Настройка DNS-сервера

Лабораторная работа №2

Элсаиед Адел

2 января 2026

Российский университет дружбы народов, Москва, Россия

Цели и задачи работы

Цель лабораторной работы

Приобретение практических навыков установки и конфигурирования DNS-сервера на базе BIND, а также изучение принципов работы системы доменных имён.

Выполнение работы

Установка DNS-сервера

На виртуальной машине server выполнена установка пакетов bind и bind-utils.

В процессе установки были автоматически разрешены зависимости и подготовлена среда для работы DNS-сервера.

```
[sudo] password for elsaiedadel:
[root@server.elsaiedadel.net ~]# dnf -y install bind bind-utils
Last metadata expiration check: 0:08:47 ago on Fri 02 Jan 2026 08:58:24 AM UTC.
Package bind-utils-32:9.18.33-10.el10_1.2.x86_64 is already installed.
Dependencies resolved.
================================================================================
 Package                 Architecture    Version                 Repository  Size
================================================================================
Installing:
 bind                    x86_64          32:9.18.33-10.el10_1.2  appstream  333 k
Installing weak dependencies:
 bind-dnssec-utils       x86_64          32:9.18.33-10.el10_1.2  appstream  151 k

Transaction Summary
================================================================================
Install  2 Packages

Total download size: 483 k
Installed size: 1.3 M
Downloading Packages:
(1/2): bind-dnssec-utils-9.18.33-10.el10_1.2.x86_64.rpm  1.9 MB/s | 151 kB  00:00
(2/2): bind-9.18.33-10.el10_1.2.x86_64.rpm               2.6 MB/s | 333 kB  00:00
--------------------------------------------------------------------------------
Total                                                    923 kB/s | 483 kB  00:00
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :                                                        1/1
  Installing       : bind-dnssec-utils-32:9.18.33-10.el10_1.2.x86_64        1/2
  Running scriptlet: bind-32:9.18.33-10.el10_1.2.x86_64                     2/2
```

Проверка DNS-разрешения

Для проверки работы DNS-клиента выполнен запрос к доменному имени www.yandex.ru.

Получен корректный ответ со статусом NOERROR и набором A-записей.

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

; <<>> DiG 9.18.33 <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14492
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
www.yandex.ru.          56      IN      A       5.255.255.77
www.yandex.ru.          56      IN      A       77.88.44.55
www.yandex.ru.          56      IN      A       77.88.55.88

;; Query time: 28 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Fri Jan 02 09:07:40 UTC 2026
;; MSG SIZE  rcvd: 90
```

Анализ конфигурационных файлов

Проанализированы основные конфигурационные файлы DNS: - /etc/resolv.conf — настройки DNS-клиента; - /etc/named.conf — основная конфигурация BIND.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search elsaiedadel.net
nameserver 10.0.2.3
[root@server.elsaiedadel.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.
```

Корневые DNS-серверы

Рассмотрен файл named.ca, содержащий сведения о корневых DNS-серверах Интернета, используемых для инициализации DNS-кэша.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# cat /var/named/named.ca
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update:     December 20, 2023
;       related version of root zone:     2023122001
;
; FORMERLY NS.INTERNIC.NET
;
.                       3600000      NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:ba3e::2:30
;
; FORMERLY NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     170.247.170.2
B.ROOT-SERVERS.NET.     3600000      AAAA  2801:1b8:10::b
```

Локальные зоны

Проанализированы файлы named.localhost и named.loopback, обеспечивающие корректную работу локального DNS-разрешения.

```
[root@server.elsaiedadel.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.elsaiedadel.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.
```

Проверка локального DNS-сервера

Выполнен DNS-запрос с явным указанием локального сервера 127.0.0.1.

Полученный ответ показал необходимость дополнительной настройки сервера.

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

; <<>> DiG 9.18.33 <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 11124
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b322f7f10df2b23c0100000069578c16b29105ec077c44b1 (good)
;; QUESTION SECTION:
;www.yandex.ru.                  IN      A

;; Query time: 4058 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Jan 02 09:12:54 UTC 2026
;; MSG SIZE  rcvd: 70

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

Настройка DNS по умолчанию

Сетевое соединение eth0 настроено на использование DNS-сервера 127.0.0.1.

Изменения подтверждены в файле resolv.conf.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.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, ipv
6, 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' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.elsaiedadel.net ~]# systemctl restart NetworkManager
[root@server.elsaiedadel.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search elsaiedadel.net
nameserver 127.0.0.1
[root@server.elsaiedadel.net ~]#
```

Рис. 7: Настройка NetworkManager

Разрешение запросов из сети

В файле named.conf разрешена обработка DNS-запросов от внутренней сети и включено прослушивание всех интерфейсов.

Open | named.conf /etc | Save

```
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         directory       "/var/named";
13         dump-file       "/var/named/data/cache_dump.db";
14         statistics-file "/var/named/data/named_stats.txt";
15         memstatistics-file "/var/named/data/named_mem_stats.txt";
16         secroots-file   "/var/named/data/named.secroots";
17         recursing-file  "/var/named/data/named.recursing";
18         allow-query     { localhost; 192.168.0.0/16; };
19
20         /*
```

Рис. 8: Изменение named.conf

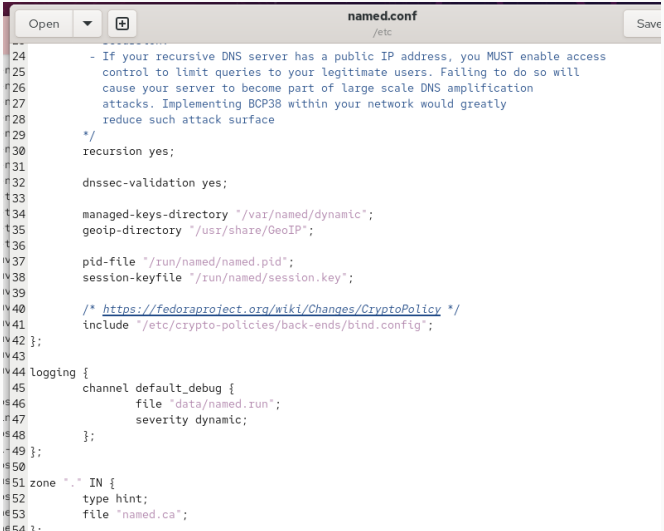
Проверка работы службы named

Проверено, что демон named прослушивает UDP-порт 53 и корректно обрабатывает DNS-запросы.

```
[root@server.elsaiedadel.net ~]#
[root@server.elsaiedadel.net ~]# firewall-cmd --add-service=dns
success
[root@server.elsaiedadel.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.elsaiedadel.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  1090                          avahi   12u     IPv4               8944       0t0        UDP *:mdns
avahi-dae  1090                          avahi   13u     IPv6               8945       0t0        UDP *:mdns
chronyd    1159                         chrony    5u     IPv4              10196       0t0        UDP localhost:323
chronyd    1159                         chrony    6u     IPv6              10197       0t0        UDP localhost:323
named     14085                          named   25u     IPv4              54250       0t0        UDP localhost:domain
named     14085                          named   26u     IPv4              54251       0t0        UDP localhost:domain
named     14085                          named   31u     IPv6              54254       0t0        UDP localhost:domain
named     14085                          named   32u     IPv6              54255       0t0        UDP localhost:domain
named     14085 14086 isc-net-0          named   25u     IPv4              54250       0t0        UDP localhost:domain
named     14085 14086 isc-net-0          named   26u     IPv4              54251       0t0        UDP localhost:domain
named     14085 14086 isc-net-0          named   31u     IPv6              54254       0t0        UDP localhost:domain
named     14085 14086 isc-net-0          named   32u     IPv6              54255       0t0        UDP localhost:domain
named     14085 14087 isc-net-0          named   25u     IPv4              54250       0t0        UDP localhost:domain
named     14085 14087 isc-net-0          named   26u     IPv4              54251       0t0        UDP localhost:domain
named     14085 14087 isc-net-0          named   31u     IPv6              54254       0t0        UDP localhost:domain
named     14085 14087 isc-net-0          named   32u     IPv6              54255       0t0        UDP localhost:domain
named     14085 14088 isc-net-0          named   25u     IPv4              54250       0t0        UDP localhost:domain
named     14085 14088 isc-net-0          named   26u     IPv4              54251       0t0        UDP localhost:domain
named     14085 14088 isc-net-0          named   31u     IPv6              54254       0t0        UDP localhost:domain
named     14085 14088 isc-net-0          named   32u     IPv6              54255       0t0        UDP localhost:domain
named     14085 14089 isc-net-0          named   25u     IPv4              54250       0t0        UDP localhost:domain
named     14085 14089 isc-net-0          named   26u     IPv4              54251       0t0        UDP localhost:domain
```

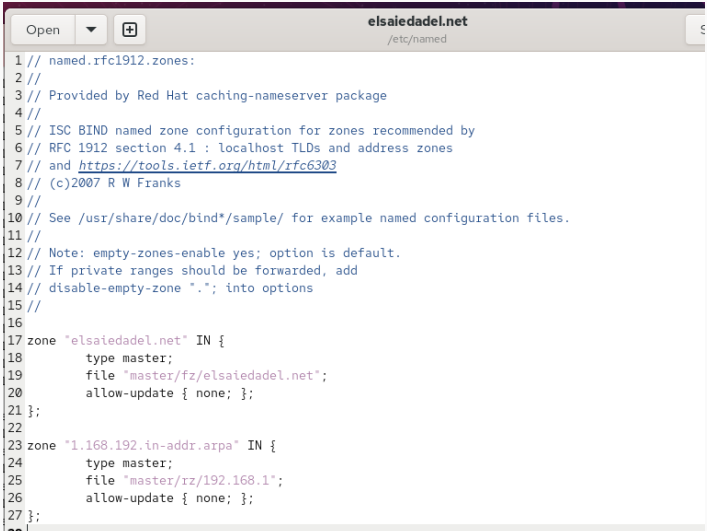
Описание DNS-зон

Создан файл описания зон elsaiedadel.net и подключён в основной конфигурации named.



Прямая и обратная зоны

Настроены: - прямая зона elsaiedadel.net; - обратная зона 1.168.192.in-addr.arpa.



Файл прямой зоны

В файле прямой зоны определены записи SOA, NS и A для домена elsaiedadel.net.

Open

elsaiedadel.net
/var/named/master/fz

```
$TTL 1D
@       IN SOA  @ server.elsaiedadel.net. (
                                        2026010200      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
$ORIGIN elsaiedadel.net.
servar  A       192.168.1.1
ns      A       192.168.1.1
```

Рис. 12: Прямая зона

Файл обратной зоны

В файле обратной зоны заданы PTR-записи для IP-адреса 192.168.1.1.

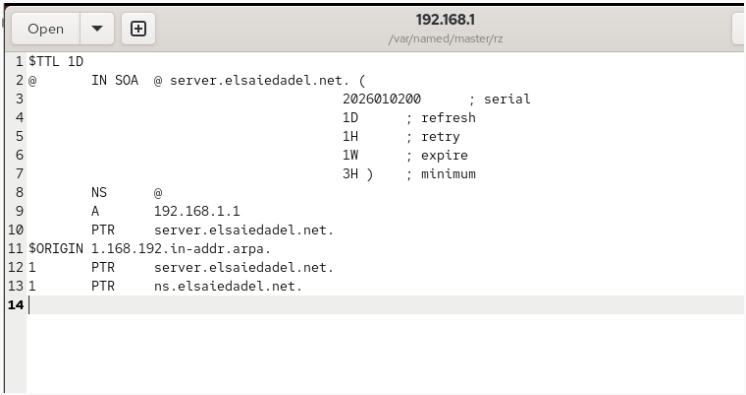


Рис. 13: Обратная зона

Выполнена настройка прав доступа и восстановление контекстов безопасности SELinux для корректной работы named.

```
[root@server.elsaledadel.net rz]# chown -R named:named /etc/named
[root@server.elsaledadel.net rz]# chown -R named:named /var/named
[root@server.elsaledadel.net rz]# restorecon -vR /etc
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.elsaledadel.net rz]# restorecon -vR /var/named/
[root@server.elsaledadel.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.elsaledadel.net rz]# systemctl restart named
[root@server.elsaledadel.net rz]#
```

Рис. 14: SELinux

Проверка dig

Выполнен запрос к ns.elsaiedadel.net.

Получен авторитативный ответ от локального DNS-сервера.

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

; <<>> DiG 9.18.33 <<>> ns.elsaiedadel.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3309
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: f8f4853fef2631330100000006957913eb071bc0354d335fe (good)
;; QUESTION SECTION:
;ns.elsaiedadel.net.            IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Fri Jan 02 09:34:54 UTC 2026
;; MSG SIZE  rcvd: 91

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

Проверка host

С помощью утилиты host проверены: - список записей зоны; - A-записи; - PTR-записи.

```
[root@server.elsaiedadel.net rz]#
[root@server.elsaiedadel.net rz]# host -l elsaiedadel.net
elsaiedadel.net name server elsaiedadel.net.
elsaiedadel.net has address 192.168.1.1
ns.elsaiedadel.net has address 192.168.1.1
servar.elsaiedadel.net has address 192.168.1.1
[root@server.elsaiedadel.net rz]# host -a elsaiedadel.net
Trying "elsaiedadel.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32390
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
elsaiedadel.net.        86400   IN      SOA     elsaiedadel.net. server.elsaiedadel.net. 2026010200 86400 3600 604800 108
00
elsaiedadel.net.        86400   IN      NS      elsaiedadel.net.
elsaiedadel.net.        86400   IN      A       192.168.1.1

Received 106 bytes from 127.0.0.1#53 in 1 ms
[root@server.elsaiedadel.net rz]# host -t A elsaiedadel.net
elsaiedadel.net has address 192.168.1.1
[root@server.elsaiedadel.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.elsaiedadel.net.
1.1.168.192.in-addr.arpa domain name pointer ns.elsaiedadel.net.
[root@server.elsaiedadel.net rz]#
```

Рис. 16: Проверка host

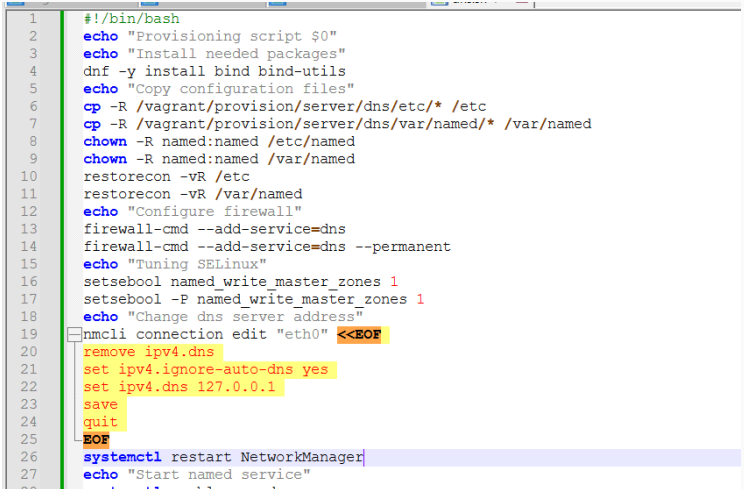
Создана структура каталогов для хранения DNS-конфигурации в /vagrant/provision/server/dns и скопированы необходимые файлы.

```
[root@server.elsaiedadel.net rz]#
[root@server.elsaiedadel.net rz]# cd /vagrant/
[root@server.elsaiedadel.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.elsaiedadel.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named /vagrant/provision/server/dns/etc/
named/              named.conf          named.rfc1912.zones  named.root.key
[root@server.elsaiedadel.net vagrant]# cp -R /etc/named/elsaiedadel.net /vagrant/provision/server/dns/etc/named/
[root@server.elsaiedadel.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.elsaiedadel.net vagrant]# cd provision/server/
[root@server.elsaiedadel.net server]# touch dns.sh
[root@server.elsaiedadel.net server]# chmod +x dns.sh
[root@server.elsaiedadel.net server]#
```

Рис. 17: Подготовка каталогов

Скрипт dns.sh

Создан provisioning-скрипт dns.sh, автоматизирующий установку, настройку и запуск DNS-сервера при старте виртуальной машины.



```
#!/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"
```

Выводы

Вывод

В ходе лабораторной работы был установлен и настроен DNS-сервер на базе BIND. Реализована работа кэширующего и первичного DNS-сервера, настроены прямая и обратная зоны, проверена корректность разрешения имён и автоматизирован процесс развёртывания. Полученные результаты подтверждают корректную работу DNS-сервера и его готовность к использованию во внутренней виртуальной сети.