Отчёт по лабораторной работе 2

Настройка DNS-сервера

Метвалли Ахмед Фарг Набеех

Содержание

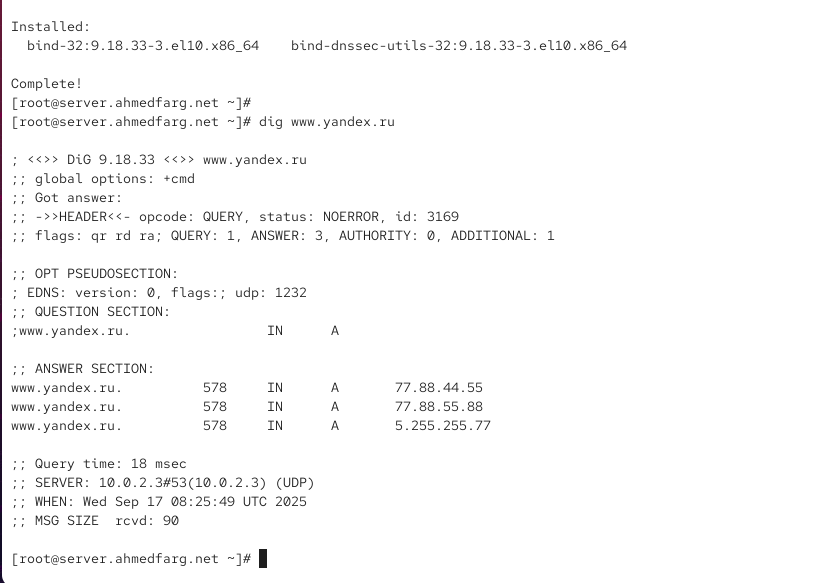
# 1 Цель работы

Приобрести практические навыки по установке и конфигурации DNS-сервера, а также закрепить теоретические знания о принципах работы системы доменных имен.

# 2 Выполнение

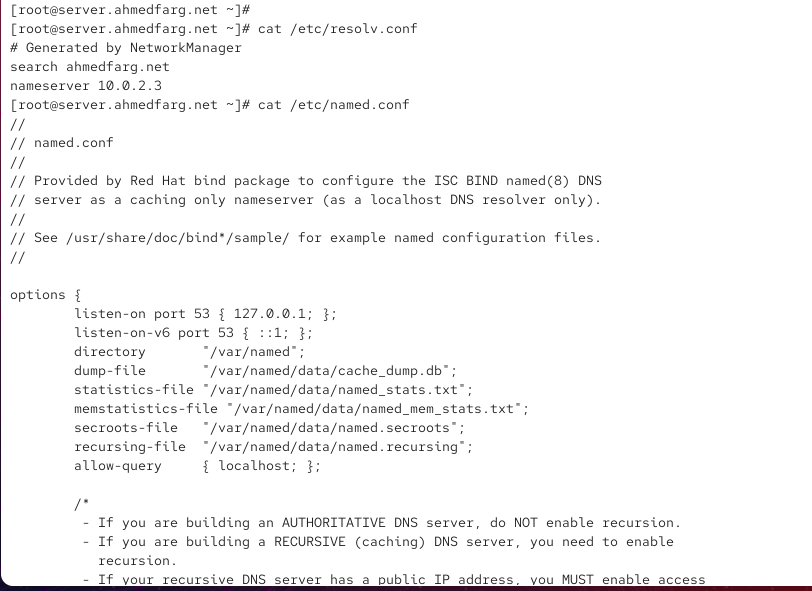
## 2.1 Установка и первичная проверка DNS-сервера

1. На виртуальной машине server установлен пакет **bind** и утилиты для работы с DNS.
2. С помощью команды **dig** выполнен тестовый запрос к DNS-адресу www.yandex.ru.  
   На экране отобразилась структура ответа: заголовок, вопрос, секция ответа с IP-адресами.

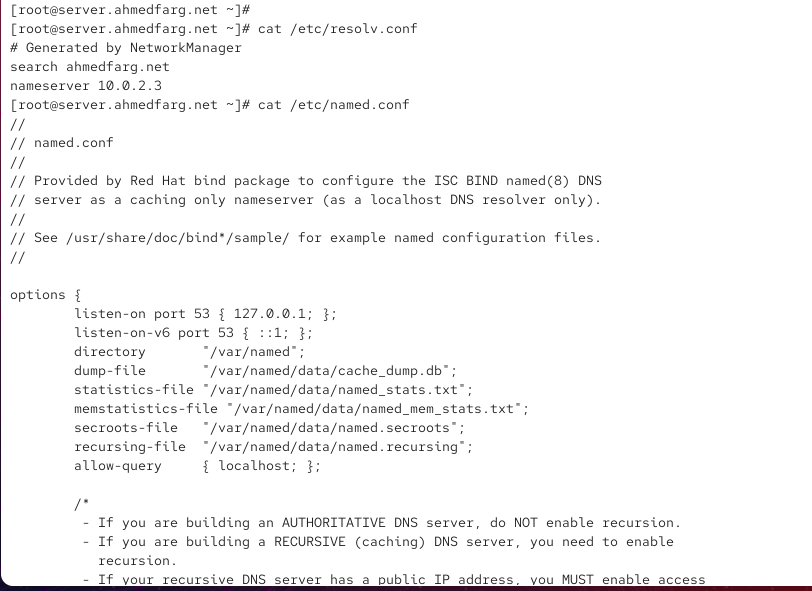
* 
* Рис. 1: Результат dig www.yandex.ru

## 2.2 Конфигурация DNS-сервера

1. Содержимое файла /etc/resolv.conf показывает, что ранее использовался внешний DNS (10.0.2.3).

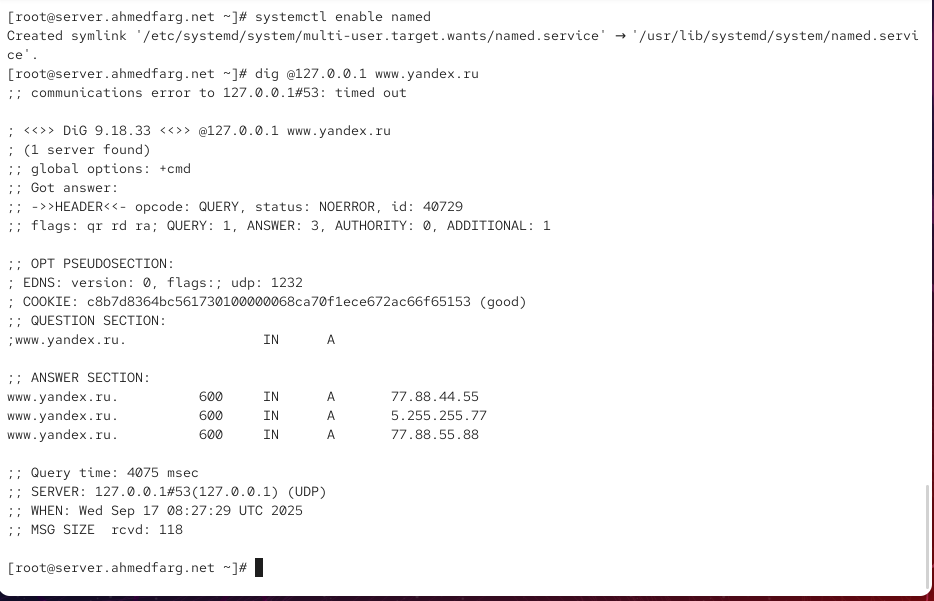
* 
* Рис. 2: Файл resolv.conf

1. В файле /etc/named.conf заданы параметры работы DNS-сервера:
   * слушает порт 53 на 127.0.0.1,
   * указывает путь для хранения кэша и статистики,
   * разрешает запросы только с localhost.

* 
* Рис. 3: Файл named.conf (начальная конфигурация)

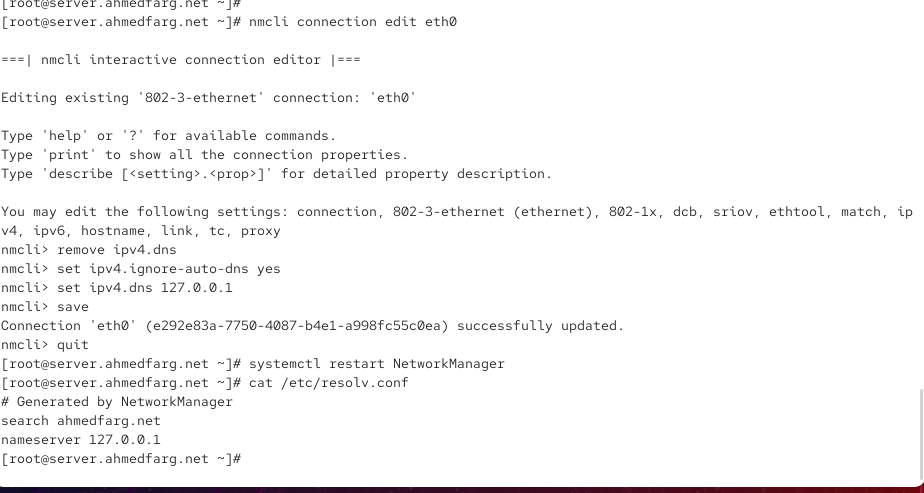
## 2.3 Запуск и тестирование работы

1. Сервис named добавлен в автозагрузку и запущен.
2. Проверка через dig показала отличие в результатах при запросе напрямую (dig www.yandex.ru) и через локальный сервер (dig @127.0.0.1 www.yandex.ru).  
   Ответ от локального DNS имеет увеличенное время запроса, так как данные кэшируются впервые.

* 
* Рис. 4: Результаты dig с локальным сервером

## 2.4 Настройка DNS по умолчанию для хоста

1. Через nmcli выполнены изменения конфигурации соединения eth0:
   * отключён авто-DNS,
   * в качестве сервера указан 127.0.0.1.

* 
* Рис. 5: Настройка DNS в NetworkManager

1. После перезапуска NetworkManager в файле /etc/resolv.conf появился новый nameserver — 127.0.0.1.

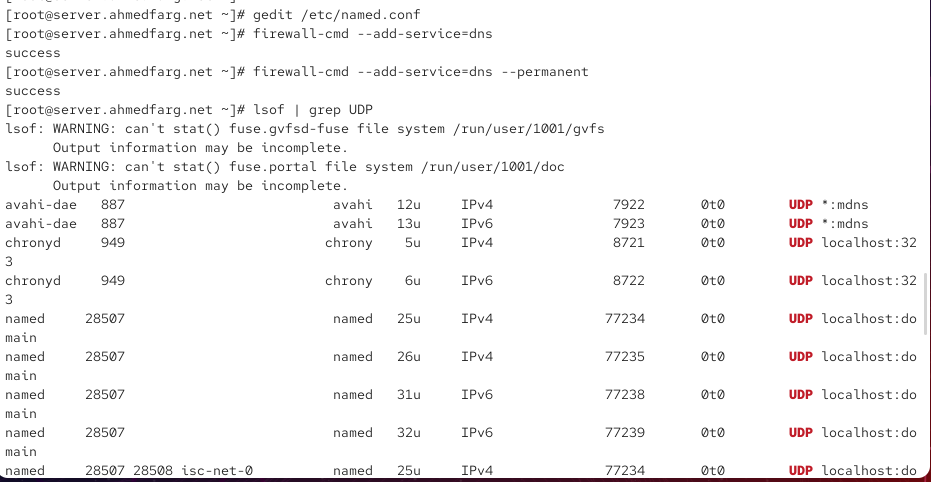
## 2.5 Разрешение запросов от внутренних узлов

1. В файле /etc/named.conf внесены изменения:
   * listen-on port 53 { 127.0.0.1; any; }; — разрешено прослушивание всех интерфейсов,
   * allow-query { localhost; 192.168.0.0/16; }; — разрешены запросы от внутренней сети.

* 
* Рис. 6: Файл named.conf (доработанный)

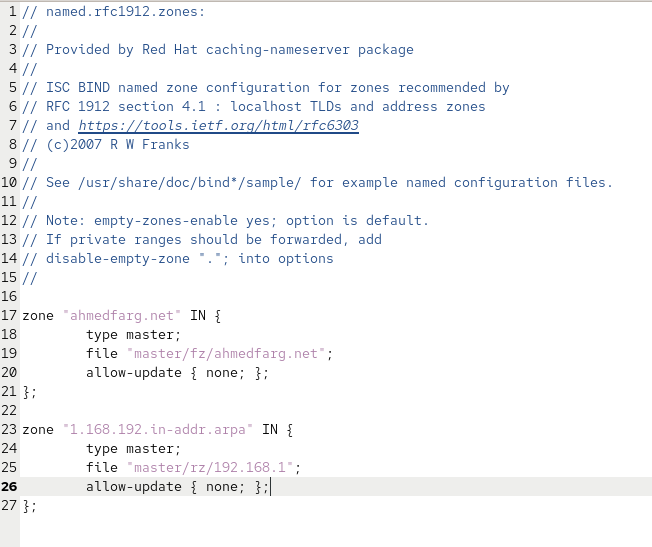
## 2.6 Настройка firewall и проверка

1. Внесены изменения в правила брандмауэра для разрешения работы службы DNS.
2. Проверка через lsof подтвердила, что процесс **named** прослушивает порт 53 по протоколу UDP.

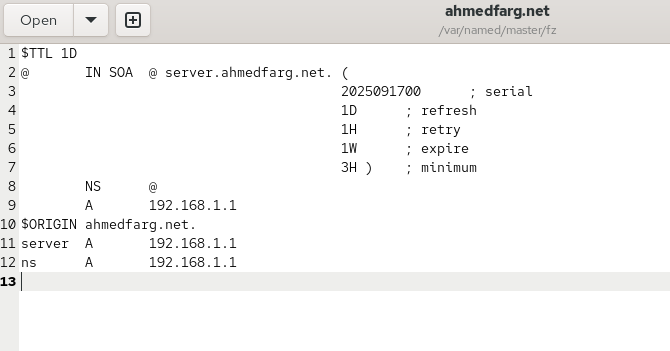
* 
* Рис. 7: Проверка через lsof

## 2.7 Конфигурирование первичного DNS-сервера

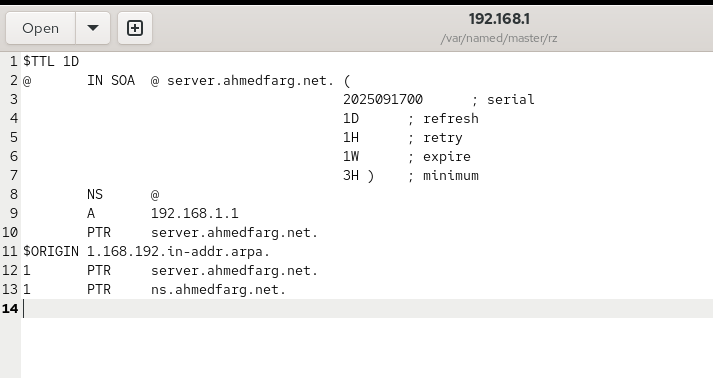
1. На основе шаблона named.rfc1912.zones создан новый файл описания зон user.net.  
   В конфигурационном файле /etc/named.conf подключён данный файл с помощью директивы include.

* 
* Рис. 8: Файл user.net с описанием зон

1. Для прямой зоны ahmedfarg.net создан файл /var/named/master/fz/ahmedfarg.net.  
   В нём определены:
   * SOA-запись с главным сервером server.ahmedfarg.net,
   * NS-запись,
   * A-записи для узлов server и ns, указывающие на 192.168.1.1.

* 
* Рис. 9: Прямая зона ahmedfarg.net

1. Для обратной зоны 1.168.192.in-addr.arpa создан файл /var/named/master/rz/192.168.1.  
   В нём заданы:
   * SOA-запись,
   * NS-запись,
   * PTR-записи, сопоставляющие IP-адрес 192.168.1.1 с именами server.ahmedfarg.net и ns.ahmedfarg.net.

* 
* Рис. 10: Обратная зона 192.168.1

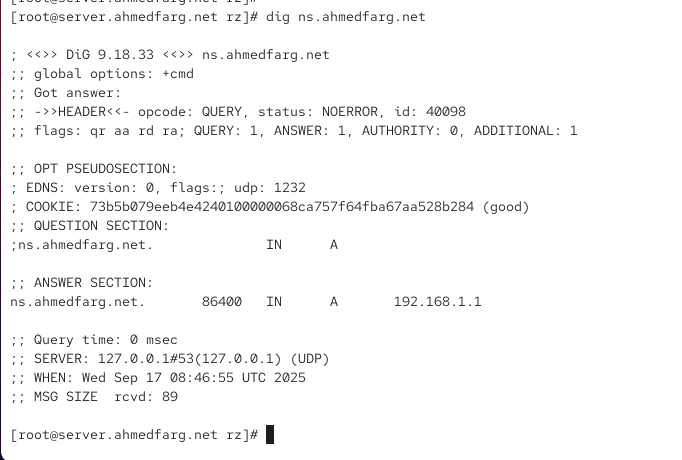
1. Для корректной работы демона **named** были исправлены права доступа и SELinux-контексты:
   * рекурсивно изменены владельцы каталогов /etc/named и /var/named на named:named,
   * выполнено восстановление контекстов командой restorecon,
   * включён параметр SELinux named\_write\_master\_zones.

* 
* Рис. 11: Настройка прав и SELinux для named

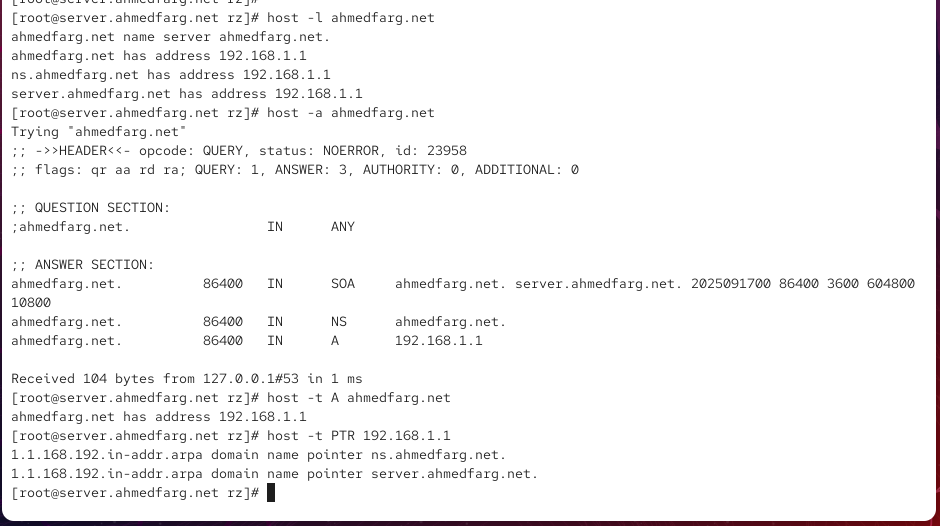
1. После внесённых изменений сервис named был перезапущен. Ошибки при проверке логов отсутствуют, зоны были загружены успешно.

## 2.8 Анализ работы DNS-сервера

1. С помощью утилиты dig был выполнен запрос к серверу ns.ahmedfarg.net.  
   Ответ показал, что доменное имя ns.ahmedfarg.net корректно сопоставляется с адресом 192.168.1.1.

* 
* Рис. 12: Результат dig ns.ahmedfarg.net

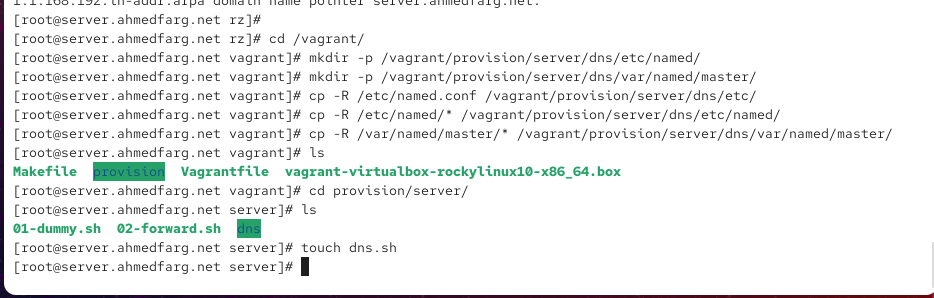
1. С помощью утилиты host проведён анализ зоны ahmedfarg.net:
   * перечислены все записи зоны (A, NS, SOA),
   * подтверждено наличие привязки имени ahmedfarg.net к адресу 192.168.1.1,
   * проверены обратные PTR-записи для IP-адреса 192.168.1.1.

* 
* Рис. 13: Анализ зоны через host

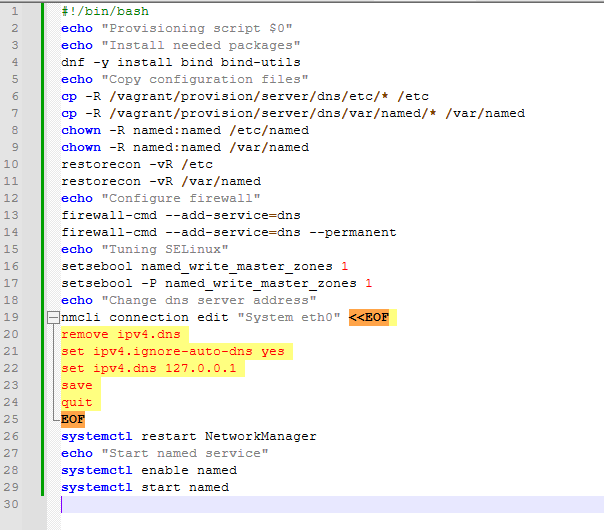
Результаты подтверждают корректную работу как прямой, так и обратной зон.

## 2.9 Внесение изменений в настройки окружения

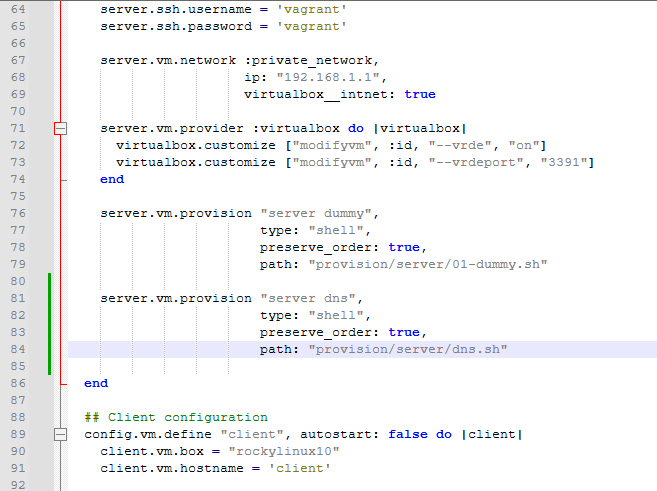
1. В каталоге /vagrant/provision/server/ создан подкаталог dns, куда были помещены конфигурационные файлы DNS.

* 
* Рис. 14: Подготовка каталогов для DNS

1. В каталоге /vagrant/provision/server/ создан исполняемый скрипт dns.sh.  
   В нём описаны:
   * установка необходимых пакетов (bind, bind-utils),
   * копирование конфигурации,
   * настройка владельцев и контекстов SELinux,
   * настройка firewall,
   * правка DNS-параметров в сетевом соединении,
   * запуск и автозапуск сервиса named.

* 
* Рис. 15: Скрипт автоматической настройки dns.sh

1. В файле Vagrantfile добавлен вызов скрипта dns.sh для автоматической настройки DNS при развёртывании виртуальной машины.

* 
* Рис. 16: Vagrantfile с настройкой DNS

# 3 Заключение

DNS-сервер был успешно установлен, настроен для прямой и обратной зон и проверен, после чего его конфигурация автоматизирована с помощью скрипта и Vagrant.

# 4 Контрольные вопросы

1. **Что такое DNS?**  
   DNS — система доменных имён, преобразующая доменные адреса в IP и обратно.
2. **Каково назначение кэширующего DNS-сервера?**  
   Хранит результаты запросов для ускорения доступа и снижения нагрузки на внешние DNS.
3. **Чем отличается прямая DNS-зона от обратной?**  
   Прямая зона сопоставляет имена с IP (A-записи), обратная — IP с именами (PTR-записи).
4. **В каких каталогах и файлах располагаются настройки DNS-сервера?**
   * /etc/named.conf — основной конфиг;
   * /etc/named/\*.zones — описание зон;
   * /var/named/ — файлы прямых и обратных зон;
   * /etc/resolv.conf — DNS-серверы по умолчанию.
5. **Что указывается в файле resolv.conf?**  
   Адреса DNS-серверов, домен поиска и суффиксы поиска.
6. **Какие типы записи описания ресурсов есть в DNS?**
   * A — IPv4-адрес
   * AAAA — IPv6-адрес
   * NS — серверы имён
   * SOA — начальная запись зоны
   * PTR — обратное разрешение
   * MX — почтовые сервера
   * CNAME — псевдоним
   * TXT — произвольный текст
7. **Для чего используется домен in-addr.arpa?**  
   Для обратного разрешения IP → имя.
8. **Для чего нужен демон named?**  
   Это служба (BIND), реализующая работу DNS-сервера.
9. **Функции slave-сервера и master-сервера?**  
   Master хранит оригинальные зоны, slave получает копии через zone transfer.
10. **Какие параметры отвечают за время обновления зоны?**  
    В SOA-записи: serial, refresh, retry, expire, minimum.
11. **Как обеспечить защиту зоны от скачивания?**  
    Настроить allow-transfer и ACL для ограничения zone transfer.
12. **Какая запись применяется для почтовых серверов?**  
    MX (Mail Exchanger).
13. **Как протестировать работу DNS-сервера?**  
    Утилитами dig, host, nslookup.
14. **Как управлять службой?**  
    systemctl start|stop|restart|status <служба>.
15. **Как посмотреть отладочную информацию службы?**  
    journalctl -xe или запуск с повышенным логированием.
16. **Где хранится отладочная информация?**  
    В journalctl и в /var/log/ (например, /var/log/messages).
17. **Как посмотреть файлы процесса?**  
    lsof -p <PID>, lsof -i :53, cat /proc/<PID>/fd/.
18. **Примеры nmcli:**
    * nmcli con show — список соединений
    * nmcli con mod eth0 ipv4.addresses 192.168.1.10/24 — задать IP
    * nmcli con mod eth0 ipv4.gateway 192.168.1.1 — задать шлюз
    * nmcli con mod eth0 ipv4.dns 8.8.8.8 — задать DNS
19. **Что такое SELinux?**  
    Система обязательного контроля доступа в Linux.
20. **Что такое контекст SELinux?**  
    Метка безопасности, определяющая доступ к объекту.
21. **Как восстановить контекст SELinux?**  
    restorecon -Rv /путь.
22. **Как создать правила из логов SELinux?**  
    С помощью audit2allow на основе /var/log/audit/audit.log.
23. **Что такое булевый переключатель SELinux?**  
    Параметр, включающий или отключающий определённые функции политики.
24. **Как посмотреть переключатели SELinux?**  
    getsebool -a.
25. **Как изменить значение переключателя SELinux?**  
    setsebool имя on/off или setsebool -P имя on/off для сохранения.