Отчёт по лабораторной работе №2

Администрирование сетевых подсистем

Ищенко Ирина Олеговна

Содержание

# 1 Цель работы

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

# 2 Выполнение лабораторной работы

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом: cd /var/tmp/ioithenko/vagrant Далее запустим виртуальную машину server: vagrant up server (рис. 1).

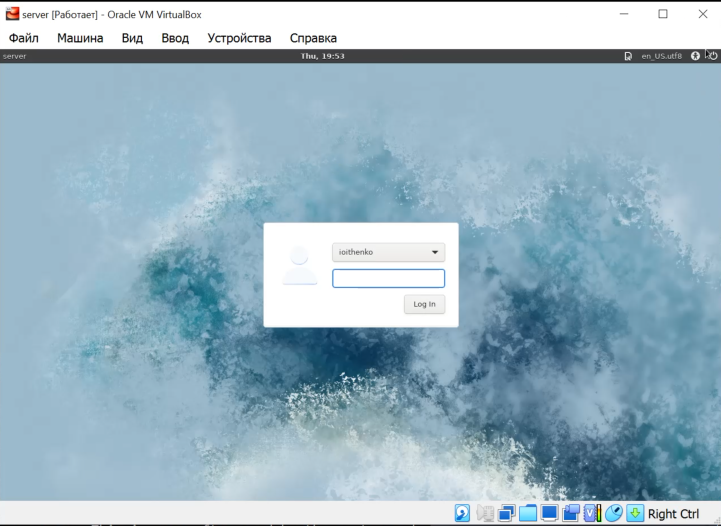


Рис. 1: Запуск ВМ

Перейдём в режим суперпользователя: sudo -i И установим bind и bind-utils (рис. 2): dnf -y install bind bind-utils

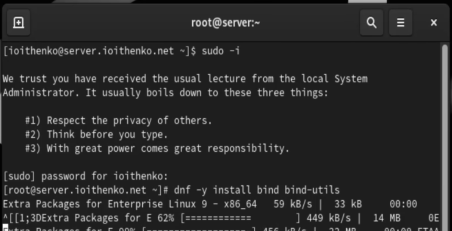


Рис. 2: Установка bind

С помощью утилиты dig сделаем запрос к DNSадресу www.yandex.ru (рис. 3): dig www.yandex.ru

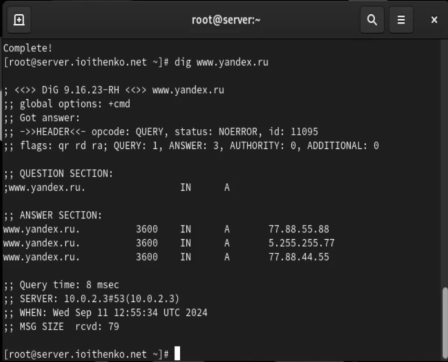


Рис. 3: dig

Просмотрим содержание файлов /etc/resolv.conf, /etc/named.conf (рис. 4), /var/named/named.ca (рис. 5), /var/named/named.localhost, /var/named/named.loopback (рис. 6).

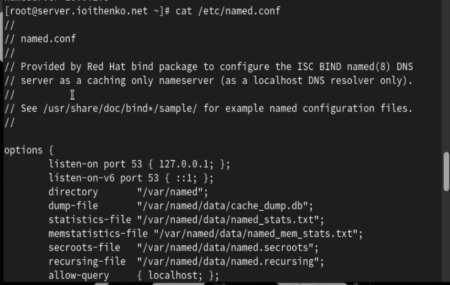


Рис. 4: named.conf

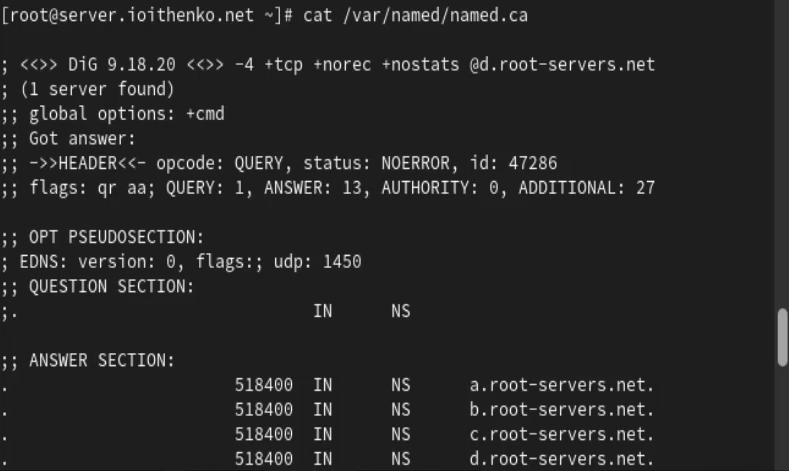


Рис. 5: named.ca

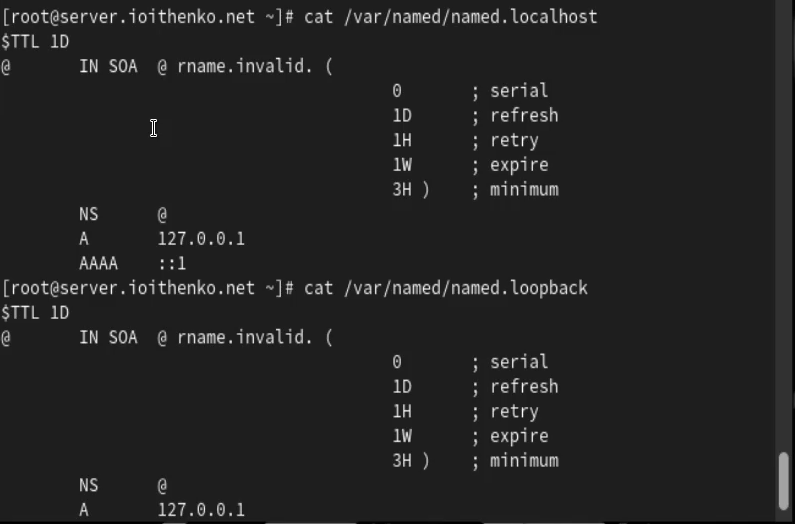


Рис. 6: named.localhost

Запустим DNS-сервер: systemctl start named Включим запуск DNS-сервера в автозапуск при загрузке системы (рис. 7): systemctl enable named

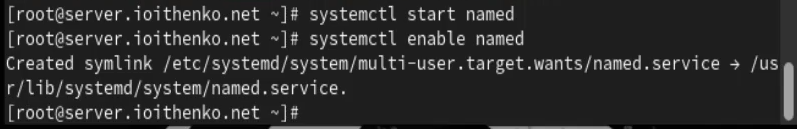


Рис. 7: Запуск сервера

dig [**127.0.0.1?**] www.yandex.ru. Выводится более подробная информация (рис. 8):

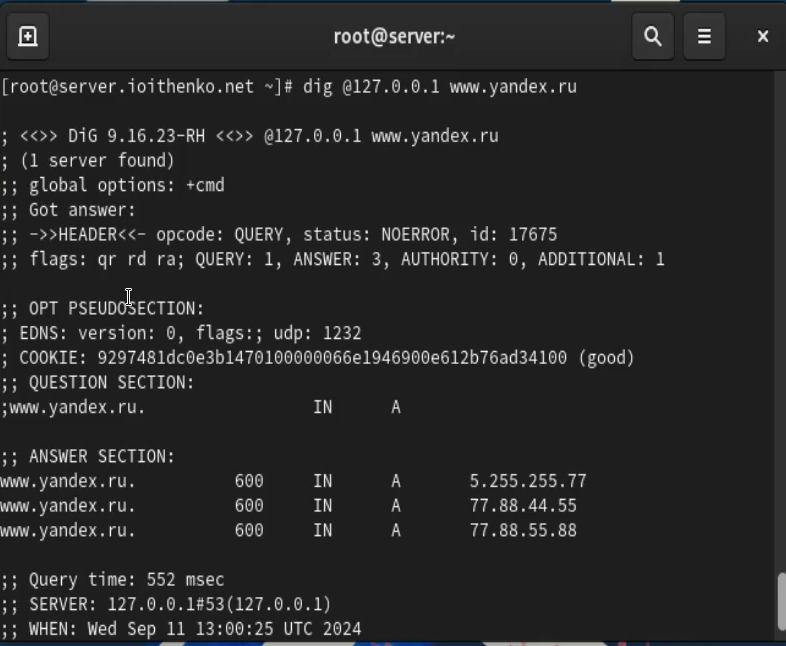


Рис. 8: dig

Сделаем 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. 9).

Перезапускаем NetworkManager и проверяем наличие изменений в файле /etc/resolv.conf (рис. 10).

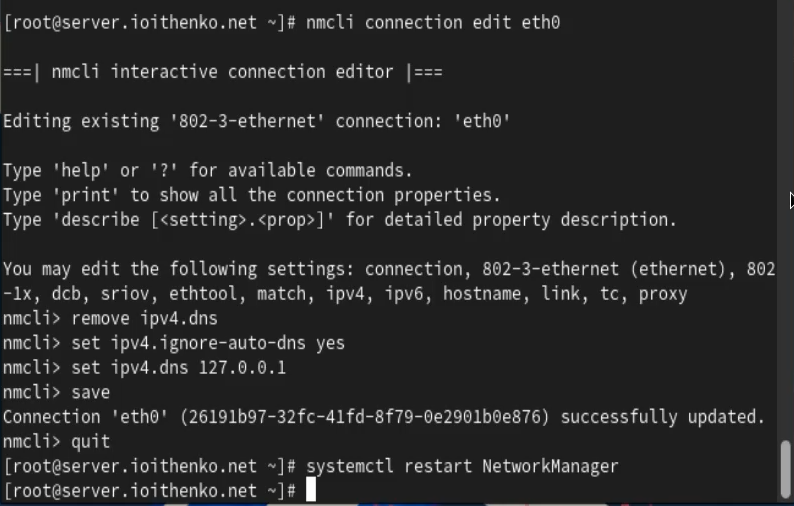


Рис. 9: Изменение настроек сетевого соединения eth0

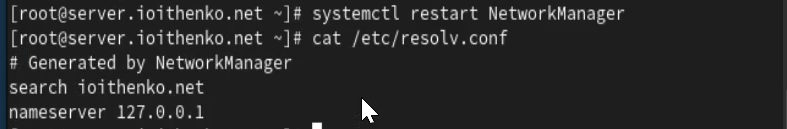


Рис. 10: Перезапуск NetworkManager и просмотр файла

Вносим изменения в файл /etc/named.conf (рис. 11).

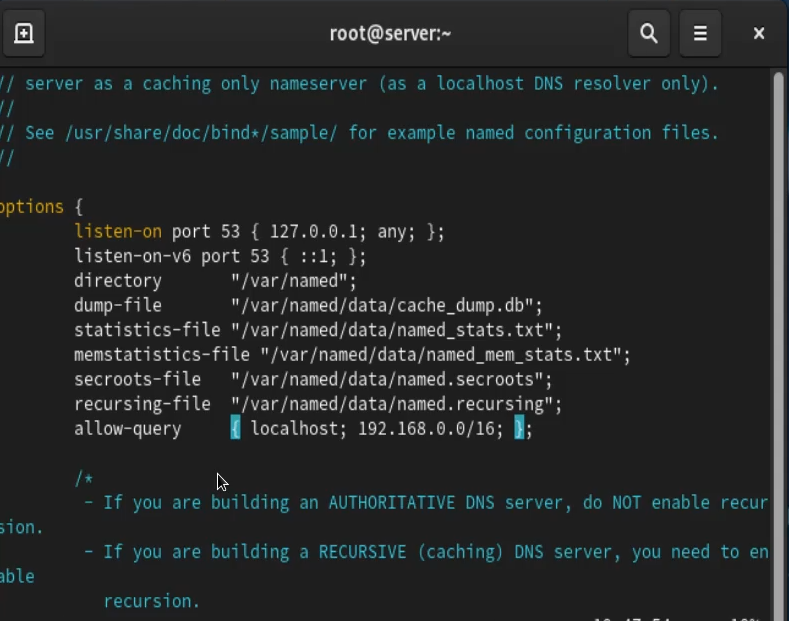


Рис. 11: Внесение изменений в файл /etc/named.conf

Вносим изменения в настройки межсетевого экрана узла server, разрешив работу с DNS. Убеждаемся, что DNS-запросы идут через узел server, который прослушивает порт 53 (рис. 12).

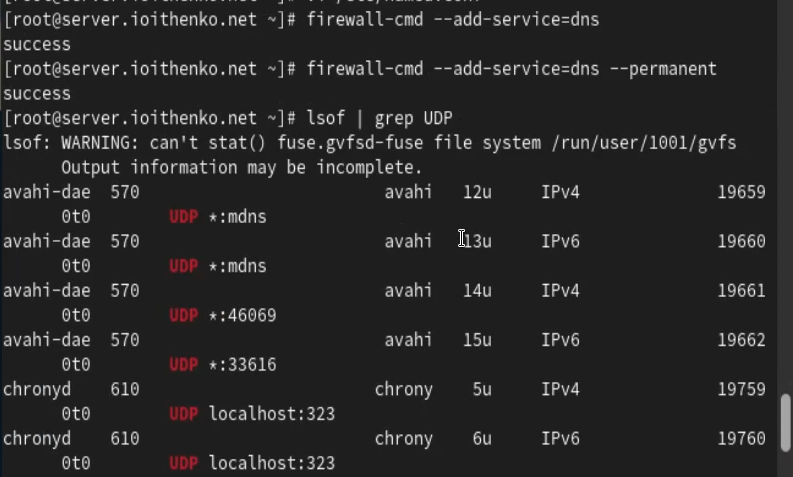


Рис. 12: Внесение изменений в настройки межсетевого экрана узла server, проверка

Для конфигурирования кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами вносим изменения в файл named.conf (рис. 13)

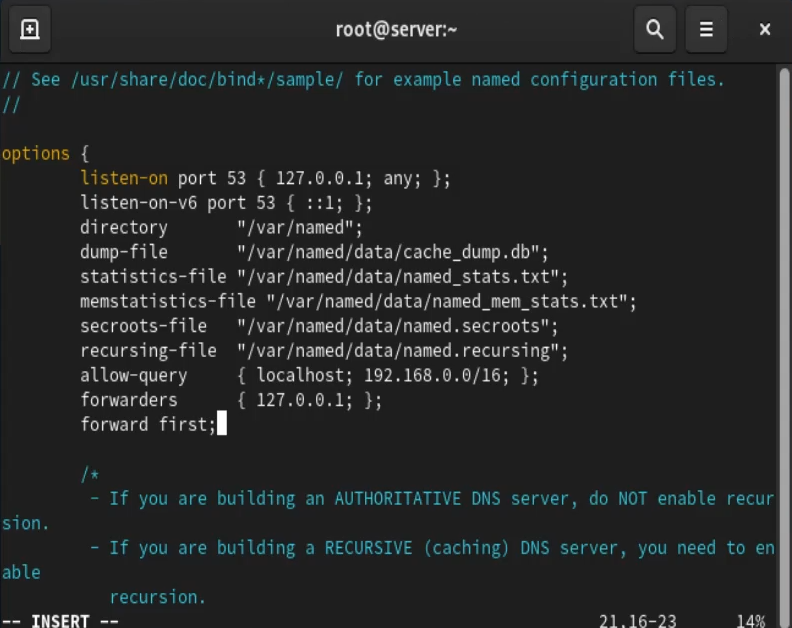


Рис. 13: Редактирование named.conf

Вводим команды(рис. 14): cp /etc/named.rfc1912.zones /etc/named/ cd /etc/named mv /etc/named/named.rfc1912.zones /etc/named/ioithenko.net

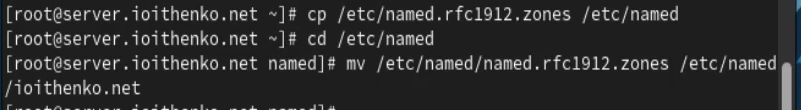


Рис. 14: Команды

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

Редактируем файл /etc/named/ioithenko.net (рис. 15)

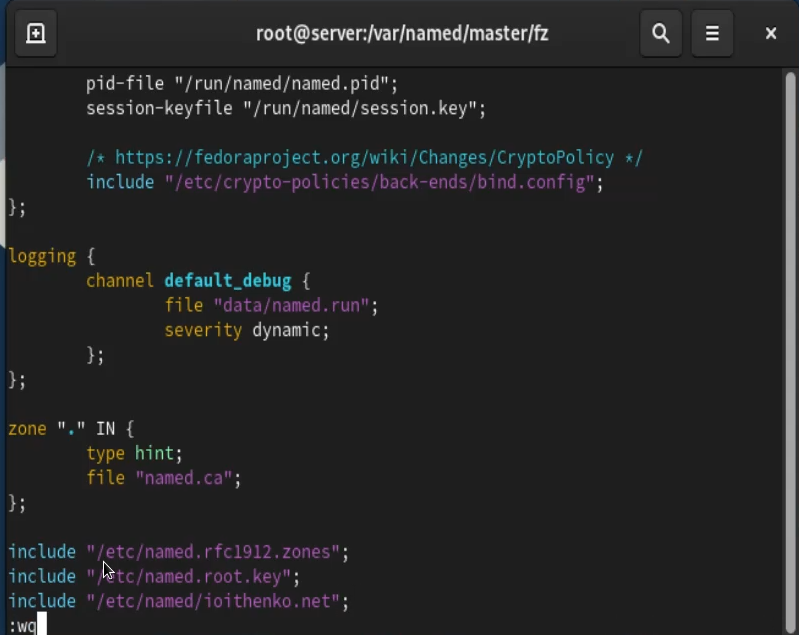


Рис. 15: Редактирование файла /etc/named/ioithenko.net

В каталоге /var/named создаем подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно. Копируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz, переименовав его в ioithenko.net (рис. 16).

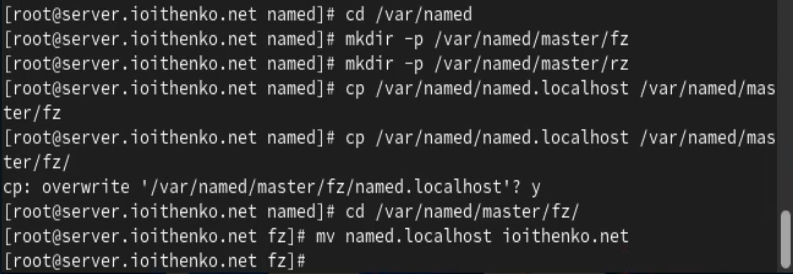


Рис. 16: Создание каталогов, копирование шаблона прямой зоны, переименование

Изменяем файл /var/named/master/fz/ioithenko.net (рис. 17).

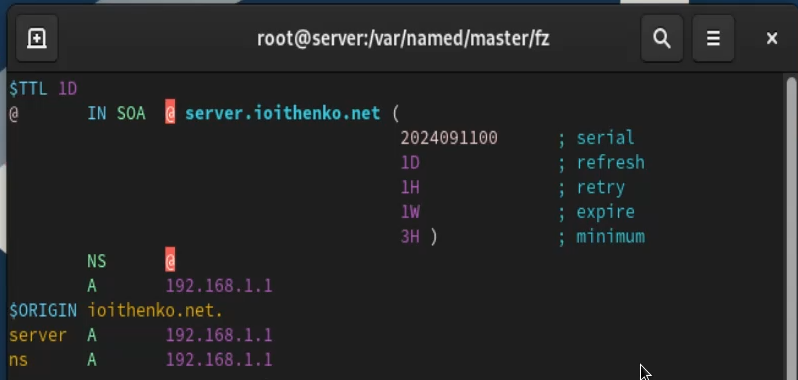


Рис. 17: Редактирование /var/named/master/fz/ioithenko.net

Копируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуйте его в 192.168.1 (рис. 18).

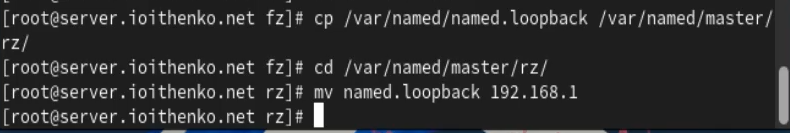


Рис. 18: Копирование шаблона обратной зоны, переименование

Изменяем файл /var/named/master/rz/192.168.1 (рис. 19).

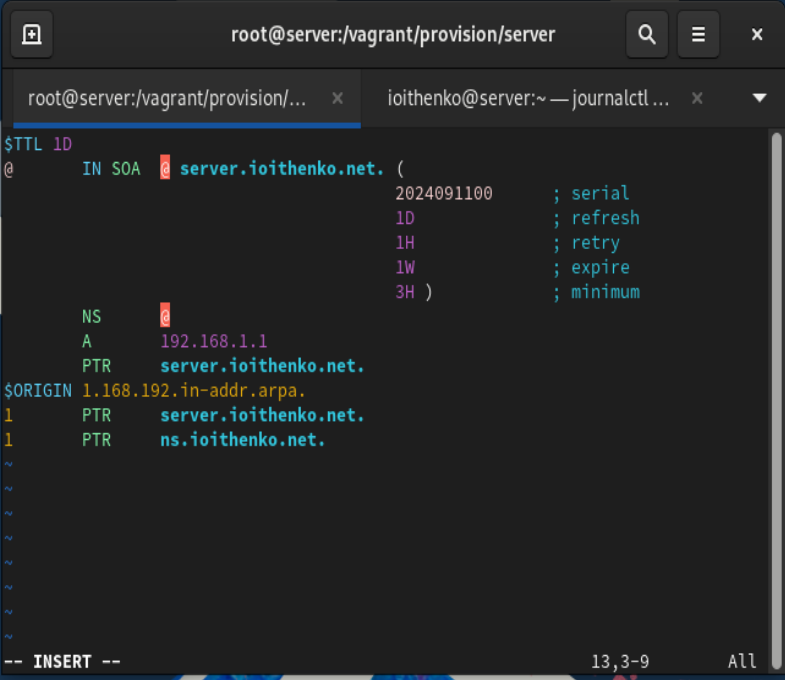


Рис. 19: Редактирование /var/named/master/rz/192.168.1

Изменяем права доступа, восстанавливаем метки SELinux, проверяем (рис. 20).

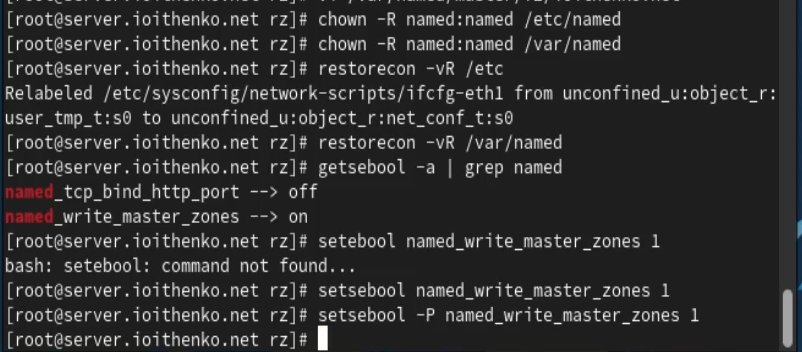


Рис. 20: Изменение прав доступа, восстановление меток SELinux, проверка

Во втором терминале открываем лог системных сообщений. В первом терминале перезапускаем DNS-сервер. После исправления всех ошибок и опечаток DNS-сервер запускается успешно. При помощи утилиты dig получаем описание DNS-зоны с сервера ns.ioithenko.net (рис. 21).

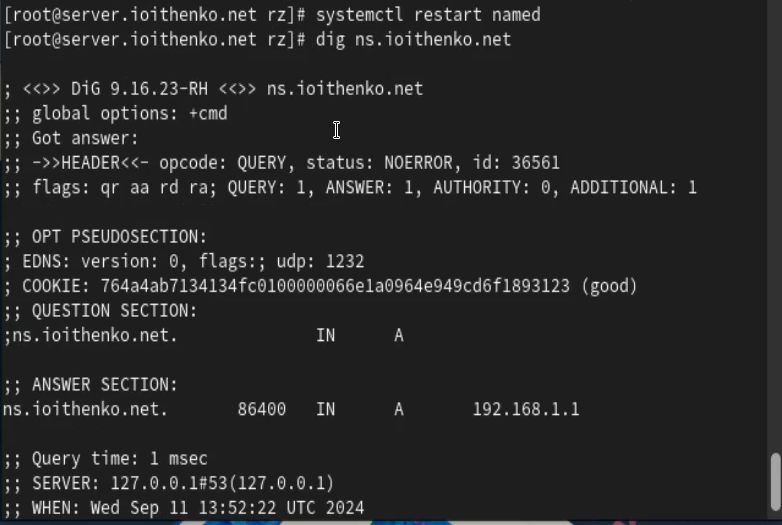


Рис. 21: Описание DNS-зоны с сервера ns.ioithenko.net

Анализируем корректность работы DNS-сервера (рис. 22), (рис. 23), (рис. 24).

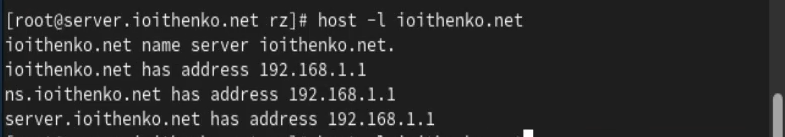


Рис. 22: Анализ корректности работы DNS-сервера

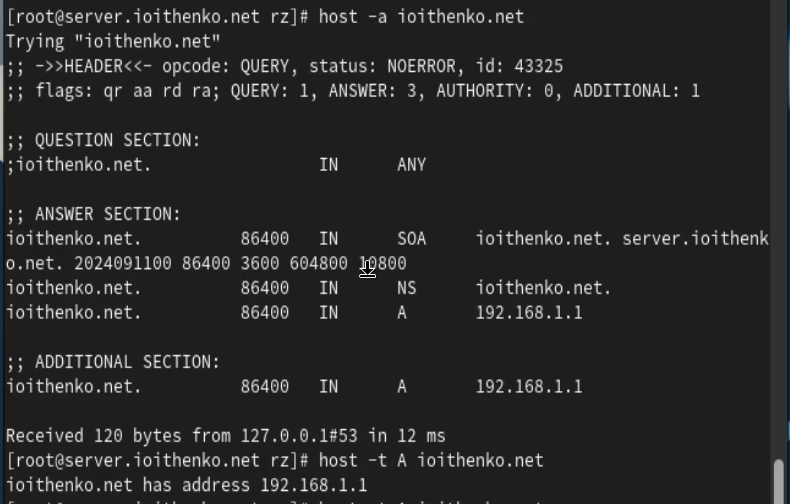


Рис. 23: Анализ корректности работы DNS-сервера

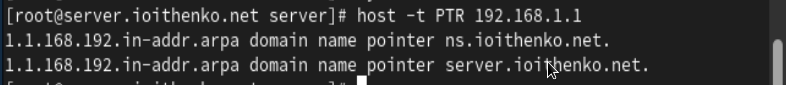


Рис. 24: Анализ корректности работы DNS-сервера

Переходим в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаем в нём каталог dns, в который помещаем в соответствующие каталоги конфигурационные файлы DNS (рис. 25).

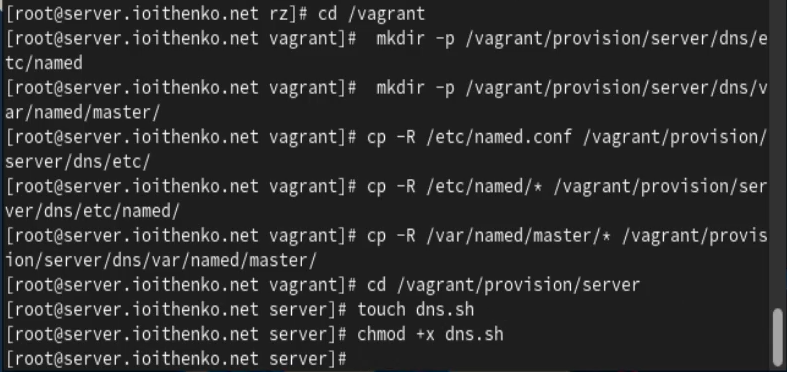


Рис. 25: Размещение конфигурационных файлов в каталог /vagrant/provision/server/dns

Создаем скрипт dns.sh (рис. 26).

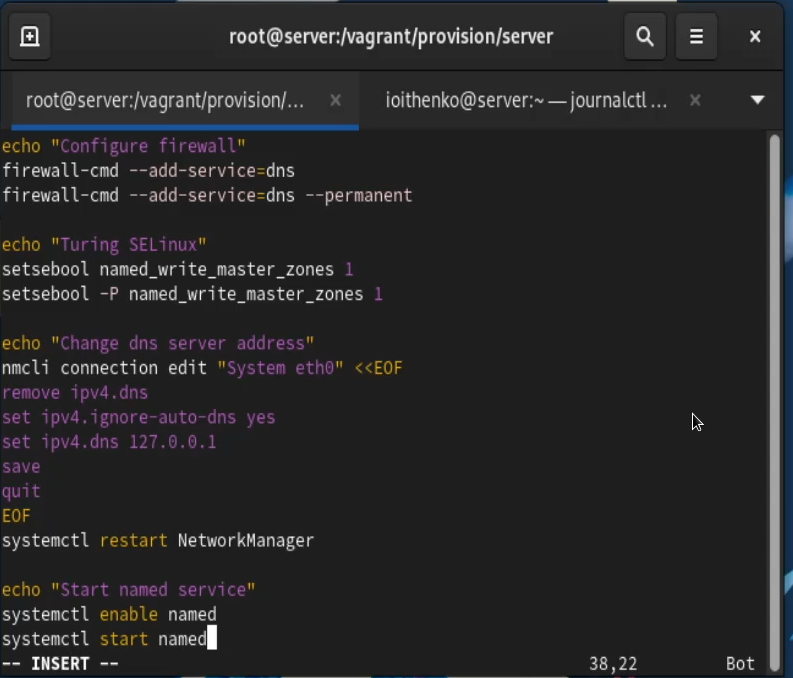


Рис. 26: Редактирование скрипта dns.sh

Для отработки созданного скрипта во время загрузки виртуальной машины в конфигурационном файле Vagrantfile вносим изменения в разделе конфигурации для сервера (рис. 27).



Рис. 27: Редактирование Vagrantfile

# 3 Выводы

В ходе лабораторной работы я приобрела практические навыки по установке и конфигурированию DNSсервера, усвоила принципы работы системы доменных имён.

# 4 Ответы на контрольные вопросы

1. Что такое DNS?

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?

Задача сервера - 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?

Использовать опции -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?

Использовать 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>.