

# **Отчёт по лабораторной работе 2**

## **Настройка DNS-сервера**

Заур Мустафаев

# **Содержание**

<b>1 Цель работы</b>	<b>5</b>
<b>2 Выполнение работы</b>	<b>6</b>
2.1 Установка DNS-сервера . . . . .	6
2.2 Настройка кэширующего DNS-сервера . . . . .	7
2.3 Настройка первичного DNS-сервера . . . . .	10
2.4 Проверка работы DNS-сервера . . . . .	12
2.5 Автоматизация с помощью Vagrant . . . . .	14
<b>3 Вывод</b>	<b>15</b>
<b>4 Контрольные вопросы</b>	<b>16</b>
<b>5 Список литературы</b>	<b>19</b>

# Список иллюстраций

2.1 Установка bind и bind-utils . . . . .	6
2.2 Запрос dig к www.yandex.ru . . . . .	7
2.3 Сравнение dig-запросов . . . . .	8
2.4 Настройка подключения через nmcli . . . . .	8
2.5 Изменения в named.conf . . . . .	9
2.6 Проверка работы DNS через lsof . . . . .	9
2.7 Подключение файла зоны zmustafaev.net . . . . .	10
2.8 Файл прямой зоны zmustafaev.net . . . . .	10
2.9 Файл обратной зоны 192.168.1 . . . . .	11
2.10 Настройка прав и SELinux . . . . .	11
2.11 Файл конфигурации зон . . . . .	12
2.12 Файл конфигурации прямой зоны zmustafaev.net . . . . .	12
2.13 Проверка зоны через dig . . . . .	13
2.14 Проверка зоны через host . . . . .	13

# **Список таблиц**

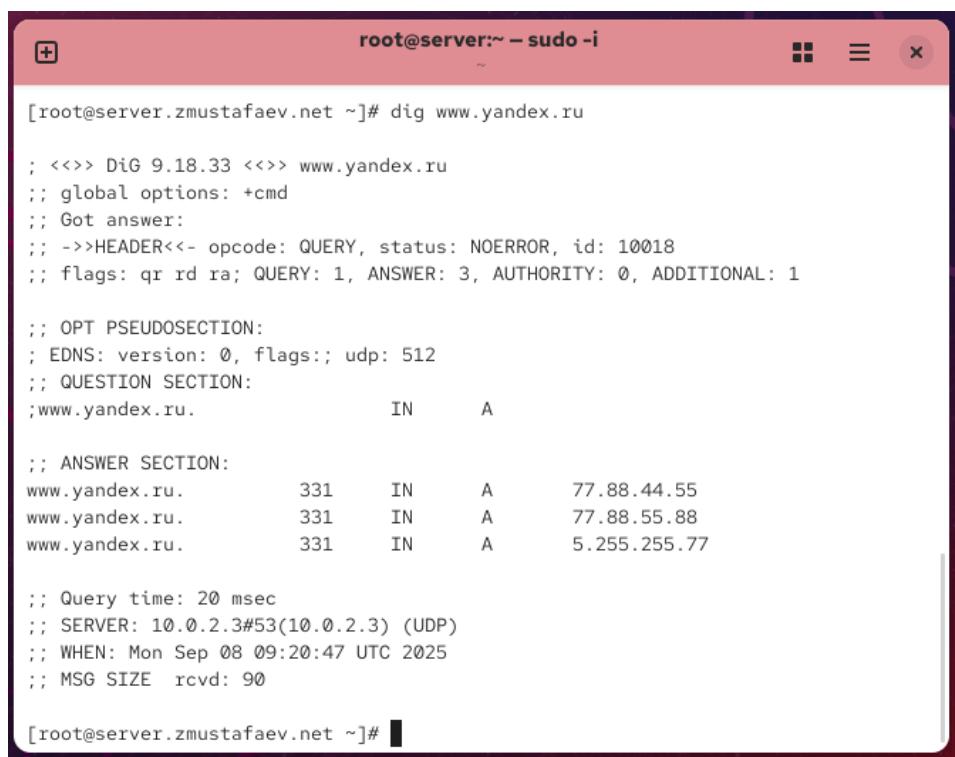
# **1 Цель работы**

Получить практические навыки установки и настройки DNS-сервера, а также закрепить понимание принципов работы системы доменных имён.

## 2 Выполнение работы

### 2.1 Установка DNS-сервера

1. Запущена виртуальная машина **server**, подготовлено окружение для установки служб.
2. Установлены пакеты **bind** и **bind-utils**, необходимые для работы сервера имён и диагностики.



The screenshot shows a terminal window with a red header bar containing the text "root@server:~ - sudo -i". The main area of the terminal displays the output of the "dig" command:

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

; <>> DiG 9.18.33 <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10018
;; 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.        331     IN      A      77.88.44.55
www.yandex.ru.        331     IN      A      77.88.55.88
www.yandex.ru.        331     IN      A      5.255.255.77

;; Query time: 20 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Mon Sep 08 09:20:47 UTC 2025
;; MSG SIZE rcvd: 90

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

Рис. 2.1: Установка bind и bind-utils

3. Проверена работоспособность сервиса с помощью утилиты **dig**, сделан запрос к ресурсу в сети Интернет.

```
; <>> 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: 9829
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 60058798dc672a250100000068bea0578f8c1747001fb9c2 (good)
;; QUESTION SECTION:
;www.yandex.ru.           IN      A

;; ANSWER SECTION:
www.YANDEX.ru.        579     IN      A      5.255.255.77
www.YANDEX.ru.        579     IN      A      77.88.44.55
www.YANDEX.ru.        579     IN      A      77.88.55.88

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Sep 08 09:22:31 UTC 2025
;; MSG SIZE  rcvd: 131

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

Рис. 2.2: Запрос dig к www.yandex.ru

## 2.2 Настройка кэширующего DNS-сервера

1. Изучен файл `/etc/resolv.conf`, где задаются адреса серверов DNS по умолчанию.
2. Рассмотрены файлы `named.localhost` и `named.loopback`, отвечающие за тестовые зоны.
3. Сервис **named** был запущен и добавлен в автозагрузку.
4. Сравнены результаты запросов через внешний сервер и через локальный. Установлено, что сервер корректно выполняет резолвинг.

```
[root@server.zmustafaev.net ~]# nmcli connection edit eth0
==| nmcli interactive connection editor |==

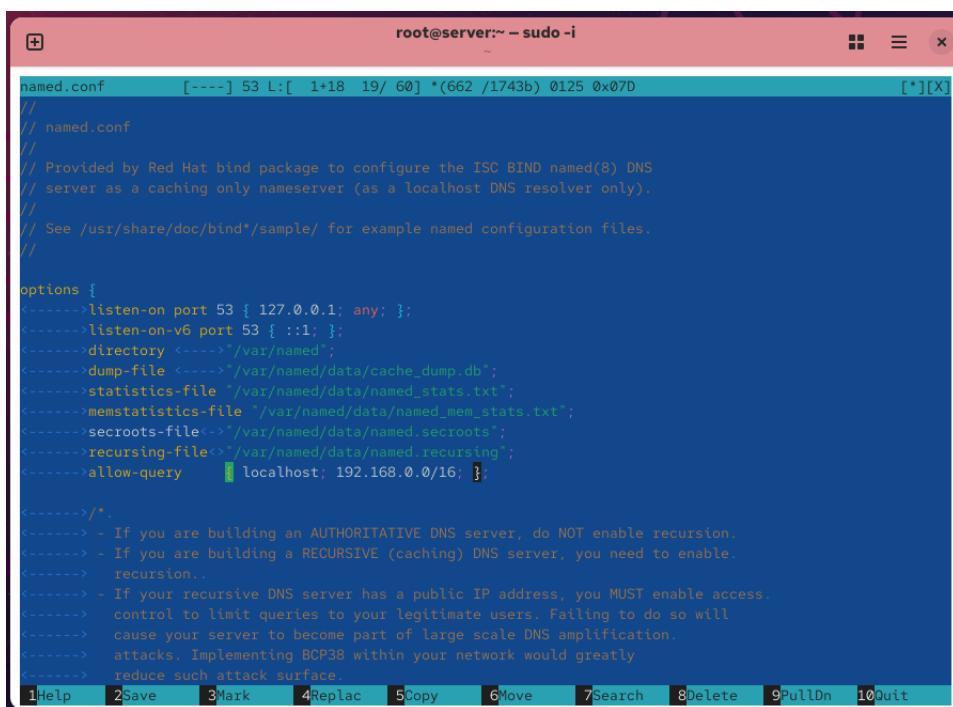
Editing existing '802-3-ethernet' connection: 'eth0'

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, et
h, ipv4, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e292e83a-7750-4087-b4e1-a998fc55c0ea) successfully updated.
nmcli> quit
[root@server.zmustafaev.net ~]#
```

Рис. 2.3: Сравнение dig-запросов

5. Настройки сетевого соединения были изменены с помощью **nmcli**, что позволило использовать локальный сервер как основной DNS.



```
root@server:~ - sudo -i
[named.conf      [---] 53 L:[ 1+18 19/ 60] *(662 /1743b) 0125 0x07D
// 
// 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; 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.recurising";
    allow-query { localhost; 192.168.0.0/16; };

}

/*
 - 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.

```

Рис. 2.4: Настройка подключения через nmcli

6. Внесены изменения в файл **named.conf**: расширен список допустимых клиентов, добавлена поддержка сети 192.168.0.0/16.

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	887	avahi	12u	IPv4	8033	0t0
avahi-dae	887	avahi	13u	IPv6	8034	0t0
chrony	964	chrony	5u	IPv4	8146	0t0
st:323						UDP *:mdns
chrony	964	chrony	6u	IPv6	8147	0t0
st:323						UDP localho
named	26885	named	25u	IPv4	62978	0t0
st:domain						UDP localho
named	26885	named	26u	IPv4	62979	0t0
st:domain						UDP localho
named	26885	named	31u	IPv6	62982	0t0
st:domain						UDP localho
named	26885	named	32u	IPv6	62983	0t0
st:domain						UDP localho
named	26885 26886 isc-net-0	named	25u	IPv4	62978	0t0
st:domain						UDP localho
named	26885 26886 isc-net-0	named	26u	IPv4	62979	0t0
st:domain						UDP localho
named	26885 26886 isc-net-0	named	31u	IPv6	62982	0t0
st:domain						UDP localho
named	26885 26886 isc-net-0	named	32u	IPv6	62983	0t0
st:domain						UDP localho
named	26885 26887 isc-net-0	named	25u	IPv4	62978	0t0
st:domain						UDP localho
named	26885 26887 isc-net-0	named	26u	IPv4	62979	0t0
st:domain						UDP localho
named	26885 26887 isc-net-0	named	31u	IPv6	62982	0t0
st:domain						UDP localho

Рис. 2.5: Изменения в named.conf

## 7. Добавлены правила для файрвола, разрешающие обращения к DNS.

```

root@server:/etc/named - sudo -i
[...]
named.conf      [---] 36 L:[ 32+27 59/ 60 ] *(1778/1779b) 0010 0x00A
[*][X]

<----->dnssec-validation yes;

<----->managed-keys-directory "/var/named/dynamic";
<----->geolite-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;
    };
};

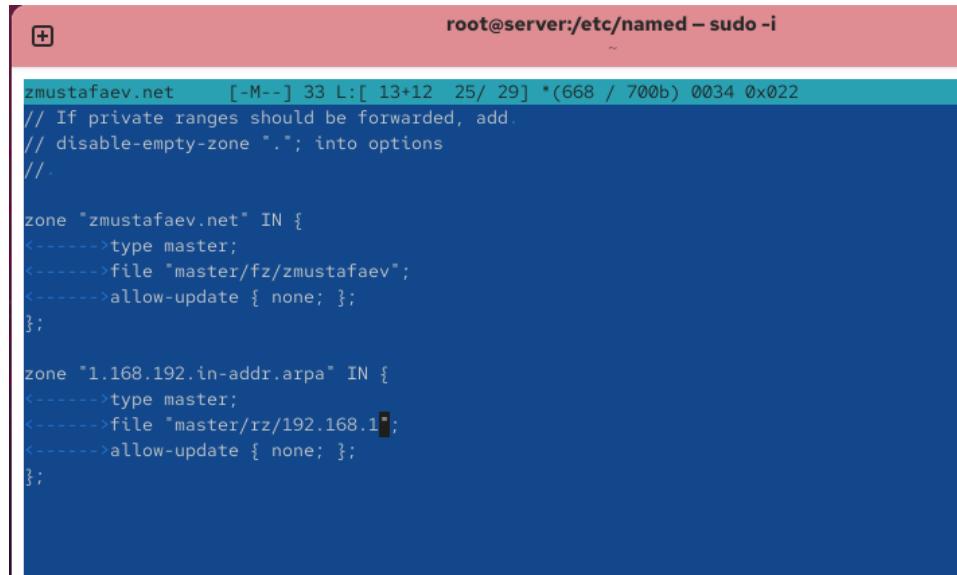
zone "." IN {
<----->type hint;
<----->file "named.ca";
};

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

Рис. 2.6: Проверка работы DNS через lsof

## 2.3 Настройка первичного DNS-сервера

- Создан файл зоны `zmustafaev.net`, где прописаны прямые и обратные записи.



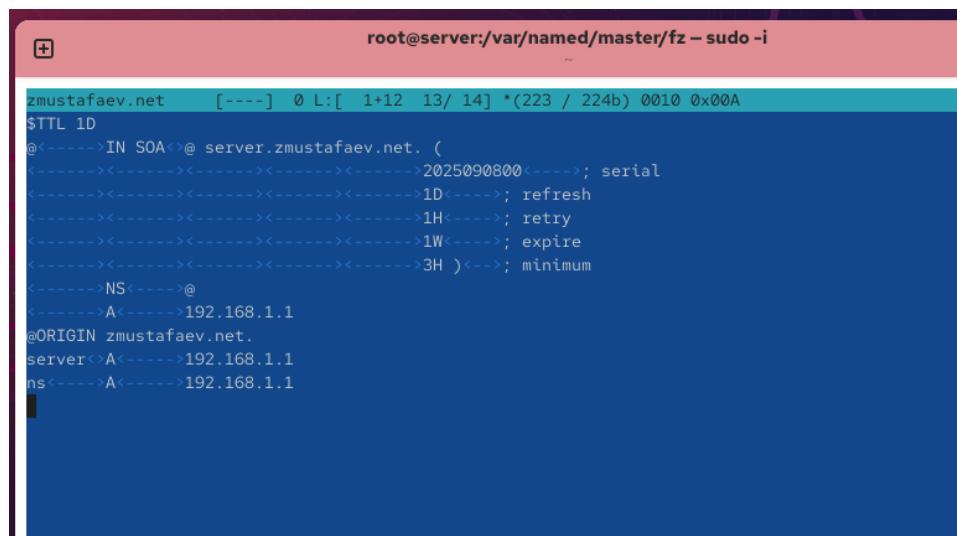
```
root@server:/etc/named - sudo -i
zmustafaev.net      [-M--] 33 L:[ 13+12 25/ 29] *(668 / 700b) 0034 0x022
// If private ranges should be forwarded, add.
// disable-empty-zone "."; into options
//.

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

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

Рис. 2.7: Подключение файла зоны `zmustafaev.net`

- Настроен файл прямой зоны с A- и NS-записями.



```
root@server:/var/named/master/fz - sudo -i
zmustafaev.net      [---]  0 L:[ 1+12 13/ 14] *(223 / 224b) 0010 0x00A
$TTL 1D
@<---->IN SOA <@> server.zmustafaev.net. (
<-----><-----><-----><-----><-----> 2025090800 <----->; serial
<-----><-----><-----><-----><-----> 1D <----->; refresh
<-----><-----><-----><-----><-----> 1H <----->; retry
<-----><-----><-----><-----><-----> 1W <----->; expire
<-----><-----><-----><-----><-----> 3H ) <--->; minimum
<----->NS <----> @
<----->A <-----> 192.168.1.1
@ORIGIN zmustafaev.net.
server <A> 192.168.1.1
ns <----->A <-----> 192.168.1.1
```

Рис. 2.8: Файл прямой зоны `zmustafaev.net`

- В обратной зоне добавлены PTR-записи для IP-адресов.

```
root@server:/var/named/master/rz - sudo -i
192.168.1      [-M--]  0 L:[ 1+13 14/ 15] *(275 / 276b) 0010 0x00A
$TTL 1D
@<---->IN SOA<>@ server.zmustafaev.net. (
<-----><----><----><----><----> 2025090800<---->; serial
<-----><----><----><----><---->1D<---->; refresh
<-----><----><----><----><---->1H<---->; retry
<-----><----><----><----><---->1W<---->; expire
<-----><----><----><----><---->3H )<---->; minimum
<----->NS<---->@
<----->A<---->192.168.1.1
<----->PTR<--->server.zmustafaev.net.
$ORIGIN 1.168.192.in-addr.arpa.
1<---->PTR<--->server.zmustafaev.net.
1<---->PTR<--->ns.zmustafaev.net.
```

Рис. 2.9: Файл обратной зоны 192.168.1

4. Сервис **named** был перезапущен для применения настроек, также исправлены ошибки.

```
[root@server.zmustafaev.net rz]#
[root@server.zmustafaev.net rz]# chown -R named:named /etc/named
[root@server.zmustafaev.net rz]# chown -R named:named /var/named
[root@server.zmustafaev.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_e
tc_t:s0
Relabeled /etc/lvm/devices/backup/system.devices-20250908.091354.0005 from system_u:object_r:lvm_metadata_t:s
0 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 t
o unconfined_u:object_r:NetworkManager_etc_rw_t:s0
[root@server.zmustafaev.net rz]# restorecon -vR /var/named/
[root@server.zmustafaev.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.zmustafaev.net rz]#
```

Рис. 2.10: Настройка прав и SELinux

```
zmustafaev.net      [-M--] 38 L:[ 4+15 19/ 29] *(565 / 704b) 0034 0x022
// 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 "zmustafaev.net" IN {
<----->type master;
<----->file "master/fz/zmustafaev.net";
<----->allow-update { none; };
};

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

1Help 2Save 3Mark 4Replace 5Copy 6Move 7Search 8Delete 9PullDn 10Quit
```

Рис. 2.11: Файл конфигурации зон

```
zmustafaev.net      [---] 1 L:[ 1+ 9 10/ 14] *(162 / 224b) 0079 0x04F
$TTL 1D
@<---->IN SOA<>@ server.zmustafaev.net. (
<----><----><----><----><---->2025090800<---->; serial
<----><----><----><----><---->10<---->; refresh
<----><----><----><----><---->1H<---->; retry
<----><----><----><----><---->1W<---->; expire
<----><----><----><----><---->3H )<-->; minimum
<---->NS<---->@
<---->A<---->192.168.1.1
$ORIGIN zmustafaev.net.
server<>A<---->192.168.1.1
ns<---->A<---->192.168.1.1
```

Рис. 2.12: Файл конфигурации прямой зоны zmustafaev.net

## 2.4 Проверка работы DNS-сервера

1. С помощью утилиты **dig** произведена проверка: запрос к ns.zmustafaev.net вернул корректный IP.

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

; <>> DiG 9.18.33 <>> ns.zmustafaev.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4043
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 04308167320029a00100000068beac5269320040a95f6434 (good)
;; QUESTION SECTION:
;ns.zmustafaev.net.           IN      A

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

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Mon Sep 08 10:13:38 UTC 2025
;; MSG SIZE  rcvd: 90

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

---

Рис. 2.13: Проверка зоны через dig

## 2. Утилита host подтвердила корректность прямых и обратных записей.

```
[root@server.zmustafaev.net rz]# host -l zmustafaev.net
zmustafaev.net name server zmustafaev.net.
zmustafaev.net has address 192.168.1.1
ns.zmustafaev.net has address 192.168.1.1
server.zmustafaev.net has address 192.168.1.1
[root@server.zmustafaev.net rz]# host -a zmustafaev.net
Trying "zmustafaev.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35593
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
zmustafaev.net.    86400   IN      SOA     zmustafaev.net. server.zmustafaev.net. 2025090800 86400 3600
604800 10800
zmustafaev.net.    86400   IN      NS      zmustafaev.net.
zmustafaev.net.    86400   IN      A       192.168.1.1

Received 105 bytes from 127.0.0.1#53 in 0 ms
[root@server.zmustafaev.net rz]# host -t A zmustafaev.net
zmustafaev.net has address 192.168.1.1
[root@server.zmustafaev.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.zmustafaev.net.
1.1.168.192.in-addr.arpa domain name pointer server.zmustafaev.net.
[root@server.zmustafaev.net rz]#
```

---

Рис. 2.14: Проверка зоны через host

## 2.5 Автоматизация с помощью Vagrant

Создан скрипт `dns.sh`, выполняющий установку пакетов, копирование конфигураций, настройку прав и SELinux, а также запуск службы **named**.

В файл `Vagrantfile` добавлен вызов скрипта, что обеспечивает автоматическое развертывание настроенного DNS-сервера.

## **3 Вывод**

В ходе работы был развернут и сконфигурирован DNS-сервер на основе BIND. Реализованы прямая и обратная зоны, проведена проверка их работы. Настроен кэширующий режим. Добавлен скрипт автоматизации для Vagrant, что упростило повторное развёртывание и снизило вероятность ошибок при настройке вручную.

# 4 Контрольные вопросы

## 1. Что такое DNS?

Это система, которая преобразует доменные имена в IP-адреса и обратно.

## 2. Назначение кэширующего DNS-сервера?

Он ускоряет обработку повторных запросов, сохраняя результаты в кэше.

## 3. Разница между прямой и обратной зоной?

Прямая зона связывает имя с адресом, обратная – адрес с именем.

## 4. Где хранятся настройки DNS-сервера?

Основные файлы: /etc/named.conf (главная конфигурация), /etc/named/ (доп. зоны), /var/named/ (файлы зон).

## 5. Что содержится в resolv.conf?

Адреса серверов DNS и параметры поиска доменов.

## 6. Основные типы ресурсных записей DNS?

SOA, NS, A, AAAA, PTR, CNAME, MX, TXT.

## 7. Зачем нужен домен in-addr.arpa?

Для организации обратного разрешения адресов.

## 8. Функция демона named?

Это процесс, реализующий работу DNS-сервера BIND.

## 9. Разница между master и slave-серверами?

Master хранит оригинальные зоны, slave синхронизируется с ним.

**10. Какие параметры отвечают за обновление зоны?**

Serial, refresh, retry, expire, minimum.

**11. Как ограничить доступ к зоне?**

С помощью ACL, allow-query, аутентификации TSIG.

**12. Какая запись нужна для почтовых серверов?**

Используется MX-запись.

**13. Как протестировать работу DNS?**

С помощью dig, host, nslookup, а также через логи.

**14. Как управлять службами?**

Через systemctl: start, stop, restart.

**15. Как получить отладочную информацию о сервисе?**

Через journalctl -xe или настройку режима debug.

**16. Где хранится отладка работы системы?**

В журналах /var/log и через journalctl.

**17. Как узнать, какие файлы использует процесс?**

Через lsof или /proc/PID/fd.

**18. Примеры команд nmcli:**

show, edit, up, down.

**19. Что такое SELinux?**

Это механизм принудительного контроля доступа в Linux.

**20. Что такое контекст SELinux?**

Метка безопасности объекта, определяющая его права.

**21. Как восстановить контекст SELinux?**

restorecon -vR .

**22. Как создать правила SELinux из логов?**

Использовать audit2allow.

**23. Что такое булевый параметр SELinux?**

Переключатель, меняющий часть политики.

**24. Как посмотреть список булевых параметров?**

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 1912. – DOI: 10.17487/rfc1912.
2. Security-Enhanced Linux: руководство пользователя. – URL: [https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced\\_Linux/index.html](https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html)
3. Systemd. – URL: <https://wiki.archlinux.org/index.php/Systemd>
4. Костромин В. А. Утилита lsof. – URL: <http://rus-linux.net/kos.php?name=/papers/lsof/lsof.html>
5. Поттеринг Л. Systemd для администраторов. – URL: <http://wiki.opennet.ru/Systemd>
6. NetworkManager project. – URL: <https://wiki.gnome.org/Projects/NetworkManager>
7. nmcli project. – URL: <https://developer.gnome.org/NetworkManager/stable/nmcli.html>