

Настройка DNS для офисов HQ и BR.

## Пункт 1

Настройка DNS-сервера, начинается с установки пакета BIND, с помощью команды:

```
apt-get update && apt-get install bind -y
```

Далее выполняется редактирование конфигурационного файла `/var/lib/bind/etc/options.conf` согласно скриншоту, используя текстовый редактор `vim`:

```
options {
    version "unknown";
    directory "/etc/bind/zone";
    dump-file "/var/run/named/named_dump.db";
    statistics-file "/var/run/named/named.stats";
    recursing-file "/var/run/named/named.recursing";
    secroots-file "/var/run/named/named.secroots";

    // disables the use of a PID file
    pid-file none;

    /*
     * Oftenly used directives are listed below.
     */

    listen-on { 192.168.100.1; };
    listen-on-v6 { none; };

    /*
     * If the forward directive is set to "only", the server will only
     * query the forwarders.
     */
    //forward only;
    forwarders { 77.88.8.8; };

    /*
     * Specifies which hosts are allowed to ask ordinary questions.
     */
    allow-query { any; };

    /*
     * This lets "allow-query" be used to specify the default zone access
     * level rather than having to have every zone override the global
     * value. "allow-query-cache" can be set at both the options and view
     * levels. If "allow-query-cache" is not set then "allow-recursion" is
     * used if set, otherwise "allow-query" is used if set unless
     * "recursion no;" is set in which case "none;" is used, otherwise the
     * default (localhost; localnets;) is used.
     */
    //allow-query-cache { localnets; };

    /*
     * Specifies which hosts are allowed to make recursive queries
     * through this server. If not specified, the default is to allow
     * recursive queries from all hosts. Note that disallowing recursive
     * queries for a host does not prevent the host from retrieving data
     * that is already in the server's cache.
     */
    allow-recursion { any; };
}
```

`listen-on` – параметр задает адреса и порты, на которых DNS-сервер будет слушать запросы.

`forwarders` – задаются сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне.

`allow-query` – IP-адреса и подсети от которых будут обрабатываться запросы.

Далее необходимо добавить зоны прямого и обратного просмотра в файл `/var/lib/bind/etc/rfc1912.conf`, используя текстовый редактор `vim`:

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

zone "100.168.192.in-addr.arpa" {
    type master;
    file "100.168.192.in-addr.arpa";
};
```

Необходимо перейти в директорию `/var/lib/bind/etc/zone` и путем копирования создать файлы зон:

```
(root@hq-srv ~)# cd /var/lib/bind/etc/zone/
(root@hq-srv zone)# cp empty au-team.irpo
(root@hq-srv zone)# cp empty 100.168.192.in-addr.arpa
(root@hq-srv zone)#
```

Необходимо сконфигурировать файл `au-team.irpo`, который является прямой зоной следующим образом:

```
(root@hq-srv zone)## cat au-team.irpo
; BIND reverse data file for empty rfc1918 zone

; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it and use that copy.

$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025020600    ; serial
                                12H            ; refresh
                                1H            ; retry
                                1W            ; expire
                                1H            ; ncache
                        )

                IN      NS       au-team.irpo.
                IN      A        192.168.100.1
hq-rtr     IN      A        192.168.100.62
hq-rtr     IN      A        192.168.100.78
hq-rtr     IN      A        192.168.100.86
pr-rtr     IN      A        192.168.200.30
hq-srv     IN      A        192.168.100.1
hq-cli     IN      A        192.168.100.65
moodle     IN      CNAME      hq-rtr.au-team.irpo.
wiki       IN      CNAME      hq-rtr.au-team.irpo.
(root@hq-srv zone)##
```

Далее необходимо настроить обратную зону и привести файл 100.168.192.in-addr.arpa к следующему виду:

```

[root@hq-srv zone]# cat 100.168.192.in-addr.arpa
; BIND reverse data file for empty rfc1918 zone
;
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it and use that copy.
;
$TTL      1D
@         IN      SOA      au-team.irpo. root.au-team.irpo. (
                                2025020600      ; serial
                                12H               ; refresh
                                1H               ; retry
                                1W               ; expire
                                1H               ; ncache
                        )
                        IN      NS      au-team.irpo.
62        IN      PTR      hq-rtr.au-team.irpo.
78        IN      PTR      hq-rtr.au-team.irpo.
86        IN      PTR      hq-rtr.au-team.irpo.
1         IN      PTR      hq-srv.au-team.irpo.
65        IN      PTR      hq-cli.au-team.irpo.
[root@hq-srv zone]#

```

После того, как конфигурация зон была завершена, для корректной работы службы bind необходимо выполнить команду:

```
rndc-confgen > /etc/bind/rndc.key
```

Затем выполнить команду:

```
sed -i '6,$d' rndc.key
```

Перед запуском службы надо заменить группу у файлов зон, которые были созданы ранее, на named, а также проверить конфигурационные файлы и файлы зон командами named-checkconf и named-checkconf -z соответственно:

```

[root@hq-srv etc]# chgrp -R named /var/lib/bind/etc/zone/
[root@hq-srv etc]# named-checkconf
[root@hq-srv etc]# named-checkconf -z
zone localhost/IN: loaded serial 2025020600
zone localdomain/IN: loaded serial 2025020600
zone 127.in-addr.arpa/IN: loaded serial 2025020600
zone 0.in-addr.arpa/IN: loaded serial 2025020600
zone 255.in-addr.arpa/IN: loaded serial 2025020600
zone au-team.irpo/IN: loaded serial 2025020600
zone 100.168.192.in-addr.arpa/IN: loaded serial 2025020600
[root@hq-srv etc]#

```

После этого

можно запустить службу bind командой:

```
systemctl enable --now bind.service
```

Проверить статус службы можно при помощи команды:

```
systemctl status bind:
```

```

[root@hq-srv etc]# systemctl enable --now bind
Synchronizing state of bind.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable bind
Created symlink /etc/systemd/system/multi-user.target.wants/bind.service → /lib/systemd/system/bind.service.
[root@hq-srv etc]# systemctl status bind.service
bind.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/lib/systemd/system/bind.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2025-04-08 09:34:10 MSK; 4s ago
     Process: 19285 ExecStartPre=/etc/init.d/bind rndc_keygen (code=exited, status=0/SUCCESS)
     Process: 19289 ExecStartPre=/usr/sbin/named-checkconf $CHROOT -z /etc/named.conf (code=exited, status=0/SUCCESS)
     Process: 19290 ExecStart=/usr/sbin/named -u named $CHROOT $RETAIN_CAPS $EXTRAOPTIONS (code=exited, status=0/SUCCESS)
    Tasks: 8 (limit: 2339)
   Memory: 18.5M
     CPU: 64ms
   CGroup: /system.slice/bind.service
           └─ 19291 /usr/sbin/named -u named

Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 192.58.12.1
Apr 08 09:34:10 hq-srv.au-team.irpo named[19291]: REFUSED unexpected RCODE resolving './NS/IN': 192.58.12.1

```

Проверить доступ в сеть Интернет средствами утилиты ping, учитывая, что в качестве DNS-сервера используется HQ-SRV:

```

[root@hq-srv etc]# ping -c3 ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data:
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=241 time=0.042 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=241 time=0.041 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=241 time=0.041 ms

```

Используя утилиту host или nslookup проверить записи типа A, PTR и CNAME.

Закончить задание 10