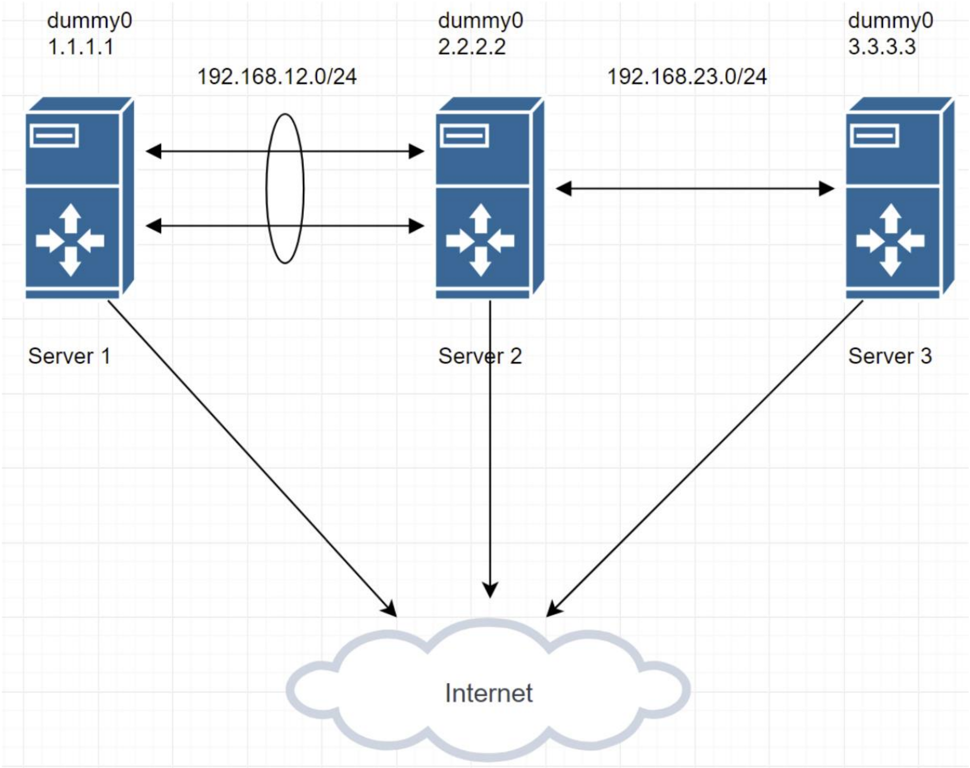
ЗАДАНИЕ №2

Топология:



1) Настроить nic teaming между двумя интерфейсами — server1 и server2. Подсеть 192.168.12.0/24 будет находиться теперь на team0-интерфейсе.

2) На интерфейсе team0 сервера server2 назначить статический IP из подсети 192.168.12.0/24.

3) На сервере server2 настроить DHCP-сервер для выдачи динамического IP-адреса интерфейсу team0 сервера server1, а также IP-адрес DNS-сервера 3.3.3.3.

4) При помощи DHCP выдать серверу Server1 2 статических маршрута 4.4.4.4/32 и 5.5.5.0/24 с next hop интерфейса team0 на сервере server2

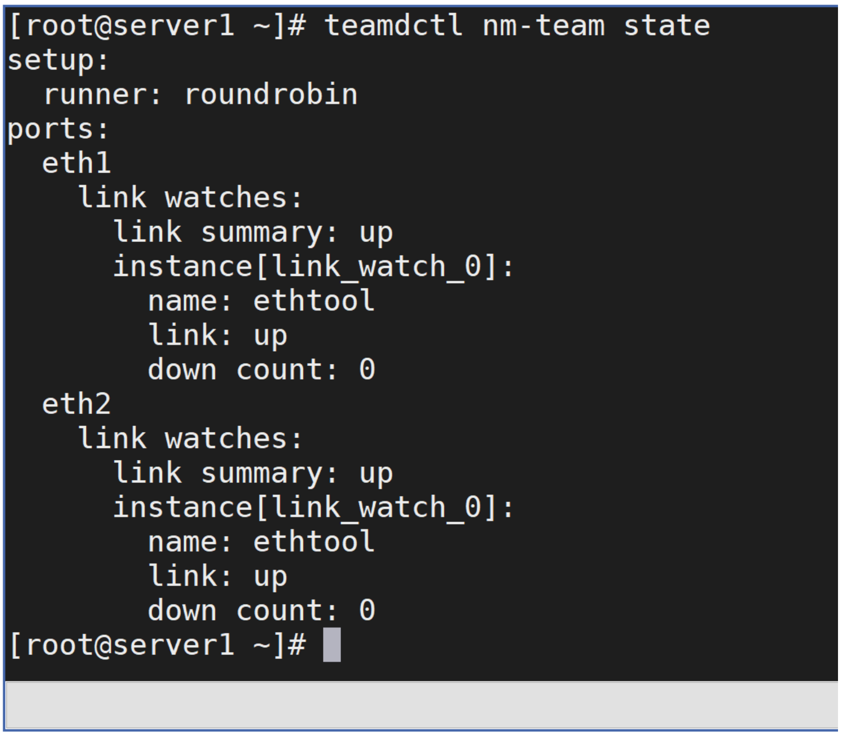
5) Настроить DNS-сервер для зоны example.com на сервере server3. Создать прямую и обратную зоны, а также несколько записей с разными RR. Убедиться, что только запросы на IP-адрес 3.3.3.3 будут обслуживаться этим DNS-сервером.

6) Настроить фаервол на серверах server2 и server3, чтобы разрешить только соответствующие запросы (DHCP/DNS).

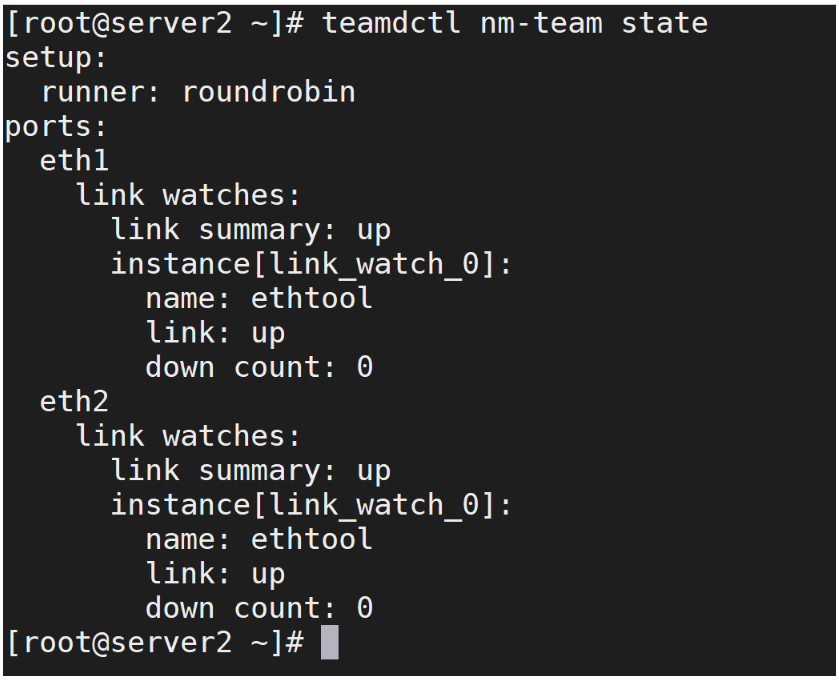
* Настроить slave для DNS-сервера server3. Убедиться, что репликация записей происходит.

РЕШЕНИЕ:

1) Настроен team в режиме roundrobin



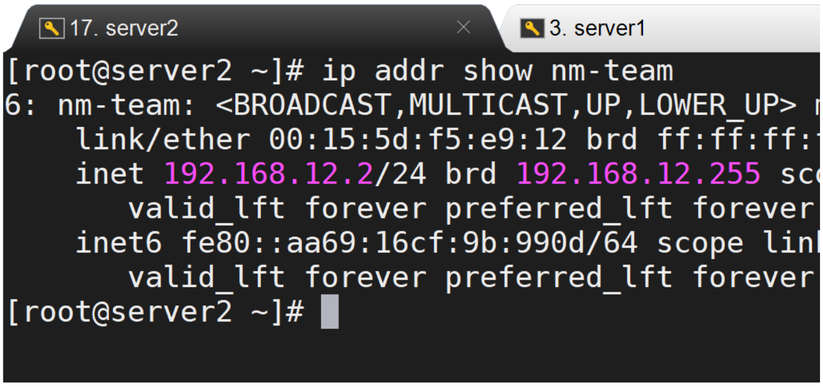
```
[root@server1 ~]# teamdctl nm-team state
setup:
  runner: roundrobin
ports:
  eth1
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  eth2
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
[root@server1 ~]#
```



```
[root@server2 ~]# teamdctl nm-team state
setup:
  runner: roundrobin
ports:
  eth1
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  eth2
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
[root@server2 ~]#
```

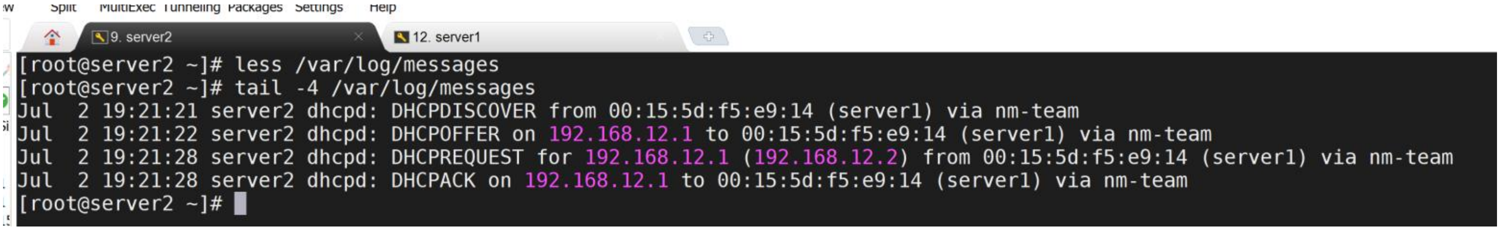
2)

Статический IP установлен



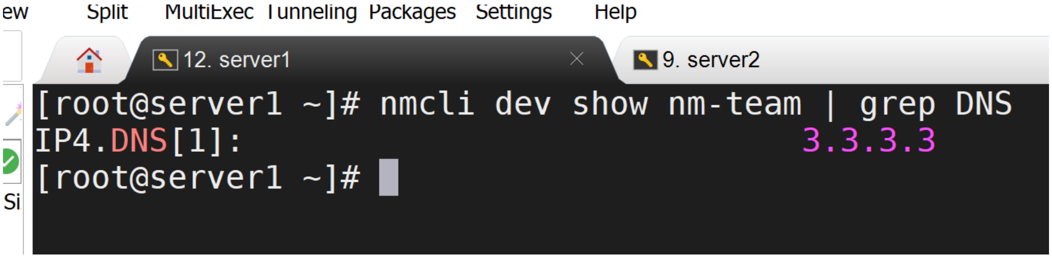
```
[root@server2 ~]# ip addr show nm-team
6: nm-team: <BROADCAST,MULTICAST,UP,LOWER_UP> m
    link/ether 00:15:5d:f5:e9:12 brd ff:ff:ff:f
    inet 192.168.12.2/24 brd 192.168.12.255 sc
       valid_lft forever preferred_lft forever
    inet6 fe80::aa69:16cf:9b:990d/64 scope lin
       valid_lft forever preferred_lft forever
[root@server2 ~]#
```

3) Со стороны сервера выданы сетевые настройки серверу “server1”



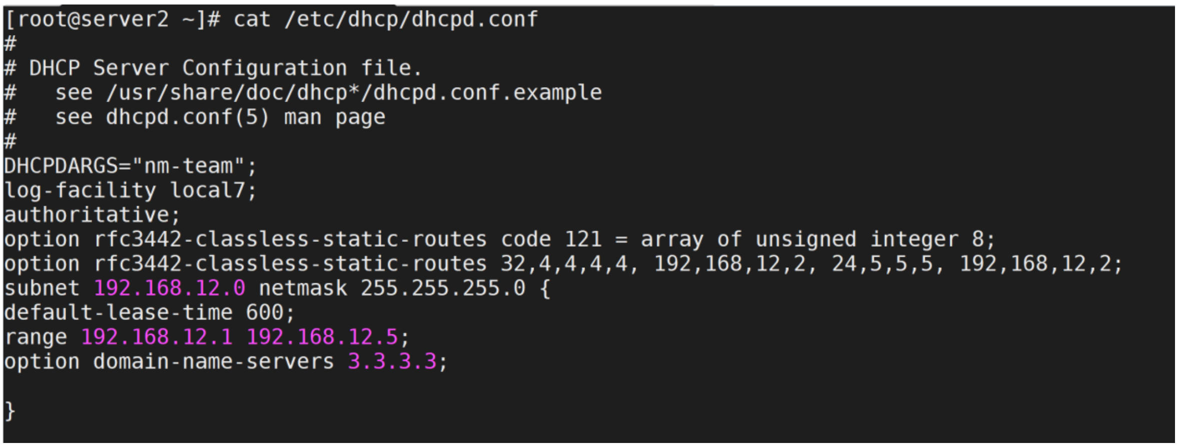
```
[root@server2 ~]# less /var/log/messages
[root@server2 ~]# tail -4 /var/log/messages
Jul  2 19:21:21 server2 dhcpd: DHCPDISCOVER from 00:15:5d:f5:e9:14 (server1) via nm-team
Jul  2 19:21:22 server2 dhcpd: DHCPOFFER on 192.168.12.1 to 00:15:5d:f5:e9:14 (server1) via nm-team
Jul  2 19:21:28 server2 dhcpd: DHCPREQUEST for 192.168.12.1 (192.168.12.2) from 00:15:5d:f5:e9:14 (server1) via nm-team
Jul  2 19:21:28 server2 dhcpd: DHCPACK on 192.168.12.1 to 00:15:5d:f5:e9:14 (server1) via nm-team
[root@server2 ~]#
```

На стороне клиента также получен адрес DNS сервера

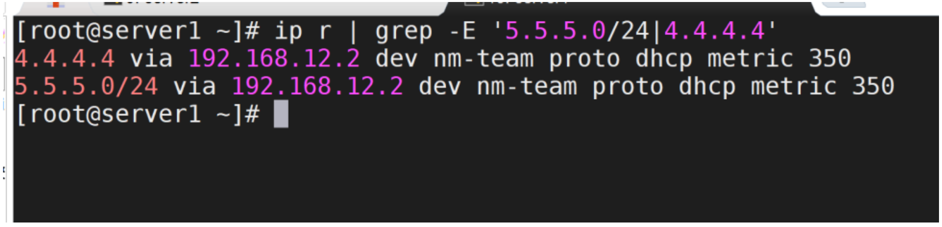


```
[root@server1 ~]# nmcli dev show nm-team | grep DNS
IP4.DNS[1]:                             3.3.3.3
[root@server1 ~]#
```

4) Добавлены маршруты к  4.4.4.4/32 и 5.5.5.0/24

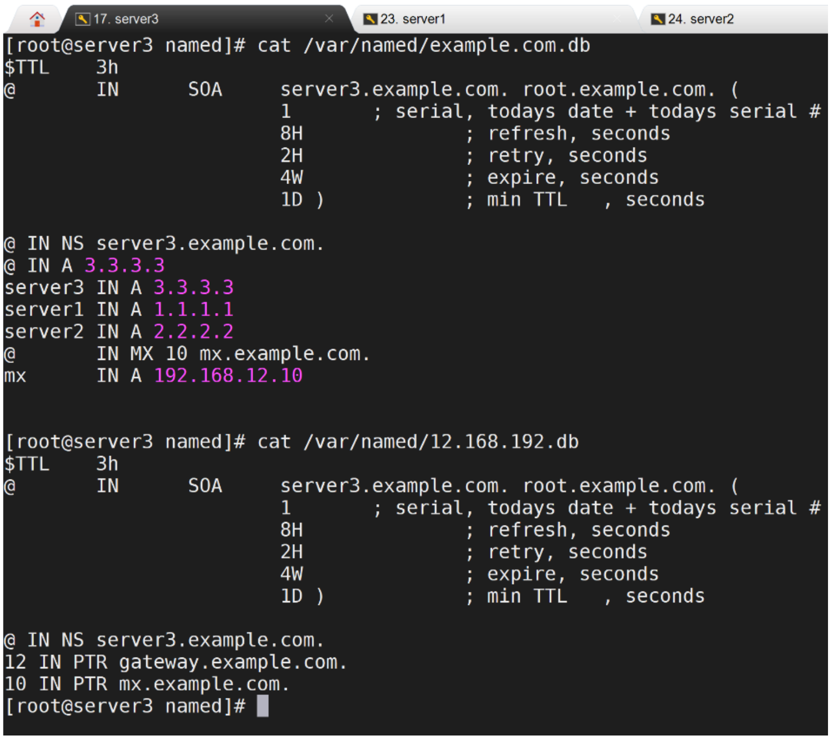


```
[root@server2 ~]# cat /etc/dhcp/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
DHCPDARGS="nm-team";
log-facility local7;
authoritative;
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;
option rfc3442-classless-static-routes 32,4,4,4,4, 192,168,12,2, 24,5,5,5, 192,168,12,2;
subnet 192.168.12.0 netmask 255.255.255.0 {
default-lease-time 600;
range 192.168.12.1 192.168.12.5;
option domain-name-servers 3.3.3.3;

}
```



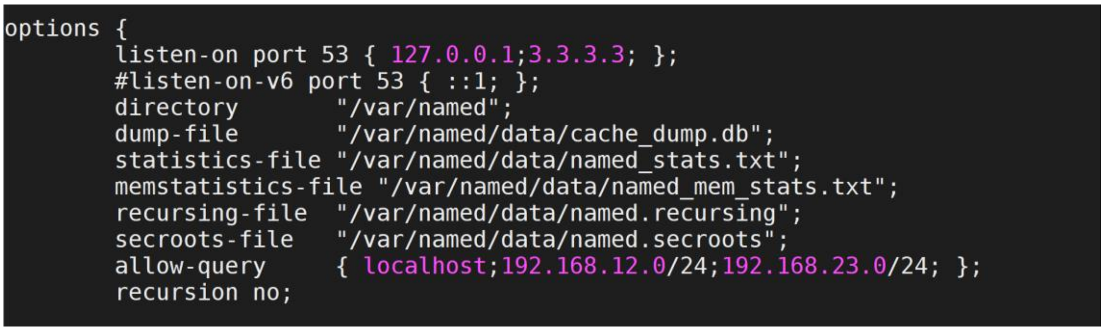
```
[root@server1 ~]# ip r | grep -E '5.5.5.0/24|4.4.4.4'
4.4.4.4 via 192.168.12.2 dev nm-team proto dhcp metric 350
5.5.5.0/24 via 192.168.12.2 dev nm-team proto dhcp metric 350
[root@server1 ~]#
```

5) Установлен DNS сервер, созданы прямая и обратная зоны



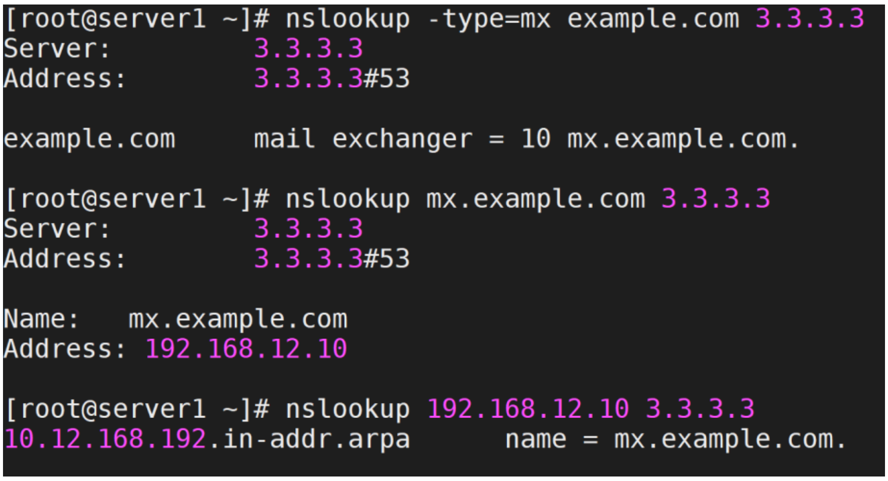
```
[root@server3 named]# cat /var/named/example.com.db
$TTL    3h
@       IN      SOA     server3.example.com. root.example.com. (
                        1       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; min TTL    , seconds

@ IN NS server3.example.com.
@ IN A 3.3.3.3
server3 IN A 3.3.3.3
server1 IN A 1.1.1.1
server2 IN A 2.2.2.2
@       IN MX 10 mx.example.com.
mx      IN A 192.168.12.10

[root@server3 named]# cat /var/named/12.168.192.db
$TTL    3h
@       IN      SOA     server3.example.com. root.example.com. (
                        1       ; serial, todays date + todays serial #
                        8H              ; refresh, seconds
                        2H              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; min TTL    , seconds

@ IN NS server3.example.com.
12 IN PTR gateway.example.com.
10 IN PTR mx.example.com.
[root@server3 named]#
```

Обращаться к серверу DNS возможно только по 3.3.3.3



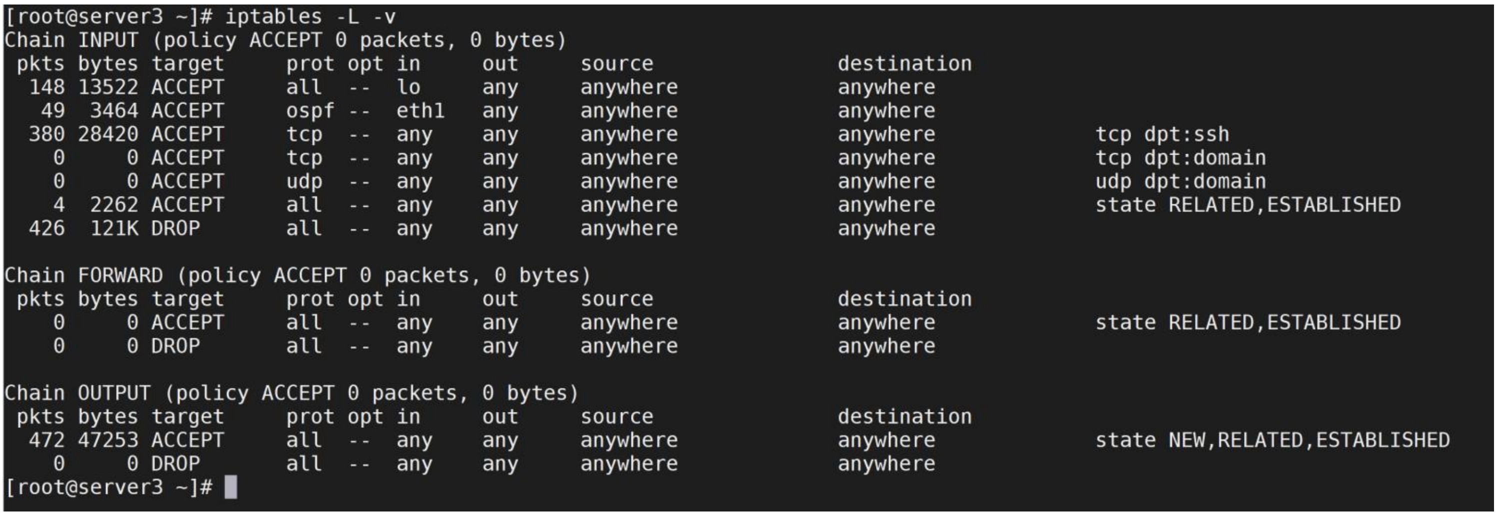
```
options {
        listen-on port 53 { 127.0.0.1;3.3.3.3; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;192.168.12.0/24;192.168.23.0/24; };
        recursion no;
```

Пример разрешения записей



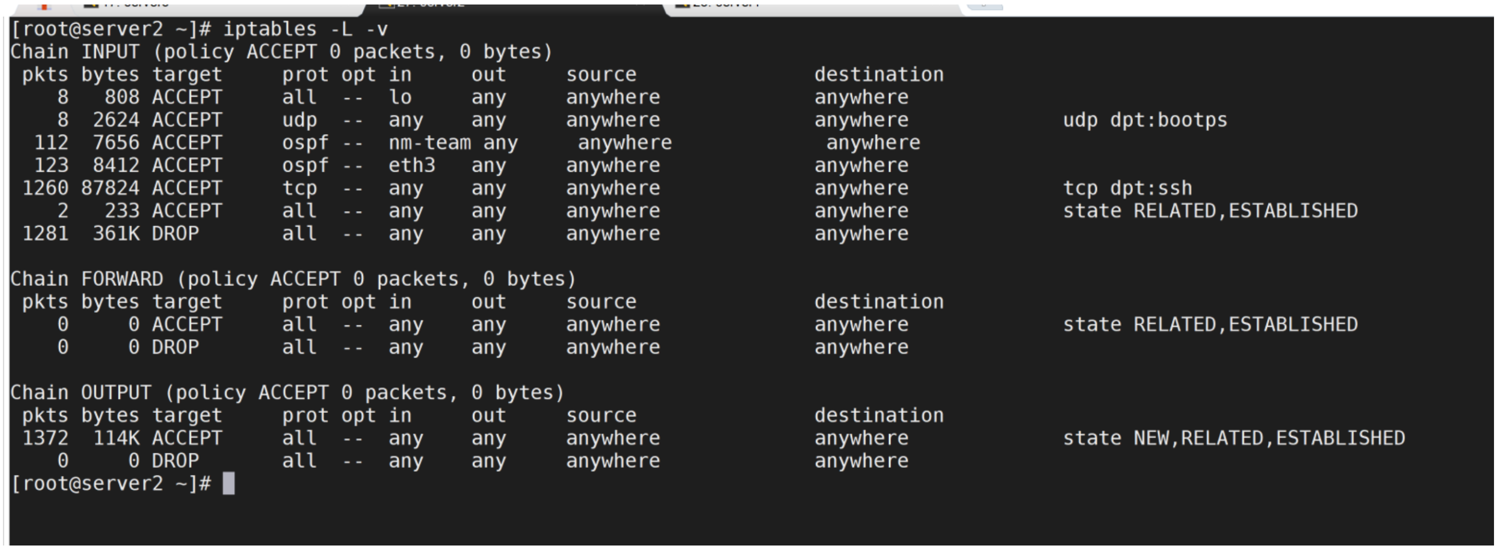
```
[root@server1 ~]# nslookup -type=mx example.com 3.3.3.3
Server:         3.3.3.3
Address:        3.3.3.3#53

example.com     mail exchanger = 10 mx.example.com.

[root@server1 ~]# nslookup mx.example.com 3.3.3.3
Server:         3.3.3.3
Address:        3.3.3.3#53

Name:   mx.example.com
Address: 192.168.12.10

[root@server1 ~]# nslookup 192.168.12.10 3.3.3.3
10.12.168.192.in-addr.arpa      name = mx.example.com.
```

6) Для server3 разрешим ssh(чтобы подключиться), ospf(из предыдущего задания), добавим 53 порт TCP UDP



```
[root@server3 ~]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  148 13522 ACCEPT     all  --  lo     any     anywhere             anywhere
   49  3464 ACCEPT     ospf --  eth1   any     anywhere             anywhere
  380 28420 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:domain
    0     0 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:domain
    4  2262 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
  426  121K DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
  472 47253 ACCEPT     all  --  any    any     anywhere             anywhere             state NEW,RELATED,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere
[root@server3 ~]#
```

Для server2 разрешим ssh(чтобы подключиться), ospf(из предыдущего задания), добавим 67 порт UDP

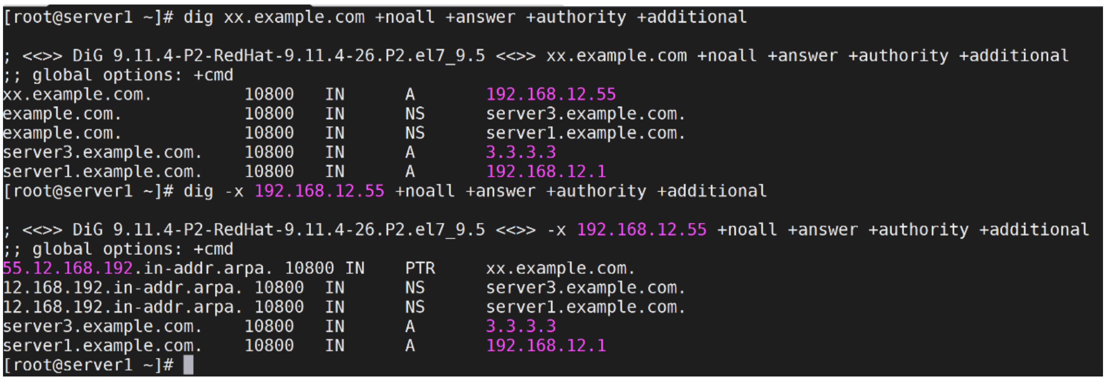


```
[root@server2 ~]# iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    8   808 ACCEPT     all  --  lo     any     anywhere             anywhere
    8  2624 ACCEPT     udp  --  any    any     anywhere             anywhere             udp dpt:bootps
  112  7656 ACCEPT     ospf --  nm-team any     anywhere             anywhere
  123  8412 ACCEPT     ospf --  eth3   any     anywhere             anywhere
 1260 87824 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
    2   233 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
 1281  361K DROP       all  --  any    any     anywhere             anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  any    any     anywhere             anywhere             state RELATED,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
 1372  114K ACCEPT     all  --  any    any     anywhere             anywhere             state NEW,RELATED,ESTABLISHED
    0     0 DROP       all  --  any    any     anywhere             anywhere
[root@server2 ~]#
```

*)

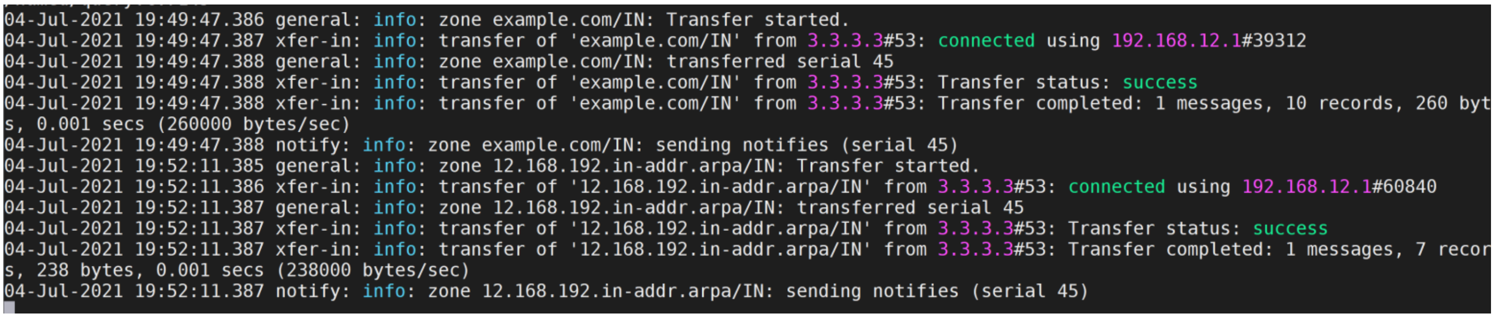
Bind в конфигурации Slave развернут на server1.

Пример разрешения записей:



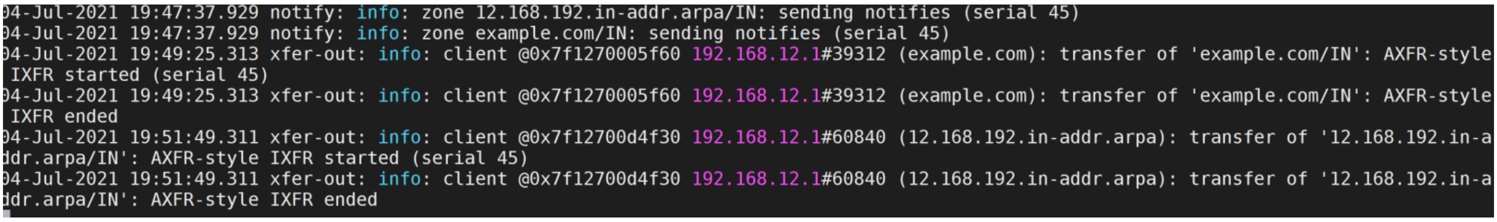
```
[root@server1 ~]# dig xx.example.com +noall +answer +authority +additional

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.5 <<>> xx.example.com +noall +answer +authority +additional
;; global options: +cmd
xx.example.com.         10800   IN      A       192.168.12.55
example.com.            10800   IN      NS      server3.example.com.
example.com.            10800   IN      NS      server1.example.com.
server3.example.com.    10800   IN      A       3.3.3.3
server1.example.com.    10800   IN      A       192.168.12.1
[root@server1 ~]# dig -x 192.168.12.55 +noall +answer +authority +additional

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.5 <<>> -x 192.168.12.55 +noall +answer +authority +additional
;; global options: +cmd
55.12.168.192.in-addr.arpa. 10800 IN    PTR     xx.example.com.
12.168.192.in-addr.arpa. 10800  IN      NS      server3.example.com.
12.168.192.in-addr.arpa. 10800  IN      NS      server1.example.com.
server3.example.com.    10800   IN      A       3.3.3.3
server1.example.com.    10800   IN      A       192.168.12.1
[root@server1 ~]# 
```

Лог репликации зон со стороны Slave:



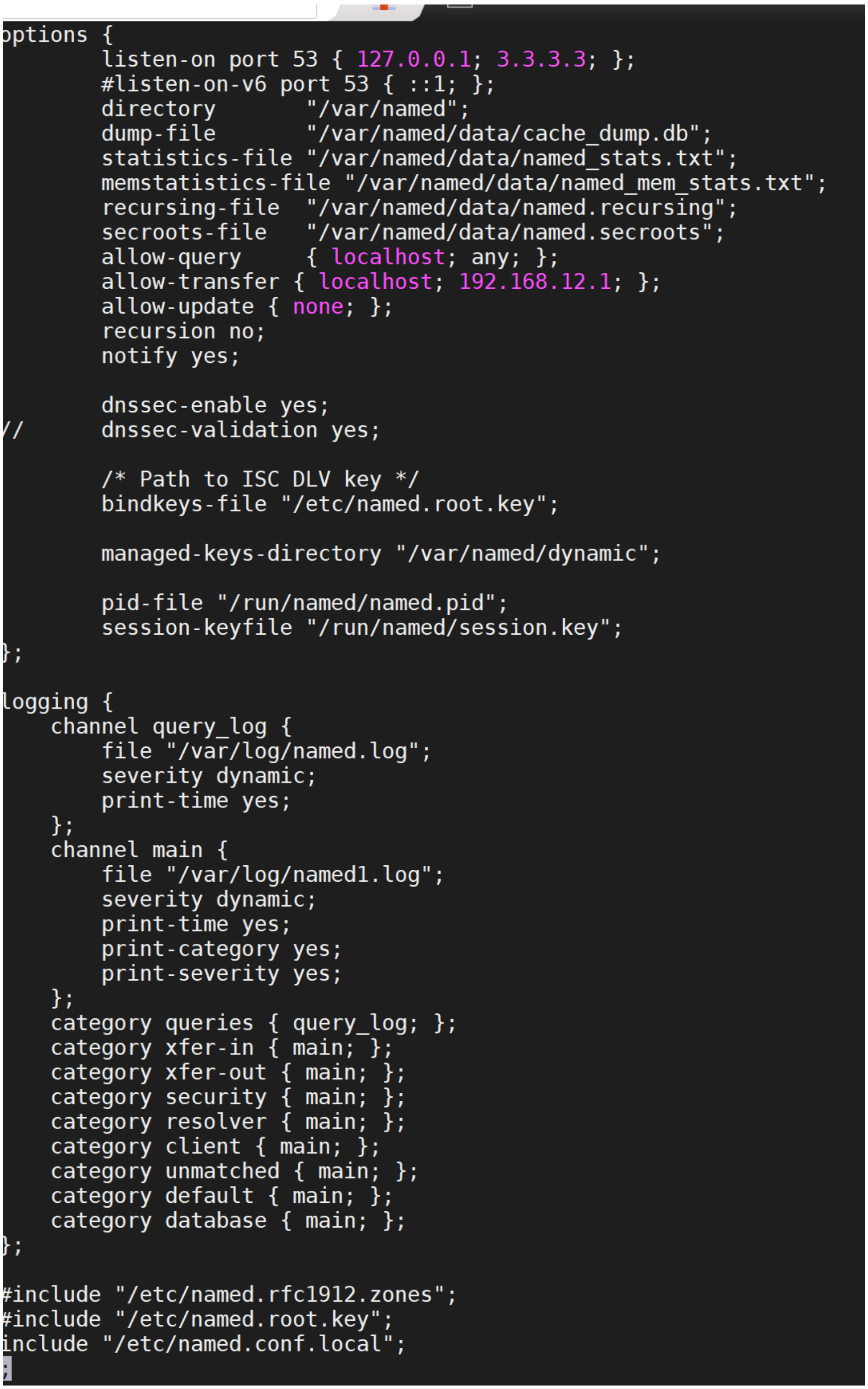
```
04-Jul-2021 19:49:47.386 general: info: zone example.com/IN: Transfer started.
04-Jul-2021 19:49:47.387 xfer-in: info: transfer of 'example.com/IN' from 3.3.3.3#53: connected using 192.168.12.1#39312
04-Jul-2021 19:49:47.388 general: info: zone example.com/IN: transferred serial 45
04-Jul-2021 19:49:47.388 xfer-in: info: transfer of 'example.com/IN' from 3.3.3.3#53: Transfer status: success
04-Jul-2021 19:49:47.388 xfer-in: info: transfer of 'example.com/IN' from 3.3.3.3#53: Transfer completed: 1 messages, 10 records, 260 byt
s, 0.001 secs (260000 bytes/sec)
04-Jul-2021 19:49:47.388 notify: info: zone example.com/IN: sending notifies (serial 45)
04-Jul-2021 19:52:11.385 general: info: zone 12.168.192.in-addr.arpa/IN: Transfer started.
04-Jul-2021 19:52:11.386 xfer-in: info: transfer of '12.168.192.in-addr.arpa/IN' from 3.3.3.3#53: connected using 192.168.12.1#60840
04-Jul-2021 19:52:11.387 general: info: zone 12.168.192.in-addr.arpa/IN: transferred serial 45
04-Jul-2021 19:52:11.387 xfer-in: info: transfer of '12.168.192.in-addr.arpa/IN' from 3.3.3.3#53: Transfer status: success
04-Jul-2021 19:52:11.387 xfer-in: info: transfer of '12.168.192.in-addr.arpa/IN' from 3.3.3.3#53: Transfer completed: 1 messages, 7 recor
s, 238 bytes, 0.001 secs (238000 bytes/sec)
04-Jul-2021 19:52:11.387 notify: info: zone 12.168.192.in-addr.arpa/IN: sending notifies (serial 45)
```

Лог репликации зон со стороны Master:

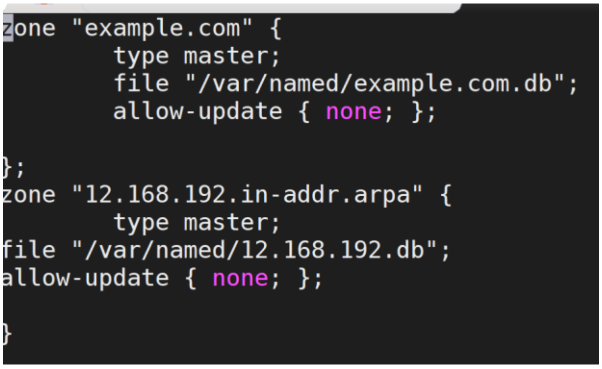


```
04-Jul-2021 19:47:37.929 notify: info: zone 12.168.192.in-addr.arpa/IN: sending notifies (serial 45)
04-Jul-2021 19:47:37.929 notify: info: zone example.com/IN: sending notifies (serial 45)
04-Jul-2021 19:49:25.313 xfer-out: info: client @0x7f1270005f60 192.168.12.1#39312 (example.com): transfer of 'example.com/IN': AXFR-style
 IXFR started (serial 45)
04-Jul-2021 19:49:25.313 xfer-out: info: client @0x7f1270005f60 192.168.12.1#39312 (example.com): transfer of 'example.com/IN': AXFR-style
 IXFR ended
04-Jul-2021 19:51:49.311 xfer-out: info: client @0x7f12700d4f30 192.168.12.1#60840 (12.168.192.in-addr.arpa): transfer of '12.168.192.in-a
ddr.arpa/IN': AXFR-style IXFR started (serial 45)
04-Jul-2021 19:51:49.311 xfer-out: info: client @0x7f12700d4f30 192.168.12.1#60840 (12.168.192.in-addr.arpa): transfer of '12.168.192.in-a
ddr.arpa/IN': AXFR-style IXFR ended
```

**Config мастер сервера:**

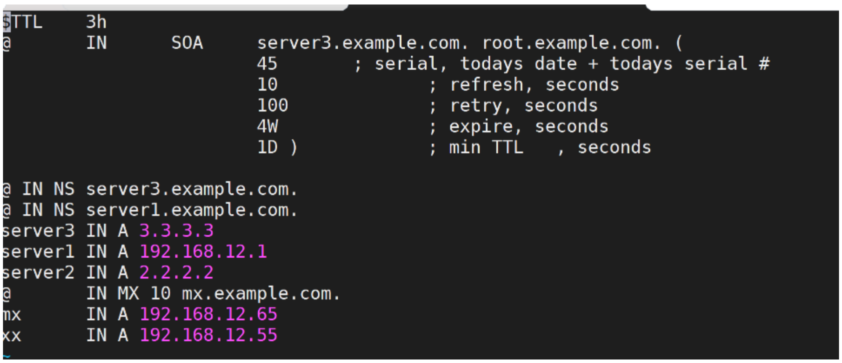


```
options {
        listen-on port 53 { 127.0.0.1; 3.3.3.3; };
        #listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost; any; };
        allow-transfer { localhost; 192.168.12.1; };
        allow-update { none; };
        recursion no;
        notify yes;

        dnssec-enable yes;
//      dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";

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

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

logging {
    channel query_log {
        file "/var/log/named.log";
        severity dynamic;
        print-time yes;
    };
    channel main {
        file "/var/log/named1.log";
        severity dynamic;
        print-time yes;
        print-category yes;
        print-severity yes;
    };
    category queries { query_log; };
    category xfer-in { main; };
    category xfer-out { main; };
    category security { main; };
    category resolver { main; };
    category client { main; };
    category unmatched { main; };
    category default { main; };
    category database { main; };
};

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

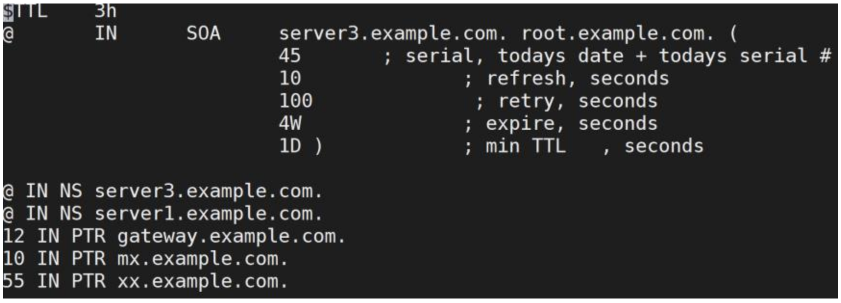


```
zone "example.com" {
        type master;
        file "/var/named/example.com.db";
        allow-update { none; };

};
zone "12.168.192.in-addr.arpa" {
        type master;
file "/var/named/12.168.192.db";
allow-update { none; };

}
```

Зоны:

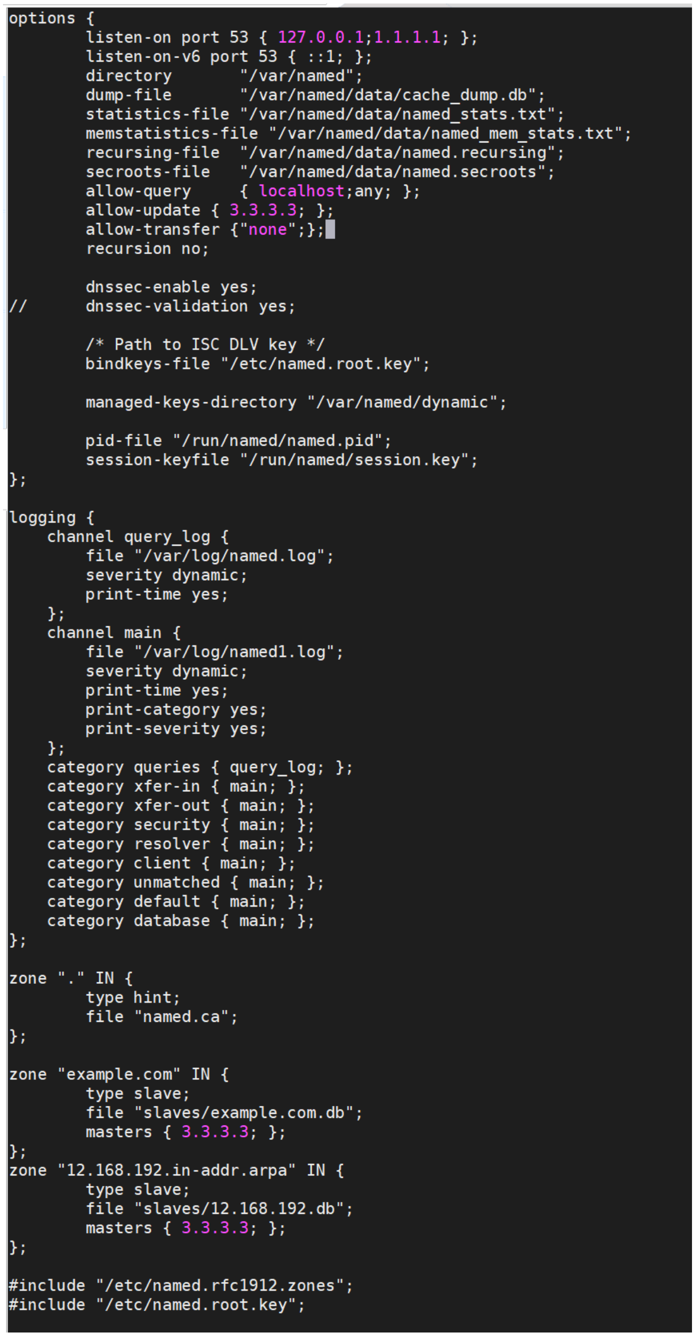


```
$TTL    3h
@       IN      SOA     server3.example.com. root.example.com. (
                        45       ; serial, todays date + todays serial #
                        10              ; refresh, seconds
                        100             ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; min TTL    , seconds

@ IN NS server3.example.com.
@ IN NS server1.example.com.
server3 IN A 3.3.3.3
server1 IN A 192.168.12.1
server2 IN A 2.2.2.2
@       IN MX 10 mx.example.com.
mx      IN A 192.168.12.65
xx      IN A 192.168.12.55
```



```
$TTL    3h
@       IN      SOA     server3.example.com. root.example.com. (
                        45       ; serial, todays date + todays serial #
                        10              ; refresh, seconds
                        100              ; retry, seconds
                        4W              ; expire, seconds
                        1D )            ; min TTL    , seconds

@ IN NS server3.example.com.
@ IN NS server1.example.com.
12 IN PTR gateway.example.com.
10 IN PTR mx.example.com.
55 IN PTR xx.example.com.
```

**Config slave сервера:**



```
options {
        listen-on port 53 { 127.0.0.1;1.1.1.1; };
        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";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { localhost;any; };
        allow-update { 3.3.3.3; };
        allow-transfer {"none";};
        recursion no;

        dnssec-enable yes;
//      dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.root.key";

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

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

logging {
    channel query_log {
        file "/var/log/named.log";
        severity dynamic;
        print-time yes;
    };
    channel main {
        file "/var/log/named1.log";
        severity dynamic;
        print-time yes;
        print-category yes;
        print-severity yes;
    };
    category queries { query_log; };
    category xfer-in { main; };
    category xfer-out { main; };
    category security { main; };
    category resolver { main; };
    category client { main; };
    category unmatched { main; };
    category default { main; };
    category database { main; };
};

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

zone "example.com" IN {
        type slave;
        file "slaves/example.com.db";
        masters { 3.3.3.3; };
};
zone "12.168.192.in-addr.arpa" IN {
        type slave;
        file "slaves/12.168.192.db";
        masters { 3.3.3.3; };
};

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