**РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ**

**Факультет физико-математических и естественных наук**

**Кафедра теории вероятностей и кибербезопасности**

**ОТЧЁТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ №2**

*дисциплина: Администрирование сетевых подсистем*

Студент: Махорин Иван Сергеевич

Студ. билет № 1032211221

Группа: НПИбд-02-21

**МОСКВА**

2023 г.

# Цель работы:

# Целью данной работы является приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

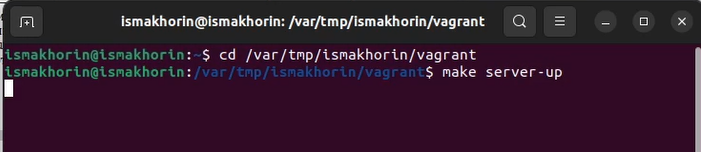
**Выполнение работы:**

Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

cd /var/tmp/ismakhorin/vagrant

Далее запустим виртуальную машину server (Рис. 1.1):

make server-up

****

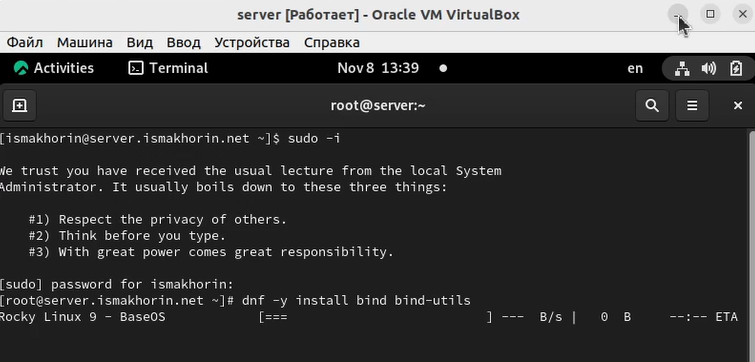
**Рис. 1.1.** Открытие рабочего каталога с проектом и запуск виртуальной машины server.

На виртуальной машине server войдём под созданным нами в предыдущей работе пользователем и откройте терминал. Перейдём в режим суперпользователя:

sudo -i

И установим bind и bind-utils (Рис. 1.2):

dnf -y install bind bind-utils

****

**Рис. 1.2.** Переход в режим суперпользователя и установка bind,bind-utils.

С помощью утилиты dig сделаем запрос к DNSадресу www.yandex.ru (Рис. 1.3):

dig www.yandex.ru

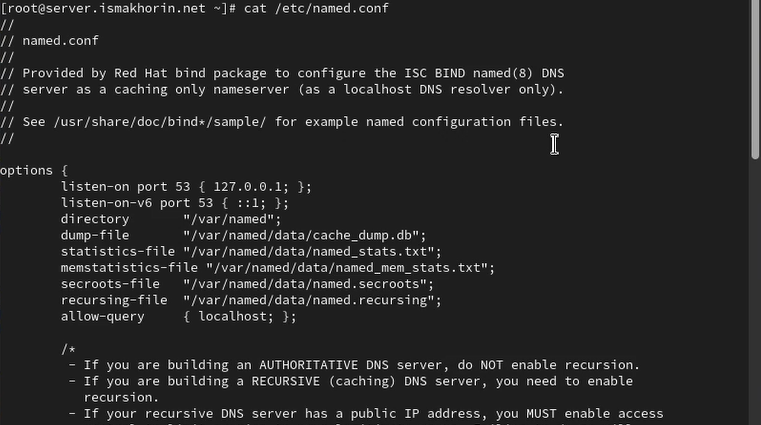
****

**Рис. 1.3.** Запрос с помощью утилиты dig.

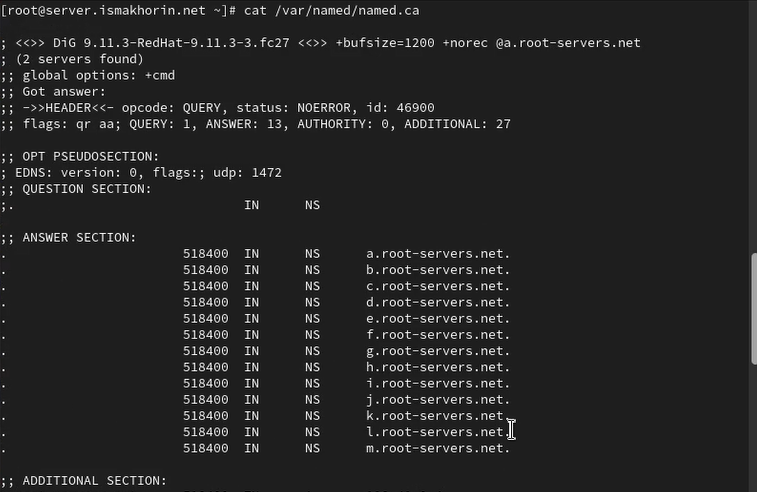
Просмотрим содержание файлов /etc/resolv.conf (Рис. 2.1), /etc/named.conf (Рис. 2.2), /var/named/named.ca (Рис. 2.3), /var/named/named.localhost (Рис. 2.4), /var/named/named.loopback (Рис. 2.5).

****

**Рис. 2.1.** Просмотр содержания файла /etc/resolv.conf.

****

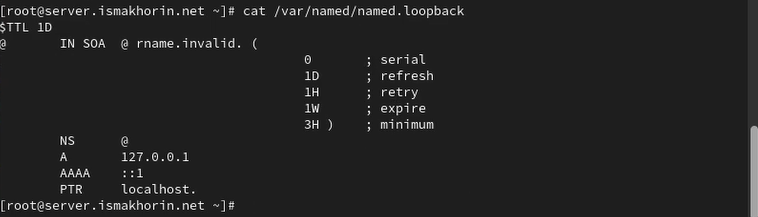
**Рис. 2.2.** Просмотр содержания файла /etc/named.conf.

****

**Рис. 2.3.** Просмотр содержания файла /var/named/named.ca.

****

**Рис. 2.4.** Просмотр содержания файла /var/named/named.localhost.

****

**Рис. 2.5.** Просмотр содержания файла /var/named/named.loopback.

Запустим DNS-сервер:

systemctl start named

Включим запуск DNS-сервера в автозапуск при загрузке системы:

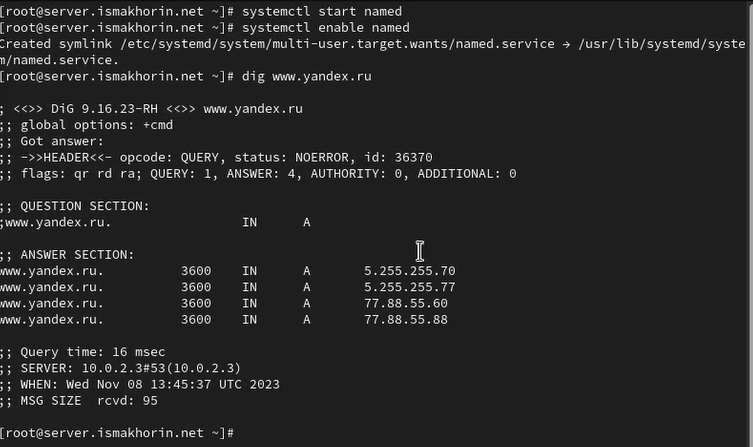
systemctl enable named

Проанализируем отличие в выведенной на экран информации при выполнении команд:

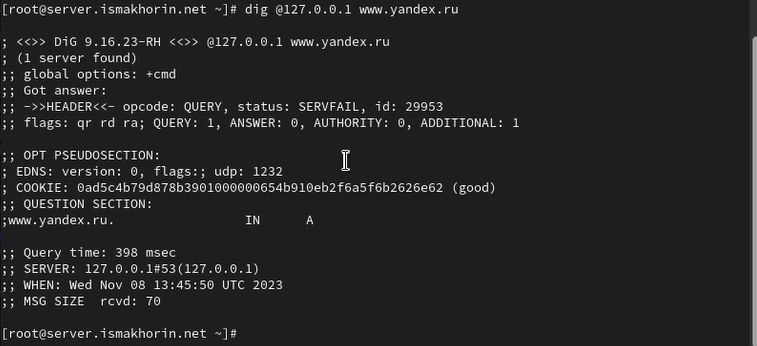
dig www.yandex.ru (Рис. 2.6)

и

dig @127.0.0.1 www.yandex.ru (Рис. 2.7)

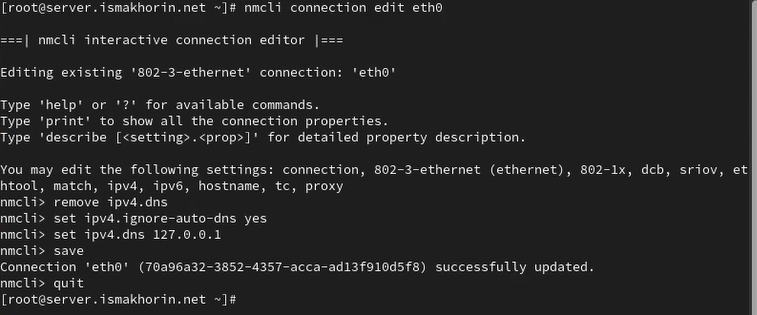
****

**Рис. 2.6.** Запуск DNS-сервера, включение запуска DNS-сервера в автозапуск при загрузке системы, анализ выведенной на экран информации при выполнении команды dig www.yandex.ru.

****

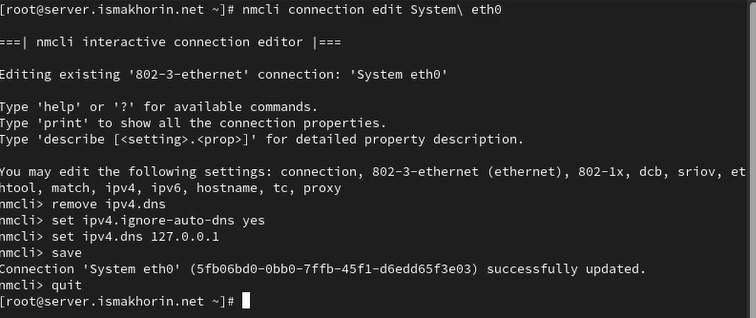
**Рис. 2.7.** Анализ выведенной на экран информации при выполнении команды dig @127.0.0.1 www.yandex.ru.

Сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого 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 127.0.0.1 (рис. 2.8):

****

**Рис. 2.8.** Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети.

Сделаем тоже самое для соединения System eth0 (рис. 2.9):

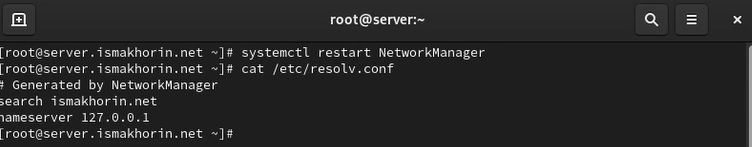
****

**Рис. 2.9.** Повторяем действия для соединения System eth0.

Перезапустим NetworkManager:

systemctl restart NetworkManager

Проверим наличие изменений в файле /etc/resolv.conf (рис. 2.10):

****

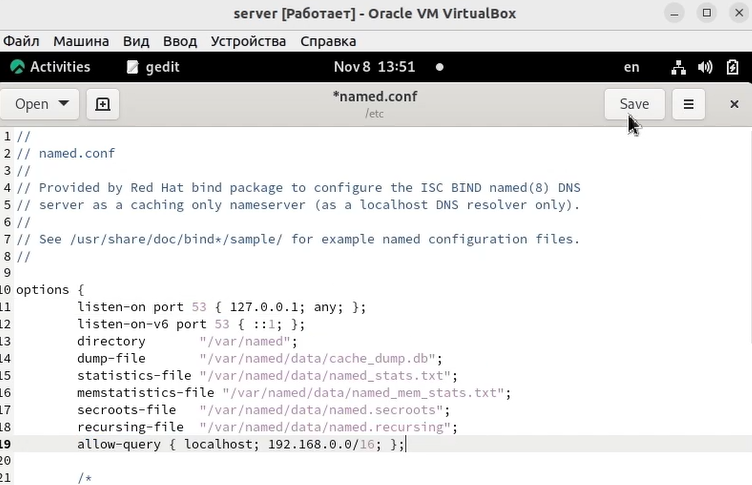
**Рис. 2.10.** Перезапуск NetworkManager и проверка наличия изменений в файле /etc/resolv.conf.

Теперь нам требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server (рис. 2.11). Для этого внесём изменения в файл /etc/named.conf, заменив строку

listen-on port 53 { 127.0.0.1; }; на listen-on port 53 { 127.0.0.1; any; };

и строку

allow-query { localhost; }; на allow-query { localhost; 192.168.0.0/16; };

****

**Рис. 2.11.** Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server.

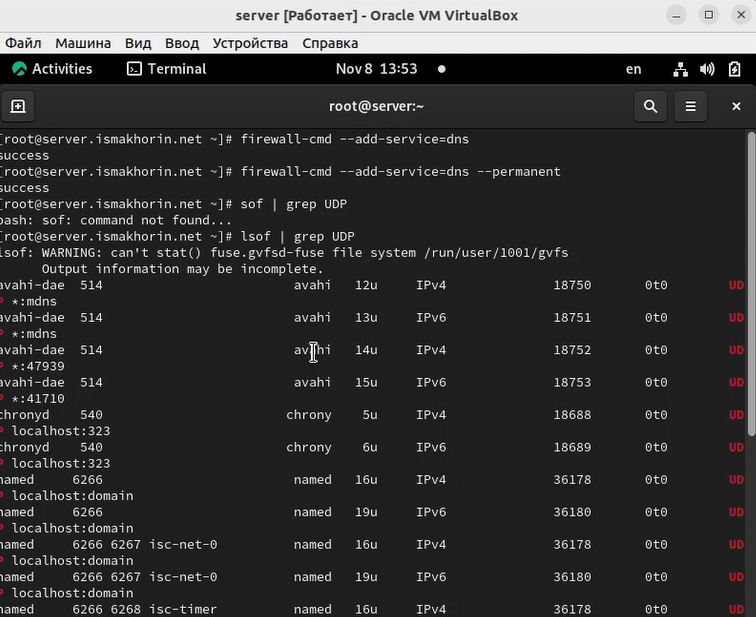
Внесём изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:

firewall-cmd --add-service=dns

firewall-cmd --add-service=dns --permanent

Убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используем команду lsof (рис. 2.12):

lsof | grep UDP

****

**Рис. 2.12.** Внос изменений в настройки межсетевого экрана узла server, разрешив работу с DNS. Проверка, что DNS-запросы идут через узел server, который прослушивает порт 53.

В случае возникновения в сети 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:

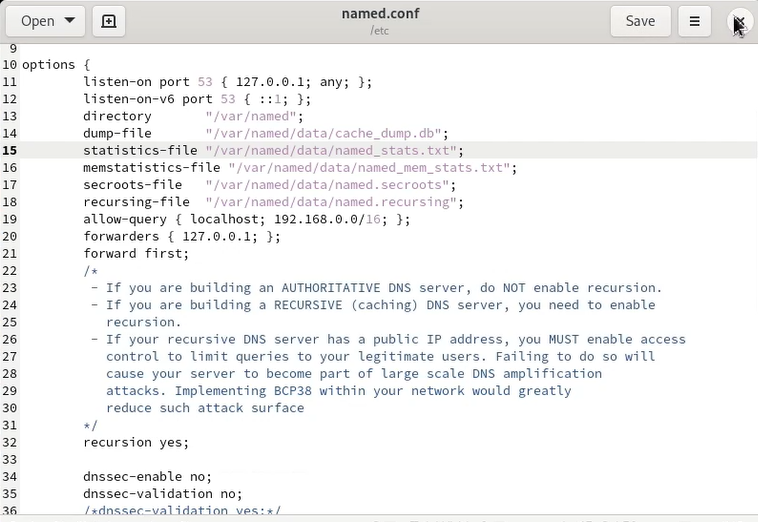
forwarders { список DNS-серверов };

forward first;

Кроме того, возможно вышестоящий DNS-сервер может не поддерживать технологию DNSSEC, тогда в конфигурационном файле named.conf укажем следующие настройки (рис. 3):

dnssec-enable no;

dnssec-validation no;

****

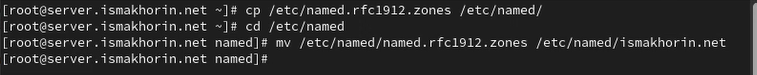
**Рис. 3.** Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек.

Скопируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуем его в ismakhorin.net (рис. 4.1):

cp /etc/named.rfc1912.zones /etc/named/

cd /etc/named

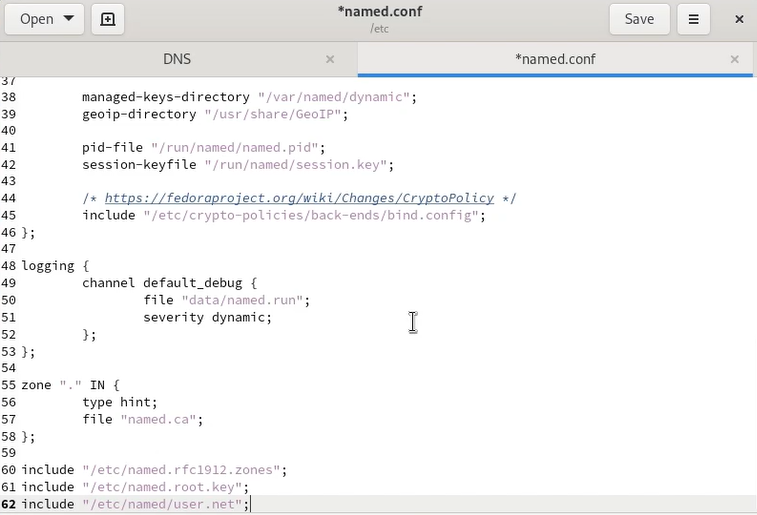
mv /etc/named/named.rfc1912.zones /etc/named/user.net

****

**Рис. 4.1.** Копирование шаблона описания DNS-зон из каталога /etc в каталог /etc/named и изменение его названия.

Включим файл описания зоны /etc/named/ismakhorin.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку (рис. 4.2):

include "/etc/named/ismakhorin.net"

****

**Рис. 4.2.** Включение файла описания зоны /etc/named/ismakhorin.net в конфигурационном файле DNS /etc/named.conf.

Откроем файл /etc/named/user.net на редактирование и вместо зоны пропишем свою прямую зону. Далее, вместо зоны пропишем свою обратную зону. Остальные записи в файле /etc/named/ismakhorin.net удалим (рис. 4.3):

****

**Рис. 4.3.** Открытие файла /etc/named/user.net на редактирование. Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле.

В каталоге /var/named создадим подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно (рис. 4.4):

cd /var/named

mkdir -p /var/named/master/fz

mkdir -p /var/named/master/rz

****

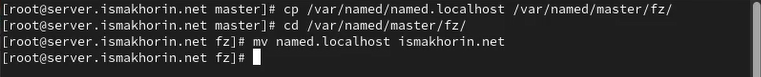
**Рис. 4.4.** В каталоге /var/named создание подкаталогов master/fz и master/rz.

Скопируем шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуем его в ismakhorin.net (рис. 4.5):

cp /var/named/named.localhost /var/named/master/fz/

cd /var/named/master/fz/

mv named.localhost ismakhorin.net

****

**Рис. 4.5.** Копирование шаблона прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и изменение его названия.

Изменим файл /var/named/master/fz/ismakhorin.net, указав необходимые DNS записи для прямой зоны. В этом файле DNS-имя сервера @ rname.invalid. заменим на @ server.ismakhorin.net. Формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии) [1]; адрес в A- заменим с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN зададим текущее имя домена ismakhorin.net, а затем укажем имена и адреса серверов в этом домене в виде A-записей DNS (на данном этапе пропишем сервер с именем ns и адресом 192.168.1.1) (рис. 4.6):

****

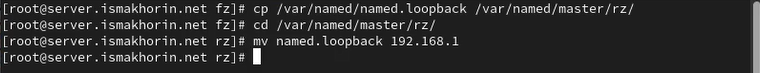
**Рис. 4.6.** Изменение файла /var/named/master/fz/ismakhorin.net, указав необходимые DNS записи для прямой зоны.

Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуем его в 192.168.1 (рис. 4.7):

cp /var/named/named.loopback /var/named/master/rz/

cd /var/named/master/rz/

mv named.loopback 192.168.1

****

**Рис. 4.7.** Копирование шаблона обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и изменение его названия.

Изменим файл /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны. В этом файле DNS-имя сервера @ rname.invalid заменим на @ server.ismakhorin.net. формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в A-записи заменим с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN зададим название обратной зоны в виде 1.168.192.in-addr.arpa., затем зададим PTR-записи (на данном этапе зададим PTR запись, ставящая в соответствие адресу 192.168.1.1 DNS-адрес ns.ismakhorin.net) (рис. 4.8):

****

**Рис. 4.8.** Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны.

Далее исправим права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать:

chown -R named:named /etc/named

chown -R named:named /var/named

В системах с запущенным SELinux все процессы и файлы имеют специальные метки безопасности (так называемый «контекст безопасности»), используемые системой для принятия решений по доступу к этим процессам и файлам. После изменения доступа к конфигурационным файлам named требуется корректно восстановить их метки в SELinux:

restorecon -vR /etc

restorecon -vR /var/named

Для проверки состояния переключателей SELinux, относящихся к named, введём:

getsebool -a | grep named

Теперь дадим named разрешение на запись в файлы DNS-зоны:

setsebool named\_write\_master\_zones 1

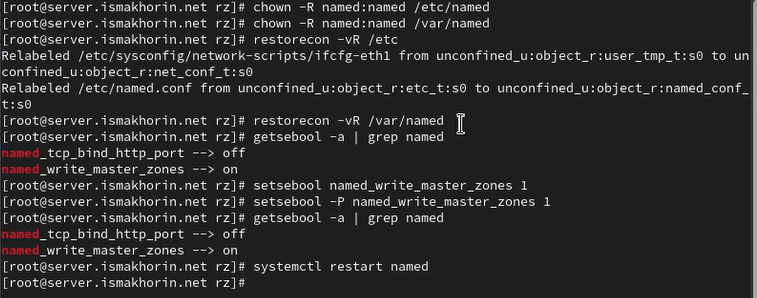
setsebool -P named\_write\_master\_zones 1

В дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы (рис. 4.10):

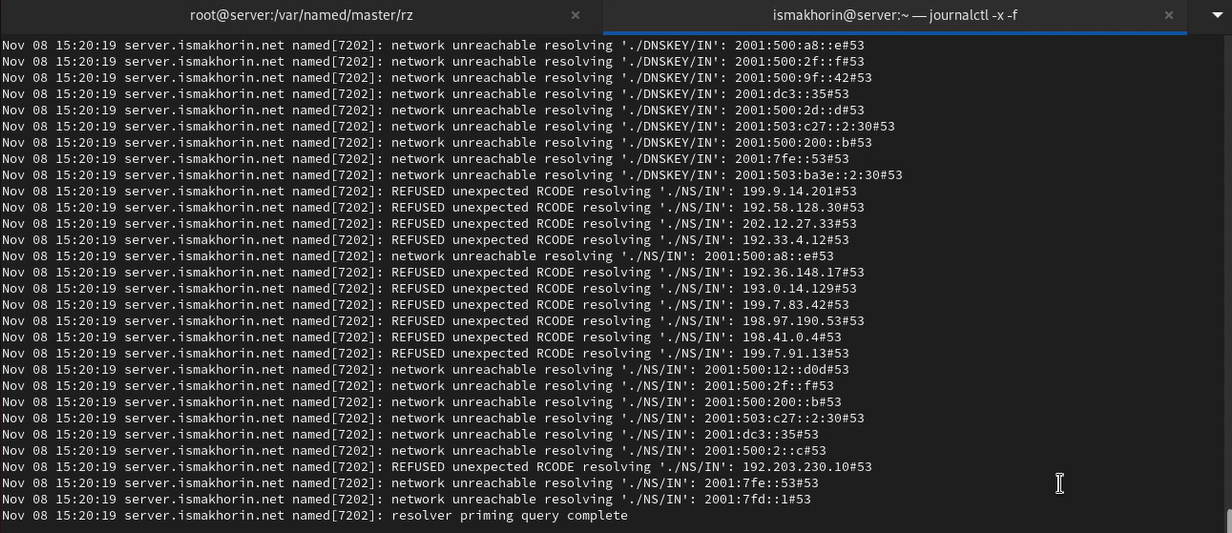
journalctl -x -f

и в первом терминале перезапустим DNS-сервер (рис. 4.9):

systemctl restart named

****

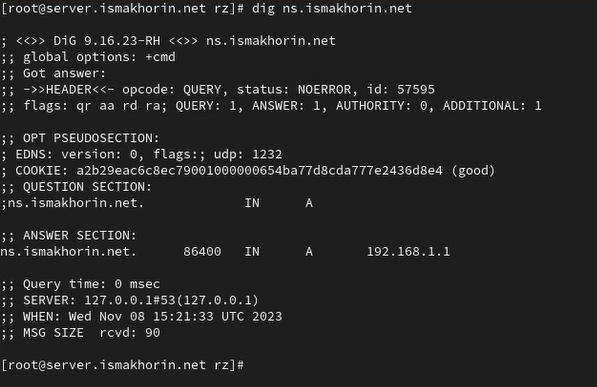
**Рис. 4.9.** Исправление прав доступа к файлам в каталогах /etc/named и /var/named, корректное восстановление их меток в SELinux, проверка состояния переключателей SELinux и перезапуск DNS-сервера.

****

**Рис. 4.10.** Проверка корректности работы системы.

При помощи утилиты dig получим описание DNS-зоны с сервера ns.ismakhorin.net (рис. 5.1):

dig ns.user.net

****

**Рис. 5.1.** Получение описания DNS-зоны с сервера ns.ismakhorin.net.

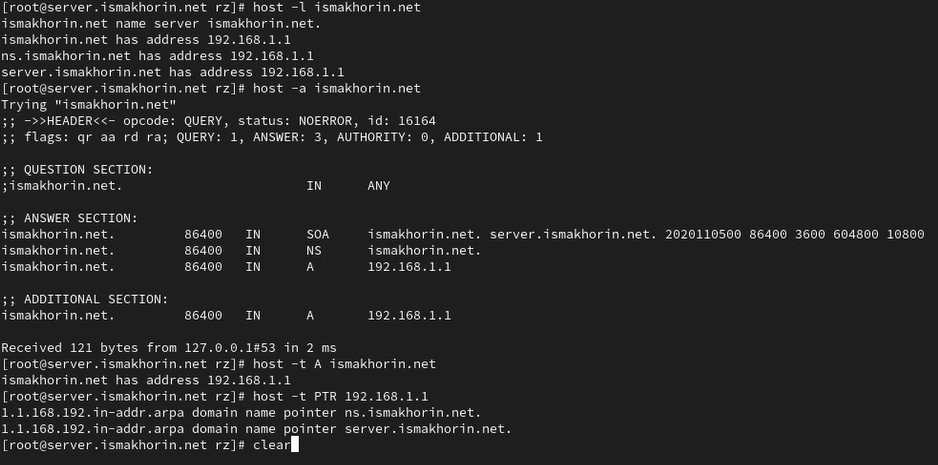
При помощи утилиты host проанализируем корректность работы DNS-сервера (рис. 5.2):

host -l ismakhorin.net

host -a ismakhorin.net

host -t A ismakhorin.net

host -t PTR 192.168.1.1

****

**Рис. 5.2.** Анализ корректности работы DNS-сервера.

На виртуальной машине server перейдём в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создадим в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS (рис. 6.1):

cd /vagrant

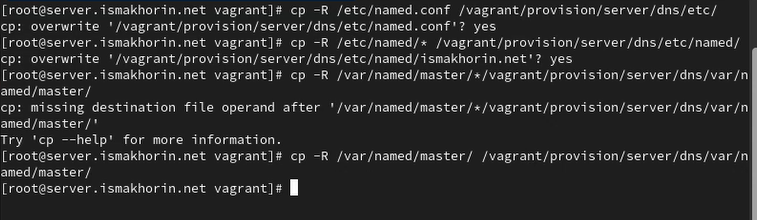
mkdir -p /vagrant/provision/server/dns/etc/named

mkdir -p /vagrant/provision/server/dns/var/named/master/

cp -R /etc/named.conf /vagrant/provision/server/dns/etc/

cp -R /etc/named/\* /vagrant/provision/server/dns/etc/named/

cp -R /var/named/master/\* /vagrant/provision/server/dns/var/named/master/

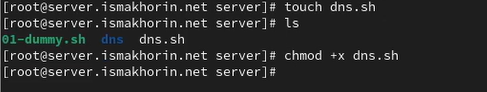
****

**Рис. 6.1.** Переход в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога dns, в который помещаем в соответствующие каталоги конфигурационные файлы DNS.

В каталоге /vagrant/provision/server создадим исполняемый файл dns.sh (рис. 6.2):

touch dns.sh

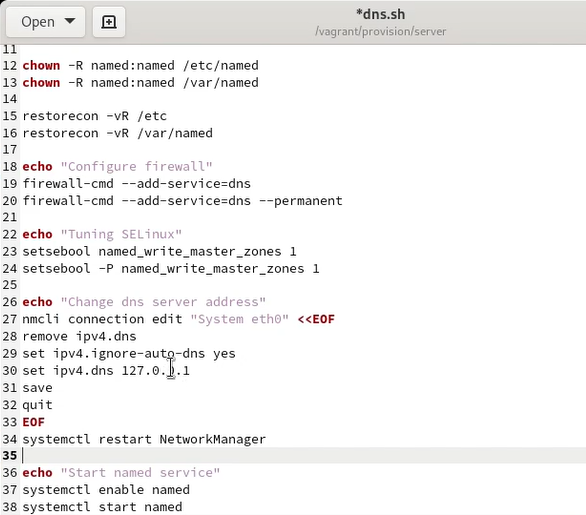
chmod +x dns.sh

****

**Рис. 6.2.** Создание в каталоге /vagrant/provision/server исполняемого файла dns.sh.

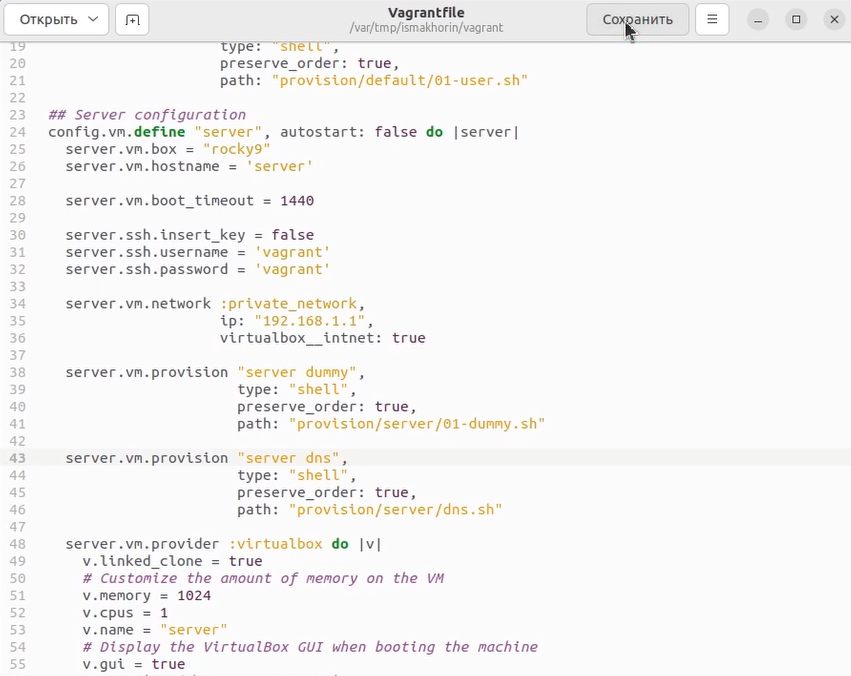
Откроем его на редактирование и пропишем в нём следующий скрипт (приведён в лабораторной работе). Этот скрипт, по сути, повторяет произведённые нами действия по установке и настройке DNS-сервера (рис. 6.3):

1. подставляет в нужные каталоги подготовленные вами конфигурационные файлы;
2. меняет соответствующим образом права доступа, метки безопасности SELinux и правила межсетевого экрана;
3. настраивает сетевое соединение так, чтобы сервер выступал DNS-сервером по умолчанию для узлов внутренней виртуальной сети;
4. запускает DNS-сервер;

****

**Рис. 6.3.** Открытие файла на редактирование и прописывание в нём скрипта.

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile добавим определённые параметры в разделе конфигурации для сервера (рис. 6.4):

****

**Рис. 6.4.** Добавление параметров в конфигурационном файле Vagrantfile в разделе конфигурации для сервера.

**Вывод:**

# В ходе выполнения лабораторной работы были приобретены практические навыки по установке и конфигурированию DNS-сервера, а также усвоили принципы работы системы доменных имён.

**Ответы на контрольные вопросы:**

1. Что такое DNS? - Это система, предназначенная для преобразования человекочитаемых доменных имен в IP-адреса, используемые компьютерами для идентификации друг друга в сети.
2. 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.
3. 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.
4. 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.
5. Что указывается в файле resolv.conf? - Содержит информацию о DNS-серверах, используемых системой, а также о параметрах конфигурации.
6. 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).
7. Для чего используется домен in-addr.arpa? - Используется для обратного маппинга IP-адресов в доменные имена.
8. Для чего нужен демон named? - Это DNS-сервер, реализация BIND (Berkeley Internet Name Domain).
9. В чём заключаются основные функции slave-сервера и master-сервера? - Master-сервер хранит оригинальные записи зоны, slave-серверы получают копии данных от master-сервера.
10. Какие параметры отвечают за время обновления зоны? - refresh, retry, expire, и minimum.
11. Как обеспечить защиту зоны от скачивания и просмотра? - Это может включать в себя использование TSIG (Transaction SIGnatures) для аутентификации между серверами.
12. Какая запись RR применяется при создании почтовых серверов? - MX (Mail Exchange).
13. Как протестировать работу сервера доменных имён? - Используйте команды nslookup, dig, или host.
14. Как запустить, перезапустить или остановить какую-либо службу в системе? - systemctl start|stop|restart <service>.
15. Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы? - Используйте опции, такие как -d или -v при запуске службы.
16. Где храниться отладочная информация по работе системы и служб? Как её посмотреть? - В системных журналах, доступных через journalctl.
17. Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров. - lsof -p <pid> или fuser -v <file>.
18. Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli. - Примеры включают nmcli connection up|down <connection\_name>.
19. Что такое SELinux? - Это мандатный контроль доступа для ядра Linux.
20. Что такое контекст (метка) SELinux? - Метка, определяющая, какие ресурсы могут быть доступны процессу или объекту.
21. Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы? - restorecon -Rv <directory>.
22. Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций? - Используйте audit2allow.
23. Что такое булевый переключатель в SELinux? - Это параметр, который включает или отключает определенные аспекты защиты SELinux.
24. Как посмотреть список переключателей SELinux и их состояние? - getsebool -a.
25. Как изменить значение переключателя SELinux? - setsebool -P <boolean\_name> <on|off>.