Лабораторная работа 2

Настройка DNS-сервера

Лушин Артём Андреевич

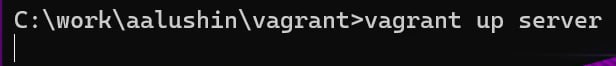
Содержание

# 1 Цель работы

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

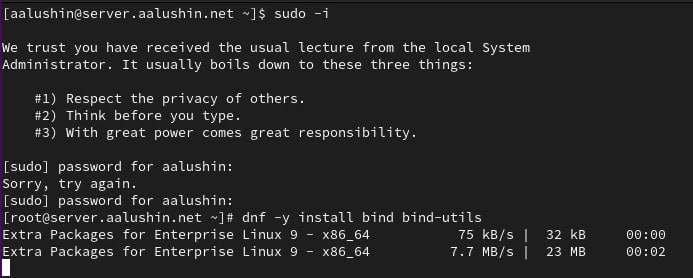
# 2 Выполнение лабораторной работы

1. Я перешёл в каталог vagrant и запустил виртуальную машину server.



Запуск машины

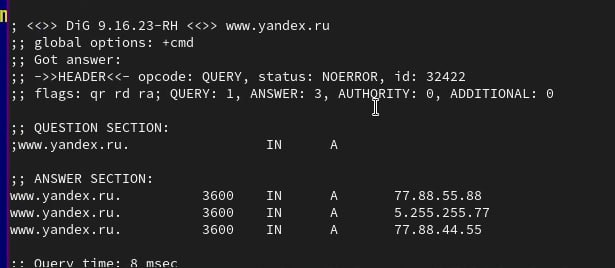
1. Я перешёл в суперпользователя и установил bind и bind-utils.



Установка ПО

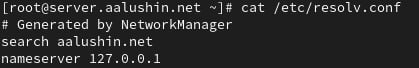
1. Я сделал запрос с DNS-адресу Яндекса. Проанализируем строки вывода:

* HEADER (заголовок): показывает версию dig, глобальные опции используемые с командой и другую дополнительную информацию
* QUESTION SECTION: Показывает наш запрос, то есть мы запросили показать A-запись (команда dig без параметров) для домена www.yandex.ru
* ANSWER SECTION: 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 (8 мс), имя DNS-сервера который запрашивался, когда был создан запрос и размер сообщения



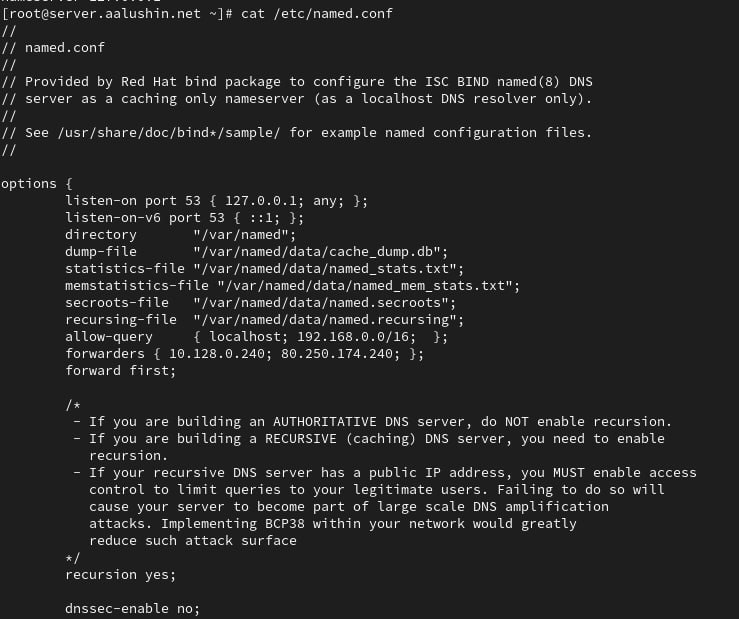
Запрос с яндекс

1. С помощью утилиты проанализируем содержание файла /etc/resolv.conf. Cодержит имя сервера и его адрес Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.



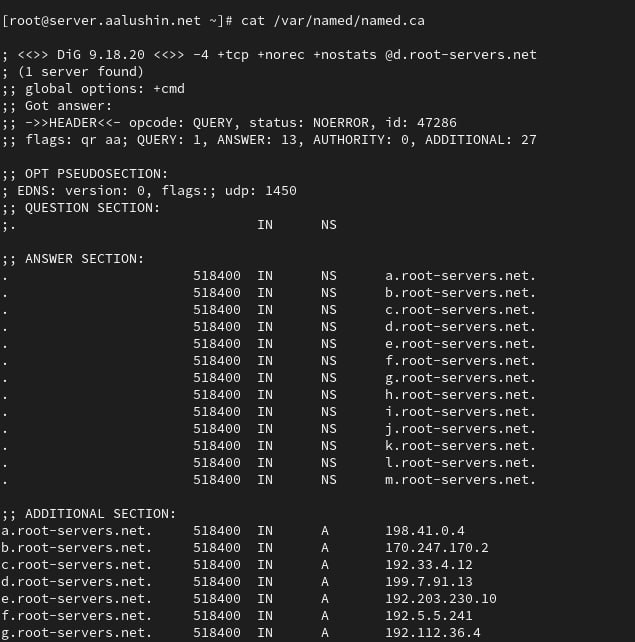
Анализ /etc/resolv.conf

1. С помощью утилиты проанализируем содержание файла /etc/named.conf. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.



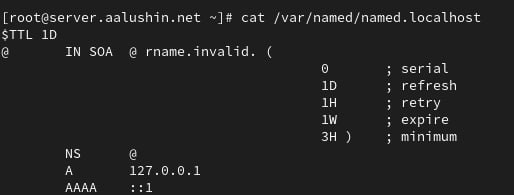
Анализ /etc/named.conf

1. С помощью команды проанализируем содержание файла /var/named/named.ca.Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.



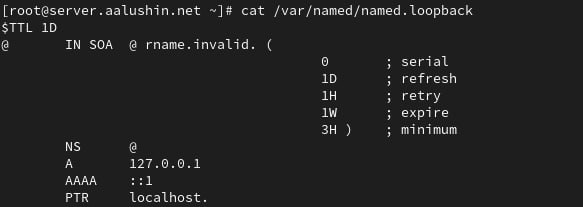
Содержание /var/named/named.ca

1. С помощью команды проанализируем содержание файла /var/named/named.localhost. В данном файле есть следующие строки: запись начала полномочий, которая указывает начало зоны и включает имя хоста на которых находится файл данных. Запись сервера имён, идентифицирующая главный и подчинённый серверы DNS. Указаны IP адреса локального хоста. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.



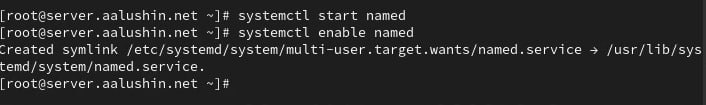
Содержание

1. С помощью утилиты проанализируем содержание файла /var/named/named.loopback. Данный файл практически полностью идентичен как и файл localhost, но добавляется PTR-запись для локального хоста. Фотографии сделаны после выполнения лабораторной, поэтому содержание может отличаться от изначальных скриптов.



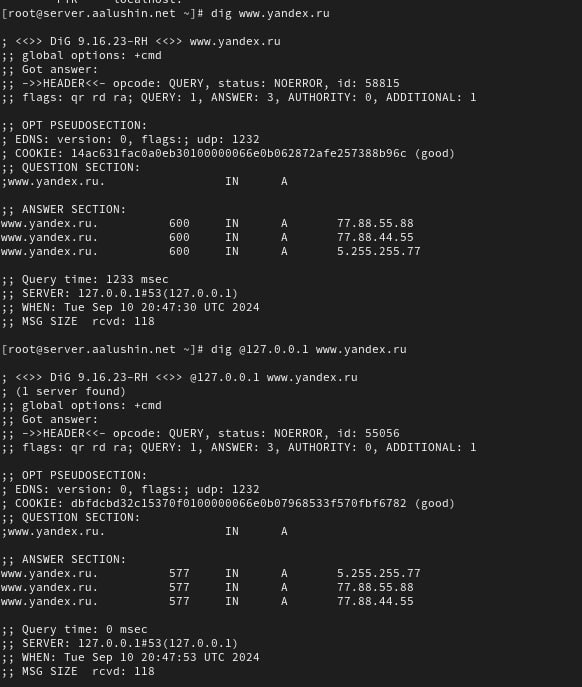
Содержание /var/named/named.loopback

1. Я запустил DNS-сервер и включил автозапуск.



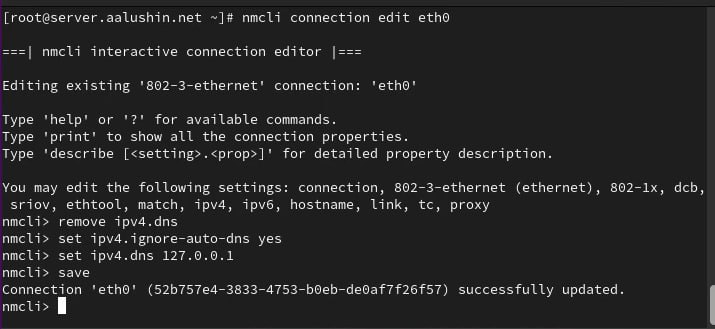
Запуск сервера

1. Сравним вывод информации после анализа www.yandex.ru и 127.0.0.1 www.yandex.ru. При указании запрашиваемого адреса в строке с адресом написан адрес, который указывали, а также куки и увеличилось время запроса.



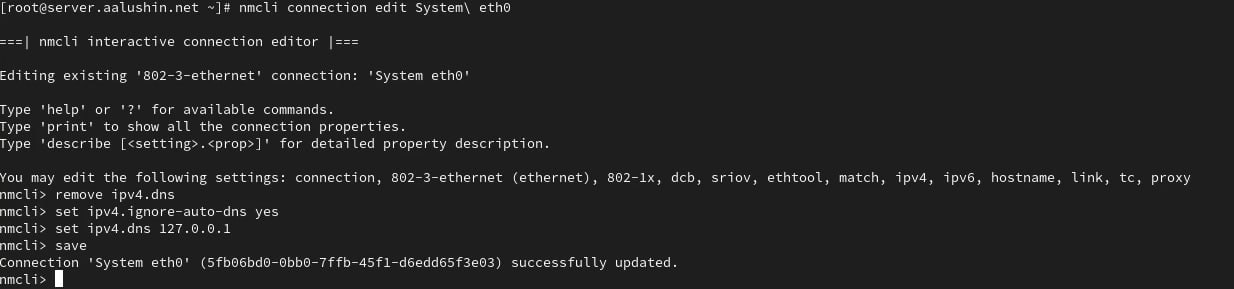
Сравнение яндекса и айпи яндекса

1. Я сделал dns-сервер по умолчанию для хоста сервер и внутренней виртуальной сети.



Сервер по умолчанию

1. Сделал ту же операцию для соединения system eth0.



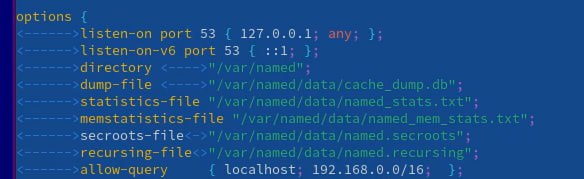
System eth0

1. Перезапустили NetworkManager.

Перезапуск

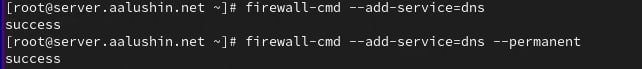
Перезапуск

1. Я настроил направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла сервер, через узел сервер.



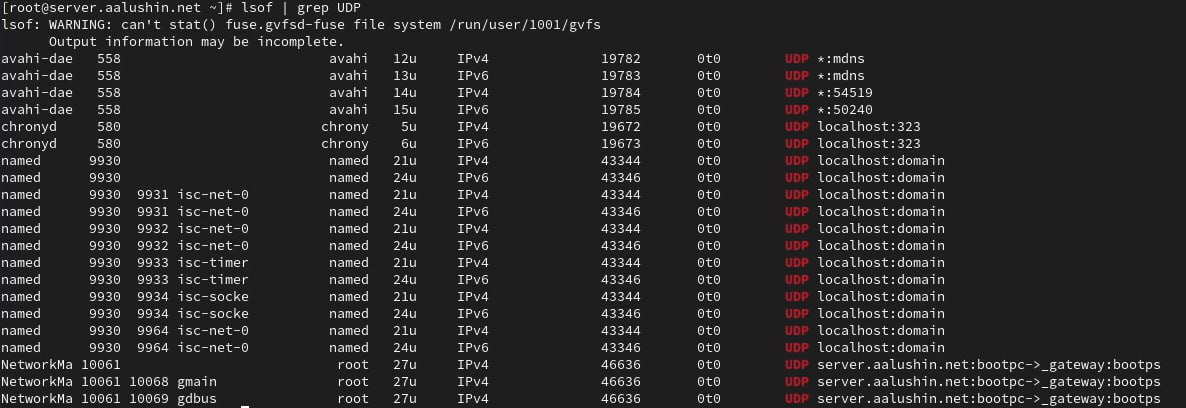
Настройка днс-запросов

1. Внесли изменения в настройки межсетевого экрана узла сервер, разрешив работу с ДНС.

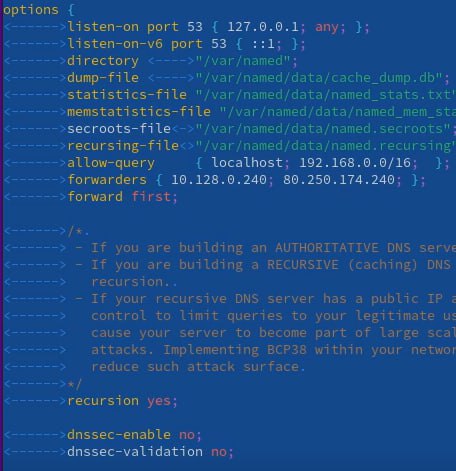


Изменения межсетевого экрана

1. Убедился, что запросы идут через узел сервер, который прослушивает порт 53.

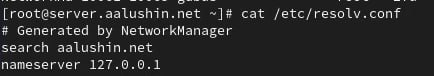


1. Я перенаправил запросы DNS на конкретный сервер и сделал так, чтобы сервер поддерживал запросы.



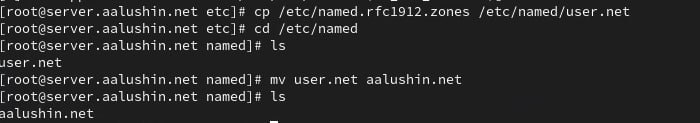
Перенаправление запросов

1. Получил текущие список серверов.



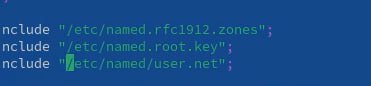
Список серверов

1. Скопировал описание днс-зоны, переместил и переименовал его.



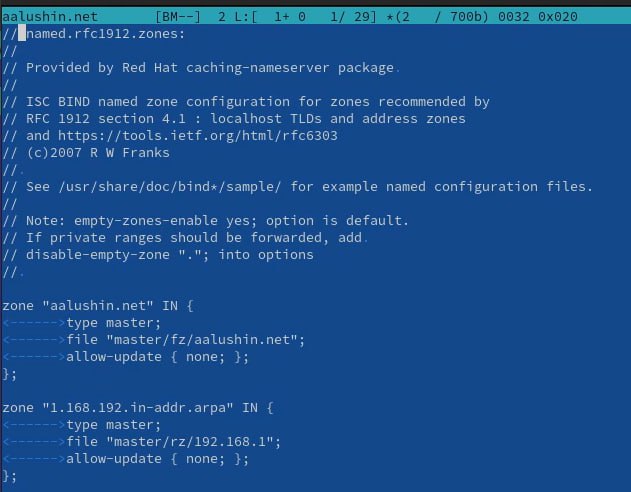
Перенос днс-зоны

1. Включил файл описания днс-зоны в конфигурационный файл.



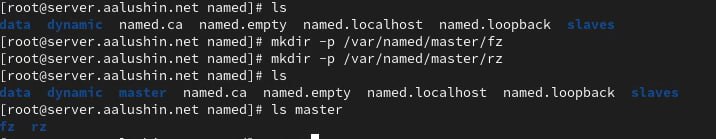
Внос в конфигурационный файл

1. Изменил файл днс-зоны, чтобы он корректно работал.



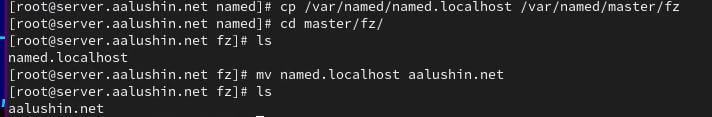
Изменение файла днс-зоны

1. Создал каталоги для обратной fz и rz для файлов прямой и обратной зоны.



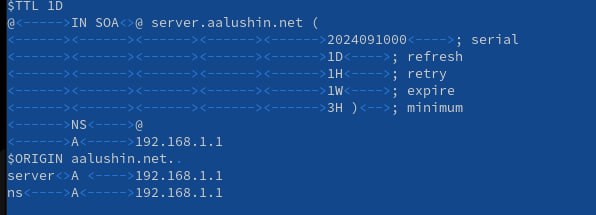
Создание файлов fz и rz

1. Скопировал шаблон для прямой днс-зоны и перенёс в каталог Fz.



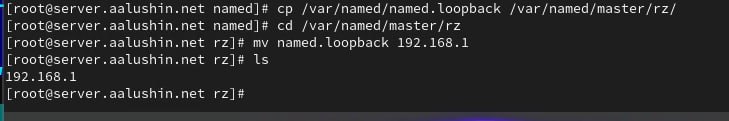
Файл прямой днс-зоны

1. Изменил скрипт файла прямой зоны, чтобы он корректно работал на моей машине.



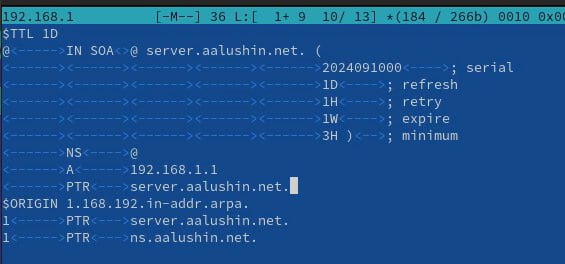
Изменение прямой зоны

1. Скопировал шаблон обратной днс-зоны и перенёс его в каталог rz.



Обратная днс-зоны

1. Изменил скрипт файла обратной зоны, чтобы он корректно работал.



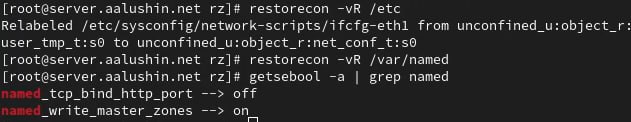
Изменение обратной зоны

1. Изменил права доступа к файлам в каталогах Etc/named u var/named, чтобы файл named мог с ними работать.

Изменение прав

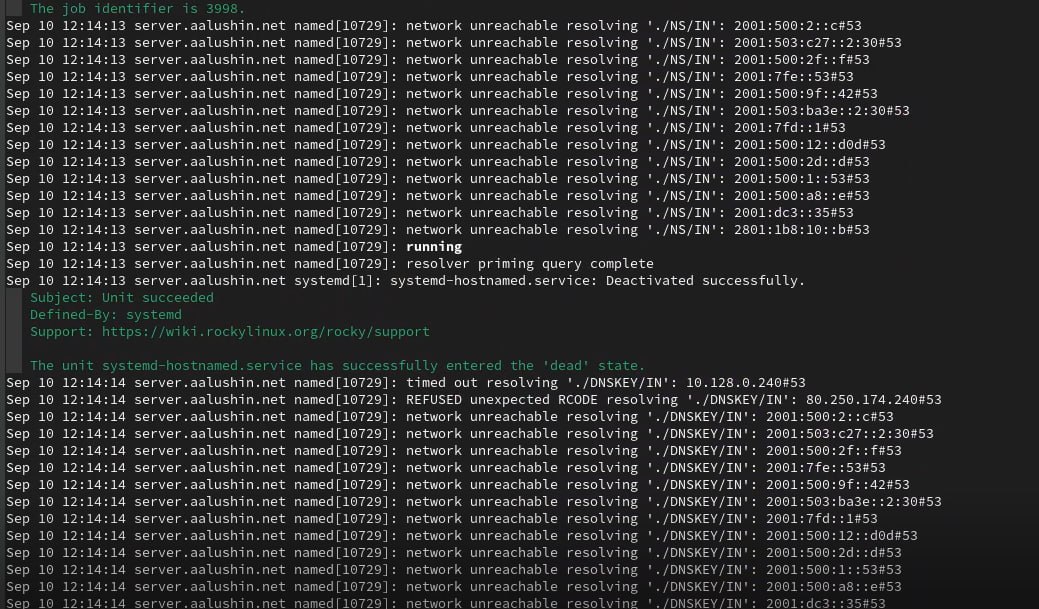
Изменение прав

1. После изменений доступа в конфигурационных файлах корректно восстановили метки безопасности в Selinux. Проверил состояние переключателей.



Восстановление меток

1. Запустил во втором терминале расширенный лог системных сообщений и перезапустил днс-сервер. Проверил на наличие ошибок, ошибок нет.



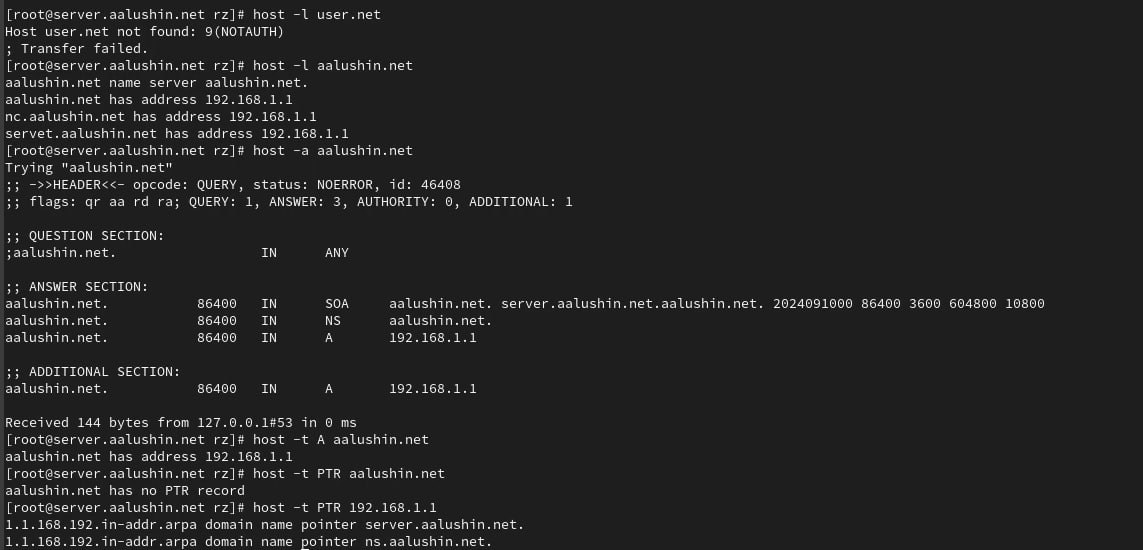
Проверка на наличие ошибок

1. При помощи утилиты получил описание днс-зоны.



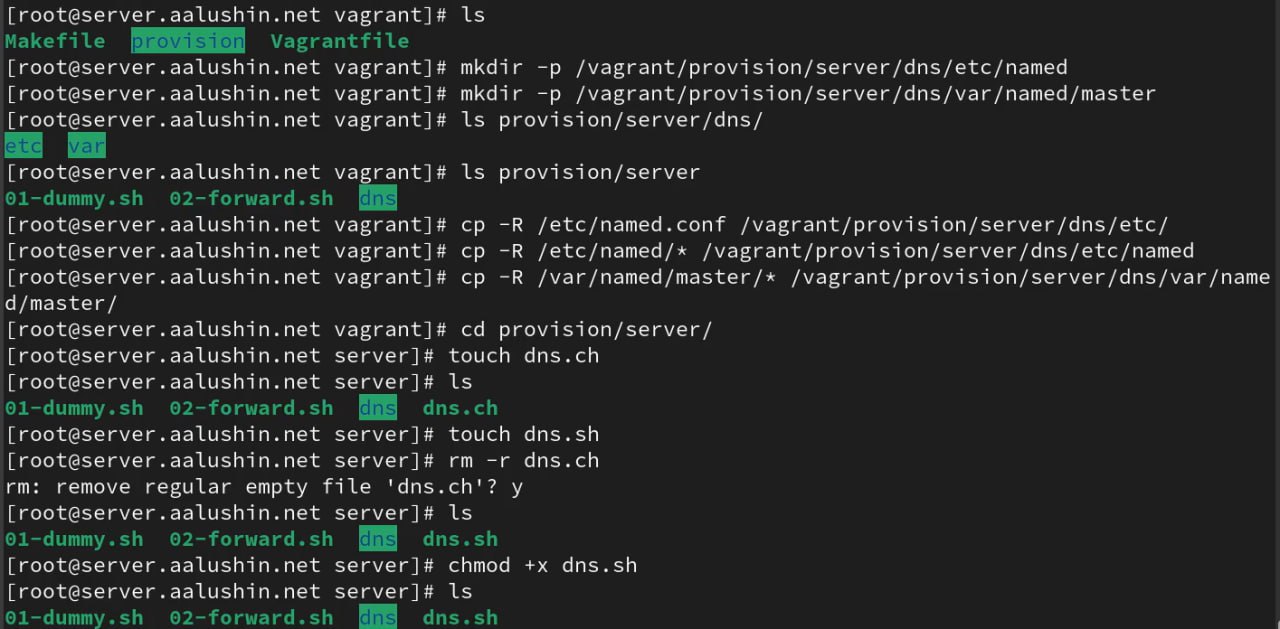
Описание днс-зоны

1. При помощи утилиты host проанализировал корректность работы днс-сервера.



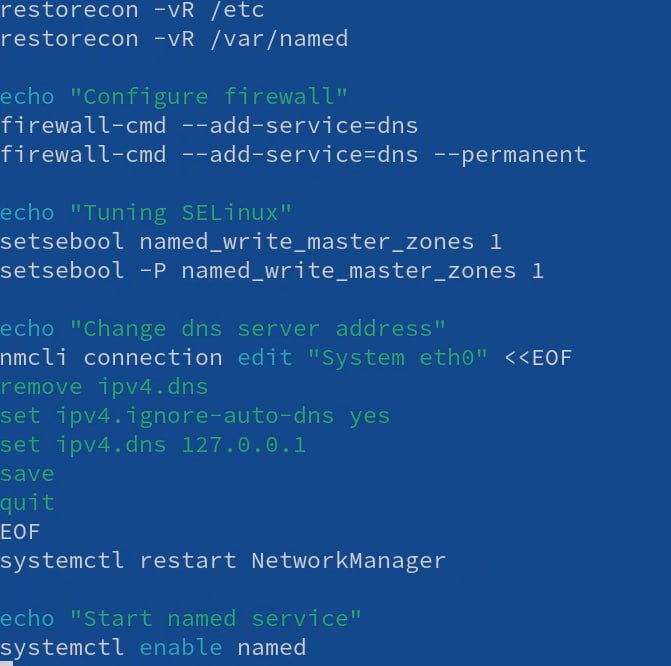
Корректность работы сервера

1. Зашёл в каталог /vagrant/provision/server/, создал подкаталог dns в который поместил соответствующие подкаталоги и конфигурационные файлы.А так же создал исполняющий файл.



размещение файлов на машине

1. Создание скрипта в исполняющем файле dns.



Скрипт в исполняющем файле

1. Чтобы скрипт отрабатывал при запуске машины, внёс изменения в vagrantfile.



Изменение vagrantfile

# 3 Вывод

Я приобрёл практические навыки по установке и конфигурированию DNS-сервера, усвоил принцип работы системы доменных имён.

# 4 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.

1. 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?

* Прямая DNS зона - зона хранения записей соответствия доменного имени ip адресу. Обратная DNS зона - зона хранения записей соответствия ip адреса доменному имени.

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

* В каталоге /etc хранится файл named.conf, в котором есть информация об опциях сервера, его разрешениях, настройках безопасности и подключены файлы зон. В каталоге /named хранится файл описания DNS-зон, также в каталоге /var/named хранится файл named.loopback, описывающий обратную зону, и файл named.localhost, описывающий прямую зону.

1. Что указывается в файле resolv.conf?

* В этом файле указывается имя сервера и его адрес.

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

Основные типы ресурсных записей (Resource Records):

* A-запись — задает преобразование имени хоста в IP-адрес.
* MX-запись — определяет почтовый ретранслятор для доменного имени, т.е. узел, который обработает или передаст дальше почтовые сообщения, предназначенные адресату в указанном домене. При наличии нескольких MX-записей сначала происходит попытка доставить почту на ретранслятор с наименьшим приоритетом.
* NS-записи — определяют DNS-серверы, которые являются авторитативными для данной зоны.
* CNAME-запись — определяет отображение псевдонима в каноническое имя узла.
* SRV-запись — позволяет получить имя для искомой службы, а также протокол, по которому эта служба работает.
* TXT-запись — содержит общую текстовую информацию. Эти записи могут использоваться в любых целях, например, для указания месторасположения хоста.
* AAAA-запись — задает преобразование имени хоста в IPV6-адрес.
* SSHFP-запись — используется для хранения слепка ключей SSH в DNS.

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

* Домен in-addr.arpa используется для всех сетей TCP/IP, основанным на адресации протокола Интернета 4 (IPv4).

1. Для чего нужен демон named?

* Демон named отвечает на запросы об именах машин и их IP-адресах. Если named не знает ответа на какой-либо запрос, он опрашивает другие серверы и помещает их ответы в кэш. Этот демон, кроме того, отвечает за выполнение зонных пересылок, обеспечивающих копирование данных между серверами одного домена. Запросы демона named используют протокол UDP и порт 53. Если объем ответов превышает 512 байтов, то для их доставки используется протокол TCP. В зонных пересылках между серверами также применяется протокол TCP.

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

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

1. Какие параметры отвечают за время обновления зоны?

* SOA-запись (Start of Authority) — начальная запись зоны, которая указывает местоположение эталонной записи о домене. Она хранит параметр TTL – время, в течение которого информация будет кешироваться другими DNS-серверами. Также параметр Refresh – время (в секундах) ожидания ответа вторичного DNS перед запросом SOA-записи с первичных серверов. По истечении данного времени вторичный DNS обращается к первичному для получения копии текущей SOA-записи. Первичный DNS-сервер выполняет этот запрос. Вторичный DNS-сервер сравнивает полученный серийный номер зоны с имеющимся. Если они отличаются, то осуществляется запрос к первичному DNS-серверу на трансфер зоны. И Expire – время (в секундах), в течение которого вторичный DNS будет пытаться завершить синхронизацию зоны с первичным. Если это время истечет до того, как синхронизация закончится, то зона на вторичном DNS-сервере перестанет обслуживать запросы об этой зоне.

1. Как обеспечить защиту зоны от скачивания и просмотра?

Можно делать следующее для защиты данных DNS доменов с помощью DNSSEC:

* Подписывать зоны или удалить подпись в соответствии со спецификациями DNSSEC
* (Необязательно) Указывать индивидуальные настройки для создания ключей
* Получать уведомления
* Просматривать и копировать записи ресурсов DS
* Просматривать и копировать наборы записей ресурсов DNSKEY.

1. Какая запись RR применяется при создании почтовых серверов?

* Заппись MX (от англ. mail exchanger) — тип DNS-записи, предназначенный для маршрутизации электронной почты с использованием протокола SMTP.

1. Как протестировать работу сервера доменных имён?

* Для этого можно воспользоваться командой nslookup, которая позволяет получить информацию о DNS-записях для заданного домена или IP-адреса.

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

* systemctl restart named - перезапустить DNS-сервер
* systemctl stop named - перезапустить DNS-сервер
* systemctl start named - перезапустить DNS-сервер

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

* В дополнительном терминале запуститm в режиме реального времени расширенный лог системных сообщений: journalctl -x -f

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

* Журналы службы находятся в директории “/var/log/” в виде обычных текстовых файлов.

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

* lsof – есокращение от LiSt of Open Files, утилита эта служит для вывода информации о том, какие файлы используются теми или иными процессами. В качестве примера могу привести 16 пункт моей лабораторной работы. Там мы используем команду grep.

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

* В качестве примера могу привести 11 и 12 пункты моей лабораторной.

1. Что такое SELinux?

* SELinux (англ. Security-Enhanced Linux — Linux с улучшенной безопасностью) — реализация системы принудительного контроля доступа, которая может работать параллельно с классической избирательной системой контроля доступа.

1. Что такое контекст (метка) SELinux?

* SELinux — это система принудительного управления доступом, что означает, что каждый процесс имеет метку (label). Каждый файл, каталог и системный объект так же имеют метки. Правила политики управляют доступом между промаркированными процессами и объектами.
* Контекст безопасности — это совокупность всех атрибутов, которые связаны с объектами и субъектами

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

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, надо ввести:

getsebool -a | grep named

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

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

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

* Чтобы создать необходимые политики:

1. Создайте новый файл с исходным кодом политики SELinux (.te файл). Данный файл определяет ограничения, относящиеся к описываемому модулю.
2. При необходимости отредактируйте сгенерированный исходный файл политики [module\_name].te, а затем, используя утилиту checkmodule, создайте бинарное представление (.mod файл) исходного файла локальной политики.
3. Создайте устанавливаемый модуль политики (.pp файл) с помощью утилиты semodule\_package.
4. Для установки созданного модуля политики воспользуйтесь утилитой semodule.
5. Что такое булевый переключатель в SELinux?

* Булевый переключатель в SELinux - это параметр, который управляет разрешениями безопасности на уровне SELinux. Он может быть включен (true) или выключен (false) и используется для разрешения или запрещения определенных действий.

1. Как посмотреть список переключателей SELinux и их состояние?

* Для просмотра списка переключателей SELinux и их состояния можно использовать команду “semanage boolean -l” в терминале.

1. Как изменить значение переключателя SELinux?

* Чтобы изменить значение переключателя SELinux, можно использовать команду “setsebool”. Например, для включения переключателя с именем “httpd\_can\_network\_connect” можно выполнить команду “setsebool -P httpd\_can\_network\_connect 1”. Здесь -P указывает, что изменение должно быть постоянным (постоянно сохраняться после перезагрузки).