

По заданию

1. Процесс конфигурирования

По шагам из инструкции выше

2. Конфигурационные файлы

◦ Debian

■ `/etc/bind/named.conf.options` (комментарии удалены)

```
1 options {  
2     directory "/var/cache/bind";  
3  
4     forwarders {  
5         10.10.10.10;  
6     };  
7     // dnssec-validation auto;  
8     allow-query { any; };  
9     listen-on-v6 { any; };  
10 };
```

■ `/etc/bind/named.conf.default-zones`

```
1 zone "skill39.wsr" {  
2     type master;  
3     file "/opt/dns/skill39.wsr.db";  
4     allow-transfer {192.168.20.10; };  
5 };  
6  
7 zone "20.16.172.in-addr.arpa" {  
8     type master;  
9     file "/opt/dns/20.16.172.in-addr.arpa.db";  
10    allow-transfer {192.168.20.10; };  
11 };  
12  
13 zone "100.16.172.in-addr.arpa" {  
14     type master;  
15     file "/opt/dns/100.16.172.in-addr.arpa.db";  
16     allow-transfer {192.168.20.10; };  
17 };  
18  
19 zone "200.16.172.in-addr.arpa" {  
20     type master;  
21     file "/opt/dns/200.16.172.in-addr.arpa.db";  
22     allow-transfer {192.168.20.10; };  
23 };  
24  
25 zone "20.168.192.in-addr.arpa" {  
26     type master;  
27     file "/opt/dns/20.168.192.in-addr.arpa.db";  
28     allow-transfer {192.168.20.10; };  
29 };
```

- Файл прямой зоны **skill39.wsr (/opt/dns/)**

```

1 ;
2 ; BIND data file for local loopback interface
3 ;
4 $TTL      604800
5 @         IN      SOA      ns01.skill39.wsr. root.skill39.wsr. (
6                               10          ; Serial
7                               604800      ; Refresh
8                               86400       ; Retry
9                               2419200     ; Expire
10                              604800 )     ; Negative Cache TTL
11 ;
12 @         IN      NS       ns01.skill39.wsr.
13 @         IN      NS       ns02.skill39.wsr.
14 l-srv     IN      A        172.16.20.10
15 ns01      IN      A        172.16.20.10
16 ns02      IN      A        192.168.20.10
17 server    IN      CNAME    l-srv
18 l-fw      IN      A        172.16.20.1
19 l-fw      IN      A        172.16.50.1
20 l-fw      IN      A        172.16.55.1
21 r-fw      IN      A        192.168.20.1
22 www       IN      CNAME    r-fw
23 r-srv     IN      A        192.168.20.10
24 l-cli-a   IN      A        172.16.100.65
25 l-cli-b   IN      A        172.16.200.61

```

- Файл обратной зоны **20.16.172.in-addr.arpa (/opt/dns)**

```

1 ;
2 ; BIND reverse data file for local loopback interface
3 ;
4 $TTL      604800
5 @         IN      SOA      ns01.skill39.wsr. root.skill39.wsr. (
6                               5          ; Serial
7                               604800      ; Refresh
8                               86400       ; Retry
9                               2419200     ; Expire
10                              604800 )     ; Negative Cache TTL
11 ;
12 @         IN      NS       ns01.skill39.wsr.
13 @         IN      NS       ns02.skill39.wsr.
14 10        IN      PTR      ns01.skill39.wsr.
15 10        IN      PTR      l-srv.skill39.wsr.
16 1         IN      PTR      l-fw.skill39.wsr.

```

- CentOS

- /etc/named.conf (комментарии сокращены)

```

1 //
2 // named.conf
3 //
4 options {

```

```

5      listen-on port 53 { any; };
6      listen-on-v6 port 53 { ::1; };
7      directory      "/var/named";
8      dump-file       "/var/named/data/cache_dump.db";
9      statistics-file "/var/named/data/named_stats.txt";
10     memstatistics-file
11     "/var/named/data/named_mem_stats.txt";
12     secroots-file   "/var/named/data/named.secroots";
13     recursing-file  "/var/named/data/named.recursing";
14
15     allow-notify {172.16.20.10; };
16     allow-query     { any; };
17
18     recursion yes;
19
20     // dnssec-enable yes;
21     // dnssec-validation yes;
22
23     managed-keys-directory "/var/named/dynamic";
24
25     pid-file "/run/named/named.pid";
26     session-keyfile "/run/named/session.key";
27
28     /* https://fedoraproject.org/wiki/Changes/CryptoPolicy
29     */
30     include "/etc/crypto-policies/back-ends/bind.config";
31 };
32
33 logging {
34     channel default_debug {
35         file "data/named.run";
36         severity dynamic;
37     };
38 };
39
40 zone "." IN {
41     type hint;
42     file "named.ca";
43 };
44
45 include "/etc/named.rfc1912.zones";
46 include "/etc/named.root.key";

```

■ **/etc/named.rfc1912.zones** (комментарии сокращены)

```

1 // named.rfc1912.zones:
2 //
3 // Provided by Red Hat caching-nameserver package
4 //
5 // ISC BIND named zone configuration for zones recommended by
6 // RFC 1912 section 4.1 : localhost TLDs and address zones
7 // and https://tools.ietf.org/html/rfc6303
8 // (c)2007 R W Franks
9 //
10 // See /usr/share/doc/bind*/sample/ for example named
11 // configuration files.

```

```

12 // Note: empty-zones-enable yes; option is default.
13 // If private ranges should be forwarded, add
14 // disable-empty-zone "."; into options
15 //
16
17 zone "skill39.wsr" IN {
18     type slave;
19     file "/var/named/slaves/slave.skill39.wsr.db";
20     masters {172.16.20.10; };
21     allow-transfer {"none"; };
22     allow-notify {172.16.20.10; };
23     masterfile-format text;
24 };
25
26 zone "20.16.172.in-addr.arpa" IN {
27     type slave;
28     file "/var/named/slaves/slave.20.16.172.in-
29 addr.arpa.db";
30     masters {172.16.20.10; };
31     allow-transfer {"none"; };
32     allow-notify {172.16.20.10; };
33     masterfile-format text;
34 };
35
36 zone "100.16.172.in-addr.arpa" IN {
37     type slave;
38     file "/var/named/slaves/slave.100.16.172.in-
39 addr.arpa.db";
40     masters {172.16.20.10; };
41     allow-transfer {"none"; };
42     allow-notify {172.16.20.10; };
43     masterfile-format text;
44 };
45
46 zone "200.16.172.in-addr.arpa" IN {
47     type slave;
48     file "/var/named/slaves/slave.200.16.172.in-
49 addr.arpa.db";
50     masters {172.16.20.10; };
51     allow-transfer {"none"; };
52     allow-notify {172.16.20.10; };
53     masterfile-format text;
54 };
55
56 zone "20.168.192.in-addr.arpa" IN {
57     type slave;
58     file "/var/named/slaves/slave.20.168.192.in-
59 addr.arpa.db";
60     masters {172.16.20.10; };
61     allow-transfer {"none"; };
62     allow-notify {172.16.20.10; };
63     masterfile-format text;
64 };

```

- **/var/named/slaves/slave.skill39.wsr.db** (прямая зона полученная с мастер сервера)

```

1 $ORIGIN .
2 $TTL 604800 ; 1 week
3 skill139.wsr IN SOA ns01.skill139.wsr.
  root.skill139.wsr. (
4                          10 ; serial
5                          604800 ; refresh (1 week)
6                          86400 ; retry (1 day)
7                          2419200 ; expire (4 weeks)
8                          604800 ; minimum (1 week)
9                          )
10                         NS ns01.skill139.wsr.
11                         NS ns02.skill139.wsr.
12 $ORIGIN skill139.wsr.
13 l-cli-a A 172.16.100.65
14 l-cli-b A 172.16.200.61
15 l-fw A 172.16.20.1
16 A 172.16.50.1
17 A 172.16.55.1
18 l-srv A 172.16.20.10
19 ns01 A 172.16.20.10
20 ns02 A 192.168.20.10
21 r-fw A 192.168.20.1
22 r-srv A 192.168.20.10
23 server CNAME l-srv
24 www CNAME r-fw

```

- **/var/named/slaves/slave.20.16.172.in-addr.arpa.db** (обратная зона полученная с мастер сервера)

```

1 $ORIGIN .
2 $TTL 604800 ; 1 week
3 20.16.172.in-addr.arpa IN SOA ns01.skill139.wsr.
  root.skill139.wsr. (
4                          5 ; serial
5                          604800 ; refresh (1 week)
6                          86400 ; retry (1 day)
7                          2419200 ; expire (4 weeks)
8                          604800 ; minimum (1 week)
9                          )
10                         NS ns01.skill139.wsr.
11                         NS ns02.skill139.wsr.
12 $ORIGIN 20.16.172.in-addr.arpa.
13 1 PTR l-fw.skill139.wsr.
14 10 PTR ns01.skill139.wsr.
15 PTR l-srv.skill139.wsr.

```

3. Проверка

- nslookup
 - L-RTR-A

```

1 root@L-RTR-A:~# nslookup l-srv
2   Server:          172.16.20.10
3   Address:         172.16.20.10#53
4
5   Name:    l-srv.skill39.wsr
6   Address: 172.16.20.10
7
8
9 root@L-RTR-A:~# nslookup 172.16.20.10
10  10.20.16.172.in-addr.arpa      name = ns01.skill39.wsr.
11  10.20.16.172.in-addr.arpa      name = l-srv.skill39.wsr.

```

```

1 root@L-RTR-A:~# nslookup r-srv
2   Server:          172.16.20.10
3   Address:         172.16.20.10#53
4
5   Name:    r-srv.skill39.wsr
6   Address: 192.168.20.10
7
8
9 root@L-RTR-A:~# nslookup 192.168.20.10
10  10.20.168.192.in-addr.arpa     name = r-srv.skill39.wsr.
11  10.20.168.192.in-addr.arpa     name = ns02.skill39.wsr.

```

■ R-RTR

```

1 [root@R-RTR ~]# nslookup r-srv
2   Server:          192.168.20.10
3   Address:         192.168.20.10#53
4
5   Name:    r-srv.skill39.wsr
6   Address: 192.168.20.10
7
8
9 [root@R-RTR ~]# nslookup 192.168.20.10
10  10.20.168.192.in-addr.arpa     name = ns02.skill39.wsr.
11  10.20.168.192.in-addr.arpa     name = r-srv.skill39.wsr.

```

```

1 [root@R-RTR ~]# nslookup l-srv
2   Server:          192.168.20.10
3   Address:         192.168.20.10#53
4
5   Name:    l-srv.skill39.wsr
6   Address: 172.16.20.10
7
8
9 [root@R-RTR ~]# nslookup 172.16.20.10
10  10.20.16.172.in-addr.arpa      name = l-srv.skill39.wsr.
11  10.20.16.172.in-addr.arpa      name = ns01.skill39.wsr.

```

