11. Модуль 1. Задание 10

Задание

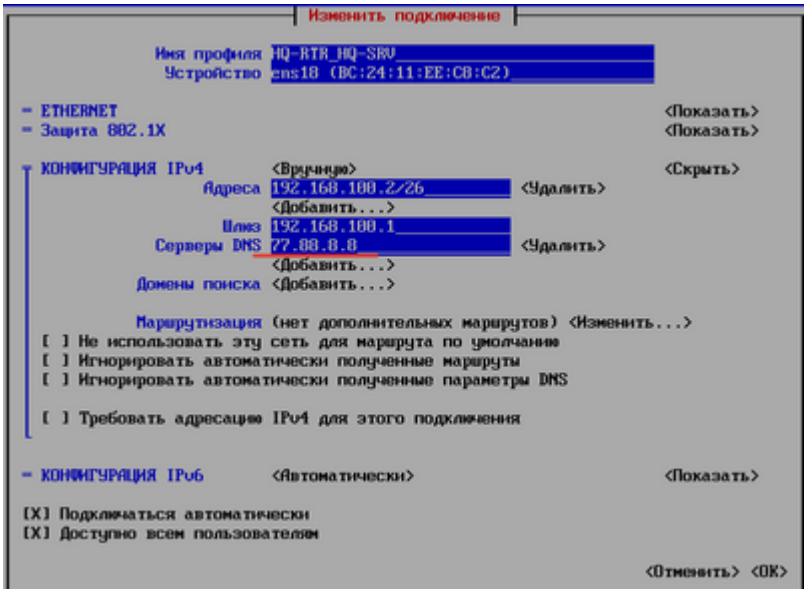
Настройка DNS для офисов HQ и BR.

- Основной DNS-сервер реализован на HQ-SRV.
- Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 2
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер

Реализация

Установка и настройка

Для установки пакетов `bind` **и** `bind-utils` **в настройках** `HQ-SRV` **добавим адрес** `DNS- сервер`



Устанавливаем пакета DNS-сервера `bind`

```
# dnf install bind bind-utils
```

Редактируем конфигурационный файл `/var/named.conf`

```
# nano  /etc/named.conf
```

В данном файле необходимо изменить следующие строки, содержащие

`listen-on port 53 ;`
`listen-on-v6 port 53 ;`
`allow-query ;`
`forwarders ;` (*дописать строку)*
`dnssec-validation` (заменить на `none`)

и привести их к виду

```
 GNU nano 7.2                                                /etc/named.conf.bak
//
// 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; 192.168.100.0/26; 192.168.100.64/28; 192.168.200.0/27; };
        listen-on-v6 port 53 { none; };
        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     { any; };
        forwarders      { 77.88.8.8;};

        /*
         - 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 legitimate users. Failing to do so will
           cause your server to become part of large scale DNS amplification
           attacks. Implementing BCP38 within your network would greatly
           reduce such attack surface
        */
        recursion yes;

        dnssec-validation no;

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

где:

`listen-on port 53 { 127.0.0.1; 192.168.0.0/26; 192.168.100.64/28; 192.1 };` — IP-сети DNS-сервера, на котором он будет принимать запросы; (можно прописать `any` - слушать везде)

`listen-on-v6 port 53` присвоим значение `none` , тем самым отключив `ipv6`

`allow-query` разрешает выполнять запросы всем, но из соображений безопасности можно ограничить доступ для конкретной сети.

`forwarders` перенаправляем запросы, которые сами не резолвим, на DNS сервер Яндекса.

Объявляем файлы зон, дописываем в конец файла `/var/named.conf` следующие строки

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

zone "au-team.irpo" {
        type master;
        file "master/au-team.db";
};

zone "100.168.192.in-addr.arpa" {
        type master;
        file "master/au-team_rev.db";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

где:

Прямая зона

zone "au-team.irpo"{ ... }; определения зоны `au-team.irpo` . В кавычках указывается имя зоны, которое следует разрешать на этом сервере.

type master ; Указывает тип зоны. `type master` означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.

file "au-team.db"; Указывает путь к файлу, который содержит данные зоны `au-team.irpo` . Файлы зоны используются для хранения записей DNS, таких как A-записи, CNAME-записи, MX-записи и т. д.

Обратная зона

zone "100.168.192.in-addr.arpa"{ ... }; определения обратной зоны `au-team.irpo` .

type master ; Указывает тип зоны. `type master` означает, что эта зона является мастер-зоной, то есть она содержит авторитетные записи, которые могут быть изменены и обновлены на этом сервере.

file "au-team_rev.db"; Указывает путь к файлу обратной зоны, который содержит данные обратной зоны `au-team.irpo` .

С помощью утилиты `named-checkconf` проверяется наличие ошибок в конфигурационном файле, если результат выполнения команды пуст - ошибок нет.

```
# named-checkconf
```

Создание локальных зон DNS

Создайте папку с мастер зонами:

```
# mkdir /var/named/master
```

Зона прямого просмотра

Для сокращения времени написания файла прямой зоны (`au-team.db`) скопируем шаблон и отредактируем его

```
# cp /var/named/named.localhost /var/named/master/au-team.db
```

Открываем на редактирование файл зоны `au-team.db`

```
# nano /var/named/master/au-team.db
```

И приводим его к следующему виду

```
 GNU nano 7.2
$TTL 1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        IN      NS      au-team.irpo.
        IN      A       192.168.100.2
hq-rtr  IN      A       192.168.100.1
br-rtr  IN      A       192.168.200.1
hq-srv  IN      A       192.168.100.2
hq-cli  IN      A       192.168.100.66
br-srv  IN      A       192.168.200.2
moodle  CNAME   hq-rtr.au-team.irpo.
wiki    CNAME   hq-rtr.au-team.irpo.
```

Зона обратного просмотра

Для сокращения времени написания файла обратной зоны (`au-team_rev.db`) скопируем шаблон и отредактируем его

```
# cp /var/named/named.loopback /var/named/master/au-team_rev.db
```

Открываем на редактирование файл зоны `au-team_rev.db`

```
# nano /var/named/master/au-team.db
```

И приводим его к следующему виду

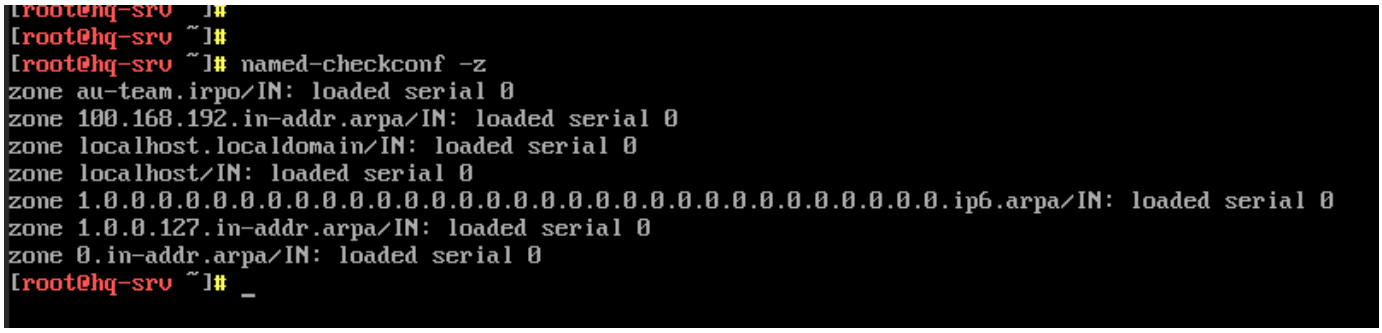
```
 GNU nano 7.2
$TTL 1D
@       IN SOA  au-team.irpo. root.au-team.irpo. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum

        IN      NS      au-team.irpo.
1       IN      PTR     hq-rtr.au-team.irpo.
2       IN      PTR     hq-srv.au-team.irpo.
66      IN      PTR     hq-cli.au-team.irpo.
```

Назначаем владельца и права.

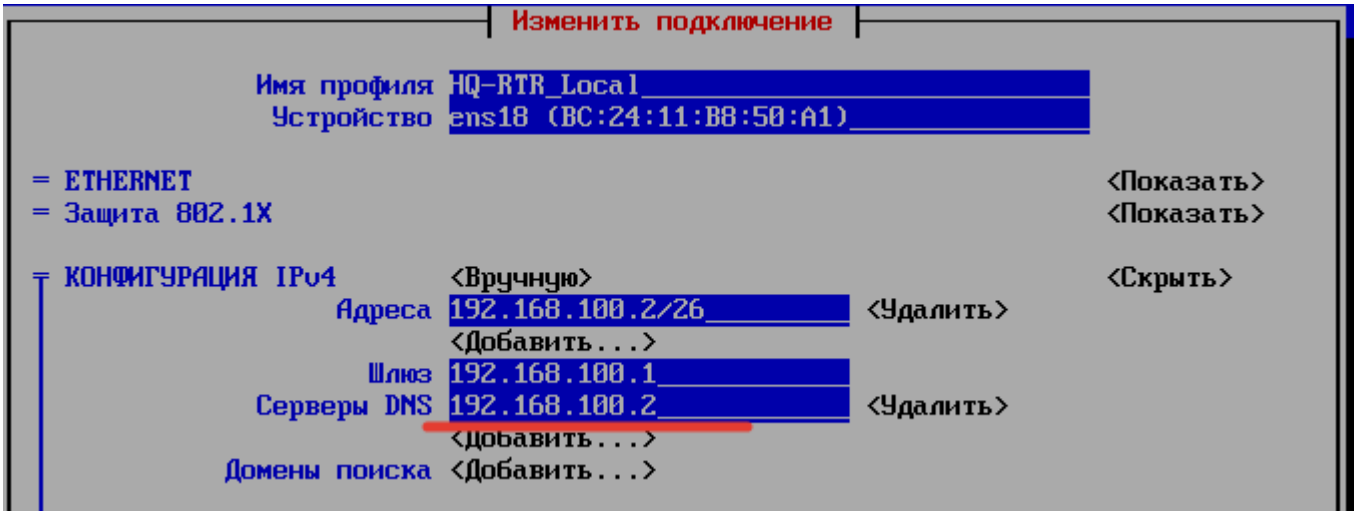
```
# chown -R root:named /var/named/master

# chmod 0640 /var/named/master/*
```

С помощью утилиты `named-checkconf -z` **проверяется наличие ошибок в конфигурационном файле и файлах зон.**

```
# named-checkconf -z
```



На `HQ-SRV` **в настройках сетевого интерфейса убедиться, что в качестве первичного** `DNS` **сервера указан его собственный** `IP – адрес`



Также необходимо проверить
на `BR-SRV` , что в качестве первичного `DNS` сервера указан `IP – адрес HQ-SRV`
`HQ-CLI` - должен получать автоматически по DHCP

Запуск и добавление в автозагрузку DNS - сервера:

```
# systemctl enable --now named
```

Тестирование

Проверяем работу DNS на HQ-SRV с BR-SRV с помощью команды `host`

```
[root@br-srv ~]#
[root@br-srv ~]# ping -c4 au-team.irpo
PING au-team.irpo (192.168.100.2) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.100.2): icmp_seq=1 ttl=62 time=2.35 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.2): icmp_seq=2 ttl=62 time=1.79 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.2): icmp_seq=3 ttl=62 time=1.85 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.2): icmp_seq=4 ttl=62 time=1.57 ms

--- au-team.irpo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.570/1.889/2.353/0.286 ms
[root@br-srv ~]#
```

Прямая зона

```
[root@br-srv ~]#
[root@br-srv ~]#
[root@br-srv ~]# host hq-rtr.au-team.irpo
hq-rtr.au-team.irpo has address 192.168.100.1
[root@br-srv ~]#
[root@br-srv ~]# host br-rtr.au-team.irpo
br-rtr.au-team.irpo has address 192.168.200.1
[root@br-srv ~]#
[root@br-srv ~]# host hq-srv.au-team.irpo
hq-srv.au-team.irpo has address 192.168.100.2
[root@br-srv ~]#
[root@br-srv ~]# host hq-cli.au-team.irpo
hq-cli.au-team.irpo has address 192.168.100.66
[root@br-srv ~]#
[root@br-srv ~]# host br-srv.au-team.irpo
br-srv.au-team.irpo has address 192.168.200.2
[root@br-srv ~]#
[root@br-srv ~]# host moodle.au-team.irpo
moodle.au-team.irpo is an alias for hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo has address 192.168.100.1
[root@br-srv ~]#
[root@br-srv ~]# host wiki.au-team.irpo
wiki.au-team.irpo is an alias for hq-rtr.au-team.irpo.
hq-rtr.au-team.irpo has address 192.168.100.1
[root@br-srv ~]# _
```

Обратная зона

```
[root@br-srv ~]#
[root@br-srv ~]# host 192.168.100.1
1.100.168.192.in-addr.arpa domain name pointer hq-rtr.au-team.irpo.
[root@br-srv ~]#
[root@br-srv ~]# host 192.168.100.2
2.100.168.192.in-addr.arpa domain name pointer hq-srv.au-team.irpo.
[root@br-srv ~]#
[root@br-srv ~]# host 192.168.100.66
66.100.168.192.in-addr.arpa domain name pointer hq-cli.au-team.irpo.
[root@br-srv ~]#
```

Проверка работоспособности DNS с помощью `nslookup`

Для определения IP-адреса сервера по его доменному:

```
# nslookup <доменное_имя>
```

```
[root@br-srv ~]#
[root@br-srv ~]# nslookup hq-rtr.au-team.irpo
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.1

[root@br-srv ~]#
[root@br-srv ~]# nslookup wiki.au-team.irpo
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
wiki.au-team.irpo       canonical name = hq-rtr.au-team.irpo.
Name:   hq-rtr.au-team.irpo
Address: 192.168.100.1

[root@br-srv ~]#
```

Также с помощью утилиты `nslookup` может быть выполнено обратное преобразование IP-адреса в доменное имя.

```
# nslookup <IP-адрес>
```

```
[root@br-srv ~]#
[root@br-srv ~]# nslookup  192.168.100.2
2.100.168.192.in-addr.arpa      name = hq-srv.au-team.irpo.

Authoritative answers can be found from:

[root@br-srv ~]#
[root@br-srv ~]# nslookup  192.168.100.66
66.100.168.192.in-addr.arpa     name = hq-cli.au-team.irpo.

Authoritative answers can be found from:

[root@br-srv ~]# _
```

Выполнить команду `ping` по доменному инеми

```
[root@br-srv ~]#
[root@br-srv ~]# ping -c4 hq-cli.au-team.irpo
PING hq-cli.au-team.irpo (192.168.100.66) 56(84) bytes of data.
64 bytes from hq-cli.au-team.irpo (192.168.100.66): icmp_seq=1 ttl=62 time=1.87 ms
64 bytes from hq-cli.au-team.irpo (192.168.100.66): icmp_seq=2 ttl=62 time=1.69 ms
64 bytes from hq-cli.au-team.irpo (192.168.100.66): icmp_seq=3 ttl=62 time=1.63 ms
64 bytes from hq-cli.au-team.irpo (192.168.100.66): icmp_seq=4 ttl=62 time=1.92 ms

--- hq-cli.au-team.irpo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.633/1.778/1.924/0.120 ms
[root@br-srv ~]#
[root@br-srv ~]# ping -c4 hq-rtr.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.100.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=1 ttl=63 time=1.47 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=2 ttl=63 time=1.35 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=3 ttl=63 time=1.19 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=4 ttl=63 time=1.34 ms

--- hq-rtr.au-team.irpo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.194/1.337/1.465/0.096 ms
[root@br-srv ~]#
[root@br-srv ~]# ping -c4 wiki.au-team.irpo
PING hq-rtr.au-team.irpo (192.168.100.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=1 ttl=63 time=1.77 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=2 ttl=63 time=1.47 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=3 ttl=63 time=1.58 ms
64 bytes from hq-rtr.au-team.irpo (192.168.100.1): icmp_seq=4 ttl=63 time=1.46 ms

--- hq-rtr.au-team.irpo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.459/1.570/1.767/0.123 ms
[root@br-srv ~]# _
```