DNS服务基础

• DNS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

DNS服务器分类：

根域名服务器 一级DNS服务器 二级DNS服务器 三级DNS服务器

DNS的域名的分布式结构：树型结构

1）所有的域名都必须以点作为结尾,所有的浏览器自动补全最后的点

www.qq.com. www.baidu.com.

根域名 ： . 点

一级域名： .cn .us .tw .hk .jp .kr .....

二级域名： .com.cn .net.cn .org.cn .tedu.cn .....

三级域名： dc.com.cn tc.com.cn dcc.com.cn tcc.com.cn

完整的主机名（FQDN）：主机头部+合格的域名

• Full Qualified Domain Name,完全合格主机名

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

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(牢笼政策)

– 运行时的虚拟根环境:/var/named/chroot/

– 系统服务:named

– 默认端口:TCP/UDP 53

• 主配置文件:/etc/named.conf #设置本DNS服务器负责解析的域名 tedu.cn

• 地址库文件:/var/named/ #完整的主机名与IP地址的对应关系

构建DNS服务器

虚拟机A：

1.安装软件包

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

2.修改主配置文件

[root@svr7 ~]# cp /etc/named.conf /etc/named.bak

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

options {

directory "/var/named"; #设置地址库文件存放路径

};

zone "tedu.cn" IN { #设置负责解析的域名

type master; #本服务器为权威DNS

file "tedu.cn.zone"; #设置地址库文件名

};

3.建立新的地址库文件tedu.cn.zone

保证named用户对该文件具备读取权限

所有的域名都必须以点结尾

如果没有以点作为结尾，那么默认补全本地址库负责的域名

• NS,域名服务器(Name Server)声明记录

• A,地址(Address)记录,仅用于正向解析区域

]# cd /var/named/

]# cp -p named.localhost tedu.cn.zone #-p保持权限不变

]# ls -l tedu.cn.zone

]# vim tedu.cn.zone

tedu.cn. NS svr7 #声明负责域名解析的DNS服务器

svr7 A 192.168.4.7 #声明DNS服务器具体的IP地址

www A 1.1.1.1

ftp A 2.2.2.2

]# systemctl restart named

虚拟机B：客户端

1.指定DNS服务器地址，测试解析

]# echo nameserver 192.168.4.7 > /etc/resolv.conf

]# nslookup www.tedu.cn

]# nslookup ftp.tedu.cn

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

多区域的DNS解析

1.修改主配置文件，添加zone的配置

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

.......

zone "qq.com" IN { #负责解析qq.com域名

type master; #权威主服务器

file "qq.com.zone"; #地址库文件名

};

2.建立新的地址库文件

]# cd /var/named/

]# cp -p tedu.cn.zone qq.com.zone

]# vim 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

[root@svr7 named]# !sys

systemctl restart named

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

主机名映射文件:/etc/hosts #直接起到DNS域名解析的作用

只能为本机提供解析

/etc/hosts最高优先级

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

.......

192.168.4.110 www.360.com

[root@svr7 /]# ping www.360.com #测试是否能够解析

Nginx的Web服务器，虚拟Web主机 基于域名 基于端口 基于IP地址

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

特殊解析记录

1.DNS轮询，基于DNS的站点负载均衡

– 一个域名 ---> 多个不同IP地址

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

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.1

www A 192.168.4.2

www A 192.168.4.3

ftp A 2.2.2.2

[root@svr7 /]# !sys

systemctl restart named

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

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

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

2.泛域名解析

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

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.1

www A 192.168.4.2

www A 192.168.4.3

ftp A 2.2.2.2

\* A 1.2.3.4

[root@svr7 /]# systemctl restart named

虚拟机B：测试验证

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

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

3.有规律的泛域名解析

pc1.tedu.cn -----> 192.168.10.1

pc2.tedu.cn -----> 192.168.10.2

pc3.tedu.cn -----> 192.168.10.3

........

pc30.tedu.cn -----> 192.168.10.30

内置函数: $GENERATE 制造连续的数字

$GENERATE 起始点-结束点 # $符号代表制造出的连续数字

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

$GENERATE 1-30 pc$ A 192.168.10.$

[root@svr7 /]# !sys

systemctl restart named

虚拟机B：测试验证

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

[root@pc207 ~]# nslookup pc20.tedu.cn

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

4.解析记录别名

虚拟机A：

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

vip CNAME ftp #vip的解析结果与ftp一致

[root@svr7 /]# !sys

systemctl restart named

虚拟机B：测试验证

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

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

DNS的资源解析记录那些？

NS解析记录：DNS服务器声明记录

A解析记录：正向地址解析记录

CNAME解析记录：解析记录的别名

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

真机运行clone-vm7快速产生一台虚拟机

虚拟机C

1.配置eth0的IP地址:192.168.4.10/24

2.配置主机名:svr10.tedu.cn

3.配置Yum仓库,以真机提供FTP作为服务端

4.安装httpd软件包进行测试

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

DNS子域授权

父域：www.qq.com www.tedu.cn

子域：www.bj.qq.com www.bj.tedu.cn

qq.com域名有虚拟机A负责解析

bj.qq.com域名有虚拟机B负责解析

递归解析：客户端发送请求给主DNS服务器，主DNS服务器与其他DNS服务器交互最终，将解析结果带回来的过程

迭代解析：主DNS服务器与其他DNS服务器交互

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

DNS主/从结构:备份 解决单点故障

以qq.com域名为例

虚拟机A为主DNS服务器（首选DNS服务器）

虚拟机B为从DNS服务器（备用DNS服务器）

虚拟机A：构建主DNS服务器

1.修改主配置文件，允许虚拟机B进行同步数据

[root@svr7 /]# man named.conf #查看man帮助信息

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

options {

directory "/var/named";

allow-transfer { 192.168.4.207; }; #允许从服务器同步数据

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

2.在地址库文件中，声明从服务器的IP地址

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

qq.com. NS svr7 #声明DNS服务器

qq.com. NS pc207 #声明DNS服务器

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 3.3.3.10

ftp A 4.4.4.4

3.重起named服务

[root@svr7 /]# systemctl restart named

虚拟机B构建为从DNS服务器（备用DNS服务器）

备用DNS服务器地址库文件不需要自己创建，地址库文件是从主DNS服务器进行同步

1.安装软件包bind bind-chroot

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

2.修改主配置文件

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

options {

directory "/var/named";

};

zone "qq.com" IN {

type slave; #类型为从服务器

file "slaves/qq.com.slave";

masters { 192.168.4.7; }; #指定主服务器位置

};

#将备份数据起名为qq.com.slave，存放在/var/named/slaves

#slaves目录默认named用户对其拥有rwx权限

[root@pc207 /]# ls /var/named/slaves/

[root@pc207 /]# systemctl restart named

[root@pc207 /]# ls /var/named/slaves/ #验证同步数据

qq.com.slave

[root@pc207 /]#

虚拟机C：客户端验证

]# echo nameserver 192.168.4.7 > /etc/resolv.conf

]# echo nameserver 192.168.4.207 >> /etc/resolv.conf

]# cat /etc/resolv.conf

nameserver 192.168.4.7 #首选DNS服务器

nameserver 192.168.4.207 #备用DNS服务器

]# nslookup www.qq.com

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

数据更新,一定要在主DNS服务器完成

虚拟机A：

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

2019082001 ; serial #数据的版本号格式：年月日次数 10位组成

1D ; refresh #主与从同步数据时间

1H ; retry #失连后同步数据的时间

1W ; expire #完全失效时间

3H ) ; minimum #无效记录 记忆时间

每次数据更新，数据的版本号必须要变大

数据的版本号：主与从数据同步时，唯一标准

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