DNS相关

1. DNS主从

环境：centos7.4虚拟机2台，关闭防火墙、SELinux，清空iptables规则，搭建好yum

IP地址：192.168.1.1、192.168.1.2

#安装软件

[root@node01 ~]# yum -y install bind bind-chroot

[root@node02 ~]# yum -y install bind bind-chroot

#修改配置文件

[root@node01 ~]# vim /etc/named.conf

[root@node01 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

allow-transfer {

192.168.1.2;

};

};

[root@node01 ~]# cd /var/named/

[root@node01 named]# cp -p named.localhost tedu.cn.zone

[root@node01 named]# vim tedu.cn.zone

[root@node01 named]# ll tedu.cn.zone

-rw-r----- 1 root named 209 12月 6 16:33 tedu.cn.zone

[root@node01 named]# cat tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

node02 A 192.168.1.2

www A 192.168.1.100

#测试解析

[root@node01 named]# systemctl start named

[root@node01 named]# nslookup www.tedu.cn 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.tedu.cn

Address: 192.168.1.100

#搭建从服务器

[root@node02 ~]# vim /etc/named.conf

[root@node02 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "tedu.cn" IN {

type slave;

masters {

192.168.1.1;

};

file "slaves/tedu.cn.zone";

};

[root@node02 ~]# systemctl restart named

[root@node02 ~]# ls /var/named/slaves/

tedu.cn.zone

#验证结果

[root@node02 ~]# nslookup www.tedu.cn 192.168.1.2

Server: 192.168.1.2

Address: 192.168.1.2#53

Name: www.tedu.cn

Address: 192.168.1.100

#增加解析记录

[root@node01 named]# vim tedu.cn.zone

[root@node01 named]# tail -1 tedu.cn.zone

ftp A 192.168.1.200

[root@node01 named]# systemctl restart named

[root@node01 named]# nslookup ftp.tedu.cn 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: ftp.tedu.cn

Address: 192.168.1.200

[root@node02 ~]# rm -rf /var/named/slaves/tedu.cn.zone

[root@node02 ~]# systemctl restart named

[root@node02 ~]# nslookup ftp.tedu.cn 192.168.1.2

Server: 192.168.1.2

Address: 192.168.1.2#53

Name: ftp.tedu.cn

Address: 192.168.1.200

1. DNS子域授权

环境：centos7.4虚拟机两台，关闭防火墙、SELinux，清空iptables规则，搭建好yum

#省略安装过程

#修改配置文件

[root@node01 ~]# vim /etc/named.conf

[root@node01 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

[root@node01 ~]# cat /var/named/tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

1 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

node02 A 192.168.1.2

www A 192.168.1.100

ftp A 192.168.1.200

[root@node01 ~]# systemctl restart named

[root@node01 ~]# nslookup www.tedu.cn 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.tedu.cn

Address: 192.168.1.100

[root@node02 ~]# vim /etc/named.conf

[root@node02 ~]# cd /var/named/

[root@node02 named]# cd

[root@node02 ~]#

[root@node02 ~]# vim /etc/named.conf

[root@node02 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "bj.tedu.cn" IN {

type master;

file "bj.tedu.cn.zone";

};

[root@node02 ~]# cd /var/named/

[root@node02 named]# cp -p named.localhost bj.tedu.cn.zone

[root@node02 named]# vim bj.tedu.cn.zone

[root@node02 named]# cat bj.tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node02

node02 A 192.168.1.2

www A 192.168.1.150

[root@node02 named]# systemctl restart named

[root@node02 named]# nslookup www.bj.tedu.cn 192.168.1.2

Server: 192.168.1.2

Address: 192.168.1.2#53

Name: www.bj.tedu.cn

Address: 192.168.1.150

[root@node02 named]# nslookup www.bj.tedu.cn 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

\*\* server can't find www.bj.tedu.cn: NXDOMAIN

#添加子域授权

[root@node01 ~]# vim /var/named/tedu.cn.zone

[root@node01 ~]# cat /var/named/tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

2 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

node02 A 192.168.1.2

www A 192.168.1.100

ftp A 192.168.1.200

bj.tedu.cn. NS node02.bj.tedu.cn.

node02.bj.tedu.cn. A 192.168.1.2

[root@node01 ~]# systemctl restart named

[root@node01 ~]# nslookup www.bj.tedu.cn 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Non-authoritative answer:

Name: www.bj.tedu.cn

Address: 192.168.1.150

1. DNS分离解析实验

环境：centos7.4虚拟机4台，关闭防火墙，SELinux，清空iptables规则，搭好yum

IP地址：dns服务器192.168.1.1

Client：192.168.1.2

Web1: 192.168.1.3

Web2： 192.168.1.4

#配置

[root@node01 ~]# yum -y install bind bind-chroot

[root@node03 ~]# yum -y install httpd

[root@node04 ~]# yum -y install httpd

[root@node01 ~]# vim /etc/named.conf

[root@node01 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

view "beijing" {

match-clients {

192.168.1.1;

};

zone "qq.com" IN {

type master;

file "qq.com.beijing";

};

zone "163.com" IN {

type master;

file "163.com.bejing";

};

};

view "shanghai" {

match-clients {

192.168.1.2;

};

zone "qq.com" IN {

type master;

file "qq.com.shanghai";

};

zone "163.com" IN {

type master;

file "163.com.shanghai";

};

};

[root@node01 ~]# named-checkconf /etc/named.conf

[root@node01 ~]# cd /var/named/

[root@node01 named]# cp -p named.localhost qq.com.beijing

[root@node01 named]# cp -p qq.com.beijing qq.com.shanghai

[root@node01 named]# cp -p qq.com.beijing 163.com.bejing

[root@node01 named]# cp -p 163.com.bejing 163.com.shanghai

[root@node01 named]# vim qq.com.beijing

[root@node01 named]# vim 163.com.bejing

[root@node01 named]# vim qq.com.shanghai

[root@node01 named]# vim 163.com.shanghai

[root@node01 named]# cat qq.com.beijing

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

www A 192.168.1.3

[root@node01 named]# cat qq.com.shanghai

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

www A 192.168.1.4

[root@node01 named]# cat 163.com.bejing

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

www A 192.168.1.3

[root@node01 named]# cat 163.com.shanghai

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node01

node01 A 192.168.1.1

www A 192.168.1.4

[root@node01 named]# systemctl start named

#测试解析

[root@node01 named]# nslookup www.qq.com 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.qq.com

Address: 192.168.1.3

[root@node01 named]# nslookup www.163.com 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.163.com

Address: 192.168.1.3

[root@node02 ~]# nslookup www.qq.com 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.qq.com

Address: 192.168.1.4

[root@node02 ~]# nslookup www.163.com 192.168.1.1

Server: 192.168.1.1

Address: 192.168.1.1#53

Name: www.163.com

Address: 192.168.1.4

#配置web服务器

[root@node03 ~]# vim /etc/httpd/conf.d/00-vhosts.conf

[root@node03 ~]# cat /etc/httpd/conf.d/00-vhosts.conf

<VirtualHost \*:80>

ServerName "www.qq.com"

DocumentRoot "/var/www/qq/"

</VirtualHost>

<VirtualHost \*:80>

ServerName "www.163.com"

DocumentRoot "/var/www/163/"

</VirtualHost>

[root@node03 ~]# mkdir /var/www/{qq,163}

[root@node03 ~]# echo "I'm Beijing QQ" >> /var/www/qq/index.html

[root@node03 ~]# echo "I'm Beijing 163" >> /var/www/163/index.html

[root@node03 ~]# systemctl start httpd

[root@node04 ~]# vim /etc/httpd/conf.d/00-vhosts.conf

[root@node04 ~]# cat /etc/httpd/conf.d/00-vhosts.conf

<VirtualHost \*:80>

ServerName "www.qq.com"

DocumentRoot "/var/www/qq/"

</VirtualHost>

<VirtualHost \*:80>

ServerName "www.163.com"

DocumentRoot "/var/www/163/"

</VirtualHost>

[root@node04 ~]# mkdir /var/www/{qq,163}

[root@node04 ~]# echo "I'm shanghai 163" >> /var/www/163/index.html

[root@node04 ~]# echo "I'm shanghai QQ" >> /var/www/qq/index.html

[root@node04 ~]# systemctl start httpd

#测试分离解析

[root@node01 ~]# echo "nameserver 192.168.1.1" > /etc/resolv.conf

[root@node01 ~]# curl www.qq.com

I'm Beijing QQ

[root@node01 ~]# curl www.163.com

I'm Beijing 163

[root@node01 ~]#

[root@node02 ~]# echo "nameserver 192.168.1.1" > /etc/resolv.conf

[root@node02 ~]# curl www.qq.com

I'm shanghai QQ

[root@node02 ~]# curl www.163.com

I'm shanghai 163

1. 缓存dns服务器

环境：centos7.4虚拟机两台，关闭防火墙、SELinux，搭建好yum，清空iptables规则

IP地址：dns服务器192.168.1.3

Client：192.168.1.4

配置：

[root@node03 ~]# curl -I [www.baidu.com](http://www.baidu.com)

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: private, no-cache, no-store, proxy-revalidate, no-transform

Connection: keep-alive

Content-Length: 277

Content-Type: text/html

Date: Sat, 07 Dec 2019 03:52:45 GMT

Etag: "575e1f60-115"

Last-Modified: Mon, 13 Jun 2016 02:50:08 GMT

Pragma: no-cache

Server: bfe/1.0.8.18

[root@node04 ~]# curl -I www.baidu.com

curl: (6) Could not resolve host: www.baidu.com; 未知的错误

#在node03上构建缓存dns

[root@node03 ~]# yum -y install bind bind-chroot

[root@node03 ~]# vim /etc/named.conf

[root@node03 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

forwarders {

192.168.1.254;

};

};

[root@node03 ~]# named-checkconf /etc/named.conf

[root@node03 ~]# systemctl start named

[root@node03 ~]# nslookup www.badiu.com 192.168.1.3

Server: 192.168.1.3

Address: 192.168.1.3#53

Non-authoritative answer:

Name: www.badiu.com

Address: 47.254.33.193

#验证结果

[root@node04 ~]# echo "nameserver 192.168.1.3" > /etc/resolv.conf

[root@node04 ~]# curl -I www.baidu.com

HTTP/1.1 200 OK

Accept-Ranges: bytes

Cache-Control: private, no-cache, no-store, proxy-revalidate, no-transform

Connection: keep-alive

Content-Length: 277

Content-Type: text/html

Date: Sat, 07 Dec 2019 03:58:25 GMT

Etag: "575e1f60-115"

Last-Modified: Mon, 13 Jun 2016 02:50:08 GMT

Pragma: no-cache

Server: bfe/1.0.8.18

1. 父域转发

环境：centos7.4虚拟机两台，关闭防火墙、SELinux，清空iptables规则，搭建好yum

IP地址： 父域：192.168.1.3

子域：192.168.1.4

#配置

[root@node03 ~]# yum -y install bind bind-chroot

[root@node04 ~]# yum -y install bind bind-chroot

[root@node03 ~]# vim /etc/named.conf

[root@node03 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "tedu.cn" IN {

type master;

file "tedu.cn.zone";

};

[root@node03 ~]# cd /var/named/

[root@node03 named]# cp -p named.localhost tedu.cn.zone

[root@node03 named]# vim tedu.cn.zone

[root@node03 named]# cat tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node03

node03 A 192.168.1.3

www A 192.168.1.100

[root@node03 named]# systemctl restart named

[root@node03 named]# nslookup www.tedu.cn 192.168.1.3

Server: 192.168.1.3

Address: 192.168.1.3#53

Name: www.tedu.cn

Address: 192.168.1.100

[root@node04 ~]# vim /etc/named.conf

[root@node04 ~]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { any; };

recursion yes;

};

zone "bj.tedu.cn" IN {

type master;

file "bj.tedu.cn.zone";

};

[root@node04 ~]# cd /var/named/

[root@node04 named]# cp -p named.localhost bj.tedu.cn.zone

[root@node04 named]# vim bj.tedu.cn.zone

[root@node04 named]# cat bj.tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node04

node04 A 192.168.1.4

www A 192.168.1.200

[root@node04 named]# systemctl restart named

[root@node04 named]# nslookup www.bj.tedu.cn 192.168.1.4

Server: 192.168.1.4

Address: 192.168.1.4#53

Name: www.bj.tedu.cn

Address: 192.168.1.200

[root@node04 named]# nslookup www.tedu.cn 192.168.1.4

Server: 192.168.1.4

Address: 192.168.1.4#53

Non-authoritative answer:

www.tedu.cn canonical name = www.tedu.cn.cdn20.com.

Name: www.tedu.cn.cdn20.com

Address: 211.161.84.168

#此处解析记录为官方递归解析，并不是我们自定义的解析地址

#修改配置

[root@node04 named]# vim /etc/named.conf

[root@node04 named]# cat /etc/named.conf

options {

directory "/var/named";

allow-query { localhost; };

recursion yes;

};

zone "bj.tedu.cn" IN {

type master;

file "bj.tedu.cn.zone";

};

zone "tedu.cn" IN {

type forward;

forwarders {

192.168.1.3;

};

};

[root@node04 named]# systemctl restart named

[root@node04 named]# nslookup www.tedu.cn 192.168.1.4

Server: 192.168.1.4

Address: 192.168.1.4#53

Non-authoritative answer:

Name: www.tedu.cn

Address: 192.168.1.100

#父域转发成功

#添加子域授权

[root@node04 named]# nslookup www.bj.tedu.cn 192.168.1.3

Server: 192.168.1.3

Address: 192.168.1.3#53

\*\* server can't find www.bj.tedu.cn: NXDOMAIN

[root@node03 named]# vim tedu.cn.zone

[root@node03 named]# cat tedu.cn.zone

$TTL 1D

@ IN SOA @ rname.invalid. (

0 ; serial

1D ; refresh

1H ; retry

1W ; expire

3H ) ; minimum

NS node03

node03 A 192.168.1.3

www A 192.168.1.100

bj.tedu.cn. NS node04.bj.tedu.cn.

node04.bj.tedu.cn. A 192.168.1.4

[root@node03 named]# systemctl restart named

[root@node04 named]# nslookup www.bj.tedu.cn 192.168.1.3

Server: 192.168.1.3

Address: 192.168.1.3#53

Non-authoritative answer:

Name: www.bj.tedu.cn

Address: 192.168.1.200