

Лабораторная работа

Номер 2

Мошаров Д.М.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Информация

Докладчик

- Мошаров Денис Максимович
- Студент
- Российский университет дружбы народов

Цель

Приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

Запуск ВМ

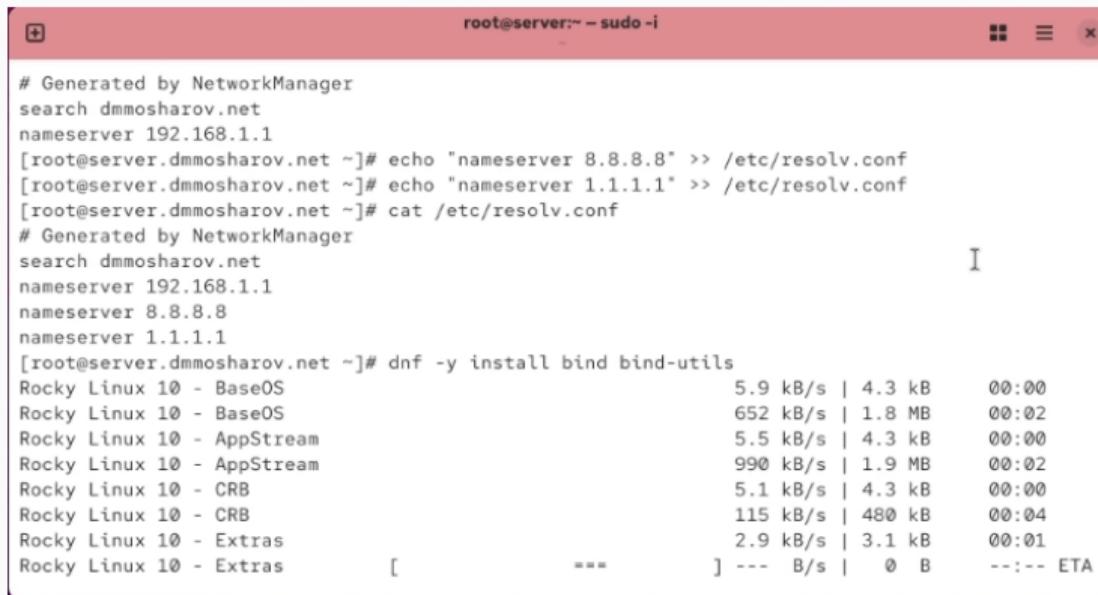
Для начала запустим виртуальную машину через vagrant

```
C:\work_asp\dmmosharov\vagrant>vagrant up server
Bringing machine 'server' up with 'virtualbox' provider...
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: You assigned a static IP ending in ".1" or ":1" to this machine.
==> server: This is very often used by the router and can cause the
==> server: network to not work properly. If the network doesn't work
==> server: properly, try changing this IP.
==> server: Clearing any previously set forwarded ports...
==> server: Clearing any previously set network interfaces...
==> server: Preparing network interfaces based on configuration...
      server: Adapter 1: nat
      server: Adapter 2: intnet
==> server: Forwarding ports...
      server: 22 (guest) => 2222 (host) (adapter 1)
==> server: Running 'pre-boot' VM customizations...
==> server: Booting VM...
==> server: Waiting for machine to boot. This may take a few minutes...
      server: SSH address: 127.0.0.1:2222
      server: SSH username: vagrant
      server: SSH auth method: password
```

Рис. 1: Запуск ВМ

Скачивание пакетов

Теперь скачаем пакет bind utils



```
# Generated by NetworkManager
search dmmosharov.net
nameserver 192.168.1.1
[root@server.dmmosharov.net ~]# echo "nameserver 8.8.8.8" >> /etc/resolv.conf
[root@server.dmmosharov.net ~]# echo "nameserver 1.1.1.1" >> /etc/resolv.conf
[root@server.dmmosharov.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search dmmosharov.net
nameserver 192.168.1.1
nameserver 8.8.8.8
nameserver 1.1.1.1
[root@server.dmmosharov.net ~]# dnf -y install bind bind-utils
Rocky Linux 10 - BaseOS                  5.9 kB/s | 4.3 kB   00:00
Rocky Linux 10 - BaseOS                  652 kB/s | 1.8 MB  00:02
Rocky Linux 10 - AppStream                5.5 kB/s | 4.3 kB   00:00
Rocky Linux 10 - AppStream                990 kB/s | 1.9 MB  00:02
Rocky Linux 10 - CRB                     5.1 kB/s | 4.3 kB   00:00
Rocky Linux 10 - CRB                     115 kB/s | 480 kB  00:04
Rocky Linux 10 - Extras                  2.9 kB/s | 3.1 kB   00:01
Rocky Linux 10 - Extras                  --- B/s | 0 B    --:-- ETA
```

Рис. 2: Скачивание пакетов

Используем команду dig для проверки сервисов яндекса

```
;; communications error to 192.168.1.1#53: connection refused
;
; <>> DiG 9.18.33 <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57962
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;
;; QUESTION SECTION:
;www.yandex.ru.           IN      A
;
;; ANSWER SECTION:
www.yandex.ru.          0       IN      A      5.255.255.77
;
;; Query time: 110 msec
;; SERVER: 8.8.8.8#53(8.8.8.8) (UDP)
;; WHEN: Wed Nov 26 15:59:40 UTC 2025
;; MSG SIZE  rcvd: 47
[root@server.dmmosharov.net ~]#
```

Рис. 3: dig ya.ru

Файлы конфигурации

Посмотрим на содержание файлов конфигурации dns в etc

```
[root@server.dmmosharov.net ~]# cat /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.
//

options {
    listen-on port 53 { 127.0.0.1; };
```

Рис. 4: Файлы конфигурации

Просмотрим теперь файл named.ca

Рис. 5: named.ca

named.localhost и named.loopback

Содержимое named.localhost и named.loopback

```
; End of file[root@server.dmmosharov.net ~]# cat /var/named/named.localhost
$TTL 1D
@      IN SOA  @ rname.invalid. (
                           0          ; serial
                           1D         ; refresh
                           1H         ; retry
                           1W         ; expire
                           3H )       ; minimum
NS      @
A       127.0.0.1
AAAA    ::1
[root@server.dmmosharov.net ~]#
```

Рис. 6: named.localhost и named.loopback

Запуск named

Запустим теперь named и осуществим снова dig yandex.ru

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

Рис. 7: Запуск named

Теперь настроим порт 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), 80
2-1x, 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' (7d681962-577a-4b13-870c-753bf3ebbc71) successfully updated.
nmcli> quit
[root@server.dmmosharov.net ~]#
```

Рис. 8: eth0

named.conf

Откроем и отредактируем named.conf

```
GNU nano 8.1          /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.  
  
options {  
    listen-on port 53 { 127.0.0.1; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
  
    ^G Help      ^O Write Out   ^F Where Is   ^K Cut        ^T Execute  
    ^X Exit      ^R Read File   ^V Replace    ^U Paste     ^J Justify
```

Рис. 9: named.conf

Правила фаервола

Установим правила фаервола

```
[root@server.dmmosharov.net ~]# firewall-cmd --add-service=dns  
success  
[root@server.dmmosharov.net ~]# firewall-cmd --add-service=dns --permanent  
success  
[root@server.dmmosharov.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 871 avahi 12u IPv4 87  
01 0t0 UDP *:mdns  
avahi-dae 871 avahi 13u IPv6 87  
02 0t0 UDP *:mdns  
chronyd 957 chrony 5u IPv4 93  
66 0t0 UDP localhost:323
```

Рис. 10: Правила фаервола

перемещение файла

Теперь переместим файл с настройкой конфига

```
[root@server.dmmosharov.net ~]# cp /etc/named.rfc1912.zones /etc/named  
[root@server.dmmosharov.net ~]# cd /etc/named  
[root@server.dmmosharov.net named]# mv /etc/named/named.rfc1912.zones /etc/nam  
ed/dmmosharov.net  
[root@server.dmmosharov.net named]# nano /etc/named/dmmosharov.net  
[root@server.dmmosharov.net named]# nano /etc/named/dmmosharov.net
```

Рис. 11: перемещение файла

Редактирование файла

И отредактируем наш файл под наши параметры

```
GNU nano 8.1          /etc/named/dmmosharov.net
// disable-empty-zone "."; into options
//

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

zone "localhost" IN {
    type primary;
    file "named.localhost";
    allow-update { none; }; █
```

Рис. 12: Редактирование файла

Файл зон

То же самое сделаем с файлом зон

```
GNU nano 8.1          /etc/named/dmmosharov.net
// named.rfc1912.zones:
//
// 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.
//                                         I
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add
[ Wrote 34 lines ]
^G Help      ^O Write Out   ^F Where Is   ^K Cut       ^T Execute
^X Exit      ^R Read File    ^\ Replace    ^U Paste     ^J Justify
```

Рис. 13: Файл зон

Создание папок и настроек днс

Создадим папки с настройками днс

```
[root@server.dmmosharov.net named]# cd /var/named
[root@server.dmmosharov.net named]# mkdir -p /var/named/master/fz
[root@server.dmmosharov.net named]# mkdir -p /var/named/master/rz
[root@server.dmmosharov.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.dmmosharov.net named]# cd /var/named/master/fz/
[root@server.dmmosharov.net fz]# mv named.localhost dmmosharov.net
[root@server.dmmosharov.net fz]# █
```

Рис. 14: Создание папок и настроек днс

Отредактируем файл dmmosharov.net

```
GNU nano 8.1          /var/named/master/fz/dmmosharov.net      Modified
$TTL 1D
@       IN SOA  @ server.dmmosharov.net. (
                        2025112600      ; serial
                        1D              ; refresh
                        1H              ; retry
                        1W              ; expire
                        3H )            ; minimum
NS      @
A       192.168.1.1
$ORIGIN dmmosharov.net
server      A      192.168.1.1
ns        A      192.168.1.1
|
^G Help      ^O Write Out    ^F Where Is     ^K Cut        ^T Execute
^X Exit      ^R Read File    ^V Replace      ^U Paste      ^J Justify
```

Рис. 15: dmmosharov.net

Папка rz

Теперь посмотрим на файлы из папки rz

```
[root@server.dmmosharov.net fz]# cp /var/named/named.loopback /var/named/master/rz/rz
[root@server.dmmosharov.net fz]# cd /var/named/master/rz/
[root@server.dmmosharov.net rz]# mv named.loopback 192.168.1
[root@server.dmmosharov.net rz]# nano /var/named/master/rz/192.168.1
```

Рис. 16: Папка rz

Редактирование файла

Отредактируем следующим образом

```
GNU nano 8.1          /var/named/master/rz/192.168.1      Mod
$TTL 1D
@      IN SOA  @ server.dmmosharov.net. (
                                20251126      ; serial
                                1D            ; refresh
                                1H            ; retry
                                1W            ; expire
                                3H )          ; minimum
NS      @
A       192.168.1.1
PTR    server.dmmosharov.net
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR    server.dmmosharov.net
1      PTR    ns.dmmosharov.net.
```

Рис. 17: Редактирование файла

Настроим Selinux

```
[root@server.dmmosharov.net rz]# chown -R named:named /etc/named
[root@server.dmmosharov.net rz]# chown -R named:named /var/named
[root@server.dmmosharov.net rz]# restorecon -vR /etc
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:object_t:s0 to unconfined_u
:object_r:NetworkManager_etc_rw_t:s0
[root@server.dmmosharov.net rz]# restorecon -vR /var/named
[root@server.dmmosharov.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.dmmosharov.net rz]# setsebool named_write_master_zones 1
[root@server.dmmosharov.net rz]# setsebool -P named_write_master_zones 1
[root@server.dmmosharov.net rz]# systemctl restart_named
```

Рис. 18: Selinux

Через dig попробуем подключиться к собственному днс

```
[root@server.dmmosharov.net rz]# host -l dmmosharov.net
dmmosharov.net name server dmmosharov.net.
dmmosharov.net has address 192.168.1.1
ns.dmmosharov.net has address 192.168.1.1
server.dmmosharov.net has address 192.168.1.1
[root@server.dmmosharov.net rz]# host -a dmmosharov.net
Trying "dmmosharov.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44894
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
dmmosharov.net.      86400   IN      SOA     dmmosharov.net. server.dmmosharov.net. 2025121501 86400 3600 604800 10800
dmmosharov.net.      86400   IN      NS      dmmosharov.net.
dmmosharov.net.      86400   IN      A       192.168.1.1

Received 105 bytes from 127.0.0.1#53 in 1 ms
[root@server.dmmosharov.net rz]# host -t A dmmosharov.net
dmmosharov.net has address 192.168.1.1
[root@server.dmmosharov.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.dmmosharov.net.
1.1.168.192.in-addr.arpa domain name pointer ns.dmmosharov.net.
```

Рис. 19: dig

Конфиг вагрант

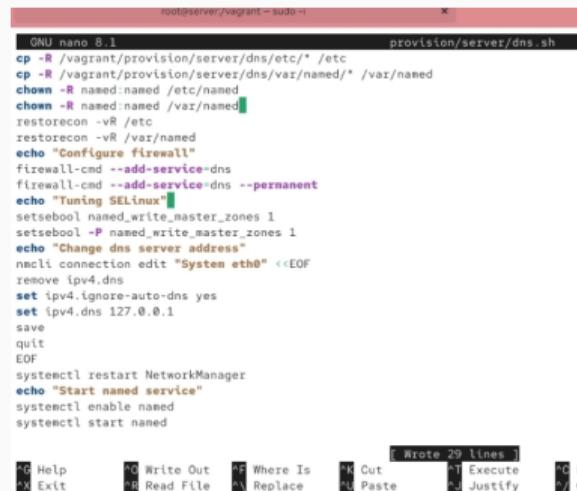
Оформим нашу работу как конфигурацию для вагранта

```
[root@server.dmmosharov.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.dmmosharov.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
bash: mkdir-p: command not found...
[root@server.dmmosharov.net vagrant]# mkdir -p /vagrant/provision/server/dns/vat/named/master/
[root@server.dmmosharov.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.dmmosharov.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.dmmosharov.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/named/master/
cp: target '/vagrant/provision/server/dns/named/master/*': No such file or directory
[root@server.dmmosharov.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/named/master/
cp: missing destination file operand after '/var/named/master/*' /vagrant/provision/server/dns/named/master/*
Try 'cp --help' for more information.
[root@server.dmmosharov.net vagrant]# cp -R /etc/named/*/* /vagrant/provision/server/dns/etc/named/
cp: missing destination file operand after '/etc/named/*/*' /vagrant/provision/server/dns/etc/named/*
Try 'cp --help' for more information.
[root@server.dmmosharov.net vagrant]# cp /etc/named.conf provision/server/dns/etc/
cp: overwrite 'provision/server/dns/etc/named.conf' ? yes
[root@server.dmmosharov.net vagrant]# cp -R /etc/named/* provision/server/dns/etc/named/
cp: overwrite 'provision/server/dns/etc/named/dmmosharov.net' ? y
[root@server.dmmosharov.net vagrant]# cp -R /var/named/master/* provision/server/dns/var/named/master/
[root@server.dmmosharov.net vagrant]# touch provision/server/dns.sh
[root@server.dmmosharov.net vagrant]# chmod +x provision/server/dns.sh
[root@server.dmmosharov.net vagrant]# nano provision/server/dns.sh
```

Рис. 20: Конфиг вагрант

скрипт

И напишем скрипт для загрузки вагранта



The screenshot shows a terminal window titled "root@server:/vagrant - sudo -i". Inside the terminal, a script is being edited in the nano text editor. The script contains commands for provisioning a Vagrant server, including copying files, changing ownership, configuring SELinux, setting network parameters, and restarting services. The status bar at the bottom indicates "Wrote 29 lines".

```
GNU nano 8.1
#!/bin/bash
# Provisioning script for Vagrant

# 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 "System 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
```

Рис. 21: скрипт

vagrantfile

И в vagrantfile будем загружать этот скрипт

```
54     |         path: "provision/default/01-user.sh"
55
56     server.vm.provision "server dns",
57     |         type: "shell",
58     |         preserve_order: true,
59     |         path: "provision/server/dns.sh"
60
61     ## Server configuration
62     config.vm.define "server", autostart: false do |server|
```

Рис. 22: vagrantfile

Выводы

В результате выполнения работы были получены навыки настройки днс