8-20

1. DNS服务基础

[root@svr7 ~]# yum -y install bind bind-chroot #专门实现DNS软件包

bind : 主程序包 域名服务包

bind-chroot : 提供虚拟根支持 (牢笼政策) (待在内存,不提供解释域名工作)

-运行时的虚拟根环境 : /var/named/chroot (囚禁位置)

所有域名都必须以” . “ 点结尾

1)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 (需熟练掌握)

-反向解释 : 根据IP地址查找对应的注册域名,不常用 (默认情况下不启用,需要手动配置)

2)DNS分类: (4类)

根域名服务器 一级DNS服务器 : 专门维护一级域名DNS服务器 (二,三级以此类推)

3)DNS的域名的分布式结构 : 树形结构

1.所有的域名都必须以**点.**作为结尾

完整域名 : [www.baidu.com.](http://www.baidu,com.) (最后带点,一般浏览器自动补全最后的 “点”)

“点” 为 根域名

一级域名 : .cn .us .tw .hk ......

二级域名 : .com.cn (商业组织常用) .net.cn (运营商) .org.cn (募捐网站)

.tedu.cn (教育机构)

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

完整主机名 (FQDN) : 主机头部(自定义) + 合格的域名(需购买)

(代表完全合格的主机名)

IANA 互联网数字分配机构 (全球顶级域名系统最高权威机构)

4)BIND服务端程序 :

-运行时的虚拟根环境 : /var/named/chroot (囚禁位置)

-系统服务 : named

-默认端口 : TCP/UDP 53

*主配置文件 : /etc/name.conf #设置本DNS服务器负责解析的域名*

*地址库文件 : /var/named/ #完整的主机名与IP地址的对应关系*

(前面是ip,后面是域名)

1. 构建DNS服务器
2. 安装软件包 bind bind-chroot
3. *修改主配置文件* ( 不一定要加点 )

因该文件较脆弱,空格,;,等格式不对----->服务起不来 -----> 备份

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

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

options {

directory "/var/named";

};

zone "tedu.cn" IN { ---------> #设置负责解析的域名

type master; -------->#本服务器为权威DNS master :主DNS sleve :

file "named.ca"; --------> #设置地址库文件名

}; |

|

地址库文件默认是不存在的,需要到/var/named/ 下创建目录 |named.ca 需要完全对应

1. 服务端Server

建立新的地址库文件tedu.cn.zone ( 地址库文件需加点 )

保证named用户对该文件具备读取权限

所有域名都必须以” . “ 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

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

[root@svr7 named]# cp -p named.localhost tedu.cn.zone #-p 保持权限不变

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

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

(不加-p 会变成root )

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

[root@svr7 named]# systemctl restart named

A : 地址记录, 仅用于正向解析区域

NS : 域名服务器(声明)记录 声明DNS服务器具体的IP地址

AAAA : ipv6

tedu.cn. NS svr7.tedu.cn. <----------少最后一个点会补全 tedu

(区域) (负责人) (尽量写DNS主机名,上下一致)

Svr7.tedu.cn. A 192.168.4.7

(负责人) (IP地址)

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

ftp.tedu.cn. A 2.2.2.2

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

ftp A 2.2.2.2

www A 1.1.1.1

4.客户端desktop

1.指定DNS服务器地址,测试解析

[root@pa207 ~]# ls /etc/resolv.conf

[root@pa207 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@pa207 ~]# nslookup [www.tedu.cn](http://www.tedu.cn)

Host [www.tedu.cn](http://www.qq.com)

Dig+域名 #可以查询到域名的反向解释

6)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

};

1. 建立新的地址库文件

[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]# !sys

systemctl restart named

qq.com. NS svr7

svr7 A 192.168.4.7

ftp A 3.3.3.3

www A 4.4.4.4

7)主机名映射文件:/etc/hosts #直接起到域名解析的作用

缺点 : 只能为本机提供解析

nslookup 不读 /etc/hosts 这文件

ping 不通是正常的 但可以解析

/etc/hosts 具有最高优先级,且优于DNS服务器

(即解析机器时,是第一个访问,匹配即停止)

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

192.168.4.110 www.360.com

[root@svr7 ~]# ping [www.360.com](http://www.360.com) #测试是否能够解析

PING www.360.com (192.168.4.110) 56(84) bytes of data.

From svr7.tedu.cn (192.168.4.7) icmp\_seq=1 Destination Host Unreachable

网络不可达

1. 特殊解析记录
2. DNS轮询,基于DNS的站点负载均衡

-一个域名 ---> 对应 多个不用IP地址

2.泛域名解析

-直接以\* 条目匹配

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

tedu.cn. NS svr7

svr7 A 192.168.4.7

ftp A 2.2.2.2

www A 1.1.1.1

www A 192.168.4.8

www A 192.168.4.9

www A 192.168.4.10

\* A 2.3.4.5

[root@svr7 ~]# !sys

[root@pa207 ~]# nslookup wdass.tedu.cn

本机没指定前,无法解析域名,需向本机声明

echo nameserver 192.168.4.7 > /etc/resolv.conf

3.有规律的泛域名解析

内置函数 : $GENERATE 制造连续的数字

内置:不需人去操作,

$GENERATE 起始点-结束点

$GENERATE 1-30 pc$.tedu.cn A 192.168.10.$

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

$GENERATE 1-30 PC$ A 192.168.10.$

[root@svr7 ~]# !sys

测试验证:

[root@pa207 ~]# nslookup pc31.tedu.cn --> 2.3.4.5

[root@pa207 ~]# nslookup pc3.tedu.cn --> 192.168.10.3

4.解析记录别名 CNAME

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

vip CNAME ftp #vip解析结果与ftp一致

[root@svr7 ~]# !sys

测试验证:

[root@pa207 ~]# nslookup vip.tedu.cn

5.DNS资源解析记录有哪些?

Web资源有那些------>页面有多少个

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

DNS 子域授权(理论)

父域 : [www.qq.com](http://www.qq.com) ( 较短 )

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

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 (根域DNS服务器不支持递归,即会帮忙分析,不会帮忙跑腿)

也可关闭 : recursion no; (禁用递归)

迭代解析 : 主DNS服务器与其他DNS服务器交互

一次递归,多次迭代

DNS 主从结构 备份

虚拟机A构建为从DNS服务器 (主要DNS服务器)

虚拟机B构建为从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

2.修改配置文件

[root@pa207 ~]# 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

#slave目录默认为named用户对其拥有rwx权限

file “slaves/qq.com.slave”; 相对于 /var/named/

[root@pa207 ~]# ls /var/named/slaves/

[root@pa207 ~]# systemctl restart named

[root@pa207 ~]# ls /var/named/slaves/ #验证同步数据

qq.com.slave (从DNS服务器是看不到的 , 只有登录到主 192.168.4.7 去看)

虚拟机C : 客户端验证

1.配置eth0的IP地址:192.168.4.10/24

2.主机名:svr10.tedu.cn

3.搭建yum

4.装包:httpd

[root@svr10 ~]# echo nameserver 192.168.4.7 > /etc/resolv.conf

[root@svr10 ~]# echo nameserver 192.168.4.207 >> /etc/resolv.conf

[root@svr10 ~]# cat /etc/resolv.conf

nameserver 192.168.4.7 #主DNS服务器

nameserver 192.168.4.207　　　　＃备用DNS服务器

数据更新:一定要在主DNS服务器进行

每次数据更新,数据版本号必须变大 ,主不能往小的改,否则从会崩溃

数据版本号 : 主与从数据同步时唯一标准

需重启,同步更新数据