例]: nb.com.cn dc.com.cn tc.com.cn ...

1.2.4 www:主机头部

1.2.5 Full Qualified Domain Name[FQDN]完全合格的域名=主机头部+注册的域名

1.2.6 IANA:互联数字分配机构,整个域名系统的最高权威机构

CNNIC:中国互联网信息中心

**二 构建基本DNS服务器**

**2.1 BIND[Berkeley Internet Name Daemon]**

yum -y install bind-chroot #提供虚拟根支持;牢笼政策,监控bind

yum -y install bind #域名服务包

rpm -qa bind\* #查询

**2.2 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 #决定本机负责解析的域名

地址库文件存放路径:/var/named/ #域名的解析结果[域名-IP对照文件]

**2.3 主配置文件修改**

cp **-p** /etc/named.conf /etc/named.bak #备份主配置文件named.conf

vim /etc/named.conf #修改主配置文件

**删除多余项目并修改,最后代码:**

options {

directory "/var/named"; #指定地址库文件位置

};

zone "**tedu.cn**" IN { #修改 . 为tedu.cn

type **master**; #修改hint为master[解析以tedu.cn结尾的

域名的主服务器,若为slave表示副服务器]

file "**tedu.cn.zone**";

#修改named.ca为tedu.cn.zone,设置地址库文件名,存放域名-IP解析关系文件.

};

[hint为根域名服务器使用]

**2.4 建立地址库文件tedu.cn.zone**

cd /var/named

错误操作:

cp named.localhost tedu.cn.zone

vim tedu.cn.zone

ls -l tedu.cn.zone,查看权限，负责运行此文件的用户为named,无r权限

**正确操作:**

cp **-p** named.localhost tedu.cn.zone

#-p保持named对新生成的文件的权限不变

ls -l tedu.cn.zone #查看新生成文件的权限

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

#named组有r权限

修改tedu.cn.zone

原代码:

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS @ #NS表示nameserver

A 127.0.0.1 #A表示address

AAAA ::1 #AAAA表示ipv6的地址解析

最后三行修改后[所有域名必须以点结尾]:

tedu.cn. NS svr7.tedu.cn. #设置虚拟机A为NS服务器

svr7.tedu.cn. A 192.168.4.7 #设置本机的地址

www.tedu.cn. A 1.1.1.1 #1.1.1.1为暂时随便写

ftp.tedu.cn. A 2.2.2.2 #2.2.2.2为暂时随便写

***当遗忘点时,系统自动补齐点,此时最后书写如下:***

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 1.1.1.1 #1.1.1.1为暂时随便写

ftp A 2.2.2.2 #2.2.2.2为暂时随便写

systemctl restart named #重启服务

**2.5 客户机设置及验证**

**echo nameserver 192.168.4.7 > /etc/resolv.conf**

#为虚拟机B指定DNS服务器

nslookup svr7.tedu.cn

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: svr7.tedu.cn

Address: 192.168.4.7

nslookup [www.tedu.cn](http://www.tedu.cn)

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: www.tedu.cn

Address: 1.1.1.1

**三 构建多域名DNS服务器**

解析qq.com域名

**3.1 修改主配置文件**vim /etc/named.conf

添加以下代码

**zone "qq.com" IN {**

**type master;**

**file "qq.com.zone";**

**};**

**3.2 创建地址库文件**qq.com.zone

cd /var/named

cp **-p** tedu.cn.zone qq.com.zone **[复制后先查看文件的组权限]**

vim qq.com.zone #修改qq.come.zone,添加qq.com的参数

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

**qq.com. NS svr7**

**svr7 A 192.168.4.7**

**www A 1.1.1.1**

**ftp A 2.2.2.2**

systemctl restart named #重启服务

客户机验证

[root@pc207 ~]# nslookup svr7.qq.com

Server: 192.168.4.7 #NS服务器IP

Address: 192.168.4.7#53 #NS服务器地址及端口

Name: svr7.qq.com #查询的域名

Address: 192.168.4.7 #查询的域名的IP

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

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: www.qq.com

Address: 1.1.1.1

[root@pc207 ~]# nslookup ftp.qq.com

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: ftp.qq.com

Address: 2.2.2.2

**四 特殊解析记录**

**4.1 基于DNS负载均衡**

服务器端修改地址库文件tedu.cn.zone

cd /var/named

vim tedu.cn.zone

tedu.cn. NS svr7

svr7 A 192.168.4.7

**www A 192.168.4.10 #添加此3行**

**www A 192.168.4.20**

**www A 192.168.4.30**

ftp A 2.2.2.2 #2.2.2.2为暂时随便写

systemctl restart named #重启服务

客服的访问www.tedu.cn时,三个IP随机分配.

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

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: www.tedu.cn

Address: 192.168.4.30

Name: www.tedu.cn

Address: 192.168.4.10

Name: www.tedu.cn

Address: 192.168.4.20

**4.2 泛域名解析**

服务器端修改地址库文件tedu.cn.zone

vim /var/named/tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

tedu.cn. NS svr7.tedu.cn.

svr7.tedu.cn. A 192.168.4.7

[www.tedu.cn.](http://www.tedu.cn.) A 1.1.1.1

ftp.tedu.cn. A 2.2.2.2

**\* A 1.2.3.4 #添加此行**

systemctl restart named #重启服务

客户机验证

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

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: haha.tedu.cn

Address: 1.2.3.4

**4.3 解析记录的别名**

服务器修改文件tedu.cn.zone

vim /var/named/tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

tedu.cn. NS svr7.tedu.cn.

svr7.tedu.cn. A 192.168.4.7

[www.tedu.cn.](http://www.tedu.cn.) A 1.1.1.1

ftp.tedu.cn. A 2.2.2.2

\* A 1.2.3.4

**mail.tedu.cn. CNAME ftp.tedu.cn.**

#同mail.tedu.cn. A 2.2.2.2[CNAME方法更安全]

systemctl restart named #重启服务

客户机验证

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

Server: 192.168.4.7

Address: 192.168.4.7#53

mail.tedu.cn canonical name = ftp.tedu.cn.

#同被收录的域名ftp.tedu.cn.

Name: ftp.tedu.cn

Address: 2.2.2.2

**4.4 有规律的泛域名解析**

pc1 ---> 192.168.10.1

Pc2 ---> 192.168.10.2

Pc3 ---> 192.168.10.3

......

Pc50 ---> 192.168.10.50

**内置函数:$GENERATE** 制造连续范围的数字

$GENERATE 1-50 pc$.tedu.cn A 192.168.10.$

4.4.1 服务器端修改地址库文件tedu.cn.zone

vim /var/named/tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

tedu.cn. NS svr7.tedu.cn.

svr7.tedu.cn. A 192.168.4.7

www.tedu.cn. A 192.168.4.10

www.tedu.cn. A 192.168.4.20

www.tedu.cn. A 192.168.4.30

ftp.tedu.cn. A 2.2.2.2

\* A 1.2.3.4

mail.tedu.cn. CNAME ftp.tedu.cn.

**$GENERATE 1-50 pc$.tedu.cn. A 192.168.10.$ #添加此行**

[root@svr7 ~]# systemctl restart named #重启服务

4.4.2客服机验证

[root@pc207 ~]# nslookup pc1.tedu.cn

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: pc1.tedu.cn

Address: 192.168.10.1

[root@pc207 ~]# nslookup pc10.tedu.cn

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: pc10.tedu.cn

Address: 192.168.10.10

[root@pc207 ~]# nslookup pc30.tedu.cn

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: pc30.tedu.cn

Address: 192.168.10.30

[root@pc207 ~]# nslookup pc51.tedu.cn

Server: 192.168.4.7

Address: 192.168.4.7#53

Name: pc51.tedu.cn

Address: 1.2.3.4

**Q:DNS资源解析记录有那些?**

**正向解析记录(A记录) DNS声明记录(NS记录) 解析记录的别名(CNAME记录)**

**五 DNS的子域授权**

父域:以相同域名结尾的,较短的 如qq.com 由虚拟机A进行解析 svr7.tedu.cn

子域:以相同域名结尾的,较长的 如bj.qq.com 由虚拟机B进行解析 pc207.tedu.cn

**5.1 在虚拟机B上安装bind bind-chroot**

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

**5.2 在虚拟机B备份主配置文件并修改**

[root@pc207 etc]# cd /etc

[root@pc207 etc]# cp **-p** named.conf named.bak

#备份主配置文件

vim named.conf

options {

directory "/var/named";

};

zone "**bj.qq.com**" IN {

type **master**;

file "**bj.qq.com.zone**";

};

**5.3 在虚拟机B修改地址库文件**

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

[root@pc207 named]# cp **-p** named.localhost bj.qq.com.zone

vim bj.qq.com.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

**bj.qq.com. NS pc207**

**pc207 A 192.168.4.207**

**www A 50.60.70.80**

[root@pc207 named]# systemctl restart named

#重启服务

虚拟机B测试

nslookup [www.bj.qq.com](http://www.bj.qq.com) 192.168.4.207

nslookup [www.qq.com](http://www.qq.com) 192.168.4.7

**5.4 子域授权**

让父域的DNS服务器知晓子域DNS服务器

让父域的DNS服务器可以解析子域的域名

虚拟机A

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

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

qq.com. NS svr7

**bj.qq.com. NS pc207 #必须在此处添加此行**

svr7 A 192.168.4.7

**pc207 A 192.168.4.207 #必须在此处添加此行**

www A 3.3.3.3

ftp A 2.2.2.2

[root@svr7 ~]# systemctl restart named #重启服务

[root@pc207 /]# nslookup www.bj.qq.com 192.168.4.7 #测试

Server: 192.168.4.7

Address: 192.168.4.7#53

Non-authoritative answer: #非权威解答

Name: www.bj.qq.com

Address: 50.60.70.80

**5.5 递归解析**

由客户端发出请求,由首选DNS服务器接受请求,将解析结果带回来的过程.

关闭递归解析功能

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

options {

directory "/var/named";

**recursion no**; **#添加此行,禁用递归解析**

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

**5.6 迭代解析**

首选DNS服务器与其他DNS服务器交换的过程

**5.7 专业测试DNS工具:dig**

[root@svr7 /]#dig [www.bj.qq.com](http://www.bj.qq.com)

QUESTION SECTION:

;www.bj.qq.com. IN A #查询的域名

;; AUTHORITY SECTION:

bj.qq.com. 86400 IN NS pc207.qq.com.

#父域为bj.qq.com.,NS为pc207.qq.com.

;; ADDITIONAL SECTION:

pc207.qq.com. 86400 IN A 192.168.4.207

#NS服务器的IP地址

**六 主机名映射记录文件:/etc/host**

在没有DNS服务器的前提下,提供域名解析[但只能为本机做域名解析]

ping 一个不存在的域名

[root@svr7 etc]# ping www.nb.com

ping: www.nb.com: 未知的名称或服务

在/etc/hosts下为此域名添加IP映射地址

[root@svr7 etc]# **vim /etc/hosts**

**192.168.4.110 [www.nb.com](http://www.nb.com) #添加此行**

测试

[root@svr7 ~]# ping www.nb.com

**域名解析过程中最高优先级为/etc/host,匹配即停止,然后读**

**取/etc/resolv.conf 中的nameserver的数据**

**七 缓存DNS服务器**

作用:缓存解析结果,加快解析过程

缺点:缓存存于内存中,断电后需要重新缓存

三个角色:客户端 缓存DNS服务器 真DNS服务器

虚拟机A:真DNS服务器

虚拟机A:缓存DNS服务器

虚拟机c:客户端

**7.1 虚拟机C**

配置IP为192.168.4.10/24,主机名为svr10.tedu.cn

**7.2 虚拟机B:缓存DNS服务**

修改named.conf主配置文件

[root@pc207 ~]# vim /etc/named.conf

options {

directory "/var/named";

**forwarders { 192.168.4.7; }; #添加此行**

};

zone "bj.qq.com" IN {

type master;

file "bj.qq.com.zone";

};

[root@pc207 ~]# systemctl restart named

虚拟机C上测试

[root@svr10 ~]# nslookup www.tedu.cn 192.168.4.207

Server: 192.168.4.207

Address: 192.168.4.207#53

Non-authoritative answer:

Name: www.tedu.cn

Address: 192.168.4.10

Name: www.tedu.cn

Address: 192.168.4.30

Name: www.tedu.cn

Address: 192.168.4.20

**八 wc命令**

[root@svr7 etc]# wc /etc/passwd

22 40 1027 /etc/passwd #行数,?,文件大小

[root@svr7 etc]# wc -l /etc/passwd

22 /etc/passwd #显示行数

[root@svr7 etc]# wc -l /etc/hosts

3 /etc/hosts #显示行数

[root@svr7 etc]# wc -l /etc/passwd /etc/hosts

22 /etc/passwd #显示passwd行数

3 /etc/hosts #显示hosts行数

25 总用量 #显示综合行数

[root@svr7 etc]# find /etc/ -name "\*tab" | wc -l

9 #显示/etc下以tab结尾的文件数

[root@svr7 etc]# find /etc/ -name "\*conf" | wc -l

113 #显示/etc下以conf结尾的文件数