

Отчёт по лабораторной работе №2

Дисциплина: Администрирование сетевых подсистем

Ибрахим Мохсейн Алькамаль

Содержание

1 Цель работы	5
2 Выполнение лабораторной работы	6
2.1 Установка DNS-сервера	6
2.2 Конфигурирование кэширующего DNS-сервера	8
2.3 Конфигурирование первичного DNS-сервера	15
2.4 Проверка работоспособности первичного DNS-сервера	17
2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины	19
3 Выводы	22
4 Контрольные вопросы:	23
5 Список литературы	26

Список иллюстраций

2.1	Переход в режим суперпользователя sudo -i	6
2.2	Установка пакетов bind и bind-utils через dnf	7
2.3	Результат запроса dig www.yandex.ru	7
2.4	Содержимое файла /etc/resolv.conf	8
2.5	Конфигурация файла /etc/named.conf	9
2.6	Содержимое файла named.ca (корневые серверы)	10
2.7	Содержимое файла named.localhost	11
2.8	Содержимое файла named.loopback	11
2.9	Проверка работы named и сравнение запросов dig	12
2.10	Настройка DNS через nmcli и проверка resolv.conf	13
2.11	Изменение параметров listen-on и allow-query	13
2.12	Проверка прослушивания порта 53 процессом named	14
2.13	Добавление forwarders и отключение DNSSEC в named.conf	14
2.14	Копирование и подключение файла зоны alkamal.net в named.conf	15
2.15	Определение прямой и обратной зон в файле alkamal.net	15
2.16	Создание каталогов master/fz и master/rz и подготовка файла прямой зоны	16
2.17	Настройка файла обратной DNS-зоны 192.168.1	16
2.18	Восстановление SELinux-контекста и перезапуск службы named	17
2.19	Результат выполнения команды dig для ns.alkamal.net	18
2.20	Вывод команды host -l для зоны alkamal.net	18
2.21	Расширенный запрос host -a для alkamal.net	18
2.22	Проверка A- и PTR-записей зоны alkamal.net	19
2.23	Подготовка структуры каталогов и копирование конфигурации DNS в /vagrant	19
2.24	Содержимое provisioning-скрипта dns.sh	20
2.25	Добавление provisioning-скрипта dns.sh в конфигурацию Vagrantfile	21

Список таблиц

1 Цель работы

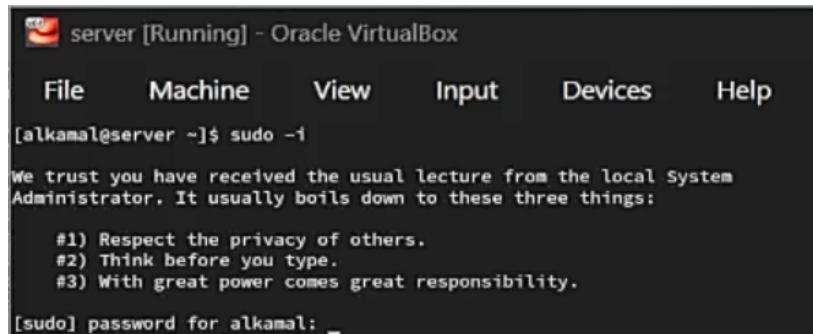
Здесь приводится формулировка цели лабораторной работы. Формулировки цели для каждой лабораторной работы приведены в методических указаниях.

Цель данного шаблона — максимально упростить подготовку отчётов по лабораторным работам. Модифицируя данный шаблон, студенты смогут без труда подготовить отчёт по лабораторным работам, а также познакомиться с основными возможностями разметки Markdown.

2 Выполнение лабораторной работы

2.1 Установка DNS-сервера

На виртуальной машине server выполнен вход под пользователем alkamal и переход в режим суперпользователя с помощью команды sudo -i, что подтверждается сменой приглашения командной строки на root (рис. 2.1).



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a command line interface. The user has typed "[alkamal@server ~]\$ sudo -i" and is presented with a root shell. The terminal displays a standard sudo root prompt message: "We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things: #1) Respect the privacy of others. #2) Think before you type. #3) With great power comes great responsibility." Finally, it asks for a password with the message "[sudo] password for alkamal:".

Рисунок 2.1: Переход в режим суперпользователя sudo -i

В режиме суперпользователя установлены пакеты bind и bind-utils с использованием dnf -y install bind bind-utils; транзакция завершена успешно, зависимости разрешены, пакеты установлены (рис. 2.2).

```
[root@server.alkamal.net ~]# dnf -y install bind bind-utils
Rocky Linux 9 - BaseOS
Rocky Linux 9 - AppStream
Rocky Linux 9 - Extras
Package bind-utils-32:9.16.23-34.el9_7.1.x86_64 is already installed.
Dependencies resolved.
=====
Transaction Summary
=====
Install 5 Packages
=====
Total download size: 809 k
Installed size: 2.0 M
Downgrading Packages:
(1/5) bind-dnssec-doc-9.16.23-34.el9_7.1.noarch.rpm           7.7 kB/s | 4.3 kB  00:00
(2/5) python3-ply-3.11-14.el9.0.1.noarch.rpm                  10 kB/s | 4.8 kB  00:00
(3/5) bind-dnssec-32:9.16.23-34.el9_7.1.x86_64.rpm          7.0 kB/s | 3.1 kB  00:00
(4/5) bind-9.16.23-34.el9_7.1.x86_64.rpm                     00:00
(5/5) python3-bind-9.16.23-34.el9_7.1.noarch.rpm            7.0 kB/s | 61 kB  00:00
=====
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
=====
  Installing : bind-dnssec-doc-32:9.16.23-34.el9_7.1.noarch      1/1
  Installing : python3-ply-3.11-14.el9.0.1.noarch               1/5
  Installing : bind-dnssec-32:9.16.23-34.el9_7.1.x86_64        2/5
  Installing : bind-dnssec-utils-32:9.16.23-34.el9_7.1.x86_64   3/5
  Running scriptlet: bind-32:9.16.23-34.el9_7.1.x86_64       4/5
  Installing : bind-9.16.23-34.el9_7.1.x86_64                 5/5
  Running scriptlet: bind-32:9.16.23-34.el9_7.1.x86_64       5/5
  Verifying  : bind-dnssec-doc-32:9.16.23-34.el9_7.1.noarch     1/5
  Verifying  : bind-dnssec-32:9.16.23-34.el9_7.1.x86_64        2/5
  Verifying  : bind-dnssec-utils-32:9.16.23-34.el9_7.1.x86_64   3/5
  Verifying  : python3-bind-9.16.23-34.el9_7.1.noarch          4/5
  Verifying  : python3-bind-32:9.16.23-34.el9_7.1.noarch         5/5
=====
Installed:
bind-32:9.16.23-34.el9_7.1.x86_64      bind-dnssec-doc-32:9.16.23-34.el9_7.1.noarch      bind-dnssec-utils-32:9.16.23-34.el9_7.1.x86_64
python3-bind-32:9.16.23-34.el9_7.1.noarch    python3-ply-3.11-14.el9.0.1.noarch
=====
Complete!
```

Рисунок 2.2: Установка пакетов bind и bind-utils через dnf

С помощью утилиты `dig` выполнен DNS-запрос к имени `www.yandex.ru`; в выводе отображены заголовок ответа (opcode: QUERY, status: NOERROR), флаги (qr, rd, ra), секции QUESTION и ANSWER с тремя A-записями и временем отклика, что подтверждает корректное разрешение имени через внешний DNS-сервер (рис. 2.3).

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

; <>> _D I G 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27330
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x0187, udp: 512
;; QUESTION SECTION:
;www.yandex.ru.      IN      A

;; ANSWER SECTION:
www.yandex.ru.      391      IN      A      77.88.44.55
www.yandex.ru.      391      IN      A      77.88.55.88
www.yandex.ru.      391      IN      A      5.255.255.77

;; Query time: 25 msec
;; SERVER: 172.249.0.7#53(172.249.0.7)
;; WHEN: Sat Feb 07 13:34:04 UTC 2026
;; MSG SIZE  rcvd: 129
```

Рисунок 2.3: Результат запроса dig www.yandex.ru

2.2 Конфигурирование кэширующего DNS-сервера

Проанализировано содержимое файла `/etc/resolv.conf`: указан поисковый домен `alkamal.net` и заданы внешние DNS-серверы (`172.249.0.7`, `8.8.8.8`, `8.8.4.4`), что определяет порядок разрешения имён до изменения конфигурации (рис. 2.4).

```
[root@server.alkamal.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search rudn.ru alkamal.net
nameserver 172.249.0.7
nameserver 8.8.8.8
nameserver 8.8.4.4
```

Рисунок 2.4: Содержимое файла `/etc/resolv.conf`

Проанализирован файл `/etc/named.conf`: сервер настроен как кэширующий (`recursion yes`), прослушивает порт 53 только на `127.0.0.1`, разрешены запросы от `localhost`, определены параметры каталогов и подключены стандартные зоны (рис. 2.5).

```
[root@server.alkamal.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.recurse";
    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
       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-validation yes;
    managed-keys-directory "/var/named/dynamic";
    geoip-directory "/usr/share/GeoIP";
    pid-file "/run/named/named.pid";
    session-keyfile "/run/named/session.key";
    /* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
    include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Рисунок 2.5: Конфигурация файла /etc/named.conf

Рассмотрено содержимое файлов /var/named/named.ca, /var/named/named.localhost и /var/named/named.loopback: первый содержит список корневых DNS-серверов (NS, A, AAAA-записи), второй и третий определяют локальные зоны localhost и обратного разрешения 127.0.0.1 (рис. 2.6, рис. 2.7, рис. 2.8).

```
[root@server.alkamal.net ~]# cat /var/named/named.ca
; <>> DiG 9.18.20 <>> -4 +tcp +norec +nostats @d.root-servers.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; -->HEADER<- opcode: QUERY, status: NOERROR, id: 47286
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1450
; QUESTION SECTION:
;.

; IN NS

;; ANSWER SECTION:
. 518400 IN NS a.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS c.root-servers.net.
. 518400 IN NS d.root-servers.net.
. 518400 IN NS e.root-servers.net.
. 518400 IN NS f.root-servers.net.
. 518400 IN NS g.root-servers.net.
. 518400 IN NS h.root-servers.net.
. 518400 IN NS i.root-servers.net.
. 518400 IN NS j.root-servers.net.
. 518400 IN NS k.root-servers.net.
. 518400 IN NS l.root-servers.net.
. 518400 IN NS m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net. 518400 IN A 198.41.0.4
b.root-servers.net. 518400 IN A 170.247.170.2
c.root-servers.net. 518400 IN A 192.33.4.12
d.root-servers.net. 518400 IN A 199.7.91.13
e.root-servers.net. 518400 IN A 192.203.230.10
f.root-servers.net. 518400 IN A 192.5.5.241
g.root-servers.net. 518400 IN A 192.112.36.4
h.root-servers.net. 518400 IN A 198.97.190.53
i.root-servers.net. 518400 IN A 192.36.148.17
j.root-servers.net. 518400 IN A 192.58.128.30
k.root-servers.net. 518400 IN A 193.0.14.129
l.root-servers.net. 518400 IN A 199.7.83.42
m.root-servers.net. 518400 IN A 202.12.27.33
a.root-servers.net. 518400 IN AAAA 2001:503:ba3e::2:30
b.root-servers.net. 518400 IN AAAA 2001:1b8:10::b
c.root-servers.net. 518400 IN AAAA 2001:500:2::c
d.root-servers.net. 518400 IN AAAA 2001:500:500::d
e.root-servers.net. 518400 IN AAAA 2001:500:a8::e
f.root-servers.net. 518400 IN AAAA 2001:500:2f::f
g.root-servers.net. 518400 IN AAAA 2001:500:12::d0d
h.root-servers.net. 518400 IN AAAA 2001:500:1::53
i.root-servers.net. 518400 IN AAAA 2001:7fe::53
j.root-servers.net. 518400 IN AAAA 2001:503:c27::2:30
k.root-servers.net. 518400 IN AAAA 2001:7fd::1
l.root-servers.net. 518400 IN AAAA 2001:500:9f::42
m.root-servers.net. 518400 IN AAAA 2001:dc3::35
```

Рисунок 2.6: Содержимое файла named.ca (корневые серверы)

```
[root@server.alkamal.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
```

Рисунок 2.7: Содержимое файла named.localhost

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

Рисунок 2.8: Содержимое файла named.loopback

DNS-сервер запущен и добавлен в автозагрузку командами `systemctl start named` и `systemctl enable named`; сравнение результатов `dig www.yandex.ru` и `dig @127.0.0.1 www.yandex.ru` показало отсутствие ответа от локального сервера до изменения настроек прослушивания (рис. 2.9).

```
[root@server.alkamal.net ~]# systemctl start named
[root@server.alkamal.net ~]# systemctl enable named
[root@server.alkamal.net ~]# dig www.yandex.ru

; <>> DiG 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28173
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; MBZ: 0x00ad, udp: 512
;; QUESTION SECTION:
;www.yandex.ru.           IN      A

;; ANSWER SECTION:
www.yandex.ru.        173     IN      A      77.88.44.55
www.yandex.ru.        173     IN      A      77.88.55.88
www.yandex.ru.        173     IN      A      5.255.255.77

;; Query time: 45 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Sat Feb 07 14:29:46 UTC 2026
;; MSG SIZE  rcvd: 129

[root@server.alkamal.net ~]# dig @127.0.0.1 www.yandex.ru

; <>> DiG 9.16.23-RH <>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Рисунок 2.9: Проверка работы named и сравнение запросов dig

В NetworkManager изменены параметры соединений eth0 и System eth0: удалены автоматические DNS, включено игнорирование auto-DNS и установлен сервер 127.0.0.1; после перезапуска NetworkManager файл /etc/resolv.conf содержит nameserver 127.0.0.1 (рис. 2.10).

```
[root@server.alkamal.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, prefix-delegation, 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' (d9959f89-4530-41f4-b47c-eb8665daf556) successfully updated.
nmcli> ^[[200~quit
Unknown command: 'quit'
nmcli> quit
[root@server.alkamal.net ~]# nmcli connection edit System\ eth0
==| nmcli interactive connection editor |==

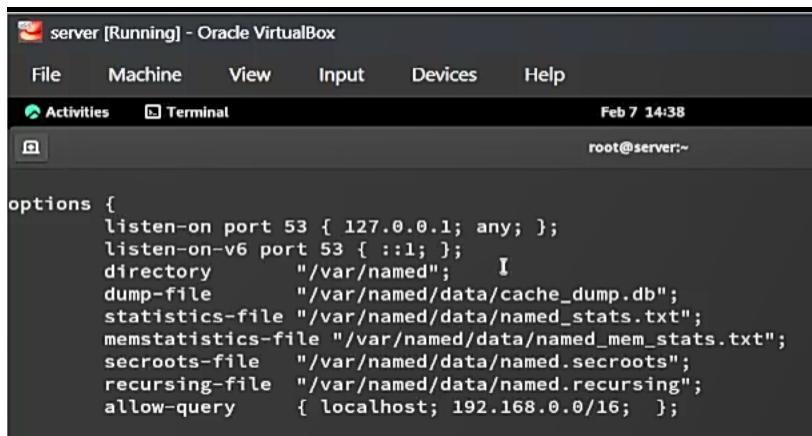
Editing existing '802-3-ethernet' connection: 'System eth0'

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, prefix-delegation, 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 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
[root@server.alkamal.net ~]# systemctl restart NetworkManager
[root@server.alkamal.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search alkamal.net
nameserver 127.0.0.1
[root@server.alkamal.net ~]#
```

Рисунок 2.10: Настройка DNS через nmcli и проверка resolv.conf

В файл `/etc/named.conf` внесены изменения: добавлено прослушивание на всех интерфейсах (`127.0.0.1; any;`) и разрешены запросы от сети `192.168.0.0/16`; также в межсетевом экране разрешена служба DNS (рис. 2.11).



```
options {
    listen-on port 53 { 127.0.0.1; any; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    I
    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.recurse";
    allow-query   { localhost; 192.168.0.0/16; };
}
```

Рисунок 2.11: Изменение параметров listen-on и allow-query

С помощью команды `lsof | grep UDP` подтверждено, что процесс named прослушивает порт 53 (UDP), что свидетельствует о корректной работе DNS-сервера и направлении запросов через узел server (рис. 2.12).

```
[root@server.alkamal.net ~]# firewall-cmd --add-service=dns
success
[root@server.alkamal.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.alkamal.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 558 avahi 12u IPv4 21230 0t0 UDP *:
mdns
avahi-dae 558 avahi 13u IPv6 21231 0t0 UDP *:
mdns
chronyd 604 chrony 5u IPv4 21300 0t0 UDP lo
calhost:323
chronyd 604 chrony 6u IPv6 21301 0t0 UDP lo
calhost:323
named 947 named 21u IPv4 22889 0t0 UDP lo
calhost:domain
named 947 named 24u IPv6 22891 0t0 UDP lo
calhost:domain
named 947 948 isc-net-0 named 21u IPv4 22889 0t0 UDP lo
calhost:domain
named 947 948 isc-net-0 named 24u IPv6 22891 0t0 UDP lo
calhost:domain
named 947 949 isc-net-0 named 21u IPv4 22889 0t0 UDP lo
calhost:domain
named 947 949 isc-net-0 named 24u IPv6 22891 0t0 UDP lo
calhost:domain
named 947 950 isc-timer named 21u IPv4 22889 0t0 UDP lo
calhost:domain
named 947 950 isc-timer named 24u IPv6 22891 0t0 UDP lo
calhost:domain
named 947 951 isc-socke named 21u IPv4 22889 0t0 UDP lo
calhost:domain
named 947 951 isc-socke named 24u IPv6 22891 0t0 UDP lo
calhost:domain
NetworkMa 10969 root 27u IPv4 53305 0t0 UDP se
rver.alkamal.net:bootpc->_gateway:bootps
NetworkMa 10969 10970 gmain root 27u IPv4 53305 0t0 UDP se
rver.alkamal.net:bootpc->_gateway:bootps
NetworkMa 10969 10988 gdbus root 27u IPv4 53305 0t0 UDP se
rver.alkamal.net:bootpc->_gateway:bootps
```

Рисунок 2.12: Проверка прослушивания порта 53 процессом named

В конфигурационном файле `/etc/named.conf` в секцию `options` добавлены директивы `forwarders { 127.0.0.1; };` и `forward first;`, а также отключены параметры `dnssec-enable` и `dnssec-validation`, что обеспечивает перенаправление DNS-запросов на вышестоящий сервер и отказ от проверки DNSSEC (рис. 2.13).

```
options {
    listen-on port 53 { 127.0.0.1; any; };
    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; 192.168.0.0/16; };
    forwarders { 127.0.0.1; };
    forward first;

    /*
     - 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-enable no;
    dnssec-validation no;
    /* dnssec-validation yes; */
```

Рисунок 2.13: Добавление forwarders и отключение DNSSEC в `named.conf`

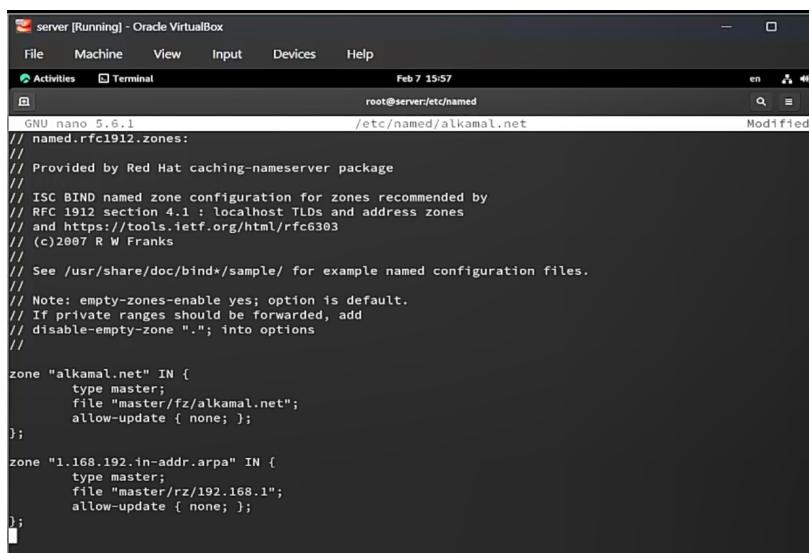
2.3 Конфигурирование первичного DNS-сервера

На первом этапе выполнено копирование шаблона зон DNS `named.rfc1912.zones` в каталог `/etc/named` с последующим переименованием файла в `alkamal.net`, после чего данный файл был подключён в конфигурации `/etc/named.conf` директивой `include "/etc/named/alkamal.net";` (рис. 2.14).

```
[root@server.alkamal.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.alkamal.net ~]# cd /etc/named
[root@server.alkamal.net named]# mv /etc/named/named.rfc1912.zones /etc/named/alkamal.net
[root@server.alkamal.net named]# nano /etc/named.conf
[root@server.alkamal.net named]#
```

Рисунок 2.14: Копирование и подключение файла зоны `alkamal.net` в `named.conf`

Далее в файле `/etc/named/alkamal.net` вместо стандартных зон `localhost.localdomain` и `1.0.0.127.in-addr.arpa` были определены собственные зоны: прямая зона `alkamal.net` с файлом `master/fz/alkamal.net` и обратная зона `1.168.192.in-addr.arpa` с файлом `master/rz/192.168.1` (рис. 2.15).



```
GNU nano 5.6.1
// 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.
//
// Note: empty-zones-enable yes; option is default.
// If private ranges should be forwarded, add
// disable-empty-zone "."; into options
//

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

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

Рисунок 2.15: Определение прямой и обратной зон в файле `alkamal.net`

После этого в каталоге `/var/named` созданы подкаталоги `master/fz` и `master/rz` для размещения файлов прямой и обратной зон. В каталог

master/fz скопирован шаблон named.localhost, который был переименован в alkamal.net (рис. 2.16).

```
[root@server.alkamal.net named]# cd /var/named  
[root@server.alkamal.net named]# pwd  
/var/named  
[root@server.alkamal.net named]# mkdir -p /var/named/master/fz  
[root@server.alkamal.net named]# mkdir -p /var/named/master/rz  
[root@server.alkamal.net named]# ls  
data dynamic master named.ca named.empty named.localhost named.loopback slaves  
[root@server.alkamal.net named]# cd master/  
[root@server.alkamal.net master]# ls  
fz rz  
[root@server.alkamal.net master]# cp /var/named/named.localhost /var/named/master/fz/  
[root@server.alkamal.net master]# cd /var/named/master/fz/  
[root@server.alkamal.net fz]# mv named.localhost alkamal.net  
[root@server.alkamal.net fz]# ls  
alkamal.net
```

Рисунок 2.16: Создание каталогов master/fz и master/rz и подготовка файла прямой зоны

Затем был отредактирован файл обратной зоны /var/named/master/rz/192.168.1: указана директива \$TTL 1D, задана запись SOA с сервером server.alkamal.net., установлен серийный номер формата ГГГММДВВ, добавлена A-запись с адресом 192.168.1.1, а также PTR-записи для соответствия IP-адреса имени server.alkamal.net. и ns.alkamal.net.; директивы \$ORIGIN установлена в 1.168.192.in-addr.arpa. (рис. 2.17).

```
$TTL 1D
@ IN SOA @ server.alkamal.net. ( 2024072700; serial
    1D ; refresh
    1H ; retry
    1W ; expire
    3H ) ; minimum

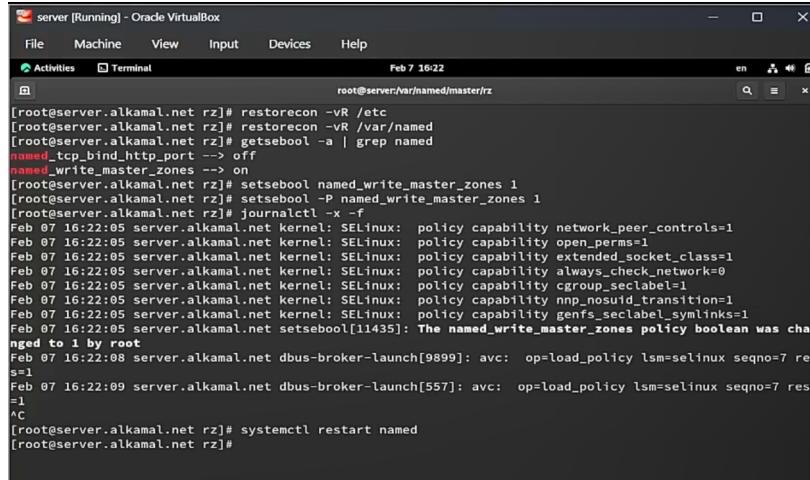
NS @
A 192.168.1.1
PTR server.alkamal.net.

$ORIGIN 1.168.192.in-addr.arpa.
1 PTR server.alkamal.net.
1 PTR ns.alkamal.net.
```

Рисунок 2.17: Настройка файла обратной DNS-зоны 192.168.1

Далее выполнено восстановление контекстов безопасности SELinux для каталогов /etc и /var/named, проверены SELinux-переключатели для службы

named, после чего активирован параметр `named_write_master_zones` и сервер DNS перезапущен командой `systemctl restart named` (рис. 2.18).



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The terminal session is as follows:

```
[root@server:~]# restorecon -vR /etc
[root@server:~]# restorecon -vR /var/named
[root@server:~]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server:~]# setsebool named_write_master_zones 1
[root@server:~]# setsebool -P named_write_master_zones 1
[root@server:~]# journalctl -x -f
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability network_peer_controls=1
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability open_perms=1
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability extended_socket_class=1
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability always_check_network=0
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability cgroup_seclabel=1
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability nnp_nosuid_transition=1
Feb 07 16:22:05 server.alkamal.net kernel: SELinux: policy capability genfs_seclabel_symlinks=1
Feb 07 16:22:05 server.alkamal.net setsebool[11435]: The named_write_master_zones policy boolean was changed to 1 by root
Feb 07 16:22:08 server.alkamal.net dbus-broker-launch[9899]: avc: op=load_policy lsm=selinux seqno=7 res=s=1
Feb 07 16:22:09 server.alkamal.net dbus-broker-launch[557]: avc: op=load_policy lsm=selinux seqno=7 res=s=1
^C
[root@server:~]# systemctl restart named
[root@server:~]#
```

Рисунок 2.18: Восстановление SELinux-контекста и перезапуск службы named

2.4 Проверка работоспособности первичного DNS-сервера

После перезапуска службы named выполнена проверка разрешения имени `ns.alkamal.net` с помощью утилиты `dig`. В ответе сервера получен статус NOERROR, в разделе ANSWER возвращена A-запись `192.168.1.1`, сервером указан `127.0.0.1#53`, что подтверждает корректную работу локального DNS-сервера (рис. 2.19).

```
[root@server.alkamal.net rz]# dig ns.alkamal.net
; <>> DiG 9.16.23-RH <>> ns.alkamal.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 23157
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;;
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; COOKIE: f26d31abcbab90501000000698766d71e79e3e79341671c (good)
;; QUESTION SECTION:
;ns.alkamal.net.           IN      A
;;
;; ANSWER SECTION:
ns.alkamal.net.     86400   IN      A      192.168.1.1
;;
;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Feb 07 16:22:47 UTC 2026
;; MSG SIZE rcvd: 87
```

Рисунок 2.19: Результат выполнения команды dig для ns.alkamal.net

Далее выполнена передача зоны командой host -l alkamal.net. В выводе отображаются NS-запись server.alkamal.net. и A-записи для alkamal.net, ns.alkamal.net и server.alkamal.net с адресом 192.168.1.1, что подтверждает корректную настройку прямой зоны (рис. 2.20).

```
[root@server.alkamal.net rz]# host -l alkamal.net
alkamal.net name server server.alkamal.net.
alkamal.net has address 192.168.1.1
ns.alkamal.net has address 192.168.1.1
server.alkamal.net has address 192.168.1.1
```

Рисунок 2.20: Вывод команды host -l для зоны alkamal.net

Командой host -a alkamal.net выполнен расширенный запрос типа ANY. В разделе ANSWER присутствуют записи SOA, NS и A, что подтверждает корректность параметров зоны и серийного номера (рис. 2.21).

```
[root@server.alkamal.net rz]# host -a alkamal.net
Trying "alkamal.net"
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 26115
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;;
;; QUESTION SECTION:
;alkamal.net.           IN      ANY
;;
;; ANSWER SECTION:
alkamal.net.      86400   IN      SOA    alkamal.net. server.alkamal.net. 2026020701 86400 3600 6
04800 10800
alkamal.net.      86400   IN      NS     server.alkamal.net.
alkamal.net.      86400   IN      A      192.168.1.1
Received 182 bytes from 127.0.0.1#53 in 0 ms
```

Рисунок 2.21: Расширенный запрос host -a для alkamal.net

Затем выполнена проверка прямого и обратного разрешения имени. Команда host -t A alkamal.net возвращает IP-адрес 192.168.1.1. Команда host -t PTR 192.168.1.1 возвращает PTR-записи server.alkamal.net. и

`ns.alkamal.net.`, что подтверждает корректную настройку обратной зоны `1.168.192.in-addr.arpa` (рис. 2.22).

```
[root@server.alkamal.net rz]# host -t A alkamal.net
alkamal.net has address 192.168.1.1
[root@server.alkamal.net rz]# host -t PTR alkamal.net
alkamal.net has no PTR record
[root@server.alkamal.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.alkamal.net.
1.1.168.192.in-addr.arpa domain name pointer ns.alkamal.net.
```

Рисунок 2.22: Проверка A- и PTR-записей зоны alkamal.net

2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

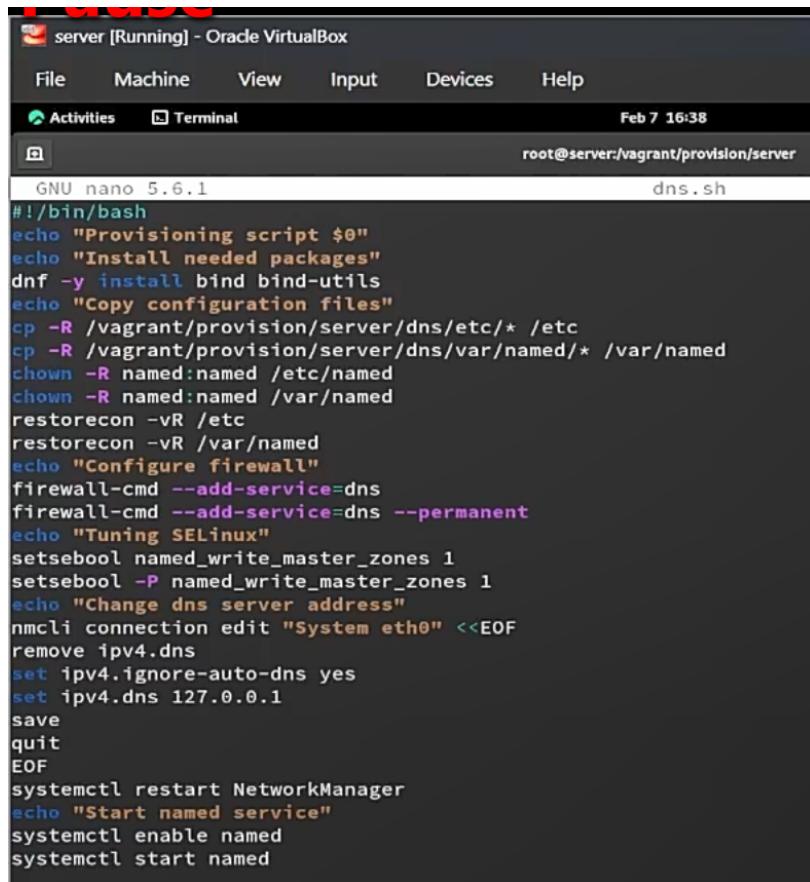
На виртуальной машине `server` выполнен переход в каталог `/vagrant`, после чего созданы подкаталоги `provision/server/dns/etc/named` и `provision/server/dns/var/named/master`. Далее скопированы файлы `/etc/named.conf`, содержимое `/etc/named/` и файлы зон из `/var/named/master/` в соответствующие каталоги внутри `/vagrant/provision/server` (рис. 2.23).

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

Рисунок 2.23: Подготовка структуры каталогов и копирование конфигурации DNS в `/vagrant`

Затем в каталоге `/vagrant/provision/server` создан исполняемый файл `dns.sh`, в который внесён скрипт автоматической установки и настройки DNS-сервера: установка пакетов `bind` и `bind-utils`, копирование конфигурационных файлов в системные каталоги `/etc` и `/var/named`, изменение владельца на `named:named`, восстановление SELinux-контекстов, настройка межсетевого экрана для службы `dns`, включение параметра `named_write_master_zones`, изменение DNS-адреса соединения `System eth0` на `127.0.0.1`, перезапуск

NetworkManager, а также включение и запуск службы named (рис. 2.24).



The screenshot shows a terminal window titled "server [Running] - Oracle VirtualBox". The window has a dark theme with white text. At the top, there's a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu is a toolbar with "Activities" and "Terminal". The status bar at the bottom right shows "Feb 7 16:38" and "root@server:/vagrant/provision/server". The main area of the terminal contains a script named "dns.sh" which is being edited in nano 5.6.1. The script content is as follows:

```
GNU nano 5.6.1
#!/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 "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
```

Рисунок 2.24: Содержимое provisioning-скрипта dns.sh

Для автоматического выполнения данного скрипта при загрузке виртуальной машины в файл Vagrantfile в разделе конфигурации сервера добавлен provision-блок типа shell с путём provision/server/dns.sh и параметром preserve_order: true, что обеспечивает последовательное выполнение сценария при старте VM (рис. 2.25).

```
C: > work > alkamal > vagrant > Vagrantfile
19  ## Server configuration
20  config.vm.define "server", autostart: false do |server|
21    server.vm.box = "rocky9"
22    server.vm.hostname = 'server'
23    server.vm.boot_timeout = 1440
24    server.ssh.insert_key = false
25    server.ssh.username = 'vagrant'
26    server.ssh.password = 'vagrant'
27    server.vm.network :private_network,
28      ip: "192.168.1.1",
29      virtualbox_intnet: true
30    server.vm.provision "server dummy",
31      type: "shell",
32      preserve_order: true,
33      path: "provision/server/01-dummy.sh"
34    server.vm.provision "server dns",
35      type: "shell",
36      preserve_order: true,
37      path: "provision/server/dns.sh"
```

Рисунок 2.25: Добавление provisioning-скрипта dns.sh в конфигурацию Vagrantfile

3 Выводы

В ходе работы выполнена установка и настройка кэширующего и первичного DNS-сервера на базе BIND.

Сервер успешно сконфигурирован для работы в режиме recursive caching, а также в режиме первичного (master) сервера для прямой зоны **alkamal.net** и обратной зоны **1.168.192.in-addr.arpa**.

Настроены A- и PTR-записи, подтверждена авторитетность сервера по флагу **aa** в ответах **dig**. Проверка утилитами **dig** и **host** показала корректное разрешение имён и обратное разрешение IP-адреса 192.168.1.1.

Обеспечена работа DNS через внутреннюю виртуальную сеть: – изменены параметры **listen-on** и **allow-query**; – открыт сервис DNS в firewall; – настроены политики SELinux; – сервер назначен DNS-сервером по умолчанию (127.0.0.1).

Дополнительно выполнена автоматизация конфигурации с использованием provisioning-скрипта **dns.sh** и интеграции в **Vagrantfile**, что обеспечивает воспроизводимость настройки при перезапуске виртуальной машины.

4 Контрольные вопросы:

1. Что такое DNS? - Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса, используемые компьютерами для идентификации друг друга в сети.
2. Каково назначение кэширующего DNS-сервера? - Его задача - хранить результаты предыдущих DNS-запросов в памяти. Когда клиент делает запрос, кэширующий DNS проверяет свой кэш, и если он содержит соответствующую информацию, сервер возвращает ее без необходимости обращаться к другим DNS-серверам. Это ускоряет процесс запроса.
3. Чем отличается прямая DNS-зона от обратной? - Прямая зона преобразует доменные имена в IP-адреса, обратная зона выполняет обратное: преобразует IP-адреса в доменные имена.
4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают. - В Linux-системах обычно используется файл /etc/named.conf для общих настроек. Зоны хранятся в файлах в каталоге /var/named/, например, /var/named/example.com.zone.
5. Что указывается в файле resolv.conf? - Содержит информацию о DNS-серверах, используемых системой, а также о параметрах конфигурации.
6. Какие типы записи описания ресурсов есть в DNS и для чего они используются? - A (IPv4-адрес), AAAA (IPv6-адрес), CNAME (каноническое

имя), MX (почтовый сервер), NS (имя сервера), PTR (обратная запись), SOA (начальная запись зоны), TXT (текстовая информация).

7. Для чего используется домен in-addr.arpa? - Используется для обратного маппинга IP-адресов в доменные имена.
8. Для чего нужен демон named? - Это DNS-сервер, реализация BIND (Berkeley Internet Name Domain).
9. В чём заключаются основные функции slave-сервера и master-сервера? - Master-сервер хранит оригинальные записи зоны, slave-серверы получают копии данных от master-сервера.
10. Какие параметры отвечают за время обновления зоны? - refresh, retry, expire, и minimum.
11. Как обеспечить защиту зоны от скачивания и просмотра? - Это может включать в себя использование TSIG (Transaction SIGnatures) для аутентификации между серверами.
12. Какая запись RR применяется при создании почтовых серверов? - MX (Mail Exchange).
13. Как протестировать работу сервера доменных имён? - Используйте команды nslookup, dig, или host.
14. Как запустить, перезапустить или остановить какую-либо службу в системе? - systemctl start|stop|restart .
15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы? - Используйте опции, такие как -d или -v при запуске службы.
16. Где храниться отладочная информация по работе системы и служб? Как её посмотреть? - В системных журналах, доступных через journalctl.

17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров. - lsof -r или fuser -v .
18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli. - Примеры включают nmcli connection up|down .
19. Что такое SELinux? - Это мандатный контроль доступа для ядра Linux.
20. Что такое контекст (метка) SELinux? - Метка, определяющая, какие ресурсы могут быть доступны процессу или объекту.
21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы? - restorecon -Rv .
22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций? - Используйте audit2allow.
23. Что такое булевый переключатель в SELinux? - Это параметр, который включает или отключает определенные аспекты защиты SELinux.
24. Как посмотреть список переключателей SELinux и их состояние? - getsebool -a.
25. Как изменить значение переключателя SELinux? - setsebool -P <on|off>.

5 Список литературы

1. Barr D. *Common DNS Operational and Configuration Errors*: RFC / RFC Editor. — 02/1996. — DOI: 10.17487/rfc1912.
2. McAllister M., Radvan S., Walsh D., Grift D., Paris E., Morris J. *Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя*. — URL: https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html (дата обращения: 13.09.2021).
3. *Systemd*. — 2015. — URL: <https://wiki.archlinux.org/index.php/Systemd> (visited on 09/13/2021).
4. Костромин В. А. *Утилита lsof – инструмент администратора*. — URL: <http://rus-linux.net/kos.php?name=/papers/lsof/lsof.html> (дата обращения: 13.09.2021).
5. Поттеринг Л. *Systemd для администраторов: цикл статей*. — 2010. — URL: <http://wiki.opennet.ru/Systemd> (дата обращения: 13.09.2021).
6. *Сайт проекта NetworkManager*. — URL: <https://wiki.gnome.org/Projects/NetworkManager> (visited on 09/13/2021).

7. *Cañm proekta nmcli.* –

URL: <https://developer.gnome.org/NetworkManager/stable/nmcli.html>

(visited on 09/13/2021).