

Лабораторная работа №2

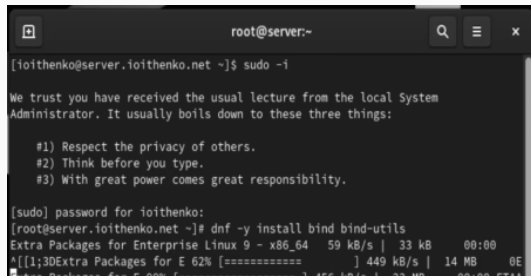
Администрирование сетевых подсистем

Ищенко Ирина НПИбд-02-22

Российский университет дружбы народов, Москва, Россия

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

Выполнение лабораторной работы



```
root@server:~  
[ioithenko@server.ioithenko.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 ioithenko:  
[root@server.ioithenko.net ~]# dnf -y install bind bind-utils  
Extra Packages for Enterprise Linux 9 - x86_64 59 kB/s | 33 kB 00:00  
^[[1;3DEExtra Packages for E 62% [=====] 449 kB/s | 14 MB 0E  
Extra Packages for E 60% [=====] 455 kB/s | 33 MB 00:00 5741
```

Рис. 1: Установка bind

```
root@server:~  
Complete!  
[root@server.ioithenko.net ~]# dig www.yandex.ru  
  
; <<>> DiG 9.16.23-RH <<>> www.yandex.ru  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 11095  
;; 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      77.88.55.88  
www.yandex.ru.                3600    IN      A      5.255.255.77  
www.yandex.ru.                3600    IN      A      77.88.44.55  
  
;; Query time: 8 msec  
;; SERVER: 10.0.2.3#53(10.0.2.3)  
;; WHEN: Wed Sep 11 12:55:34 UTC 2024  
;; MSG SIZE rcvd: 79  
  
[root@server.ioithenko.net ~]#
```

Рис. 2: dig

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

Рис. 3: Запуск сервера

```
root@server:~  
[root@server.ioithenko.net ~]# dig @127.0.0.1 www.yandex.ru  
; <<>> DiG 9.16.23-RH <<>> @127.0.0.1 www.yandex.ru  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 17675  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
;; OPT PSEUDOSECTION:  
;; EDNS: version: 0, flags:; udp: 1232  
;; COOKIE: 9297481dc0e3b1470100000066e1946900e612b76ad34100 (good)  
;; QUESTION SECTION:  
;www.yandex.ru.                IN      A  
;; ANSWER SECTION:  
www.yandex.ru.                600     IN      A      5.255.255.77  
www.yandex.ru.                600     IN      A      77.88.44.55  
www.yandex.ru.                600     IN      A      77.88.55.88  
;; Query time: 552 msec  
;; SERVER: 127.0.0.1#53(127.0.0.1)  
;; WHEN: Wed Sep 11 13:00:25 UTC 2024
```

Рис. 4: dig

```
[root@server.ioithenko.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'eth0'

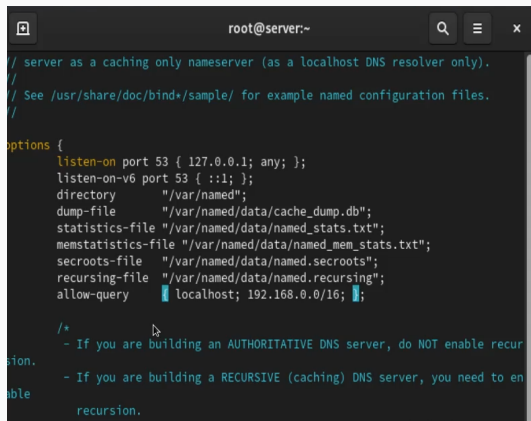
Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-
-lx, 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' (26191b97-32fc-41fd-8f79-0e2901b0e876) successfully updated.
nmcli> quit
[root@server.ioithenko.net ~]# systemctl restart NetworkManager
[root@server.ioithenko.net ~]#
```

Рис. 5: Изменение настроек сетевого соединения eth0


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

Рис. 6: Перезапуск NetworkManager и просмотр файла

A terminal window titled 'root@server:~' with search, menu, and close icons. It displays the configuration for the BIND DNS server in the 'options' block of /etc/named.conf. The configuration includes listening on port 53 for IPv4 and IPv6, setting various data files, and restricting queries to localhost and the 192.168.0.0/16 network. Comments explain the difference between authoritative and recursive server configurations.

```
// 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; ;  
  
    /*  
     * - If you are building an AUTHORITATIVE DNS server, do NOT enable recur  
     *   sion.  
     * - If you are building a RECURSIVE (caching) DNS server, you need to en  
     *   able  
     *   recursion.  
     */  
}
```

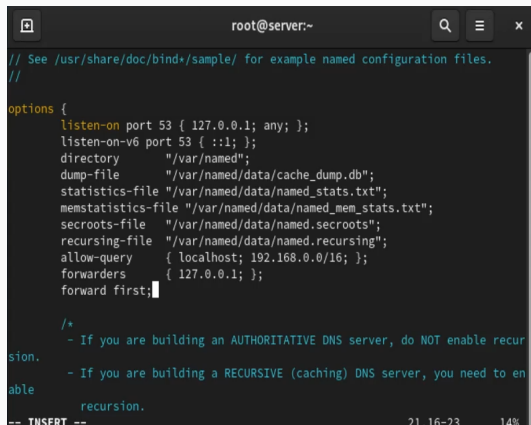
Рис. 7: Внесение изменений в файл /etc/named.conf

```

[root@server.ioithenko.net ~]# firewall-cmd --add-service=dns
success
[root@server.ioithenko.net ~]# firewall-cmd --add-service=dns --permanent
success
[root@server.ioithenko.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
Output information may be incomplete.
avahi-daemon 570      0t0      UDP *:mdns          avahi    12u      IPv4          19659
avahi-daemon 570      0t0      UDP *:mdns          avahi    13u      IPv6          19660
avahi-daemon 570      0t0      UDP *:46069        avahi    14u      IPv4          19661
avahi-daemon 570      0t0      UDP *:33616        avahi    15u      IPv6          19662
chronyd      610      0t0      UDP localhost:323   chrony    5u      IPv4          19759
chronyd      610      0t0      UDP localhost:323   chrony    6u      IPv6          19760

```

Рис. 8: Внесение изменений в настройки межсетевого экрана узла **server**, проверка



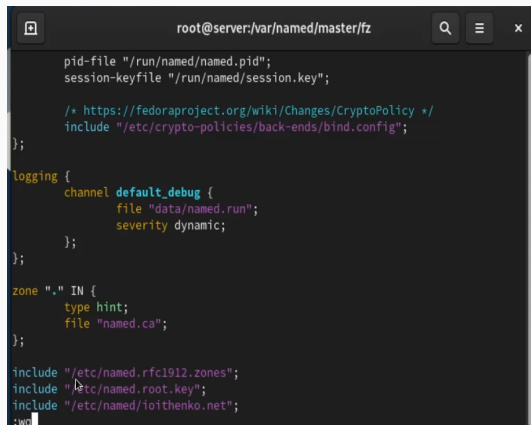
```
root@server:~
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
options {
    listen-on port 53 { 127.0.0.1; any; };
    listen-on-v6 port 53 { ::1; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    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; };
    forwarders      { 127.0.0.1; };
    forward first;
}

/*
- If you are building an AUTHORITATIVE DNS server, do NOT enable recur
sion.
- If you are building a RECURSIVE (caching) DNS server, you need to en
able
    recursion.
-- INSERT --
```

Рис. 9: Редактирование named.conf

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

Рис. 10: Команды

A terminal window with a dark background and light-colored text. The title bar at the top shows the user is root at a server, in the directory /var/named/master/fz. The terminal content shows a configuration file for BIND. It includes settings for pid-file, session-keyfile, and logging. A comment refers to the Fedora project's CryptoPolicy wiki. The logging section is configured with a default debug channel. A zone "." is defined with a hint type and a file named named.ca. At the bottom, three include statements are present: /etc/named.rfc1912.zones, /etc/named.root.key, and /etc/named/ioithenko.net. The cursor is positioned at the end of the last include statement.

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

pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";

/* https://fedoraproject.org/wiki/Changes/CryptoPolicy */
include "/etc/crypto-policies/back-ends/bind.config";
};

logging {
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
};

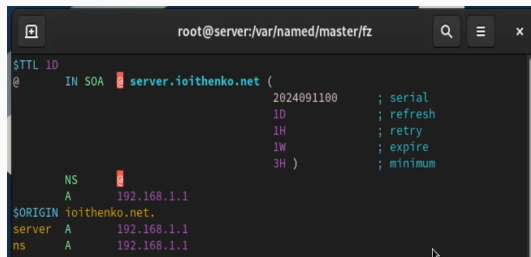
zone "." IN {
    type hint;
    file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/ioithenko.net";
:WQ
```

Рис. 11: Редактирование файла /etc/named/ioithenko.net

```
[root@server.ioithenko.net named]# cd /var/named
[root@server.ioithenko.net named]# mkdir -p /var/named/master/fz
[root@server.ioithenko.net named]# mkdir -p /var/named/master/rz
[root@server.ioithenko.net named]# cp /var/named/named.localhost /var/named/master/fz
[root@server.ioithenko.net named]# cp /var/named/named.localhost /var/named/master/rz/
cp: overwrite '/var/named/master/fz/named.localhost'? y
[root@server.ioithenko.net named]# cd /var/named/master/fz/
[root@server.ioithenko.net fz]# mv named.localhost ioithenko.net
[root@server.ioithenko.net fz]#
```

Рис. 12: Создание каталогов, копирование шаблона прямой зоны, переименование

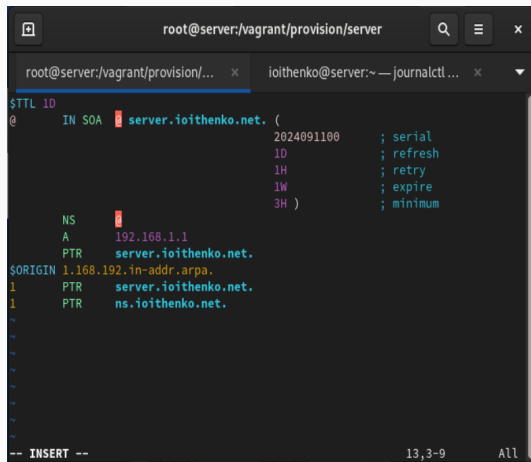
A terminal window with a dark background and light-colored text. The title bar shows 'root@server:/var/named/master/fz'. The terminal content shows a DNS zone file configuration for 'server.ioithenko.net'. It includes an SOA record with a serial number of 2024091100, refresh interval of 1D, retry interval of 1H, expire interval of 1W, and a minimum TTL of 3H. It also includes an NS record pointing to 192.168.1.1. At the bottom, there are three A records: '\$ORIGIN ioithenko.net.', 'server A 192.168.1.1', and 'ns A 192.168.1.1'.

```
root@server:/var/named/master/fz
$TTL 1D
@      IN SOA  server.ioithenko.net (
                                2024091100      ; serial
                                1D                ; refresh
                                1H                ; retry
                                1W                ; expire
                                3H )              ; minimum
      NS  server.ioithenko.net.
      A   192.168.1.1
$ORIGIN ioithenko.net.
server A 192.168.1.1
ns      A 192.168.1.1
```

Рис. 13: Редактирование `/var/named/master/fz/ioithenko.net`


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

Рис. 14: Копирование шаблона обратной зоны, переименование



The image shows a terminal window with a dark background. The title bar at the top reads 'root@server:/vagrant/provision/server'. There are two tabs open: 'root@server:/vagrant/provision/...' and 'ioithenko@server:~ — journalctl ...'. The terminal content shows a DNS zone file being edited. The first section is the SOA record for 'server.ioithenko.net.' with parameters: serial 2024091100, refresh 1D, retry 1H, expire 1W, and minimum 3H. The second section is the NS record pointing to 'server.ioithenko.net.'. The third section is the A record pointing to '192.168.1.1'. The fourth section is the PTR record for '1.168.192.in-addr.arpa.' pointing to 'server.ioithenko.net.'. The fifth section is the PTR record for 'ns.ioithenko.net.' pointing to 'ns.ioithenko.net.'. The terminal ends with a prompt '-- INSERT --' and a status bar showing '13,3-9' and 'All'.

```
root@server:/vagrant/provision/server
root@server:/vagrant/provision/... x ioithenko@server:~ — journalctl ... x
$TTL 1D
@      IN SOA  server.ioithenko.net. (
                                2024091100 ; serial
                                1D          ; refresh
                                1H          ; retry
                                1W          ; expire
                                3H )        ; minimum

      NS   server.ioithenko.net.
      A    192.168.1.1
      PTR  server.ioithenko.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR  server.ioithenko.net.
1      PTR  ns.ioithenko.net.
~
~
~
~
~
~
~
~
-- INSERT --                               13,3-9    All
```

Рис. 15: Редактирование /var/named/master/rz/192.168.1

```
[root@server.ioithenko.net rz]# chown -R named:named /etc/named
[root@server.ioithenko.net rz]# chown -R named:named /var/named
[root@server.ioithenko.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.ioithenko.net rz]# restorecon -vR /var/named
[root@server.ioithenko.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.ioithenko.net rz]# setsebool named_write_master_zones 1
bash: setsebool: command not found...
[root@server.ioithenko.net rz]# setsebool named_write_master_zones 1
[root@server.ioithenko.net rz]# setsebool -P named_write_master_zones 1
[root@server.ioithenko.net rz]#
```

Рис. 16: Изменение прав доступа, восстановление меток SELinux, проверка

```
[root@server.ioithenko.net rz]# systemctl restart named
[root@server.ioithenko.net rz]# dig ns.ioithenko.net

; <<>> DiG 9.16.23-RH <<>> ns.ioithenko.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36561
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 764a4ab7134134fc0100000066e1a0964e949cd6f1893123 (good)
;; QUESTION SECTION:
ns.ioithenko.net.      IN      A

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

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Sep 11 13:52:22 UTC 2024
```

Рис. 17: Описание DNS-зоны с сервера ns.ioithenko.net

```
[root@server.ioithenko.net rz]# host -l ioithenko.net
ioithenko.net name server ioithenko.net.
ioithenko.net has address 192.168.1.1
ns.ioithenko.net has address 192.168.1.1
server.ioithenko.net has address 192.168.1.1
```

```
[root@server.ioithenko.net rz]# host -a ioithenko.net
Trying "ioithenko.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43325
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

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

;; ANSWER SECTION:
ioithenko.net.                86400   IN      SOA      ioithenko.net. server.ioithen
o.net. 2024091100 86400 3600 604800 10800
ioithenko.net.                86400   IN      NS       ioithenko.net.
ioithenko.net.                86400   IN      A        192.168.1.1

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

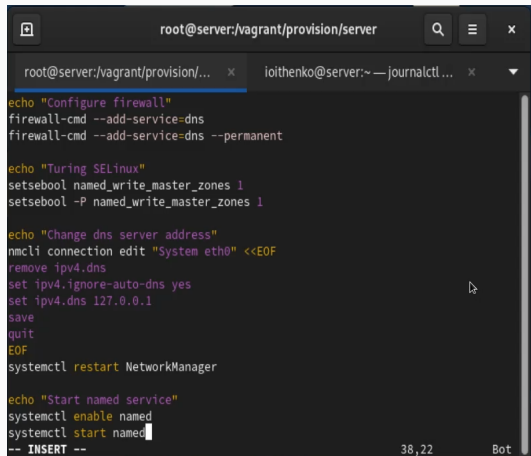
Received 120 bytes from 127.0.0.1#53 in 12 ms
[root@server.ioithenko.net rz]# host -t A ioithenko.net
ioithenko.net has address 192.168.1.1
```

```
[root@server.ioithenko.net server]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.ioithenko.net.
1.1.168.192.in-addr.arpa domain name pointer server.ioithenko.net.
```

Рис. 18: Анализ корректности работы DNS-сервера

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

Рис. 19: Размещение конфигурационных файлов в каталог /vagrant/provision/server/dns



```
root@server:/vagrant/provision/server
root@server:/vagrant/provision/... x ioithenko@server:~ — journalctl ... x
echo "Configure firewall"
firewall-cmd --add-service=dns
firewall-cmd --add-service=dns --permanent

echo "Turing 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
-- INSERT --
38,22 Bot
```

Рис. 20: Редактирование скрипта dns.sh



The image shows a screenshot of a text editor window titled "Vagrantfile - Блокнот". The menu bar includes "Файл", "Правка", "Формат", "Вид", and "Справка". The editor contains the following Vagrantfile configuration:

```
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"
```

Рис. 21: Редактирование Vagrantfile

В ходе лабораторной работы я приобрела практические навыки по установке и конфигурированию DNSсервера, усвоила принципы работы системы доменных имён.