

Лабораторная работа №2

Администрирование сетевых подсистем

Мишина А. А.

13 сентября 2024

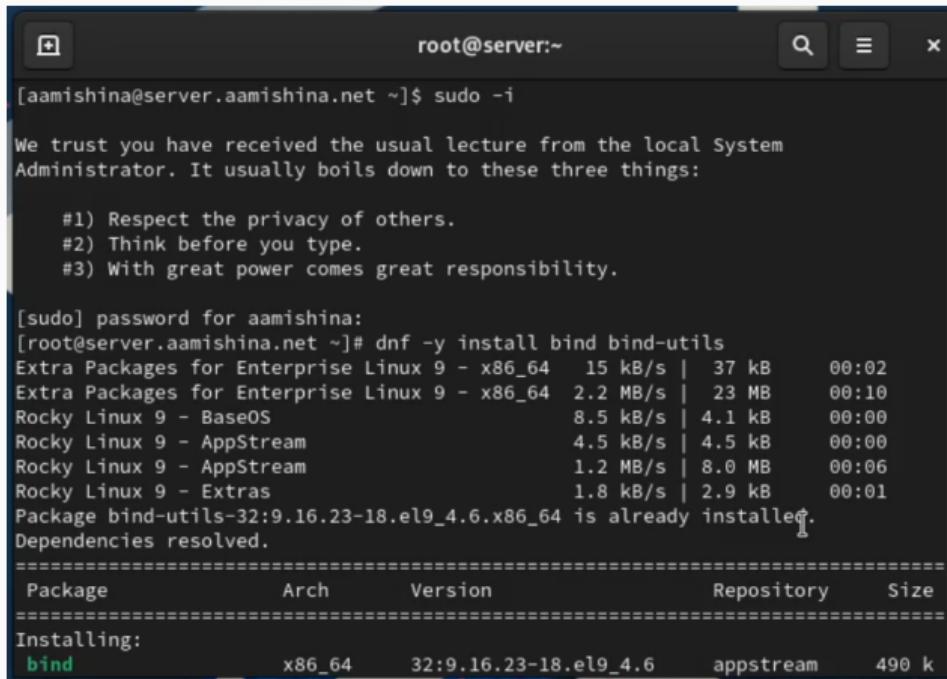
Цели и задачи

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

Выполнение лабораторной работы

Установка DNS-сервера

Bind и bind-utils

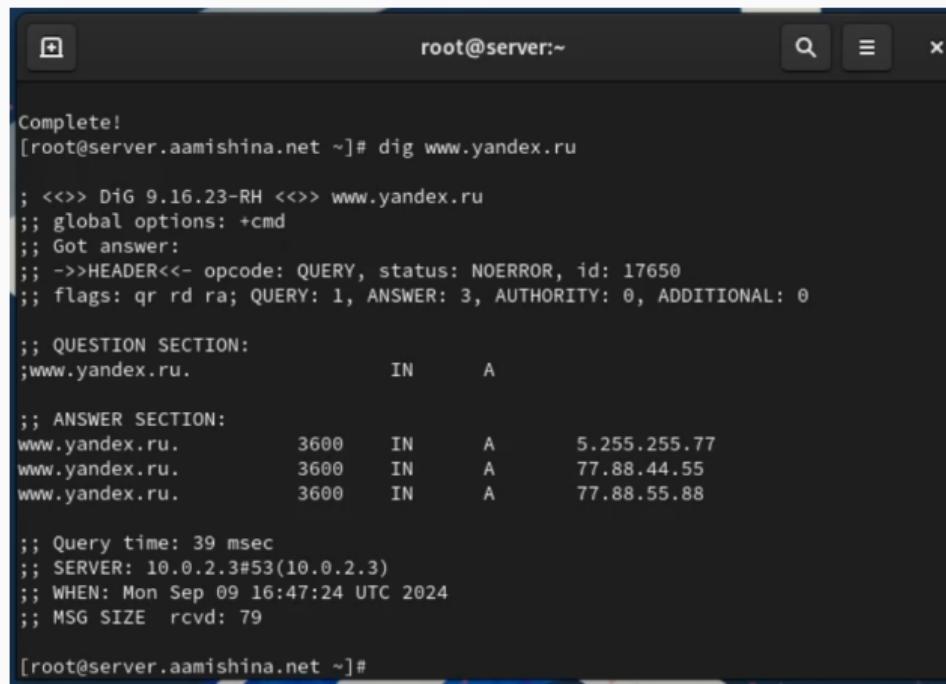


The screenshot shows a terminal window with the following session:

```
[aamishina@server.aamishina.net ~]$ sudo -i  
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:  
#1) Respect the privacy of others.  
#2) Think before you type.  
#3) With great power comes great responsibility.  
[sudo] password for aamishina:  
[root@server.aamishina.net ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 15 kB/s | 37 kB 00:02  
Extra Packages for Enterprise Linux 9 - x86_64 2.2 MB/s | 23 MB 00:10  
Rocky Linux 9 - BaseOS 8.5 kB/s | 4.1 kB 00:00  
Rocky Linux 9 - AppStream 4.5 kB/s | 4.5 kB 00:00  
Rocky Linux 9 - AppStream 1.2 MB/s | 8.0 MB 00:06  
Rocky Linux 9 - Extras 1.8 kB/s | 2.9 kB 00:01  
Package bind-utils-32:9.16.23-18.el9_4.6.x86_64 is already installed.  
Dependencies resolved.  
=====  
 Package Arch Version Repository Size  
=====  
 Installing:  
 bind x86_64 32:9.16.23-18.el9_4.6 appstream 490 k
```

Рис. 1: Переход в режим суперпользователя и установка bind, bind-utils

Запрос к DNS-адресу



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

; <>> DiG 9.16.23-RH <>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17650
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

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

;; ANSWER SECTION:
www.yandex.ru.        3600    IN      A      5.255.255.77
www.yandex.ru.        3600    IN      A      77.88.44.55
www.yandex.ru.        3600    IN      A      77.88.55.88

;; Query time: 39 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Mon Sep 09 16:47:24 UTC 2024
;; MSG SIZE rcvd: 79

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

Рис. 2: Запрос с помощью утилиты dig

Конфигурирование кэширующего DNS-сервера

Содержание файлов

```
[root@server.aamishina.net ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search aamishina.net
nameserver 10.0.2.3
```

Рис. 3: Просмотр содержания файла /etc/resolv.conf

Содержание файлов

```
[root@server.aamishina.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 files.
//

options {
    listen-on port 53 { 127.0.0.1; };
    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.recurising";
    allow-query     { localhost; };
```

Рис. 4: Просмотр содержания файла /etc/named.conf

Содержание файлов

```
[root@server.aamishina.net ~]# cat /var/named/named.ca

; <>> DiG 9.18.20 <>> -4 +tcp +norec +nostats @d.root-servers.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47286
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 27

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1450
;; QUESTION SECTION:
;. IN NS ; 

;; ANSWER SECTION:
. 518400 IN NS a.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS c.root-servers.net.
. 518400 IN NS d.root-servers.net.
```

Рис. 5: Просмотр содержания файла /var/named/named.ca

Содержание файлов

```
[root@server.aamishina.net ~]# cat /var/named/named.localhost
$TTL 1D
@      IN SOA  @ rname.invalid. (
                      0      ; serial
                      1D     ; refresh
                      1H     ; retry
                      1W     ; expire
                      3H )   ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
[root@server.aamishina.net ~]# █
```

Рис. 6: Просмотр содержания файла /var/named/named.localhost

Содержание файлов

```
[root@server.aamishina.net ~]# cat /var/named/named.loopback
$TTL 1D
@      IN SOA  @ rname.invalid. (
                           0      ; serial
                           1D     ; refresh
                           1H     ; retry
                           1W     ; expire
                           3H )   ; minimum
NS      @
A       127.0.0.1
AAAA    ::1
PTR    localhost.
[root@server.aamishina.net ~]# █
```

Рис. 7: Просмотр содержания файла /var/named/named.loopback

DNS-сервер

```
[root@server osintfdra.net ~]# systemctl start named
[root@server osintfdra.net ~]# systemctl enable named
[root@server osintfdra.net ~]# systemctl status named | grep target.wants/named.service + /usr/lib/systemd/system/named.service
[root@server osintfdra.net ~]# dig www.yandex.ru

;=> DNS 9.1.12-23-00 <== www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->HEADER-> opcode: QUERY, status: NOERROR, id: 1311
;; Flags: qr rd ra; QUERY: 3, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0
;;
;; QUESTION SECTION:
;www.yandex.ru. IN A
;;
;; ANSWER SECTION:
www.yandex.ru. 3600 IN A 77.88.55.48
www.yandex.ru. 3600 IN A 77.88.55.48
www.yandex.ru. 3600 IN A 5.255.255.77
;;
Query time: 20 msec
;; SERVER: 10.6.2.235#53(10.6.2.23)
;; WHEN: Mon Sep 19 18:51:36 UTC 2024
;; MSG SIZE rcvd: 79

[root@server osintfdra.net ~]# dig @127.0.0.1 www.yandex.ru

;=> DNS 9.1.12-23-00 <== 0.0.0.1 www.yandex.ru
;; server found
;; global options: +cmd
;; ->HEADER-> opcode: QUERY, status: NOERROR, id: 45465
;; Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;;
;; OPT PLSUBSECTION:
;; ->HEADER-> opcode: QUERY, status: NOERROR, id: 1272
;; CDS/CDNSKEY: 9bae2120a88724e800000000bf72792a070404465e7009 (good)
;;
;; QUESTION SECTION:
;www.yandex.ru. IN A
;;
;; ANSWER SECTION:
www.yandex.ru. 800 IN A 77.88.55.48
www.yandex.ru. 800 IN A 5.255.255.77
www.yandex.ru. 800 IN A 77.88.55.48
;;
Query time: 800 msec
;; SERVER: 10.6.2.235#53(10.6.2.23)
;; WHEN: Mon Sep 19 18:51:36 UTC 2024
;; MSG SIZE rcvd: 118

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

Рис. 8: Запуск DNS-сервера, включение запуска DNS-сервера в автозапуск при загрузке системы, анализ выведенной на экран информации при выполнении команды dig www.yandex.ru и dig 127.0.0.1 www.yandex.ru

DNS-сервер

```
[root@server.aamishina.net ~]# nmcli connection edit eth0
==| nmcli interactive connection editor |==

Editing existing '802-3-ethernet' connection: '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, sriov, ethtool, match, ipv4,
ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (e777ed2f-6d6c-4f97-9eac-03b7e6fc3f51) successfully updated.
nmcli> quit
[root@server.aamishina.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, sriov, ethtool, match, ipv4,
ipv6, hostname, link, 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.aamishina.net ~]#
```

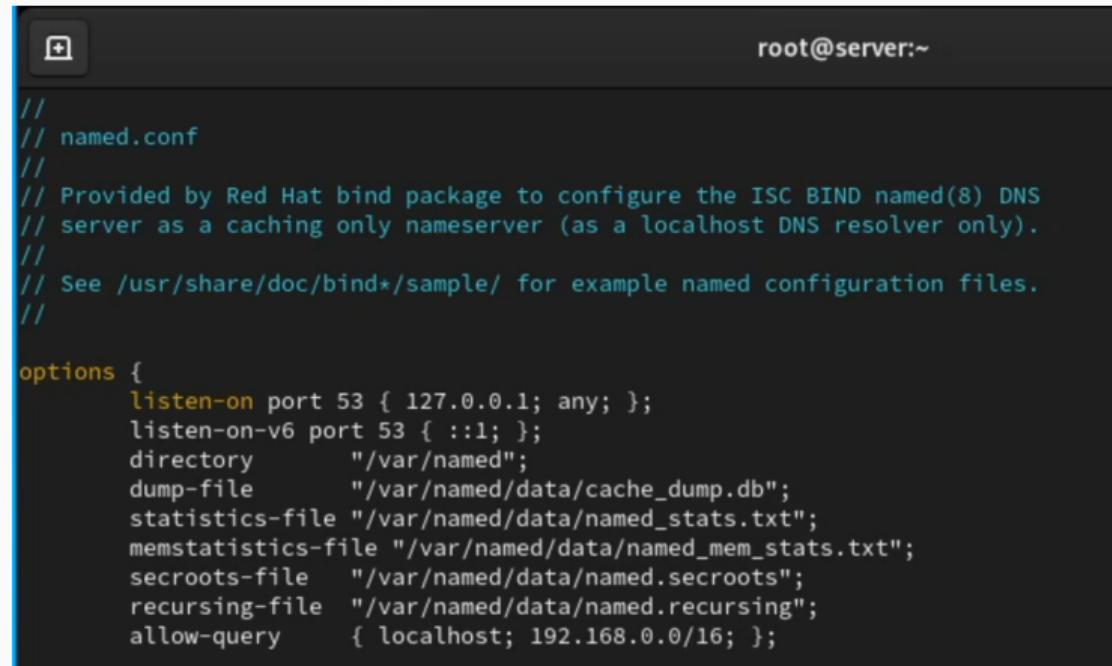
Рис. 9: Настройка DNS-сервера сервером по умолчанию для хоста server и внутренней виртуальной сети. Повторяем действия для соединения System eth0

NetworkManager

```
[root@server.aamishina.net ~]#  
[root@server.aamishina.net ~]# systemctl restart NetworkManager  
[root@server.aamishina.net ~]# cat /etc/resolv.conf  
# Generated by NetworkManager  
search aamishina.net  
nameserver 127.0.0.1  
[root@server.aamishina.net ~]# █
```

Рис. 10: Перезапуск NetworkManager и проверка наличия изменений в файле /etc/resolv.conf

DNS-запросы



```
//  
// 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; };  
};
```

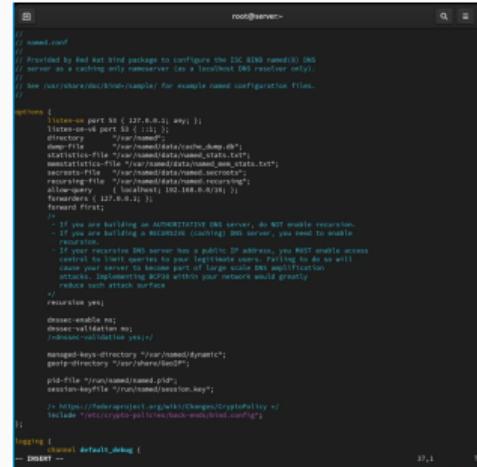
Рис. 11: Настройка направление DNS-запросов от всех узлов внутренней сети, включая запросы от узла server, через узел server

Внос изменений

```
[root@server.aamishina.net ~]# vim /etc/named.conf
[root@server.aamishina.net ~]# firewall-cmd --add-service=dns
success
[root@server.aamishina.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.aamishina.net ~]# lsof | grep UDP
lsof: can't stat() / fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
avahi-dae 569          avahi  12u    IPv4  19739  0t0  UDP *:mdns
avahi-dae 569          avahi  13u    IPv4  19739  0t0  UDP *:mdns
avahi-dae 569          avahi  14u    IPv4  19731  0t0  UDP +:44550
avahi-dae 569          avahi  15u    IPv6  19732  0t0  UDP +:32091
chronyd  667           chrony  5u    IPv4  19891  0t0  UDP localhost:323
chronyd  667           chrony  6u    IPv6  19892  0t0  UDP localhost:323
named   9938           named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938           named  2lu    IPv6  47384  0t0  UDP localhost:domain
named   9938  9939 isc-net-0 named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938  9939 isc-net-0 named  24u   IPv6  47384  0t0  UDP localhost:domain
named   9938  9940 isc-net-0 named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938  9940 isc-net-0 named  24u   IPv6  47384  0t0  UDP localhost:domain
named   9938  9941 isc-timer named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938  9941 isc-timer named  24u   IPv6  47384  0t0  UDP localhost:domain
named   9938  9942 isc-socke named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938  9942 isc-socke named  24u   IPv6  47384  0t0  UDP localhost:domain
named   9938  9970 isc-net-0 named  2lu    IPv4  47382  0t0  UDP localhost:domain
named   9938  9970 isc-net-0 named  24u   IPv6  47384  0t0  UDP localhost:domain
NetworkMa 10000         root   27u    IPv4  50282  0t0  UDP server.aamishin
a.net:bootpc->_gateway:bootps
NetworkMa 10000 10014 gmain root   27u    IPv4  50282  0t0  UDP server.aamishin
a.net:bootpc->_gateway:bootps
NetworkMa 10000 10015 gibus root   27u    IPv4  50282  0t0  UDP server.aamishin
a.net:bootpc->_gateway:bootps
[root@server.aamishina.net ~]#
```

Рис. 12: Внос изменений в настройки межсетевого экрана узла server, разрешив работу с DNS.
Проверка, что DNS-запросы идут через узел server, который прослушивает порт 53

Перенаправление DNS-запросов



```
root@server: /etc/named.conf
// named.conf
// Provided by Red Hat bind package to configure the ISC BIND named() DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
// See /usr/share/doc/bind-sample/etc/named.conf.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";
    secrets-file   "/var/named/data/named_secrets.txt";
    recursion      "/var/named/data/named_recursion";
    allow-transfer  { 127.0.0.1; 192.168.0.0/16; };
    forwarders { 127.0.0.1; };
    forward first;
    // If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
    // If you are building a recursive (caching) DNS server, you need to enable
    // recursion.
    // If your recursive DNS server has a public IP address, you MUST enable access
    // control to limit queries to your network, otherwise an attacker will
    // cause your server to become part of large scale DNS amplification
    // attacks. Implementing BGP6P within your network would greatly
    // reduce this attack surface
    recursion yes;
};

dnssec-enable no;
dnssec-validation no;
//dnssec-validation yes;

managed-keys-directory "/var/named/dynamic";
geoip-directory "/var/named/GeoIP";

pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";
// https://fedoraproject.org/wiki/Changes/CryptoPolicy
// include "/etc/crypt-police/named/named.conf";
};

logging {
    channel default_debug {
        file "/var/named/named.log";
        severity info;
    };
};
```

Рис. 13: Добавление перенаправлений DNS-запросов на конкретный вышестоящий DNS-сервер и дополнительных настроек

Конфигурирование первичного DNS-сервера

Шаблон

```
[root@server.aamishina.net ~]# cp /etc/named.rfc1912.zones /etc/named/
[root@server.aamishina.net ~]# cd /etc/named
[root@server.aamishina.net named]# mv /etc/named/named.rfc1912.zones /etc/named/aamishina.net
[root@server.aamishina.net named]# vim /etc/named.conf
```

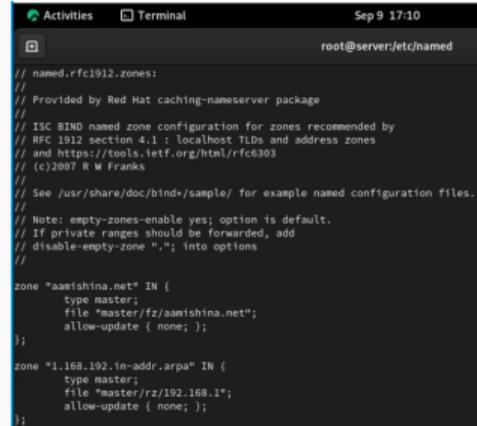
Рис. 14: Копирование шаблона описания DNS-зон из каталога /etc в каталог /etc/named и изменение его названия

Файл описания зоны

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/aamishina.net";
-- INSERT --
```

Рис. 15: Включение файла описания зоны /etc/named/aamishina.net в конфигурационном файле DNS /etc/named.conf

Файл /etc/named/aamishina.net



```
Activities Terminal Sep 9 17:10
root@server:/etc/named
// 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 "aamishina.net" IN {
    type master;
    file "master/fz/aamishina.net";
    allow-update { none; };
};

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

Рис. 16: Открытие файла /etc/named/user.net на редактирование. Прописывание своей прямой зоны, обратной зоны и удаление остальных записей в файле

Файлы прямой и обратной зоны

```
[root@server.aamishina.net named]# cd /var/named
[root@server.aamishina.net named]# mkdir -p /var/named/master/fz
[root@server.aamishina.net named]# mkdir -p /var/named/master/rz
[root@server.aamishina.net named]# cp /var/named/named.localhost /var/named/master/fz/
[root@server.aamishina.net named]# cd /var/named/master/fz/
[root@server.aamishina.net fz]# mv named.localhost aamishina.net
[root@server.aamishina.net fz]# ls
aamishina.net
[root@server.aamishina.net fz]# vim /var/named/master/fz/aamishina.net
```

Рис. 17: В каталоге /var/named создание подкаталогов master/fz и master/rz. Копирование шаблона прямой DNS-зоны named.localhost из каталога /var/named в каталог /var/named/master/fz и изменение его названия

Прямая зона

```
root@server:/var/named/master/fz

$TTL 1D
@ IN SOA @ server.aamishina.net. (
    2024072700 ; serial
    1D          ; refresh
    1H          ; retry
    1W          ; expire
    3H )        ; minimum
NS      @
A      192.168.1.1
$ORIGIN aamishina.net.
server A      192.168.1.1
ns     A      192.168.1.1
~
~
```

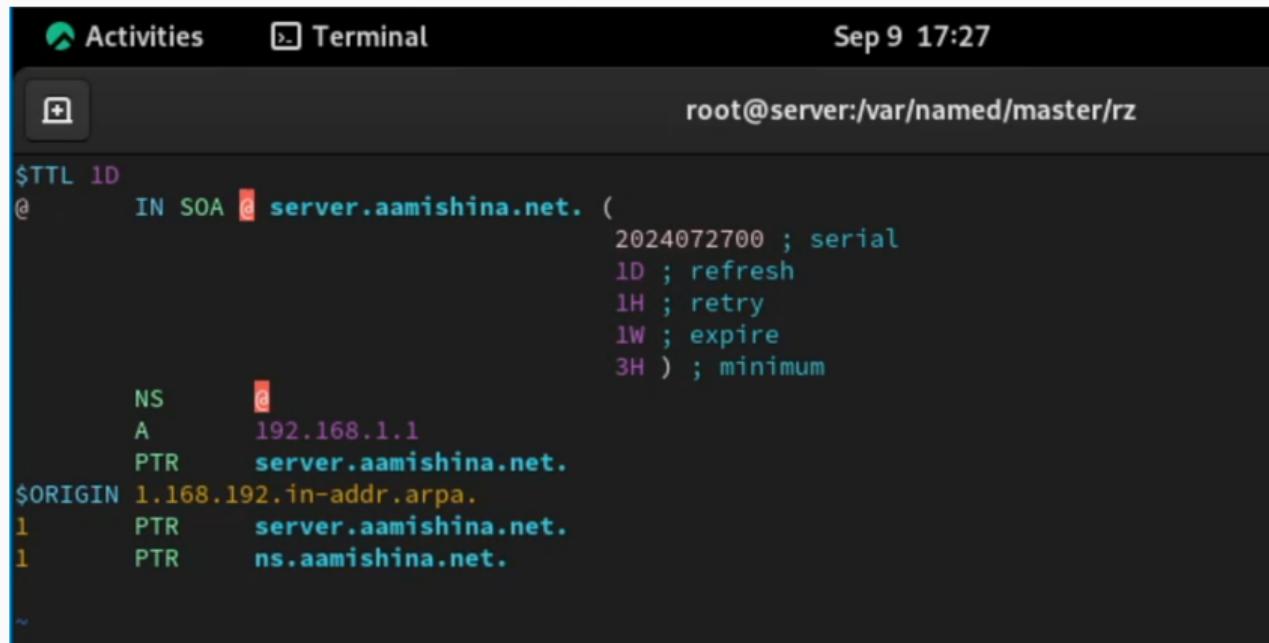
Рис. 18: Изменение файла /var/named/master/fz/aamishina.net, указав необходимые DNS записи для прямой зоны

Обратная зона

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

Рис. 19: Копирование шаблона обратной DNS-зоны named.loopback из каталога /var/named в каталог /var/named/master/rz и изменение его названия

Обратная зона



The screenshot shows a terminal window titled "Terminal" running as "root" on a server. The current directory is "/var/named/master/rz". The terminal displays the contents of a DNS zone file:

```
$TTL 1D
@ IN SOA @ server.aamishina.net. (
                                2024072700 ; serial
                                1D ; refresh
                                1H ; retry
                                1W ; expire
                                3H ) ; minimum
        NS      @
        A       192.168.1.1
        PTR    server.aamishina.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR    server.aamishina.net.
1      PTR    ns.aamishina.net.

~
```

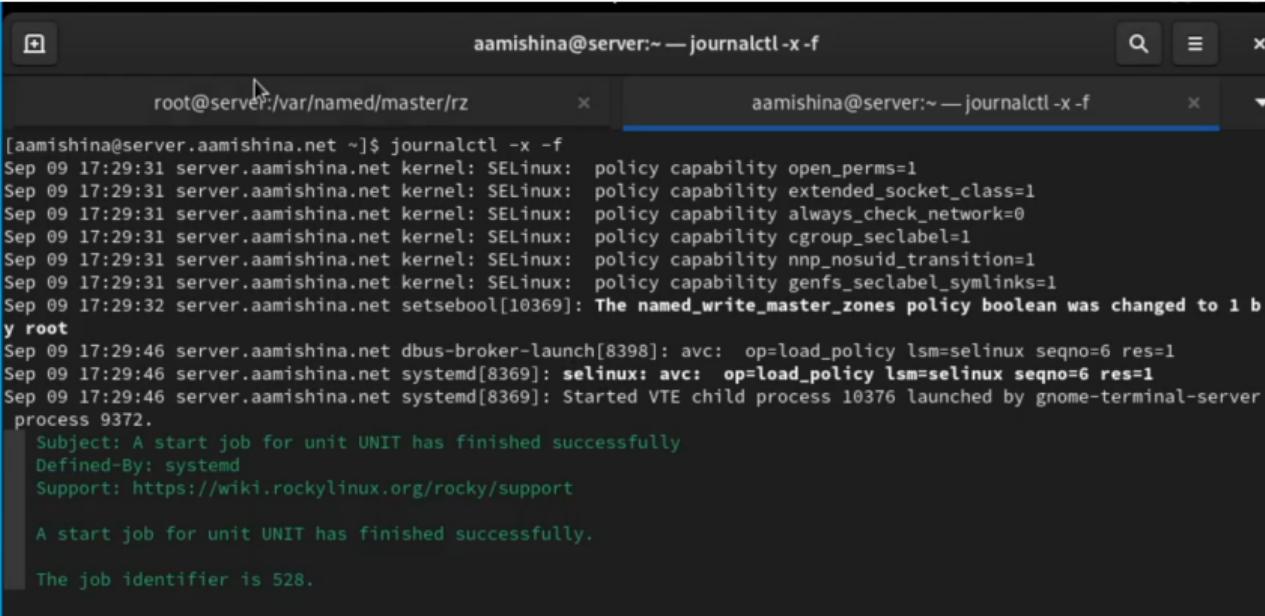
Рис. 20: Изменение файла /var/named/master/rz/192.168.1, указав необходимые DNS записи для обратной зоны

Права доступа

```
[root@server.aamishina.net rz]# chown -R named:named /etc/named
[root@server.aamishina.net rz]# chown -R named:named /var/named
[root@server.aamishina.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.aamishina.net rz]# restorecon -vR /var/named
[root@server.aamishina.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.aamishina.net rz]# setsebool named_write_master_zones 1
[root@server.aamishina.net rz]# setsebool -P named_write_master_zones 1
[root@server.aamishina.net rz]# █
```

Рис. 21: Исправление прав доступа к файлам в каталогах /etc/named и /var/named, корректное восстановление их меток в SELinux, проверка состояния переключателей SELinux

Лог системных сообщений



The screenshot shows a terminal window with two tabs. The left tab is titled "root@server:/var/named/master/rz" and the right tab is titled "aamishina@server:~ — journalctl -x -f". Both tabs have a search icon and a close button. The right tab is active and displays the command "journalctl -x -f" followed by its output. The output shows kernel messages about SELinux policy changes and systemd unit start jobs. One job is for the "dbus-broker-launch" service, and another is for the "systemd" service. The logs also mention the "gnome-terminal-server" process.

```
[aamishina@server.aamishina.net ~]$ journalctl -x -f
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability open_perms=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability extended_socket_class=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability always_check_network=0
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability cgroup_seclabel=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability nnp_nosuid_transition=1
Sep 09 17:29:31 server.aamishina.net kernel: SELinux: policy capability genfs_seclabel_symlinks=1
Sep 09 17:29:32 server.aamishina.net setsebool[10369]: The named_write_master_zones policy boolean was changed to 1 by root
Sep 09 17:29:46 server.aamishina.net dbus-broker-launch[8398]: avc: op=load_policy lsm=selinux seqno=6 res=1
Sep 09 17:29:46 server.aamishina.net systemd[8369]: selinux: avc: op=load_policy lsm=selinux seqno=6 res=1
Sep 09 17:29:46 server.aamishina.net systemd[8369]: Started VTE child process 10376 launched by gnome-terminal-server process 9372.
Subject: A start job for unit UNIT has finished successfully
Defined-By: systemd
Support: https://wiki.rockylinux.org/rocky/support

A start job for unit UNIT has finished successfully.

The job identifier is 528.
```

Рис. 22: Запуск расширенного лога системных сообщений

```
[root@server.aamishina.net rz]# systemctl restart named  
[root@server.aamishina.net rz]# █
```

Рис. 23: Перезапуск DNS-сервера

Лог системных сообщений

Рис. 24: Проверка корректности работы системы

Анализ работы DNS-сервера

Описание DNS-зоны

```
[root@server.aamishina.net rz]# dig ns.aamishina.net

; <>> DiG 9.16.23-RH <>> ns.aamishina.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14222
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 0fe6f20b93ee4fad0100000066df30db6b33879431200bea (good)
;; QUESTION SECTION:
;ns.aamishina.net.           IN      A

;; ANSWER SECTION:
ns.aamishina.net.    86400   IN      A      192.168.1.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Sep 09 17:31:07 UTC 2024
;; MSG SIZE  rcvd: 89

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

Рис. 25: Получение описания DNS-зоны с сервера ns.aamishina.net.

DNS-сервер

```
[root@server.aamishina.net rz]# host -l aamishina.net
aamishina.net name server aamishina.net.
aamishina.net has address 192.168.1.1
ns.aamishina.net has address 192.168.1.1
server.aamishina.net has address 192.168.1.1
[root@server.aamishina.net rz]# host -a aamishina.net
Trying "aamishina.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57685
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;aamishina.net.           IN      ANY

;; ANSWER SECTION:
aamishina.net.      86400   IN      SOA     aamishina.net. server.aamishina.net. 2024072700 86400 3600 604800 108
00
aamishina.net.      86400   IN      NS      aamishina.net.
aamishina.net.      86400   IN      A       192.168.1.1

;; ADDITIONAL SECTION:
aamishina.net.      86400   IN      A       192.168.1.1

Received 120 bytes from 127.0.0.1#53 in 0 ms
[root@server.aamishina.net rz]# host -t A aamishina.net
aamishina.net has address 192.168.1.1
[root@server.aamishina.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer server.aamishina.net.
1.1.168.192.in-addr.arpa domain name pointer ns.aamishina.net.
[root@server.aamishina.net rz]#
```

Рис. 26: Анализ корректности работы DNS-сервера

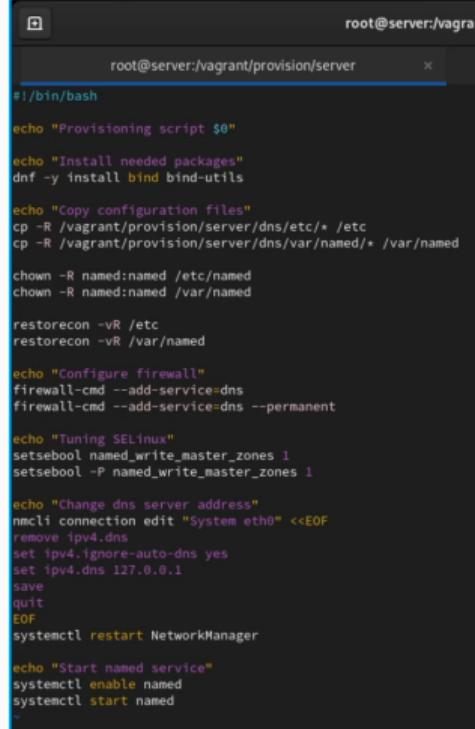
Внесение изменений в настройки внутреннего окружения виртуальной машины

Файл dns.sh

```
[root@server.aamishina.net rz]# cd /vagrant
[root@server.aamishina.net vagrant]# mkdir -p /vagrant/provision/server/dns/etc/named
[root@server.aamishina.net vagrant]# mkdir -p /vagrant/provision/server/dns/var/named/master/
[root@server.aamishina.net vagrant]# cp -R /etc/named.conf /vagrant/provision/server/dns/etc/
[root@server.aamishina.net vagrant]# cp -R /etc/named/* /vagrant/provision/server/dns/etc/named/
[root@server.aamishina.net vagrant]# cp -R /var/named/master/* /vagrant/provision/server/dns/var/named/master/
[root@server.aamishina.net vagrant]# cd /vagrant/provision/server/
[root@server.aamishina.net server]# touch dns.sh
[root@server.aamishina.net server]# chmod +x dns.sh
[root@server.aamishina.net server]# vim dns.sh
```

Рис. 27: Переход в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создание в нём каталога dns, в который помещаем конфигурационные файлы DNS. Создание в каталоге /vagrant/provision/server исполняемого файла dns.sh

Файл dns.sh



```
root@server:/vagrant/provision/server
#!/bin/bash

echo "Provisioning script $0"

echo "Install needed packages"
dnf -y install bind bind-utils

echo "Copy configuration files"
cp -R /vagrant/provision/server/dns/etc/* /etc
cp -R /vagrant/provision/server/dns/var/named/* /var/named

chown -R named:named /etc/named
chown -R named:named /var/named

restorecon -vR /etc
restorecon -vR /var/named

echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

echo "Tuning SELinux"
setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1

echo "Change dns server address"
nmcli connection edit "System eth0" <<EOF
remove ipv4.dns
set ipv4.ignore-auto-dns yes
set ipv4.dns 127.0.0.1
save
quit
EOF
systemctl restart NetworkManager

echo "Start named service"
systemctl enable named
systemctl start named
"
```

Рис. 28: Открытие файла на редактирование и прописывание в нём скрипта

Vagrantfile



```
## Server configuration
config.vm.define "server", autostart: false do |server|
  server.vm.box = "rocky9"
  server.vm.hostname = 'server'

  server.vm.boot_timeout = 1440

  server.ssh.insert_key = false
  server.ssh.username = 'vagrant'
  server.ssh.password = 'vagrant'

  server.vm.network :private_network,
    ip: "192.168.1.1",
    virtualbox_intnet: true

  server.vm.provision "server dummy",
    type: "shell",
    preserve_order: true,
    path: "provision/server/01-dummy.sh"

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

  server.vm.provider :virtualbox do |v|
    v.linked_clone = true
    # Customize the amount of memory on the VM
  end
end
```

Рис. 29: Добавление параметров в конфигурационном файле Vagrantfile в разделе конфигурации для сервера

Вывод

- В ходе выполнения данной лабораторной работы я приобрела практические навыки по установке и конфигурированию DNS-сервера, усвоила принципы работы системы доменных имён.