

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: Сетевые технологии

Студент: Карташова А.С.

Группа: НФИбд-03-18

МОСКВА

2020 г.

Оглавление

Цель работы	2
Задачи	2
Ход работы	2
Установка DNS-сервера	3
Конфигурирование кэширующего DNS-сервера.....	3
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами	3
Конфигурирование первичного DNS-сервера	7
Анализ работы DNS-сервера	11
Внесение изменений в настройки внутреннего окружения виртуальной машины	12
Заключение	13
Контрольные вопросы.....	13

Цель работы

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

Задачи

1. Установить на виртуальной машине server DNS-сервер bind и bind-utils
2. Сконфигурировать на виртуальной машине server кэширующий DNS-сервер
3. Сконфигурировать на виртуальной машине server первичный DNS-сервер
4. При помощи утилит dig и host проанализировать работу DNS-сервера
5. Написать скрипт для Vagrant, фиксирующий действия по установке и конфигурированию DNS-сервера во внутреннем окружении виртуальной машины server.

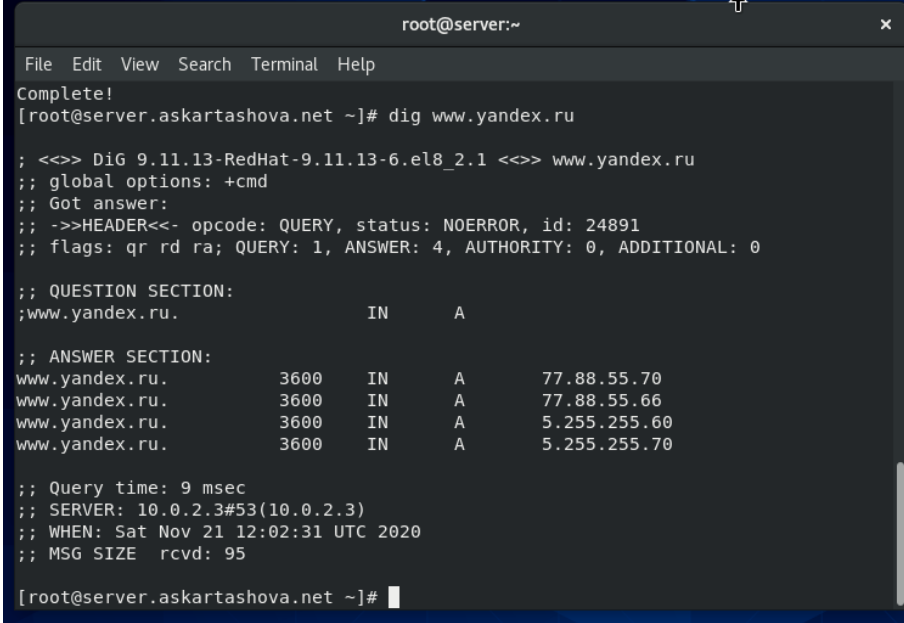
Ход работы

Установка DNS-сервера

На виртуальной машине server войдем под созданным вами в предыдущей работе пользователем и откроем терминал. Перейдем в режим суперпользователя. Установим bind и bind-utils:

С помощью утилиты dig сделаем запрос к DNS-адресу `www.yandex.ru`:

`dig www.yandex.ru`



```
root@server:~  
File Edit View Search Terminal Help  
Complete!  
[root@server.askartashova.net ~]# dig www.yandex.ru  
  
; <<>> DiG 9.11.13-RedHat-9.11.13-6.el8_2.1 <<>> www.yandex.ru  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24891  
;; 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       77.88.55.70  
www.yandex.ru.                3600    IN      A       77.88.55.66  
www.yandex.ru.                3600    IN      A       5.255.255.60  
www.yandex.ru.                3600    IN      A       5.255.255.70  
  
;; Query time: 9 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Sat Nov 21 12:02:31 UTC 2020  
;; MSG SIZE rcvd: 95  
  
[root@server.askartashova.net ~]#
```

- **HEADER** (заголовок): показывает версию dig, глобальные опции используемые с командой и другую доп.информацию
- **QUESTION SECTION** (секция запроса): Показывает наш запрос (мы запросили показать A-запись для домена `ya.ru`)
- **ANSWER SECTION** (секция ответа): показывает ответ полученный от DNS, в нашем случае показывает адреса для `ya.ru`

Конфигурирование кэширующего DNS-сервера

Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами

Запустим DNS-сервер и включим запуск DNS-сервера в автозапуск при загрузке системы:

`systemctl enable named`

При выполнении команды `dig www.yandex.ru` выводятся те же ip-адреса. `dig @127.0.0.1 www.yandex.ru` не выводит ответ

```
root@server:~  
File Edit View Search Terminal Help  
[root@server.askartashova.net ~]# dig www.yandex.ru  
;<<>> DiG 9.11.13-RedHat-9.11.13-6.el8_2.1 <<>> www.yandex.ru  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7020  
;; 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      5.255.255.60  
www.yandex.ru.                3600    IN      A      77.88.55.66  
www.yandex.ru.                3600    IN      A      5.255.255.70  
www.yandex.ru.                3600    IN      A      77.88.55.70  
;; Query time: 8 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Sat Nov 21 13:07:22 UTC 2020  
;; MSG SIZE rcvd: 95  
[root@server.askartashova.net ~]# S
```

```
root@server:~  
File Edit View Search Terminal Help  
;; MSG SIZE rcvd: 95  
[root@server.askartashova.net ~]# dig @127.0.0.1 www.yandex.ru  
;<<>> DiG 9.11.13-RedHat-9.11.13-6.el8_2.1 <<>> @127.0.0.1 www.yandex.ru  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 46140  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:;; udp: 4096  
; COOKIE: 54244ab446d7023f0d3890755fb9115e3abb45b275674681 (good)  
;; QUESTION SECTION:  
;www.yandex.ru.                IN      A  
;; Query time: 377 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Sat Nov 21 13:08:46 UTC 2020  
;; MSG SIZE rcvd: 70
```

Сделаем DNS-сервер сервером по умолчанию для хоста server и внутренней виртуальной сети.

```
root@server:~  
File Edit View Search Terminal Help  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Sat Nov 21 13:08:46 UTC 2020  
;; MSG SIZE rcvd: 70  
  
[root@server.askartashova.net ~]# nmcli connection edit System\ eth0  
===| nmcli interactive connection editor |===  
Editing existing '802-3-ethernet' connection: 'System eth0'  
  
Type 'help' or '?' for available commands.  
Type 'print' to show all the connection properties.  
Type 'describe [<setting>.<prop>]' for detailed property description.  
  
You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sr  
iov, ethtool, match, ipv4, ipv6, tc, proxy  
nmcli> remove ipv4.dns  
nmcli> set ipv4.ignore-auto-dns yes  
nmcli> set ipv4.dns 127.0.0.1  
nmcli> save  
Connection 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.  
nmcli> quit  
[root@server.askartashova.net ~]#
```

Перезапустим NetworkManager и проверим наличие изменений в файле /etc/resolv.conf.

```
root@server:~  
File Edit View Search Terminal Help  
GNU nano 2.9.8 /etc/resolv.conf  
  
# Generated by NetworkManager  
search askartashova.net  
nameserver 127.0.0.1
```

Настроим направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server. Для этого внесем 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; };*

```
GNU nano 2.9.8 /etc/named.conf Modified
//
// 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 files.
//
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; };
}
```

Внесем изменения в настройки межсетевого экрана узла server, разрешив работу с DNS.

Убедимся, что DNS-запросы идут через узел server, который прослушивает порт 53. Для этоо используем команду lsof:

lsof | grep UDP

```
Nov 21 13:54 en
root@server:~
File Edit View Search Terminal Help
success
[root@server.askartashova.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
[root@server.askartashova.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
systemd 1 root 58u IPv4 17755 0t0 UDP *:sunrpc
systemd 1 root 61u IPv6 17757 0t0 UDP *:sunrpc
rpcbind 689 rpc 5u IPv4 17755 0t0 UDP *:sunrpc
rpcbind 689 rpc 7u IPv6 17757 0t0 UDP *:sunrpc
avahi-dae 722 avahi 15u IPv4 22555 0t0 UDP *:mdns
avahi-dae 722 avahi 16u IPv6 22556 0t0 UDP *:mdns
avahi-dae 722 avahi 17u IPv4 22557 0t0 UDP *:52088
avahi-dae 722 avahi 18u IPv6 22558 0t0 UDP *:44303
chronyd 742 chrony 6u IPv4 21902 0t0 UDP localhost:323
chronyd 742 chrony 7u IPv6 21903 0t0 UDP localhost:323
systemd-r 1109 systemd-resolve 12u IPv4 26936 0t0 UDP *:hostmon
systemd-r 1109 systemd-resolve 14u IPv6 26939 0t0 UDP *:hostmon
systemd-r 1109 systemd-resolve 18u IPv4 26942 0t0 UDP 127.0.0.53:domain
dnsmasq 1239 dnsmasq 3u IPv4 28318 0t0 UDP *:bootps
dnsmasq 1239 dnsmasq 5u IPv4 28321 0t0 UDP server.askartashova.net:domain
named 9064 named 512u IPv4 92089 0t0 UDP localhost:domain
named 9064 named 513u IPv6 92092 0t0 UDP localhost:domain
named 9064 9065 isc-worke named 512u IPv4 92089 0t0 UDP localhost:domain
named 9064 9065 isc-worke named 513u IPv6 92092 0t0 UDP localhost:domain
named 9064 9066 isc-timer named 512u IPv4 92089 0t0 UDP localhost:domain
named 9064 9066 isc-timer named 513u IPv6 92092 0t0 UDP localhost:domain
named 9064 9067 isc-socket named 512u IPv4 92089 0t0 UDP localhost:domain
named 9064 9067 isc-socket named 513u IPv6 92092 0t0 UDP localhost:domain
NetworkMa 9257 root 28u IPv4 95043 0t0 UDP server.askartashova.net:bootpc->_gateway:
bootps
NetworkMa 9257 9258 gmain root 28u IPv4 95043 0t0 UDP server.askartashova.net:bootpc->_gateway:
bootps
NetworkMa 9257 9259 gdbus root 28u IPv4 95043 0t0 UDP server.askartashova.net:bootpc->_gateway:
bootps
[root@server.askartashova.net ~]# lsof -i udp:53
COMMAND PID USER FD TYPE DEVICE SIZE/OFF NODE NAME
systemd-r 1109 systemd-resolve 18u IPv4 26942 0t0 UDP 127.0.0.53:domain
dnsmasq 1239 dnsmasq 5u IPv4 28321 0t0 UDP server.askartashova.net:domain
named 9064 named 512u IPv4 92089 0t0 UDP localhost:domain
named 9064 named 513u IPv6 92092 0t0 UDP localhost:domain
[root@server.askartashova.net ~]# s
```

Конфигурирование первичного DNS-сервера

Скопируем шаблон описания DNS-зон `named.rfc1912.zones` из каталога `/etc` в каталог `/etc/named` и переименуйте его в `user.net`

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

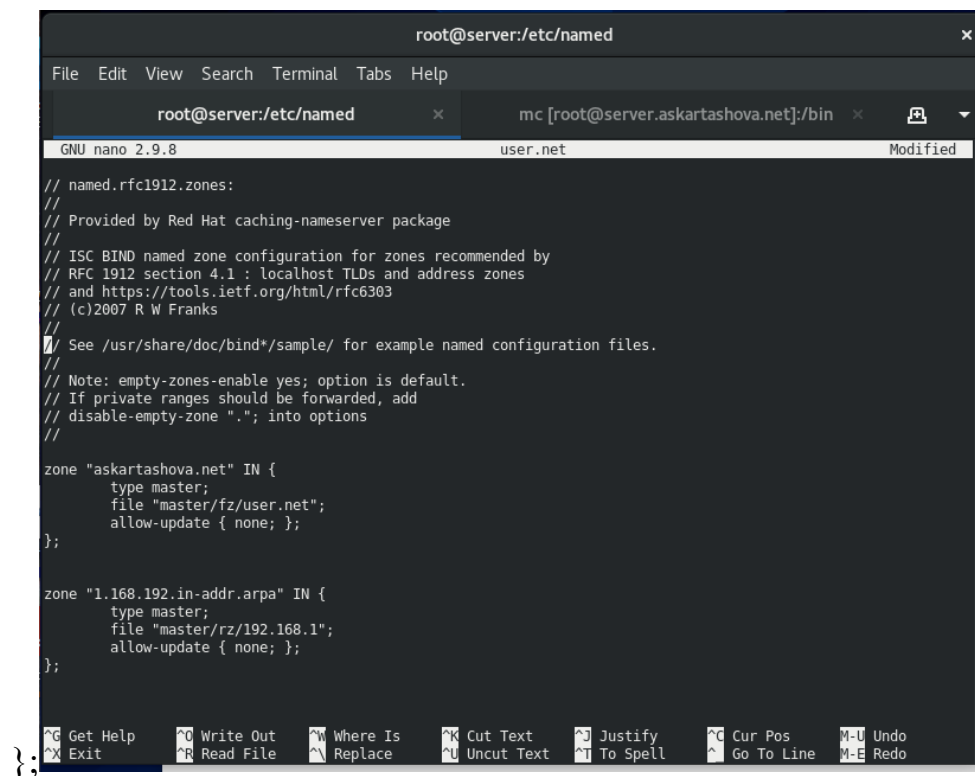
```
include "/etc/named/user.net";
```

Откройте файл `/etc/named/user.net` на редактирование и вместо пропишем свою прямую зону:

```
zone "user.net" IN {  
    type master;  
    file "master/fz/user.net";  
    allow-update { none; };  
};
```

И свою обратную зону:

```
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "master/rz/192.168.1";  
    allow-update { none; };  
};
```



The screenshot shows a terminal window titled 'root@server:/etc/named'. The window contains the configuration for the 'user.net' zone in the 'named.conf' file. The configuration is as follows:

```
// named.rfc1912.zones:  
//  
// Provided by Red Hat caching-nameserver package  
//  
// ISC BIND named zone configuration for zones recommended by  
// RFC 1912 section 4.1 : localhost TLDs and address zones  
// and https://tools.ietf.org/html/rfc6303  
// (c)2007 R W Franks  
//  
// See /usr/share/doc/bind/sample/ for example named configuration files.  
//  
// Note: empty-zones-enable yes; option is default.  
// If private ranges should be forwarded, add  
// disable-empty-zone "."; into options  
//  
zone "askartashova.net" IN {  
    type master;  
    file "master/fz/user.net";  
    allow-update { none; };  
};  
  
zone "1.168.192.in-addr.arpa" IN {  
    type master;  
    file "master/rz/192.168.1";  
    allow-update { none; };  
};
```

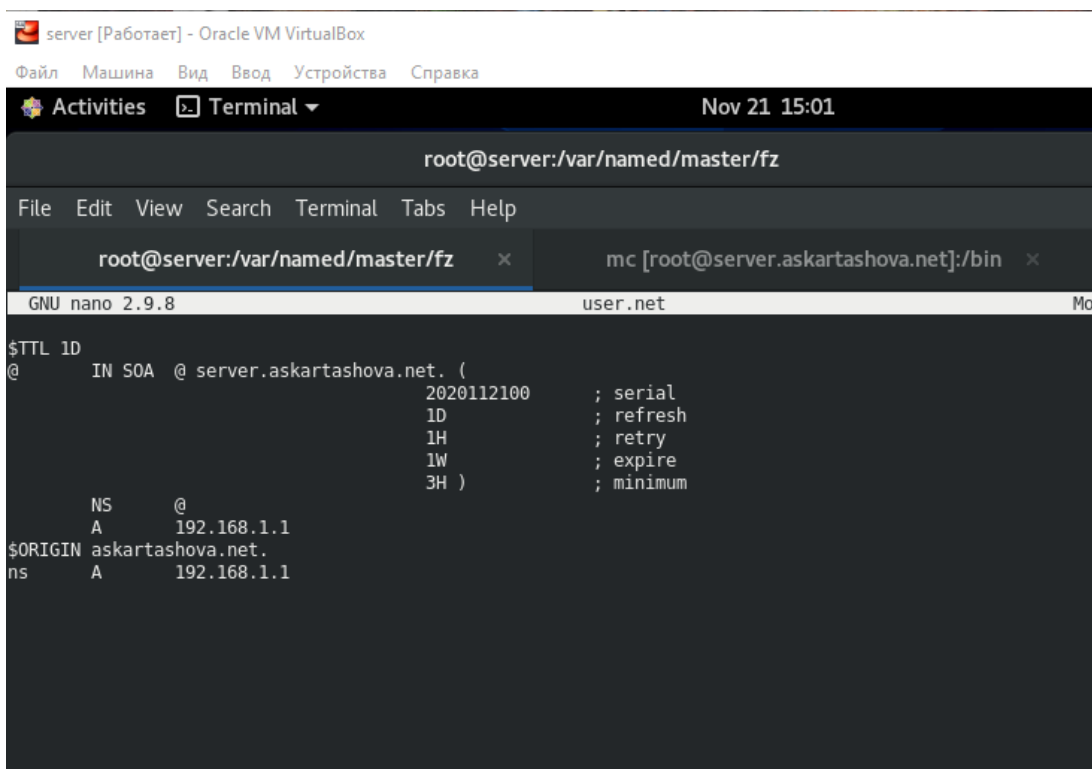
В каталоге `/var/named` создайте подкаталоги `master/fz` и `master/rz`, в которых

будут располагаться файлы прямой и обратной зоны соответственно.

Скопируйте шаблон прямой DNS-зоны `named.localhost` из каталога `/var/named` в каталог `/var/named/master/fz` и переименуйте его в `user.net`.

```
[root@server.askartashova.net ~]# cd /var/named/
[root@server.askartashova.net named]# mkdir -p /var/named/master/fz
[root@server.askartashova.net named]# mkdir -p /var/named/master/rz
[root@server.askartashova.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.askartashova.net named]# cd /var/named/master/fz/
[root@server.askartashova.net fz]# mv named.localhost user.net
[root@server.askartashova.net fz]#
```

Изменим файл `/var/named/master/fz/user.net`, указав необходимые DNS-записи для прямой зоны.



The screenshot shows a terminal window titled "server [Работает] - Oracle VM VirtualBox". The terminal is running as root on a server named "server.askartashova.net". The current directory is `/var/named/master/fz`. A nano editor window is open, editing the file `user.net`. The content of the file is as follows:

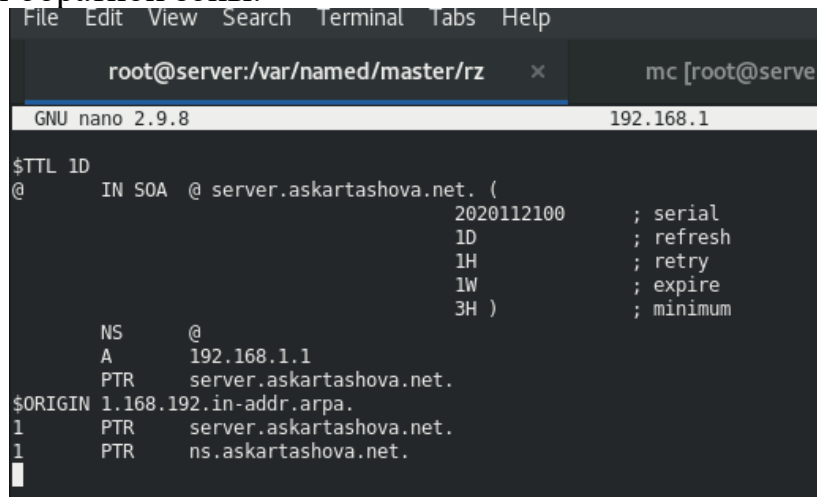
```
$TTL 1D
@      IN SOA  @ server.askartashova.net. (
                                2020112100      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H )              ; minimum

      NS      @
      A      192.168.1.1
$ORIGIN askartashova.net.
ns      A      192.168.1.1
```

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

```
[root@server.askartashova.net fz]# nano user.net
[root@server.askartashova.net fz]# cp /var/named/named.loopback /var/named/master/rz/
[root@server.askartashova.net fz]# cd /var/named/master/rz/
[root@server.askartashova.net rz]# mv named.loopback 192.168.1
[root@server.askartashova.net rz]#
```


Изменим файл `/var/named/master/rz/192.168.1`, указав необходимые DNS-записи для обратной зоны.

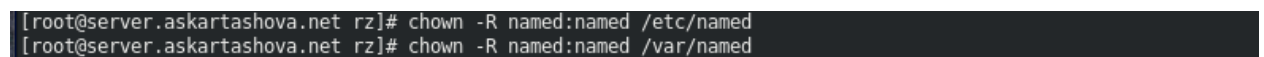


```
File Edit View Search Terminal Tabs Help
root@server:/var/named/master/rz x mc [root@server
GNU nano 2.9.8 192.168.1

$TTL 1D
@      IN SOA  @ server.askartashova.net. (
                                2020112100      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H )              ; minimum

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

Исправим права доступа к файлам в каталогах `/etc/named` и `/var/named`, чтобы демон `named` мог с ними работать:



```
[root@server.askartashova.net rz]# chown -R named:named /etc/named
[root@server.askartashova.net rz]# chown -R named:named /var/named
```

Корректно восстановить метки в SELinux:

`restorecon -vR /etc`

`restorecon -vR /var/named`

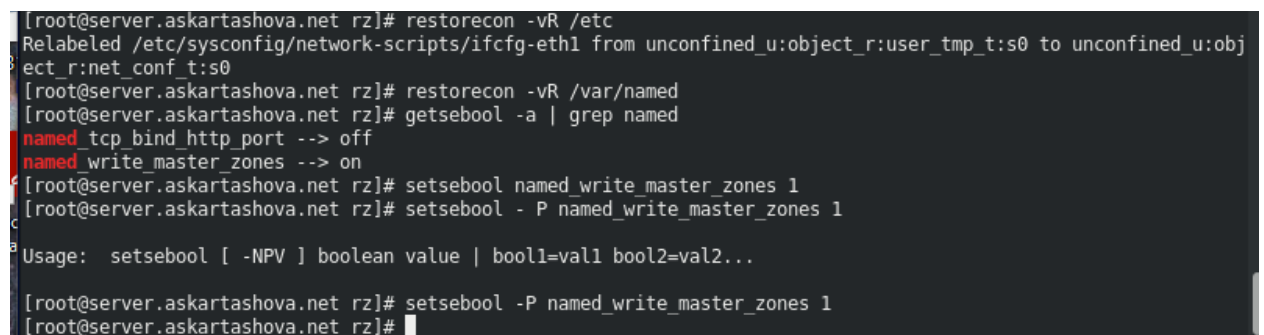
Для проверки состояния переключателей SELinux, относящихся к `named`, введем:

`getsebool -a | grep named`

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

`setsebool named_write_master_zones 1`

`setsebool -P named_write_master_zones 1`



```
[root@server.askartashova.net rz]# restorecon -vR /etc
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:obj
ect_r:net_conf_t:s0
[root@server.askartashova.net rz]# restorecon -vR /var/named
[root@server.askartashova.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.askartashova.net rz]# setsebool named_write_master_zones 1
[root@server.askartashova.net rz]# setsebool -P named_write_master_zones 1
Usage: setsebool [ -NPV ] boolean value | bool1=val1 bool2=val2...

[root@server.askartashova.net rz]# setsebool -P named_write_master_zones 1
[root@server.askartashova.net rz]#
```

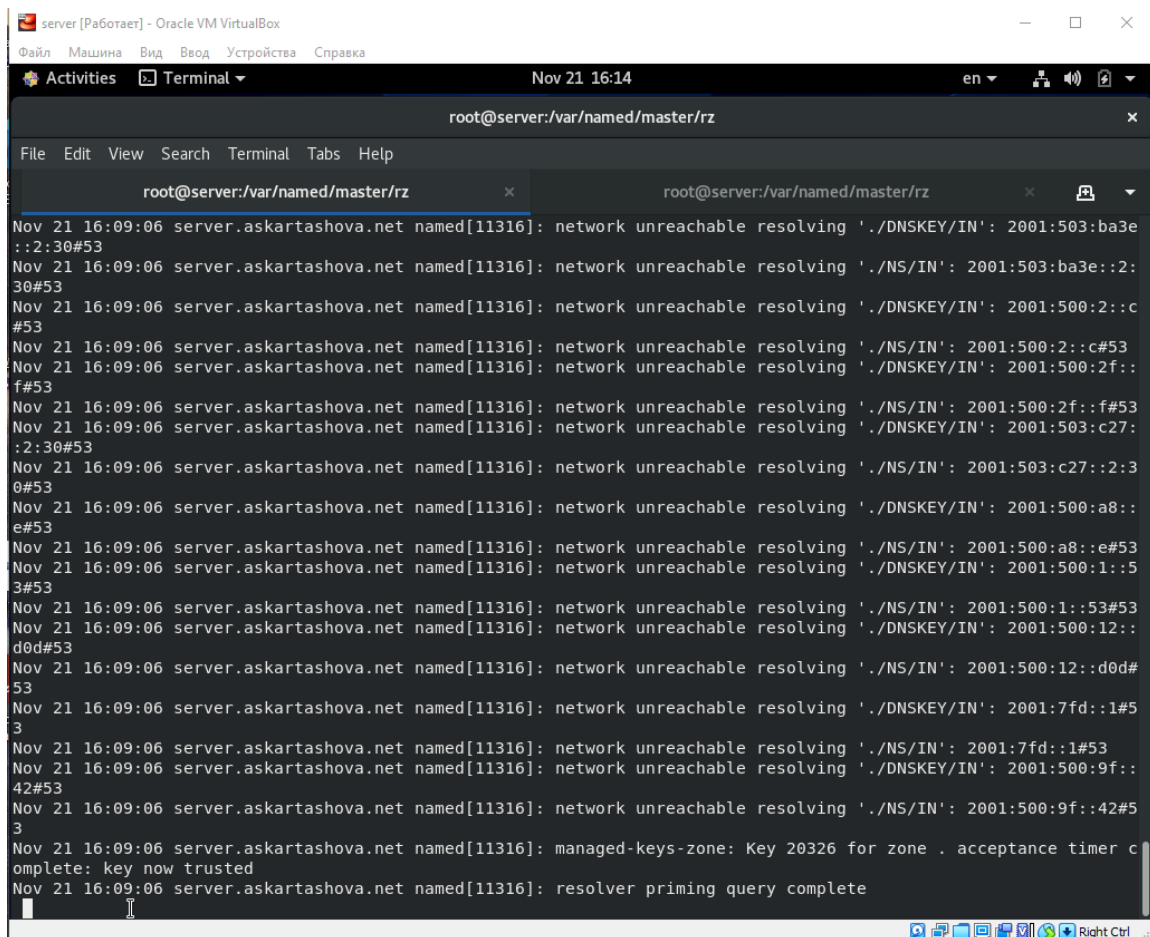
```
Nov 21 16:13 en [Speaker Icon] [Window Icon]
```

root@server:/var/named/master/rz

File Edit View Search Terminal Tabs Help

root@server:/var/named/master/rz x root@server:/var/named/master/rz x [User Icon] v

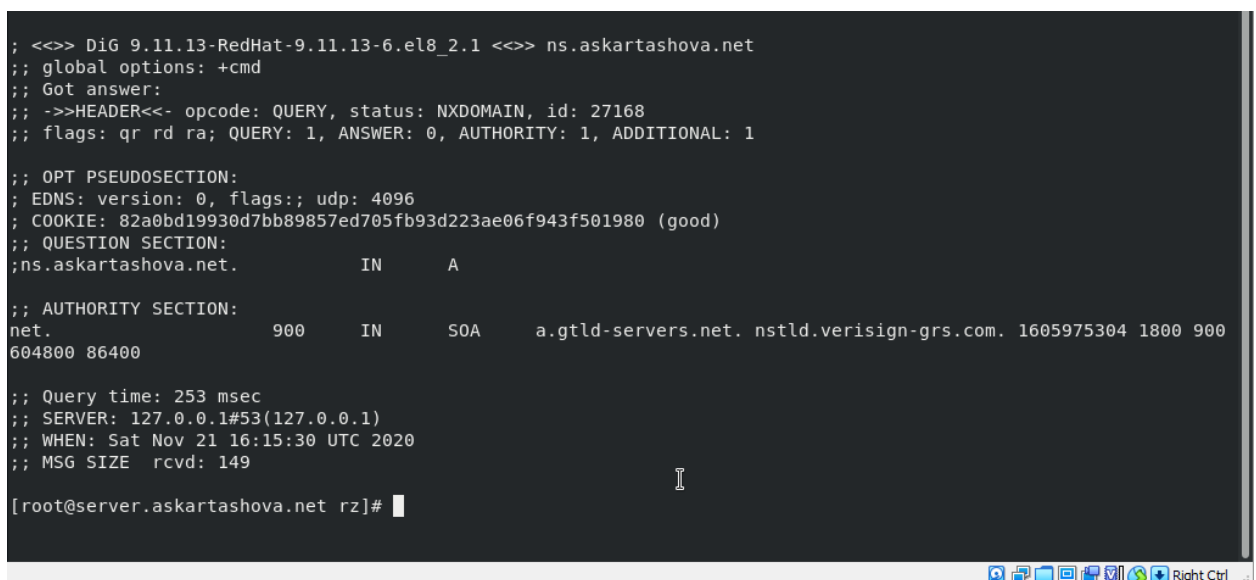
```
Nov 21 16:09:05 server.askartashova.net named[9064]: no longer listening on 127.0.0.1#53
Nov 21 16:09:05 server.askartashova.net named[9064]: no longer listening on ::1#53
Nov 21 16:09:05 server.askartashova.net named[9064]: exiting
Nov 21 16:09:05 server.askartashova.net systemd[1]: Stopped Berkeley Internet Name Domain (DNS).
-- Subject: Unit named.service has finished shutting down
-- Defined-By: systemd
-- Support: https://access.redhat.com/support
..
-- Unit named.service has finished shutting down.
Nov 21 16:09:05 server.askartashova.net systemd[1]: Starting Generate rndc key for BIND (DNS)...
-- Subject: Unit named-setup-rndc.service has begun start-up
-- Defined-By: systemd
-- Support: https://access.redhat.com/support
..
-- Unit named-setup-rndc.service has begun starting up.
Nov 21 16:09:05 server.askartashova.net systemd[1]: Started Generate rndc key for BIND (DNS).
-- Subject: Unit named-setup-rndc.service has finished start-up
-- Defined-By: systemd
-- Support: https://access.redhat.com/support
..
-- Unit named-setup-rndc.service has finished starting up.
..
-- The start-up result is done.
Nov 21 16:09:05 server.askartashova.net systemd[1]: Starting Berkeley Internet Name Domain (DNS)...
-- Subject: Unit named.service has begun start-up
-- Defined-By: systemd
-- Support: https://access.redhat.com/support
..
-- Unit named.service has begun starting up.
Nov 21 16:09:05 server.askartashova.net bash[11311]: zone localhost.localdomain/IN: loaded serial 0
Nov 21 16:09:05 server.askartashova.net bash[11311]: zone localhost/IN: loaded serial 0
Nov 21 16:09:05 server.askartashova.net bash[11311]: zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 0
Nov 21 16:09:05 server.askartashova.net bash[11311]: zone 1.0.0.127.in-addr.arpa/IN: loaded serial 0
Nov 21 16:09:05 server.askartashova.net bash[11311]: zone 0.in-addr.arpa/IN: loaded serial 0
```



```
server [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
Nov 21 16:14
en
root@server:/var/named/master/rz
File Edit View Search Terminal Tabs Help
root@server:/var/named/master/rz
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:503:ba3e::2:30#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:503:ba3e::2:30#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:2::c#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:2::c#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:503:c27::2:30#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:12::d0d#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:7fd::1#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:7fd::1#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './DNSKEY/IN': 2001:500:9f::42#53
Nov 21 16:09:06 server.askartashova.net named[11316]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Nov 21 16:09:06 server.askartashova.net named[11316]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
Nov 21 16:09:06 server.askartashova.net named[11316]: resolver priming query complete
```

Анализ работы DNS-сервера

При помощи утилиты `dig` получим описание DNS-зоны с сервера `ns.user.net`



```
; <<>> DiG 9.11.13-RedHat-9.11.13-6.el8_2.1 <<>> ns.askartashova.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 27168
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 82a0bd19930d7bb89857ed705fb93d223ae06f943f501980 (good)
;; QUESTION SECTION:
;ns.askartashova.net.          IN      A

;; AUTHORITY SECTION:
net.                900     IN      SOA     a.gtld-servers.net. nstld.verisign-grs.com. 1605975304 1800 900
604800 86400

;; Query time: 253 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 21 16:15:30 UTC 2020
;; MSG SIZE rcvd: 149

[root@server.askartashova.net rz]#
```

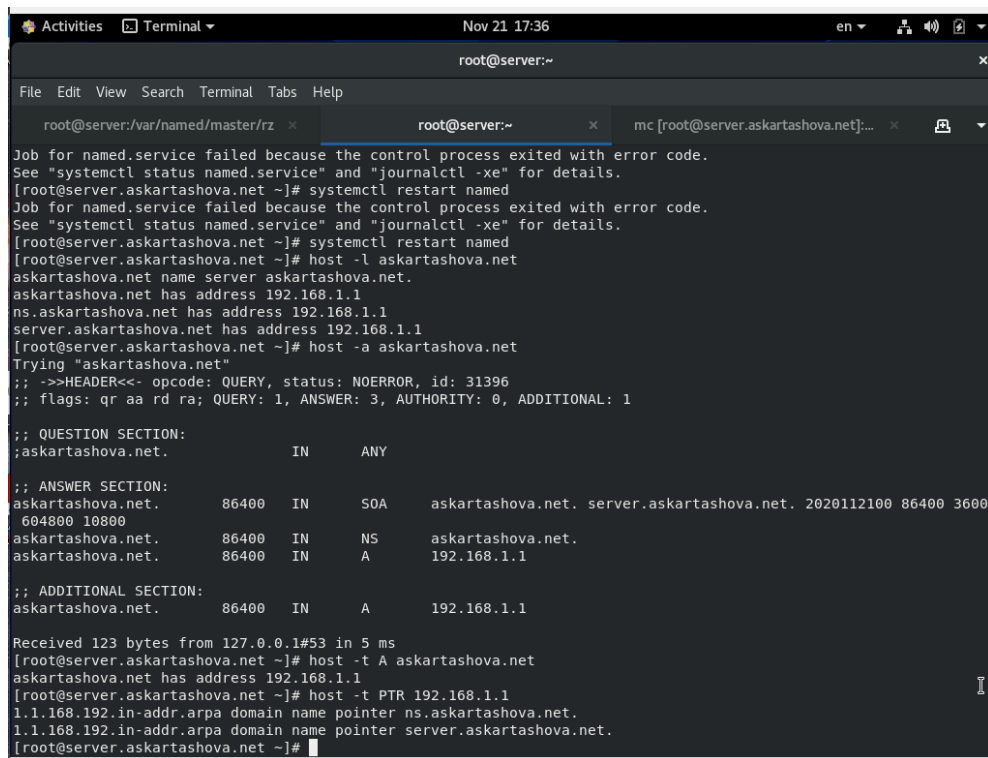
При помощи утилиты `host` проанализируйте корректность работы DNS-сервера:

`host -l user.net`

host -a user.net

host -t A user.net

host -t PTR 192.168.1.1

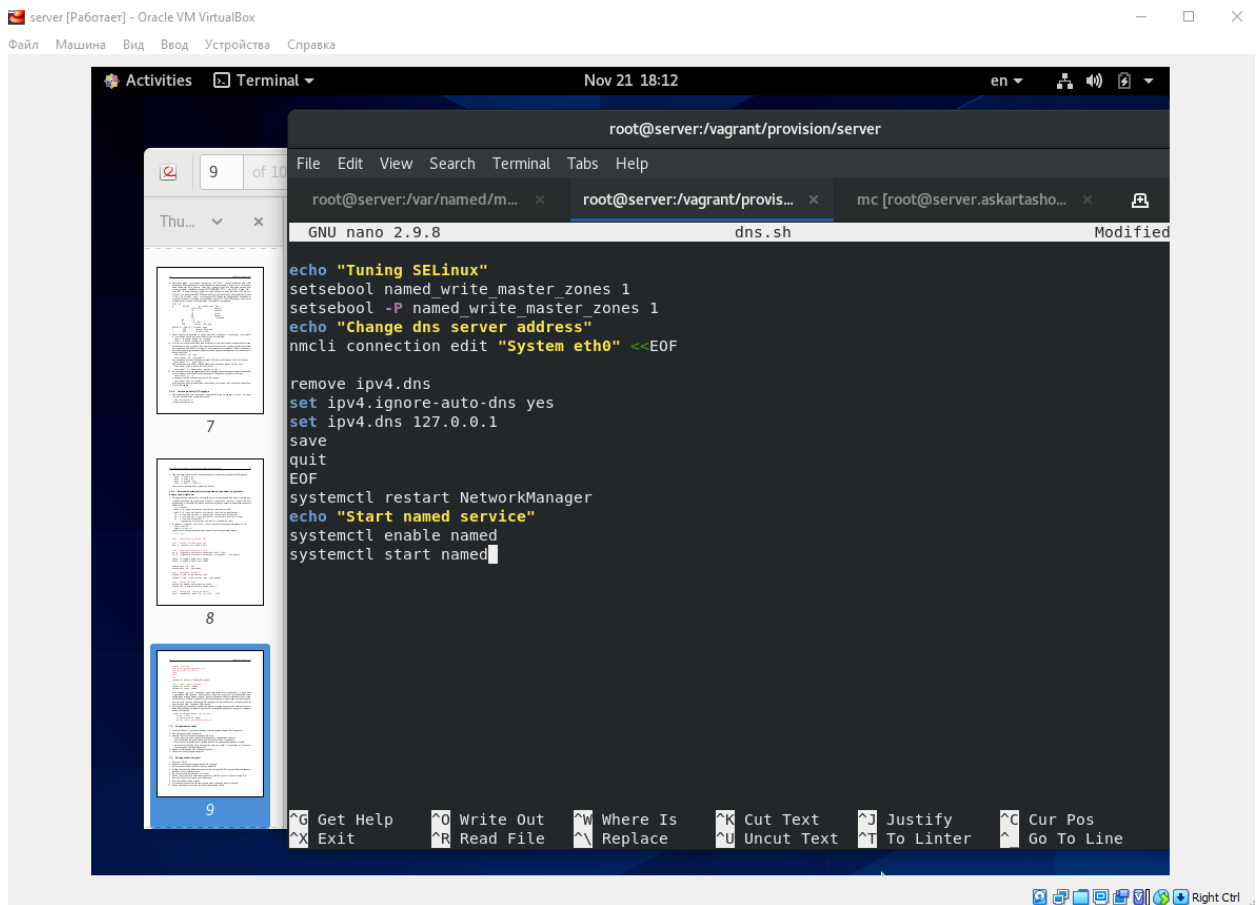


```
root@server:~  
Job for named.service failed because the control process exited with error code.  
See "systemctl status named.service" and "journalctl -xe" for details.  
[root@server.askartashova.net ~]# systemctl restart named  
Job for named.service failed because the control process exited with error code.  
See "systemctl status named.service" and "journalctl -xe" for details.  
[root@server.askartashova.net ~]# systemctl restart named  
[root@server.askartashova.net ~]# host -l askartashova.net  
askartashova.net name server askartashova.net.  
askartashova.net has address 192.168.1.1  
ns.askartashova.net has address 192.168.1.1  
server.askartashova.net has address 192.168.1.1  
[root@server.askartashova.net ~]# host -a askartashova.net  
Trying "askartashova.net"  
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 31396  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
;askartashova.net.  
IN ANY  
  
;; ANSWER SECTION:  
askartashova.net. 86400 IN SOA askartashova.net. server.askartashova.net. 2020112100 86400 3600  
604800 10800  
askartashova.net. 86400 IN NS askartashova.net.  
askartashova.net. 86400 IN A 192.168.1.1  
  
;; ADDITIONAL SECTION:  
askartashova.net. 86400 IN A 192.168.1.1  
  
Received 123 bytes from 127.0.0.1#53 in 5 ms  
[root@server.askartashova.net ~]# host -t A askartashova.net  
askartashova.net has address 192.168.1.1  
[root@server.askartashova.net ~]# host -t PTR 192.168.1.1  
1.1.168.192.in-addr.arpa domain name pointer ns.askartashova.net.  
1.1.168.192.in-addr.arpa domain name pointer server.askartashova.net.  
[root@server.askartashova.net ~]#
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dns, в который поместим в соответствующие каталоги конфигурационные файлы DNS

каталоге /vagrant/provision/server создайте исполняемый файл dns.sh. Открыв его на редактирование, пропишем в нём скрипт, повторяющий действия по конфигурированию сервера



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

```
server.vm.provision "server dns",  
type: "shell",  
preserve_order: true,  
path: "provision/server/dns.sh"
```

```
server.vm.provision "server dns",  
type: "shell",  
preserve_order: true,  
path: "provision/server/dns.sh"
```

Заключение

Мы приобрели навыки по установке и конфигурированию DNS сервера и усвоили принципы работы системы доменных имён

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 предусматривает преобразование имени в IP-адреса. Зоны обратного просмотра выполняют прямо противоположную операцию. Они предусматривают сопоставление IP-адресов с обычным именем.

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

`/etc/resolv.conf` — это основной файл настройки библиотеки распознавателя имен DNS.

`/etc/named.conf` - составляет основу конфигурации сервера DNS.

`/var/named/named.ca`- файл кэша. Показывает типовые записи корневого сервера имен.

`/var/named/named.localhost` и `/var/named/named.loopback` - описывают прямую и обратную зоны.

6. Что указывается в файле `resolv.conf`?

Этот файл содержит список ключевых слов с пользовательскими значениями, которые представляют собой различные типы информации преобразователя.

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

А-запись (Address record). Address record указывает на конкретный IP-адрес домена.

AAAA-запись (Address record to IPv6). AAAA запись DNS — аналог предыдущей А-записи. В значении указывается внешний IP-адрес в формате IPv6.

CNAME-запись (Canonical name). CNAME («каноническое имя») указывает на расположение хостов на одном сервере. С ее помощью можно прописать несколько доменов и поддоменов в рамках одного сервера.

MX-запись (Mail exchanger). MX-запись задает почтовый сервер, который будет принимать и отправлять почту для данного домена.

NS-запись (Name Server) определяет доменный адрес DNS-сервера, обслуживающий конкретный домен.

TXT-запись (Text String) используется для хранения текстовых данных о домене.

SOA-запись (Start of Authority) указывает местоположение сервера с эталонной информацией о домене.

PTR-запись служит для связывания отдельного IP-адреса с доменным именем.

RP-запись (Responsible person). Здесь прописаны реквизиты ответственных за домен.

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

Для отображения IP-адресов IPv4 в пространство доменных имен.

9. Для чего нужен домен named?

named - это сервер доменных имен пакета BIND.

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

Master-сервер (primary, первичный) доменных имен является ответственным (authoritative) за информацию о зоне. Он читает описание зоны с локального диска компьютера, на котором он функционирует и отвечает в соответствии с этим описанием на запросы resolver-ов.

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.

11. Какие параметры отвечают за время обновления зоны?

- *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;

12. Как обеспечить защиту зоны от скачивания и просмотра?

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*

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?

С помощью команд:

systemctl start <имя службы>

systemctl restart <имя службы>

systemctl stop <имя службы>

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

Systemctl status <название службы>

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

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

Приведем несколько примеров.

1. *ps*

2. *htop*

18. Приведите несколько примеров по изменению сетевого соединения при помощи

командного интерфейса *nmcli*.

1. nmcli connection edit System\ eth0

remove ipv4.dns

set ipv4.ignore-auto-dns yes

set ipv4.dns 127.0.0.1

save

quit

2. nmcli connection modify ethernet-enp0s8 ipv4.address 192.168.4.26/24

nmcli connection modify ethernet-enp0s8 ipv4.method manual

save

quit

19. Что такое SELinux?

SELinux (SELinux) — это система принудительного контроля доступа, реализованная на уровне ядра.

20. Что такое контекст (метка) SELinux?

Процессы и файлы маркируются метками - контекстом SELinux, который содержит информацию: пользователь SELinux, роль, тип и уровень (опционально)

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

restorecon -vR /etc

restorecon -vR /var/named

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

С помощью утилиты audit2allow.

23. Что такое булевый переключатель в SELinux?

Переключатели позволяют изменять части политики SELinux во время работы(без перезапуска и остановки), не обладая глубоким пониманием создания политики SELinux. Это позволяет вносить изменения, такие как: разрешение доступа службам к файловым системам NFS, без перезагрузки или recompilации политики SELinux.

24. Как посмотреть список переключателей SELinux и их состояние?

Команда: *getsebool*

25. Как изменить значение переключателя SELinux?

Команда: *setseboo*