学习资料链接地址：

正式课程笔记：码云

https://gitee.com/niubenlinux/nsd2011

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

1. **两台虚拟机**进行环境准备

1.SELinux设置宽松模式

[root@svr7 ~]# setenforce 0 #设置当前系统SELinux为宽松

[root@svr7 ~]# getenforce #查看当前系统SELinux模式

Permissive

[root@svr7 ~]# vim /etc/selinux/config

SELINUX=permissive

2.防火墙设置

]# systemctl stop firewalld

1. DNS服务

为什么需要DNS系统

www.baidu.com 与 119.75.217.56，哪个更好记？

互联网中的114查号台/导航员

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

域名系统: 所有的域名都必须要以点作为结尾，树型结构

www.qq.com www.qq.com.

根域名 :  **.**

一级域名： .cn .us .tw .hk .jp .kr ……….

二级域名: .com.cn .org.cn .net.cn ………

三级域名： haha.com.cn xixi.com.cn .nb.com.cn …..

FQDN（完全合格的主机名）：站点名+注册的域名

* BIND（Berkeley Internet Name Daemon）
  + 伯克利 Internet 域名服务
  + 官方站点：<https://www.isc.org/>
* BIND服务器端程序
  + 主要执行程序：/usr/sbin/named
  + 系统服务：named
  + DNS协议默认端口：TCP/UDP **53**
  + 运行时的虚拟根环境：/var/named/chroot/
* 主配置文件：/etc/named.conf #设置负责解析的域名
* 地址库文件：/var/named/ #完全合格的主机名与IP地址对应关系

虚拟机A：构建DNS服务器

1.安装软件包

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

bind（主程序）

bind-chroot（提供牢笼政策）

2.修改主配置文件

[root@svr7 ~]# cp /etc/named.conf /root #备份数据

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

options {

directory "/var/named"; #定义地址库文件存放路径

};

zone "**tedu.cn**" IN { #定义负责的解析tedu.cn域名

type **master**; #权威主DNS服务器

file "**tedu.cn.zone**"; #地址库文件名称

};

3.建立地址库文件

保证named用户对地址库文件有读取权限

所有的域名都要以点作为结尾

如果没有以点作为结尾，那么默认**补全**本地库文件负责的域名

]# cd /var/named/

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

]# ls -l tedu.cn.zone

]# vim tedu.cn.zone

……此处省略一万字

tedu.cn**.** NS svr7 #声明DNS服务器为svr7

svr7 A 192.168.4.7 #svr7解析结果为192.168.4.7

www A 1.1.1.1

ftp A 2.2.2.2

[root@svr7 named]# systemctl restart named

虚拟机B：测试DNS服务器

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

]# cat /etc/resolv.conf

]# nslookup www.tedu.cn

]# nslookup ftp.tedu.cn

1. 多区域的DNS服务器

虚拟机A：

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

options {

directory "/var/named";

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

**zone "lol.com" IN {**

**type master;**

**file "lol.com.zone";**

**};**

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

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

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

……此处省略一万字

lol.com**.** NS svr7

svr7 A 192.168.4.7

www A 4.4.4.4

vip A 5.5.5.5

[root@svr7 named]# systemctl restart named

虚拟机B

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

六、特殊解析

* **DNS的轮询(负载均衡)**

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

……此处省略一万字

tedu.cn. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.20

www A 192.168.4.21

www A 192.168.4.22

ftp A 2.2.2.2

[root@svr7 /]# systemctl restart named

* **DNS的泛域名解析**

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

……此处省略一万字

tedu.cn**.** NS svr7

svr7 A 192.168.4.7

www A 192.168.4.20

ftp A 2.2.2.2

\* A 6.6.6.6

tedu.cn**.** A 7.7.7.7

[root@svr7 /]# systemctl restart named

虚拟机B测试：

[root@pc207 /]# nslookup wwwwww.tedu.cn

[root@pc207 /]# nslookup tedu.cn

* **DNS的解析记录的别名**

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

……此处省略一万字

tedu.cn**.**  NS svr7

svr7 A 192.168.4.7

www A 192.168.4.20

**ftp A 2.2.2.2**

\* A 6.6.6.6

tedu.cn**.** A 7.7.7.7

**vip CNAME ftp**  #vip解析结果与ftp解析结果一致

[root@svr7 /]# systemctl restart named

虚拟机B：测试

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

DNS服务器资源解析记录的类型：

NS:DNS服务器声明记录

A：正向解析记录

CNAME：解析记录的别名

七、递归查询（递归解析）与迭代查询 （迭代解析）

递归查询：客户端发送请求给首选DNS服务器，首选DNS服务器与其他的DNS服务器交互，最终将解析结果带回来过程

迭代查询: 客户端发送请求给首选DNS服务器，首选DNS服务器告知下一个DNS服务器地址

虚拟机B：构建DNS服务器负责bj.tedu.cn

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

options {

directory "/var/named";

};

zone "bj.tedu.cn" IN {

type master;

file "bj.tedu.cn.zone";

};

]# cd /var/named/

]# cp -p named.localhost bj.tedu.cn.zone

]# vim bj.tedu.cn.zone

……此处省略一万字

bj.tedu.cn. NS pc207

pc207 A 192.168.4.207

www A 9.9.9.9

]# systemctl restart named

虚拟机A:子域授权

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

tedu.cn. NS svr7

bj.tedu.cn. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 192.168.4.20

ftp A 2.2.2.2

\* A 4.4.4.4

tedu.cn. A 5.5.5.5

vip CNAME ftp

[root@svr7 /]# systemctl restart named

虚拟机B：测试

[root@pc207 /]# 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: 9.9.9.9

虚拟机A:禁止递归查询

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

options {

directory "/var/named";

recursion no; #禁止递归查询

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "lol.com" IN {

type master;

file "lol.com.zone";

};

[root@svr7 /]# systemctl restart named

[root@pc207 /]# dig @192.168.4.7 www.bj.tedu.cn #专业域名解析的工具

bj.tedu.cn. 86400 IN NS pc207.tedu.cn.

;; ADDITIONAL SECTION:

pc207.tedu.cn. 86400 IN A 192.168.4.207

八、DNS主从架构

作用：提高可靠性，从DNS服务器备份主DNS服务器的数据

虚拟机A：主DNS服务器，以lol.com域名

虚拟机B：从DNS服务器，以lol.com域名

虚拟机A：主DNS服务器

1. 授权从DNS服务器

[root@svr7 /]# man named.conf #参考man帮助

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

options {

directory "/var/named";

allow-transfer { 192.168.4.207; }; #允许谁进行传输数据

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "lol.com" IN {

type master;

file "lol.com.zone";

};

1. 声明从DNS服务器

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

……此处省略一万字

lol.com. NS svr7

lol.com. NS pc207 #声明从DNS服务器

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 4.4.4.4

[root@svr7 /]# systemctl restart named

虚拟机B：从DNS服务器

1.安装软件包

[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 "lol.com" IN {

type **slave**; #类型为从服务器

file "/var/named/slaves/lol.com.slave"; #确保named用户有读写执行权限

masters { 192.168.4.7; }; #指定主DNS服务器

masterfile-format text; #地址库文件明文存储

};

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

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

lol.com.slave

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

nameserver 192.168.4.7

nameserver 192.168.4.207

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

九、DNS主从数据同步

虚拟机A：

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

…….此处省略一万字

2020111801 ; serial #数据的版本号，由10个数字组成

1D ; refresh #每隔1天主从进行数据交互

1H ; retry #失效之后的时间间隔每一个1小时

1W ; expire #真正的失效时间，1周

3H ) ; minimum #失效记录的记忆时间3小时

lol.com. NS svr7

lol.com. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A **11.12.13.14**

[root@svr7 /]# systemctl restart named

虚拟机B：

[root@pc207 /]# nslookup www.lol.com 192.168.4.207