Отчет по лабораторной работе №2

Настройка DNS-сервера

Галацан Николай, НПИбд-01-22

Содержание

# 1 Цель работы

Приобретение практических навыков по установке и конфигурированию DNSсервера, усвоение принципов работы системы доменных имён.

# 2 Выполнение лабораторной работы

## 2.1 Установка DNS-сервера

Запускаю ВМ через рабочий каталог. На ВМ server вхожу под собственным пользователеми перехожу в режим суперпользователя. Устанавливаю bind и bind-utils (рис. 1).

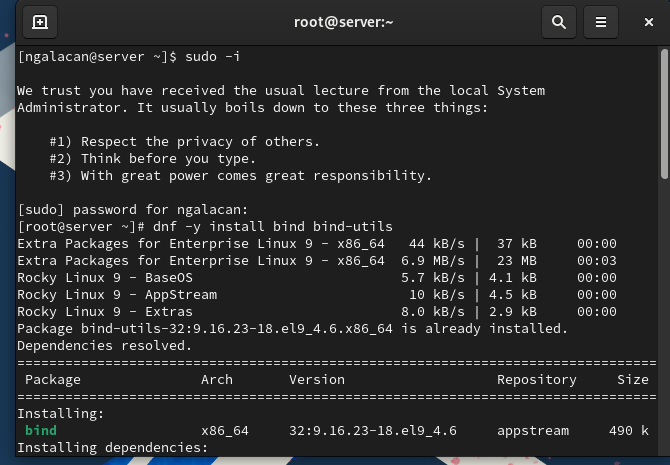


Рис. 1: Установка bind, bind-utils

С помощью утилиты dig делаю запрос к DNS-адресу (рис. 2)

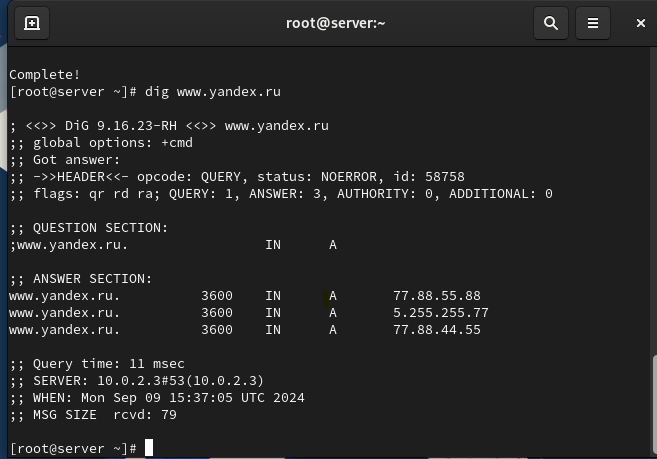


Рис. 2: Использование dig

## 2.2 Конфигурирование кэширующего DNS-сервера

Просматриваю файлы /etc/resolv.conf, /etc/named.conf (рис. 3), /var/named/named.ca (рис. 4), /var/named/named.localhost, /var/named/named.loopback (рис. 5).

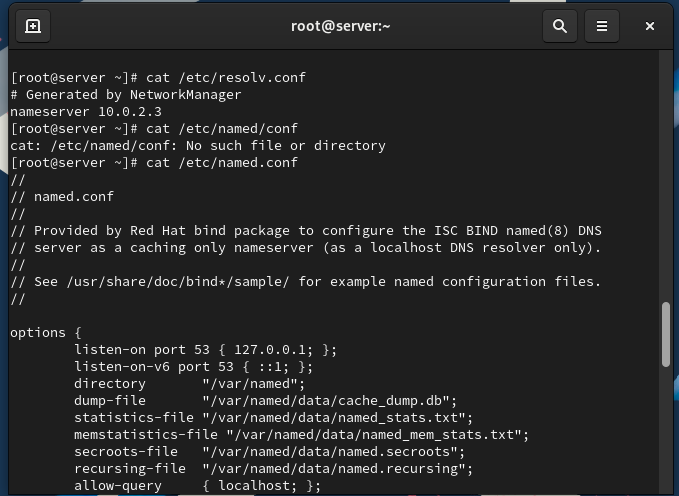


Рис. 3: /etc/resolv.conf, /etc/named.conf

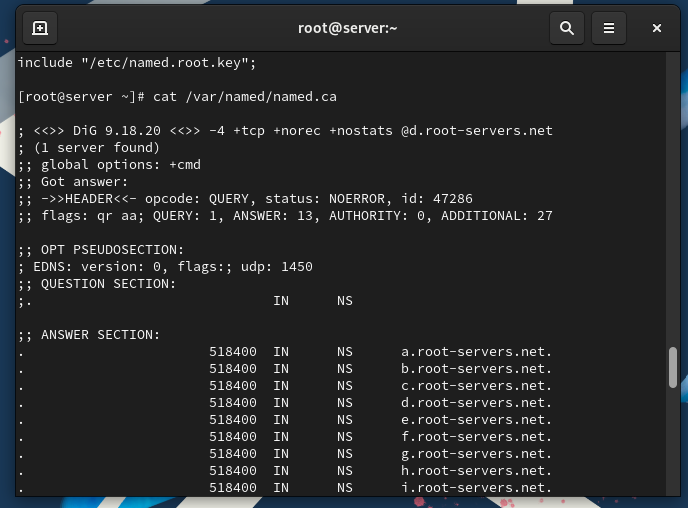


Рис. 4: /var/named/named.ca

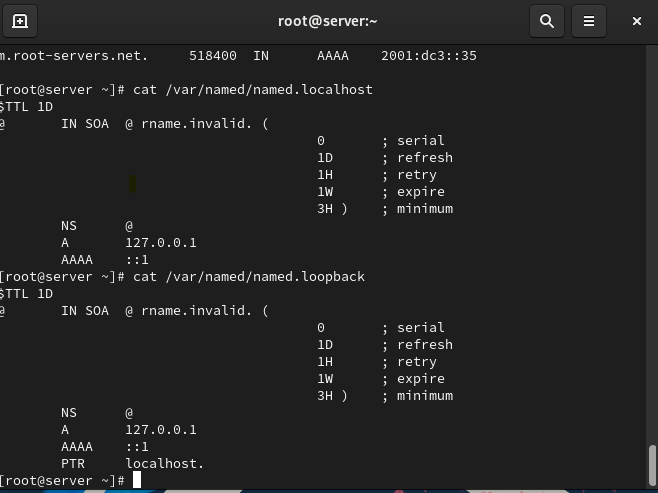


Рис. 5: /var/named/named.localhost, /var/named/named.loopback

Запускаю DNS-сервер и включаю в автозапуск:

systemctl start named  
systemctl enable named

Ввожу dig @127.0.0.1 www.yandex.ru и анализирую отличия в информации от рис. 2. В данном случае выводится больше данных (рис. 6).

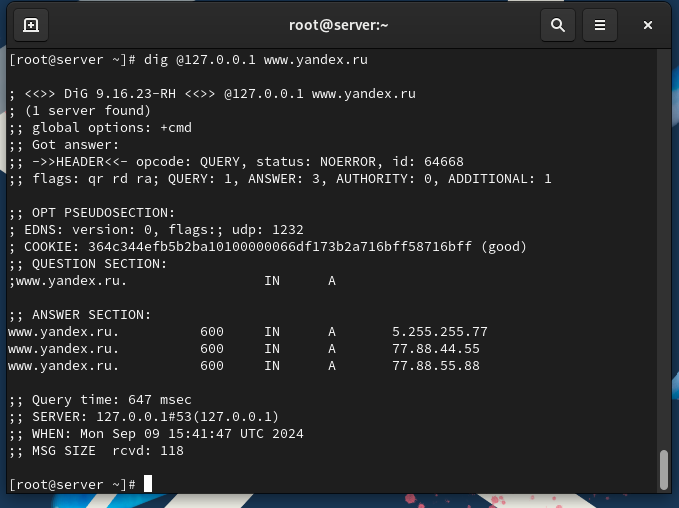


Рис. 6: Использование dig (2)

Сделаю DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить настройки сетевого соединения eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0.1 (рис. 7). То же самое делаю для System eth0 (рис. 8)

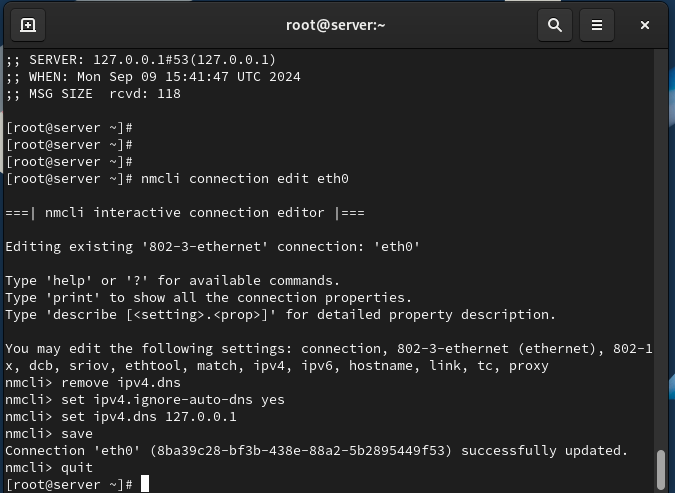


Рис. 7: Изменение настроек сетевого соединения eth0

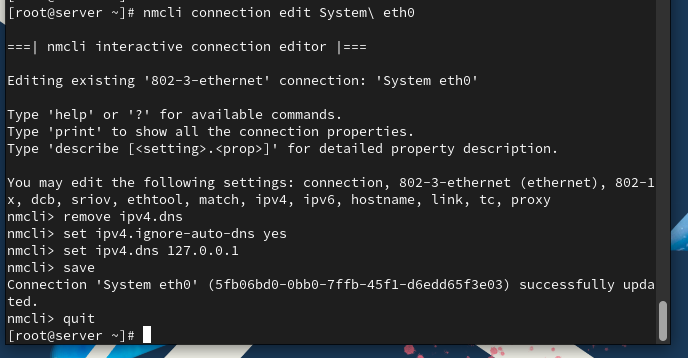


Рис. 8: Изменение настроек сетевого соединения System eth0

Перезапускаю NetworkManager и проверяю наличие изменений в файле /etc/resolv.conf (рис. 9).

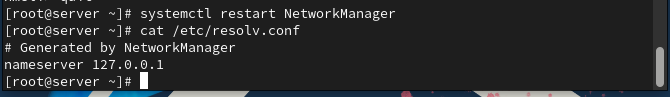


Рис. 9: Перезапуск NetworkManager и просмотр файла

Вношу изменения в файл /etc/named.conf (рис. 10).

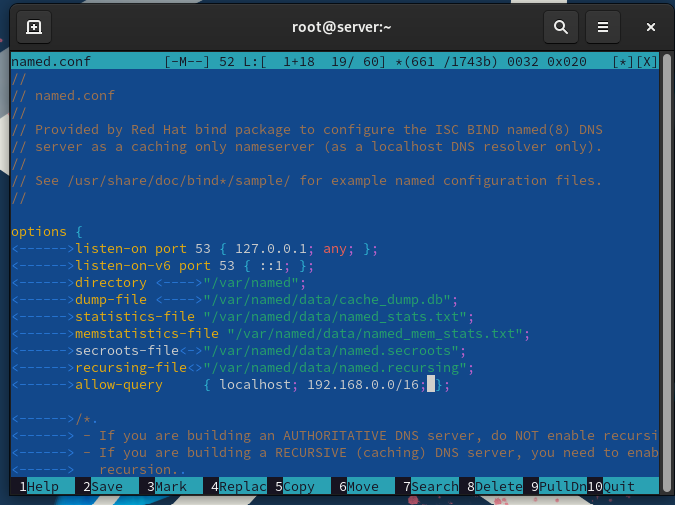


Рис. 10: Внесение изменений в файл /etc/named.conf

Вношу изменения в настройки межсетевого экрана узла server, разрешив работу с DNS. Убеждаюсь, что DNS-запросы идут через узел server, который прослушивает порт 53 (рис. 11).

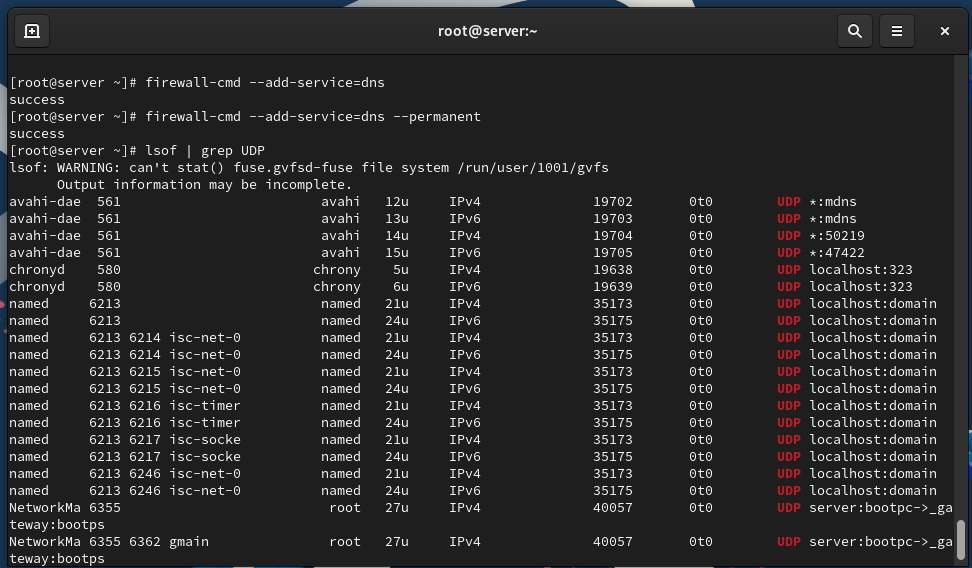


Рис. 11: Внесение изменений в настройки межсетевого экрана узла server, проверка

Для конфигурирования кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами вношу изменения в файл named.conf (рис. 12)

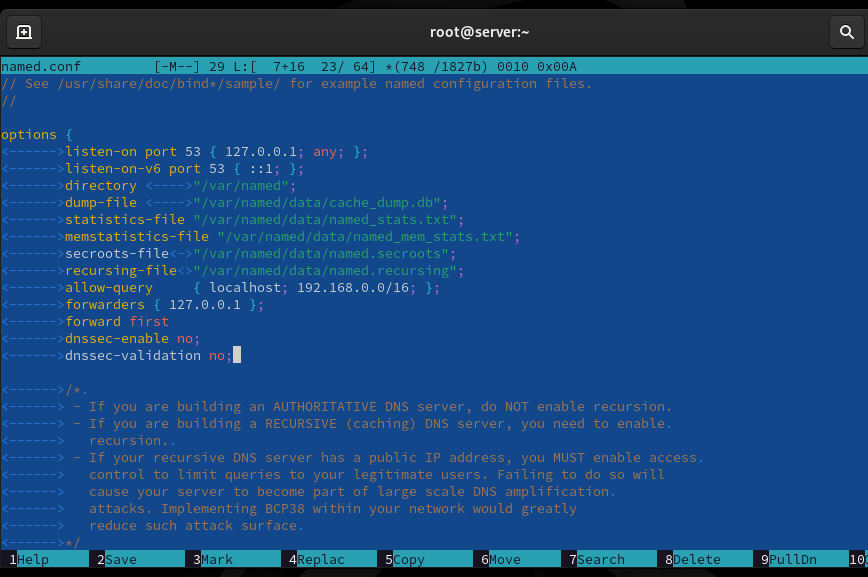


Рис. 12: Редактирование named.conf

## 2.3 Конфигурирование первичного DNS-сервера

Ввожу команды:

cp /etc/named.rfc1912.zones /etc/named/  
cd /etc/named  
mv /etc/named/named.rfc1912.zones /etc/named/ngalacan.net

Включаю файл описания зоны /etc/named/ngalacan.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку: include "/etc/named/user.net";.

Редактирую файл /etc/named/user.net (рис. 13)

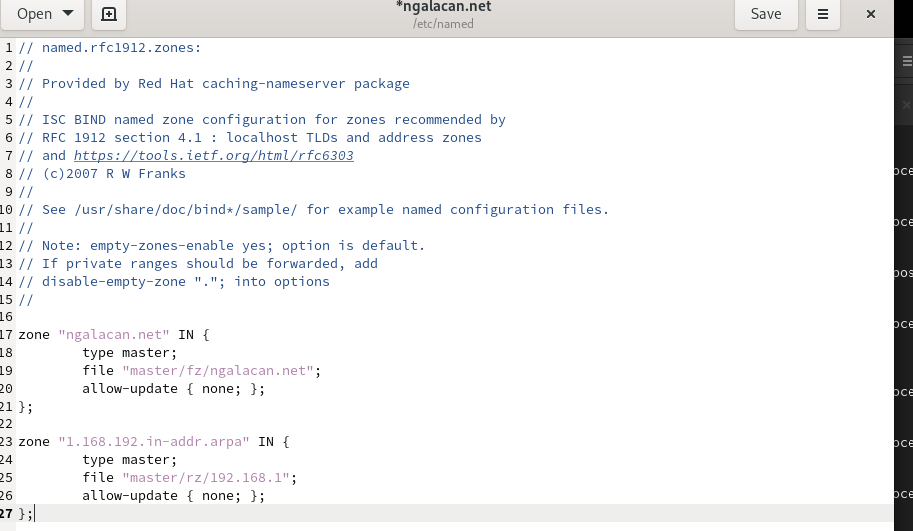


Рис. 13: Редактирование файла /etc/named/user.net

В каталоге /var/named создаю подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно. Копирую шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz, переименовав его в ngalacan.net (рис. 14).

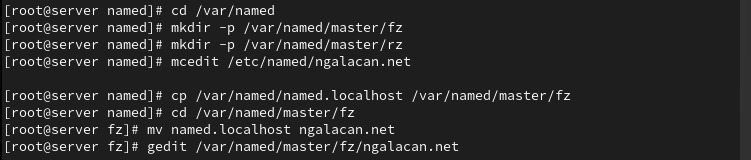


Рис. 14: Создание каталогов, копирование шаблона прямой зоны, переименование

Изменяю файл /var/named/master/fz/ngalacan.net (рис. 15).

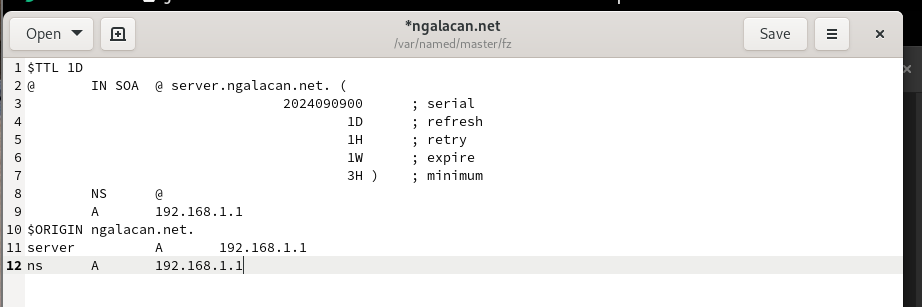


Рис. 15: Редактирование /var/named/master/fz/ngalacan.net

Копирую шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуйте его в 192.168.1 (рис. 16).

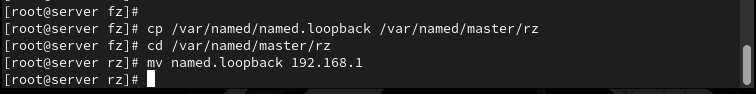


Рис. 16: Копирование шаблона обратной зоны, переименование

Изменяю файл /var/named/master/rz/192.168.1 (рис. 17).

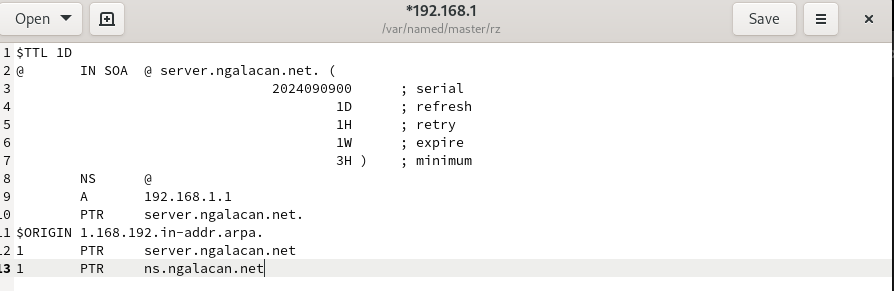


Рис. 17: Редактирование /var/named/master/rz/192.168.1

Изменяю права доступа, восстанавливаю метки SELinux, проверяю (рис. 18).

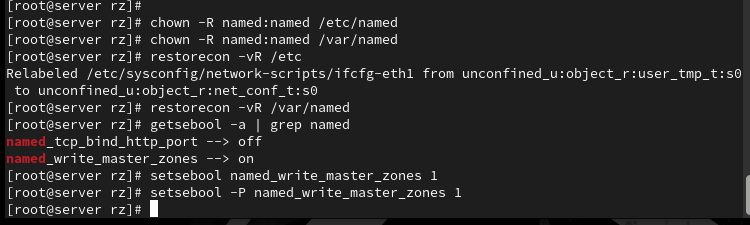


Рис. 18: Изменение прав доступа, восстановление меток SELinux, проверка

Во втором терминале открываю лог системных сообщений. В первом терминале перезапускаю DNS-сервер. После исправления всех ошибок и опечаток DNS-сервер запускается успешно (рис. 19).

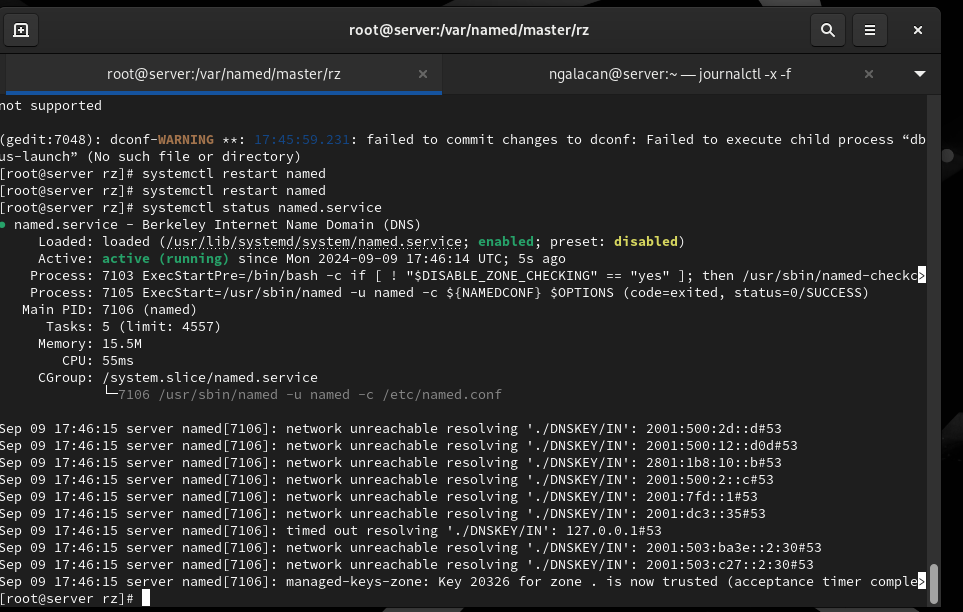


Рис. 19: Запуск DNS-сервера после исправления ошибок

## 2.4 Анализ работы DNS-сервера

При помощи утилиты dig получаю описание DNS-зоны с сервера ns.ngalacan.net (рис. 20).

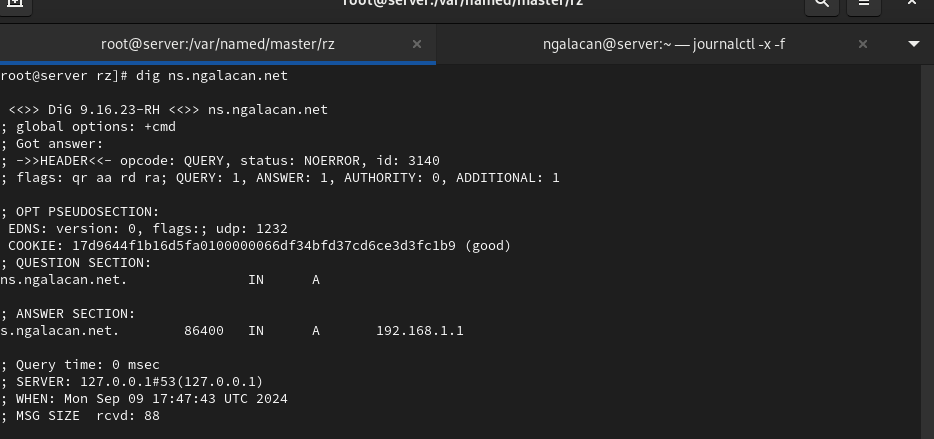


Рис. 20: Описание DNS-зоны с сервера ns.ngalacan.net

Анализирую корректность работы DNS-сервера (рис. 21).

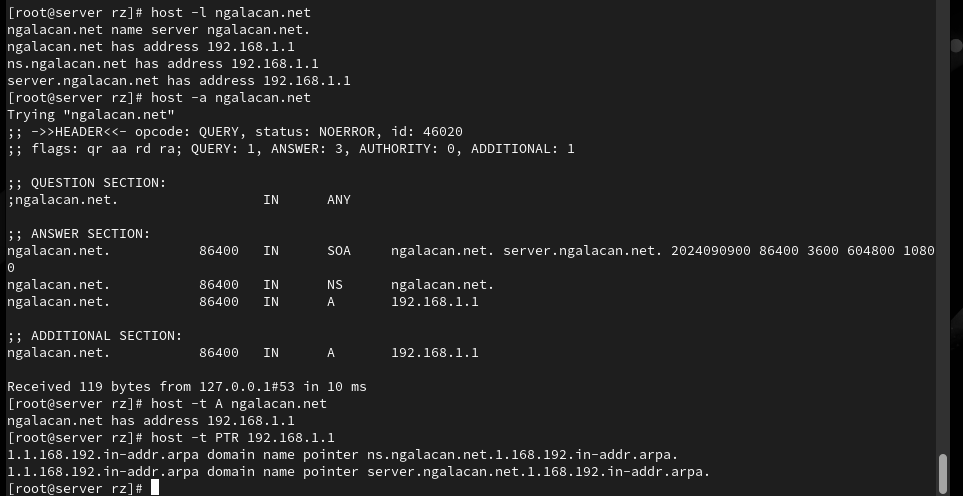


Рис. 21: Анализ корректности работы DNS-сервера

## 2.5 Внесение изменений в настройки внутреннего окружения виртуальной машины

Перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаю в нём каталог dns, в который помещаю в соответствующие каталоги конфигурационные файлы DNS (рис. 22).

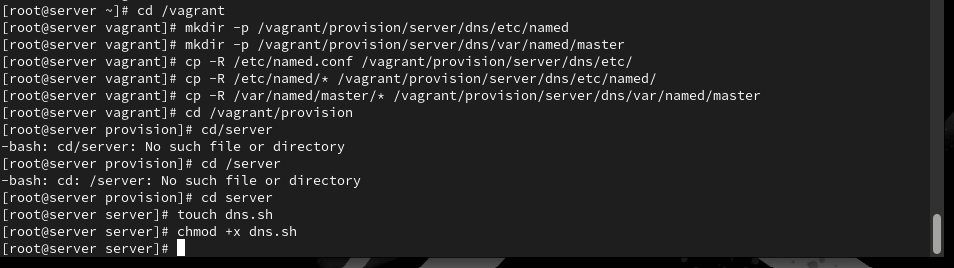


Рис. 22: Размещение конфигурационных файлов в каталог /vagrant/provision/server/dns

Создаю скрипт dns.sh (рис. 23).

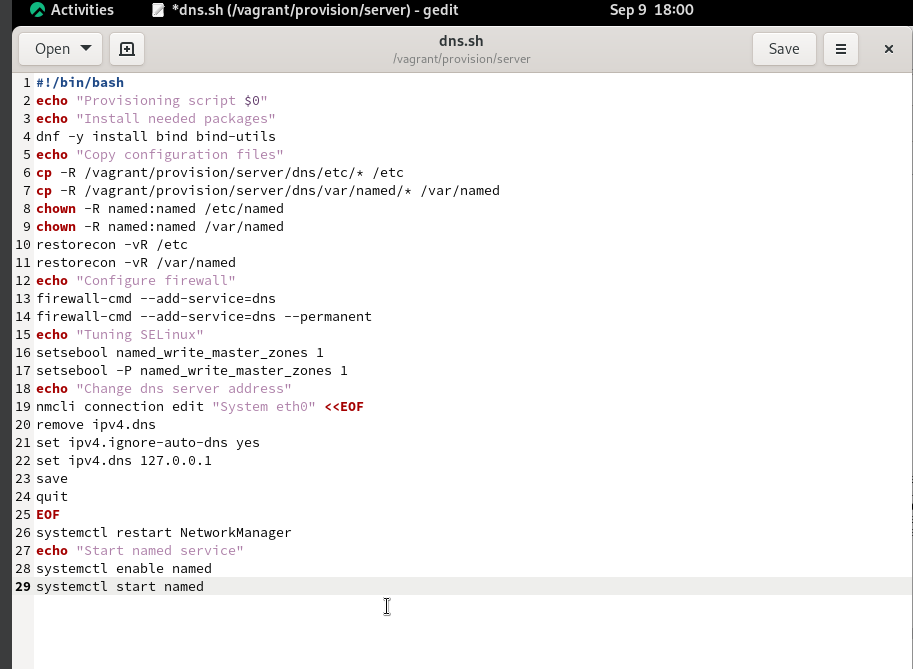


Рис. 23: Редактирование скрипта dns.sh

Для отработки созданного скрипта во время загрузки виртуальной машины в конфигурационном файле Vagrantfile вношу изменения в разделе конфигурации для сервера (рис. 24).

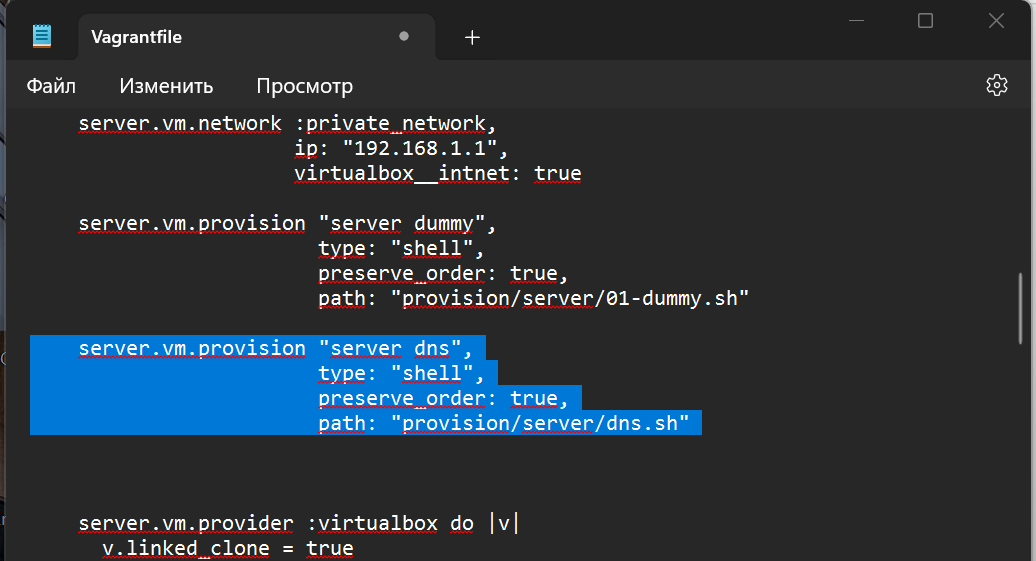


Рис. 24: Редактирование Vagrantfile

# 3 Выводы

В результате выполнения работы были приобретены практические навыки по установке и конфигурированию DNS-сервера, усвоены принципы работы системы доменных имён.

# 4 Ответы на контрольные вопросы

1. Что такое DNS?

* Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса компьютерами для идентификации друг друга в сети.

1. 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.

1. 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.

1. 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.

1. Что указывается в файле resolv.conf?

* Содержит информацию о DNS-серверах, используемых системой, а также о параметрах конфигурации.

1. 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).

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

* Используется для обратного маппинга IP-адресов в доменные имена.

1. Для чего нужен демон named?

* Это DNS-сервер, реализация BIND (Berkeley Internet Name Domain).

1. В чём заключаются основные функции slave-сервера и master-сервера?

* Master-сервер хранит оригинальные записи зоны, slave-серверы получают копии данных от master-сервера.

1. Какие параметры отвечают за время обновления зоны?

* refresh, retry, expire, и minimum.

1. Как обеспечить защиту зоны от скачивания и просмотра?

* Это может включать в себя использование TSIG (Transaction SIGnatures) для аутентификации между серверами.

1. Какая запись RR применяется при создании почтовых серверов?

* MX (Mail Exchange).

1. Как протестировать работу сервера доменных имён?

* Используйте команды nslookup, dig, или host.

1. Как запустить, перезапустить или остановить какую-либо службу в системе?

* systemctl start|stop|restart .

1. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?

* Используйте опции, такие как -d или -v при запуске службы.

1. Где хранится отладочная информация по работе системы и служб? Как её посмотреть?

* В системных журналах, доступных через journalctl.

1. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров.

* lsof -p или fuser -v .

1. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli.

* Примеры включают nmcli connection up|down .

1. Что такое SELinux?

* Это мандатный контроль доступа для ядра Linux.

1. Что такое контекст (метка) SELinux?

* Метка, определяющая, какие ресурсы могут быть доступны процессу или объекту.

1. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?

* restorecon -Rv .

1. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?

* Используйте audit2allow.

1. Что такое булевый переключатель в SELinux?

* Это параметр, который включает или отключает определенные аспекты защиты SELinux.

1. Как посмотреть список переключателей SELinux и их состояние?

* getsebool -a.

1. Как изменить значение переключателя SELinux?

* setsebool -P <on|off>.