РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

**Факультет физико-математических и естественных наук**

**Кафедра прикладной информатики и теории вероятностей**

ОТЧЕТ

по лабораторной работе № 2

дисциплина: Администрирование сетевых подсистем

Студент:

Группа:

**МОСКВА**

2023 г.

# Цель работы:

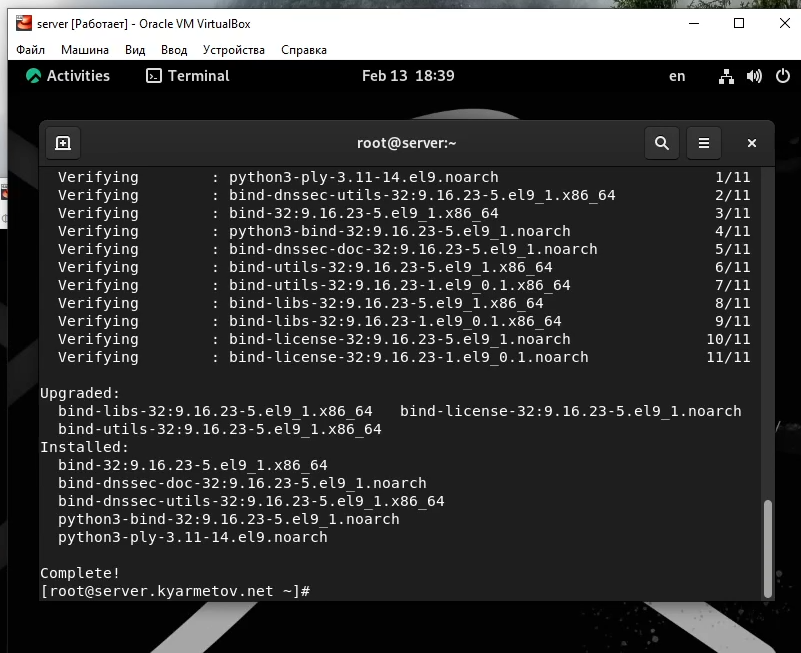
Приобретение практических навыков по установке и конфигурированию DNS-

сервера, усвоение принципов работы системы доменных имён.

# Ход работы:

## Установка DNS-сервера

1. Загружаю операционную систему и перехожу в рабочий каталог с проектом:
2. Запускаю виртуальную машину server: make server
3. На виртуальной машине server захожу под созданным в предыдущей работе пользователем (kyarmetov) и открываю терминал. Перехожу в режим суперпользователя: sudo –i
4. Устанавливаю bind и bind-utils



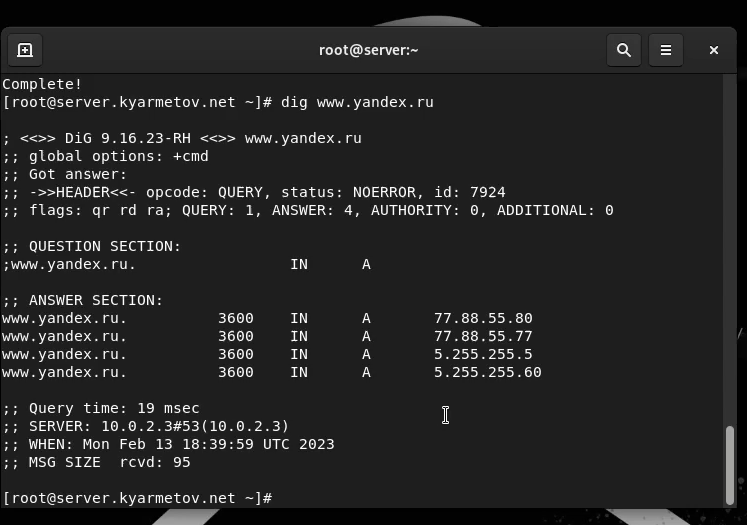
1. C помощью утилиты dig делаю запрос, к DNS-адресу www.yandex.ru: dig [www.yandex.ru](http://www.yandex.ru)

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без ошибок, использовались флаги qr rd ra, запрос отправлен один, ответов получено четыре.

Информация AUTHORITY SECTION (содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени) и ADDITIONAL SECTION (содержит IP-адреса серверов доменных имен, перечисленных в предыдущей секции). Не предоставляется.

QUESTION SECTION (секция запроса): Показывает наш запрос, то есть в данной лабораторной работе запросили показать A-запись (команда DIG без параметров) для домена www.yandex.ru;

ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS, в нашем случае показывает A-запись для www.yandex.ru.  
Последняя секция — это статистика по запросу (служебная информация) - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.



## Конфигурирование кэширующего DNS-сервера

1. Анализирую содержание файлов
2. /etc/resolv.conf

Содержит указание на поиск kyarmetov.net – локального домена, а также адрес сервера имен в Интернет.

1. /etc/named.conf

Оператор **options** определяет параметры глобальной конфигурации сервера и устанавливает значения по умолчанию для других операторов.

options {

listen-on port 53 { 127.0.0.1; }; Задает сетевой интерфейс, по которому named прослушивает запросы, и адрес сети.

listen-on-v6 port 53 { ::1; }; Задает сетевой интерфейс, по которому named прослушивает запросы, и адрес IPv6 сети.

directory "/var/named"; Задает рабочий каталог для named.

dump-file "/var/named/data/cachedump.db"; Задает дамп файл.

statistics-file "/var/named/data/namedstats.txt"; Задает альтернативное расположение файлов статистики.

memstatistics-file "/var/named/data/named\_mem\_stats.txt"; Имя файла со статистикой использования памяти.

allow-query { localhost; };Указывает клиентов, которым разрешено запрашивать информацию об этой зоне. По умолчанию разрешены все запросы.

recursion yes; Опция, разрешающая или запрещающая рекурсию.

dnssec-enable yes; Включение или отключение dnssec(функция позволяет криптографически подписывать зоны с помощью ключа зоны) на уровне сервера.

dnssec-validation yes; Проверка корректности ответов.

/\* Путь до ключа ISC DLV \*/

bindkeys-file "/etc/named.iscdlv.key"; Альтернативный репозиторий для доверенных ключей.

managed-keys-directory "/var/named/dynamic"; Каталог ключей управления.

pid-file "/run/named/named.pid"; Задает расположение файла идентификатора процесса, созданного named.

session-keyfile "/run/named/session.key"; Каталог сеансовых ключей.

};

logging { Ведение журнала.

channel default\_debug {Канал, который обрабатывает

отладочные сообщения

file "data/named.run"; Файл отладочных сообщений

severity dynamic; Версия журнала

};

};

zone "." IN {Описание оператора зоны, идентифицируемой "."

type hint; hint - специальный тип зоны, используемый для указания на корневые серверы имен, которые разрешают запросы, когда зона не известна иначе. Никакая конфигурация, кроме значения по умолчанию, не требуется с помощью зоны подсказки.

file "named.ca"; Файл, на который даётся указание на чтение сервисом named.

};

/\*Подключение файлов описания зон\*/

include "/etc/named.rfcl912.zones";

include "/etc/named.root.key";

1. /var/named/named.ca

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без ошибок, id – 17380, использовались флаги qr aa, запрос отправлен один, ответов получено тринадцать.

Информация AUTHORITY SECTION (содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени) и ADDITIONAL SECTION (содержит IP-адреса серверов доменных имен, перечисленных в предыдущей секции). Представлены 27 элементов.

QUESTION SECTION (секция запроса): Показывает наличие запроса на A-запись; ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS.  
Последняя секция — это статистика по запросу (служебная информация) - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.

1. /var/named/named.localhost

$TTL 1d - время, в течение которого DNS-запись для определенного хоста остается в кэш-памяти DNS-сервера после того, как последний установил соответствующий IP-адрес хоста. В данном случае 1 день.

SOA-запись — указывает на авторитативность для зоны;

rname.invalid — почтовый адрес лица, осуществляющего администрирование зоны;

0; serial — серийный номер файла зоны в нотации ГГГГММДДВВ (учёт изменений файла описания зоны);

1D; refresh — интервал времени, после которого slave-сервер обязан обратиться к master-серверу с запросом на верификацию своего описания зоны (1 день);

1H; retry — интервал времени, после которого slave-сервер должен повторить попытку синхронизировать описание зоны с master сервером (1 час);

1W; 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 неделя);

3H; minimum — время негативного кэширования (negative caching), т.е. время кэширования ответов, которые утверждают, что установить соответствие между доменным именем и IP-адресом нельзя (3 часа).

NS @-доменное имя сервера

А 127.0.0. - IP-адрес машины

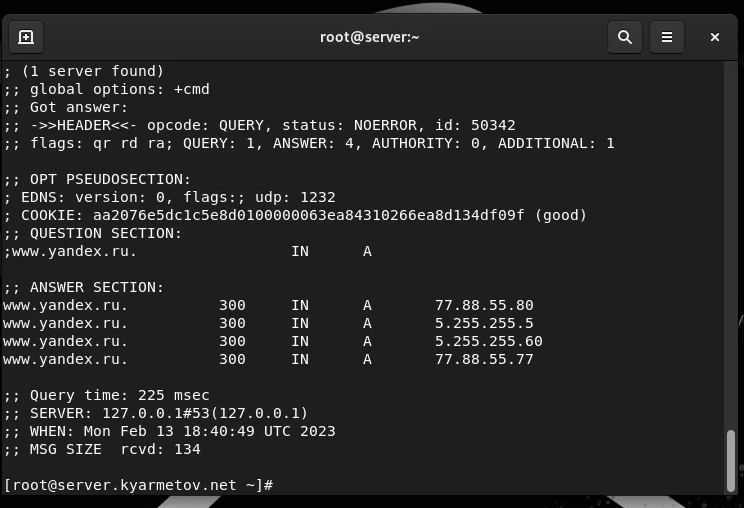
AAAA ::1 - IPv6 -адрес

1. /var/named/named.loopback

Описание первой части совпадает с описанием предыдущего файла ((4)/var/named/named.localhost)

PTR localhost — доменное имя хоста.

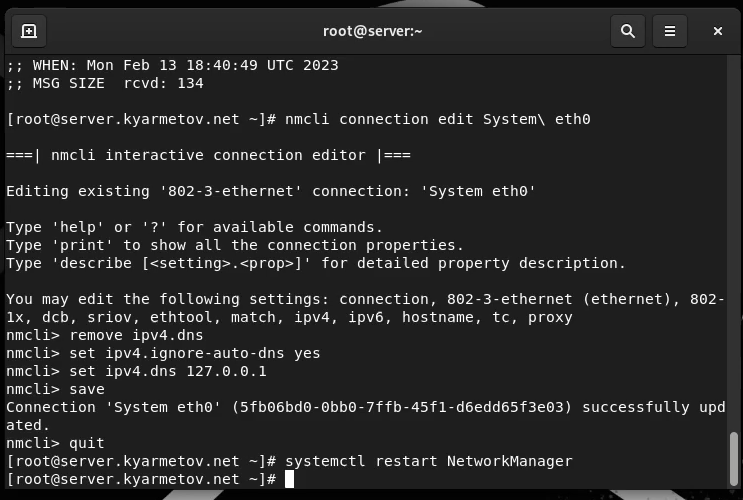
1. Запускаю DNS-сервер
2. Включаю запуск DNS-сервера в автозапуск при загрузке системы
3. Выведенная на экран информацию при выполнении команды dig @127.0.0.1 [www.yandex.ru](http://www.yandex.ru)



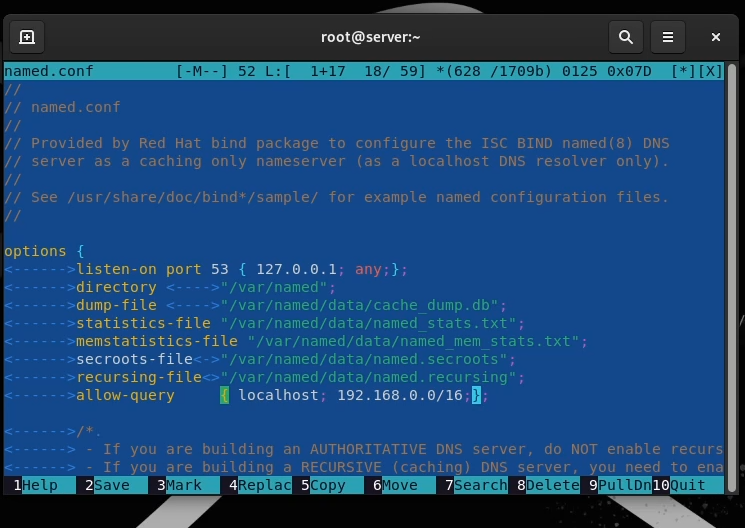
Отличие от вывода команды dig [www.yandex.ru](http://www.yandex.ru) состоит в том, что запрос не выполнен, о чём нам говорит status. Следовательно, ответов нет (0).

Записи с серверов, поддерживающих EDNS0, включают OPT RR (специфичный тип RR-записи, которая не несёт DNS-данные, нужна исключительно для стандартизации обмена служебной информацией), который не имеет текстового формата rdata, поэтому он не печатается, но можно видеть, что он описан в комментариях выше раздела вопросов как «OPT PSEUDOSECTION».

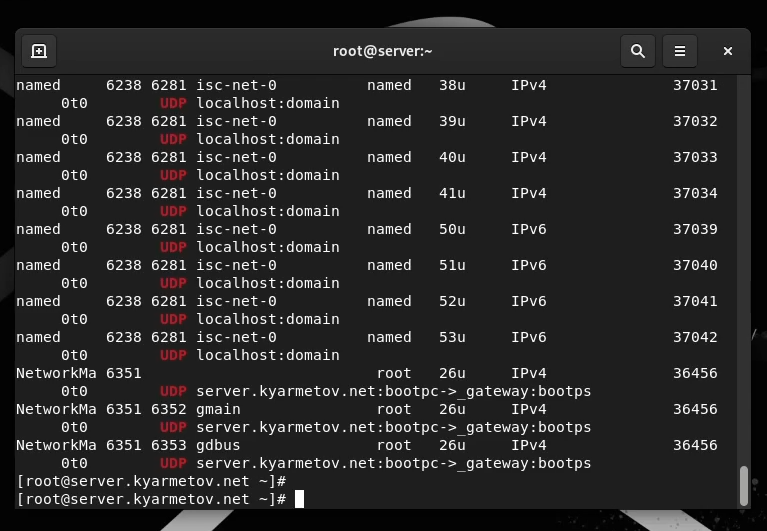
1. Устанавливаю DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого требуется изменить настройки сетевого соединения System eth0 в NetworkManager, переключив его на работу с внутренней сетью и указав для него в качестве DNS-сервера по умолчанию адрес 127.0.0.1:
2. Перезапускаю NetworkManager: systemctl restart NetworkManager



1. Настраиваю направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server.

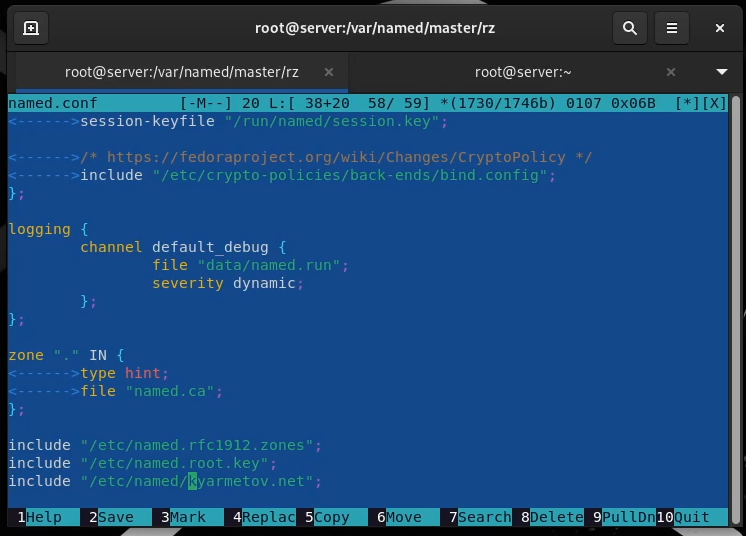


1. Вношу изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:
2. Проверяю, что DNS-запросы идут через узел server, который прослушивает порт 53.

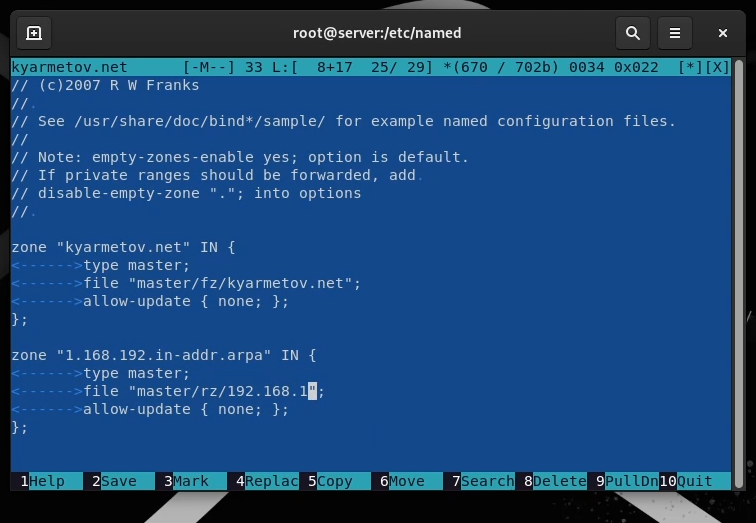


## Конфигурирование первичного DNS-сервера

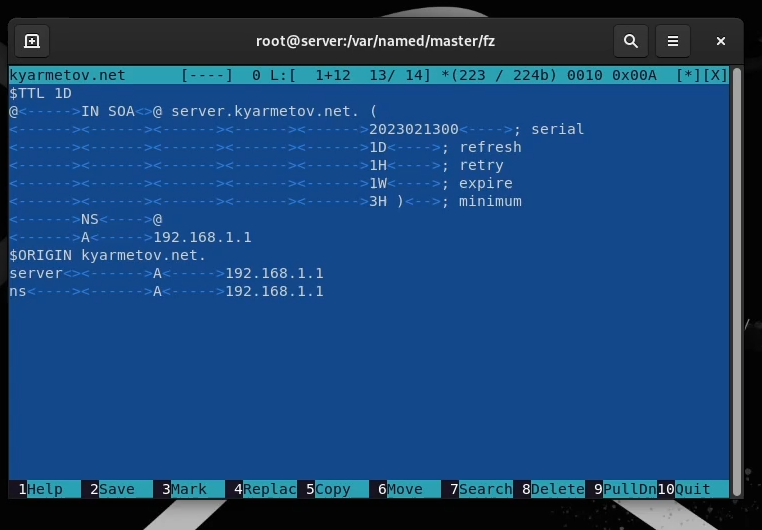
1. Копирую шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименовываю его в kyarmetov.net:
2. Включаю файл описания зоны /etc/named/user.net в конфигурационном файле DNS /etc/named.conf;



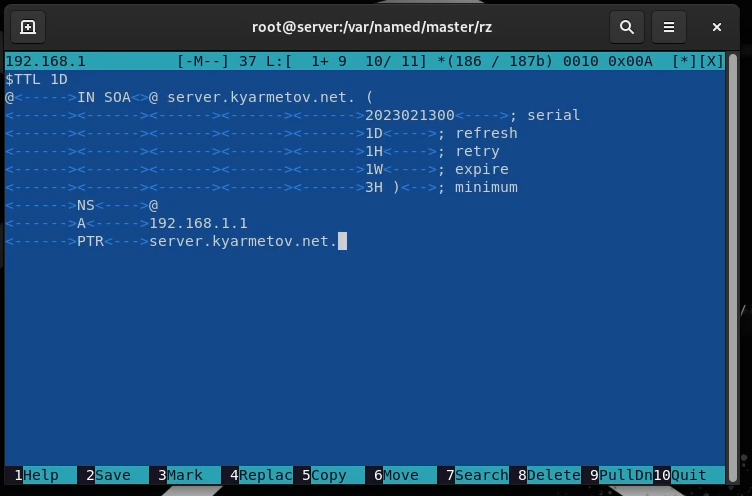
1. Открываю файл /etc/named/user.net на редактирование



1. В каталоге /var/named создаю подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно:
2. Копирую шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименовываю его в kyarmetov.net:
3. Изменяю файл /var/named/master/fz/kyarmetov.net, указав необходимые DNS записи для прямой зоны. В этом файле DNS-имя сервера @ rname.invalid. должно быть заменено на @ server.kyarmetov.net. 2020111400 - формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в A-записи должен быть заменён с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN должно быть задано текущее имя домена kyarmetov.net., а затем указаны имена и адреса серверов в этом домене в виде A-записей DNS (на данном этапе должен быть прописан сервер с именем ns и адресом 192.168.1.1):



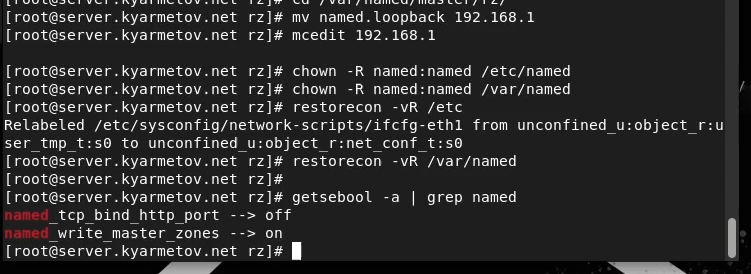
1. Копирую шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переименовываю его в 192.168.1:
2. Изменяю файл /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны. В этом файле DNS-имя сервера @ rname.invalid. должно быть заменено на @ server.kyarmetov.net. 2020111400 - формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в A-записи должен быть заменён с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN должно быть задано название обратной зоны в виде 1.168.192.in-addr.arpa., затем заданы PTR-записи (на данном этапе должна быть задана PTR запись, ставящая в соответствие адресу 192.168.1.1 DNS-адрес ns.kyarmetov.net):



1. Исправляю права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать:
2. 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:

Для проверки состояния переключателей SELinux, относящихся к named, ввожу: getsebool -a | grep named

Даю named разрешение на запись в файлы DNS-зоны:

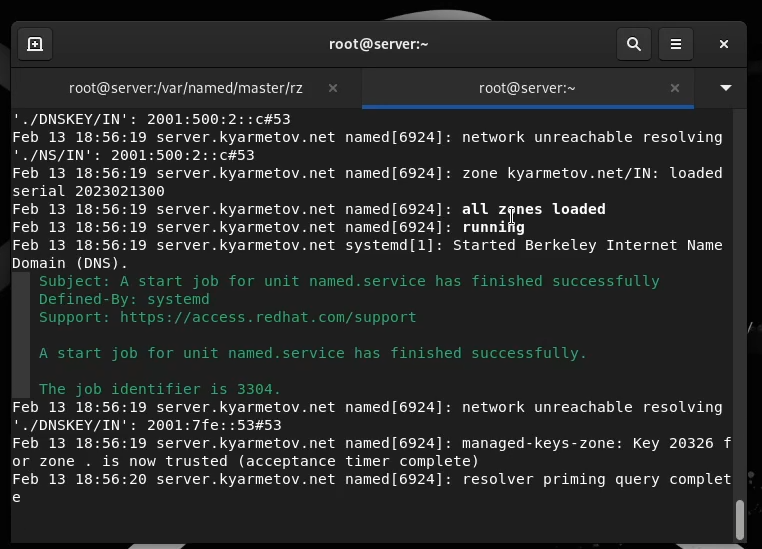


1. В дополнительном терминале запускаю в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы:

journalctl -x -f

и в первом терминале перезапускаю DNS-сервер:

systemctl restart named



## Анализ работы DNS-сервера

* 1. При помощи утилиты dig получаю описание DNS-зоны с сервера ns.kyarmetov.net;

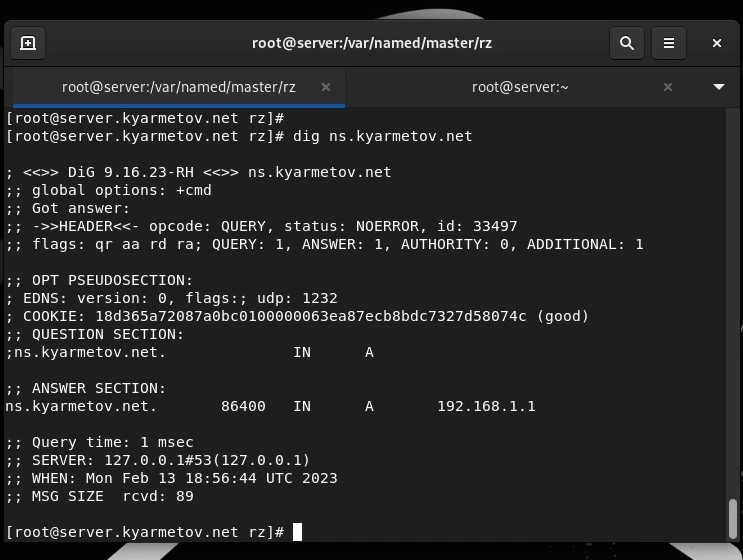
Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без ошибок, использовались флаги qr аа rd ra, запрос отправлен один, ответов получено один.

Информация AUTHORITY SECTION содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени – kyarmetov.net и ADDITIONAL SECTION содержит IP-адреса серверов доменных имен, перечисленных в предыдущей секции – 192.168.1.1.

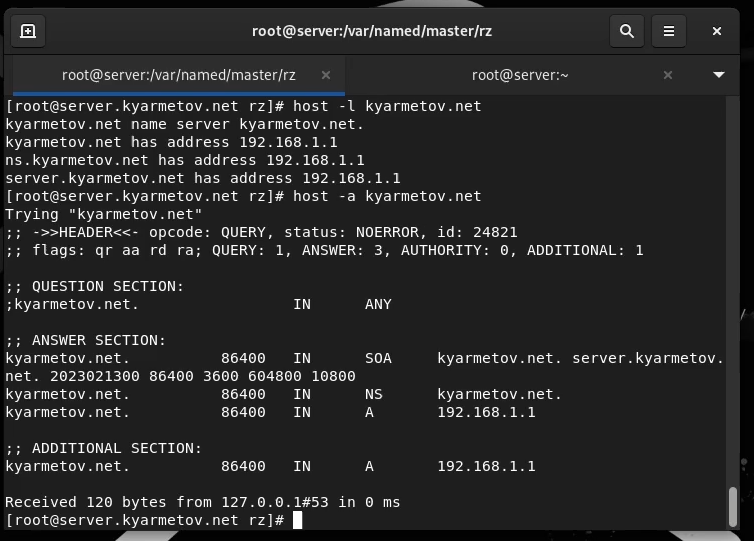
QUESTION SECTION (секция запроса): Показывает запрос показать A-запись (команда DIG без параметров) для домена ns.kyarmetov.net;

ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS – A-запись для ns.kyarmetov.net.  
Последняя секция — это статистика по запросу - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.

Записи с серверов, поддерживающих EDNS0, включают OPT RR(специфичный тип RR-записи, которая не несёт DNS-данные, нужна исключительно для стандартизации обмена служебной информацией), который не имеет текстового формата rdata, поэтому он не печатается, но можно видеть, что он описан в комментариях выше раздела вопросов как «OPT PSEUDOSECTION».

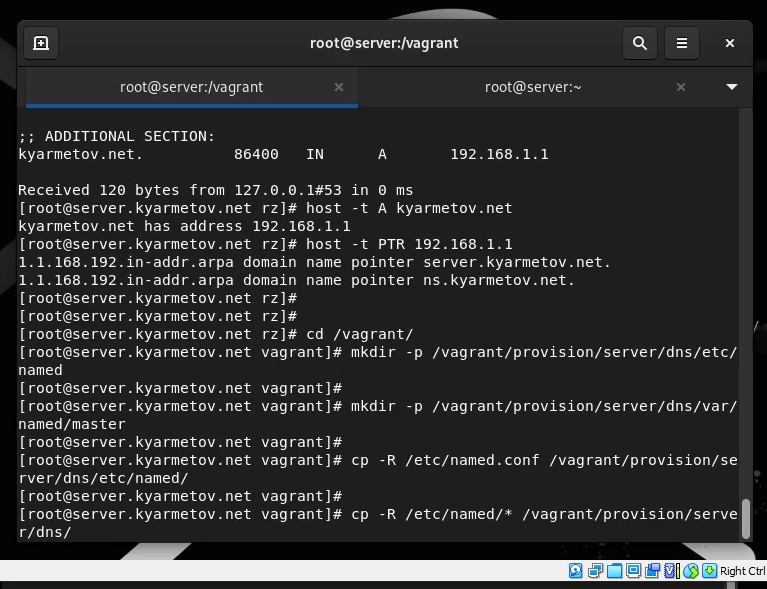


* 1. При помощи утилиты host анализирую корректность работы DNS-сервера:

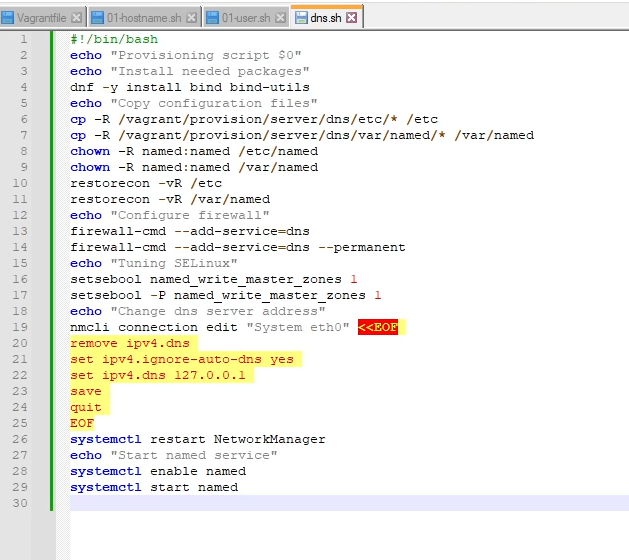


## Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server 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:



1. В каталоге /vagrant/provision/server создаю исполняемый файл dns.sh:



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

# Вывод:

Я приобрел практические навыки по установке и конфигурированию DNS-

сервера, усвоение принципов работы системы доменных имён.