Linux服务器构建与运维管理

第08章：域名服务器

阮晓龙

13938213680 / ruanxiaolong@hactcm.edu.cn

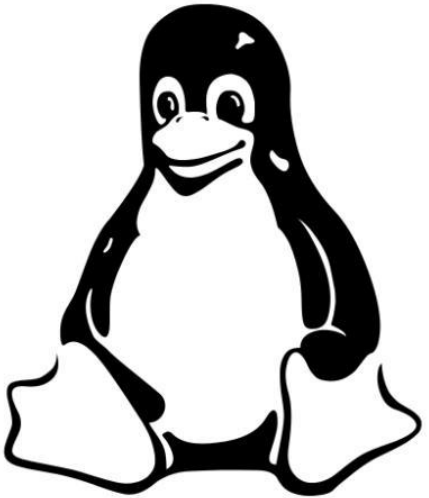
https://internet.hactcm.edu.cn
http://www.51xueweb.cn

河南中医药大学信息管理与信息系统教研室
河南中医药大学信息技术学院互联网技术教学团队
河南中医药大学医疗健康信息工程技术研究所

2022.10

提纲

- 什么是DNS
  - DNS简介
  - DNS查询
  - 域名解析
- 域名记录类型
- 实现DNS查询与域名解析
  - 任务1：安装BIND
  - 任务2：使用BIND实现DNS查询服务
  - 任务3：使用BIND实现域名解析服务
- 智能解析与高可用
  - 任务4：使用BIND实现智能解析
  - 任务5：域名解析服务的高可靠性



1.什么是DNS

- DNS是互联网的一项重要服务，DNS客户端与DNS服务端进行请求--响应的通信时，遵循DNS协议规范。
- 安装DNS服务端软件的设备叫做DNS服务器。

- DNS主要功能是提供域名解析和DNS查询两项服务。
  - DNS服务器中保存着域名和IP地址的对应关系，根据请求把域名转换成为IP地址的过程叫做域名解析。
  - DNS客户端发起域名解析请求并得到查询结果的过程叫做DNS查询。

1.什么是DNS

- 在DNS系统里，提供DNS服务的主机被称为DNS服务器或域名服务器，而提出“域名查询”请求的主机，被称为DNS客户端。
  - 本地主机访问一个网站时，通常是输入域名地址，而不是IP地址。
  - 本地主机会首先调用DNS客户端软件查询本地hosts文件，如果里面有对应的域名记录则直接使用，如果没有则会把域名解析请求发送到本地域名服务器进行查询。
  - 本地域名服务器查询自身的资源记录或者向上查询，最后把结果返回给本地主机的DNS客户端软件。
  - 本地主机获得网站域名地址对应的IP地址后，向网站服务器的IP地址发送访问网站的请求。

1.什么是DNS

- DNS查询方式
  - DNS客户端软件向本地域名服务器的查询一般采用递归查询。
    - DNS客户端软件向本地域名服务器发出DNS查询请求，如果本地域名服务器能够解析就直接返回结果，如果不能，本地域名服务器就代替去其他的域名服务器进行查询（其他的域名服务器是递归查询还是迭代查询由其自身决定），直到查询到结果后返回给主机。
  - 本地域名服务器向根域名服务器的查询通常采用迭代查询。
    - 本地域名服务器向根域名服务器进行DNS查询，根域名服务器告诉本地域名服务器去哪里查询能够得到结果，而不是替本地域名服务器进行查询。

1.什么是DNS

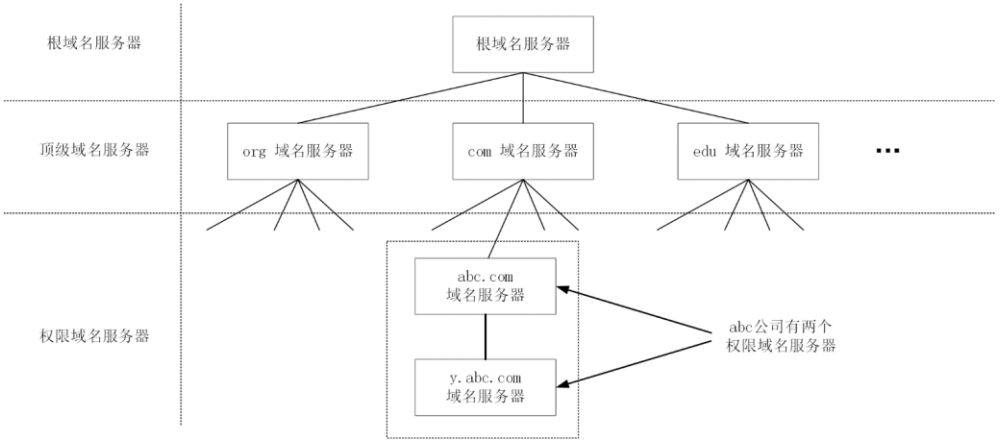
- 本地域名服务器
  - 本地域名服务器一般是指DNS客户端上网时IPv4或者IPv6设置中填写的首选DNS，是手工指定的或者是DHCP自动分配的。
  - 如果DNS客户端是直连运营商网络，一般情况下默认设置DNS为DHCP分配到的运营商的域名服务器地址。
  - 如果DNS客户端和运营商之间有无线路由器，通常无线路由器本身内置DNS转发器，其作用是将收到的所有DNS请求转发到上层DNS服务器，此时主机的本地域名服务器地址配置为无线路由器的地址。无线路由器的DNS转发器将请求转发到上层ISP的DNS服务器或无线路由器内设定的DNS服务器。

1.什么是DNS

- 域名到IP地址的解析是由分布在因特网上的许多域名服务器程序共同完成的。
  - 域名服务器程序在专设的结点上运行，通常把运行域名服务器程序的机器称为域名服务器。
  - 域名服务器是一个分布式的提供域名查询服务的数据库，域名解析实质就是在数据库中建立域名和IP地址之间联系的过程。
  - 只有在数据库中建立了解析记录，其他的客户机才能通过DNS服务器查询到与域名相对应的IP地址，进而访问目的主机。

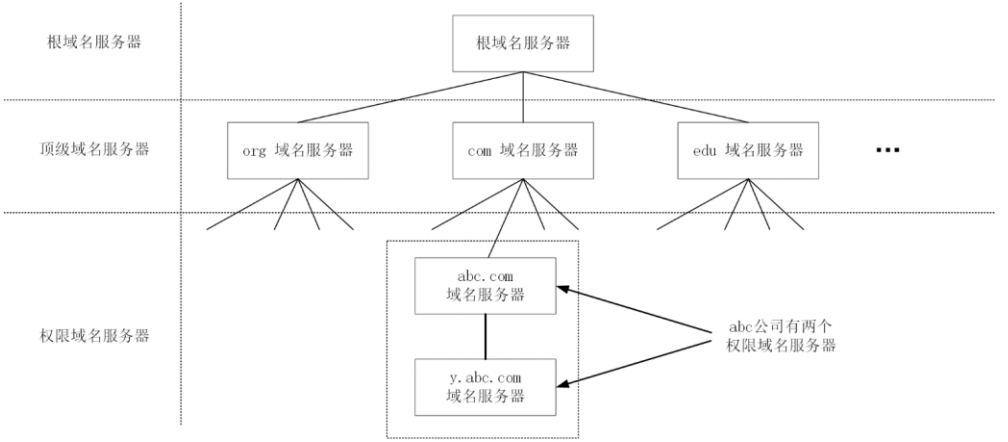
1.什么是DNS

- 域名服务器分四种：根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器。
  - 理论上，所有域名查询都必须先查询根域名，所有的顶级域名和IP地址对应关系都保存在DNS根区文件中，保存DNS根区文件的服务器叫做根域名服务器。
  - 顶级域名服务器保存下设的二级域名和IP地址对应关系，每一个二级域名都设有权限域名服务器，保存域名下所有子域名和主机名对应的IP地址。



1.什么是DNS

- 域名服务器分四种：根域名服务器、顶级域名服务器、权限域名服务器和本地域名服务器。
  - 本地域名服务器并不属于域名服务器层次结构，但它对域名系统非常重要。
  - 当一个主机发出DNS查询请求时，查询请求报文就发送给本地域名服务器，由本地域名服务器作下一步处理。



2.域名记录

- NS记录
  - 名称服务器（Name Server，NS）资源记录定义了该域名由哪个DNS服务器负责解析，NS资源记录定义的服务器称为权限域名服务器。
  - 权限域名服务器负责维护和管理所管辖区域中的数据，它被其他服务器或客户端当作权威的来源，为DNS客户端提供数据查询，并且能肯定应答区域内所含名称的查询。

- SOA记录
  - SOA是Start of Authority（起始授权机构）的缩写，是主要名称区域文件中必须设定的资源记录，表示创建它的DNS服务器是主要名称服务器。
  - SOA资源记录定义了域名数据的基本信息和属性（更新或过期间隔）。通常应将SOA资源记录放在区域文件的第一行或紧跟在$ttl选项之后。

2.域名记录

- A记录
  - 主机地址（Address，A）资源记录是最常用的记录，定义域名记录对应IP地址的信息。
    - dns IN A 192.168.16.15
    - www.example.com. IN A 192.168.16.243
    - mail.example.com. IN A 192.168.16.156
  - 在上面的例子中，使用了两种方式定义A资源记录：一种是使用相对名称，另一种是使用完全规范域名（Fully Qualifiied Domain Name，FQDN）。这两种方式只是书写形式不同而已，在使用上没有任何区别。

- AAAA记录
  - AAAA记录（AAAA record）是用来定义域名记录对应IPv6地址的记录。用户可以将一个域名记录解析为IPv6地址，也可以将子域名解析为IPv6地址。

2.域名记录

- MX记录
  - 邮件交换器（Mail eXchanger，MX）资源记录指向一个邮件服务器，用于电子邮件系统发邮件时根据收件人邮件地址后缀来定位邮件服务器。例如，当一个邮件要发送到地址linux@example.com时，邮件服务器通过DNS服务查询example.com域名的MX资源记录，如果MX资源记录存在，邮件就会发送到MX资源记录所指向的邮件服务器上。
  - 可以设置多个MX资源记录，指明多个邮件服务器，优先级别由MX后的0-99的数字决定，数字越小，邮件服务器的优先级别越高。优先级别高的邮件服务器是邮件传送的主要对象，当邮件传送给优先级高的邮件服务器失败时，再依次传送给优先级别低的邮件服务器。
  - 由于MX资源记录值登记了邮件服务器的域名，而在邮件实际传输时，是通过邮件服务器的IP地址进行通信的，因此邮件服务器还必须在区域文件中有一个A资源记录，以指明邮件服务器的IP地址，否则会导致传输邮件失败。

2.域名记录

- PTR记录
  - PTR（Pointer Record）指针记录，执行通过IP查询域名的解析。
  - 原则上，PTR记录与A记录是相匹配的，一条A记录对应一条PTR记录，两者不匹配或者遗漏PTR记录会导致依赖域名的业务系统服务性能降低。

- CNAME记录
  - 别名（Canonical Name，CNAME）资源记录也被称为规范名字资源记录。CNAME资源记录允许将多个名称映射到同一台计算机上。
  - 例如，对于同时提供Web、Samba和BBS服务的计算机（IP地址为192.168.16.9），可以建立一条A记录“www.example.com. IN A 192.168.16.9”，并设置两个别名bbs和samba，即建立两条CNAME记录“samba IN CNAME www”和“bbs IN CNAME www”，实现不同服务对应不同域名记录，但访问的是同一个IP地址。

2.域名记录

- SRV记录
  - SRV记录的作用是指明某域名下提供的服务，一般应用于Windows的域架构。
  - Windows域架构下，DNS服务器会用SRV记录保存域控制器的名称，并且建立域控制器时会注册SRV纪录，否则域控制器和DNS服务器互相无法识别。

- TXT记录
  - TXT记录，指为某个主机名或域名设置的说明。
  - 它的重要应用场景之一是设置SPF记录，以防止邮件服务器发送的邮件被当作垃圾邮件。

3.实现DNS查询与域名解析

任务1：安装BIND

任务2：使用BIND实现DNS查询服务

任务3：使用BIND实现域名解析服务

3.实现DNS查询与域名解析

任务1：安装BIND

- 步骤1：创建虚拟机并完成CentOS的安装
- 步骤2：完成虚拟机的主机配置、网络配置及通信测试
- 步骤3：通过在线方式安装BIND
- 步骤4：启动BIND
- 步骤5：查看BIND运行信息
- 步骤6：配置named服务为开机自启动

操作视频 / 现场演示

- 任务1：安装BIND
  - 任务目标
    - 完成BIND的安装
    - 完成BIND的配置

命令指南 / 操作引导

```
1. [root@Project-08-Task-01 ~]# yum install -y bind

2. [root@Project-08-Task-01 ~]# systemctl start named
3. [root@Project-08-Task-01 ~]# systemctl status named

4. [root@Project-08-Task-01 ~]# systemctl enable named.service
5. [root@Project-08-Task-01 ~]# systemctl is-enabled named.service
6. [root@Project-08-Task-01 ~]# systemctl list-unit-files | grep named.service
```

3.实现DNS查询与域名解析

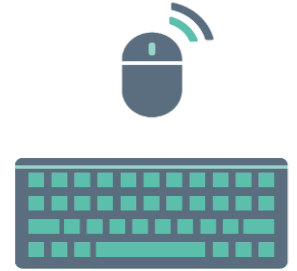
任务2：使用BIND实现DNS查询服务

- 步骤1：实现DNS查询服务配置
- 步骤2：重新载入BIND的配置文件
- 步骤3：在服务器上安装DNS测试工具dig
- 步骤4：DNS查询测试

操作视频 / 现场演示

- 任务2：使用BIND实现DNS查询服务
  - 任务目标
    - 实现DNS查询服务
    - 实现dig工具进行DNS查询服务的测试

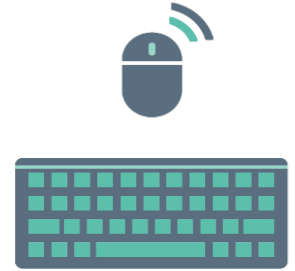
配置BIND的主配置文件



命令指南 / 操作引导

```
[root@Project-08-Task-01 ~]# cp /etc/named.conf /etc/named.conf.bak1
[root@Project-08-Task-01 ~]# vi /etc/named.conf

配置文件：/etc/named.conf
#named.conf配置文件内容较多，本部分仅显示与DNS查询配置有关的内容
options {
#修改监听地址为服务器IP
#IPV4的监听地址
listen-on port 53 { 10.10.2.120; };
#IPV6的监听地址
listen-on-v6 port 53 { ::1; };
#定义区域文件存储目录
directory       "/var/named";
#定义本域名服务器在收到rndc dump命令时，转存数据的文件路径
dump-file       "/var/named/data/cache_dump.db";
#定义本域名服务器在收到rndc stats命令时，追加统计数据的文件路径
statistics-file "/var/named/data/named_stats.txt";
#定义本域名服务器在退出时，将内存统计写到文件的路径
memstatistics-file "/var/named/data/named_mem_stats.txt";
#定义本域名服务器在收到rndc secroots命令时，转存安全根的文件路径
secroots-file   "/var/named/data/named.secroots";
#定义本域名服务器在收到rndc recursing命令时，转存当前递归请求的文件路径
recursing-file  "/var/named/data/named.recursing";
#修改授权访问范围为允许所有地址可以访问
#定义哪些主机可以进行DNS查询
allow-query     {any; };
};

[root@Project-08-Task-01 ~]# systemctl reload named
[root@Project-08-Task-01 ~]# firewall-cmd --permanent --zone=public --add-service=dns
[root@Project-08-Task-01 ~]# firewall-cmd --reload
```

使用dig进行DNS查询测试



命令指南 / 操作引导

```
[root@Project-08-Task-01 ~]# yum install -y bind-utils

[root@Project-08-Task-01 ~]# dig -t A www.baidu.com @10.10.2.120
#dig的版本号和要查询的域名
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el8 <<>> -t A www.baidu.com
#表示可以在命令后面加选项，缺省情况下显示注释
;; global options: +cmd
#以下是返回信息的内容
;; Got answer:
#返回信息的头部，总计有1条查询内容，4条应答内容，13条授权域名，27条附加内容
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29402
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 13, ADDITIONAL: 27
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 5b5b4d695823da0c5577361d5e455add890c2f38bd8ecb7a (good)
#查询内容
;; QUESTION SECTION:
;www.baidu.com.                 IN      A
#下述查询出的4条应答内容和13条权威域名表示查询成功
#应答内容
;; ANSWER SECTION:
www.baidu.com.          423     IN      CNAME   www.a.shifen.com.
#为了排版方便此处删除了部分提示信息
#附加内容
;; ADDITIONAL SECTION:
a.root-servers.net.     95610   IN      A       198.41.0.4
#为了排版方便此处删除了部分提示信息
;; Query time: 833 msec                 #查询耗时
;; SERVER: 10.10.2.120#53(10.10.2.120)  #所使用DNS服务器地址和端口
;; WHEN: Thu Feb 13 22:19:09 CST 2020   #查询时间
;; MSG SIZE  rcvd: 932                  #应答大小
```

3.实现DNS查询与域名解析

任务3：使用BIND实现域名解析服务

- 步骤1：实现域名解析服务配置
- 步骤2：实现domain.com域名和记录的配置
- 步骤3：实现demo.cn域名和记录的配置
- 步骤4：校验并重新载入BIND配置文件
- 步骤5：在服务器上测试域名解析服务
- 步骤6：在本地主机测试域名解析服务

表 8-3-1 域名规划表

域名	缓存有效期	SOA	
domain.com	1 天	权威域名	ns.domain.com.
		管理员邮箱	root.domain.com.
		版本号（serial）	0
		主辅同步周期（refresh）	1 天
		主辅同步重试间隔（retry）	1 小时
		同步数据存活期（expire）	1 周
		最小缓存有效期（minimum）	3 小时
demo.cn	1 天	权威域名	ns.demo.cn.
		管理员邮箱	root.demo.cn.
		版本号（serial）	0
		主辅同步周期（refresh）	1 天
		主辅同步重试间隔（retry）	1 小时
		同步数据存活期（expire）	1 周
		最小缓存有效期（minimum）	3 小时

表 8-3-2 domain.com 记录规划表

记录类型	记录值	解析地址
NS	ns.domain.com	
MX	mail.domain.com	
A	ns.domain.com	10.10.2.120
A	mail.domain.com	10.10.3.200
A	www.domain.com	10.10.3.200
A	ftp.domain.com	10.10.3.200
AAAA	www.domain.com	1080::8:800:200C:417A
CNAME	web.domain.com	www.domain.com

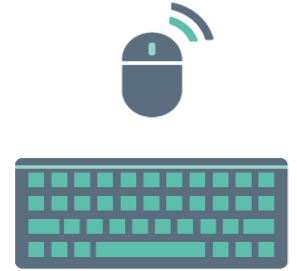
表 8-3-3 demo.cn 记录规划表

记录类型	记录值	解析地址
NS	ns.demo.cn	
MX	mail.demo.cn	
A	ns.demo.cn	10.10.2.120
A	mail.demo.cn	10.10.4.200
A	www.demo.cn	10.10.4.200
A	ftp.demo.cn	10.10.4.200
AAAA	www.demo.cn	FF60:0:0:0610:BC:0:0:05D7
CNAME	web.demo.cn	www.demo.cn

操作视频 / 现场演示

- 任务3：使用BIND实现域名解析服务
  - 任务目标
    - 实现域名解析服务
    - 实现域名解析服务的测试

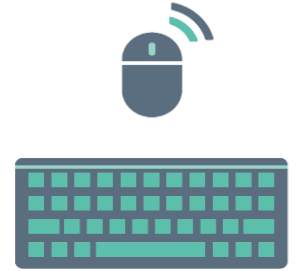
配置BIND的主配置文件



命令指南 / 操作引导

```
配置文件：/etc/named.conf
#named.conf配置文件内容较多，本部分仅显示与域名解析配置有关的内容
#设置domain.com正向解析
zone "domain.com" IN {
type master;
file "domain.com.zone";
allow-update { none; };
};
#设置domain.com反向解析
zone "3.10.10.in-addr.arpa" IN {
type master;
file "10.10.3.zone";
allow-update { none; };
};
#设置demo.cn正向解析
zone "demo.cn" IN {
type master;
file "demo.cn.zone";
allow-update { none; };
};
#设置demo.cn反向解析
zone "4.10.10.in-addr.arpa" IN {
type master;
file "10.10.4.zone";
allow-update { none; };
};
```

domain.com域名与记录配置

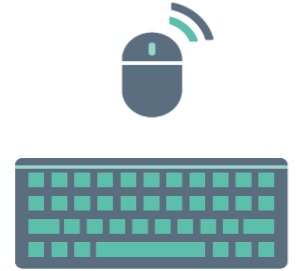


命令指南 / 操作引导

```
[root@Project-08-Task-01 ~]# cp /var/named/named.localhost /var/named/domain.com.zone
[root@Project-08-Task-01 ~]# chown named.named /var/named/domain.com.zone
[root@Project-08-Task-01 ~]# chmod 640 /var/named/domain.com.zone
[root@Project-08-Task-01 ~]# vi /var/named/domain.com.zone
```

配置文件：/var/named/domain.com.zone

```
; 定义从本域名服务器查询的记录，在客户端缓存有效期为1天
$TTL 1D
; 设置起始授权机构的权威域名和管理员邮箱
@       IN  SOA         ns.domain.com. root.domain.com. (
                0               ; 定义本配置文件的版本号为0，该值在同步辅域名服务器时使用
                1D              ; 定义本域名服务器与辅域名服务器同步的时间周期为1天
                1H              ; 定义辅域名服务器更新失败时，重试间隔时间为1小时
                1W              ; 定义辅域名服务器从本域名服务器同步的数据，存活期为1周
                3H      )       ; 定义从本域名服务器查询的记录，在客户端缓存有效期为3小时
                                ;如果第一行没有定义$TTL;，则使用该值
; NS记录
@               IN      NS              ns.domain.com.
; MX记录
@               IN      MX 10   mail.domain.com.
; A记录
ns              IN      A               10.10.2.120
mail            IN      A               10.10.3.200
www             IN      A               10.10.3.200
ftp             IN      A               10.10.3.200
; AAAA记录
www             IN      AAAA            1080::8:800:200C:417A
; CNAME记录
web             IN      CNAME           www.domain.com.
```

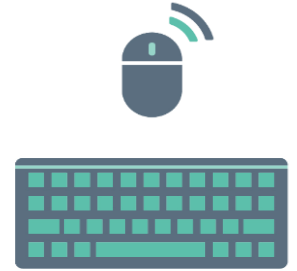


命令指南 / 操作引导

```
[root@Project-08-Task-01 ~]# cp /var/named/named.loopback /var/named/10.10.3.zone
[root@Project-08-Task-01 ~]# chown named.named /var/named/10.10.3.zone
[root@Project-08-Task-01 ~]# chmod 640 /var/named/10.10.3.zone
[root@Project-08-Task-01 ~]# vi /var/named/10.10.3.zone

配置文件：/var/named/10.10.3.zone
; 定义从本域名服务器查询的记录，在客户端缓存有效期为1天
$TTL 1D
; 设置起始授权机构的权威域名和管理员邮箱
@       IN  SOA         ns.domain.com. root.domain.com. (
                0               ; 定义本配置文件的版本号为0，该值在同步辅域名服务器时使用
                1D              ; 定义本域名服务器与辅域名服务器同步的时间周期为1天
                1H              ; 定义辅域名服务器更新失败时，重试间隔时间为1小时
                1W              ; 定义辅域名服务器从本域名服务器同步的数据，存活期为1周
                3H      )       ; 定义从本域名服务器查询的记录，在客户端缓存有效期为3小时
                                ;如果第一行没有定义$TTL;，则使用该值
; NS记录
@               IN      NS              ns.domain.com.
; PTR记录
120             IN      PTR             ns.domain.com.
200             IN      PTR             mail.domain.com.
```

demo.cn域名和记录的配置

检验配置文件的正确性



命令指南 / 操作引导

```
#对主配置文件进行正确性校验
[root@Project-08-Task-01 ~]# named-checkconf /etc/named.conf
#对域名domain.com的正向域名区域配置文件进行正确性校验
[root@Project-08-Task-01 ~]# named-checkzone domain.com  /var/named/domain.com.zone
#对域名domain.com的反向域名区域配置文件进行正确性校验
[root@Project-08-Task-01 ~]# named-checkzone 3.10.10.in-addr.arpa  /var/named/10.10.3.zone
#对域名demo.cn的正向域名区域配置文件进行正确性校验
[root@Project-08-Task-01 ~]# named-checkzone demo.cn  /var/named/demo.cn.zone
#对域名demo.cn的反向域名区域配置文件进行正确性校验
[root@Project-08-Task-01 ~]# named-checkzone 4.10.10.in-addr.arpa  /var/named/10.10.4.zone

#通过systemctl reload命令重新载入named服务
[root@Project-08-Task-01 ~]# systemctl reload named
```

使用dig和nslookup工具进行测试

表 8-3-4 域名解析服务测试结果

序号	测试命令	预期结果	测试是否通过
1	dig www.domain.com @10.10.2.120	10.10.3.200	√
2	dig -t NS domain.com @10.10.2.120	ns.domain.com.	√
3	dig -t MX domain.com @10.10.2.120	mail.domain.com.	√
4	dig -t AAAA www.domain.com @10.10.2.120	1080::8:800:200c:417a	√
5	dig -t CNAME web.domain.com @10.10.2.120	www.domain.com.	√
6	dig -x 10.10.3.200 @10.10.2.120	mail.domain.com.	√

表 8-3-5 域名解析服务测试结果

序号	测试命令	预期结果	测试是否通过
1	nslookup www.domain.com 10.10.2.120	1080::8:800:200c:417a 10.10.3.200	√
2	nslookup -q=NS domain.com 10.10.2.120	ns.domain.com	√
3	nslookup -q=MX domain.com 10.10.2.120	mail.domain.com	√
4	nslookup -q=AAAA www.domain.com 10.10.2.120	1080::8:800:200c:417a	√
5	nslookup -q=CNAME web.domain.com 10.10.2.120	www.domain.com	√
6	nslookup -qt=PTR 10.10.3.200 10.10.2.120	mail.domain.com	√

4.智能解析与高可靠

- view（视图）是 BIND 9的新功能，是一个在防火墙环境中非常有用的机制。视图能够根据请求对象的不同，返回不同的结果。
- 如果没有配置任何视图，BIND 9会自动创建默认视图，任何发送查询请求的主机所看到的都是该视图。

4.智能解析与高可靠

- 使用BIND 9提供的view功能可以实现根据不同的请求来源IP范围，实现同一个域名记录解析为不同的IP地址，view的主要应用场景有两个。
  - （1）需要将域名分成内网和外网两个不同的区域进行解析。
  - （2）在多个运营商或CDN网络上部署了镜像服务的业务，根据访问业务的用户所在位置，将域名解析为用户访问速度最快的镜像服务IP地址。
    - 例如：
      - 使用中国电信网络的用户请求域名解析，域名解析的结果为业务在中国电信网络上的镜像服务IP地址。
      - 使用中国联通网络的用户请求域名解析，域名解析的结果为业务在中国联通网络上的镜像服务IP地址。

4.智能解析与高可靠

- view的参数较多，但经常使用的参数有match-clients和zone。
  - match-clients
    - match-clients作用是匹配客户端地址。可以匹配很多形式的IP，比如内置变量any、localhost等，以及单个IP如1.1.1.1，某个网络段如61.0.0.0/8等等。
    - 如果匹配的IP很多，可以使用acl进行单独声明，也可以把IP列表信息放进数据库里再引用。

4.智能解析与高可靠

- view的参数较多，但经常使用的参数有match-clients和zone。
  - zone
    - zone语句定义了DNS服务器所管理的区，也就是哪一些域的域名是授权给该DNS服务器回答的。
    - 共有5种类型的区，由type子语句指定，具体名称和功能如下所示。
      - Master（主域）：主域用来保存某个区域（如www.domain.com）的数据信息。
      - Slave（辅域）：也叫次级域，数据来自主域，起备份作用。
      - Stub：Stub区与辅域相似，但它只复制主域的NS记录，而不是整个区数据。它不是标准DNS的功能，只是BIND 9软件提供的独有功能。
      - Forward（转发）：转发域中一般配置了forward和forwarders子句，用于把对该域的查询请求转由其他DNS服务器处理。
      - Hint：Hint域定义了一套最新的根DNS服务器地址，如果没有定义，DNS服务器会使用内建的根DNS服务器地址。

4.智能解析与高可靠

任务4：使用BIND实现智能解析

任务5：域名解析服务的高可靠性

4.智能解析与高可靠

任务4：使用BIND实现智能解析

- 步骤1：使用BIND实现DNS查询与域名解析服务
- 步骤2：配置特定区域域名记录
- 步骤3：配置通用区域域名记录
- 步骤4：校验并重新载入BIND的配置文件
- 步骤5：在主机A（10.10.2.121）上进行域名解析服务测试
- 步骤6：在主机B（10.10.2.10）测试域名解析服务

操作视频 / 现场演示

- 任务4：使用BIND实现智能解析
  - 任务目标
    - 实现BIND的view配置
    - 实现域名智能解析服务
    - 实现域名智能解析服务的测试

任务4通过BIND的view功能提供域名智能解析服务，功能满足下述要求。

① 提供domain.com域名解析服务。

② 当域名解析请求来自特定网络范围10.10.2.0/26时，域名domain.com执行特定区域的解析结果，如表8-4-1。

③ 当域名解析请求不是来自于特定网络范围时，域名domain.com执行通用区域的解析结果，如表8-4-1。

表 8-4-1 域名解析规划表

序号	domain.com 记录	记录类型	特定区域解析结果	通用区域解析结果
1	ns.domain.com	NS	10.10.2.120	10.10.2.120
2	www.domain.com	A	10.10.3.200	10.10.4.200
3	ftp.domain.com	A	10.10.3.201	10.10.4.201

任务4所需使用的服务器与主机：

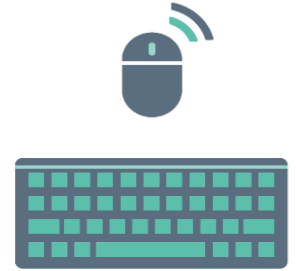
① 域名智能解析服务采用1台DNS服务器实现。

② 通过2台主机实现智能解析服务的测试。

服务器和测试主机的地址规划信息如表8-4-2所示。

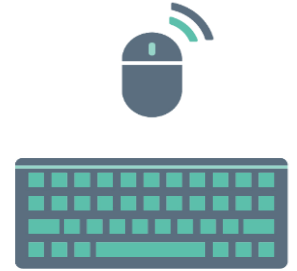
表 8-4-2 地址规划信息表

序号	主机	网络配置	用途
1	DNS 服务器	10.10.2.120	域名解析服务器
2	主机 A	10.10.2.121	域名解析测试
3	本地主机	10.10.2.10	域名解析测试



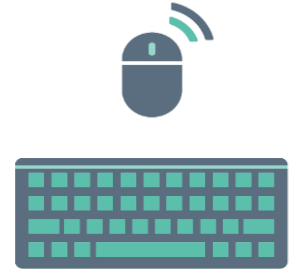
命令指南 / 操作引导

```
#Install Bind
yum install -y bind

#configure named
systemctl start named
systemctl enable named
systemctl status named
systemctl list-unit-files | grep named.service

#modify configuration file of named
cp /etc/named.conf /etc/named.conf.bak1
sed -i 's/127.0.0.1/10.10.2.120/g' /etc/named.conf
sed -i 's/localhost/any/g' /etc/named.conf
systemctl reload named

#turn off firewall tempporarilly
systemctl stop firewalld
setenforce 0

#install the dig tool，start DNS query test
yum install -y bind-utils
dig -t A www.baidu.com @10.10.2.120
```



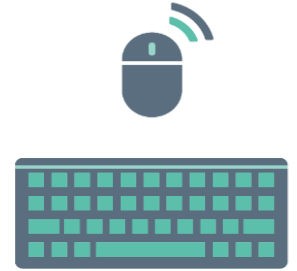
命令指南 / 操作引导

```
#configure intelligent domain name resolution service
sed -i '/zone "." IN {/,+3d' /etc/named.conf
sed -i '/named.rfc1912.zones/d' /etc/named.conf
cat >> /etc/named.conf <<EOF
view "area" {
    match-clients{10.10.2.0/26;};
    zone "." IN {
            type hint;
            file "named.ca";};
    zone "domain.com" IN {
            type master;
            file "com-domain-area";
            allow-update {none;};};
    zone "3.10.10.in-addr.arpa" IN {
            type master;
            file "10.10.3.area";};
};
view "common" {
    match-clients{any;};
    zone "." IN {
            type hint;
            file "named.ca";};
    zone "domain.com" IN {
            type master;
            file "com-domain-common";
            allow-update {none;};};
    zone "4.10.10.in-addr.arpa" IN {
            type master;
            file "10.10.4.common";};
};
EOF
```



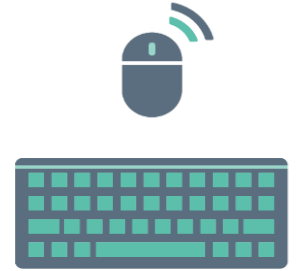
命令指南 / 操作引导

```
#configure the forward resolution zone profile com-domain-area
cp /var/named/named.localhost /var/named/com-domain-area
chown named.named /var/named/com-domain-area
chmod 640 /var/named/com-domain-area
cat > /var/named/com-domain-area <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        0 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
ns IN A 10.10.2.120
www IN A 10.10.3.200
ftp IN A 10.10.3.200
EOF

#configure the reverse resolution zone profile 10.10.3.area
cp /var/named/named.loopback /var/named/10.10.3.area
chown named.named /var/named/10.10.3.area
chmod 640 /var/named/10.10.3.area
cat > /var/named/10.10.3.area <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        0 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
120 IN PTR ns.domain.com.
200 IN PTR www.domain.com.
200 IN PTR ftp.domain.com.
EOF
```



命令指南 / 操作引导

```
#configure the forward resolution zone profile com-domain-area
cp /var/named/named.localhost /var/named/com-domain-common
chown named.named /var/named/com-domain-common
chmod 640 /var/named/com-domain-common
cat > /var/named/com-domain-common <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        0 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
ns IN A 10.10.2.120
www IN A 10.10.4.200
ftp IN A 10.10.4.200
EOF

#configure the reverse resolution zone profile 10.10.4.common
cp /var/named/named.loopback /var/named/10.10.4.common
chown named.named /var/named/10.10.4.common
chmod 640 /var/named/10.10.4.common
cat > /var/named/10.10.4.common <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        0 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
120 IN PTR ns.domain.com.
200 IN PTR www.domain.com.
EOF
```



命令指南 / 操作引导

```
#verify the correctness of the configuration file，reload named
named-checkconf /etc/named.conf
named-checkzone domain.com /var/named/com-domain-area
named-checkzone 3.10.10.in-addr.arpa /var/named/10.10.3.area
named-checkzone domain.com /var/named/com-domain-common
named-checkzone 4.10.10.in-addr.arpa /var/named/10.10.4.common
systemctl reload named

#start DNS query test
dig www.domain.com @10.10.2.120
dig -x 10.10.4.200 @10.10.2.120
```

4.智能解析与高可靠

任务5：域名解析服务的高可靠性

- 步骤1：创建虚拟机并完成CentOS 的安装
- 步骤2：完成虚拟机的主机配置、网络配置及通信测试
- 步骤3：实现DNS-Master
- 步骤4：实现DNS-Slave
- 步骤5：配置DNS-Master作为主域名解析服务
- 步骤6：配置DNS-Slave作为从域名解析服务

4.智能解析与高可靠

任务5：域名解析服务的高可靠性

- 步骤7：在DNS-Slave上查看主辅数据同步
- 步骤8：测试域名解析服务的可用性
- 步骤9：测试域名解析服务的可靠性

操作视频 / 现场演示

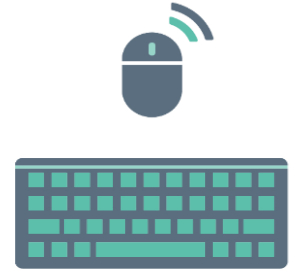
任务5：域名解析服务的高可靠性

- 任务目标
  - 实现主辅架构的域名解析服务
  - 实现主辅架构的域名解析服务的测试

命令指南 / 操作引导

```
#第1步：在DNS-Master上执行

# implementing DNS-Master
yum install -y bind
# view information
systemctl start named
systemctl status named | head -10
# set the boot
systemctl enable named.service
# view the status of the run
systemctl list-unit-files | grep named.service
# reload named
systemctl reload named
# stop firewalld
systemctl stop firewalld
setenforce 0
```

```
#第2步：在DNS-Slave上执行

# implementing DNS-Master
yum install -y bind
# view information
systemctl start named
systemctl status named | head -10
# set the boot
systemctl enable named.service
# view the status of the run
systemctl list-unit-files | grep named.service
# reload named
systemctl reload named
# stop firewalld
systemctl stop firewalld
setenforce 0
```

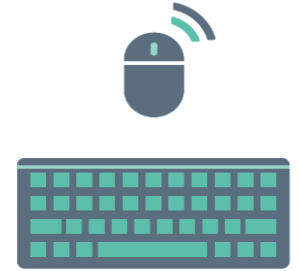


命令指南 / 操作引导

```
#第3步：在DNS-Master上执行

#configure DNS master as the primary domain name resolution service
#generate TSIG key on DNS master
cp -f /etc/named.conf /etc/named.conf.bak1
yum install -y bind-utils
tsig-keygen -a hmac-md5 area-key
tsig-keygen -a hmac-md5 common-key

#configure primary and secondary synchronization and view on DNS master
sed -i '/zone "." IN {/,+3d' /etc/named.conf
sed -i '/named.rfc1912.zones/d' /etc/named.conf
sed -i 's/127.0.0.1/10.10.2.120/g' /etc/named.conf
sed -i 's/localhost/any/g' /etc/named.conf
sed -i "/allow-query/a allow-transfer {10.10.2.122;};\nalso-notify {10.10.2.122;};\nnotify yes;\nmasterfile-format text;" /etc/named.conf

cat >> /etc/named.conf <<EOF

key "area-key" {
        algorithm hmac-md5;
        secret "areaSecret";
};

key "common-key" {
        algorithm hmac-md5;
        secret "commonSecret";
};

EOF
```

命令指南 / 操作引导

```
#第3步：在DNS-Master上执行

read -p "Please enter the secret value in the area-key: " areaSecret
sed -i 's#areaSecret#'"$areaSecret"'#g' /etc/named.conf
read -p "Please enter the secret value in the common-key: " commonSecret
sed -i 's#commonSecret#'"$commonSecret"'#g' /etc/named.conf

cat >> /etc/named.conf <<EOF

view "area" {
    match-clients{key area-key; 10.10.2.0/26;};
    server 10.10.2.122 { keys area-key; };
    zone "." IN {
            type hint;
            file "named.ca";
    };
    zone "domain.com" IN {
            type master;
            file "com-domain-area";
            allow-update {none;};
    };
    zone "3.10.10.in-addr.arpa" IN {
            type master;
            file "10.10.3.area";
    };
};
```

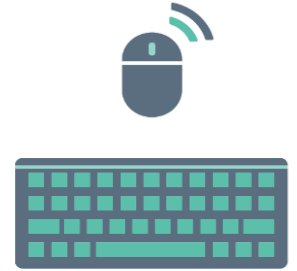


命令指南 / 操作引导

```
#第3步：在DNS-Master上执行

view "common" {
    match-clients { key common-key; any;};
    server 10.10.2.122 { keys common-key; };
    zone "." IN {
            type hint;
            file "named.ca";
    };
    zone "domain.com" IN {
            type master;
            file "com-domain-common";
            allow-update {none;};
    };
    zone "4.10.10.in-addr.arpa" IN {
            type master;
            file "10.10.4.common";
    };
};
EOF
#configure domain name records for specific zones on DNS master
cat > /var/named/com-domain-area <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
    1 ; serial
    1D ; refresh
    1H ; retry
    1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
@ IN NS ns1.domain.com.
ns IN A 10.10.2.120
ns1 IN A 10.10.2.122
www IN A 10.10.3.200
ftp IN A 10.10.3.200
EOF
```

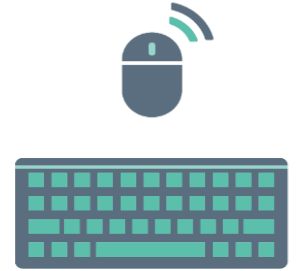
命令指南 / 操作引导

```
#第3步：在DNS-Master上执行

cat > /var/named/10.10.3.area <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        1 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
@ IN NS ns1.domain.com.
120 IN PTR ns.domain.com.
122 IN PTR ns1.domain.com.
200 IN PTR www.domain.com.
200 IN PTR ftp.domain.com.
EOF

#configure the universal zone domain name record on DNS master
cat > /var/named/com-domain-common <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        1 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
@ IN NS ns1.domain.com.
ns IN A 10.10.2.120
ns1 IN A 10.10.2.122
www IN A 10.10.4.200
ftp IN A 10.10.4.200
EOF
```



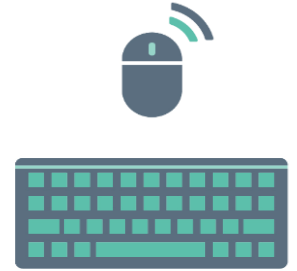
命令指南 / 操作引导

```
#第3步：在DNS-Master上执行

cat > /var/named/10.10.4.common <<EOF
\$TTL 1D
@ IN SOA ns.domain.com. root.domain.com. (
        1 ; serial
        1D ; refresh
        1H ; retry
        1W ; expire
3H ) ; minimum
@ IN NS ns.domain.com.
@ IN NS ns1.domain.com.
120 IN PTR ns.domain.com.
122 IN PTR ns1.domain.com.
200 IN PTR www.domain.com.
200 IN PTR ftp.domain.com.
EOF

#verify and reload the bind profile on DNS master
named-checkconf /etc/named.conf
named-checkzone domain.com /var/named/com-domain-area
named-checkzone 3.10.10.in-addr.arpa /var/named/10.10.3.area
named-checkzone domain.com /var/named/com-domain-common
named-checkzone 4.10.10.in-addr.arpa /var/named/10.10.4.common
systemctl reload named
```



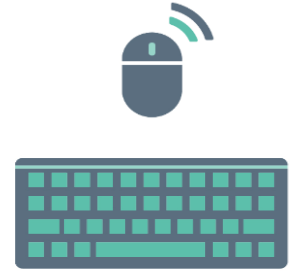
命令指南 / 操作引导

```
#第4步：在DNS-Slave上执行

#configure primary and secondary synchronization and view on DNS slave
cp -f /etc/named.conf /etc/named.conf.bak1
sed -i '/zone "." IN {/,+3d' /etc/named.conf
sed -i '/named.rfc1912.zones/d' /etc/named.conf
sed -i 's/127.0.0.1/10.10.2.122/g' /etc/named.conf
sed -i 's/localhost/any/g' /etc/named.conf
sed -i "/allow-query/a allow-transfer { none; };\nmasterfile-format text;" /etc/named.conf
cat >> /etc/named.conf <<EOF

key "area-key" {
        algorithm hmac-md5;
        secret "areaSecret";
};

key "common-key" {
        algorithm hmac-md5;
        secret "commonSecret";
};

EOF

read -p "Please enter the secret value in the area-key generated by the DNS Master host: " areaSecret
sed -i 's#areaSecret#'"$areaSecret"'#g' /etc/named.conf
read -p "Please enter the secret value in the common-key generated by the DNS Master host: " commonSecret
sed -i 's#commonSecret#'"$commonSecret"'#g' /etc/named.conf
cat >> /etc/named.conf <<EOF
```



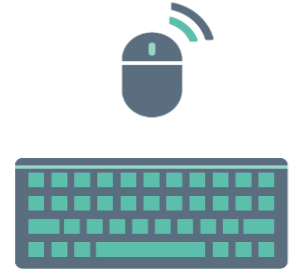
命令指南 / 操作引导

```
#第4步：在DNS-Slave上执行

view "area" {
    match-clients{key area-key; 10.10.2.0/26;};
    server 10.10.2.120 { keys area-key; };
    zone "." IN {
            type hint;
            file "named.ca";
    };
    zone "domain.com" IN {
            type slave;
            file "com-domain-area";
            masters{10.10.2.120;};
    };
    zone "3.10.10.in-addr.arpa" IN {
            type slave;
            file "10.10.3.area";
            masters{10.10.2.120;};
    };
};
```



命令指南 / 操作引导

```
#第4步：在DNS-Slave上执行

view "common" {
    match-clients { key common-key; any;};
    server 10.10.2.120 { keys common-key; };
    zone "." IN {
            type hint;
            file "named.ca";
    };
    zone "domain.com" IN {
            type slave;
            file "com-domain-common";
            masters{10.10.2.120;};
    };
    zone "4.10.10.in-addr.arpa" IN {
            type slave;
            file "10.10.4.common";
            masters{10.10.2.120;};
    };
};
EOF

#check the correctness of bind master configuration file
named-checkconf /etc/named.conf
systemctl reload named
ls /var/named
cat /var/named/com-domain-area
cat /var/named/com-domain-common
cat /var/named/10.10.3.area
cat /var/named/10.10.4.common
cat /var/named/data/named.run | head -n 60
```



命令指南 / 操作引导

```
#第4步：在DNS-Slave上执行

view "common" {
    match-clients { key common-key; any;};
    server 10.10.2.120 { keys common-key; };
    zone "." IN {
            type hint;
            file "named.ca";
    };
    zone "domain.com" IN {
            type slave;
            file "com-domain-common";
            masters{10.10.2.120;};
    };
    zone "4.10.10.in-addr.arpa" IN {
            type slave;
            file "10.10.4.common";
            masters{10.10.2.120;};
    };
};
EOF

#check the correctness of bind master configuration file
named-checkconf /etc/named.conf
systemctl reload named
ls /var/named
cat /var/named/com-domain-area
cat /var/named/com-domain-common
cat /var/named/10.10.3.area
cat /var/named/10.10.4.common
cat /var/named/data/named.run | head -n 60
```


智能运维课程体系


棒棒堂