Bind9 в chroot

```
# yum -y install bind bind-utils bind-chroot
# systemctl start named-chroot
# systemctl enable named-chroot
```

Подготовим chroot-каталог, запустив специальный скрипт:

```
# /usr/libexec/setup-named-chroot.sh /var/named/chroot on
```

Укажем параметр для использования chroot

```
# mcedit /etc/sysconfig/named
```

```
OPTIONS="-4"
```

Редактируем конфиг:

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

```
acl "bsd" { 192.168.113.0/24; 127.0.0.1; };

options {
    listen-on port 53 { 127.0.0.1; 192.168.113.1; _IP_WAN_; };
    //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";
    allow-query { bsd; };

/*
 - 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;
     allow-recursion { bsd; };

forwarders {
     127.0.0.1;
     _IP_DNS_провайдера;
     8.8.8.8;
 };

version "DNS Server";

blackhole {
    0.0.0.0/8;
    10.0.0.0/8;
    169.254.0.0/16;
    172.16.0.0/12;
    192.0.2.0/24;
    //192.168.0.0/16;
    224.0.0.0/4;
    240.0.0.0/4;
 };

dnssec-enable yes;
dnssec-validation yes;

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

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

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

logging {
 channel queries {
     file "/var/log/named/queries.log" versions 2 size 10M;
```

```
     print-time yes;
     print-category yes;
     print-severity yes;
 };
 channel bind_log {
     file "/var/log/named/named.log" size 10M;
     print-category yes;
     print-severity yes;
     print-time yes;
 };
 channel update_debug {
      file "/var/log/named/named-update.log" versions 6 size
10M;
     severity debug 10;
     print-category yes;
     print-severity yes;
     print-time yes;
 };
 channel security_info {
     file "/var/log/named/named.log" versions 6 size 10M;
     severity info;
     print-category yes;
     print-severity yes;
     print-time yes;
 };
 channel edns-disabled {
      file "/var/log/named/edns-disabled.log" versions 1 size
500K;
     severity info;
     print-category yes;
     print-severity yes;
     print-time yes;
 };
category default { bind_log; };
category xfer-in { bind_log; };
category xfer-out { bind_log; };
category update { update_debug; };
category security { security_info; };
category queries { queries; };
category edns-disabled { edns-disabled; };
category lame-servers { null; };
```

```
};

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

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

Не забыть создать директорию для логов:

```
# mkdir -p /var/named/chroot/var/log/named
# cd /var/named/chroot/var/log
# chown named:named named
```

Перечитать конфигурацию:

```
# rndc reconfig
```

Проверяем конфигурацию и зоны на ошибки:

```
# named-checkconf
#               named-checkzone               example.com
/var/named/external/example.com.zone
#               named-checkzone               example.com
/var/named/internal/example.com.zone
```

DNS-сервер работает на 53 порту UDP, а для передачи зон использует 53 порт TCP. Отвечать на запросы будет всем, но передавать зону только slave-серверу, по локальной сети.

```
# iptables -A INPUT -p udp --dport 53 -j ACCEPT -m comment --
comment "dns-query"
# iptables -A INPUT -s 172.16.0.2 -p tcp --dport 53 -j ACCEPT
-m comment --comment "dns-transfer"
```

Проверяем.

[источник](http://itzx.ru/linux/install-named-bind-chroot-on-centos)
http://itzx.ru/linux/install-named-bind-chroot-on-centos
https://webhostinggeeks.com/howto/bind-dns-server-in-chroot-jail-on-centos-7/