项目 5-配置与管理 DNS 服务器-实训任务指导书（5-2）

项目 5-配置与管理主-辅助 DNS 服务器

DNS：域名系统（英文：Domain Name System)是一个域名系统，是万维网上作为域名和 IP 地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的 IP 数串。

要求在企业内部构建一台 DNS 服务器,为局域网中的计算机提供域名解析服务。DNS 服务器管理 rjlinux.com 域的域名解析，DNS 服务器的域名为 dns.rjlinux.com，IP 地址为 192.168.1.2。辅助 DNS 服务器的 IP 地址为 192.168.1.3。同时还必须为客户提供 Internet 上的主机的域名解析。要求分别能解析以下域名:财务部（cw.rjlinux.com:192.168.1.11)，销售部(xs. rjlinux.com:192.168.1.12)，经理部(j1.rjlinux.com:192.168.1.13)，OA 系统(oa.rjlinux.com:192.168.1.13)。

子任务 1：配置主 DNS 服务器实例

子任务 2：配置辅助 DNS 服务器实例

具体实训步骤：

子任务二、配置辅助 DNS 服务器实例

DNS 服务器在网络中为全世界的服务器提供了域名解析服务，扮演着至关重要的角色。如果我们的 DNS 部署在单台服务器上，如果出现单点故障，就会造成部分域名无法解析，用户无法顺利访问到对应的服务器。我们使用相同解析的辅助 DNS，来解决单点故障问题，就算一台 DNS 服务器出现问题，也不会影响解析服务。辅助 DNS 是从主 DNS 拉取区域数据库文件的的，当主 DNS 解析的域名对应的区域数据库文件发生变化，辅助就会去找主 DNS 拉取新的区域数据库文件，保证和主的解析一致，而且是自动的不需要人为干预的，确保了主从 DNS 的区域数据库文件的一致性，这些辅助服务器的好处是它们在主 DNS 服务器关闭时提供冗余，并且它们还有助于将请求的负载分配到域，以便主服务器不会过载。

辅助 DNS 服务器的配置和主 DNS 服务器配置基本相同，所有参数均有主 DNS 服务器获取，本身不提供相应的配置文件。

一、在辅助 DNS 服务器上安装 DNS 服务，并启动服务

1．在辅助 DNS 服务器虚拟机上安装 bind 软件包

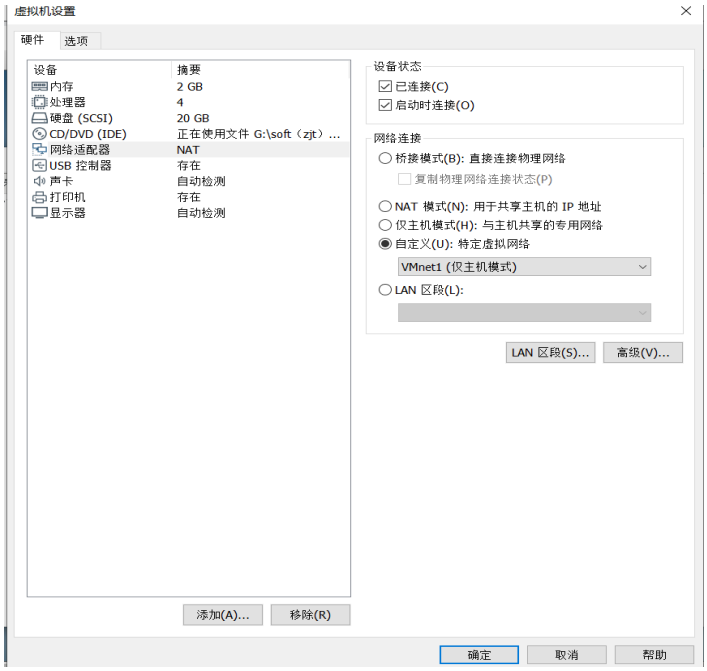
（1）使用 yum 命令安装 bind 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@server7-2～]# yum clean all                    //安装前先清除缓存
[root@ server7-2  ～]# yum    install    bind    bind-chroot -y
```

（2）安装完后再次查询，发现已安装成功。

```
[root@ server7-2  ～]# rpm -qa|grep bind
```

（3）修改网络设置模式均设置为自定义 VMnet1 仅主机模式



二、在辅助服务器虚拟主机， 启动 DNS 服务并设置开机自启动

▶ [root@server7-2 ～]# **systemctl start named**

▶ [root@ server7-2～]# **systemctl enable named**

```
[root@server7-2 ~]# systemctl start named
[root@server7-2 ~]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service t
o /usr/lib/systemd/system/named.service.
[root@server7-2 ~]#
```

三. 修改主配置文件/etc/named.conf

DNS 配置文件分为全局配置文件、主配置文件和正反向解析区域声明文件。

1. 修改主配置文件/etc/named.conf

[root@server7-1 ～]# vim /etc/named.conf

```
        options {
        listen-on port 53 { any; };    //修改 listen 侦听地址为 any，侦听所有主机端口
        listen-on-v6 port 53 { ::1; };        //限于 IPv6
        directory "/var/named";                    //指定区域配置文件所在的路径
       dump-file  "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query { any; };       //修改辅助 DNS 服务器允许客户端主机为 any，侦听任意网段。
        recursion yes;       //递归 DNS 查询
```

```
dnssec-enable     yes;
dnssec-validation     no;                    //改为 no 可以忽略 SELinux 影响
dnssec-lookaside     auto;……
};
//以下用于指定 BIND 服务的日志参数
 logging {
          channel default_debug {
                    file "data/named.run";
                    severity dynamic;
          };
};
//重要的操作是添加 zone 区域
 zone "." IN {   //用于指定根服务器的配置信息，解析当前跟区域，一般不能改动
 type hint;
 file "named.ca";     // named.ca 文件存放全球 13 台根域服务器地址和主机名的对应关系
};
zone "rjlinux.com" IN {       //添加区域名称为 rjlinux.com
 type slave;                  //类型设为 slave
 file " slaves/rjlinux.com.zone";     //文件名设为 slaves/rjlinux.com.zone
 masters { 192.168.1.2; } ;           //指向主 DNS 服务器地址
};
include "/etc/named.zones";
include "/etc/named.root.key";
保存退出
```

四、验证辅助 DNS 服务器 server7-2 和主 DNS 服务器 server7-1，实现数据同步。

1. 重新启动 named 服务：

▶ [root@server7-2 ~]# **systemctl restart named**

2. 在辅助 DNS 服务器验证和主 DNS 服务器同步

```
[root@server7-2 named]# cd slaves
[root@server7-2 slaves]# ll
-rw-r--r--. 1 named named 421 4 月   25 02:34 rjlinux.com.zone
```

```
[root@server7-2 slaves]# cat rjlinux.com.zone
rjlinux com  dnsrjlinux com*   Q@   cwrjlinux com @@    :@*04   Q@
*   Q@   xsrjlinux com @@                        +   Q@   dnsrjlinux com @@  ,   Q@   dns2rjlinux com @@  *   Q@   jlrjlinux com @@
```

五、设置开机自动加载，配置主 DNS 服务器的防火墙策略，添加允许 DNS 服务，并永久生效。

[root@server7-2 slaves]# systemctl enable named

```
[root@server7-2 slaves]# firewall-cmd --permanent --add-service=dns
success
[root@server7-2 slaves]# firewall-cmd --reload
success
[root@server7-2 slaves]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client dns ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

六、使用 nslookup 验证辅助 DNS 服务器上所有域名的地址解析。结果如下图

```
[root@server7-2 slaves]# nslookup
> server
Default server: 192.168.1.3
Address: 192.168.1.3#53
> dns2.rjlinux.com
Server:         192.168.1.3
Address:        192.168.1.3#53

Name:   dns2.rjlinux.com
Address: 192.168.1.3
> cw.rjlinux.com
Server:         192.168.1.3
Address:        192.168.1.3#53

Name:   cw.rjlinux.com
Address: 192.168.1.11
> xs.rjlinux.com
Server:         192.168.1.3
Address:        192.168.1.3#53

Name:   xs.rjlinux.com
Address: 192.168.1.12
> oa.rjlinux.com
Server:         192.168.1.3
Address:        192.168.1.3#53

Name:   oa.rjlinux.com
Address: 192.168.1.13
> jl.rjlinux.com
Server:         192.168.1.3
Address:        192.168.1.3#53

Name:   jl.rjlinux.com
Address: 192.168.1.13
>
```