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: Администрирование* *Сетевых Подсистем*

Студент: Ким Реачна

Группа: НПИбд 02-20

Студенческий билет: 1032205204

**МОСКВА**

2022 г.

**Цель работы:**

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

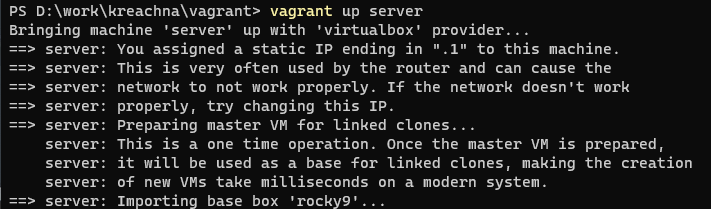
**Выполнение работы:**

1. **Установка DNS-сервера**
2. Загрузите вашу операционную систему и перейдите в рабочий каталог с проектом:

cd /var/tmp/user\_name/vagrant

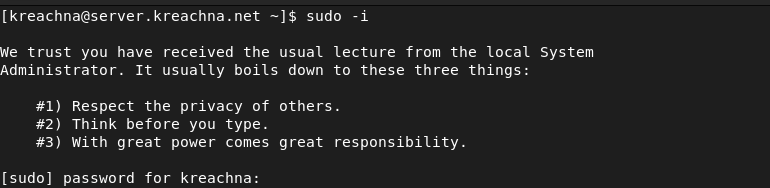
1. Запустите виртуальную машину server:

make server (или, если вы работаете под ОС Windows, то vagrant up server).



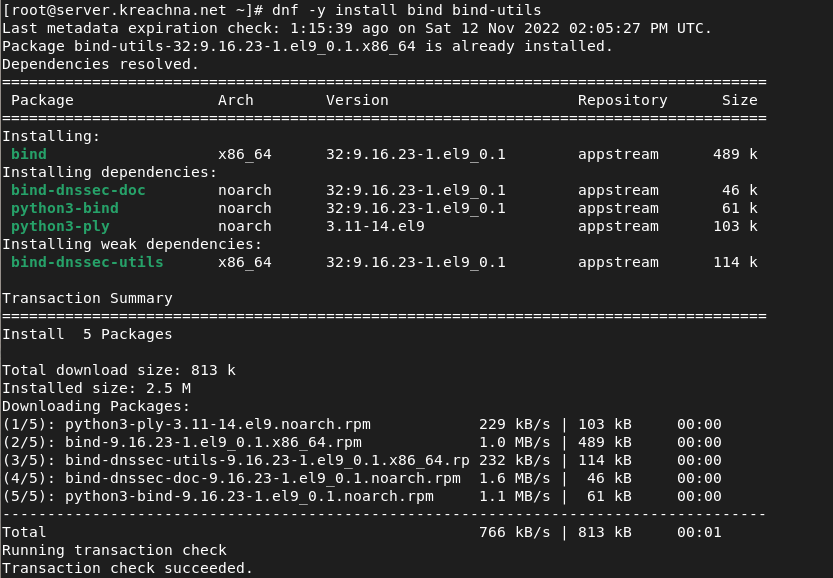
1. На виртуальной машине server войдите под созданным вами в предыдущей работе пользователем и откройте терминал. Перейдите в режим суперпользователя:

sudo -i



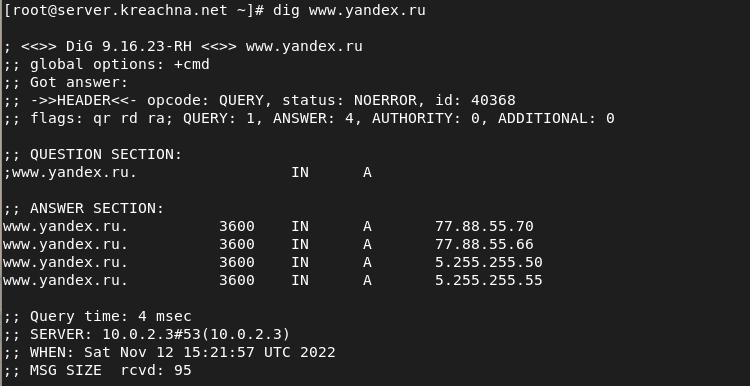
1. Установите bind и bind-utils:

dnf -y install bind bind-utils



1. В качестве упражнения с помощью утилиты dig сделайте запрос, например, к DNS-адресу [www.yandex.ru](http://www.yandex.ru):

dig [www.yandex.ru](http://www.yandex.ru)



1. **Конфигурирование кэширующего DNS-сервера**
   1. **Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами**
2. В отчёте проанализируйте построчно содержание файлов /etc/resolv.conf, /etc/named.conf, /var/named/named.ca, /var/named/named.localhost, /var/named/named.loopback.

* /etc/resolv.conf – Содержит указание на поиск nssedov.net – локального домена, а также адрес сервера имен в Интернет.
* /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";

* /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.

* /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

* /var/named/named.loopback

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

PTR localhost — доменное имя хоста.

1. Запустите DNS-сервер:

systemctl start named

1. Включите запуск DNS-сервера в автозапуск при загрузке системы:

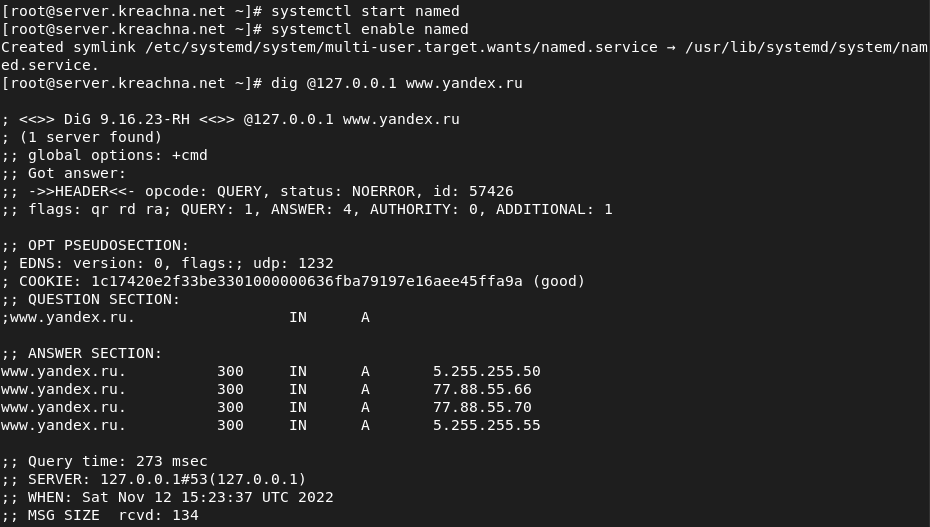
systemctl enable named

1. Проанализируйте в отчёте отличие в выведенной на экран информации при выполнении команд

dig www.yandex.ru

и

dig @127.0.0.1 [www.yandex.ru](http://www.yandex.ru)



1. Сделайте 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:

nmcli connection edit System\ eth0

remove ipv4.dns

set ipv4.ignore-auto-dns yes

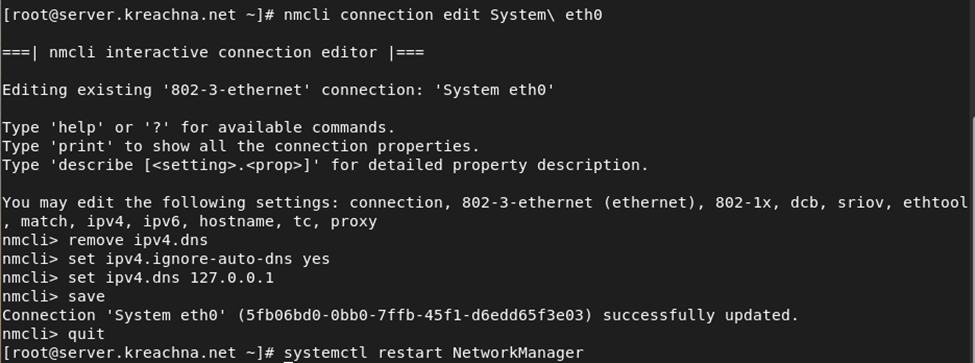
set ipv4.dns 127.0.0.1

save

quit

1. Перезапустите NetworkManager:

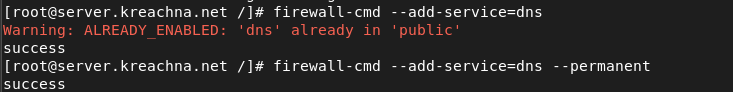
systemctl restart NetworkManager



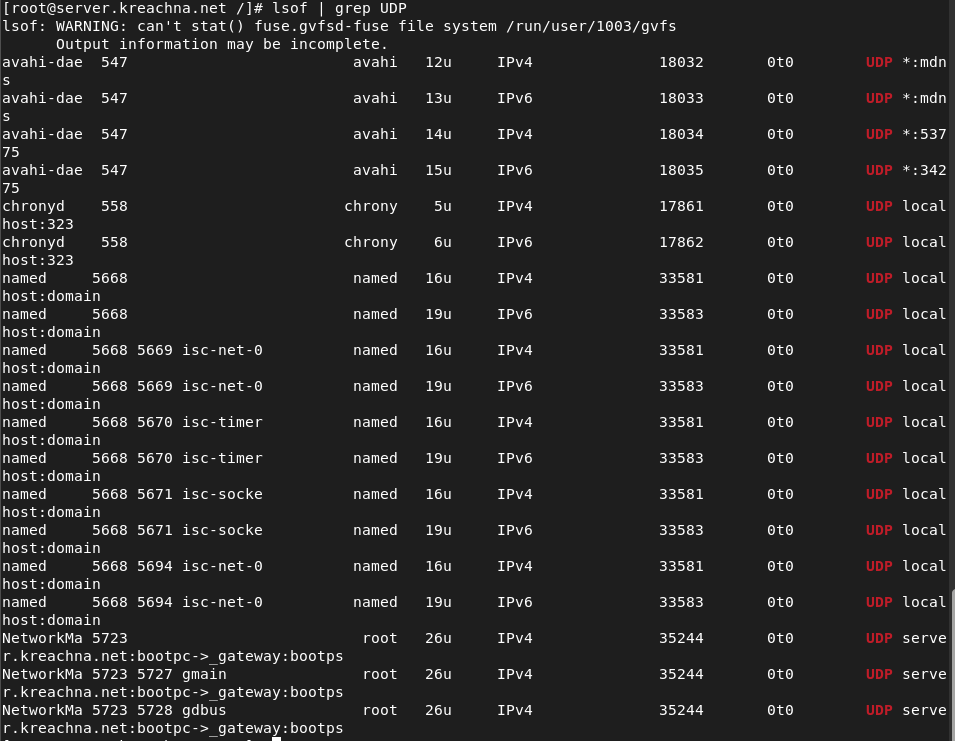
1. Требуется настроить направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесите изменения в файл /etc/named.conf, заменив строку

****

1. Внесите изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:

****

1. Убедитесь, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этого на данном этапе используйте команду lsof:

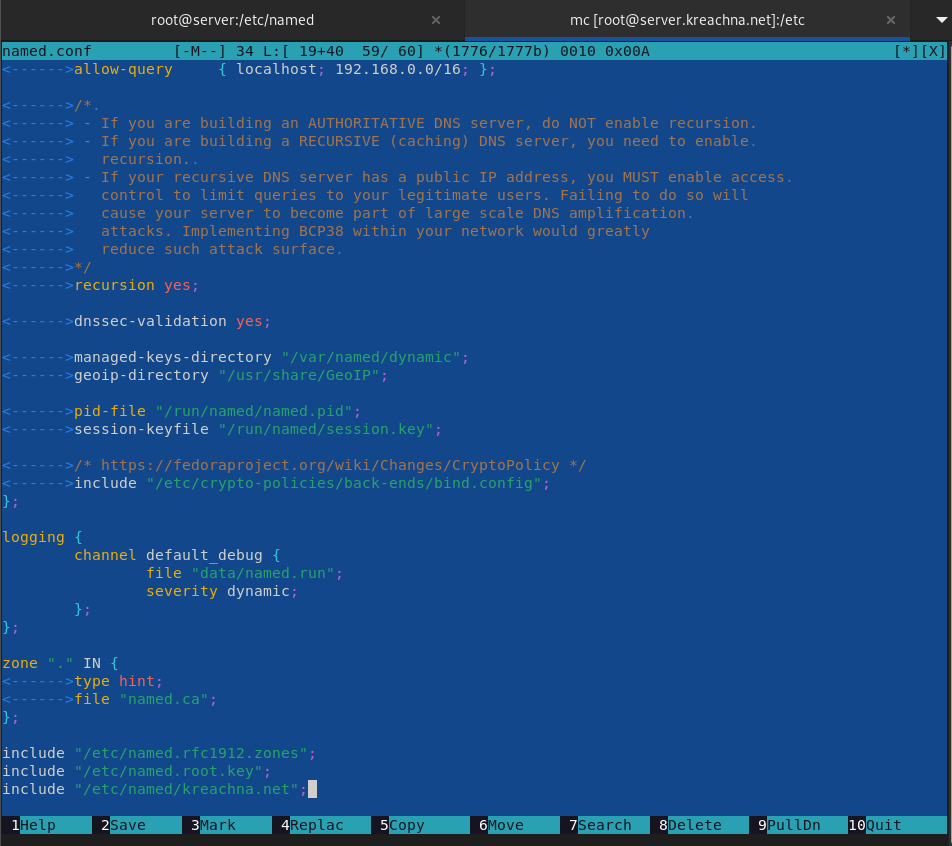
****

* 1. **Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами**
  2. **Конфигурирование первичного DNS-сервера**

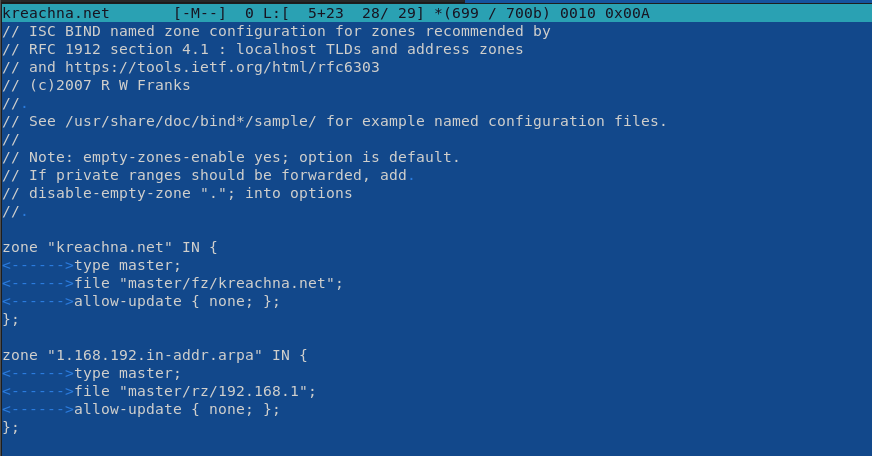
1. Скопируйте шаблон описания DNS-зон named.rfc1912.zones из каталога /etc в каталог /etc/named и переименуйте его в user.net (вместо user укажите свой логи):

****

1. Включите файл описания зоны /etc/named/user.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку:

****

1. Откройте файл /etc/named/user.net на редактирование и вместо зоны

****

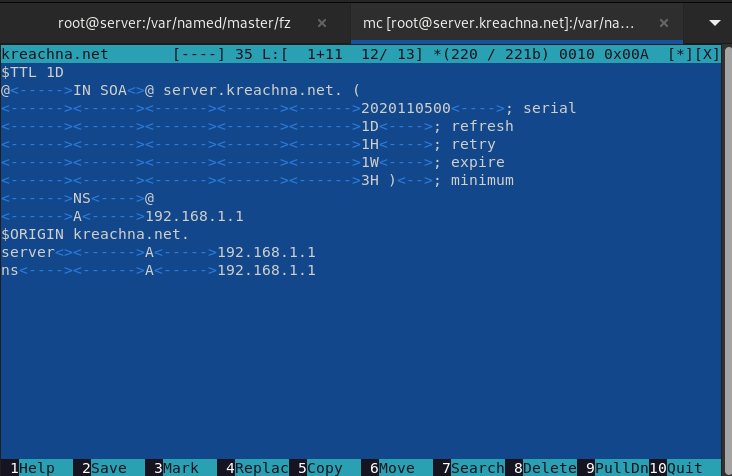
1. В каталоге /var/named создайте подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно:

****

1. Скопируйте шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименуйте его в user.net (вместо user укажите свой логин):

****

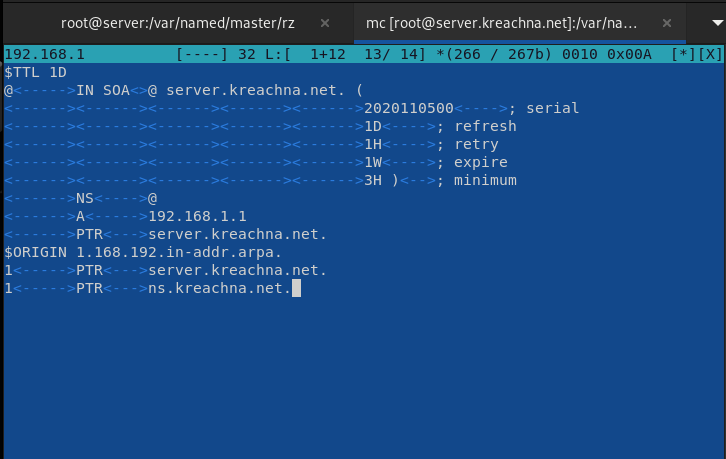
1. Измените файл /var/named/master/fz/user.net, указав необходимые DNS-записи для прямой зоны. В этом файле DNS-имя сервера @ rname.invalid. должно быть заменено на @ server.user.net. (вместо user должен быть указан ваш логин); формат серийного номера ГГГГММДДВВ (ГГГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии) [1]; 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 user.net. (вместо user должен быть указан ваш логин), 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). При этом внимательно отнеситесь к синтаксису в этом файле, а именно к пробелам и табуляции. В результате должен получиться файл следующего содержания:

****

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

****

1. Измените 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.user.net. (вместо user должен быть указан ваш логин); 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.user.net). В результате должен получиться файл следующего содержания:

****

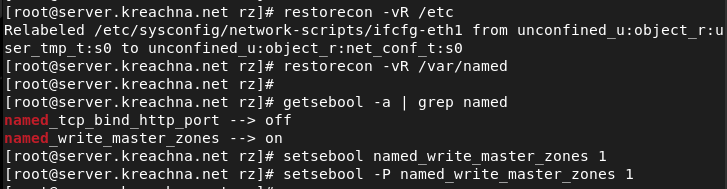
1. Далее требуется исправить права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать:

chown -R named:named /etc/named

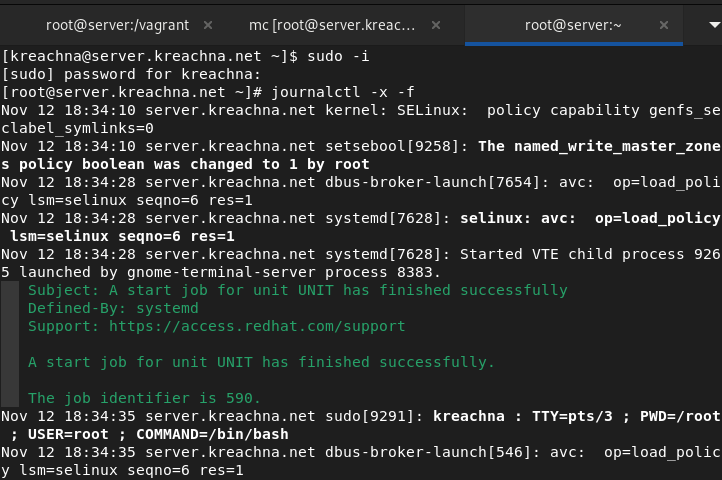
chown -R named:named /var/named

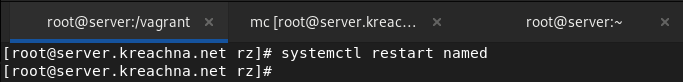


1. В системах с запущенным SELinux все процессы и файлы имеют специальные метки безопасности (так называемый «контекст безопасности»), используемые системой для принятия решений по доступу к этим процессам и файлам. После изменения доступа к конфигурационным файлам named требуется корректно восстановить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

****

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

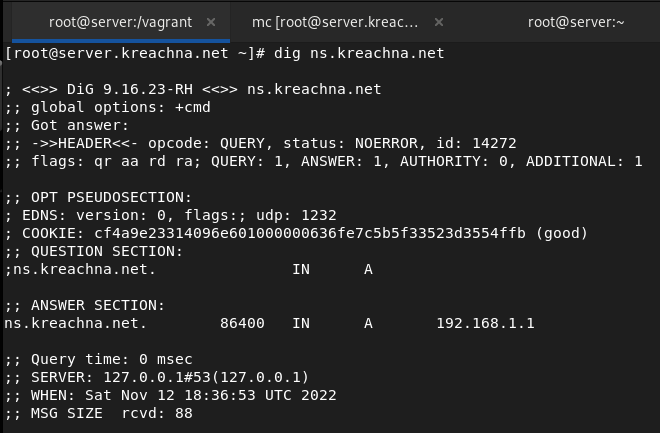
****

****

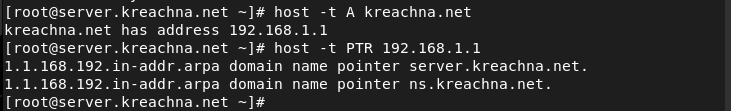
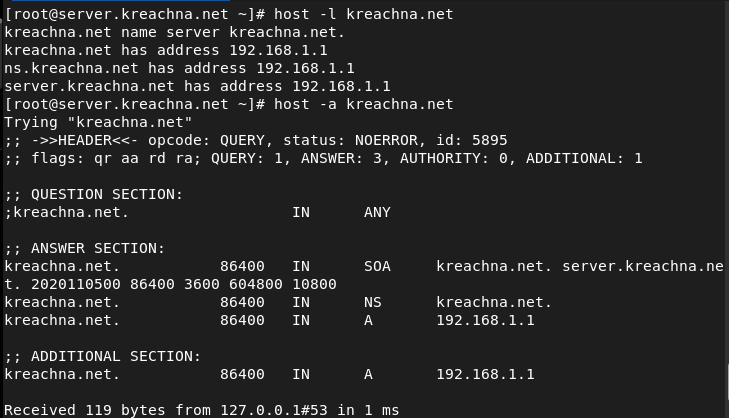
* 1. **Анализ работы DNS-сервера**

1. При помощи утилиты dig получите описание DNS-зоны с сервера ns.user.net (вместо user должен быть указан ваш логин):

dig ns.user.net

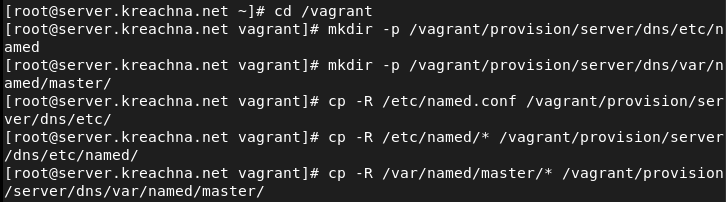


1. При помощи утилиты host проанализируйте корректность работы DNS-сервера:

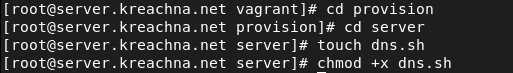
****

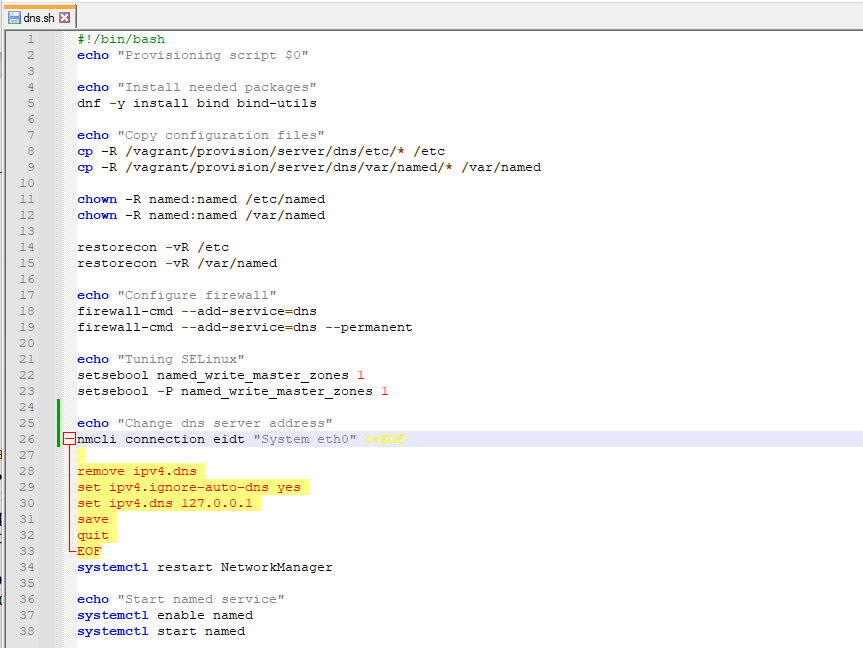
* 1. **Внесение изменений в настройки внутреннего окружения виртуальной машины**

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dns, в который поместите в соответствующие каталоги конфигурационные файлы DNS:

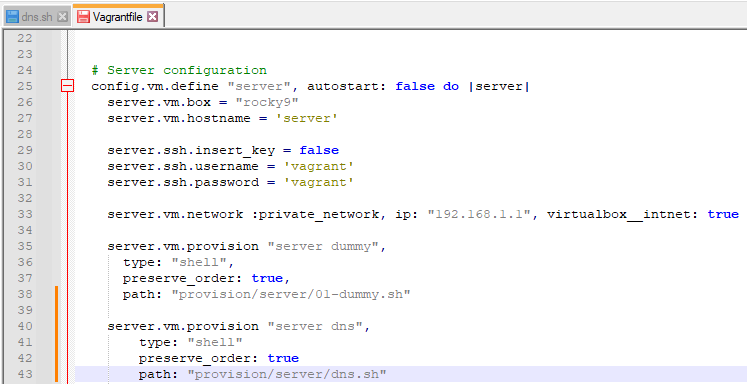
****

1. В каталоге /vagrant/provision/server создайте 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:

****

**Контрольные вопросы:**

1. Что такое 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.

1. Чем отличается прямая DNS-зона от обратной?

Задача поиска доменного имени по IP-адресу является обратной к прямой задаче — поиску IP-адреса по доменному имени. Прямая решается в DNS при помощи записей типа A (Address). Обратная же при помощи записей-указателей типа PTR (Pointer), которые совместно с записями SOA и NS составляют описание так называемой «обратной» зоны.

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

В файле host.conf содержатся опции программы-определителя, в файле resolv.conf содержатся адреса серверов имен, к которым имеет доступ данная система. Файл named.ca организует кэширование для сервера имен.

1. Что указывается в файле resolv.conf?

В файле resolv.conf содержатся адреса серверов имен, к которым имеет доступ данная система.

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

* SOA-запись — указывает на авторитативность для зоны
* NS-запись — перечисляет DNS-серверы зоны
* А — отображение имён узлов в адреса
* PTR — отображение адресов в имена узлов
* CNAME — каноническое имя (для псевдонимов)
* MX — отображение имён почтовых серверов

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

Для отображения IP-адресов IPv4 в пространство доменных имен

1. Для чего нужен демон named?

Демон named может реализовывать функции серверов любого типа: master, slave, cache.

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

* master — хранит и управляет ресурсными записями (описанием) доменной зоны. К главному серверу может быть подключено множество ведомых
* slave — получает и хранит информацию о доменных зонах с главного сервера. На ведомом сервере невозможно изменить описание доменной зоны. Служит для снижения нагрузки с главного DNS-сервера.

1. Какие параметры отвечают за время обновления зоны?

За обновление отвечает третий параметр в файле kreachna.net

1. Как обеспечить защиту зоны от скачивания и просмотра?

Задать подходящие права доступа на чтение и запись.

1. Какая запись RR применяется при создании почтовых серверов?

При создании почтовых серверов используют А записи.

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

Использовать в терминале команды systemctl start, restart, stop.

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

Посмотреть в journalctl.

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

nmcli connection edit System\ eth0

remove ipv4.dns

set ipv4.ignore-auto-dns yes

set ipv4.dns 127.0.0.1

save

quit

1. Что такое SELinux?

(SELinux) - это модуль безопасности ядра Linux, который обеспечивает механизм поддержки политик безопасности контроля доступа, включая обязательные элементы управления доступом (MAC).

1. Что такое контекст (метка) SELinux?

Каждый файл, процесс, каталог и порт имеют специальную метку безопасности, известную как контекст SELinux, который является именем, используемым для определения, может ли процесс получить доступ к файлу, каталогу или порту.

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

restorecon.

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

Использовать команду chown -R

1. Что такое булевый переключатель в SELinux?\
2. Как посмотреть список переключателей SELinux и их состояние?

Команда getsebool -a | grep named

1. Как изменить значение переключателя SELinux

Необходимо использовать команду setsebool.

**Вывод**

Я установила и сконфигурировала DNS-сервер, и разобрался с основными принципами системы доменных имён.