DNS服务器搭建

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*DNS服务器的搭建

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

官方文档：终端下输入 man named.conf 、 man named

服务器端：

前期工作：

切换到NAT模式

1. 关闭防火墙以及SeLinux.

防火墙相关设置：

systemctl stop firewalld //临时关闭防火墙

systemctl disable firewalld //禁止开机启动防火墙

selinux相关设置：

SeLinux配置文件，/etc/selinux/config

设置 SELINUX=disabled

（2）安装相应的软件包

yum -y install bind

yum -y install bind-utils //bind-utils提供DNS查询工具，如dig、host、nslookup

安装完后，检测有没有安装

[root@localhost ~]# rpm -qa | grep bind

rpcbind-0.2.0-42.el7.x86\_64

bind-libs-9.9.4-61.el7.x86\_64

bind-libs-lite-9.9.4-61.el7.x86\_64

bind-license-9.9.4-61.el7.noarch

bind-9.9.4-61.el7.x86\_64

bind-utils-9.9.4-61.el7.x86\_64

如果没有出现 rpcbind

yum -y install rpcbind //原因可能是部分镜像网站漏了一些安装包

切换到OnlyHost模式

1. 修改配置文件，dns工作目录中（/var/named/），新增正向解析文件/反向解析文件

配置文件路径： /etc/named.conf

示例配置文件：

See /usr/share/doc/bind\*/sample/ for example named configuration files.

拷贝示例配置文件到tmp文件夹下

cp /usr/share/doc/bind-9.9.4/sample/etc/named.conf /tmp

1. 重启服务

systemctl restart named

systemctl enable named //开机启动DNS服务

客户端：

切换到NAT模式下：

yum -y install bind-utils

切换到OnlyHost模式下：

配置文件 ：/etc/resolv.conf

添加如下：

nameserver 192.168.59.128(DNS IP地址)

注意问题：

（1）格式问题 （紧靠左边，别漏了'.'）

（2）权限问题（copy named.empty（默认权限640） 来编写正反向解析文件，记得chmod 644 正向解析文件，chmod 644 反向解析文件，如果自己新建正反向解析文件，那么不存在解析问题）

出错处理：

1.服务启动后报错信息

2.如果服务没有报错信息，但是没有出现指定效果，tail -30 /var/log/messages

3.google/baidu 相关错误信息

课堂案例项目：

搭建fqnu.org网站域名系统

|  |  |
| --- | --- |
| 域名 | IP地址 |
| dns.fqnu.org | 192.168.59.128 |
| dxxy.fqnu.org | 192.168.59.120 |
| jgxy.fqnu.org | 192.168.59.121 |
| wfxy.fqnu.org | 192.168.59.123 |

运行效果图：

客户端运行效果：

[root@localhost ~]# host wfxy.fqnu.org

wfxy.fqnu.org has address 192.168.59.123

[root@localhost ~]# host 192.168.59.123

123.59.168.192.in-addr.arpa domain name pointer wfxy.fqnu.org.

[root@localhost ~]# host 192.168.59.120

120.59.168.192.in-addr.arpa domain name pointer dxxy.fqnu.org.

[root@localhost ~]# host 192.168.59.121

121.59.168.192.in-addr.arpa domain name pointer jgxy.fqnu.org.

[root@localhost ~]# host jgxy.fqnu.org

jgxy.fqnu.org has address 192.168.59.121

[root@localhost ~]# host 192.168.59.128

128.59.168.192.in-addr.arpa domain name pointer dns.fqnu.org.

[root@localhost ~]# host 192.168.59.129

Host 129.59.168.192.in-addr.arpa. not found: 3(NXDOMAIN)

[root@localhost ~]# host tyxy.fqnu.org

Host tyxy.fqnu.org.localdomain not found: 2(SERVFAIL)

[root@localhost ~]#

课堂案例项目 DNS配置文件如下：

路径： /etc/named.conf

//

// named.conf

//

// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS

// server as a caching only nameserver (as a localhost DNS resolver only).

//

// See /usr/share/doc/bind\*/sample/ for example named configuration files.

//

// See the BIND Administrator's Reference Manual (ARM) for details about the

// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {

directory "/var/named";

dump-file "/var/named/data/cache\_dump.db";

statistics-file "/var/named/data/named\_stats.txt";

};

zone "fqnu.org" {

type master;

file "fqnu.org";

};

zone "59.168.192.in-addr.arpa" {

type master;

file "59.168.192";

};

正向解析文件如下：

/var/named/fqnu.org

$TTL 86400

fqnu.org. IN SOA dns.fqnu.org. root.fqnu.org (

20180511 ; serial

1H ; refresh

15M ; retry

1W ; expire

1D ) ; minimum

fqnu.org. IN NS dns.fqnu.org.

dns IN A 192.168.59.128

dxxy IN A 192.168.59.120

jgxy IN A 192.168.59.121

wfxy IN A 192.168.59.123

反向解析文件：

/var/named/59.168.192

$TTL 86400

@ IN SOA 59.168.192.in-addr.arpa. root.fqnu.org (

20180511 ; serial

1H ; refresh

15M ; retry

1W ; expire

1D ) ; minimum

@ IN NS dns.fqnu.org.

128 IN PTR dns.fqnu.org.

120 IN PTR dxxy.fqnu.org.

121 IN PTR jgxy.fqnu.org.

123 IN PTR wfxy.fqnu.org.

DNS服务器控制脚本：

#!/bin/bash

# this program is control DHCP server

# Date:2018-05-20

# Version:2.0

# Author: Zhang Peng

INSTALL(){

echo "execute INSTALL function"

command -v named || yum -y install bind bind-utils # detection dhcp modules,install dhcp modules

echo "the dhcpd has been installed"

}

RUN(){

echo "execute RUN function"

systemctl stop firewalld

echo "the status of firewalld:"

systemctl status firewalld | grep Active

SeStatus=$(getenforce)

if [ $SeStatus == "Disabled" ]

then

echo "no selinux policy is loaded"

else

echo "the selinux status is $SeStatus,And begin to change..."

sed -i 's/SELINUX=enforcing/SELINUX=disabled/' /etc/selinux/config

sed -i 's/SELINUX=permissive/SELINUX=disabled/' /etc/selinux/config

echo "change succeed, need reboot to take effort"

read -p "do u want reboot? yes or no: " REBOOT

if [ $REBOOT == "yes" ]

then

echo "begin reboot..."

#before reboot,set dns service starting up

systemctl enable named

reboot

else

echo "ok,not reboot"

fi

fi

systemctl restart named

systemctl enable named # dhcpd service starting up

}

DISPLAY(){

echo "execute DISPLAY function"

echo "dns version:"

named -v

read -p "input domain name or IP address for query: " DMN

host $DMN

}

MODIFY(){

echo "execute MODIFY function"

cat <<EOF

which one operation u want to execute?

(MMF)Modify Mapping File

(MMC)Modify Main Configuration

EOF

read -p "choose operation MMF,MMC? " OP

case $OP in

MMF)

echo "run MMF"

read -p "please input domain name: " DOMAIN

read -p "please input IP address: " IPADDR

NEWDOMAIN=$DOMAIN.

#截取域名、IP地址部分信息

L3DOMAIN=${DOMAIN%%.\*}

L3IPADDR=${IPADDR##\*.}

#echo $L3IPADDR

#echo $L3DOMAIN

echo -e "$L3DOMAIN \tIN\tA\t $IPADDR " >> /var/named/fqnu.org

echo -e "$L3IPADDR \tIN\tPTR\t $NEWDOMAIN" >> /var/named/59.168.192

systemctl restart named

;;

MMC)

echo "run MMC..."

read -p "please input forward domain file name: " FDFN

read -p "please input reverse domain file name: " RDFN

##在特定文件夹下，生成特定文件，同时修改/etc/named.conf主配置文件

touch /var/named/$FDFN

touch /var/named/$RDFN

###测试成功，后期可以将test替换成 /etc/named，再结合systemctl restart named

cat <<EOF >>test

zone "$FDFN"{

type master;

file "$FDFN";

};

zone "$RDFN.in-addr.arpa"{

type master;

file "$RDFN";

};

EOF

;;

\*)

esac

echo "please input right options ."

}

ANALYSIS(){

echo "execute ANALYSIS function"

for IPTEST in {2..253}

do

host 192.168.59.$IPTEST >> /tmp/host-tmp

done

grep -v "not found" /tmp/host-tmp | sort | uniq

echo "fetch information:"

grep -v "not found" /tmp/host-tmp | sort | uniq > /tmp/tmptmp

awk -F . 'BEGIN {OFS="."}{print $4,$3,$2,$1,$6,$7,$8}' /tmp/tmptmp | sed 's/.arpa domain name pointer//'

}

SHOW(){

echo "execute SHOW DNS Status function"

systemctl status named | grep Active

}

HINT(){

read -p "Press Enter to continue:"

}

while true

do

clear

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

echo "1.Install DNS server:"

echo "2.Run DNS server:"

echo "3.Display DNS Information:"

echo "4.Modify the configuration files"

echo "5.Analysis domain "

echo "6.Show DNS status"

echo "7.Exit Script:"

echo "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*"

read -p "please select a function(1-7):" U\_SELECT

case $U\_SELECT in

1)

INSTALL

HINT

;;

2)

RUN

HINT

;;

3)

DISPLAY

HINT

;;

4)

MODIFY

HINT

;;

5)

ANALYSIS

HINT

;;

6)

SHOW

HINT

;;

7)

exit

;;

\*)

read -p "Please Select 1-7,Press Enter to continue:"

esac

done

DNS示例配置文件如下：

/\*

Sample named.conf BIND DNS server 'named' configuration file

for the Red Hat BIND distribution.

See the BIND Administrator's Reference Manual (ARM) for details about the

configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

\*/

options

{

// Put files that named is allowed to write in the data/ directory:

directory "/var/named"; // "Working" directory

dump-file "data/cache\_dump.db";

statistics-file "data/named\_stats.txt";

memstatistics-file "data/named\_mem\_stats.txt";

/\*

Specify listenning interfaces. You can use list of addresses (';' is

delimiter) or keywords "any"/"none"

\*/

//listen-on port 53 { any; };

listen-on port 53 { 127.0.0.1; };

//listen-on-v6 port 53 { any; };

listen-on-v6 port 53 { ::1; };

/\*

Access restrictions

There are two important options:

allow-query { argument; };

- allow queries for authoritative data

allow-query-cache { argument; };

- allow queries for non-authoritative data (mostly cached data)

You can use address, network address or keywords "any"/"localhost"/"none" as argument

Examples:

allow-query { localhost; 10.0.0.1; 192.168.1.0/8; };

allow-query-cache { ::1; fe80::5c63:a8ff:fe2f:4526; 10.0.0.1; };

\*/

allow-query { localhost; };

allow-query-cache { localhost; };

/\* Enable/disable recursion - recursion yes/no;

- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.

- If you are building a RECURSIVE (caching) DNS server, you need to enable

recursion.

- If your recursive DNS server has a public IP address, you MUST enable access

control to limit queries to your legitimate users. Failing to do so will

cause your server to become part of large scale DNS amplification

attacks. Implementing BCP38 within your network would greatly

reduce such attack surface

\*/

recursion yes;

/\* DNSSEC related options. See information about keys ("Trusted keys", bellow) \*/

/\* Enable serving of DNSSEC related data - enable on both authoritative

and recursive servers DNSSEC aware servers \*/

dnssec-enable yes;

/\* Enable DNSSEC validation on recursive servers \*/

dnssec-validation yes;

/\* In RHEL-7 we use /run/named instead of default /var/run/named

so we have to configure paths properly. \*/

pid-file "/run/named/named.pid";

session-keyfile "/run/named/session.key";

managed-keys-directory "/var/named/dynamic";

};

logging

{

/\* If you want to enable debugging, eg. using the 'rndc trace' command,

\* named will try to write the 'named.run' file in the $directory (/var/named).

\* By default, SELinux policy does not allow named to modify the /var/named directory,

\* so put the default debug log file in data/ :

\*/

channel default\_debug {

file "data/named.run";

severity dynamic;

};

};

/\*

Views let a name server answer a DNS query differently depending on who is asking.

By default, if named.conf contains no "view" clauses, all zones are in the

"default" view, which matches all clients.

Views are processed sequentially. The first match is used so the last view should

match "any" - it's fallback and the most restricted view.

If named.conf contains any "view" clause, then all zones MUST be in a view.

\*/

view "localhost\_resolver"

{

/\* This view sets up named to be a localhost resolver ( caching only nameserver ).

\* If all you want is a caching-only nameserver, then you need only define this view:

\*/

match-clients { localhost; };

recursion yes;

# all views must contain the root hints zone:

zone "." IN {

type hint;

file "/var/named/named.ca";

};

/\* these are zones that contain definitions for all the localhost

\* names and addresses, as recommended in RFC1912 - these names should

\* not leak to the other nameservers:

\*/

include "/etc/named.rfc1912.zones";

};

view "internal"

{

/\* This view will contain zones you want to serve only to "internal" clients

that connect via your directly attached LAN interfaces - "localnets" .

\*/

match-clients { localnets; };

recursion yes;

zone "." IN {

type hint;

file "/var/named/named.ca";

};

/\* these are zones that contain definitions for all the localhost

\* names and addresses, as recommended in RFC1912 - these names should

\* not leak to the other nameservers:

\*/

include "/etc/named.rfc1912.zones";

// These are your "authoritative" internal zones, and would probably

// also be included in the "localhost\_resolver" view above :

/\*

NOTE for dynamic DNS zones and secondary zones:

DO NOT USE SAME FILES IN MULTIPLE VIEWS!

If you are using views and DDNS/secondary zones it is strongly

recommended to read FAQ on ISC site (www.isc.org), section

"Configuration and Setup Questions", questions

"How do I share a dynamic zone between multiple views?" and

"How can I make a server a slave for both an internal and an external

view at the same time?"

\*/

zone "my.internal.zone" {

type master;

file "my.internal.zone.db";

};

zone "my.slave.internal.zone" {

type slave;

file "slaves/my.slave.internal.zone.db";

masters { /\* put master nameserver IPs here \*/ 127.0.0.1; } ;

// put slave zones in the slaves/ directory so named can update them

};

zone "my.ddns.internal.zone" {

type master;

allow-update { key ddns\_key; };

file "dynamic/my.ddns.internal.zone.db";

// put dynamically updateable zones in the slaves/ directory so named can update them

};

};

key ddns\_key

{

algorithm hmac-md5;

secret "use /usr/sbin/dnssec-keygen to generate TSIG keys";

};

view "external"

{

/\* This view will contain zones you want to serve only to "external" clients

\* that have addresses that are not match any above view:

\*/

match-clients { any; };

zone "." IN {

type hint;

file "/var/named/named.ca";

};

recursion no;

// you'd probably want to deny recursion to external clients, so you don't

// end up providing free DNS service to all takers

// These are your "authoritative" external zones, and would probably

// contain entries for just your web and mail servers:

zone "my.external.zone" {

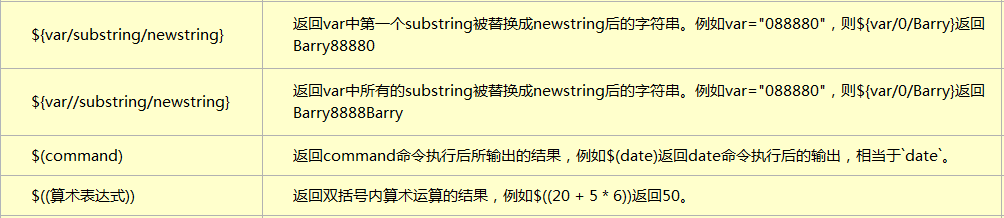
type master;

file "my.external.zone.db";

};

};

Shell变量常用的引用方式：



lynx命令教程：

yum -y install lynx

lynx内部操作命令：

移动命令

方向键上：页面上的下一个链接（用高亮显示）

方向键下：页面上的下一个链接（用高亮显示）

方向键左：回到上一个页面

方向键右：跳转到链接所指向的地址（回车键也一样）

滚动命令

Ctrl+f ：向下翻页

Ctrl+b ：向上翻页

按下q退出浏览器终端。

针对centos 7时间不一致：

执行命令 timedatectl //用法如果不清晰，可以man timedatectl

[root@localhost dns-script]# timedatectl

Local time: Thu 2018-05-24 11:51:28 PDT

Universal time: Thu 2018-05-24 18:51:28 UTC

RTC time: Mon 2018-05-28 07:05:40

Time zone: America/Los\_Angeles (PDT, -0700)

NTP enabled: yes

NTP synchronized: no

RTC in local TZ: no

DST active: yes

Last DST change: DST began at

Sun 2018-03-11 01:59:59 PST

Sun 2018-03-11 03:00:00 PDT

Next DST change: DST ends (the clock jumps one hour backwards) at

Sun 2018-11-04 01:59:59 PDT

Sun 2018-11-04 01:00:00 PST

针对时区修改：

timedatectl set-timezone Asia/Shanghai

然后reboot

[root@localhost ~]# timedatectl

Local time: Mon 2018-05-28 15:16:44 CST

Universal time: Mon 2018-05-28 07:16:44 UTC

RTC time: Mon 2018-05-28 07:16:43

Time zone: Asia/Shanghai (CST, +0800)

NTP enabled: yes

NTP synchronized: no

RTC in local TZ: no

DST active: n/a

[root@localhost ~]# date

Mon May 28 15:16:48 CST 2018

[root@localhost ~]#