

Лабораторная работа № 2

Настройка DNS-сервера

Абд эль хай мохамад

Содержание

<i>Цель работы</i>	2
<i>Выполнение лабораторной работы</i>	2
Установка DNS-сервера	2
Конфигурирование кэширующего DNS-сервера.....	4
Конфигурирование первичного DNS-сервера.....	10
Анализ работы DNS-сервера	13
Внесение изменений в настройки внутреннего окружения виртуальной машины	14
Вывод:.....	15
Ответы на контрольные вопросы:	15

Цель работы

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

Выполнение лабораторной 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 (maabedelhay) и открываю терминал. Перехожу в режим суперпользователя: `sudo -i`
4. Устанавливаю `bind` и `bind-utils`

```

[root@server:~]# ls
anaconda-ks.cfg  original-ks.cfg
[root@server.maabeldelhay.net ~]# dnf -y install bind bind-utils
Rocky Linux 9 - BaseOS                2.4 kB/s | 4.1 kB    00:01
Rocky Linux 9 - AppStream              6.6 kB/s | 4.5 kB    00:00
Rocky Linux 9 - Extras                 4.7 kB/s | 2.9 kB    00:00
Package bind-utils-32:9.16.23-11.el9_2.2.x86_64 is already installed.
Dependencies resolved.
=====
Package                Arch      Version                Repository      Size
=====
Installing:
bind                   x86_64    32:9.16.23-11.el9_2.2  appstream      487 k
Installing dependencies:
bind-dnssec-doc        noarch    32:9.16.23-11.el9_2.2  appstream      44 k
python3-bind           noarch    32:9.16.23-11.el9_2.2  appstream      60 k
python3-ply            noarch    3.11-14.el9.0.1        baseos         103 k
Installing weak dependencies:
bind-dnssec-utils      x86_64    32:9.16.23-11.el9_2.2  appstream      112 k

Transaction Summary
=====
Install 5 Packages

```

5. С помощью утилиты dig делаю запрос, к DNS-адресу www.yandex.ru: dig www.yandex.ru

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без

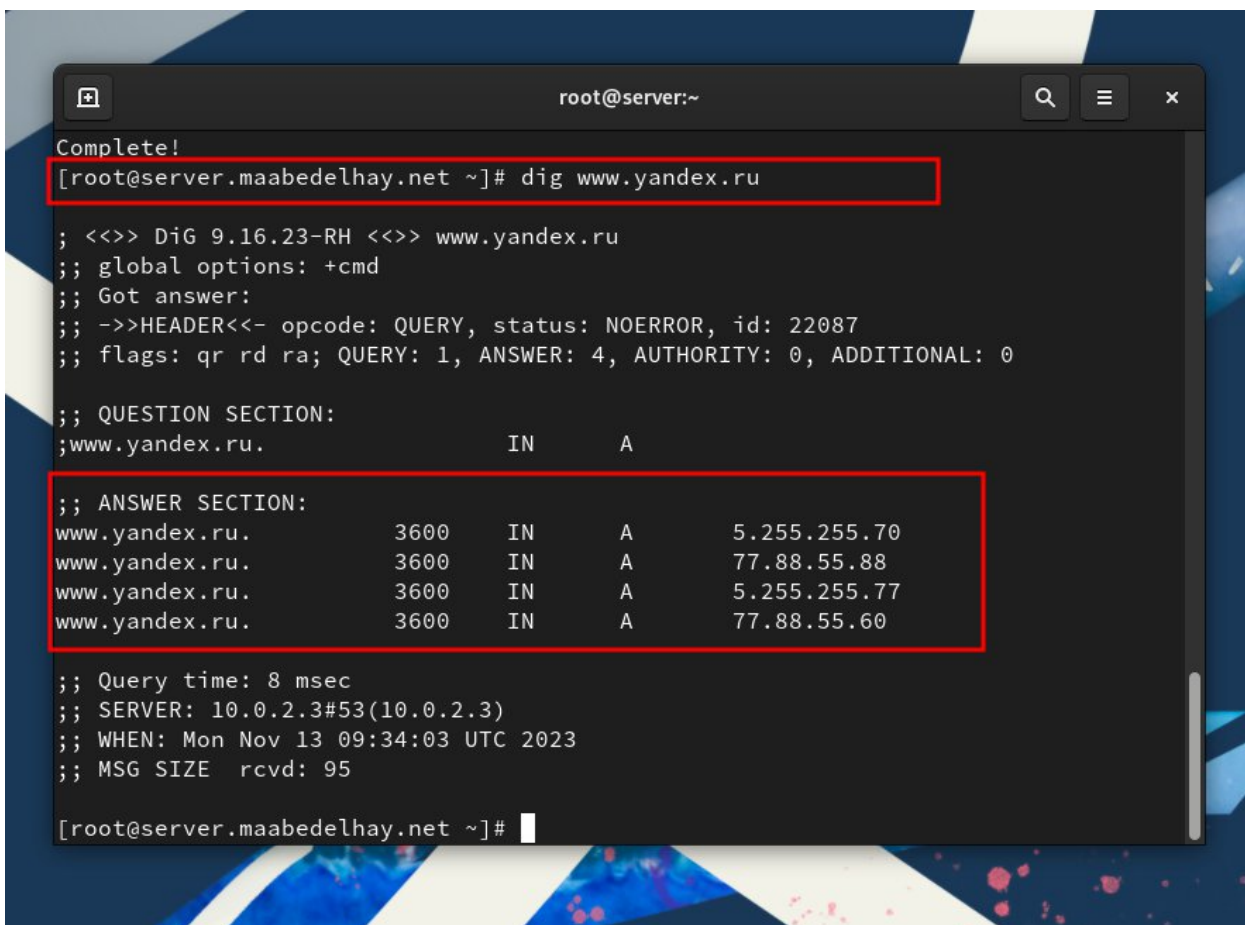
ошибок, использовались флаги qr rd ra, запрос отправлен один, ответов получено четыре.

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).

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

ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS, в нашем случае показывает А-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.



```
Complete!
[root@server.maabeldelhay.net ~]# dig www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22087
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                IN      A

;; ANSWER SECTION:
www.yandex.ru.                3600    IN      A      5.255.255.70
www.yandex.ru.                3600    IN      A      77.88.55.88
www.yandex.ru.                3600    IN      A      5.255.255.77
www.yandex.ru.                3600    IN      A      77.88.55.60

;; Query time: 8 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Mon Nov 13 09:34:03 UTC 2023
;; MSG SIZE rcvd: 95

[root@server.maabeldelhay.net ~]#
```

Конфигурирование кэширующего DNS-сервера

1. Анализирую содержание файлов

1) /etc/resolv.conf

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

2) /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/cache_dump.db"; Задает дамп файл.  
  
statistics-file "/var/named/data/named_stats.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"; Задаёт 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.rfc1912.zones";

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

```

3) /var/named/named.ca

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой. Тип посланного сообщения – запрос, выполнен без ошибок, id , 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).

QUESTION SECTION (секция запроса): Показывает наличие запроса на А-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.

4) /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

A 127.0.0. - IP-адрес машины

AAAA ::1 - IPv6 -адрес

5) /var/named/named.loopback

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

PTR localhost — доменное имя хоста.

2. Запускаю DNS-сервер
3. Включаю запуск DNS-сервера в автозапуск при загрузке системы
4. Выведенная на экран информацию при выполнении команды `dig @127.0.0.1 www.yandex.ru`

```
[root@server.maabeldelhay.net ~]# systemctl start named
[root@server.maabeldelhay.net ~]# systemctl enable named
Created symlink /etc/systemd/system/multi-user.target.wants/named.service → /usr/lib/systemd/system/named.service.
[root@server.maabeldelhay.net ~]#
```

5. 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:
6. Также повторяю действия для второго соединения
7. Перезапускаю NetworkManager: `systemctl restart NetworkManager`

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

```
[root@server.maabeldelhay.net ~]# cat /etc/named.conf
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only)
//
// See /usr/share/doc/bind*/sample/ for example named configuration file
//
options {
    listen-on port 53 { 127.0.0.1;any ; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { localhost; 192.168.0.0/16; };
```

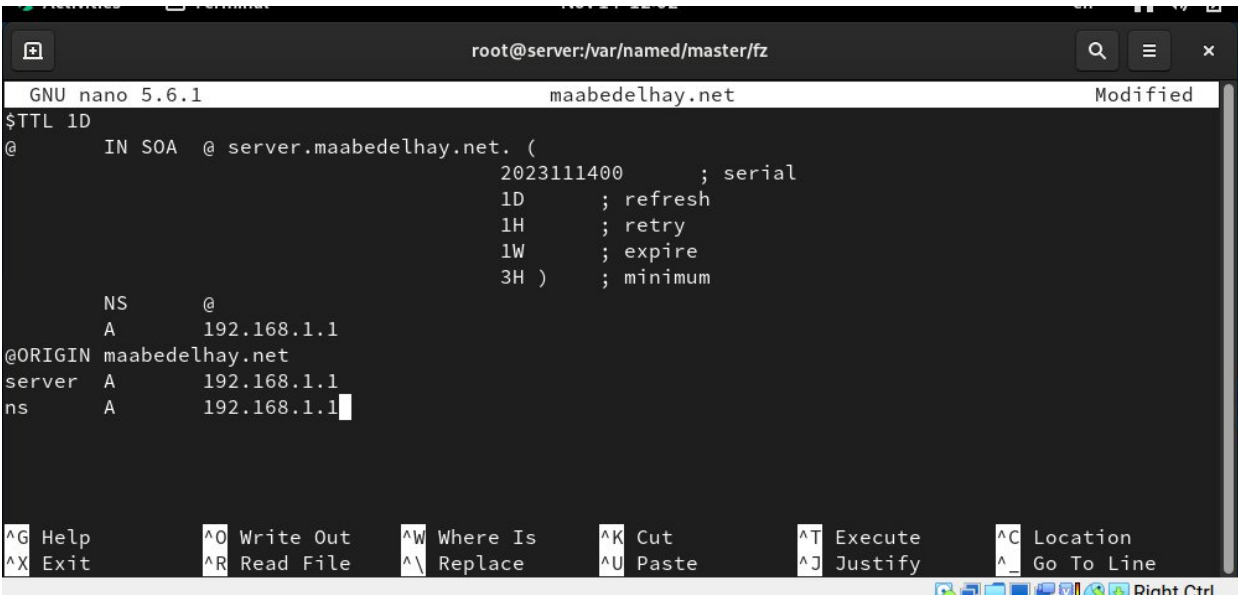
9. Вношу изменения в настройки межсетевого экрана узла server, разрешив работу с DNS:

10. Проверяю, что DNS-запросы идут через узел server, который прослушивает порт 53.

```
[root@server.maabedelhay.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1002/gvfs
Output information may be incomplete.
avahi-dae 563          avahi 12u  IPv4           18769      0t0      UDP *:mdns
avahi-dae 563          avahi 13u  IPv6           18770      0t0      UDP *:mdns
avahi-dae 563          avahi 14u  IPv4           18771      0t0      UDP *:39916
avahi-dae 563          avahi 15u  IPv6           18772      0t0      UDP *:50126
chronyd  603          chrony 5u   IPv4           18791      0t0      UDP localhost:323
chronyd  603          chrony 6u   IPv6           18792      0t0      UDP localhost:323
named    693          named 16u  IPv4           19319      0t0      UDP localhost:domain
named    693          named 19u  IPv6           19321      0t0      UDP localhost:domain
named    693 694 isc-net-0    named 16u  IPv4           19319      0t0      UDP localhost:domain
named    693 694 isc-net-0    named 19u  IPv6           19321      0t0      UDP localhost:domain
named    693 695 isc-timer    named 16u  IPv4           19319      0t0      UDP localhost:domain
named    693 695 isc-timer    named 19u  IPv6           19321      0t0      UDP localhost:domain
named    693 696 isc-socke    named 16u  IPv4           19319      0t0      UDP localhost:domain
named    693 696 isc-socke    named 19u  IPv6           19321      0t0      UDP localhost:domain
```

Конфигурирование первичного DNS-сервера

1. Копирую шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименовываю его в `maabedelhay.net`:
2. Включаю файл описания зоны `/etc/named/user.net` в конфигурационном файле DNS `/etc/named.conf`;
3. Открываю файл `/etc/named/user.net` на редактирование
4. В каталоге `/var/named` создаю подкаталоги `master/fz` и `master/rz`, в которых будут располагаться файлы прямой и обратной зоны соответственно:
5. Копирую шаблон прямой DNS-зоны `named.localhost` из каталога `/var/named` в каталог `/var/named/master/fz` и переименовываю его в `maabedelhay.net`:
6. Изменяю файл `/var/named/master/fz/maabedelhay.net`, указав необходимые DNS записи для прямой зоны. В этом файле DNS-имя сервера `@ mname.invalid.` должно быть заменено на `@ server.maabedelhay.net`. 2020111400 - формат серийного номера ГТГГММДДВВ (ГТГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-записи должен быть заменён с 127.0.0.1 на 192.168.1.1; в директиве `$ORIGIN` должно быть задано текущее имя домена `maabedelhay.net.`, а затем указаны имена и адреса серверов в этом домене в виде А-записей DNS (на данном этапе должен быть прописан сервер с именем `ns` и адресом 192.168.1.1):



```
root@server:/var/named/master/fz
GNU nano 5.6.1 maabedelhay.net Modified
$TTL 1D
@      IN SOA  @ server.maabedelhay.net. (
                                2023111400      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H      ; minimum

    NS      @
    A      192.168.1.1
@ORIGIN maabedelhay.net
server  A      192.168.1.1
ns      A      192.168.1.1
```

7. Копирую шаблон обратной DNS-зоны `named.loopback` из каталога `/var/named` в каталог `/var/named/master/rz` и переименовываю его в `192.168.1`:
8. Изменяю файл `/var/named/master/rz/192.168.1`, указав необходимые DNS записи для обратной зоны. В этом файле DNS-имя сервера `@ mname.invalid.` должно быть заменено на `@ server.maabedelhay.net`. 2020111400 - формат серийного номера ГТГГММДДВВ (ГТГГ — год, ММ — месяц, ДД — день, ВВ — номер ревизии); адрес в А-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.maabedelhay.net):

```
GNU nano 5.6.1 192.168.1
$TTL 1D
@      IN SOA  @ server.maabedelhay.net. (
                                2023111400      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )   ; minimum

      NS      @
      A      192.168.1.1
      PTR     server.maabedelhay.net.
@ORIGIN 1.168.192.in-addr.arpa.
1      PTR     server.maabedelhay.net.
1      PTR     ns.maabedelhay.net.

[ Read 13 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
Right Ctrl
```

9. Исправляю права доступа к файлам в каталогах /etc/named и /var/named, чтобы демон named мог с ними работать:
10. 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:

```
[root@server.maabedelhay.net rz]# chown -R named:named /etc/named
[root@server.maabedelhay.net rz]# chown -R named:named /var/named
[root@server.maabedelhay.net rz]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@server.maabedelhay.net rz]# restorecon -vR /var/named
[root@server.maabedelhay.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.maabedelhay.net rz]#
```

11. 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.maabeldelhay.net;

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

Информация AUTHORITY SECTION содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени – maabeldelhay.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.maabeldelhay.net;

ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS – A-запись для ns.maabeldelhay.net.

Последняя секция — это статистика по запросу - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.

2. 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:
2. В каталоге `/vagrant/provision/server` создаю исполняемый файл `dns.sh`:
3. 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.

Ответы на 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.
2. Каково назначение кэширующего DNS-сервера?
Кэширующий DNS-сервер получает рекурсивные запросы от клиентов и выполняет их с помощью нерекурсивных запросов к авторитативным серверам.
3. Чем отличается прямая DNS-зона от обратной?
Прямая зона позволяет по доменному имени получать IP-адрес. Она решает прямую задачу в DNS при помощи записей типа A (Address).
Обратная зона — по IP-адресу "выдает" информацию об имени хоста. Она решает обратную задачу при помощи записей-указателей типа PTR (Pointer) и записей SOA и NS.

4. В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.
/etc/resolve.conf,
/etc/named.conf,
/var/named/named.ca,
/var/named/named.localhost,
/var/named/named.loopback.
Содержимое и назначение файлов описано в отчете выше.
5. Что указывается в файле resolve.conf?
Файл содержит директивы, которые определяют домен поиска по умолчанию; используется для завершения заданного имени запроса для полного имени домена, если суффикс домена не указан. Он также содержит список IP-адресов серверов имен, доступных для разрешения.
6. Какие типы записи описания ресурсов есть в DNS и для чего они используются?
RR-записи описывают все узлы сети в зоне и помечают делегирование поддоменов.
Типы записи описания ресурсов:
– SOA-запись — указывает на авторитативность для зоны;
– NS-запись — перечисляет DNS-серверы зоны;
– A — задаёт отображение имени узла в IP-адрес;
– PTR — задаёт отображение IP-адреса в имя узла;
7. Для чего используется домен in-addr.arpa?
Решение, которое позволяет использовать стандартный механизм поиска доменного имени для решения "обратной" задачи, - специальный домен in-addr.arpa., структура которого совпадает со структурой IP-адресов.
8. Для чего нужен демон named?
Программой, реализующей функции сервера DNS, является демон named, запускаемый из файла /usr/sbin/in.named.
9. В чём заключаются основные функции slave-сервера и master-сервера?
Slave-сервер (secondary, вторичный, дублирующий) также является ответственным (authoritative) за зону. Его основное назначение заключается в том, чтобы подстраховать работу основного сервера доменных имен (master server), ответственного за зону, на случай его выхода из строя, а также для того, чтобы разгрузить основной сервер, приняв часть запросов на себя.

Master-сервер (primary, первичный) доменных имен является ответственным (authoritative) за информацию о зоне в том смысле, что читает описание зоны с локального диска компьютера, на котором он функционирует и отвечает в соответствии с этим описанием на запросы resolver-ов. Описание зоны master-сервера является первичным, т.к. его создает вручную администратор зоны. Соответственно, вносить изменения в описание зоны может только администратор данного сервера. Все остальные серверы только копируют информацию с master-сервера.

10. Какие параметры отвечают за время обновления зоны?

В записи SOA:

[zone] [ttl] IN SOA origin contact (serial refresh retry expire minimum)

– refresh — интервал времени, после которого slave-сервер обязан обратиться к master-серверу с запросом на верификацию своего описания зоны;

– retry — интервал времени, после которого slave-сервер должен повторить попытку синхронизировать описание зоны с master сервером;

– 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;

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

11. Как обеспечить защиту зоны от скачивания и просмотра?

В `etc/named.conf` указать в параметрах `allow-query`, `allow-transfer` только те сервера, которым разрешено запрашивать информацию о зоне.

Так же стоит отобрать права на создание подзон у всех неблагоприятных серверов.

12. Какая запись RR применяется при создании почтовых серверов?

MX — задаёт имена почтовым серверам.

13. Как протестировать работу сервера доменных имён?

При помощи утилиты `host` можно проанализировать корректность работы DNS-сервера:

host -l user.net

host -a user.net

host -t A user.net

host -t PTR 192.168.1.1

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

\$ systemctl опции команда служба служба

start — запустить службу linux

stop — остановить службу linux

reload — обновить конфигурацию службы из файла юнита

restart — перезапустить службу

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

Systemd имеет собственную систему регистрации, называемую журналом.

journalctl -u название_процесса.service

Сначала запустить журнал, потом - сервис.

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

data/named.run или в отладочных сообщениях / var / log / messages

Просмотреть # journalctl -u название_процесса.service

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

Чтобы узнать, какие файлы использует определенный процесс, выполните команду в терминале: lsof -p <PID>

18. 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
```

19. Что такое SELinux?

Linux с улучшенной безопасностью (SELinux) - это реализация мандатного управления доступом *mandatory access control* в ядре Linux, проверяющего разрешение операций после проверки стандартного дискреционного управления доступом *discretionary access controls*.

20. Что такое контекст (метка) SELinux?

В системах с запущенным SELinux, все процессы и файлы маркированы (помечены) так, чтобы представлять информацию в контексте безопасности. Эта информация называется контекстом SELinux, и просматривается с использованием команды `ls -Z`:

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

Удалить контекст `/usr/sbin/semanage fcontext -d`

И восстановить `/sbin/restorecon -R -v`

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

Команда `/usr/sbin/setenforce` используется для перехода между принудительным (*enforcing*) и разрешающим (*permissive*) режимами. Для перехода в принудительный режим выполните от имени root пользователя команду `/usr/sbin/setenforce 1`. Для перехода в разрешающий режим выполните команду `/usr/sbin/setenforce 0`.

23. Что такое булевый переключатель в SELinux?

Булевый переключатель позволяет изменять части политики SELinux, что даёт возможность вносить изменения, такие как: разрешение доступа службам к файловым системам NFS, без перезагрузки или recompilation политики SELinux.

24. Как посмотреть список переключателей SELinux и их состояние?

Для получения списка переключателей, объяснения, за что отвечает каждый

переключатель, включен или выключен, необходимо выполнить команду `semanage boolean -l` от имени пользователя `root`.

25. Как изменить значение переключателя SELinux?

Команда `setsebool boolean-name x` переводит переключатели в состояние включено или выключено, где `boolean-name` - название переключателя, а `x` - `on` для включения или `off` для выключения.