Лабораторная работа №2

Дисциплина: Администрирование сетевых подсистем

Жибицкая Евгения Дмитриевна

Содержание

# 1 Цель работы

Приобретение навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён на ОС Rocky linux.

# 2 Выполнение лабораторной работы

Для начала загружаем операционную систему, перейдся в каталог Vagrant(рис. 1).

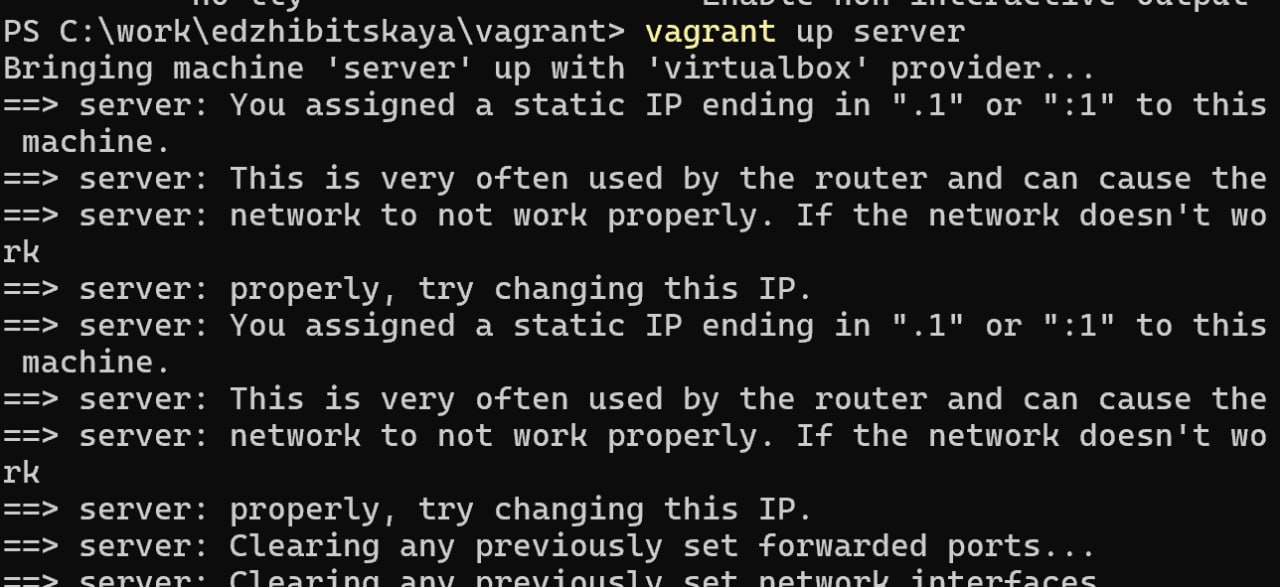


Рис. 1: Загрузка ОС

Открываем терминал, переходим в режим суперпользователя и устанавливаем bind, bind-utils(рис. 2).

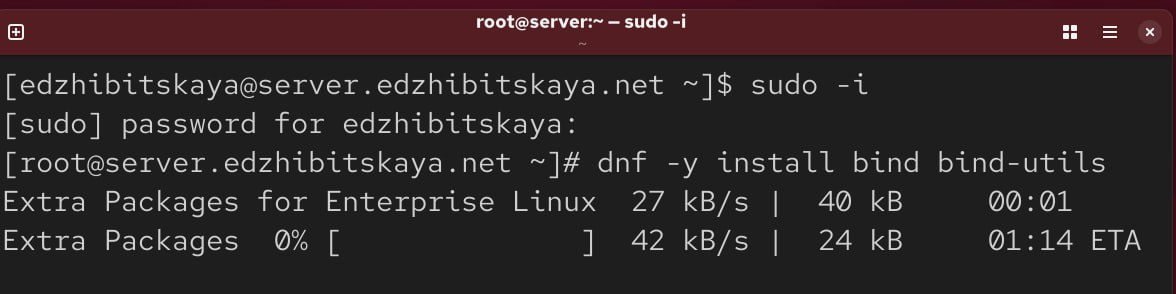


Рис. 2: bind, bind-utils

Затем в качетсве тренировки делаем запрос к DNS-адресу Яндекса(рис. 3).

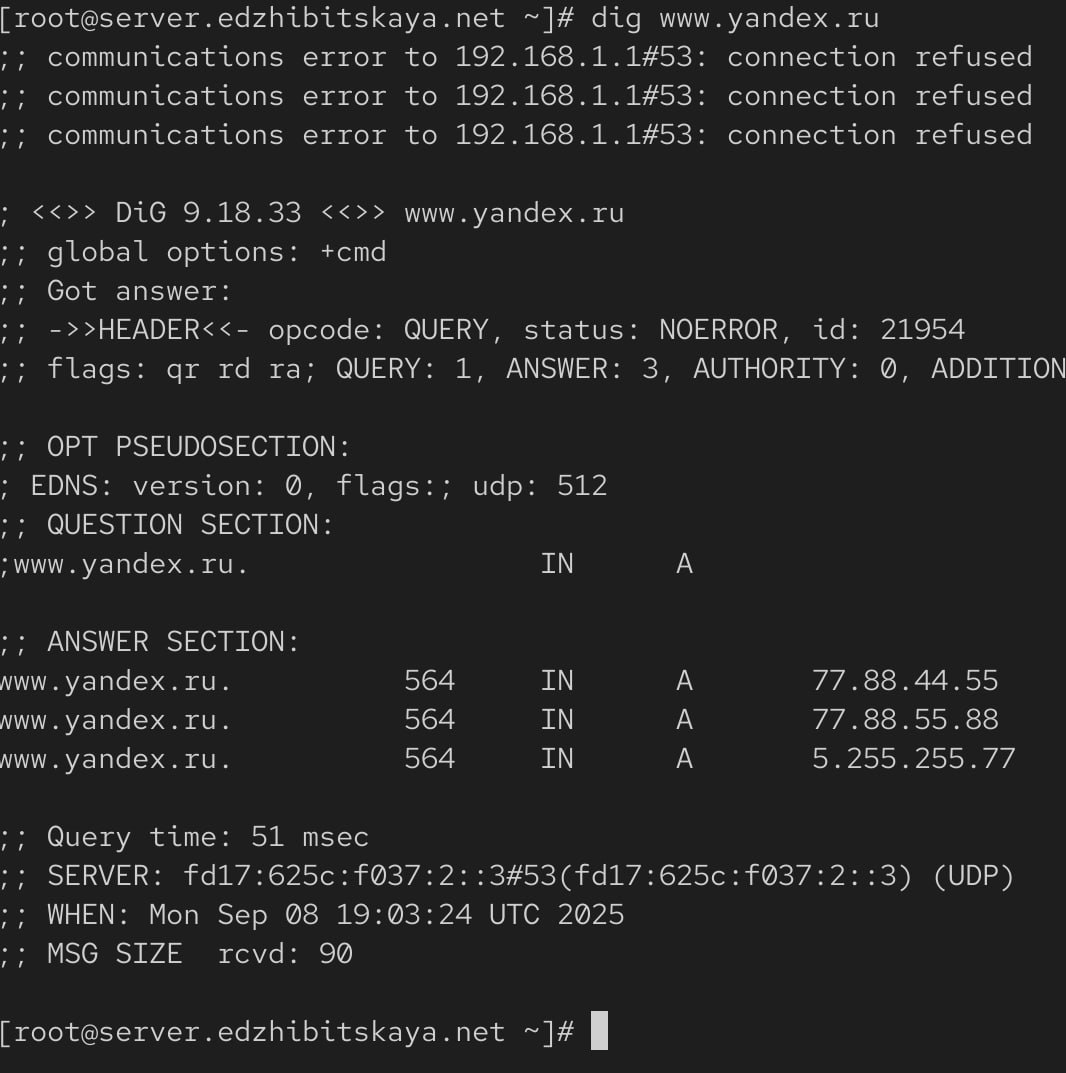


Рис. 3: Запрос к DNS-адресу Яндекса

Затем просмотрим содержимое файлов /etc/resolv.conf, /etc/named.conf, /var/named/named.ca, /var/named/named.localhost, /var/named/named.loopback.

В файле /etc/resolv.conf указано к каким DNS-серверам обращаться для преобразования доменных имен в IP-адреса и наоборот(рис. 4).



Рис. 4: Файл /etc/resolv.conf

/etc/named.conf главный конфигурационный файл демона BIND (named). Он определяет общие параметры работы DNS-сервера, зоны, которые он обслуживает, и политики доступа(рис. 5).

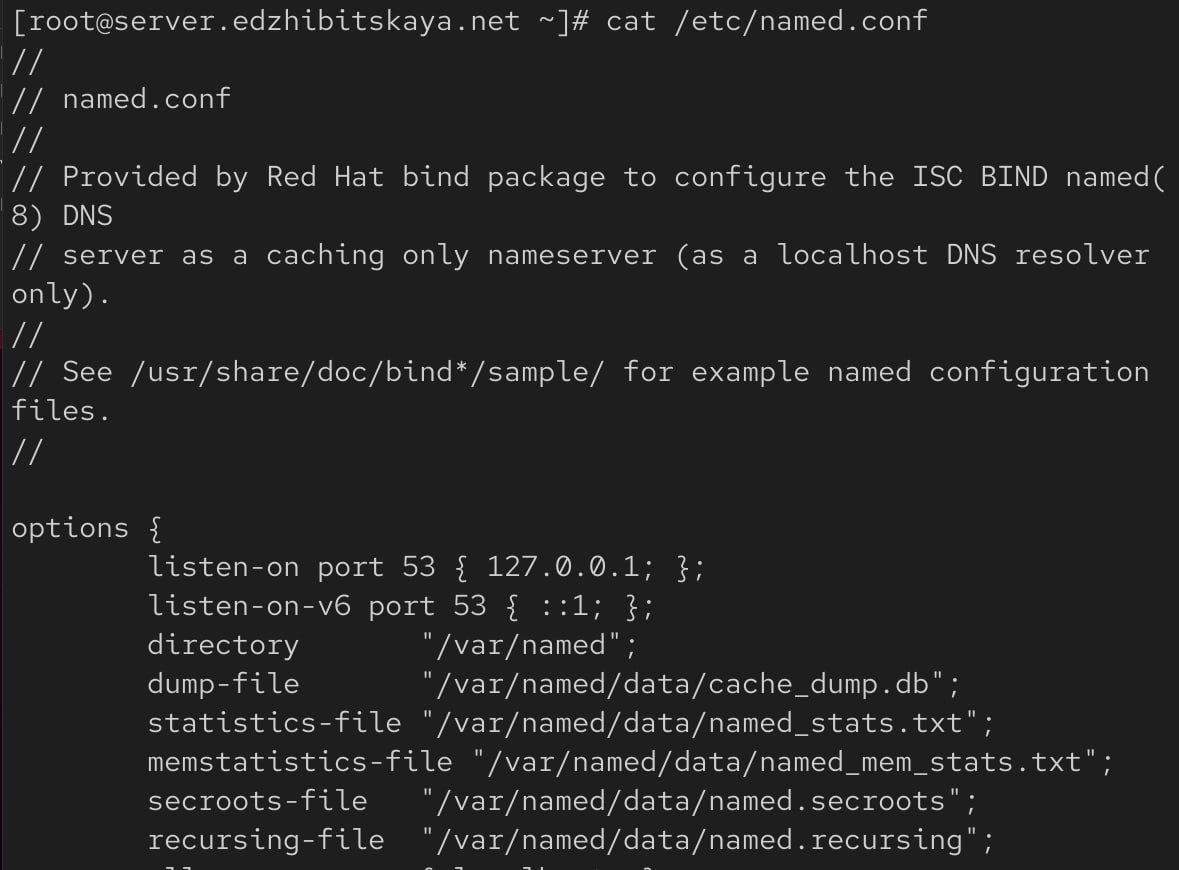


Рис. 5: Файл /etc/named.conf

/var/named/named.ca содержит список IP-адресов корневых DNS-серверов (root hints). Когда DNS-сервер не знает, куда направить запрос для какого-либо домена, он начинает поиск с этих корневых серверов

/var/named/named.localhost - это файл прямой зоны для домена localhost. Он сопоставляет имя localhost с IP-адресом 127.0.0.1

/var/named/named.loopback - это файл обратной зоны (reverse zone) для сетей IPv4 и IPv6. Он выполняет обратное преобразование: по IP-адресу 127.0.0.1 находит имя localhost(рис. 6).

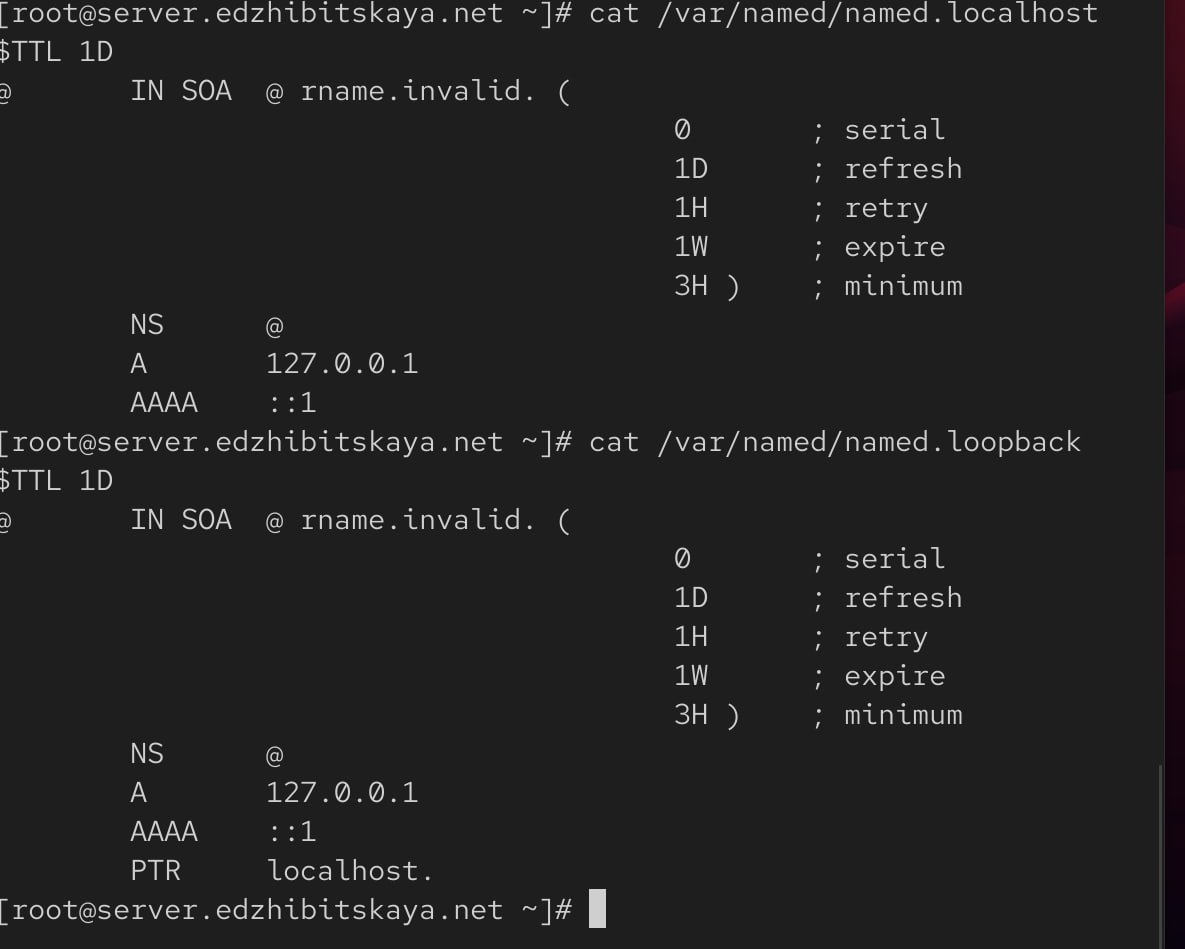


Рис. 6: Файлы named.localhost и named.loopback

Затем запустим DNS-сервер, включим его автозапуск(рис. 7).

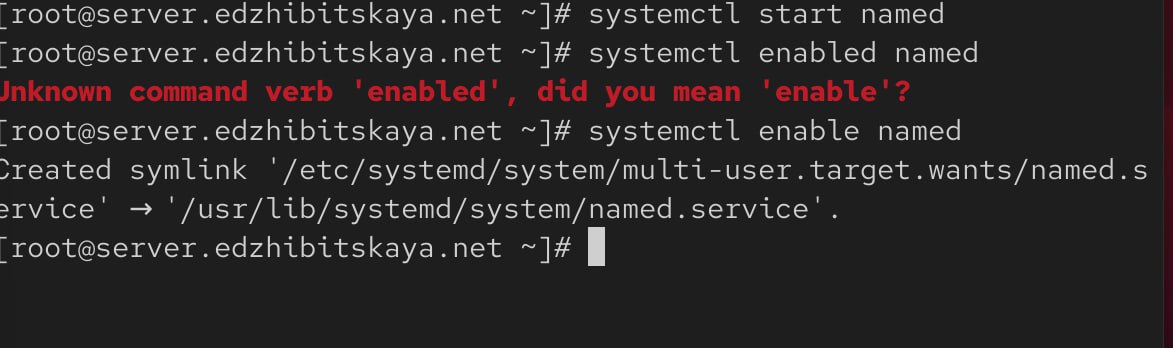


Рис. 7: Запуск сервера

Проанализируем вывод команд dig www.yandex.ru и dig [**127.0.0.1?**] www.yandex.ru(рис. 8). Вторая команда дает больший вывод, так как в ней мы еще указываем к какому серверу обращаться, она помогает в отладкеи диагностике конфигурации

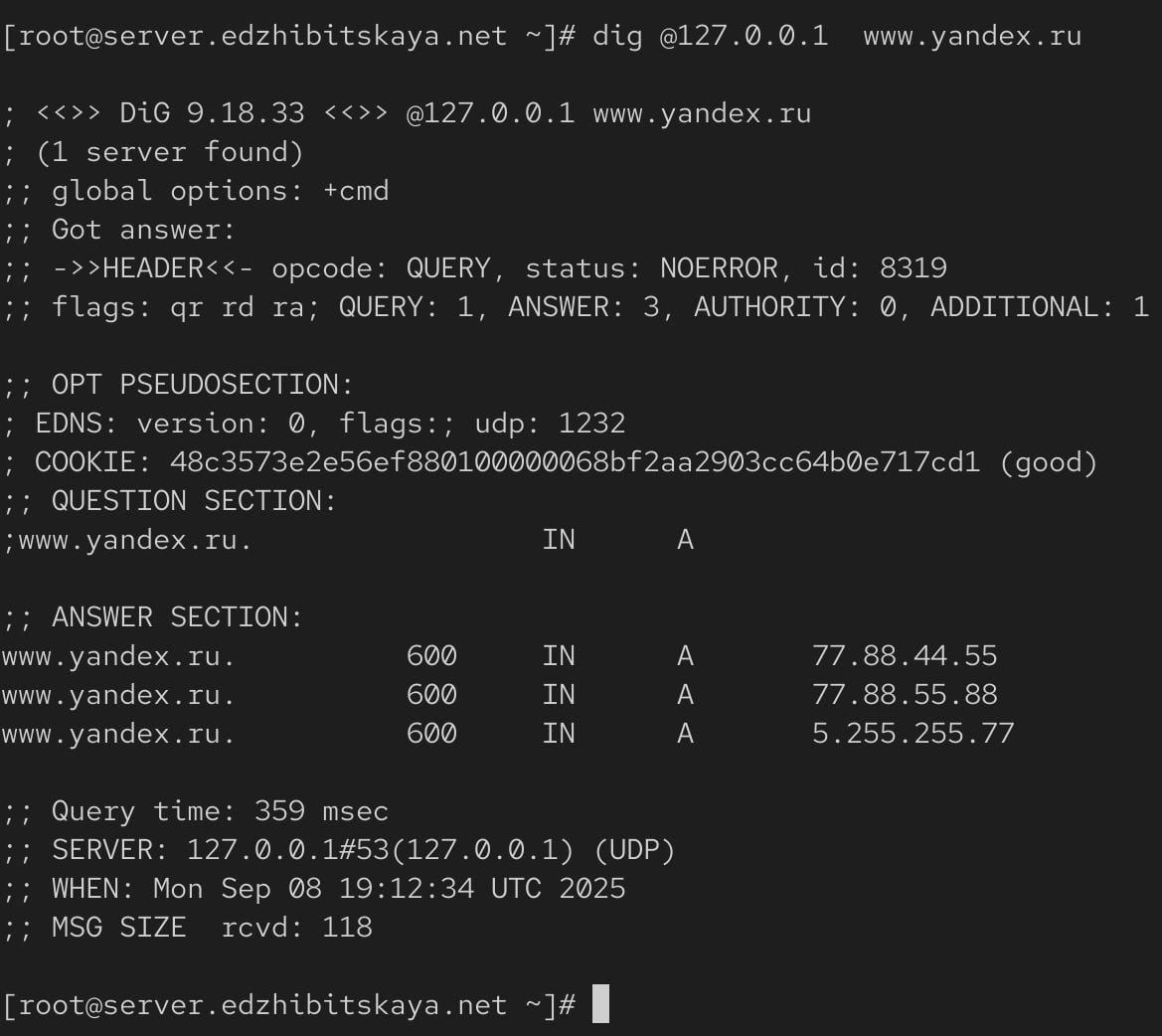


Рис. 8: Dig www.yandex.ru

Далее сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети, изменим настройки сетевого соединения eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0. Перезапускаем менеджер, проверяем наличие изменений (рис. 9).

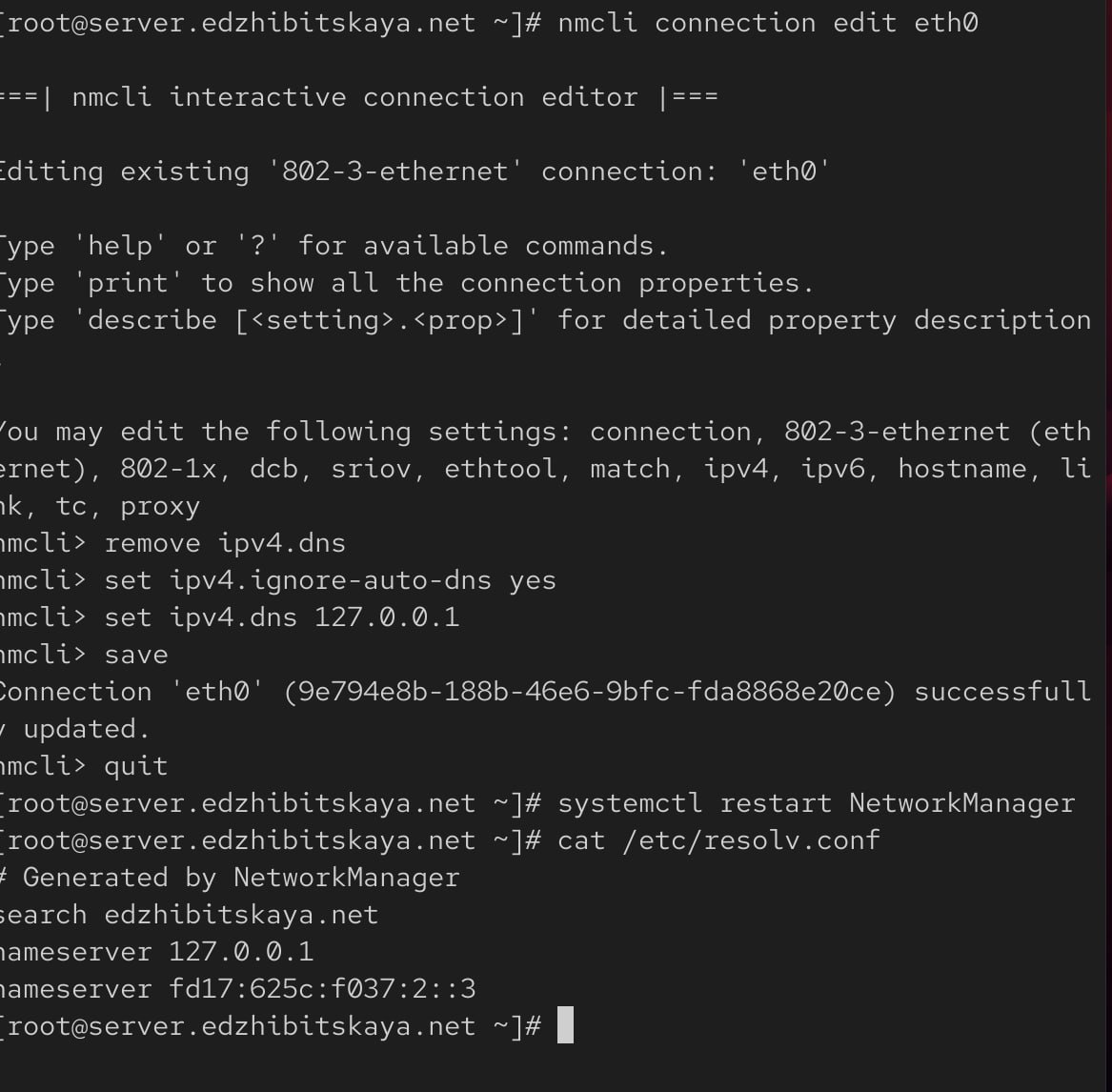


Рис. 9: Настройка соединения

Также настраиваем направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого редактируем файл /etc/named.conf(рис. 10).

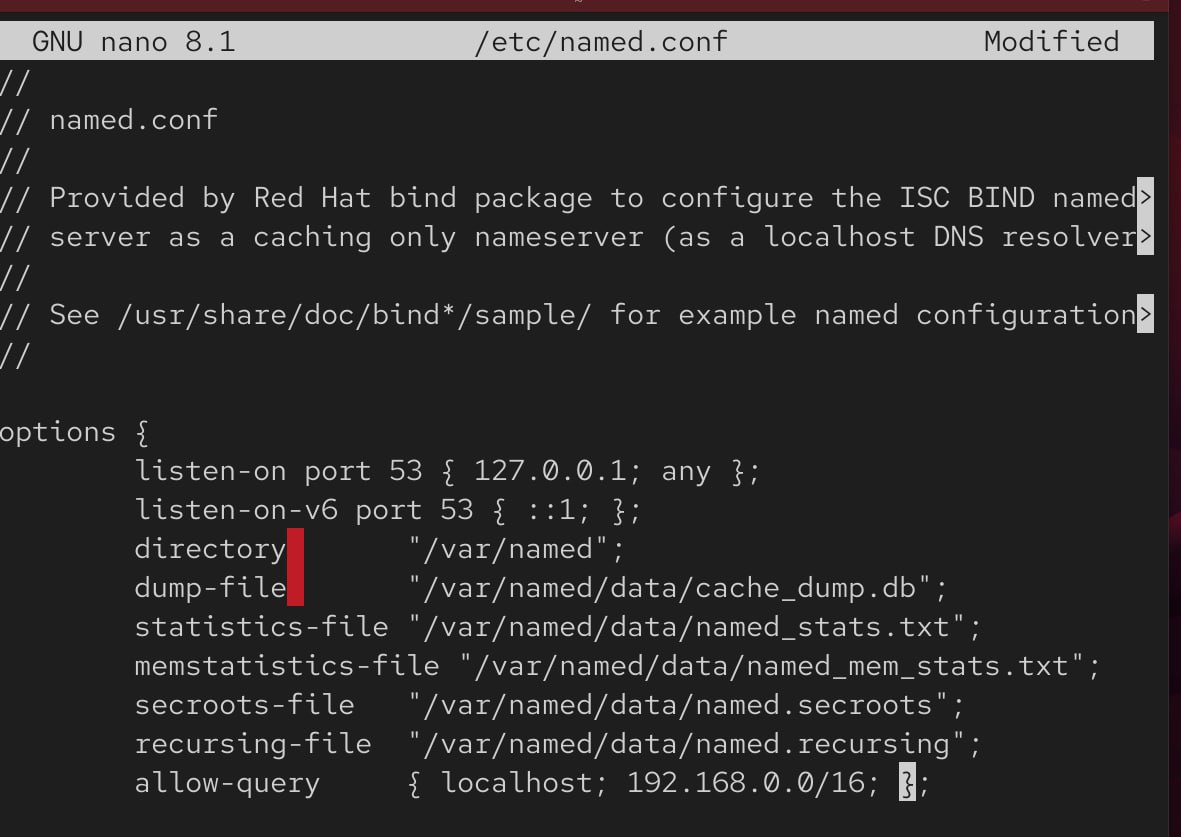


Рис. 10: Настройка направления запросов

Вносим изменения в настройки межсетевого экрана узла server, убеждаемся, что DNS-запросы идут через узел server(рис. 11).

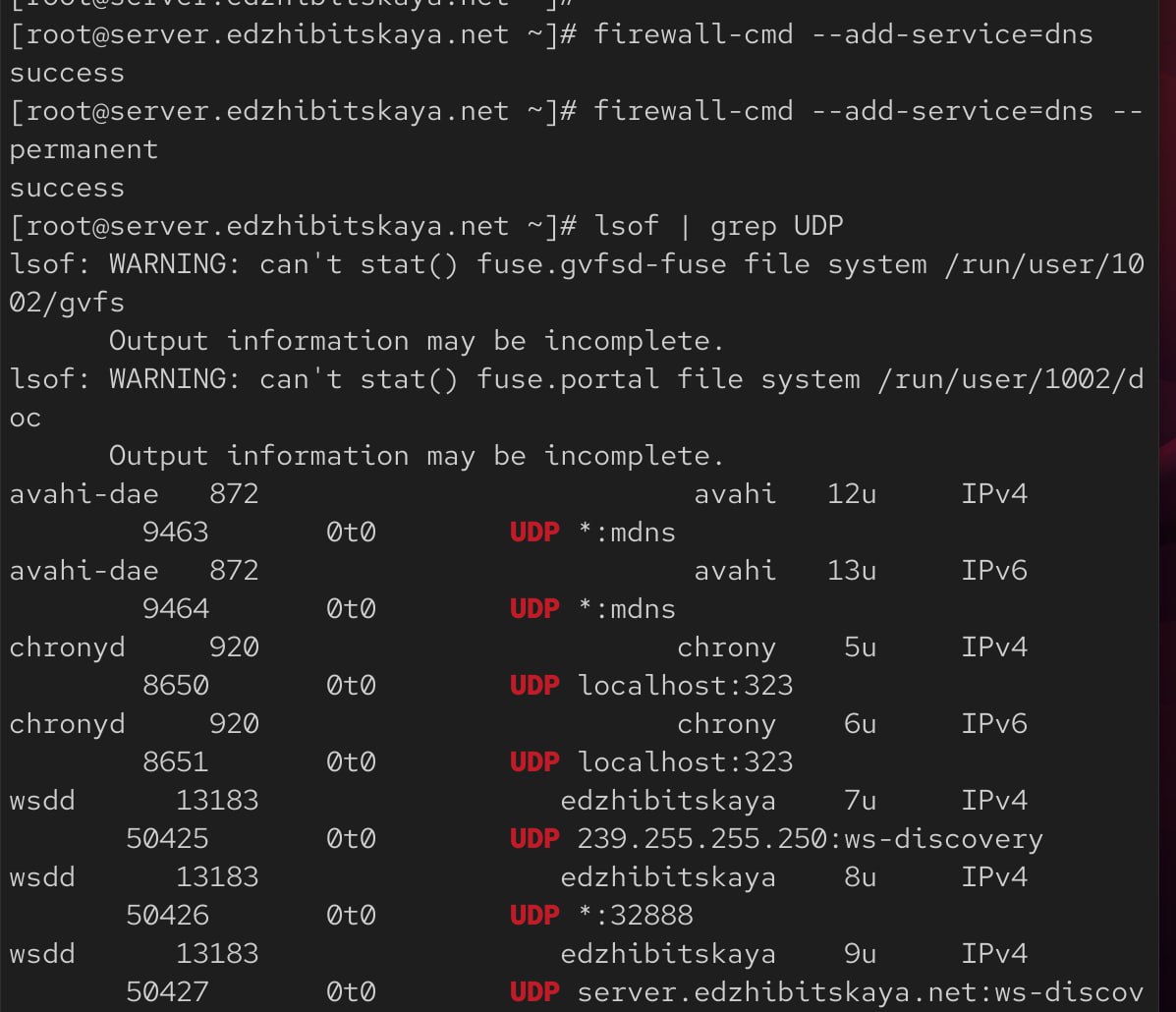


Рис. 11: Firewall

В ситуации, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер. Для этого в конфигурационный файл named.conf в секцию options добавим данные, предварительно посмотрев их на локальном хосте (рис. 12).

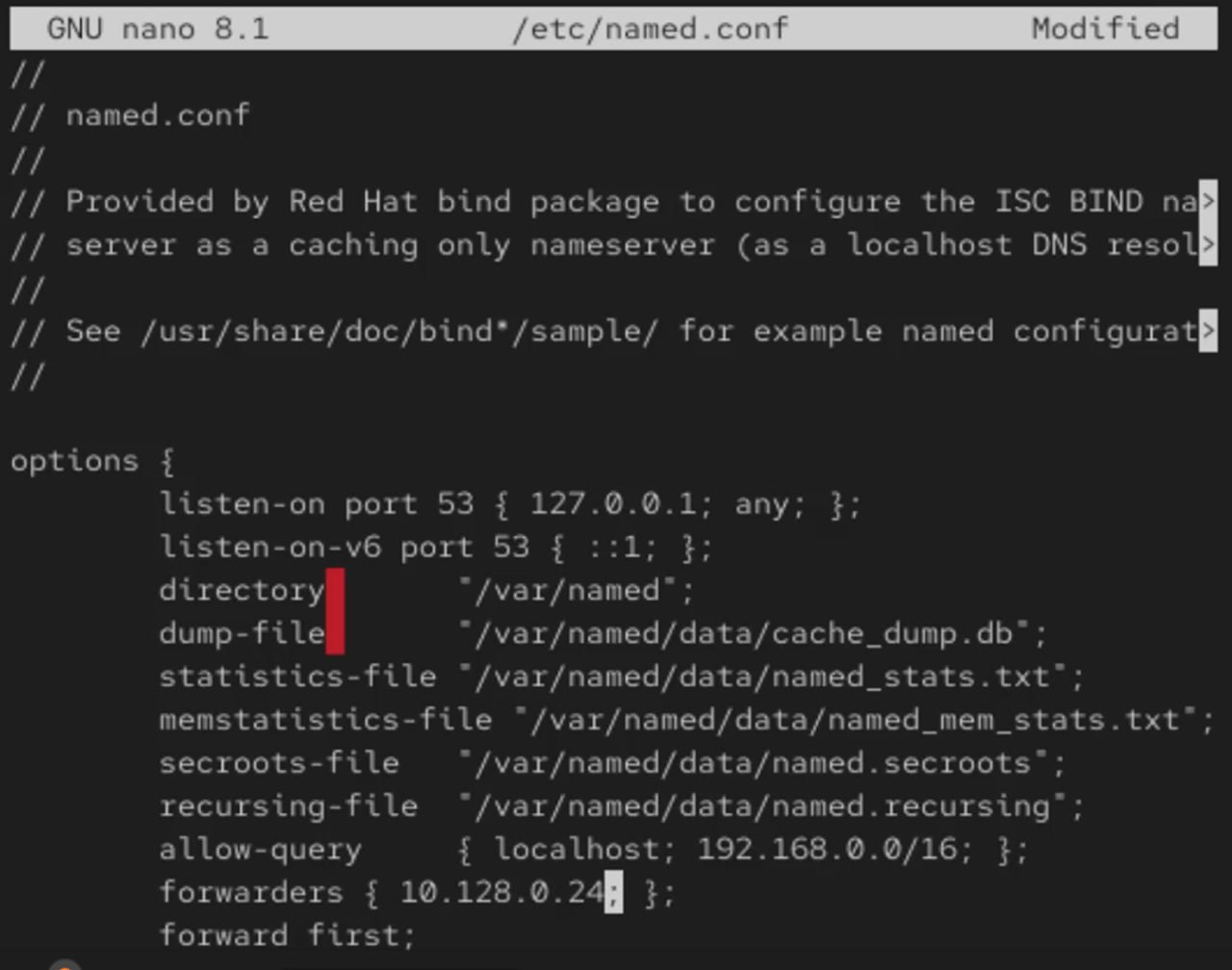


Рис. 12: Редактирование named.conf

Далее копируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименовываем его(рис. 13).

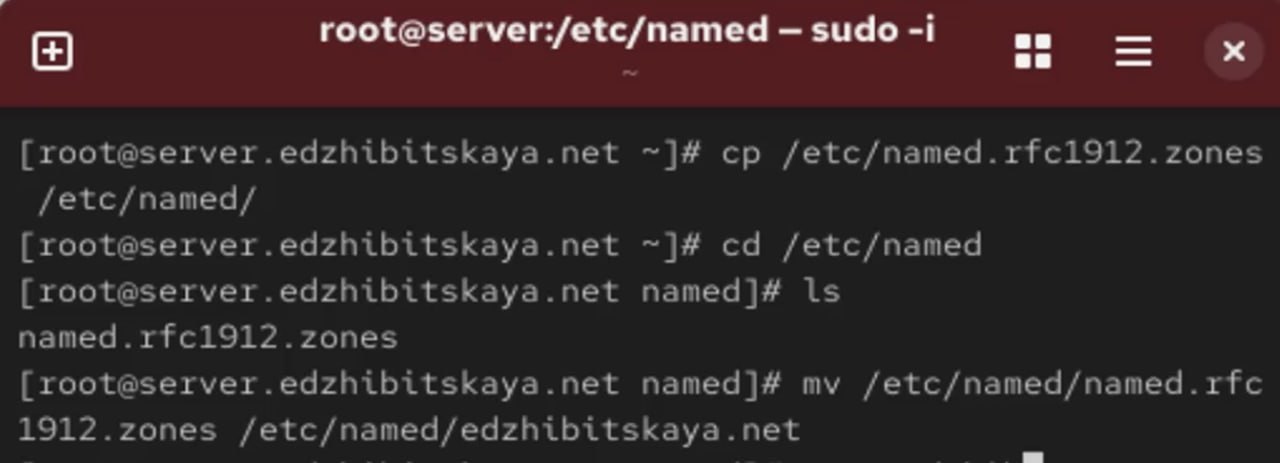


Рис. 13: Перемещение файла

Включим файл описания зоны /etc/named/user.net в конфигурационном файле DNS /etc/named.conf(рис. 14), отредактируем файл /etc/named/edzhibitskaya.net(рис. 15).

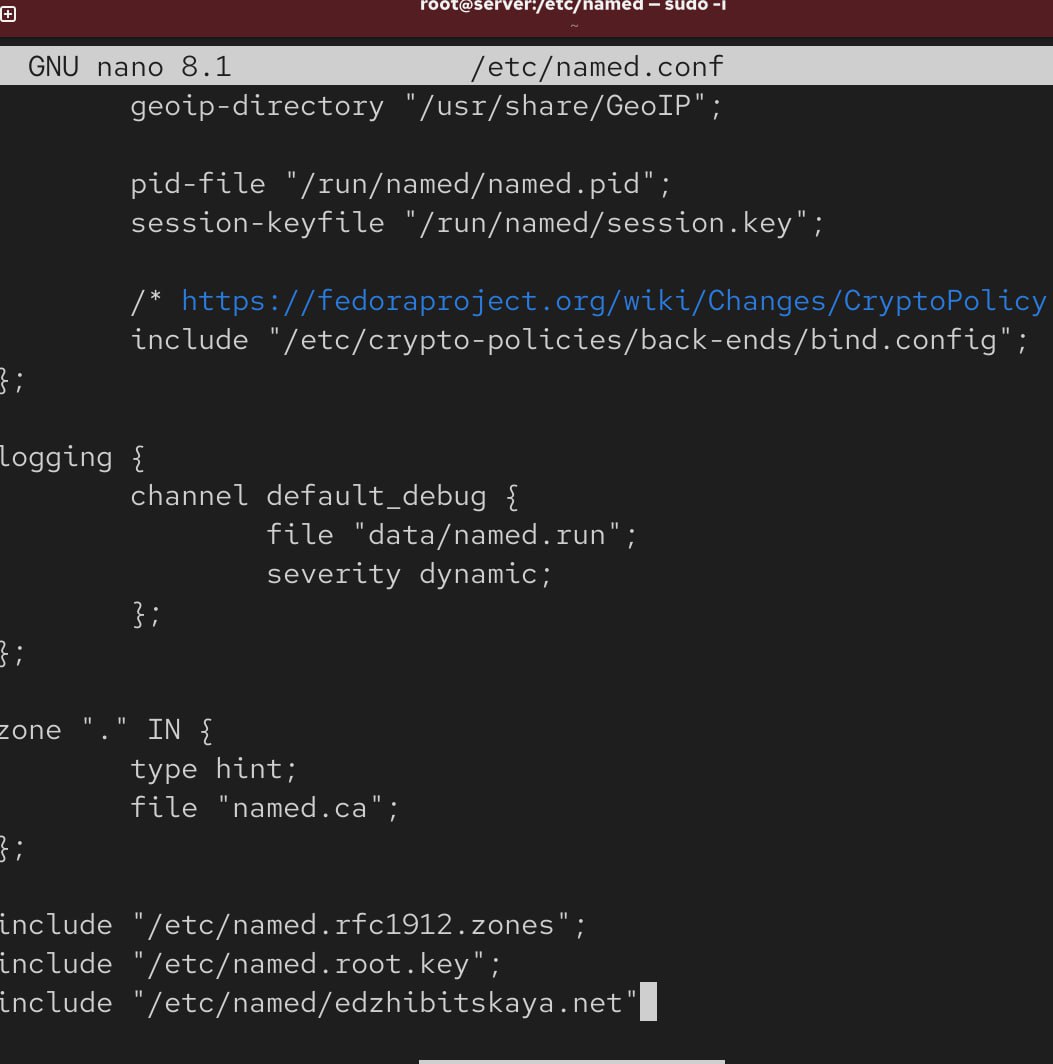


Рис. 14: /etc/named.conf

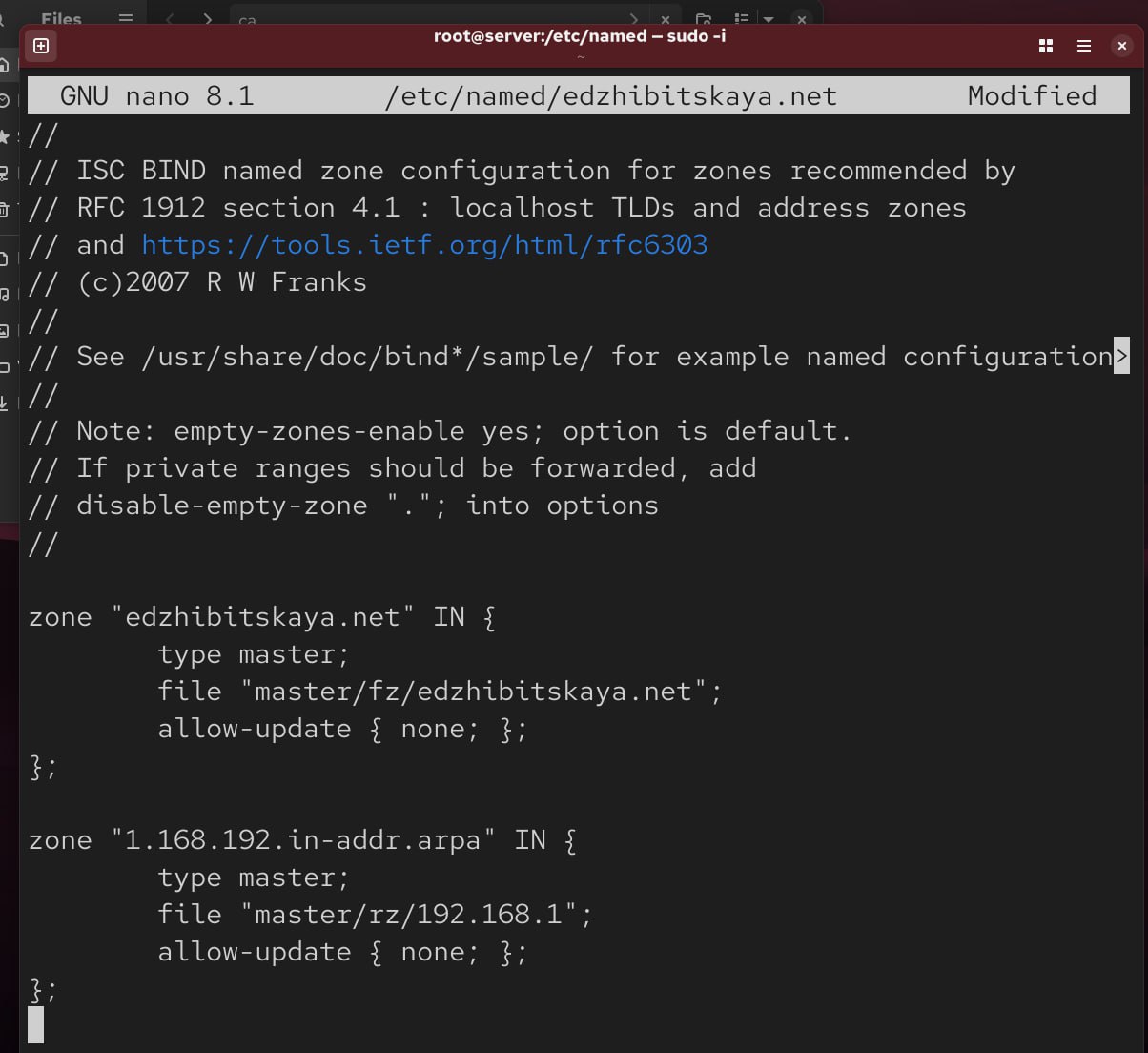


Рис. 15: /etc/named/edzhibitskaya.net

В каталоге /var/named создаем подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно, скопируем шаблон прямой DNS-зоны named.localhost и переименуем его в edzhibitskaya.net(рис. 16).

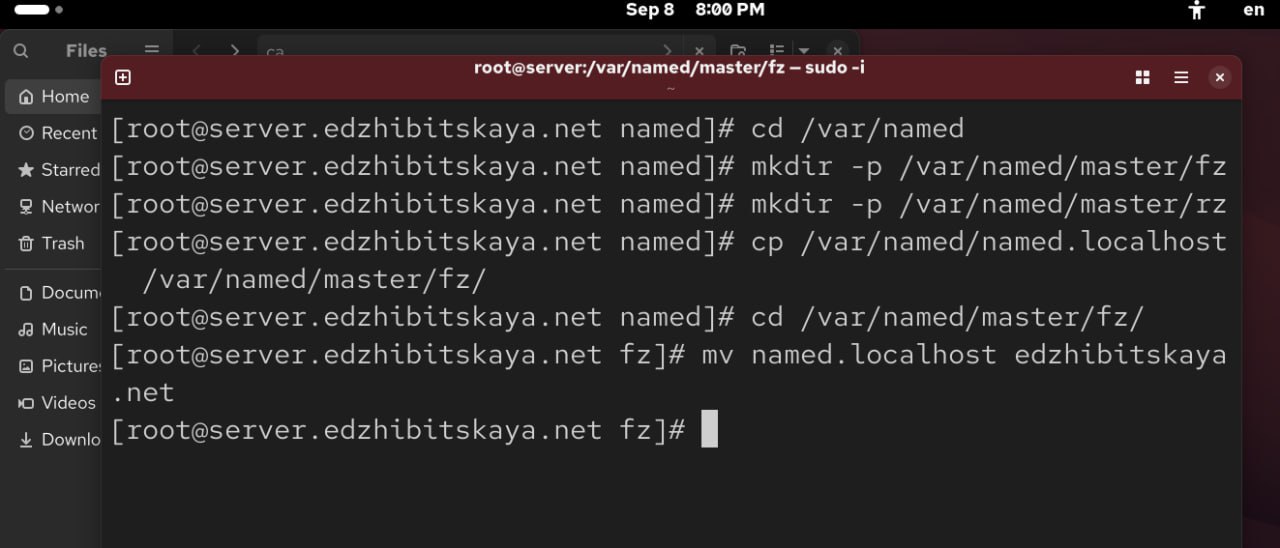


Рис. 16: Создание подкаталогов

Далее редактируем файл(рис. 17).



Рис. 17: edzhibitskaya.net

Копируем шаблон обратной DNS-зоны named.loopback, переименовываем его в 192.168.1(рис. 18), также редактируем(рис. 19).

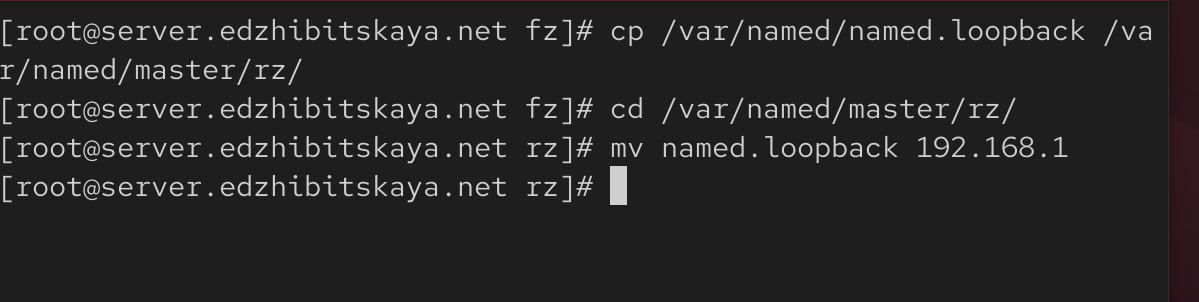


Рис. 18: Копирование файла

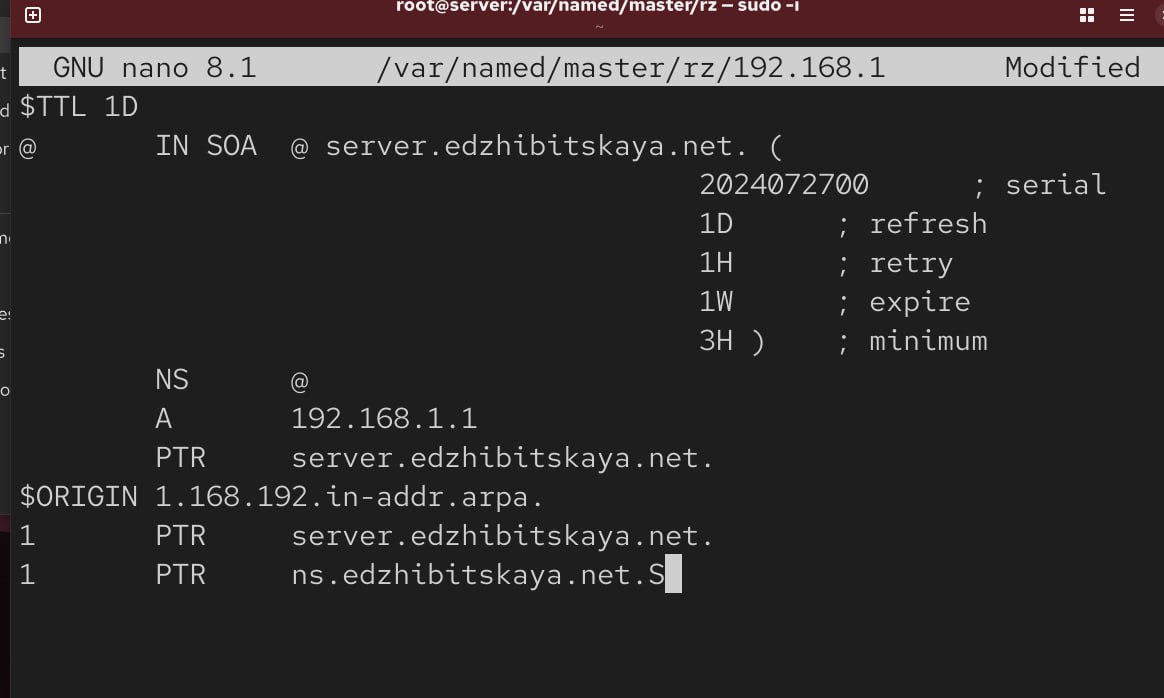


Рис. 19: 192.168.1

Исправляем права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать и после изменения доступа к конфигурационным файлам named корректно восстановливаем их метки в SELinux(рис. 20).

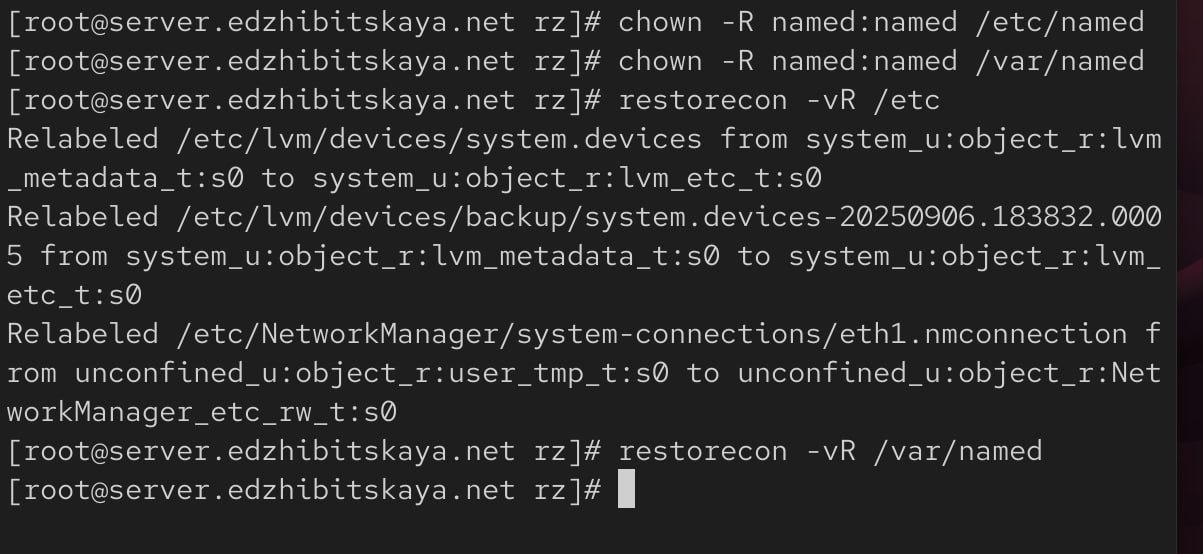


Рис. 20: Права и метки

Еще необходимо проверить состояние переключателей, дать разрешение на запись(рис. 21).

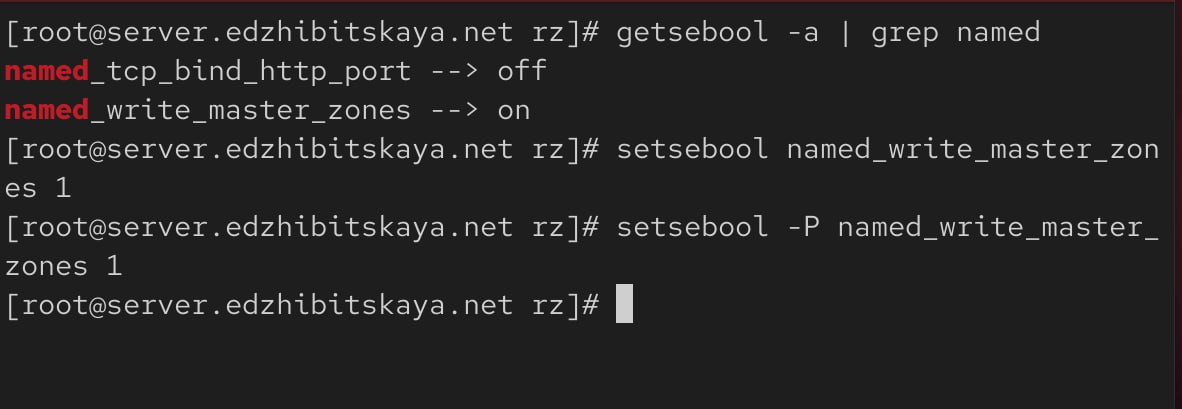


Рис. 21: Переключатели

В дополнительном терминале запускаем в режиме реального времени расширенный лог системных сообщений и в первом терминале перезапускаем сервер(рис. 22).

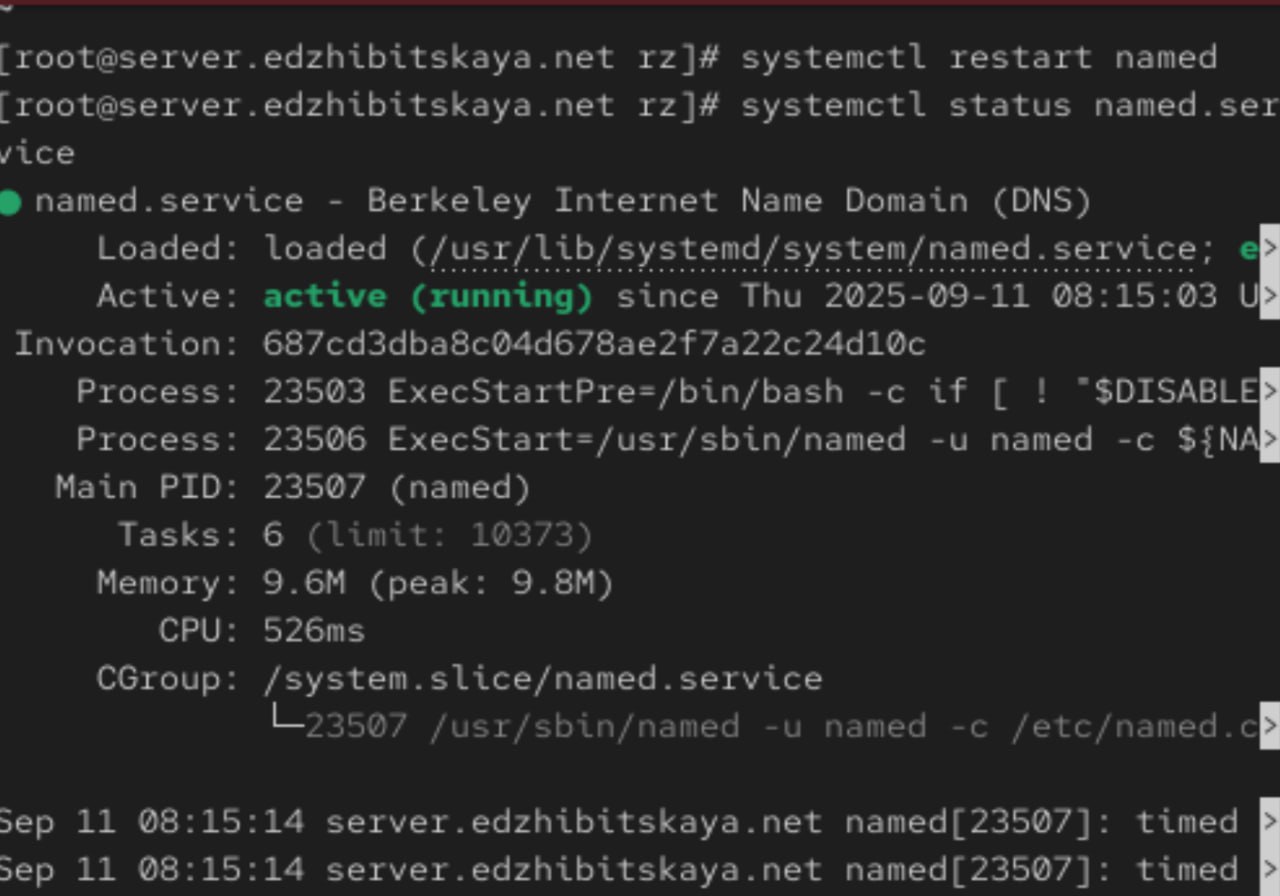


Рис. 22: Перезапуск

Для анализа работы DNS-сервера воспользуемся утилитами dig и host(рис. 23) и (рис. 24), (рис. 25).

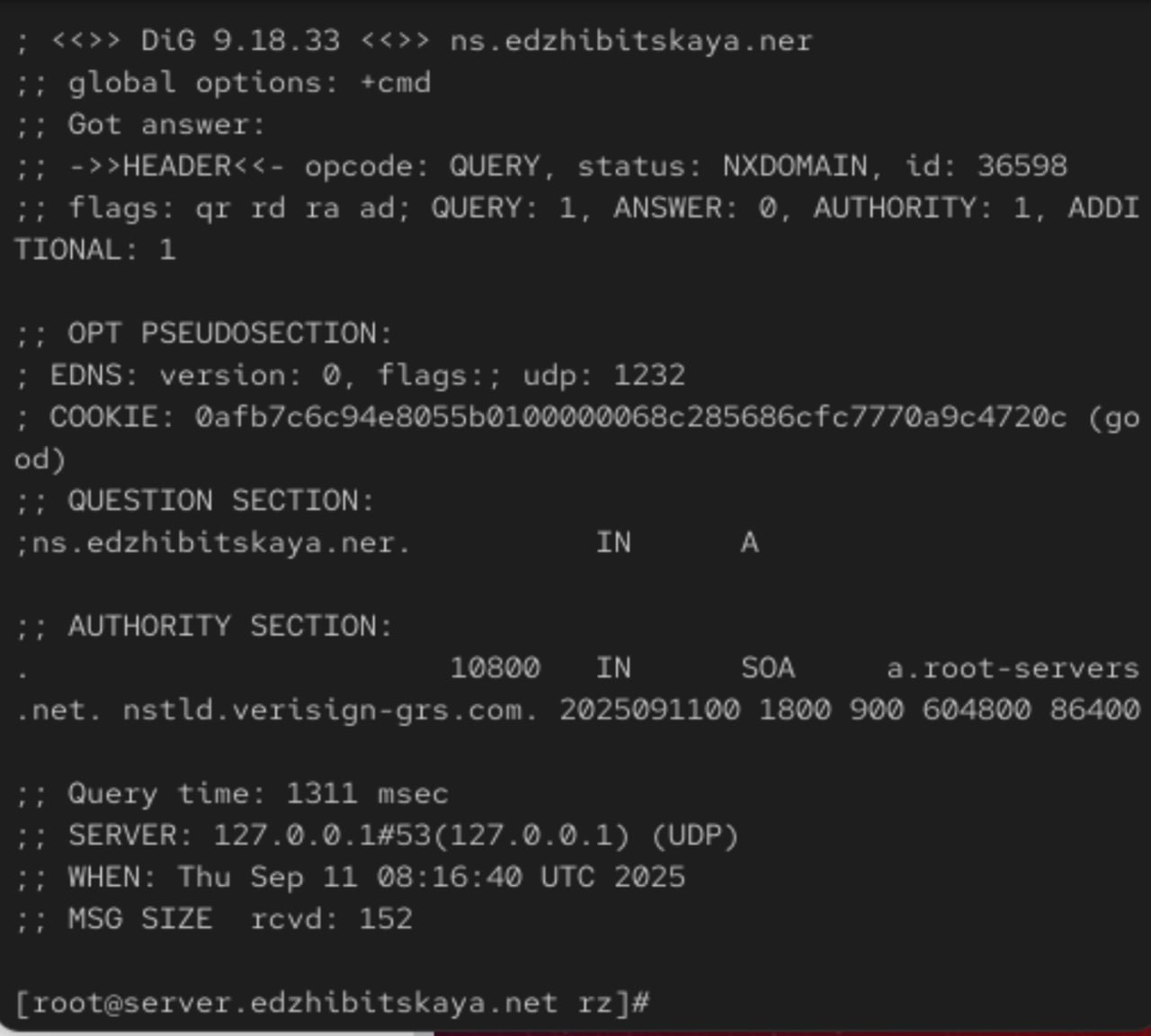


Рис. 23: Описание DNS-зоны с сервера

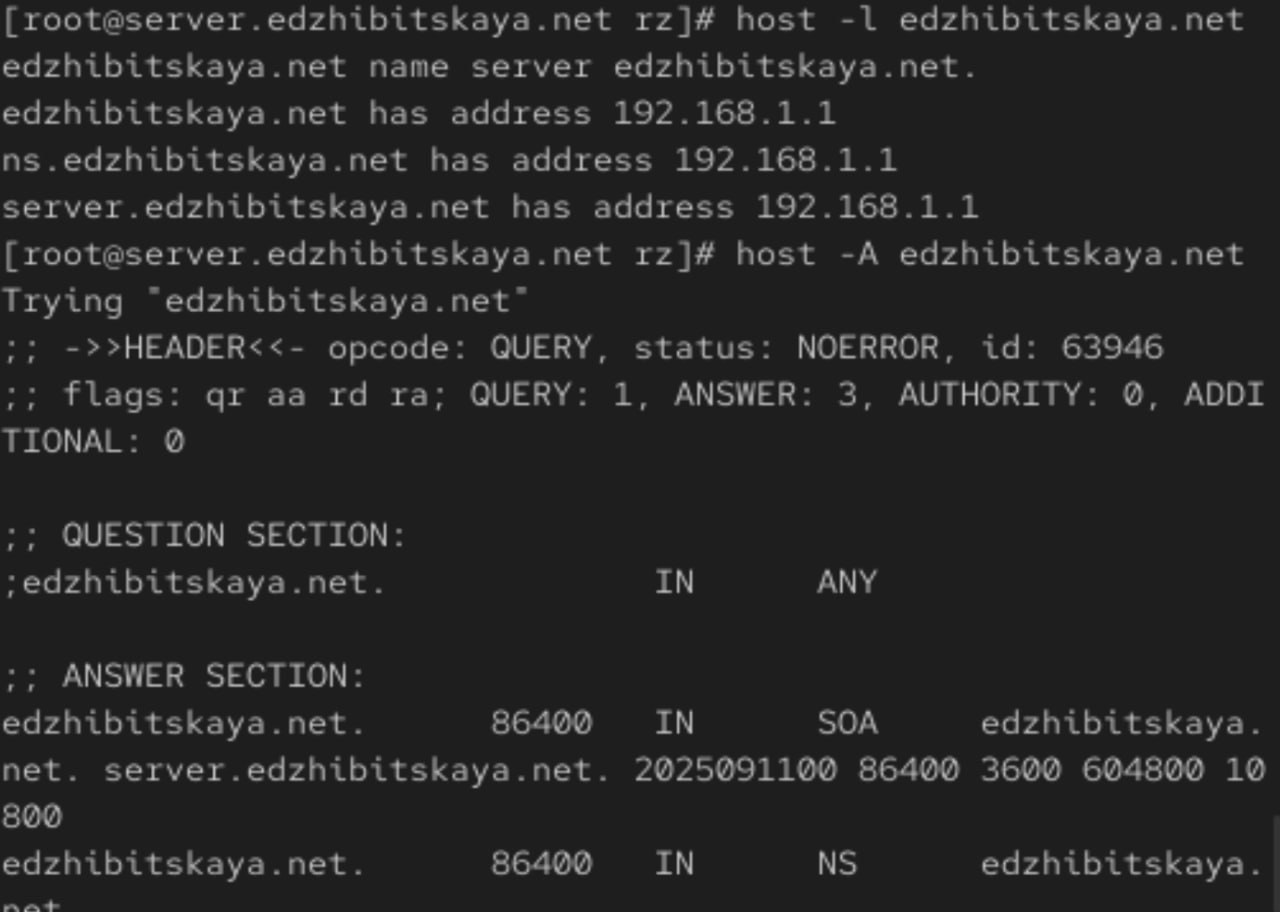


Рис. 24: host -l; host -a

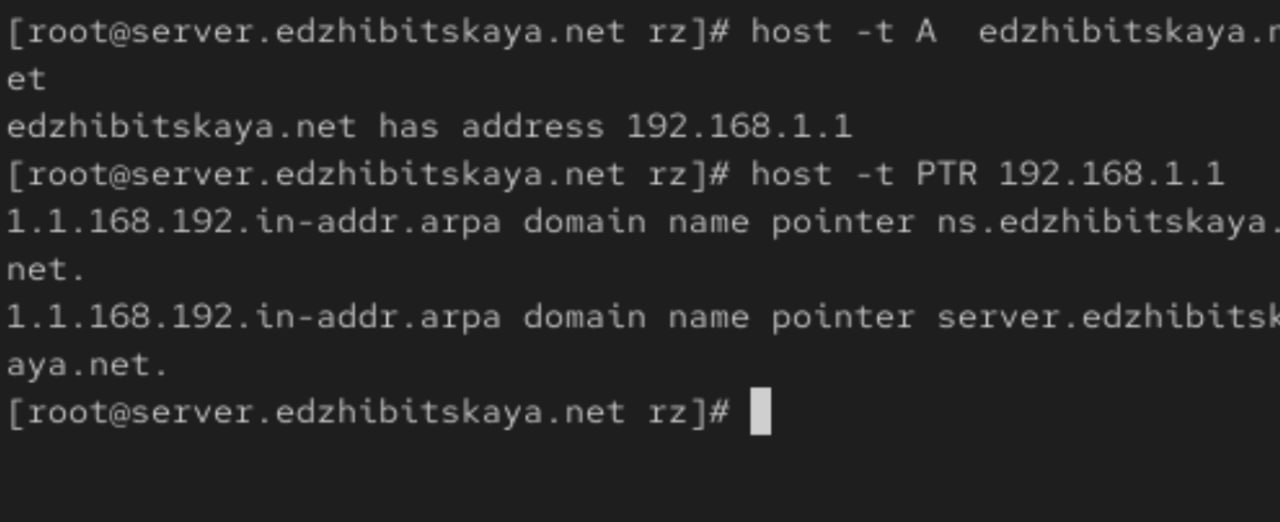


Рис. 25: host -t

Наконец, в каталог для внесения изменений в настройки внутреннего окружения добавим необходимые директории(рис. 26), создадим исполняемый файл(рис. 27) и пропишем скрипт(рис. 28).



Рис. 26: Добавление изменений

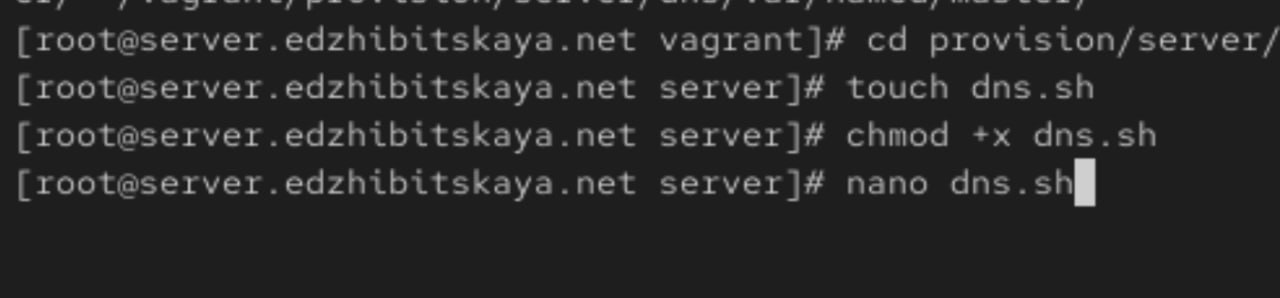


Рис. 27: Создание файла

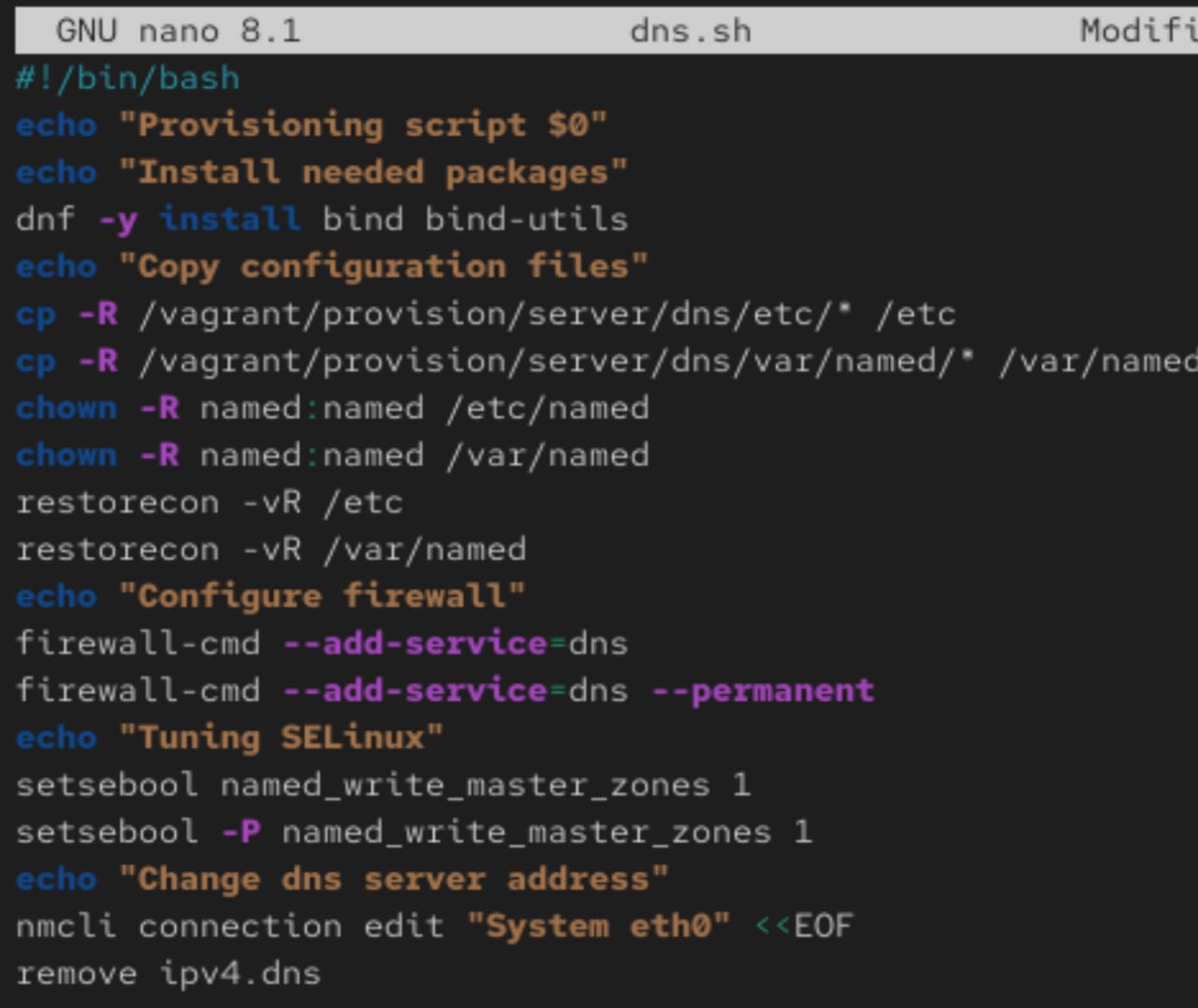


Рис. 28: Скрипт

Внесем изменения в Vagrantfile для отработки скрипта(рис. 29).

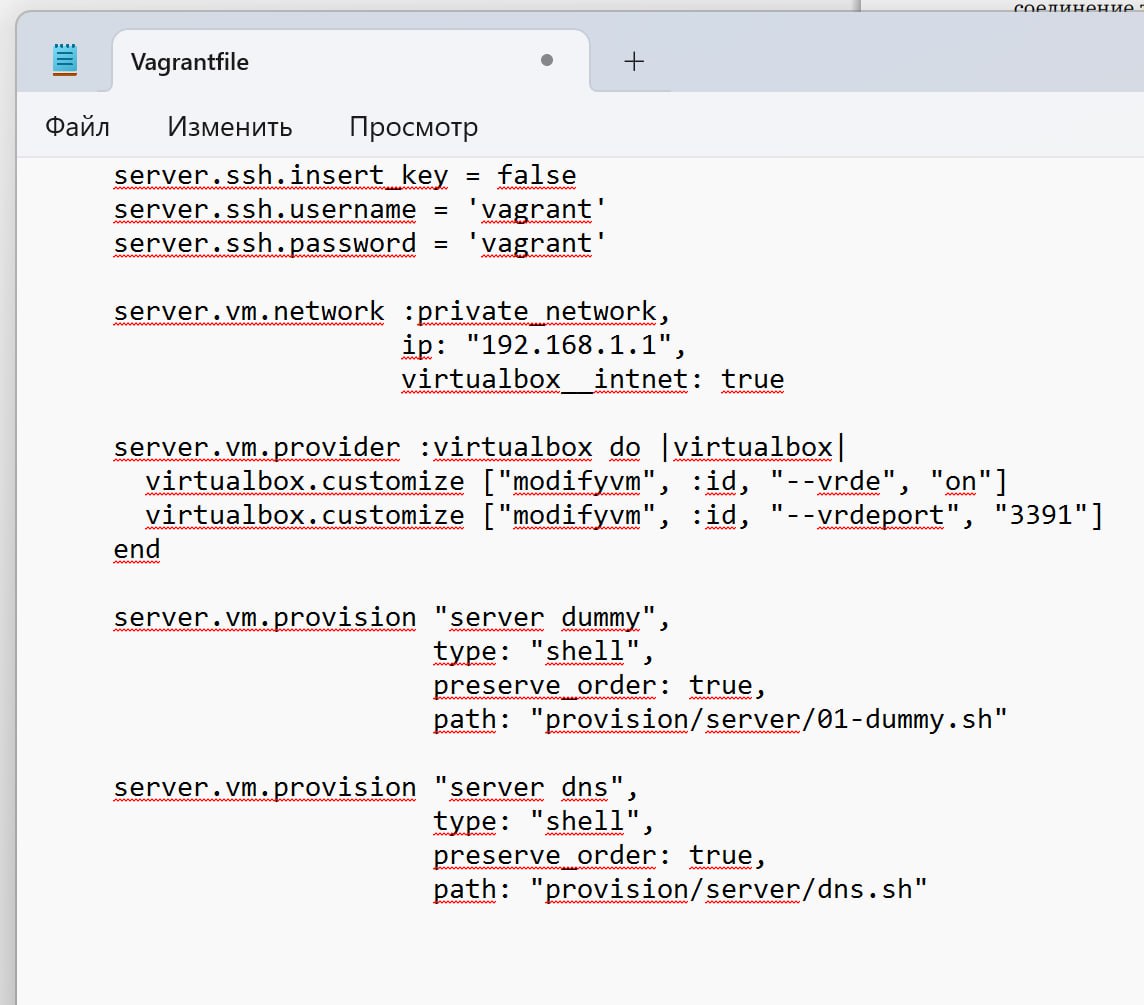


Рис. 29: Vagrantfile

# 3 Ответы на контрольные вопросы

1. Что такое DNS?

Система доменных имён, преобразующая имена в IP-адреса и обратно.

1. Каково назначение кэширующего DNS-сервера?

Кэшировать DNS-запросы для ускорения ответов и снижения сетевой нагрузки.

1. Чем отличается прямая DNS-зона от обратной?

* Прямая: имя → IP
* Обратная: IP → имя

1. В каких каталогах и файлах настройки DNS-сервера?

* /etc/named.conf – главный конфиг
* /var/named/ – файлы зон (зона.db)

1. Что указывается в файле resolv.conf?

Адреса DNS-серверов для клиента: nameserver 8.8.8.8

1. Какие есть типы записей ресурсов?

* A – IPv4 адрес
* AAAA – IPv6 адрес
* CNAME – псевдоним
* MX – почтовый сервер
* NS – DNS-сервер зоны
* PTR – обратная запись (IP → имя)

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

Для организации обратных зон DNS (поиск имени по IP).

1. Для чего нужен демон named?

Это основная служба DNS-сервера BIND, обрабатывающая запросы.

1. Функции master/slave серверов?

* Master – авторитативный, хранит оригиналы зон
* Slave – резервный, копирует зоны с master

1. Параметры времени обновления зоны?

* refresh – время обновления
* retry – время повтора при ошибке
* expire – время устаревания
* TTL – время жизни кэша

1. Как защитить зону от скачивания?

Настроить ACL и запретить трансфер зоны для посторонних.

1. Запись для почтовых серверов?

MX (Mail Exchange).

1. Как протестировать DNS?

Команды: nslookup, dig, host.

1. Управление службами?

* systemctl start
* systemctl stop
* systemctl restart

1. Просмотр отладочной информации?

journalctl -u

1. Где хранятся логи?

/var/log/. Просмотр: journalctl, tail -f /var/log/messages

1. Какие файлы использует процесс?

lsof -p

1. Примеры nmcli:

* nmcli con up eth0
* nmcli con modify eth0 ipv4.addresses “192.168.1.10/24”

1. Что такое SELinux?

Система принудительного контроля доступа, дополняющая стандартные права.

1. Что такое контекст SELinux?

Метка безопасности, определяющая политику доступа для объекта.

1. Как восстановить контекст?

restorecon -Rv /путь/

1. Как создать правила из логов?

audit2allow -a -M модуль

1. Булевый переключатель?

Параметр, который можно включить или выключить для изменения поведения политики.

1. Список переключателей?

getsebool -a

1. Изменение переключателя?

setsebool -P httpd\_can\_network\_connect on

# 4 Выводы

В ходе работы были получены навыки по установке и конфигурированию DNSсервера, усвоены принципы работы системы доменных имён на ОС Rocky linux.

# Список литературы

[ТУИС]{https://esystem.rudn.ru/pluginfile.php/2854732/mod\_resource/content/8/002-dns.pdf}