РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 2

**Настройка DNS-сервера**

Дисциплина: Сетевые технологии

Студент: Карташова А.С.

Группа: НФИбд-03-18

**МОСКВА**

2020 г.

Оглавление

[Цель работы 2](#_Toc61129245)

[Задачи 2](#_Toc61129246)

[Ход работы 2](#_Toc61129247)

[Установка DNS-сервера 3](#_Toc61129248)

[Конфигурирование кэширующего DNS-сервера 3](#_Toc61129249)

[Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами 3](#_Toc61129250)

[Конфигурирование первичного DNS-сервера 7](#_Toc61129251)

[Анализ работы DNS-сервера 11](#_Toc61129252)

[Внесение изменений в настройки внутреннего окружения виртуальной машины 12](#_Toc61129253)

[Заключение 13](#_Toc61129254)

[Контрольные вопросы 13](#_Toc61129255)

# Цель работы

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

# Задачи

1. Установить на виртуальной машине server DNS-сервер bind и bind-utils
2. Сконфигурировать на виртуальной машине server кэширующий DNS-сервер
3. Сконфигурировать на виртуальной машине server первичный DNS-сервер
4. При помощи утилит dig и host проанализировать работу DNS-сервера
5. Написать скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server.

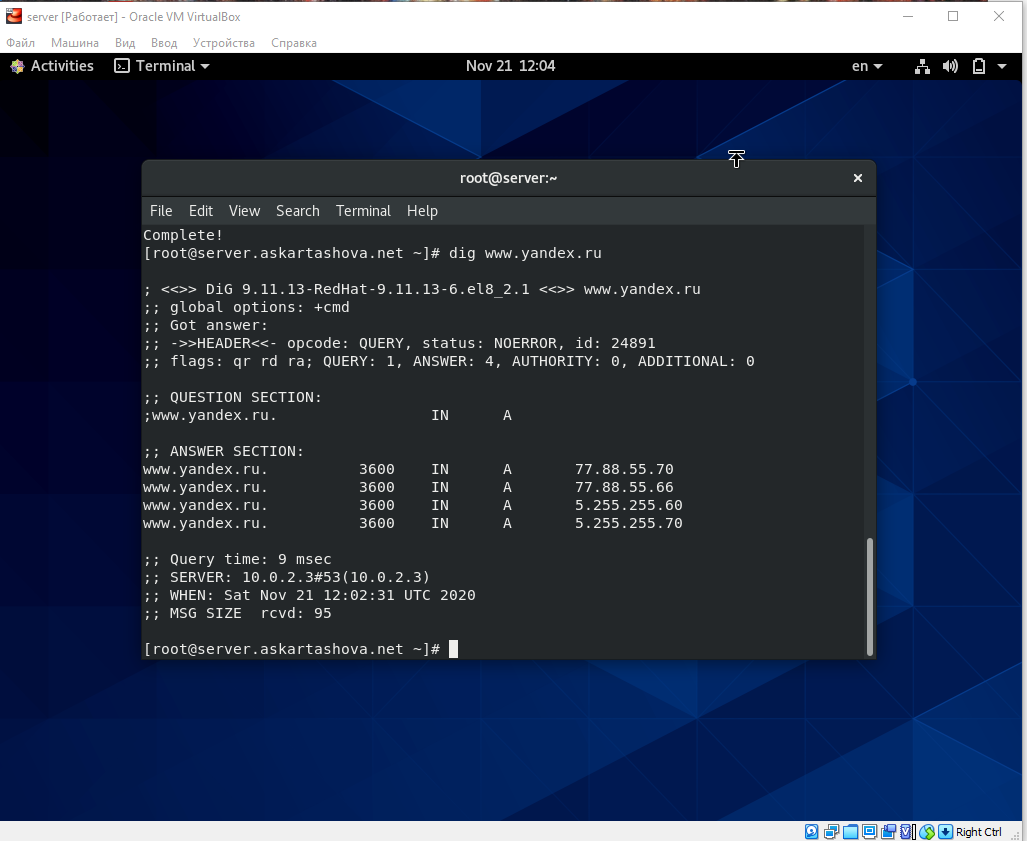
# Ход работы

## Установка DNS-сервера

На виртуальной машине server войдем под созданным вами в предыдущей работе пользователем и откроем терминал. Перейдем в режим суперпользователя. Установим bind и bind-utils:

С помощью утилиты dig сделаем запрос к DNS-адресу www.yandex.ru:

dig www.yandex.ru



- HEADER (заголовок): показывает версию dig, глобальные опции используемые с командой и другую доп.информацию

- QUESTION SECTION (секция запроса): Показывает наш запрос (мы запросили показать A-запись для домена ya.ru)

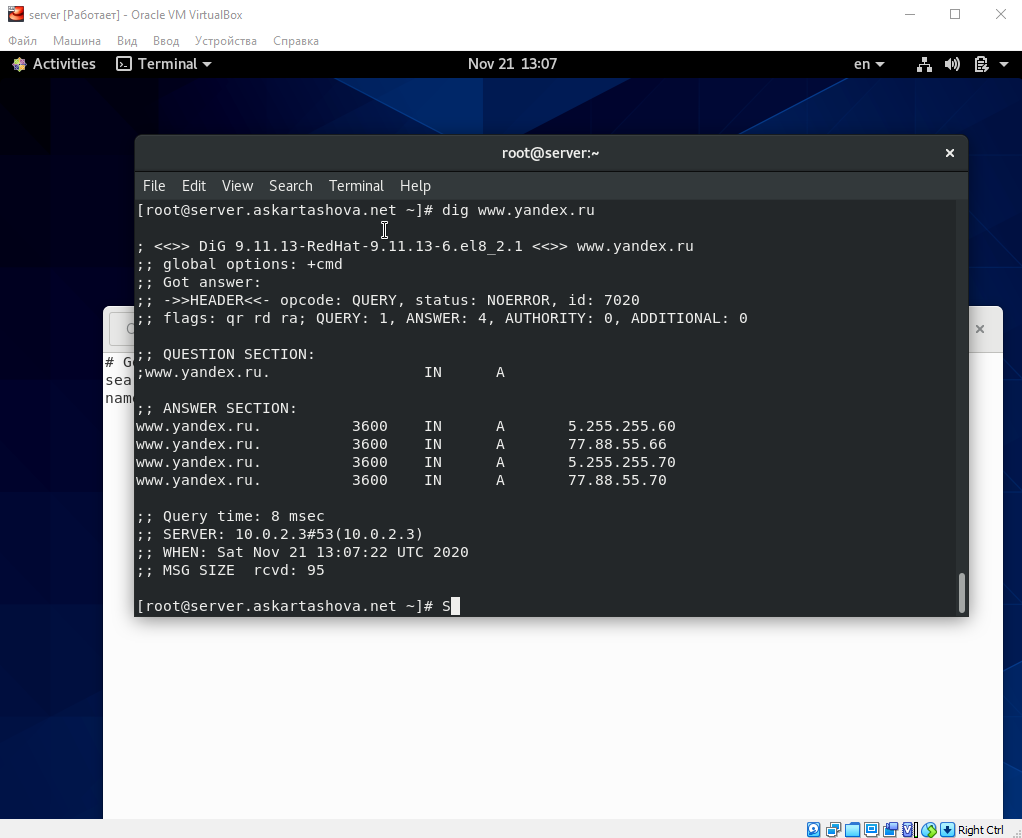
- ANSWER SECTION (секция ответа): показывает ответ полученный от DNS, в нашем случае показывает адреса для ya.ru

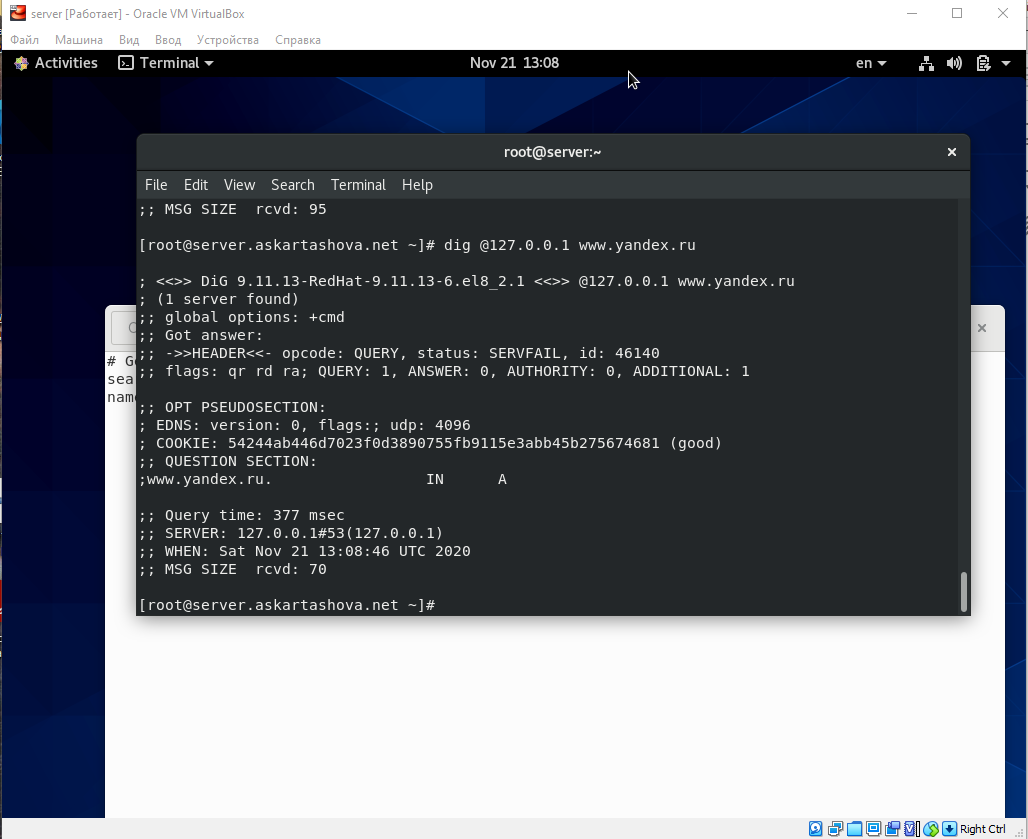
## Конфигурирование кэширующего DNS-сервера

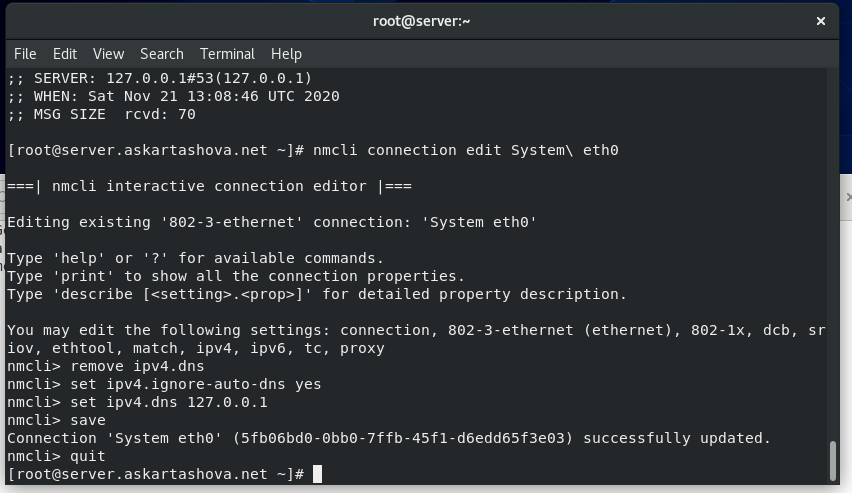
### Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

Запустим DNS-сервер и включим запуск DNS-сервера в автозапуск при загрузке системы:

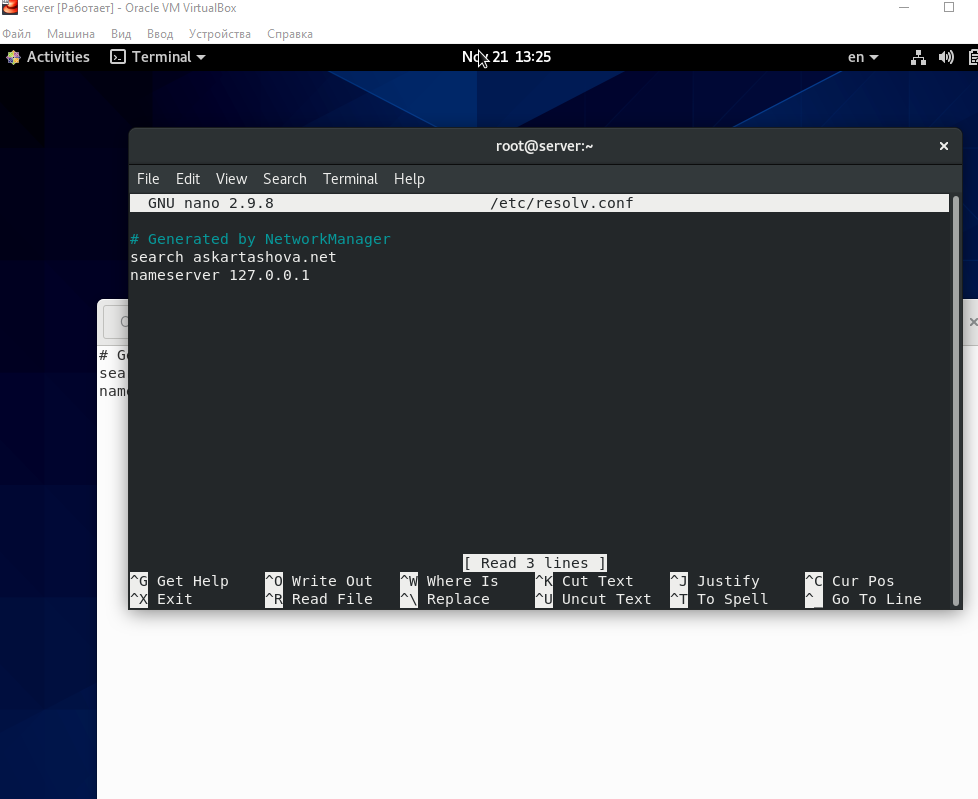
*systemctl enable named*

 При выполнении команды *dig* [*www.yandex.ru*](http://www.yandex.ru)выводятся те же ip-адресса *. dig @127.0.0.1* [*www.yandex.ru*](http://www.yandex.ru)не выводит ответ



Сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети.

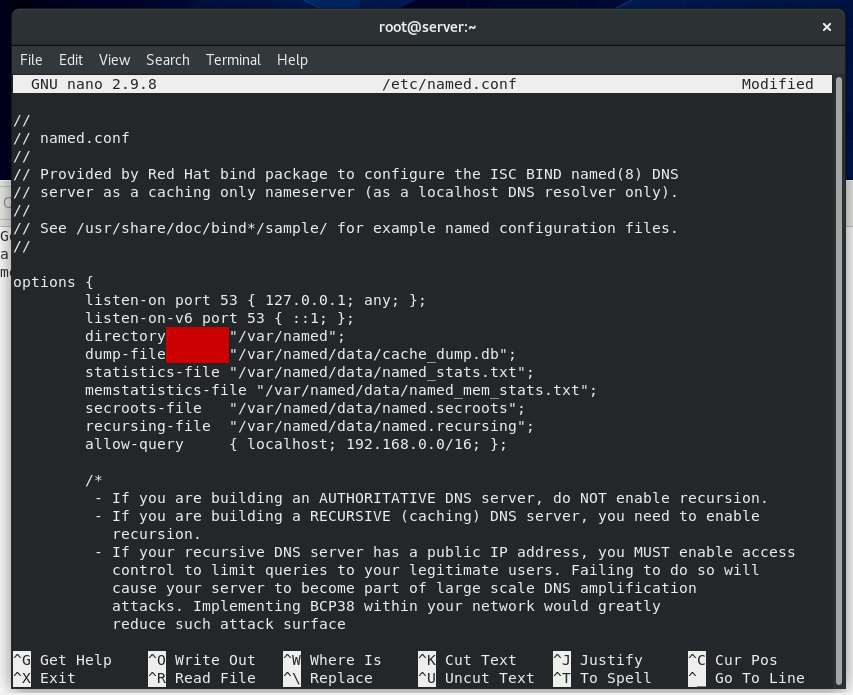
Перезапустим NetworkManager и проверим наличие изменений в файле /etc/resolv.conf.



Настроим направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесем изменения в файл /etc/named.conf, заменив строку

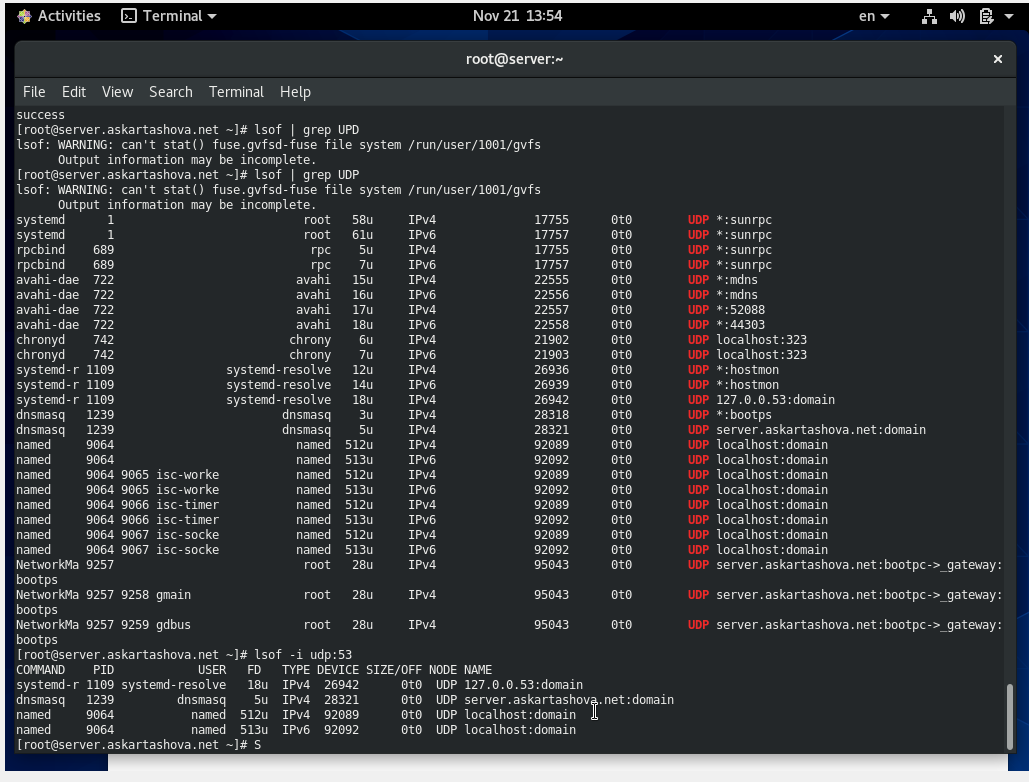
*listen-on port 53 { 127.0.0.1; }*; на *listen-on port 53 { 127.0.0.1; any; };*

и строку *allow-query { localhost; };* на *allow-query { localhost; 192.168.0.0/16; };*



Внесем изменения в настройки межсетевого экрана узла server, разрешив работу с DNS.

Убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этоо используем команду lsof:

*lsof | grep UDP*

## Конфигурирование первичного DNS-сервера

Скопируем шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуйте его в user.net

Включим файл описания зоны /etc/named/user.net в конфигурационном файле

DNS /etc/named.conf, добавив в нём в конце строку:

*include "/etc/named/user.net";*

Откройте файл /etc/named/user.net на редактирование и вместо пропишем свою прямую зону:

zone "user.net" IN {

type master;

file "master/fz/user.net";

allow-update { none; };

};

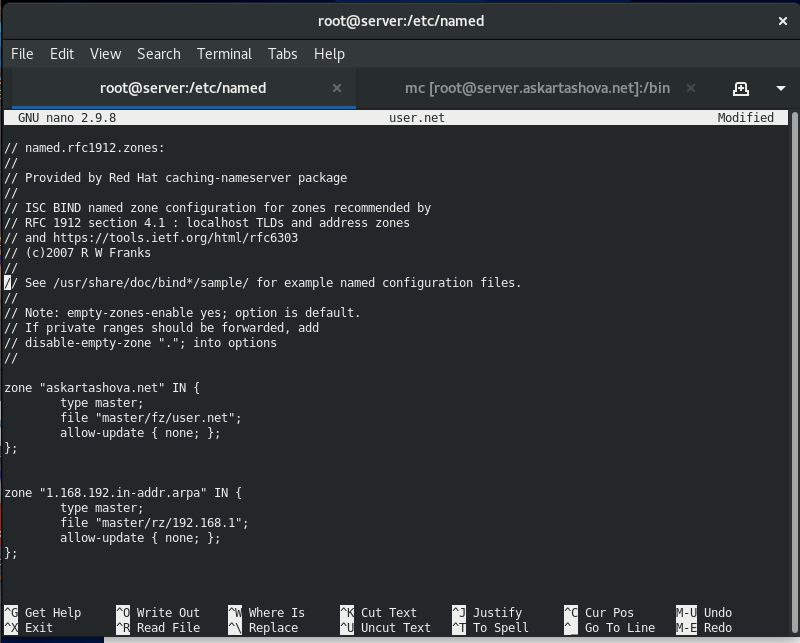
И свою обратную зону:

zone "1.168.192.in-addr.arpa" IN {

type master;

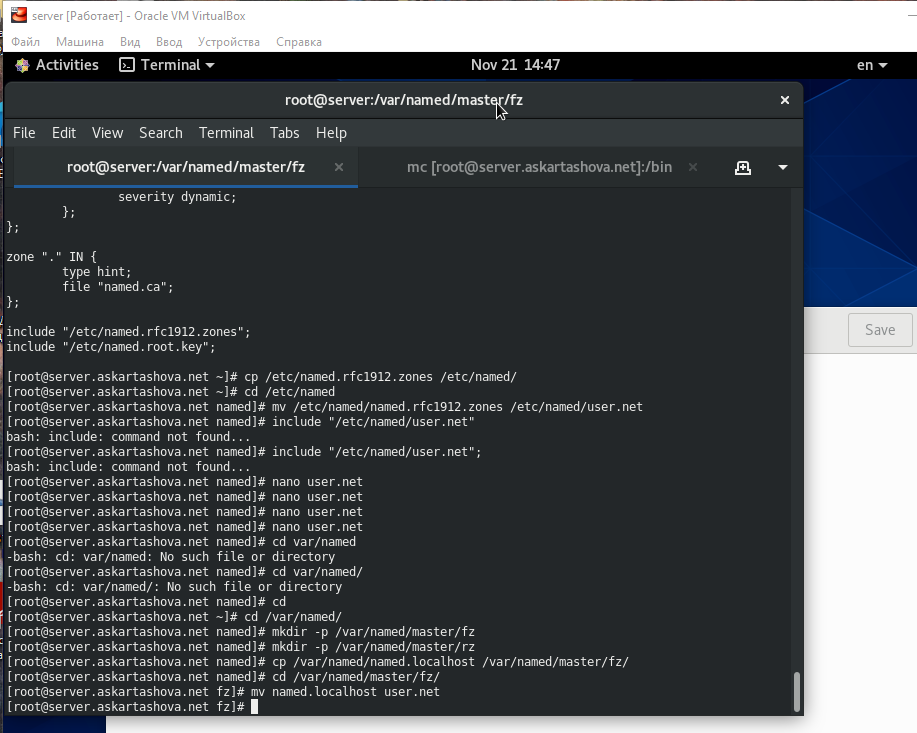
file "master/rz/192.168.1";

allow-update { none; };

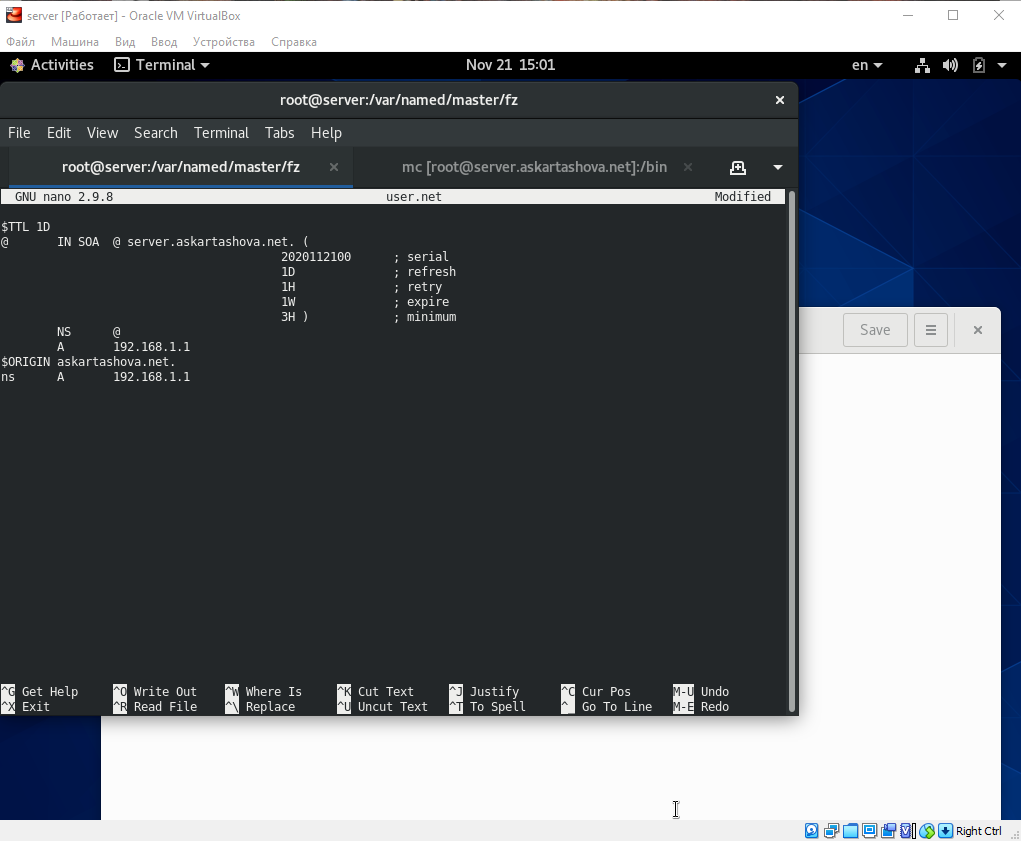
};

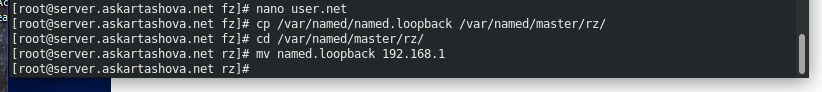
В каталоге /var/named создайте подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно.

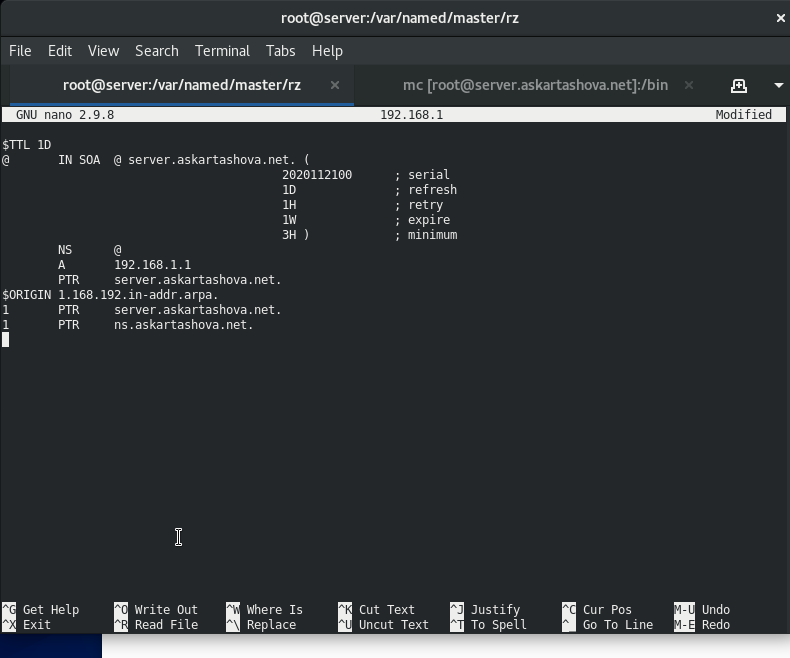
Скопируйте шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуйте его в user.net.



Изменим файл /var/named/master/fz/user.net, указав необходимые DNSзаписи для прямой зоны.



 Скопируем шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименуйте его в 192.168.1.

Изменим файл /var/named/master/rz/192.168.1, указав необходимые DNS-записи для обратной зоны.

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



Корректно восстановить метки в SELinux:

*restorecon -vR /etc*

*restorecon -vR /var/named*

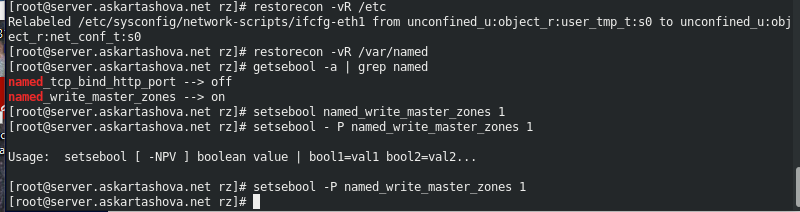
Для проверки состояния переключателей SELinux, относящихся к named, введем:

*getsebool -a | grep named*

При необходимости дайте named разрешение на запись в файлы DNS-зоны:

*setsebool named\_write\_master\_zones 1*

*setsebool -P named\_write\_master\_zones 1*

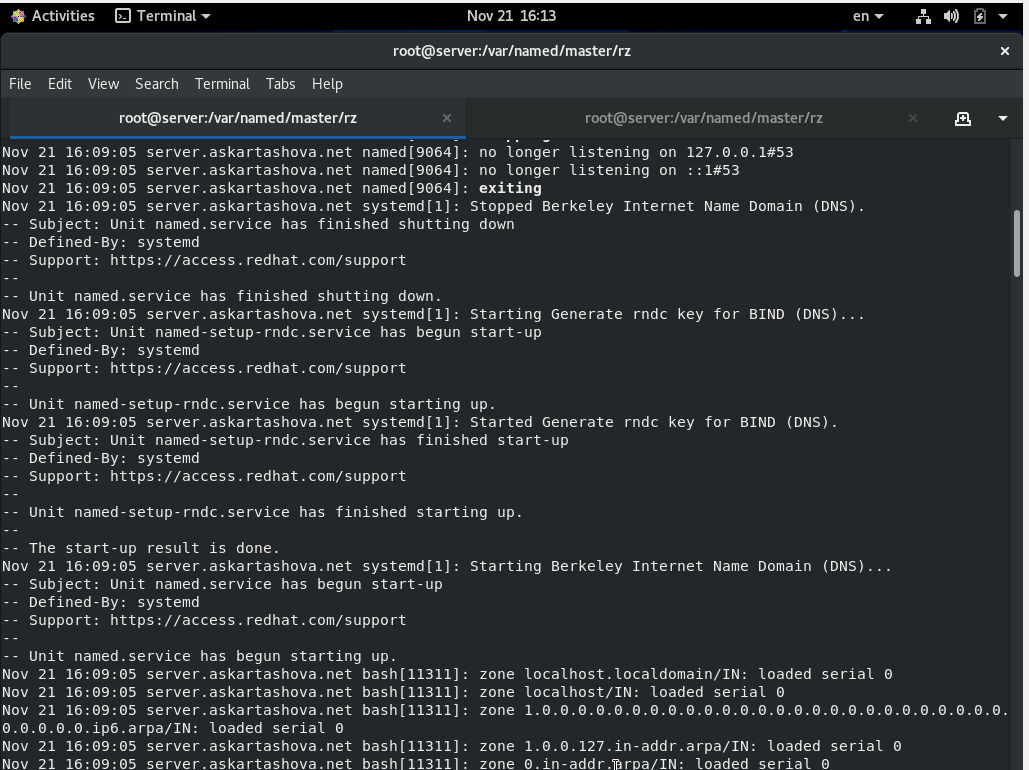


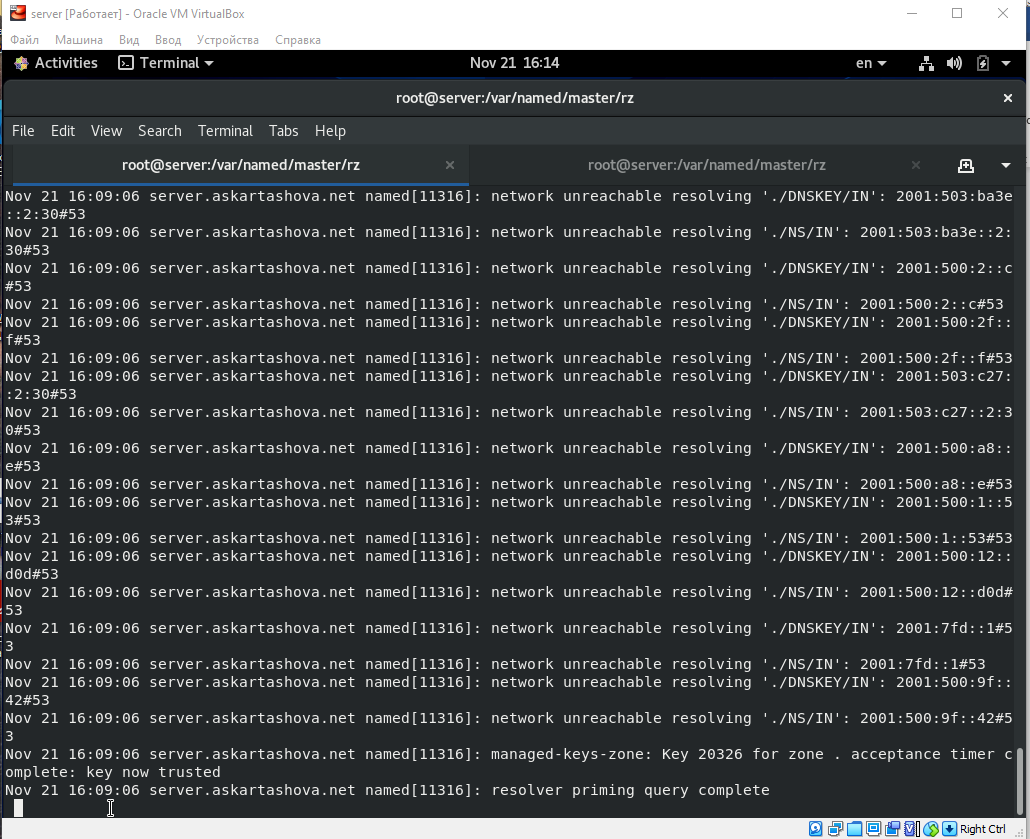
Во дополнительном терминале запустим в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:

*journalctl -x -f*

и в первом терминале перезапустим DNS-сервер:

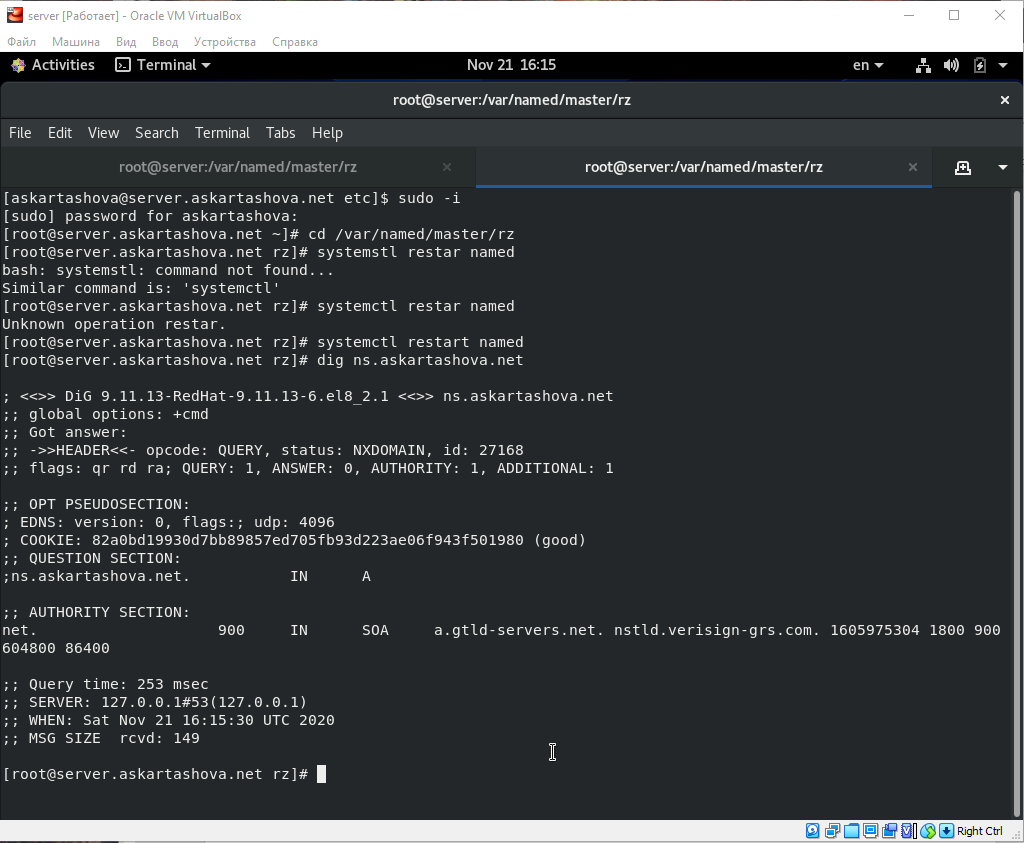
*systemctl restart named*



**

## Анализ работы DNS-сервера

При помощи утилиты dig получим описание DNS-зоны с сервера ns.user.net

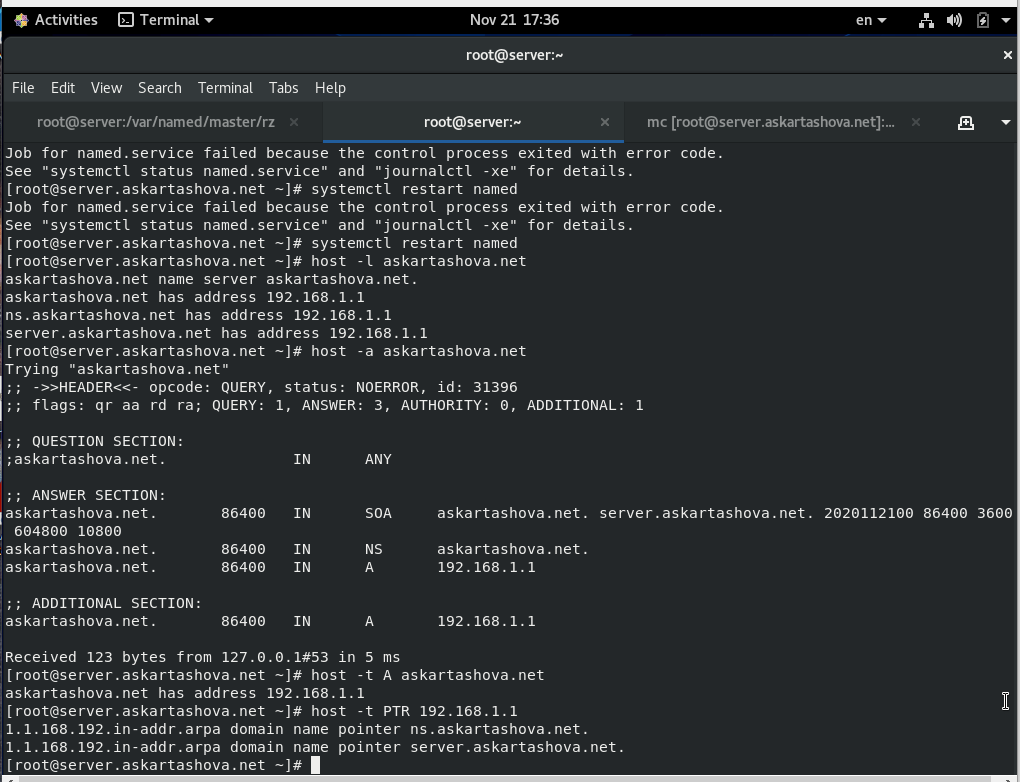
**При помощи утилиты host проанализируйте корректность работы DNS-сервера:

*host -l user.net*

*host -a user.net*

*host -t A user.net*

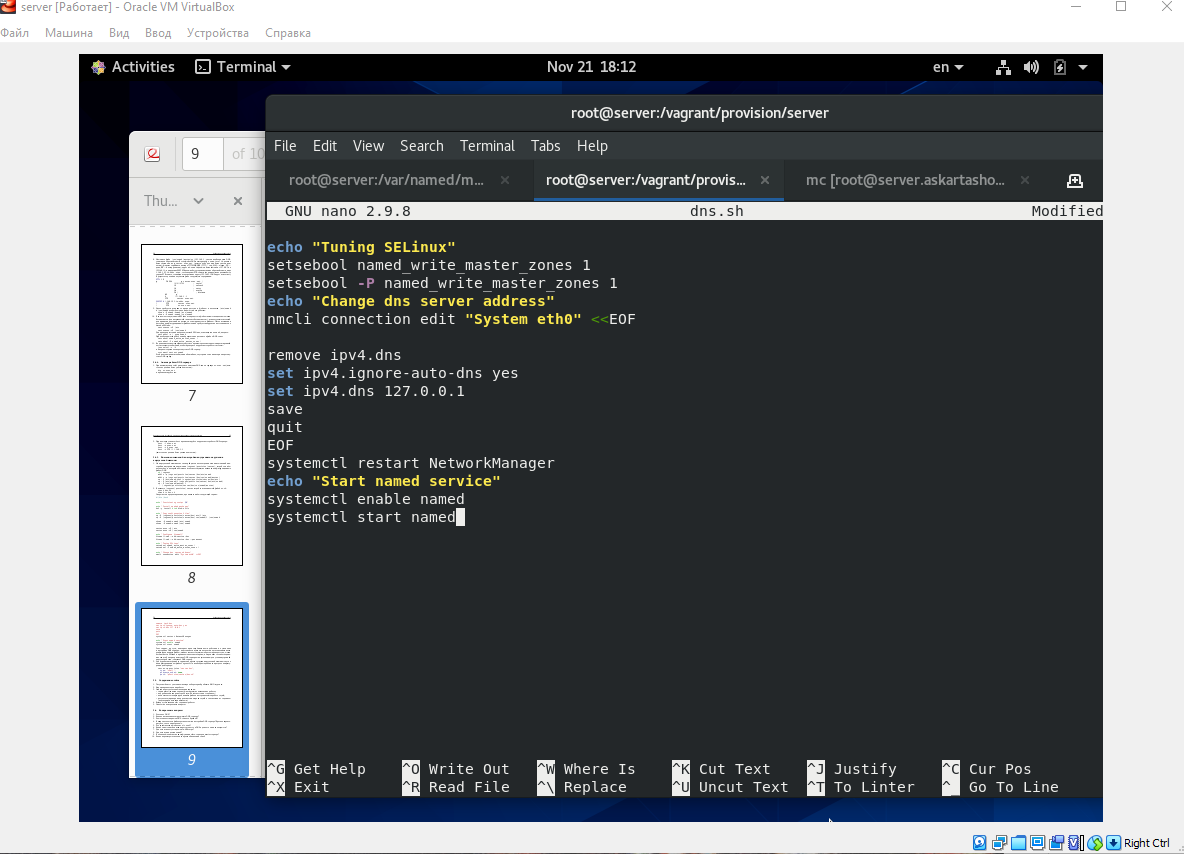
*host -t PTR 192.168*.1.1



## Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS

каталоге /vagrant/provision/server создайте исполняемый файл dns.sh. Открыв его на редактирование, пропишем в нём скрипт, повторяющий действия по конфигурированию сервера



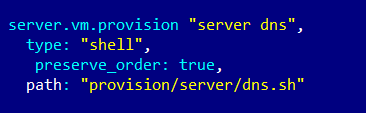
Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:

*server.vm.provision "server dns",*

*type: "shell",*

*preserve\_order: true,*

*path: "provision/server/dns.sh"*

**

# Заключение

Мы приобрели навыки по установке и конфигурированию DNS сервера и усвоении принципы работы системы доменных имён

# Контрольные вопросы

1. Что такое DNS?

Система доменных имён (Domain Name System, DNS)— распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP-адрес и наоборот.

2. Каково назначение кэширующего DNS-сервера?

Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.

3. Чем отличается прямая DNS-зона от обратной?

Прямая зона предусматривает преобразование имени в IP-адреса. Зоны обратного просмотра выполняют прямо противоположную операцию. Они предусматривают сопоставление IP-адресов с обычным именем.

4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.

/etc/resolv.conf — это основной файл настройки библиотеки распознавателя имен DNS.

/etc/named.conf - составляет основу конфигурации сервера DNS.

/var/named/named.ca- файл кэша. Показывает типовые записи корневого сервера имен.

/var/named/named.localhost и /var/named/named.loopback - описывают прямую и обратную зоны.

1. Что указывается в файле resolv.conf?

Этот файл содержит список ключевых слов с пользовательскими значениями, которые представляют собой различные типы информации преобразователя.

1. Какие типы записи описания ресурсов есть в DNS и для чего они используются?

A-запись (Address record). Address record указывает на конкретный IP-адрес домена.

AAAA-запись (Address record to IPv6). AAAA запись DNS — аналог предыдущей А-записи. В значении указывается внешний IP-адрес в формате IPv6.

CNAME-запись (Canonical name). CNAME («каноническое имя») указывает на

расположение хостов на одном сервере. С ее помощью можно прописать несколько доменов и поддоменов в рамках одного сервера.

MX-запись (Mail exchanger). MX-запись задает почтовый сервер, который будет

принимать и отправлять почту для данного домена.

NS-запись (Name Server) определяет доменный адрес DNSсервера, обслуживающий конкретный домен.

TXT-запись (Text String) используется для хранения текстовых данных о домене.

SOA-запись (Start of Authority) указывает местоположение сервера с эталонной информацией о домене.

PTR-запись служит для связывания отдельного IP-адреса с доменным именем.

RP-запись (Responsible person). Здесь прописаны реквизиты ответственных за домен.

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

Для отображения IP-адресов IPv4 в пространство доменных имен.

1. Для чего нужен домен named?

named - это сервер доменных имен пакета BIND.

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

Master-сервер (primary, первичный) доменных имен является ответственным (authoritative) за информацию о зоне. Он читает описание зоны с локального диска компьютера, на котором он функционирует и отвечает в соответствии с этим описанием на запросы resolver-ов.

Slave-сервер (secondary, вторичный, дублирующий) также является ответственным (authoritative) за зону. Его основное назначение заключается в том, чтобы подстраховать работу основного сервера доменных имен (master server), ответственного за зону, на случай его выхода из строя, а также для того, чтобы разгрузить основной сервер, приняв часть запросов на себя.

1. Какие параметры отвечают за время обновления зоны?

**–** *refresh* — интервал времени, после которого slave-сервер обязан обратиться к masterсерверу с запросом на верификацию своего описания зоны;

**–** *retry* — интервал времени, после которого slave-сервер должен повторить попытку синхронизировать описание зоны с master сервером;

**–** *expire* — интервал времени, после которого slave-сервер должен прекратить обслуживание запросов к зоне, если он не смог в течение этого времени верифицировать

описание зоны, используя информацию с master сервера;

1. Как обеспечить защиту зоны от скачивания и просмотра?

12. Какая запись RR применяется при создании почтовых серверов?

MX - задаёт имена почтовым серверам.

1. Как протестировать работу сервера доменных имён?

При помощи утилиты host

*host -l user.net*

*host -a user.net*

*host -t A user.net*

*host -t PTR 192.168.1.1*

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

С помощью команд:

systemctl start <имя службы>

systemctl restart <имя службы>

systemctl stop <имя службы>

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

Systemctl status < название службы>

16. Где храниться отладочная информация по работе системы и служб? Как её посмотреть?

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

1. ps

2. htop

18. Приведите несколько примеров по изменению сетевого соединения при помощи

командного интерфейса nmcli.

*1. nmcli connection edit System\ eth0*

*remove ipv4.dns*

*set ipv4.ignore-auto-dns yes*

*set ipv4.dns 127.0.0.1*

*save*

*quit*

*2. nmcli connection modify ethernet-enp0s8 ipv4.address 192.168.4.26/24*

*nmcli connection modify ethernet-enp0s8 ipv4.method manual*

*save*

*quit*

19. Что такое SELinux?

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра.

20. Что такое контекст (метка) SELinux?

Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально)

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

*restorecon -vR /etc*

*restorecon -vR /var/named*

22. Как создать разрешающие правила политики SELinux из файлов журналов,

содержащих сообщения о запрете операций?

С помощью утилиты audit2allow.

23. Что такое булевый переключатель в SELinux?

Переключатели позволяют изменять части политики SELinux во время работы(без перезапуска и остановки), не обладая глубоким пониманием создания политики SELinux. Это позволяет вносить изменения, такие как: разрешение доступа службам к файловым системам NFS, без перезагрузки или рекомпиляции политики SELinux.

24. Как посмотреть список переключателей SELinux и их состояние?

**Команда:** *getsebool*

25. Как изменить значение переключателя SELinux?

**Команда**: *setseboo*