Администрирование сетевых подсистем

Лабораторная работа №2

Чилеше Лупупа

13 ноября 2025

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Приобретение практических навыков по установке, конфигурированию и тестированию DNS-сервера на базе BIND.

Выполнение лабораторной работы

Первичная проверка DNS-разрешения

```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# dig www.yandex.ru

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13622
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          333     IN      A       77.88.44.55
www.yandex.ru.          333     IN      A       77.88.55.88
www.yandex.ru.          333     IN      A       5.255.255.77

;; Query time: 10 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Thu Nov 13 12:23:44 UTC 2025
;; MSG SIZE  rcvd: 90

[root@server.chileshe.net ~]#
```

Рис. 1: Результат dig www.yandex.ru

Проверка локального DNS-сервера

```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# systemctl start named
[root@server.chileshe.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.chileshe.net ~]# dig @127.0.0.1 www.yandex.ru
;; communications error to 127.0.0.1#53: timed out

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29487
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 4a4cd49aa09729d1010000006915ce0316d0c999d7338023 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          600     IN      A       77.88.44.55
www.yandex.ru.          600     IN      A       77.88.55.88
www.yandex.ru.          600     IN      A       5.255.255.77

;; Query time: 1601 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 13 12:24:35 UTC 2025
;; MSG SIZE  rcvd: 118

[root@server.chileshe.net ~]#
```

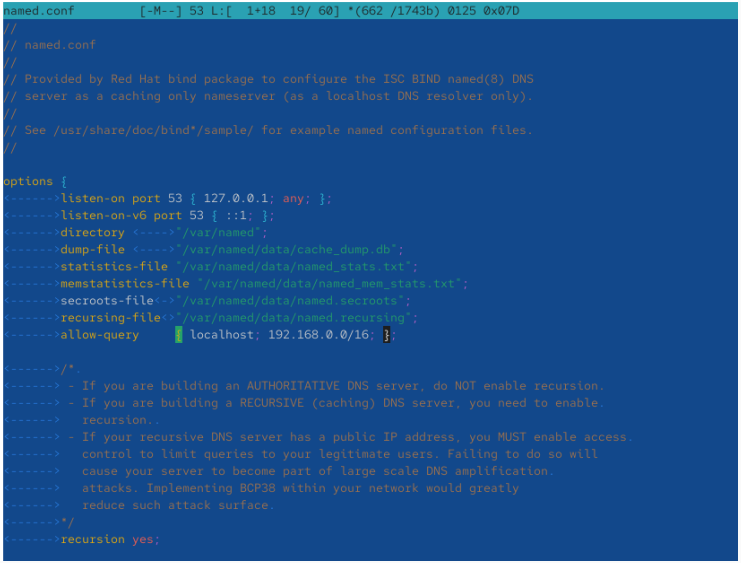
Рис. 2: Запрос dig через 127.0.0.1

Назначение локального DNS в NetworkManager

```
[root@server.chileshe.net ~]#
[root@server.chileshe.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4,
ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.chileshe.net ~]#
```

Рис. 3: Настройка DNS в NM

Настройка файла named.conf



Проверка активности порта DNS

```
[root@server.chileshe.net ~]# firewall-cmd --add-service=dns
success
[root@server.chileshe.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.chileshe.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
lsof: WARNING: can't stat() fuse.portal file system /run/user/1001/doc
      Output information may be incomplete.
avahi-dae   894                          avahi   12u     IPv4              8018       0t0        UDP *:mdns
avahi-dae   894                          avahi   13u     IPv6              8019       0t0        UDP *:mdns
chronyd     951                         chrony    5u     IPv4              8650       0t0        UDP localhost:323
chronyd     951                         chrony    6u     IPv6              8651       0t0        UDP localhost:323
named     28273                          named   25u     IPv4             83111       0t0        UDP localhost:domain

named     28273                          named   26u     IPv4             83112       0t0        UDP localhost:domain

named     28273                          named   31u     IPv6             83115       0t0        UDP localhost:domain

named     28273                          named   32u     IPv6             83116       0t0        UDP localhost:domain

named     28273 28274 isc-net-0          named   25u     IPv4             83111       0t0        UDP localhost:domain

named     28273 28274 isc-net-0          named   26u     IPv4             83112       0t0        UDP localhost:domain

named     28273 28274 isc-net-0          named   31u     IPv6             83115       0t0        UDP localhost:domain

named     28273 28274 isc-net-0          named   32u     IPv6             83116       0t0        UDP localhost:domain

named     28273 28275 isc-net-0          named   25u     IPv4             83111       0t0        UDP localhost:domain

named     28273 28275 isc-net-0          named   26u     IPv4             83112       0t0        UDP localhost:domain

named     28273 28275 isc-net-0          named   31u     IPv6             83115       0t0        UDP localhost:domain

named     28273 28275 isc-net-0          named   32u     IPv6             83116       0t0        UDP localhost:domain

named     28273 28276 isc-net-0          named   25u     IPv4             83111       0t0        UDP localhost:domain
```

Подключение пользовательских зон

```
chileshe.net       [----]  2 L:[  2+25  27/ 29] *(698 / 700b) 0010 0x00A
//
// Provided by Red Hat caching-nameserver package.
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and https://tools.ietf.org/html/rfc6303
// (c)2007 R W Franks
//.
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add.
// disable-empty-zone "."; into options
//.

zone "chileshe.net" IN {
	type master;
	file "master/fz/chileshe.net";
	allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
	type master;
	file "master/rz/192.168.1";
	allow-update { none; };
};
```

Настройка прямой зоны

```
chileshe.net       [----]  0 L:[  1+12  13/ 14] *(219 / 220b) 0010 0x00A
$TTL 1D
@<------>IN SOA<>@ server.chileshe.net. (
<------><------><------><------><------>2025111300<----> ; serial
<------><------><------><------><------>1D<----> ; refresh
<------><------><------><------><------>1H<----> ; retry
<------><------><------><------><------>1W<----> ; expire
<------><------><------><------><------>3H )<--> ; minimum
<------>NS<----->@
<------>A<------>192.168.1.1
$ORIGIN chileshe.net.
server<>A<------>192.168.1.1
ns<----->A<------>192.168.1.1
```

Рис. 7: Прямая зона

Настройка обратной зоны

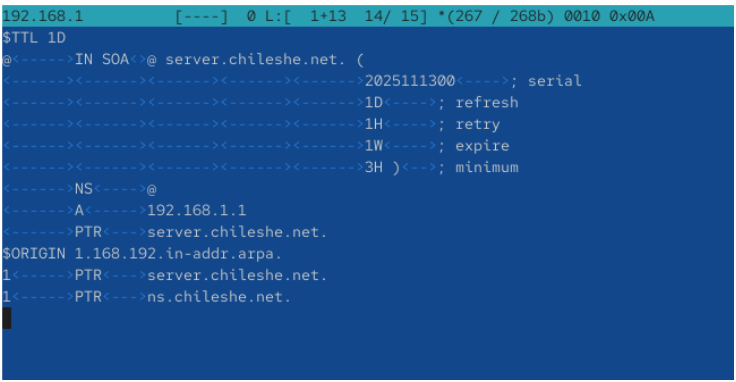


Рис. 8: Обратная зона

Настройка прав и SELinux

```
[root@server.chileshe.net rz]#
[root@server.chileshe.net rz]# chown -R named:named /etc/named
[root@server.chileshe.net rz]# chown -R named:named /var/named
[root@server.chileshe.net rz]# restorecon -vR /etc
Relabeled /etc/lvm/devices/system.devices from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20251113.120720.0005 from system_u:object_r:lvm_metadata_t:s0 to syst
em_u:object_r:lvm_etc_t:s0
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfi
ned_u:object_r:NetworkManager_etc_rw_t:s0
[root@server.chileshe.net rz]# restorecon -vR /var/named
[root@server.chileshe.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.chileshe.net rz]# systemctl restart named
[root@server.chileshe.net rz]#
```

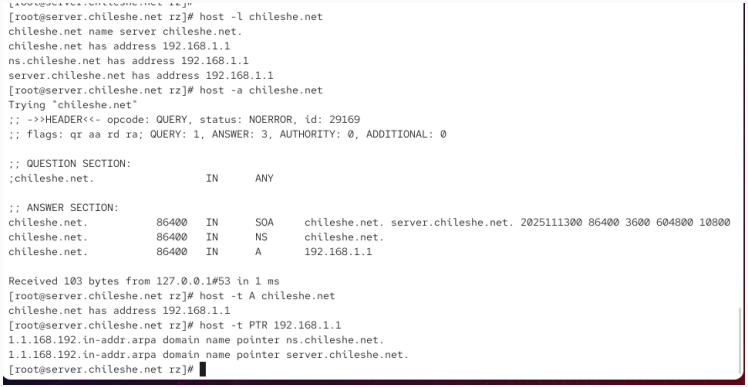
Рис. 9: SELinux и права

Проверка прямой зоны dig

```
[root@server.chileshe.net rz]# dig ns.chileshe.net

; <<>> DiG 9.18.33 <<>> ns.chileshe.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16844
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 16b0267b722b48c001000000006915d281359442664ffd1fec (good)
;; QUESTION SECTION:
;ns.chileshe.net.               IN      A

;; ANSWER SECTION:
ns.chileshe.net.        86400   IN      A       192.168.1.1

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Thu Nov 13 12:43:45 UTC 2025
;; MSG SIZE  rcvd: 88

[root@server.chileshe.net rz]#
```

Рис. 10: Проверка A-записи

Проверка прямой и обратной зоны host



```
[root@server.chileshe.net rz]# host -l chileshe.net
chileshe.net name server chileshe.net.
chileshe.net has address 192.168.1.1
ns.chileshe.net has address 192.168.1.1
server.chileshe.net has address 192.168.1.1
[root@server.chileshe.net rz]# host -a chileshe.net
Trying "chileshe.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29169
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;chileshe.net.                  IN      ANY

;; ANSWER SECTION:
chileshe.net.           86400   IN      SOA     chileshe.net. server.chileshe.net. 2025111300 86400 3600 604800 10800
chileshe.net.           86400   IN      NS      chileshe.net.
chileshe.net.           86400   IN      A       192.168.1.1

Received 103 bytes from 127.0.0.1#53 in 1 ms
[root@server.chileshe.net rz]# host -t A chileshe.net
chileshe.net has address 192.168.1.1
[root@server.chileshe.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.chileshe.net.
1.1.168.192.in-addr.arpa domain name pointer server.chileshe.net.
[root@server.chileshe.net rz]#
```

Рис. 11: Проверка host

Подготовка provisioning-каталогов

```
[root@server.chileshe.net rz]#
[root@server.chileshe.net rz]# cd /vagrant/
[root@server.chileshe.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.chileshe.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master
[root@server.chileshe.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.chileshe.net vagrant]# cp -R /etc/named/chileshe.net /vagrant/provision/server/dns/etc/named/
[root@server.chileshe.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.chileshe.net vagrant]# touch dns.sh
[root@server.chileshe.net vagrant]#
```

Рис. 12: Каталоги provisioning

Скрипт автоматизации dns.sh

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y install bind bind-utils
echo "Copy configuration files"
cp -R /vagrant/provision/server/dns/etc/* /etc
cp -R /vagrant/provision/server/dns/var/named/* /var/named
chown -R named:named /etc/named
chown -R named:named /var/named
restorecon -vR /etc
restorecon -vR /var/named
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent
echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1
echo "Change dns server address"
nmcli connection edit "eth0" <<EOF
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
EOF
systemctl restart NetworkManager
echo "Start named service"
systemctl enable named
systemctl start named
```

Выводы

Итог

В ходе работы был установлен и настроен DNS-сервер BIND, создана прямая и обратная зоны, настроены конфигурационные файлы и параметры SELinux, проведена проверка корректности работы с помощью dig и host. Создан provisioning-скрипт для автоматизации развертывания DNS-сервера в Vagrant. Все этапы выполнены успешно.