Администрирование сетевых подсистем

Лабораторная работа №2

Тойчубекова Асель Нурлановна

Содержание

# 1. Цель работы

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

# 2. Задание

1. Установите на виртуальной машине server DNS-сервер bind и bind-utils.
2. Сконфигурируйте на виртуальной машине server кэширующий DNS-сервер.
3. Сконфигурируйте на виртуальной машине server первичный DNS-сервер.
4. При помощи утилит dig и host проанализируйте работу DNS-сервера.
5. Напишите скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server. Соответствующим образом внесите изменения в Vagrantfile.

# 3. Теоретическое введение

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.

Компоненты:

* DNS-сервер – программа для обслуживания DNS-запросов (чаще BIND).
* DNS-клиент – библиотека или программа для работы с DNS.
* Зона – логический узел в дереве доменов.
* Домен – название зоны.
* Поддомен – подчинённая зона.

Типы DNS-серверов:

* Primary master – основной сервер зоны, читает данные из файла.
* Secondary master – получает данные зоны от primary.
* Кэширующий – обрабатывает рекурсивные запросы клиентов.

Файлы зоны и директивы:

* $ORIGIN – задаёт текущий домен.
* $INCLUDE – включает другой файл в описание зоны.

Записи ресурсов (RR):

* SOA – авторитетная запись зоны, содержит origin, contact, serial, refresh, retry, expire, minimum.
* NS – DNS-серверы зоны.
* A – имя хоста → IP-адрес.
* PTR – IP-адрес → имя хоста.
* CNAME – каноническое имя для псевдонимов.
* MX – почтовые серверы с приоритетом.

Примеры форматов:

* SOA: [zone] [ttl] IN SOA origin contact (serial refresh retry expire minimum)
* NS: [domain] [ttl] IN NS [server]
* A: [host] [ttl] IN A [address]
* PTR: [name] [ttl] IN PTR [host]
* MX: [name] [ttl] IN MX [preference] [host]
* CNAME: [nickname] [ttl] IN CNAME [host]

Утилита dig (domain information groper) предоставляет пользователю интерфейс командной строки для обращения к системе DNS, позволяет формировать запросы о доменах DNS-серверам. Утилита dig входит в стандартный комплект DNS сервера BIND.

Утилита host предназначена для выполнения запросов к DNS-серверам.

# 4. Выполнение лабораторной работы

Для начала выполнения второй лабораторной работы запустить виртуальную машину server. На виртуальной машине server вхожу под созданным предыдущей работе пользователем, antoychubekova и открываю терминал и перехожу в режим суперпользователя ([рис. 1](#fig-001)).

|  |
| --- |
| Рисунок 1: Переход в режим суперпользователя |

Устанавливаю bind и bind-utils. ([рис. 2](#fig-002)).

|  |
| --- |
| Рисунок 2: Установка bind |

В качестве упражнения с помощью утилиты dig делаю запрос, к DNS-адресу www.yandex.ru.

В первой строке указывается версия утилиты DiG 9.18.33 и сам домен, к которому выполняется запрос. Далее сообщается, что ответ получен, в заголовке видно, что это был обычный запрос (QUERY) со статусом NOERROR (ошибок нет), и указан идентификатор запроса. Флаги показывают, что это ответ (qr), была запрошена рекурсия (rd), и сервер её поддерживает (ra). Также указано, что в ответе одна секция запроса, три записи-ответа и одна дополнительная.

В блоке OPT PSEUDOSECTION видно, что используется расширение EDNS(0) версии 0, без дополнительных флагов, а максимальный размер UDP-пакета — 1232 байта. В секции QUESTION повторяется сам запрос: домен www.yandex.ru и тип записи A (IPv4-адрес).

В ANSWER SECTION приходят три результата: www.yandex.ru сопоставлен с IP-адресами 77.88.55.88, 77.88.44.55 и 5.255.255.77, каждая запись имеет TTL 600 секунд (10 минут), то есть столько времени она может храниться в кэше.

В дополнительной информации указывается, что запрос занял 329 мс, ответ пришёл от DNS-сервера 213.186.33.99 (порт 53, UDP). Также зафиксировано точное время выполнения запроса — 11 сентября 2025 года, 11:10:30 (UTC). Размер полученного сообщения составил 90 байт. ([рис. 3](#fig-003)).

|  |
| --- |
| Рисунок 3: Утилита dig |

Открываю файл /etc/resolv.conf.

Файл /etc/resolv.conf задаёт настройки DNS для системы: в нём указываются адреса DNS-серверов (nameserver), к которым компьютер обращается для преобразования доменных имён в IP-адреса (по порядку, пока один не ответит), и домен поиска (search antoychubekova.net), который автоматически добавляется к коротким именам хостов. ([рис. 4](#fig-004)).

|  |
| --- |
| Рисунок 4: Файл /etc/resolv.conf |

Открываю файл named.conf.

Этот файл named.conf — конфигурация DNS-сервера BIND. В нём указано, что сервер слушает запросы только на локальных адресах 127.0.0.1 (IPv4) и ::1 (IPv6), то есть работает как локальный кэширующий резолвер. Заданы служебные файлы: директория для работы /var/named, файлы для дампов кэша, статистики, памяти и ключей, а также файл для рекурсивных запросов. В настройке allow-query { localhost; }; указано, что отвечать на DNS-запросы сервер будет только самому себе (локальной машине). Включена опция recursion yes;, что делает сервер рекурсивным кэширующим DNS, пригодным для локального разрешения имён, и включена проверка DNSSEC (dnssec-validation yes;) для дополнительной безопасности. ([рис. 5](#fig-005)).

|  |
| --- |
| Рисунок 5: Файл named.conf |

Открываю файл named.ca.

Этот файл named.ca содержит список корневых DNS-серверов Интернета (root servers), необходимых для инициализации работы DNS-сервера BIND: он задаёт, какие серверы считаются корневыми и по каким IP-адресам (IPv4 и IPv6) их можно достичь. Благодаря этому DNS-сервер знает, с чего начинать поиск доменов в глобальной сети. ([рис. 6](#fig-006)).

|  |
| --- |
| Рисунок 6: Файл named.ca |

Открываю файл named.localhost.

Этот файл named.localhost описывает зону DNS для домена localhost. В нём задаётся основная запись SOA (Start of Authority) с параметрами обновления зоны и фиктивным адресом администратора (rname.invalid.), а также указываются записи: NS (сервер имён — сам localhost), A (IPv4-адрес 127.0.0.1) и AAAA (IPv6-адрес ::1). Таким образом, он нужен для того, чтобы DNS-сервер BIND правильно обрабатывал запросы к имени localhost и всегда резолвил его в локальный адрес. ([рис. 7](#fig-007)).

|  |
| --- |
| Рисунок 7: Файл named.localhost |

Открываю файл named.loopback.

Этот файл named.loopback описывает обратную (reverse) DNS-зону для интерфейса loopback. В нём задаётся запись SOA (Start of Authority) с параметрами зоны, указывается, что сервер имён (NS) — это сам localhost, и определяются адреса: A (127.0.0.1 для IPv4) и AAAA (::1 для IPv6). Дополнительно здесь есть запись PTR, которая обеспечивает обратное преобразование IP-адреса 127.0.0.1 в имя localhost. То есть этот файл нужен, чтобы при обратных DNS-запросах (по IP) адрес loopback корректно резолвился в localhost. ([рис. 8](#fig-008)).

|  |
| --- |
| Рисунок 8: Файл named.loopback |

Запускаю DNS-сервер. Включаю запуск днс-сервера в авозапуск при загрузки системы. ([рис. 9](#fig-009)).

|  |
| --- |
| Рисунок 9: Запуск DNS-сервера |

Ввожу в команду dig [**127.0.0.1?**] www.yandex.ru. dig www.yandex.ru показывает работу с внешним DNS (сразу из resolv.conf), а dig [**127.0.0.1?**] www.yandex.ru — проверку твоего локального BIND как резолвера. В твоём случае оба возвращают одинаковые IP-адреса Яндекса, но второй запрос идёт через твой сервер, а не напрямую к провайдерскому DNS. ([рис. 10](#fig-010)).

|  |
| --- |
| Рисунок 10: Вывод ig [**127.0.0.1?**] www.yandex.ru. |

Делаю DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети. Для этого изменяю 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. 11](#fig-011)).

|  |
| --- |
| Рисунок 11: DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети |

Делаю тоже самое для соединения System eth0. Оно у нас не активно. ([рис. 12](#fig-012)).

|  |
| --- |
| Рисунок 12: DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети |

Перезапускаю NetworkManager. Проверяю наличие изменений в файле /etc/resolv.conf. ([рис. 13](#fig-013)).

|  |
| --- |
| Рисунок 13: Перезапуск NetworkManager |

Настраиваю направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server. Для этого вношу 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. 14](#fig-014)).

|  |
| --- |
| Рисунок 14: Настройка направление DNS-запросов |

Вношу изменение в настройки межсетевого экрана узла server, разрешив работу с DNS. ([рис. 15](#fig-015)).

|  |
| --- |
| Рисунок 15: Внесение изменений |

Введя команду lsof | grep UDP мы убедились что DNS-запросы идут через узел server, который прослушивает порт 53. ([рис. 16](#fig-016)).

|  |
| --- |
| Рисунок 16: Проверка DNS-запросов |

В случае возникновения в сети ситуаций, когда DNS-запросы от сервера фильтруются сетевым оборудованием, следует добавить перенаправление DNS-запросов на конкретный вышестоящий DNS-сервер. Для этого в конфигурационном файле named.conf в секции option следует добавить:

forwarders { список DNS-серверов };

forward first;

Возможно вышестоящий DNS-сервер может не поддерживать технологию dnssec, из за этого в конфигурационном файлике указываю следующие настройки:

dnssec-enable no;

dnssec-validation no; ([рис. 17](#fig-017)).

|  |
| --- |
| Рисунок 17: Перенаправление DNS-запросов |

Копирую шаблон описания DNS-зон named.rfc1912.zone из каталога /etc в каталог /etc/named и переименовываю его в antoyxhubekova.net. ([рис. 18](#fig-018)).

|  |
| --- |
| Рисунок 18: Редактирование файлов |

Включаю файл описания зоны /etc/named/antoychubekova.net в конфигурационном файле DNS /etc/named.conf, добавив в нём в конце строку:

include “/etc/named/antoychubekova.net”; ([рис. 19](#fig-019)).

|  |
| --- |
| Рисунок 19: Включение файла описания зоны /etc/named/antoychubekova.net |

Открываю файл /etc/named/antoychubekova.net на редактирование и записываю:

zone “antoychubekova.net” IN {

type master;

file “master/fz/antoychubekova.net”;

allow-update { none; };

};

zone “1.168.192.in-addr.arpa” IN {

type master;

file “master/rz/192.168.1”;

allow-update { none; };

}; ([рис. 20](#fig-020)).

|  |
| --- |
| Рисунок 20: Редактирование /etc/named/antoychubekova.net |

В каталоге /var/named создаю подкаталоги master/fz и master/rz, в которых будут располагаться файлы прямой и обратной зоны соответственно. ([рис. 21](#fig-021)).

|  |
| --- |
| Рисунок 21: Редактирование /var/named |

Копирую шаблон прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и переименовываю его в antoychubekova.net. ([рис. 22](#fig-022)).

|  |
| --- |
| Рисунок 22: Копирование шаблон прямой DNS-зоны |

Изменяю файл /var/named/master/fz/antoychubekova.net, указав необходимые DNS-записи для прямой зоны. В этом файле DNS-имя сервера @ rname.invalid. заменыю на @ server.antoychubekova.net. ; формат серийного номера ГГГГММДДВВ (2025091100); адрес в A-записи заменяю с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN задаю текущее имя домена antoychubekova.net., а затем указываю имена и адреса серверов в этом домене в виде A-записей DNS. ([рис. 23](#fig-023)).

|  |
| --- |
| Рисунок 23: Редактирование /var/named/master/fz/antoychubekova.net |

Копирую шаблон обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и переминовываю его в 192.168.1 ([рис. 24](#fig-024)).

|  |
| --- |
| Рисунок 24: Копирование шаблон обратной DNS-зоны named.loopback |

Изменяю файл /var/named/master/rz/192.168.1, указав необходимые DNS-записи для обратной зоны. В этом файле DNS-имя сервера @ rname.invalid. заменяю на @ server.user.net. ; формат серийного номера ГГГГММДДВВ (2025091100); адрес в A-записи заменяю с 127.0.0.1 на 192.168.1.1; в директиве $ORIGIN задаю название обратной зоны в виде 1.168.192.in-addr.arpa., затем задаю PTR-записи. ([рис. 25](#fig-025)).

|  |
| --- |
| Рисунок 25: Редактирование /var/named/master/rz/192.168.1 |

Далее исправляю права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать. ([рис. 26](#fig-026)).

|  |
| --- |
| Рисунок 26: Изменение прав доступа к /etc/named и /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 корректно восстанавливаю их метки в SELinux. ([рис. 27](#fig-027)).

|  |
| --- |
| Рисунок 27: Корректное восстановление меток в SELinux |

Для проверки состояния переключателей SELinux, относящихся к named, ввожу: getsebool -a | grep named. ([рис. 28](#fig-028)).

|  |
| --- |
| Рисунок 28: Состояния переключателей SELinux |

Даю named разрешение на запись в файлы DNS-зоны. ([рис. 29](#fig-029)).

|  |
| --- |
| Рисунок 29: Предоставление разрешения на запись в файлы DNS-зоны |

В дополнительном терминале запускаю в режиме реального времени расширенный лог системных сообщений, чтобы проверить корректность работы системы. Мы видим, что корректно отрабатывается. ([рис. 30](#fig-030)).

|  |
| --- |
| Рисунок 30: Проверка корректности работы системы |

В первом терминале перезапускаю DNS-сервер. При помощи утилиты dig получаю описание DNS-зоны с сервера ns.antoychubekova.net. В выводе видно, что запрос успешно обработан (status: NOERROR) и возвращён авторитетный ответ (aa — authoritative answer) от вашего локального DNS-сервера на 127.0.0.1. В разделе ответа указано, что ns.antoychubekova.net имеет A-запись с адресом 192.168.1.1, TTL установлен на 86400 секунд (1 день). Время обработки запроса составило 2 мс, что подтверждает, что локальный сервер функционирует корректно и возвращает IP для указанного имени. ([рис. 31](#fig-031)).

|  |
| --- |
| Рисунок 31: Описание DNS-зоны с сервера ns.antoychubekova.net |

При помощи утилиты host проанализирую корректность работы DNS-сервера.

В выводе команды host -l antoychubekova.net видно, что указаны следующие записи: основной сервер имени antoychubekova.net и его IP 192.168.1.1, а также дополнительные записи ns.antoychubekova.net и server.antoychubekova.net, все с тем же IP 192.168.1.1. Это говорит о том, что локальный DNS-сервер правильно отвечает на запросы и возвращает все настроенные записи зоны. ([рис. 32](#fig-032)).

|  |
| --- |
| Рисунок 32: Корректность работы DNS-сервера |

Команда host a antoychubekova.net, которая по сути запрашивает все записи (ANY) для домена antoychubekova.net. В выводе видно, что сервер вернул статус NOERROR, что означает успешное выполнение запроса. В разделе ответа содержатся три записи: SOA (Start of Authority) с корректными параметрами зоны, NS-запись, указывающая на сам домен как сервер имён, и A запись с IP 192.168.1.1. Время ответа составило 8 мс, и ответ получен от локального сервера 127.0.0.1. Это говорит о том, что локальный DNS-сервер BIND работает корректно. ([рис. 33](#fig-033)).

|  |
| --- |
| Рисунок 33: Корректность работы DNS-сервера |

Команда host -t A antoychubekova.net возвращает, что antoychubekova.net имеет адрес 192.168.1.1. Значит все корректно отрабатывается. ([рис. 34](#fig-034)).

|  |
| --- |
| Рисунок 34: Корректность работы DNS-сервера |

В ответе сервер возвращает две PTR-записи: ns.antoychubekova.net и server.antoychubekova.net. Технически это означает, что обратное разрешение работает — IP связан с доменными именами. ([рис. 35](#fig-035)).

|  |
| --- |
| Рисунок 35: Корректность работы DNS-сервера |

На виртуальной машине server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, и создаю в нём каталог dns, в который помещаю в соответствующие каталоги конфигурационные файлы DNS. ([рис. 36](#fig-036)).

|  |
| --- |
| Рисунок 36: Редактирование конфигурационных файлов DNS |

В каталоге /vagrant/provision/server создаю исполняемый файл dns.sh. ([рис. 37](#fig-037)).

|  |
| --- |
| Рисунок 37: Создание исполняемого файла dns.sh |

Открыв его на редактирование, пропишите в нём скрипт, по сути, повторяющий произведённые выше действия по установке и настройке DNS-сервера: подставляет в нужные каталоги подготовленные конфигурационные файлы; меняет соответствующим образом права доступа, метки безопасности SELinux и правила межсетевого экрана; настраивает сетевое соединение так, чтобы сервер выступал DNS-сервером по умолчанию для узлов внутренней виртуальной сети; запускает DNS-сервер. ([рис. 38](#fig-038)).

|  |
| --- |
| Рисунок 38: Редактирование исполняемого файла dns.sh |

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

server.vm.provision “server dns”,

type: “shell”,

preserve\_order: true,

path: “provision/server/dns.sh” ([рис. 39](#fig-039)).

|  |
| --- |
| Рисунок 39: Редактирование Vagrantfile |

# 5. Выводы

В ходе выполнения лабораторной работы №2 я приобрела практические навыки по установке и конфигурированию DNS-сервера, усвоила принцип работы системы доменных имён.

# Список литературы

1. Barr D. Common DNS Operational and Configuration Errors: RFC / RFC Editor. —02/1996. — DOI: 10.17487/rfc1912.
2. Security-Enhanced Linux. Linux с улучшенной безопасностью: руководство пользователя / M. McAllister, S. Radvan, D. Walsh, D. Grift, E. Paris, J. Morris. — URL: https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced\_Linux/index.html (дата обр.13.09.2021).
3. Systemd. — 2015. — URL: https:/ /wiki .archlinux .org /index .php /Systemd (visited on 09/13/2021).
4. Костромин В. А. Утилита lsof — инструмент администратора. — URL: http : / / rus linux.net/kos.php?name=/papers/lsof/lsof.html (дата обр. 13.09.2021).
5. Поттеринг Л. Systemd для администраторов: цикл статей. — 2010. — URL: http : wiki.opennet.ru/Systemd (дата обр. 13.09.2021).
6. Сайт проекта NetworkManager. — URL: https : / / wiki . gnome . org / Projects / NetworkManager (visited on 09/13/2021).
7. Сайт проекта nmcli. — URL: https://developer.gnome.org/NetworkManager/stable/ nmcli.html (visited on 09/13/2021).