项目 5-配置与管理 DNS 服务器-实训任务指导书（5-1）

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

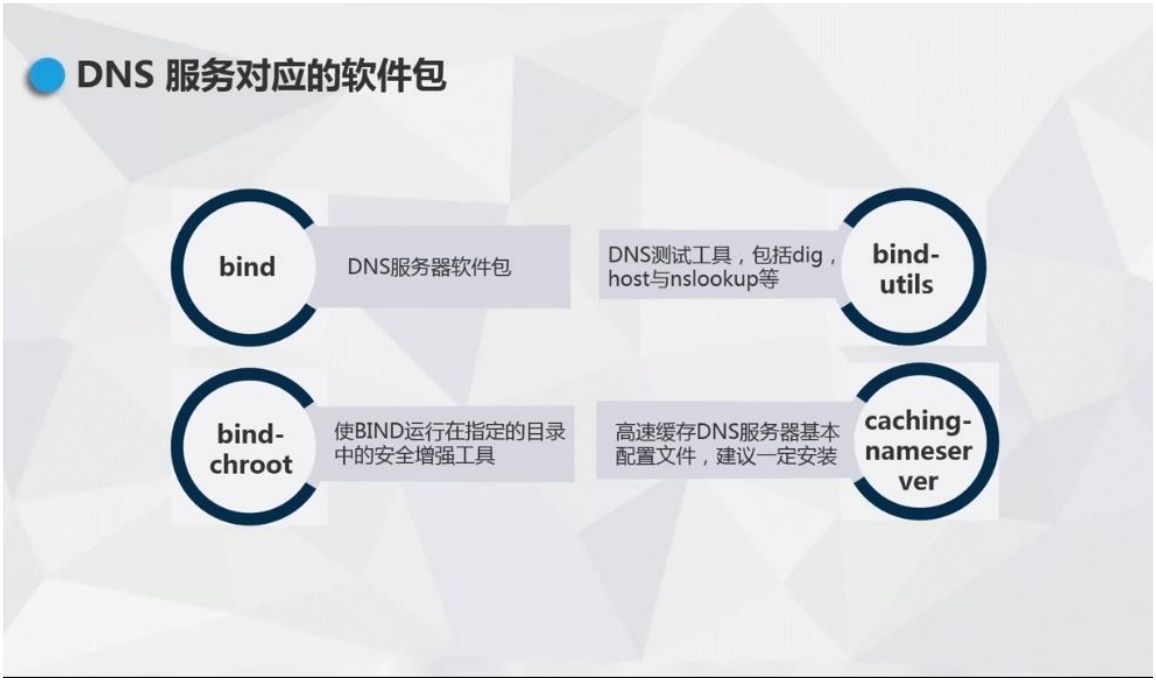
具体实训步骤：

子任务一、配置主 DNS 服务器实例

域名服务器是指保存有该网络中所有主机的域名和对应 IP 地址,并具有将域名转换为 IP 地址功能的服务器。其中域名必须对应一个 IP 地址,而 IP 地址不一定有域名。主服务器托管控制区域文件，该文件包含域的所有权威信息（这意味着它是重要信息的可信源，例如域的 IP 地址）。这包括重要信息，例如域的 IP 地址以及负责该域管理的人员。主服务器直接从本地文件获取此信息。只能在主服务器上更改区域的 DNS 记录，然后主服务器才能更新辅助服务器。

一、在主 DNS 服务器上安装 DNS 服务，并启动服务

在 Linux 下架设 DNS 服务器通常使用 BIND（Berkeley Internet Name Domain）程序来实现，其守护进程是 named。bind 软件包，BIND 是一款实现 DNS 服务器的开放源码软件。



1．在主 DNS 服务器虚拟机上安装 bind 软件包

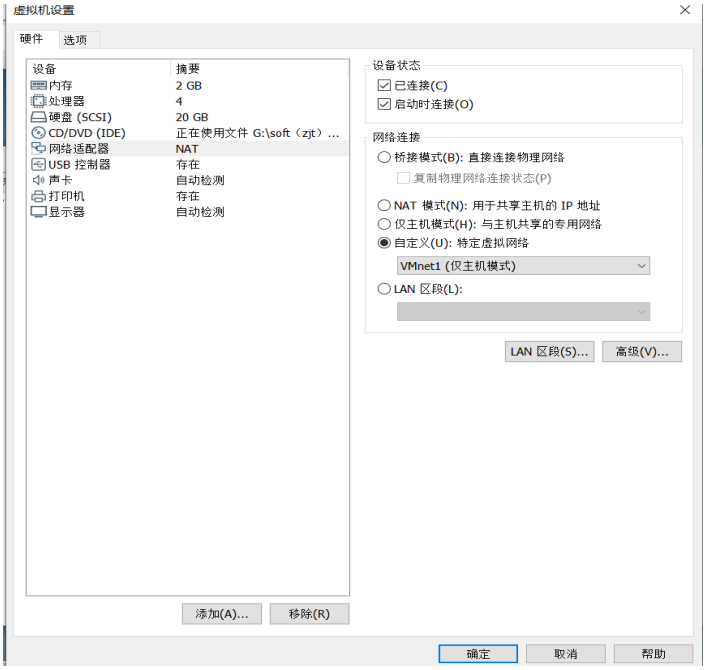
（1）使用 yum 命令安装 bind 服务。（网络 NAT 模式下，可选用 ens33 连接）

```
[root@RHEL7-1 ～]# yum clean all                    //安装前先清除缓存
[root@RHEL7-1 ～]# yum  install  bind  bind-chroot -y
```

（2）安装完后再次查询，发现已安装成功。

[root@RHEL7-1 ～]# rpm -qa|grep bind

（3）安装软件包完成后，修改网络设置模式均设置为自定义 VMnet1 仅主机模式。



二、在主服务器虚拟主机， 启动 DNS 服务并设置开机自启动

▶ [root@RHEL7-1 ～]# **systemctl start named**

▶ [root@RHEL7-1 ～]# **systemctl enable named**

```
[root@server7-1 ~]# systemctl   start  named
[root@server7-1 ~]# systemctl   enable  named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service t
o /usr/lib/systemd/system/named.service.
```

三. 修改主配置文件/etc/named.conf 和主数据文件

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
        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 { 192.168.1.0/24; };          //修改主 DNS 服务器允许客户端主机为内网主机网段 192.168.1.0/24；辅助 DNS 服务器允许客户端主机为 any。
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";
};
zone "rjlinux.com" IN {       //添加区域名称为 rjlinux.com
 type master;                 //类型设为 master
 file "rjlinux.com.zone";     //文件名设为 rjlinux.com.zone
};
include "/etc/named.zones";      //指定主配置文件，一定根据实际修改
include "/etc/named.root.key";
保存退出
```

2. 配置主数据文件

```
[root@server7-1 ~]# cd /var/named
[root@server7-1 named]# ll
总用量 16
drwxrwx---. 2 named named   23 4月   24 16:52 data
drwxrwx---. 2 named named   60 4月   24 16:52 dynamic
-rw-r-----. 1 root  named 2253 4月    5 2018 named.ca
-rw-r-----. 1 root  named  152 12月  15 2009 named.empty
-rw-r-----. 1 root  named  152 6月   21 2007 named.localhost
-rw-r-----. 1 root  named  168 12月  15 2009 named.loopback
drwxrwx---. 2 named named    6 2月   24 01:17 slaves
```

```
[root@server7-1 named]# cp named.localhost rjlinux.com.zone -p
```

带-p 选项，复制同时改变组的权限为named

```
[root@server7-1 named]# ll
总用量 20
drwxrwx---. 2 named named   23 4月   24 16:52 data
drwxrwx---. 2 named named   60 4月   24 16:52 dynamic
-rw-r-----. 1 root  named 2253 4月    5 2018 named.ca
-rw-r-----. 1 root  named  152 12月  15 2009 named.empty
-rw-r-----. 1 root  named  152 6月   21 2007 named.localhost
-rw-r-----. 1 root  named  168 12月  15 2009 named.loopback
-rw-r-----. 1 root  named  152 6月   21 2007 rjlinux.com.zone
drwxrwx---. 2 named named    6 2月   24 01:17 slaves
[root@server7-1 named]# vim rjlinux.com.zone
```

```
$TTL 1D
@       IN SOA  dns.rjlinux.com.  root.rjlinux.com. (
                                        1       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      dns.rjlinux.com.
dns     A       192.168.1.2
dns2    A       192.168.1.3
cw      A       192.168.1.11
xs      A       192.168.1.12
jl      A       192.168.1.13
oa      A       192.168.1.13
```

保存退出

3.重启域名服务 named，并设置开机自动加载。

```
[root@server7-1 named]# systemctl restart named
[root@server7-1 named]# systemctl enable named
```

四.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@server7-1 named]# firewall-cmd --permanent --add-service=dns
success
[root@server7-1 named]# firewall-cmd --reload
success
[root@server7-1 named]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens33
  sources:
  services: dhcpv6-client dns http ssh
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

五、查看端口，并使用 nslookup 命令验证测试解析结果

Nslookup 是一个监测网络中 DNS 服务器是否能正确实现域名解析的命令行工具。

①.使用 **netstat** 命令查看 **53** 号端口，并使用 **ping** 命令验证域名解析

```
[root@server7-1 named]# netstat -an |grep :53
tcp        0      0 192.168.1.2:53          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
tcp6       0      0 ::1:53                  :::*                    LISTEN
udp        0      0 0.0.0.0:5353            0.0.0.0:*
udp        0      0 192.168.122.1:53        0.0.0.0:*
udp        0      0 192.168.1.2:53          0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp        0      0 192.168.122.1:53        0.0.0.0:*
udp6       0      0 ::1:53                  :::*
[root@server7-1 named]# ping xs.rjlinux.com
PING xs.rjlinux.com (192.168.1.12) 56(84) bytes of data.
```

②.使用 **nslookup** 命令查看本任务全部域名解析情况

```
[root@server7-1 named]# nslookup
> xs.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   xs.rjlinux.com
Address: 192.168.1.12
> cw.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   cw.rjlinux.com
Address: 192.168.1.11
> jl.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   jl.rjlinux.com
Address: 192.168.1.13
> oa.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   oa.rjlinux.com
Address: 192.168.1.13
> dns.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   dns.rjlinux.com
Address: 192.168.1.2
> dns2.rjlinux.com
Server:         192.168.1.2
Address:        192.168.1.2#53

Name:   dns2.rjlinux.com
Address: 192.168.1.3
>
```