NSD SERVICES DAY02

1. 案例1：搭建单区域DNS服务器
2. 案例2：特殊DNS解析
3. 案例3：配置DNS子域授权
4. 案例4：搭建并测试缓存DNS

1 案例1：搭建单区域DNS服务器

1.1 问题

本例要求要求为DNS区域tedu.cn搭建一台DNS服务器，以便用户能通过域名的方式访问网站。测试阶段主要提供以下正向记录：

1. svr7.tedu.cn ---> 192.168.4.7
2. pc207.tedu.cn ---> 192.168.4.207
3. www.tedu.cn ---> 192.168.4.100

配置完成后在客户机上验证查询结果。

1.2 方案

快速构建DNS服务器的基本过程：

1. 安装 bind、bind-chroot 包
2. 建立主配置文件 /etc/named.conf
3. 建立地址库文件 /var/named/.. ..
4. 启动 named 服务

配置及使用DNS客户端的基本过程：

1. 修改配置文件/etc/resolv.conf，添加nameserver=DNS服务器地址
2. 使用host命令查询，提供目标域名作为参数

1.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：配置DNS服务器svr7

1）安装 bind、bind-chroot 包

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

2）建立主配置文件 /etc/named.conf

Top

```
[root@svr7 ~]# mv /etc/named.conf /etc/named.conf.origin      //备份默认配置
```

```
[root@svr7 ~]# vim /etc/named.conf                    //建立新配置
options {
    directory "/var/named";                    //地址库默认存放位置
};
zone "tedu.cn" {                              //定义正向DNS区域
    type master;                               //主区域
    file "tedu.cn.zone";                       //自定义地址库文件名
};
```

3）建立地址库文件 /var/named/tedu.cn.zone

```
[root@svr7 ~]# cd /var/named/                         //进地址库目录
[root@svr7 named]# cp -p named.localhost tedu.cn.zone     //参考范本建地址库文件
[root@svr7 named]# vim tedu.cn.zone                   //修订地址库记录
$TTL 1D                                   //文件开头部分可保持不改
@ IN SOA @ rname.invalid. (
                0 ; serial
                1D ; refresh
                1H ; retry
                1W ; expire
                3H ) ; minimum
@ NS svr7.tedu.cn.                        //本区域DNS服务器的FQDN
svr7 A 192.168.4.7                        //为NS主机提供A记录
pc207 A 192.168.4.207                     //其他正向地址记录...
www A 192.168.4.100
```

4）启动 named 服务，并设置开机自启

```
[root@svr7 named]# systemctl restart named
[root@svr7 named]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /u
```

步骤二：配置DNS客户机pc207并测试

1）修改配置文件/etc/resolv.conf，指定默认使用哪一台DNS服务器

Top

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

```
02.     nameserver  192.168.4.7
03.     .. ..
```

2）使用host命令查询，提供目标域名作为参数

```
01.     [root@pc207 ~]# host  svr7.tedu.cn
02.     svr7.tedu.cn has address 192.168.4.7
03.     [root@pc207 ~]# host  pc207.tedu.cn
04.     pc207.tedu.cn has address 192.168.4.207
05.     [root@pc207 ~]# host  www.tedu.cn
06.     www.tedu.cn has address 192.168.4.100
```

使用host测试DNS查询结果时，如果不方便修改/etc/resolv.conf文件，也可以采用“host 目标域名 DNS服务器地址”形式临时指定使用哪一台DNS服务器。

```
01.     [root@pc207 ~]# host  pc207.tedu.cn  192.168.4.7
02.     Using domain server:
03.     Name:  192.168.4.7
04.     Address:  192.168.4.7#53
05.     Aliases:
06.
07.     pc207.tedu.cn has address 192.168.4.207
```

2 案例2：特殊DNS解析

2.1 问题

沿用案例1，本例要求掌握DNS轮询、泛域名解析的配置，实现的目标如下：

1. 为站点 www.tedu.cn 提供DNS轮询解析，三台Web服务器节点的IP地址分别为：192.168.4.100、192.168.4.110、192.168.4.120
2. 配置泛域名解析实现以下解析记录：任意名称.tedu.cn ---> 119.75.217.56

2.2 方案

DNS轮询：FQDN ---> IP地址1、IP地址2、.. ..

泛域名解析（站点名不确定）：多个FQDN ---> 一个IP地址

2.3 步骤

实现此案例需要按照如下步骤进行。

Top

步骤一：配置DNS轮询

1）修改DNS服务器上tedu.cn区域的地址库文件，在末尾添加轮询地址记录

```
[root@svr7 ~]# vim /var/named/tedu.cn.zone
... ...
www     A   192.168.4.100
www     A   192.168.4.110
www     A   192.168.4.120
```

2）重启系统服务named

```
[root@svr7 named]# systemctl restart named
```

3）在客户机pc207上测试轮询记录

针对目标www.tedu.cn执行多次查询，观察第1条结果的变化：

```
[root@pc207 ~]# host www.tedu.cn
www.tedu.cn has address 192.168.4.100       //第1个结果为192.168.4.100
www.tedu.cn has address 192.168.4.110
www.tedu.cn has address 192.168.4.120

[root@pc207 ~]# host www.tedu.cn
www.tedu.cn has address 192.168.4.120       //第1个结果为192.168.4.120
www.tedu.cn has address 192.168.4.110
www.tedu.cn has address 192.168.4.100

[root@pc207 ~]# host www.tedu.cn
www.tedu.cn has address 192.168.4.110       //第1个结果为192.168.4.110
www.tedu.cn has address 192.168.4.120
www.tedu.cn has address 192.168.4.100
```

步骤二：配置多对一的泛域名解析

1）修改DNS服务器上指定区域的地址库文件，在末尾添加*通配地址记录

```
[root@svr7 ~]# vim /var/named/tedu.cn.zone
... ...
*       A   119.75.217.56
```

Top

2）重启系统服务named

```
[root@svr7 named]# systemctl restart named
```

3）在客户机pc207上测试多对一的泛域名解析记录

当查询未知站点（地址库中没有明确记录）时，以 * 对应的IP地址反馈：

```
[root@pc207 ~]# host station123.tedu.cn
station123.tedu.cn has address 119.75.217.56
[root@pc207 ~]# host movie.tedu.cn
movie.tedu.cn has address 119.75.217.56
[root@pc207 ~]# host tts8.tedu.cn
tts8.tedu.cn has address 119.75.217.56
```

3 案例3：配置DNS子域授权

3.1 问题

沿用案例1，本例要求为上下级两个DNS区域建立父子关联，实现客户机向父DNS也可以查询到子域内的FQDN，基本要求如下：

1. 构建父DNS（tedu.cn）服务器
2. 构建子DNS（bj.tedu.cn）服务器
3. 在父DNS上配置子域授权
4. 测试子域授权查询

3.2 方案

为一个DNS区域添加授权子域时，需要修改此区域的地址库，添加以下记录：

```
子域域名.          IN   NS    子DNS的FQDN.
子DNS的FQDN.       IN   A     子DNS的IP地址
```

3.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：构建父DNS（tedu.cn）服务器

1）将svr7配置为父DNS服务器，确认配置

主配置文件/etc/named.conf：

Top

```
[root@svr7 ~]# viim /etc/named.conf
options {
        directory "/var/named";
};
zone "tedu.cn" {
        type master;
        file "tedu.cn.zone";
};
.. ..
```

正向地址库文件：

```
[root@svr7 ~]# vim /var/named/tedu.cn.zone
$TTL 1D
@   IN SOA   @ rname.invalid. (
                    0   ; serial
                    1D  ; refresh
                    1H  ; retry
                    1W  ; expire
                    3H )    ; minimum
@       NS   svr7.tedu.cn.
svr7      A    192.168.4.7
pc207   A    192.168.4.207
www       A    192.168.4.100
.. ..
```

确保服务已启用：

```
[root@svr7 ~]# systemctl restart named
```

2）测试 —— 向父DNS可成功查询到父区域中的站点

```
[root@pc207 ~]# host www.tedu.cn 192.168.4.7
Using domain server:
Name: 192.168.4.7
Address: 192.168.4.7#53
Aliases:
```

Top

```
06.
07.     www.tedu.cn has address 192.168.4.100
08.     .. ..
```

步骤二：构建子DNS（bj.tedu.cn）服务器

1）将pc207配置为子DNS服务器，确认配置

安装软件包bind、bind-chroot：

```
01.     [root@pc207 ~]# yum -y  install  bind  bind-chroot
02.     .. ..
```

建立主配置文件/etc/named.conf：

```
01.     [root@pc207 ~]# mv  /etc/named.conf  /etc/named.conf.origin     //备份默认配置
02.     [root@pc207 ~]# vim  /etc/named.conf                            //建立新配置
03.     options {
04.        directory  "/var/named";
05.     };
06.     zone  "bj.tedu.cn" {                      //定义子DNS的正向区域
07.        type  master;
08.        file  "bj.tedu.cn.zone";
09.     };
```

建立地址库配置文件：

```
01.     [root@pc207 ~]# cd  /var/named/                          //进地址库目录
02.     [root@pc207 named]# cp -p  named.localhost  tedu.cn.zone     //参考范本建地址库文件
03.     [root@pc207 named]# vim  bj.tedu.cn.zone                 //修订地址库记录
04.     $TTL 1D                                 //文件开头部分可保持不改
05.     @   IN SOA  @ rname.invalid. (
06.                     0   ; serial
07.                     1D  ; refresh
08.                     1H  ; retry
09.                     1W  ; expire
10.                     3H )    ; minimum
11.     @       NS  pc207.bj.tedu.cn.                //本区域DNS服务器的FQDN
12.     pc207   A   192.168.4.207                //为NS主机提供A记录
```

Top

```
13.  www    A   1.2.3.4                  //添加测试记录 www.bj.tedu.cn
```

2）启动系统服务named，并设置开机自启

```
01.  [root@pc207 named]# systemctl  restart  named
02.  [root@pc207 named]# systemctl  enable  named
03.  Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /u
```

3）测试 —— 向子DNS可成功查询到子区域中的站点

```
01.  [root@pc207 ~]# host  www.bj.tedu.cn  192.168.4.207
02.  Using domain server:
03.  Name: 192.168.4.207
04.  Address: 192.168.4.207#53
05.  Aliases:
06.
07.  www.bj.tedu.cn has address 1.2.3.4
```

步骤三：在父DNS上配置子域授权

1）测试 —— 未配置子域授权时，向父DNS无法正确查询到子区域中的站点

若父DNS配置有 * 泛域名，则反馈的结果为对应的IP地址119.75.217.56，而不是子DNS中记录的1.2.3.4：

```
01.  [root@pc207 ~]# host  www.bj.tedu.cn  192.168.4.7
02.  Using domain server:
03.  Name: 192.168.4.7
04.  Address: 192.168.4.7#53
05.  Aliases:
06.
07.  www.bj.tedu.cn has address 119.75.217.56
```

若父DNS未配置有 * 泛域名，则找不到解析结果（not found）：

Top

```
01.  [root@pc207 ~]# host  www.bj.tedu.cn  192.168.4.7
02.  Using domain server:
```

```
Name: 192.168.4.7
Address: 192.168.4.7#53
Aliases:

Host www.bj.tedu.cn not found: 3(NXDOMAIN)
```

2）修改父DNS区域tedu.cn的地址库，添加授权子域信息

```
[root@svr7 ~]# vim /var/named/tedu.cn.zone
...
bj.tedu.cn.        NS      pc207.bj.tedu.cn.          //子区域及子DNS主机名
pc207.bj.tedu.cn.  A       192.168.4.207              //子DNS的IP地址

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

步骤四：测试子域授权查询

测试 —— 成功配置子域授权以后，向父DNS可以正确查询到子区域中的站点：

```
[root@pc207 ~]# host www.bj.tedu.cn 192.168.4.7
Using domain server:
Name: 192.168.4.7
Address: 192.168.4.7#53
Aliases:

www.bj.tedu.cn has address 1.2.3.4
```

4 案例4：搭建并测试缓存DNS

4.1 问题

本例要求熟悉缓存DNS的工作过程，准备一台可上网的RHEL7虚拟机，并完成下列任务：

1. 安装 bind、bind-chroot 包
2. 搭建并测试基于全局转发器的缓存DNS

注意：若所在机房不具备访问互联网DNS条件，此案例改由学员自行在家完成。

4.2 方案

Top

权威/官方DNS服务器的特点：

- 至少管理一个DNS区域，，需要IANA等官方机构授权

- 典型应用：根域DNS、一级域DNS、二级域DNS、三级域DNS、.. ..

缓存DNS服务器的特点：

- 不需要管理任何DNS区域，但是能够替客户机查询，而且通过缓存、复用查询结果来加快响应速度
- 典型应用：ISP服务商、企业局域网

缓存DNS服务器的解析记录来源：

- 方式1：全局转发：将请求转发给指定的公共DNS（其他缓存DNS），请求递归服务
- 方式2：根域迭代：依次向根、一级、二级……域的DNS服务器迭代

4.3 步骤

实现此案例需要按照如下步骤进行。

步骤一：为虚拟机pc207提供上网条件

1）为虚拟机添加一块新的网卡，选择NAT或Bridge模式

若选择NAT模式（地址转换），则新加网卡的上网参数由虚拟化平台自动设置。

若选择Bridge模式（桥接），则新加网卡的上网参数需要参考真实网络的主机，必要时请网络管理员提供支持。

此处所列地址信息可帮助大家理解上网条件，但不作为练习的配置依据：

```
[root@pc207 ~]# ifconfig  eth1                  //检查新增网卡的IP地址
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.70.129  netmask 255.255.255.0  broadcast 192.168.70.255
.. ..
[root@pc207 ~]# route -n                        //确认已配好默认网关
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.70.2    0.0.0.0         UG    100    0        0 eth1
192.168.70.0    0.0.0.0         255.255.255.0   U     100    0        0 eth1
.. ..
[root@pc207 ~]# cat  /etc/resolv.conf           //确认第一DNS为外部可用DNS地址
nameserver 192.168.70.2
.. ..
```

2）确保从主机pc207可访问到外部DNS

访问默认DNS可用（本机正常连网需要）：

```
[root@pc207 ~]# host  www.qq.com                                    Top
www.qq.com has address 111.30.132.101
www.qq.com has IPv6 address 240e:e1:8100:28::2:16
```

访问指定DNS可用（全局转发的前提条件）：

```
[root@pc207 ~]# host www.qq.com 202.106.0.20    //国内公共DNS服务器之一
Using domain server:
Name: 202.106.0.20
Address: 202.106.0.20#53
Aliases:

www.qq.com has address 111.30.132.101
www.qq.com is an alias for qq.com.edgesuite.net.
qq.com.edgesuite.net is an alias for a1574.b.akamai.net.
www.qq.com is an alias for qq.com.edgesuite.net.
qq.com.edgesuite.net is an alias for a1574.b.akamai.net.
```

步骤二：将pc207配置为缓存DNS（全局转发式）

1）安装bind、bind-chroot软件包

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

2）建立主配置文件/etc/named.conf

当收到来自客户机的DNS查询请求时，转发到外网的其他DNS服务器

```
[root@pc207 ~]# vim /etc/named.conf
options {
    forwarders { 202.106.0.20; };
};
```

3）启动系统服务named，并设置开机自启

```
[root@pc207 ~]# systemctl restart named
[root@pc207 ~]# systemctl enable named
```

Top

4）可向缓存DNS服务器pc207查询到公共域名（百度、网易等站点）

```
[root@pc207 ~]# host  www.baidu.com  192.168.4.207          //查百度的站点IP
Using domain server:
Name:  192.168.4.207
Address:  192.168.4.207#53
Aliases:

www.baidu.com is an alias for www.a.shifen.com.
www.a.shifen.com has address 111.13.100.92
www.a.shifen.com has address 111.13.100.91

[root@pc207 ~]# host  www.163.com  192.168.4.207           //查网易的站点IP
Using domain server:
Name:  192.168.4.207
Address:  192.168.4.207#53
Aliases:

www.163.com is an alias for www.163.com.lxdns.com.
www.163.com.lxdns.com is an alias for 163.xdwscache.ourglb0.com.
163.xdwscache.ourglb0.com has address 111.11.31.104
163.xdwscache.ourglb0.com has address 111.11.31.114
```

Top