

Отчёт по лабораторной работе 2

Настройка DNS-сервера

Метвалли Ахмед Фарг Набеев

Содержание

1	Цель работы	5
2	Выполнение	6
2.1	Установка и первичная проверка DNS-сервера	6
2.2	Конфигурация DNS-сервера	7
2.3	Запуск и тестирование работы	8
2.4	Настройка DNS по умолчанию для хоста	9
2.5	Разрешение запросов от внутренних узлов	10
2.6	Настройка firewall и проверка	11
2.7	Конфигурирование первичного DNS-сервера	12
2.8	Анализ работы DNS-сервера	14
2.9	Внесение изменений в настройки окружения	16
3	Заключение	19
4	Контрольные вопросы	20

Список иллюстраций

2.1	Результат dig www.yandex.ru	6
2.2	Файл resolv.conf	7
2.3	Файл named.conf (начальная конфигурация)	8
2.4	Результаты dig с локальным сервером	9
2.5	Настройка DNS в NetworkManager	10
2.6	Проверка через lsof	11
2.7	Файл user.net с описанием зон	12
2.8	Прямая зона ahmedfarg.net	13
2.9	Обратная зона 192.168.1	13
2.10	Настройка прав и SELinux для named	14
2.11	Результат dig ns.ahmedfarg.net	15
2.12	Анализ зоны через host	16
2.13	Подготовка каталогов для DNS	16
2.14	Скрипт автоматической настройки dns.sh	17
2.15	Vagrantfile с настройкой DNS	18

Список таблиц

1 Цель работы

Приобрести практические навыки по установке и конфигурации DNS-сервера, а также закрепить теоретические знания о принципах работы системы доменных имен.

2 Выполнение

2.1 Установка и первичная проверка DNS-сервера

1. На виртуальной машине server установлен пакет **bind** и утилиты для работы с DNS.
2. С помощью команды **dig** выполнен тестовый запрос к DNS-адресу `www.yandex.ru`.

На экране отобразилась структура ответа: заголовок, вопрос, секция ответа с IP-адресами.

```
Installed:
  bind-32:9.18.33-3.el10.x86_64   bind-dnssec-utils-32:9.18.33-3.el10.x86_64

Complete!
[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# dig www.yandex.ru

; <<> DiG 9.18.33 <<> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3169
;; 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.                 578     IN      A      77.88.44.55
www.yandex.ru.                 578     IN      A      77.88.55.88
www.yandex.ru.                 578     IN      A      5.255.255.77

;; Query time: 18 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Sep 17 08:25:49 UTC 2025
;; MSG SIZE rcvd: 90

[root@server.ahmedfarg.net ~]# █
```

Рис. 2.1: Результат dig www.yandex.ru

2.2 Конфигурация DNS-сервера

1. Содержимое файла `/etc/resolv.conf` показывает, что ранее использовался внешний DNS (10.0.2.3).

```
[root@server.ahmedfarg.net ~]#  
[root@server.ahmedfarg.net ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search ahmedfarg.net  
nameserver 10.0.2.3  
[root@server.ahmedfarg.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; };  
    listen-on-v6 port 53 { ::1; };  
    directory "/var/named";  
    dump-file "/var/named/data/cache_dump.db";  
    statistics-file "/var/named/data/named_stats.txt";  
    memstatistics-file "/var/named/data/named_mem_stats.txt";  
    secroots-file "/var/named/data/named.secroots";  
    recursing-file "/var/named/data/named.recursing";  
    allow-query { localhost; };  
  
    /*  
    - 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
```

Рис. 2.2: Файл `resolv.conf`

2. В файле `/etc/named.conf` заданы параметры работы DNS-сервера:

- слушает порт 53 на 127.0.0.1,
- указывает путь для хранения кэша и статистики,
- разрешает запросы только с localhost.

```

[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ahmedfarg.net
nameserver 10.0.2.3
[root@server.ahmedfarg.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; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { localhost; };

    /*
     - 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

```

Рис. 2.3: Файл named.conf (начальная конфигурация)

2.3 Запуск и тестирование работы

1. Сервис named добавлен в автозагрузку и запущен.
2. Проверка через dig показала отличие в результатах при запросе на-
прямую (dig www.yandex.ru) и через локальный сервер (dig @127.0.0.1
www.yandex.ru).

Ответ от локального DNS имеет увеличенное время запроса, так как данные кэшируются впервые.


```

[root@server.ahmedfarg.net ~]# systemctl enable named
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
[root@server.ahmedfarg.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: 40729
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: c8b7d8364bc56173010000068ca70f1ece672ac66f65153 (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      5.255.255.77
www.yandex.ru.                600     IN      A      77.88.55.88

;; Query time: 4075 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Sep 17 08:27:29 UTC 2025
;; MSG SIZE rcvd: 118

[root@server.ahmedfarg.net ~]# █

```

Рис. 2.4: Результаты dig с локальным сервером

2.4 Настройка DNS по умолчанию для хоста

1. Через `nmcli` выполнены изменения конфигурации соединения `eth0`:

- отключён авто-DNS,
- в качестве сервера указан `127.0.0.1`.

```

[root@server.ahmedfarg.net ~]#
[root@server.ahmedfarg.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, ip
v4, 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.ahmedfarg.net ~]# systemctl restart NetworkManager
[root@server.ahmedfarg.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search ahmedfarg.net
nameserver 127.0.0.1
[root@server.ahmedfarg.net ~]#

```

Рис. 2.5: Настройка DNS в NetworkManager

2. После перезапуска NetworkManager в файле `/etc/resolv.conf` появился новый nameserver — 127.0.0.1.

2.5 Разрешение запросов от внутренних узлов

1. В файле `/etc/named.conf` внесены изменения:
 - `listen-on port 53 { 127.0.0.1; any; };` — разрешено прослушивание всех интерфейсов,
 - `allow-query { localhost; 192.168.0.0/16; };` — разрешены запросы от внутренней сети.

```

1 //
2 // named.conf
3 //
4 // Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
5 // server as a caching only nameserver (as a localhost DNS resolver only).
6 //
7 // See /usr/share/doc/bind*/sample/ for example named configuration files.
8 //
9
10 options {
11     listen-on port 53 { 127.0.0.1; any; };
12     listen-on-v6 port 53 { ::1; };
13     directory "/var/named";
14     dump-file "/var/named/data/cache_dump.db";
15     statistics-file "/var/named/data/named_stats.txt";
16     memstatistics-file "/var/named/data/named_mem_stats.txt";
17     secroots-file "/var/named/data/named.secroots";
18     recursing-file "/var/named/data/named.recursing";
19     allow-query { localhost; 192.168.0.0/16; };
20 }
21
22 /*
23  * If you are building an AUTHORITY DNS server, do NOT enable recursion
24  */

```

2.6 Настройка firewall и проверка

1. Внесены изменения в правила брандмауэра для разрешения работы службы DNS.
2. Проверка через `lsof` подтвердила, что процесс **named** прослушивает порт 53 по протоколу UDP.

```

[root@server.ahmedfarg.net ~]# gedit /etc/named.conf
[root@server.ahmedfarg.net ~]# firewall-cmd --add-service=dns
success
[root@server.ahmedfarg.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.ahmedfarg.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-daemon	887	avahi	12u	IPv4	7922	0t0	UDP *:mdns
avahi-daemon	887	avahi	13u	IPv6	7923	0t0	UDP *:mdns
chronyd	949	chrony	5u	IPv4	8721	0t0	UDP localhost:32
chronyd	949	chrony	6u	IPv6	8722	0t0	UDP localhost:32
named	28507	named	25u	IPv4	77234	0t0	UDP localhost:do
named	28507	named	26u	IPv4	77235	0t0	UDP localhost:do
named	28507	named	31u	IPv6	77238	0t0	UDP localhost:do
named	28507	named	32u	IPv6	77239	0t0	UDP localhost:do
named	28507 28508	isc-net-0	25u	IPv4	77234	0t0	UDP localhost:do

Рис. 2.6: Проверка через `lsof`

2.7 Конфигурирование первичного DNS-сервера

1. На основе шаблона `named.rfc1912.zones` создан новый файл описания зон `user.net`.

В конфигурационном файле `/etc/named.conf` подключён данный файл с помощью директивы `include`.

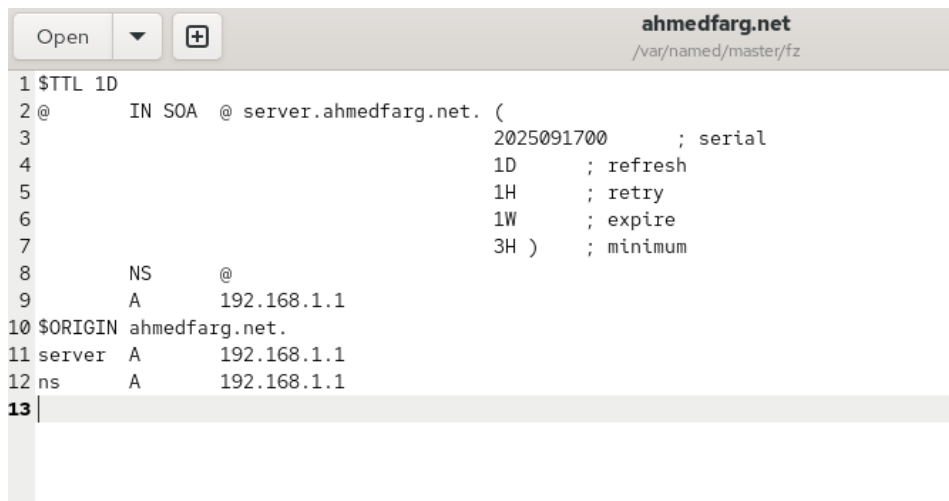
```
1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ for example named configuration files.
11 //
12 // Note: empty-zones-enable yes; option is default.
13 // If private ranges should be forwarded, add
14 // disable-empty-zone "."; into options
15 //
16
17 zone "ahmedfarg.net" IN {
18     type master;
19     file "master/fz/ahmedfarg.net";
20     allow-update { none; };
21 };
22
23 zone "1.168.192.in-addr.arpa" IN {
24     type master;
25     file "master/rz/192.168.1";
26     allow-update { none; };
27 };
```

Рис. 2.7: Файл `user.net` с описанием зон

2. Для прямой зоны `ahmedfarg.net` создан файл `/var/named/master/fz/ahmedfarg.net`.

В нём определены:

- SOA-запись с главным сервером `server.ahmedfarg.net`,
- NS-запись,
- А-записи для узлов `server` и `ns`, указывающие на `192.168.1.1`.



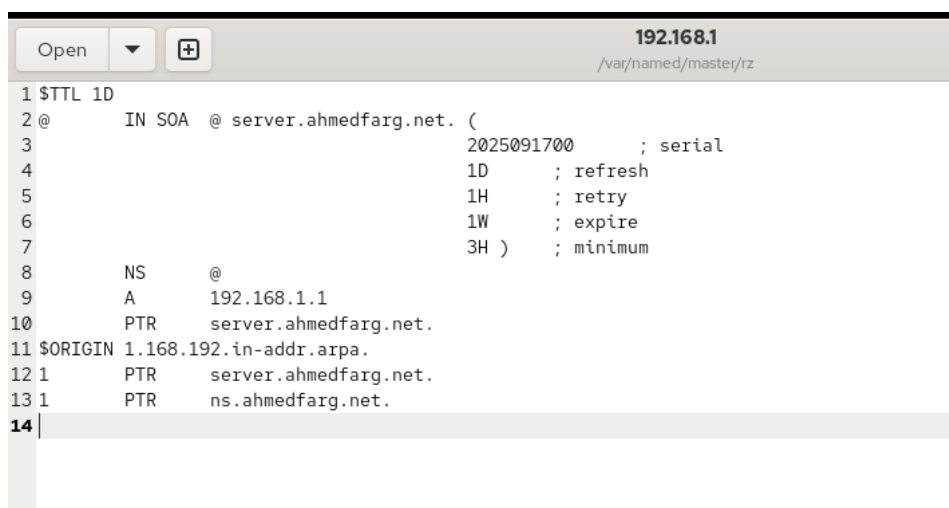
```
1 $TTL 1D
2 @      IN SOA  @ server.ahmedfarg.net. (
3                               2025091700      ; serial
4                               1D      ; refresh
5                               1H      ; retry
6                               1W      ; expire
7                               3H )    ; minimum
8      NS      @
9      A      192.168.1.1
10 $ORIGIN ahmedfarg.net.
11 server A      192.168.1.1
12 ns    A      192.168.1.1
13
```

Рис. 2.8: Прямая зона ahmedfarg.net

3. Для обратной зоны 1.168.192.in-addr.arpa создан файл /var/named/master/rz/192.168.1

В нём заданы:

- SOA-запись,
- NS-запись,
- PTR-записи, сопоставляющие IP-адрес 192.168.1.1 с именами server.ahmedfarg.net и ns.ahmedfarg.net.



```
1 $TTL 1D
2 @      IN SOA  @ server.ahmedfarg.net. (
3                               2025091700      ; serial
4                               1D      ; refresh
5                               1H      ; retry
6                               1W      ; expire
7                               3H )    ; minimum
8      NS      @
9      A      192.168.1.1
10     PTR      server.ahmedfarg.net.
11 $ORIGIN 1.168.192.in-addr.arpa.
12 1      PTR      server.ahmedfarg.net.
13 1      PTR      ns.ahmedfarg.net.
14
```

Рис. 2.9: Обратная зона 192.168.1

4. Для корректной работы демона **named** были исправлены права доступа и SELinux-контексты:

- рекурсивно изменены владельцы каталогов `/etc/named` и `/var/named` на `named:named`,
- выполнено восстановление контекстов командой `restorecon`,
- включён параметр SELinux `named_write_master_zones`.

```
[root@server.ahmedfarg.net rz]#
[root@server.ahmedfarg.net rz]# chown -R named:named /etc/named
[root@server.ahmedfarg.net rz]# chown -R named:named /var/named
[root@server.ahmedfarg.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-20250917.080347.0005 from system_u:object_r:lvm_metadata_t:s0 to system_u:object_r:lvm_etc_t:s0
Relabeled /etc/NetworkManager/system-connections/eth1.nmconnection from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:NetworkManager_etc_rw_t:s0
Relabeled /etc/named.conf from unconfined_u:object_r:etc_t:s0 to unconfined_u:object_r:named_conf_t:s0
[root@server.ahmedfarg.net rz]# restorecon -vR /var/named/
[root@server.ahmedfarg.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ahmedfarg.net rz]# systemctl restart named
[root@server.ahmedfarg.net rz]#
```

Рис. 2.10: Настройка прав и SELinux для named

5. После внесённых изменений сервис `named` был перезапущен. Ошибки при проверке логов отсутствуют, зоны были загружены успешно.

2.8 Анализ работы DNS-сервера

1. С помощью утилиты `dig` был выполнен запрос к серверу `ns.ahmedfarg.net`. Ответ показал, что доменное имя `ns.ahmedfarg.net` корректно сопоставляется с адресом `192.168.1.1`.

```

[root@server.ahmedfarg.net rz]# dig ns.ahmedfarg.net

; <<>> DiG 9.18.33 <<>> ns.ahmedfarg.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40098
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 73b5b079eeb4e4240100000068ca757f64fba67aa528b284 (good)
;; QUESTION SECTION:
;ns.ahmedfarg.net.                IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Sep 17 08:46:55 UTC 2025
;; MSG SIZE rcvd: 89

[root@server.ahmedfarg.net rz]# █

```

Рис. 2.11: Результат dig ns.ahmedfarg.net

2. С помощью утилиты host проведён анализ зоны ahmedfarg.net:

- перечислены все записи зоны (A, NS, SOA),
- подтверждено наличие привязки имени ahmedfarg.net к адресу 192.168.1.1,
- проверены обратные PTR-записи для IP-адреса 192.168.1.1.

```

[root@server.ahmedfarg.net rz]#
[root@server.ahmedfarg.net rz]# host -l ahmedfarg.net
ahmedfarg.net name server ahmedfarg.net.
ahmedfarg.net has address 192.168.1.1
ns.ahmedfarg.net has address 192.168.1.1
server.ahmedfarg.net has address 192.168.1.1
[root@server.ahmedfarg.net rz]# host -a ahmedfarg.net
Trying "ahmedfarg.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23958
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
ahmedfarg.net.                86400   IN      SOA      ahmedfarg.net. server.ahmedfarg.net. 2025091700 86400 3600 604800
10800
ahmedfarg.net.                86400   IN      NS       ahmedfarg.net.
ahmedfarg.net.                86400   IN      A        192.168.1.1

Received 104 bytes from 127.0.0.1#53 in 1 ms
[root@server.ahmedfarg.net rz]# host -t A ahmedfarg.net
ahmedfarg.net has address 192.168.1.1
[root@server.ahmedfarg.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ahmedfarg.net.
1.1.168.192.in-addr.arpa domain name pointer server.ahmedfarg.net.
[root@server.ahmedfarg.net rz]# █

```

Рис. 2.12: Анализ зоны через host

Результаты подтверждают корректную работу как прямой, так и обратной зон.

2.9 Внесение изменений в настройки окружения

1. В каталоге /vagrant/provision/server/ создан подкаталог dns, куда были помещены конфигурационные файлы DNS.

```

1.1.168.192.in-addr.arpa domain name pointer server.ahmedfarg.net.
[root@server.ahmedfarg.net rz]#
[root@server.ahmedfarg.net rz]# cd /vagrant/
[root@server.ahmedfarg.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named/
[root@server.ahmedfarg.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
[root@server.ahmedfarg.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.ahmedfarg.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.ahmedfarg.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.ahmedfarg.net vagrant]# ls
Makefile  Vagrantfile  vagrant-virtualbox-rockylinux10-x86_64.box
[root@server.ahmedfarg.net vagrant]# cd provision/server/
[root@server.ahmedfarg.net server]# ls
01-dummy.sh  02-forward.sh  dns
[root@server.ahmedfarg.net server]# touch dns.sh
[root@server.ahmedfarg.net server]# █

```

Рис. 2.13: Подготовка каталогов для DNS

2. В каталоге /vagrant/provision/server/ создан исполняемый скрипт dns.sh.

В нём описаны:

- установка необходимых пакетов (bind, bind-utils),

- копирование конфигурации,
- настройка владельцев и контекстов SELinux,
- настройка firewall,
- правка DNS-параметров в сетевом соединении,
- запуск и автозапуск сервиса named.

```

1  #!/bin/bash
2  echo "Provisioning script $0"
3  echo "Install needed packages"
4  dnf -y install bind bind-utils
5  echo "Copy configuration files"
6  cp -R /vagrant/provision/server/dns/etc/* /etc
7  cp -R /vagrant/provision/server/dns/var/named/* /var/named
8  chown -R named:named /etc/named
9  chown -R named:named /var/named
10 restorecon -vR /etc
11 restorecon -vR /var/named
12 echo "Configure firewall"
13 firewall-cmd --add-service=dns
14 firewall-cmd --add-service=dns --permanent
15 echo "Tuning SELinux"
16 setsebool named_write_master_zones 1
17 setsebool -P named_write_master_zones 1
18 echo "Change dns server address"
19 nmcli connection edit "System eth0" <<EOF
20 remove ipv4.dns
21 set ipv4.ignore-auto-dns yes
22 set ipv4.dns 127.0.0.1
23 save
24 quit
25 EOF
26 systemctl restart NetworkManager
27 echo "Start named service"
28 systemctl enable named
29 systemctl start named
30

```

Рис. 2.14: Скрипт автоматической настройки dns.sh

3. В файле Vagrantfile добавлен вызов скрипта dns.sh для автоматической настройки DNS при развёртывании виртуальной машины.

```

64     server.ssh.username = 'vagrant'
65     server.ssh.password = 'vagrant'
66
67     server.vm.network :private_network,
68                       ip: "192.168.1.1",
69                       virtualbox____intnet: true
70
71     server.vm.provider :virtualbox do |virtualbox|
72       virtualbox.customize ["modifyvm", :id, "--vrde", "on"]
73       virtualbox.customize ["modifyvm", :id, "--vrdeport", "3391"]
74     end
75
76     server.vm.provision "server dummy",
77                       type: "shell",
78                       preserve_order: true,
79                       path: "provision/server/01-dummy.sh"
80
81     server.vm.provision "server dns",
82                       type: "shell",
83                       preserve_order: true,
84                       path: "provision/server/dns.sh"
85
86   end
87
88   ## Client configuration
89   config.vm.define "client", autostart: false do |client|
90     client.vm.box = "rockylinux10"
91     client.vm.hostname = 'client'
92

```

Рис. 2.15: Vagrantfile с настройкой DNS

3 Заключение

DNS-сервер был успешно установлен, настроен для прямой и обратной зон и проверен, после чего его конфигурация автоматизирована с помощью скрипта и Vagrant.

4 Контрольные вопросы

1. Что такое DNS?

DNS — система доменных имён, преобразующая доменные адреса в IP и обратно.

2. Каково назначение кэширующего DNS-сервера?

Хранит результаты запросов для ускорения доступа и снижения нагрузки на внешние DNS.

3. Чем отличается прямая DNS-зона от обратной?

Прямая зона сопоставляет имена с IP (A-записи), обратная — IP с именами (PTR-записи).

4. В каких каталогах и файлах располагаются настройки DNS-сервера?

- `/etc/named.conf` — основной конфиг;
- `/etc/named/*.zones` — описание зон;
- `/var/named/` — файлы прямых и обратных зон;
- `/etc/resolv.conf` — DNS-серверы по умолчанию.

5. Что указывается в файле `resolv.conf`?

Адреса DNS-серверов, домен поиска и суффиксы поиска.

6. Какие типы записи описания ресурсов есть в DNS?

- A — IPv4-адрес
- AAAA — IPv6-адрес
- NS — серверы имён
- SOA — начальная запись зоны
- PTR — обратное разрешение
- MX — почтовые сервера
- CNAME — псевдоним
- TXT — произвольный текст

7. Для чего используется домен in-addr.arpa?

Для обратного разрешения IP → имя.

8. Для чего нужен демон named?

Это служба (BIND), реализующая работу DNS-сервера.

9. Функции slave-сервера и master-сервера?

Master хранит оригинальные зоны, slave получает копии через zone transfer.

10. Какие параметры отвечают за время обновления зоны?

В SOA-записи: serial, refresh, retry, expire, minimum.

11. Как обеспечить защиту зоны от скачивания?

Настроить allow-transfer и ACL для ограничения zone transfer.

12. Какая запись применяется для почтовых серверов?

MX (Mail Exchanger).

13. Как протестировать работу DNS-сервера?

Утилитами dig, host, nslookup.

14. Как управлять службой?

systemctl start|stop|restart|status <служба>.

15. Как посмотреть отладочную информацию службы?

journalctl -xe или запуск с повышенным логированием.

16. Где хранится отладочная информация?

В journalctl и в /var/log/ (например, /var/log/messages).

17. Как посмотреть файлы процесса?

lsof -p <PID>, lsof -i :53, cat /proc/<PID>/fd/.

18. Примеры nmcli:

- nmcli con show — список соединений
- nmcli con mod eth0 ipv4.addresses 192.168.1.10/24 — задать IP
- nmcli con mod eth0 ipv4.gateway 192.168.1.1 — задать шлюз
- nmcli con mod eth0 ipv4.dns 8.8.8.8 — задать DNS

19. Что такое SELinux?

Система обязательного контроля доступа в Linux.

20. Что такое контекст SELinux?

Метка безопасности, определяющая доступ к объекту.

21. Как восстановить контекст SELinux?

restorecon -Rv /путь.

22. Как создать правила из логов SELinux?

С помощью `audit2allow` на основе `/var/log/audit/audit.log`.

23. Что такое булевый переключатель SELinux?

Параметр, включающий или отключающий определённые функции политики.

24. Как посмотреть переключатели SELinux?

`getsebool -a`.

25. Как изменить значение переключателя SELinux?

`setsebool имя on/off` или `setsebool -P имя on/off` для сохранения.