一、环境准备

还原快照（xshell完成），开启虚拟机A与虚拟机B

昨日习题：

案例1:为虚拟机A 配置以下虚拟Web主机

- 实现三个网站的部署

- 实现客户端访问server0.example.com网页内容为 大圣归来

- 实现客户端访问www0.example.com网页内容为 大圣又归来

- 实现客户端访问webapp0.example.com网页内容为 大圣累了

虚拟机A：

[root@A ~]# firewall-cmd --set-default-zone=trusted

[root@A ~]# setenforce 0

[root@A ~]# yum -y install httpd

[root@A ~]# mkdir /var/www/nsd01

[root@A ~]# mkdir /var/www/nsd02

[root@A ~]# mkdir /var/www/nsd03

[root@A ~]# echo '大圣归来' > /var/www/nsd01/index.html

[root@A ~]# echo '大圣又归来' > /var/www/nsd02/index.html

[root@A ~]# echo '大圣累了' > /var/www/nsd03/index.html

[root@A ~]# vim /etc/httpd/conf.d/vhost.conf

ServerName server0.example.com

DocumentRoot /var/www/nsd01

</VirtualHost>

<VirtualHost \*:80>

ServerName www0.example.com

DocumentRoot /var/www/nsd02

</VirtualHost>

<VirtualHost \*:80>

ServerName webapp0.example.com

DocumentRoot /var/www/nsd03

</VirtualHost>

[root@A ~]# systemctl restart httpd

虚拟机B：测试

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

192.168.4.7 server0.example.com www0.example.com webapp0.example.com

[root@B ~]# curl server0.example.com

[root@B ~]# curl www0.example.com

[root@B ~]# curl webapp0.example.com

案例2:为虚拟机A 使用自定Web根目录

调整 Web 站点 http://www0.example.com 的网页目录，要求如下：

1）新建目录 /webroot，作为此站点新的网页目录

2）确保站点 http://www0.example.com 仍然可访问

虚拟机A：

[root@A ~]# vim /etc/httpd/conf.d/vhost.conf

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /var/www/nsd01

</VirtualHost>

<VirtualHost \*:80>

ServerName www0.example.com

DocumentRoot /webroot

</VirtualHost>

<VirtualHost \*:80>

ServerName webapp0.example.com

DocumentRoot /var/www/nsd03

</VirtualHost>

[root@A ~]# mkdir /webroot

[root@A ~]# echo 'wo shi webroot' > /webroot/index.html

[root@A ~]# vim /etc/httpd/conf.d/myacl.conf

<Directory /webroot>

Require all granted

</Directory>

[root@A ~]# systemctl restart httpd

虚拟机B:

[root@B ~]# curl www0.example.com

wo shi webroot

[root@B ~]#

案例3：为虚拟机A 部署站点

为站点 webapp0.example.com 进行配置，要求如下：

1）此虚拟主机侦听在端口8909

2）从浏览器访问 http://webapp0.example.com:8909

虚拟机A：

[root@A ~]# vim /etc/httpd/conf.d/vhost.conf

<VirtualHost \*:80>

ServerName server0.example.com

DocumentRoot /var/www/nsd01

</VirtualHost>

<VirtualHost \*:80>

ServerName www0.example.com

DocumentRoot /webroot

</VirtualHost>

Listen 8909

<VirtualHost \*:8909>

ServerName webapp0.example.com

DocumentRoot /var/www/nsd03

</VirtualHost>

[root@A ~]# systemctl restart httpd

虚拟机B：

[root@B ~]# curl webapp0.example.com:8909

大圣累了

案例4：普通NFS共享的实现

1.在虚拟机A上配置NFS服务，只读的方式共享目录 /public

2.在虚拟机B上访问NFS共享目录

a）将虚拟机A 的 /public 挂到本地 /mnt/nfsmount

b）这些文件系统在系统启动时自动挂载

虚拟机A：

[root@A ~]# yum -y install nfs-utils

[root@A ~]# mkdir /public

[root@A ~]# touch /public/1.txt

[root@A ~]# ls /public/

[root@A ~]# vim /etc/exports

/public \*(ro)

[root@A ~]# systemctl restart rpcbind #先重启

[root@A ~]# systemctl restart nfs-server #后重启

虚拟机B：

[root@B ~]# mkdir /mnt/nfsmount

[root@B ~]# vim /etc/fstab

192.168.4.7:/public /mnt/nfsmount nfs defaults,\_netdev 0 0

[root@B ~]# mount -a

[root@B ~]# df -h | tail -1

192.168.4.7:/public 17G 3.5G 14G 21% /mnt/nfsmount

[root@B ~]#

案例5： autofs触发挂载

在虚拟机B上访问NFS共享目录，将 虚拟机A 的 /public完成触发挂载到本地 /mnt/nfsauto

虚拟机B：

[root@B ~]# vim /etc/auto.master

.......

/mnt /etc/myauto.conf

[root@B /]# vim /etc/myauto.conf

nfsauto -fstype=nfs 192.168.4.7:/public

[root@B /]# systemctl restart autofs

[root@B /]# ls /mnt/nfsauto #测试

二、环境设置：

虚拟机A：

[root@svr7 ~]# firewall-cmd --set-default-zone=trusted

[root@svr7 ~]# setenforce 0

[root@svr7 ~]# getenforce

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

SELINUX=permissive

虚拟机B：

[root@pc207 ~]# firewall-cmd --set-default-zone=trusted

[root@pc207 ~]# setenforce 0

[root@pc207 ~]# getenforce

[root@pc207 ~]# vim /etc/selinux/config

SELINUX=permissive

三、DNS服务器简介

•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服务器的分类

根域名服务器、一级DNS服务器、 二级DNS服务器、 三级DNS服务器

•域名结构（树型结构）

所有的域名都要以点作为结尾：www.qq.com.

根域名： .

一级域名: .cn .us .hk .tw .kr .jp .........

二级域名：.com.cn .net.cn .org.cn ........

三级域名： dc.com.cn tc.com.cn nb.com.cn ........

• Full Qualified Domain Name

完全的合格的主机名（FQDN）：站点名+注册的域名

www.dc.com.cn vip.dc.com.cn ftp.dc.com.cn

四、构建DNS服务器

•BIND（Berkeley Internet Name Daemon）

–伯克利 Internet 域名服务

–bind-chroot（提供虚拟根支持，牢笼政策）  bind（域名服务包）

•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：DNS协议的端口 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地址的对应关系

虚拟机A：

1.安装软件包

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

2.修改主配置文件

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

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

options {

directory "/var/named"; #指定地址库文件存放目录

};

zone "**tedu.cn**" IN { #指定本机负责解析的域名

type master; #指定本机为权威主服务器

file "tedu.cn.zone"; #地址库文件名字

};

3.建立地址库文件

1)保证named用户对地址库文件有读权限

2)地址库文件所有的域名都要以点作为结尾

3)地址库文件如果不以点作为结尾，默认补全本地址库文件负责的域名

]# cd /var/named/

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

svr7 A 192.168.4.7

www A 1.1.1.1

ftp A 2.2.2.2

vip A 3.3.3.3

[root@svr7 named]# systemctl restart named

虚拟机B

1.指定DNS服务器地址

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

]# cat /etc/resolv.conf

]# nslookup www.tedu.cn

]# nslookup ftp.tedu.cn

]# nslookup vip.tedu.cn

五、多区域的DNS服务器

虚拟机A：

1.修改主配置文件

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

.......此处省略一万字

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

type master;

file "qq.com.zone";

};

2.建立地址库文件

]# cd /var/named/

]# cp -p named.localhost qq.com.zone #-p保持权限不变

]# vim qq.com.zone

.......此处省略一万字

qq.com. NS svr7

svr7 A 192.168.4.7

www A 5.5.5.5

[root@svr7 named]# systemctl restart named

六、特殊的解析记录

•**DNS轮询：**基于DNS的站点负载均衡

–一个域名 ---> 多个不同IP地址

–每个IP提供镜像服务内容

以www.qq.com为例

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

.......此处省略一万字

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

www A 192.168.4.20

www A 192.168.4.30

[root@svr7 /]# systemctl restart named

[root@pc207 ~]# ping www.qq.com #测试

•**泛域名解析**

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

.......此处省略一万字

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

www A 192.168.4.20

www A 192.168.4.30

\* A 6.6.6.6

qq.com. A 7.7.7.7

[root@svr7 /]# systemctl restart named

[root@pc207 ~]# nslookup wwww.qq.com #测试

[root@pc207 ~]# nslookup qq.com #测试

•**解析记录的别名**

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

.......此处省略一万字

qq.com. NS svr7

svr7 A 192.168.4.7

www A 192.168.4.10

www A 192.168.4.20

www A 192.168.4.30

\* A 6.6.6.6

qq.com. A 7.7.7.7

vip A 8.8.8.8

mail CNAME vip

[root@svr7 /]# systemctl restart named

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

Server: 192.168.4.7

Address: 192.168.4.7#53

mail.qq.com canonical name = vip.qq.com.

Name: vip.qq.com

Address: 8.8.8.8

•DNS服务器资源解析记录的类型

NS解析记录：声明DNS服务器

A解析记录：正向解析记录

CNAME解析记录：解析记录别名

七、DNS的查询方式（递归与迭代）

虚拟机A：负责域名tedu.cn(父域)

虚拟机B：负责域名bj.tedu.cn(子域)

虚拟机B：

1.安装软件包

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

2.修改主配置文件

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

[root@pc207 ~]# vim /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

]# cd /var/named/

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

]# 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，告知虚拟机A，虚拟机B是专门维护bj.tedu.cn的DNS服务器

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

.......此处省略一万字

tedu.cn. NS svr7

bj.tedu.cn. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 1.1.1.1

ftp A 2.2.2.2

vip A 3.3.3.3

[root@svr7 /]# systemctl restart named

虚拟机B：进行测试

[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

•递归解析：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

•迭代解析：客户端发送请求给首选DNS服务器，首选DNS服务器告知下一个服务器的IP地址

虚拟机A：禁止递归查询

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

options {

directory "/var/named";

recursion no; #禁止DNS递归查询

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

zone "qq.com" IN {

type master;

file "qq.com.zone";

};

[root@svr7 /]# systemctl restart named

[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:

\*\*\* Can't find www.bj.tedu.cn: No answer

专门用于DNS查询过程的命令dig

[root@pc207 /]# dig www.bj.tedu.cn 192.168.4.7

八、DNS主从架构

作用：可靠性的提升，从DNS服务器备份，主DNS服务器数据

虚拟机A：主DNS服务器，以tedu.cn域名为例

虚拟机B：从DNS服务器，以tedu.cn域名为例

虚拟机A：主DNS服务器

1.授权从服务器

[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; }; #指定从服务器地址

};

.......此处省略一万字

2.修改地址库文件

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

.......此处省略一万字

tedu.cn. NS svr7

tedu.cn. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 1.1.1.1

ftp A 2.2.2.2

vip A 3.3.3.3

[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 /]# ls -ld /var/named/slaves/

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

options {

directory "/var/named";

};

zone "tedu.cn" IN {

type slave;

file "/var/named/slaves/tedu.cn.slave";

masters { 192.168.4.7; }; #指定主DNS服务器IP地址

#保证named用户对目录有写入权限

};

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

[root@pc207 /]# systemctl restart named

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

tedu.cn.slave

九、DNS主从数据的同步

数据的版本号：由管理员进行编写，由10个数字组成。越大版本越新

虚拟机A：

1.修改地址库文件

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

$TTL 1D

@ IN SOA @ rname.invalid. (

2020061601 ; serial #数据的版本号

1D ; refresh #每个1天时间，主从自动交接一次

1H ; retry #重试时间间隔1小时

1W ; expire #失效时间1周

3H ) ; minimum #失效记录的记忆时间3小时

tedu.cn. NS svr7

tedu.cn. NS pc207

svr7 A 192.168.4.7

pc207 A 192.168.4.207

www A 10.10.10.10

ftp A 2.2.2.2

vip A 3.3.3.3

[root@svr7 /]# systemctl restart named

测试：

[root@pc207 /]# nslookup www.tedu.cn 192.168.4.7

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