第 9 讲　DNS 与 DHCP 服务配置管理

王晓庆

wangxiaoqing@outlook.com

May 24, 2016

Outline

Bind 的安装与 DNS 服务器类型

- Bind 的安装

```
rpm -qa | grep 'bind'
yum install bind bind-chroot bind-libs bind-utils
rpm -ql bind | less
```

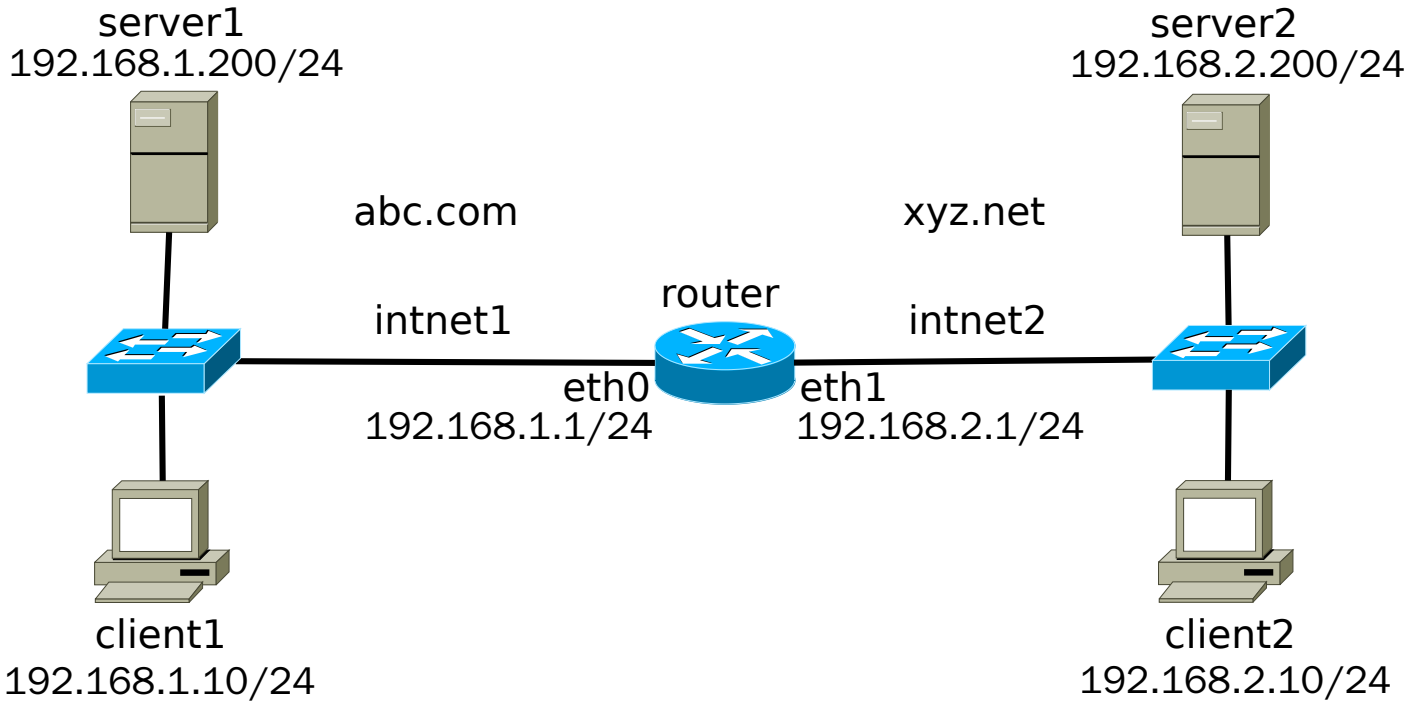
- DNS 服务器类型
  1. 缓存服务器 (Caching)
  2. 转发服务器 (Forwarding)
  3. 主域名服务器 (Master)
  4. 从域名服务器 (Slave)

注意

一台服务器可以同时充当上述多种角色。

实验环境搭建

- 实验拓扑图



- 实验准备
  - 按图配置主机名、IP、默认网关等，保证所有主机能互相 ping 通。

缓存服务器的安装配置 (server1)

- 默认情况下 bind 并未提供主配置文件
  - /var/named/chroot/etc/named.conf
- 安装缓存服务器

```
yum -y install caching-nameserver
rpm -ql caching-nameserver
service named start
```

缓存服务器的默认配置

```
cd /var/named/chroot/etc
grep -v '//' named.caching-nameserver.conf
options {
        listen-on port 53 { 127.0.0.1; }; # 仅监听环回接口
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named"; # 指定默认工作目录
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats
        allow-query     { localhost; }; # 仅允许本机访问
        allow-query-cache { localhost; }; # 本机访问缓存
};
```

缓存服务器的默认配置 (2)

```
logging {
        channel default_debug { # 定义日志通道
                file "data/named.run"; # 默认日志文件
                severity dynamic; # 默认日志等级
        };
};
view localhost_resolver { # 定义视图
        match-clients      { localhost; }; # 匹配请求源地址
        match-destinations { localhost; }; # 匹配请求目标地
        recursion yes; # 允许递归查询
        include "/etc/named.rfc1912.zones"; # 包含区域文件
};
```

修改缓存服务器默认配置

```
vim named.caching-nameserver.conf
acl corpnets { 192.168.1.0/24; 192.168.2.0/24; };
options {
        listen-on port 53 { any; }; # 监听所有接口
        directory "/var/named";
        allow-query { corpnets; }; # 允许指定客户端
        recursion yes; # 允许递归查询
};
include "/etc/named.rfc1912.zones"; # 包含区域文件

service named restart # 重启 named 服务使配置生效
cat /var/named/chroot/etc/named.rfc1912.zones
ls /var/named/chroot/var/named # 查看区域文件所在目录
```

配置主域名服务器 (server1)(1)

- 1. 配置 named.conf 文件，添加区域

```
cd /var/named/chroot/etc
cp -p named.caching-nameserver.conf named.conf
vim named.conf # 在最后添加下面几行
zone "abc.com" IN {
        type master;
        file "abc.com.zone";
};
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.1.rev";
};
```

配置主域名服务器 (server1)(2)

- 2. 创建正向区域文件 abc.com.zone

```
cp -p localhost.zone abc.com.zone
vim abc.com.zone
$TTL 86400
@       IN SOA ns1.abc.com. root.abc.com. (
                                        42    ; serial
                                        3H    ; refresh
                                        15M   ; retry
                                        1W    ; expiry
                                        1D ) ; minimum
        IN NS          ns1.abc.com.
        IN MX    5     mail.abc.com.
ns1     IN A           192.168.1.200
www     IN A           192.168.1.200
ftp     IN CNAME       www.abc.com.
mail    IN A           192.168.1.200
```

配置主域名服务器 (server1)(3)

- 3. 创建反向区域文件 192.168.1.rev

```
cp -p named.local 192.168.1.rev
vim 192.168.1.rev
$TTL 86400
@ IN SOA ns1.abc.com. root.abc.com. (
                                  2016052001 ; Serial
                                  28800      ; Refresh
                                  14400      ; Retry
                                  3600000    ; Expire
                                  86400 )    ; Minimum
         IN       NS       ns1.abc.com.
200      IN       PTR      ns1.abc.com.
200      IN       PTR      www.abc.com.
200      IN       PTR      ftp.abc.com.
200      IN       PTR      mail.abc.com.
10       IN       PTR      client1.abc.com.
```

配置主域名服务器 (server1)(4)

- 检查配置文件

```
cd /var/named/chroot/etc
named-checkconf named.conf # 检查主配置文件
cd /var/named/chroot/var/named
named-checkzone abc.com abc.com.zone # 检查区域文件
named-checkzone 1.168.192.in-addr.arpa 192.168.1.rev
```

- 重启 named 服务，使配置生效

```
service named restart
```

客户端配置及测试 (client1)

- 客户端配置

```
vim /etc/resolv.conf
nameserver 192.168.1.200
```

- 客户端测试

```
host [-t type] domain-name [dns-server]
host www.abc.com [192.168.1.200]
host -t mx abc.com [192.168.1.200]
nslookup ftp.abc.com [192.168.1.200]
nslookup [- 192.168.1.200] # 开始交互查询
set type=mx
abc.com
exit                              # 退出交互查询
dig @server domain type
dig @192.168.1.200 abc.com ns
```

配置从域名服务器 (server1)(1)

- 1. 编辑主域名服务器主配置文件

```
cd /var/named/chroot/etc
vim named.conf # 添加 allow-transfer 语句
zone "abc.com" IN {
        type master;
        file "abc.com.zone";
        allow-transfer { 192.168.2.200; };
};
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.1.rev";
        allow-transfer { 192.168.2.200; };
};
```

配置从域名服务器 (server2)(2)

- 2. 编辑从域名服务器主配置文件

```
cd /var/named/chroot/etc
scp root@192.168.1.200:/var/named/chroot\
/etc/named.conf .
chgrp named named.conf # 将配置文件归属 named 组
vim named.conf # 修改区域定义相关内容
zone "abc.com" IN {
        type slave;
        file "slaves/abc.com.zone";
        masters { 192.168.1.200; };
};
zone "1.168.192.in-addr.arpa" IN {
        type slave;
        file "slaves/192.168.1.rev";
        masters { 192.168.1.200; };
};
```

配置从域名服务器 (server1 和 server2)

- 3. 使配置生效并检查、测试从域名服务器

```
cd /var/named/chroot/var/named
ls slaves
# 重启 server1 的 named 服务
service named restart
# 重启 server2 的 named 服务
service named restart
ls slaves
```

注意

每次修改主域名服务器的区域文件后，一定不要忘记增加其 SOA 记录中的序号，否则从域名服务器将得不到区域更新！

- 4. 客户端测试（略）

练习

- 在 server2 上配置 xyz.net 域的主域名服务器
  1. 编辑 named.conf 文件
  2. 编辑 xyz.net.zone 正向区域文件
  3. 编辑 192.168.2.rev 反向区域文件
  4. 检查配置文件和区域文件
  5. 重启 named 服务
  6. 配置 dns 客户端 (client2)
  7. 客户端测试

配置区域委派 (1)

- 1. 在子域主域名服务器 (server2) 上配置子域

```
cd /var/named/chroot
vim etc/named.conf # 在最后面添加子域定义
zone "jx.abc.com" IN {
  type master;
  file "jx.abc.com.zone";
};
# 此处不需要重复定义反向区域 2.168.192.in-addr.arpa
```

配置区域委派 (2)

- 2. 在子域主域名服务器 (server2) 上配置子域正向区域文件

```
vim var/named/jx.abc.com.zone
$TTL 86400
@       IN      SOA ns1  root (
                                    42    ; serial
                                    3H    ; refresh
                                    15M   ; retry
                                    1W    ; expiry
                                    1D )  ; minimum
        IN NS           ns1.jx.abc.com.
ns1     IN A            192.168.2.200
www     IN A            192.168.2.200
ftp     IN CNAME        www.abc.com.
```

配置区域委派 (3)

- 3. 在子域主域名服务器 (server2) 上配置子域反向区域文件

```
vim var/named/192.168.2.rev # 在最后面添加几行记录
        IN      NS      ns1.jx.abc.com.
200     IN      PTR     ns1.jx.abc.com.
200     IN      PTR     www.jx.abc.com.
200     IN      PTR     ftp.jx.abc.com.
```

配置区域委派 (4)

- 4. 在父域域名服务器 (server1) 正向区域文件中上添加委派记录

```
cd /var/named/chroot/var/named
vim abc.com.zone    # 在最后面添加子域委派记录
jx          IN          NS          ns1.jx.abc.com.
ns1.jx      IN          A           192.168.2.200
```

- 5. 重启父域和子域 named 服务

```
service named restart
```

- 6. 客户端测试
  - 通过父域域名服务器查询得到的是非权威答案

```
nslookup ftp.jx.abc.com 192.168.1.200
```

配置转发器 (1)

- 在 server1 上配置全局转发

```
host ftp.xyz.net 192.168.1.200 # 无法解析！
cd /var/named/chroot/etc
vim named.conf # 添加下面几行
options {
        listen-on port 53 { any; };
        directory       "/var/named";
  forward only; # 仅转发，也可为 first(先转发)
  forwarders { 192.168.2.200; }; # 配置转发器
        allow-query     { any; };
        recursion yes;
};

service named restart # 重启 named 服务
host ftp.xyz.net 192.168.1.200 # 解析成功！
```

配置转发器 (2)

- 在 server1 上配置区域转发

```
cd /var/named/etc
vim named.conf # 修改主配置文件
options {
        listen-on port 53 { any; };
        directory       "/var/named";
        allow-query     { any; };
        recursion yes;
};
...
zone "xyz.net" IN {   # 添加转发区域
  type forward;
  forwarders: { 192.168.2.200; };
};
```

在 server1 上安装配置 dhcp 服务器 (1)

- 1. 安装 dhcp 服务

```
rpm -qa | grep dhcp
yum install dhcp
rpm -ql dhcp
```

在 server1 上安装配置 dhcp 服务器 (2)

- 2. 配置 dhcp 服务

```
cd /usr/share/doc/dhcp-3.0.5/
cp dhcpd.conf.sample /etc/dhcpd.conf
vim dhcpd.conf
ddns-update-style interim;
ignore client-updates;
subnet 192.168.1.0 netmask 255.255.255.0 {
        option routers                  192.168.1.1;
        option subnet-mask              255.255.255.0;
        option domain-name-servers      192.168.1.200;
        range 192.168.1.50 192.168.1.199;
        default-lease-time 21600;
        max-lease-time 43200;
}
```

在 server1 上安装配置 dhcp 服务器 (3)

- 3. 测试 dhcp 服务器
  - 启动 dhcpd 服务

```
chkconfig --level 3 dhcpd on
service dhcpd start
```

  - 配置 dhcp 客户端 client1

```
cd /etc/sysconfig/network-scripts
vim ifcfg-eth1
DEVICE=eth1
BOOTPROTO=dhcp
ONBOOT=yes

dhclient    # 启动 dhcp 客户端
ifconfig
cat /var/lib/dhclient/dhclient.leases #client1 上查看租约
cat /var/lib/dhcpd/dhcpd.leases #server1 上查看租约
```

安装配置 dhcp 中继代理 (1)

- 1. 配置 dhcp 服务器 server1

```
vim /etc/dhcpd.conf   # 在最后面添加子网
subnet 192.168.2.0 netmask 255.255.255.0 {
        option routers                  192.168.2.1;
        option subnet-mask              255.255.255.0;
        option domain-name-servers      192.168.2.200;
        range 192.168.2.50 192.168.2.199;
        default-lease-time 21600;
        max-lease-time 43200;
}
```

安装配置 dhcp 中继代理 (2)

- 2. 配置 dhcp 中继代理 server2

```
yum install dhcp
chkconfig --level 3 dhrelay on
vim /etc/sysconfig/dhcrelay
DHCRELAYARGS="" # 运行参数
INTERFACES=""   # 监听接口，如"eth0 eth1"
DHCPSERVERS="192.168.2.200" # 指定 dhcp 服务器
# 注意：dhcp 中继代理本身必须有静态地址并能与服务器通信
service dhrelay start
```

安装配置 dhcp 中继代理 (3)

- 3. 配置 dhcp 客户端 client2

```
cd /etc/sysconfig/network-scripts
vim ifcfg-eth1
DEVICE=eth1
BOOTPROTO=dhcp
ONBOOT=yes

dhclient    # 启动 dhcp 客户端
ifconfig
cat /var/lib/dhclient/dhclient.leases #client2 上查看租
cat /var/lib/dhcpd/dhcpd.leases #server1 上查看租约
```