Первоначальная настройка DNS

Сейчас практически не найдется сервиса или службы, которые не использовали б в своей работе DNS (англ. Domain Name System — система доменных имён). Поэтому понимание принципов работы DNS является обязательным для любого системного администратора. Итак в этой статье мы рассмотрим первоначальную настройку DNS сервера - bind

Введение

DNS — компьютерная распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты, обслуживающих узлах для протоколов в домене (SRV-запись).

Распределённая база данных DNS поддерживается с помощью иерархии DNS-серверов, взаимодействующих по определённому протоколу.

Основой DNS является представление об иерархической структуре доменного имени и зонах. Каждый сервер, отвечающий за имя, может делегировать ответственность за дальнейшую часть домена другому серверу (с административной точки зрения — другой организации или человеку), что позволяет возложить ответственность за актуальность информации на серверы различных организаций (людей), отвечающих только за «свою» часть доменного имени.

Итак, у нас в распоряжении следующая система

```
# uname -a
Linux centos5.sys-adm.local 2.6.18-194.26.1.el5 #1 SMP Tue Nov 9 12:54:40
EST 2010 i686 i686 i386 GNU/Linux

# cat /etc/redhat-release
CentOS release 5.5 (Final)
```

Настройка

Устанавливаем необходимые пакеты

```
# yum install bind bind-chroot bind-utils bind-libs
```

С учетом того, что мы будет запускать демон в chroot окружении, то корнем будет папка **/var/named/chroot/**. **В дальнейшем, все пути будут задаваться относительно этой директории.**

Итак создаем основной конфигурационный файл - **/etc/named.conf**

```
// Подключаем ключ, используемый для управляющего канала
include "/etc/rndc.key";
```

```
// Описываем сети, для которых разрешены рекурсивные запросы
acl "trusted" {
      192.168.127.0/24;
      127.0.0.0/8;
};

// Список зарезервированных и частных подсетей, описанных в RFC 1918 и RFC 5735
// Если ваши клиенты используют одну из ниже перечисленных подсетей, то ее необходимо удалить из этого списка
acl "bogus_network" {
    0.0.0.0/8;
    10.0.0.0/8;
    39.0.0.0/8;
    102.0.0.0/8;
    103.0.0.0/8;
    104.0.0.0/8;
    106.0.0.0/8;
    169.254.0.0/16;
    172.16.0.0/12;
    179.0.0.0/8;
    185.0.0.0/8;
    192.0.0.0/24;
    192.0.2.0/24;
    192.168.0.0/16;
    198.18.0.0/15;
    198.51.100.0/24;
    203.0.113.0/24;
    224.0.0.0/3;
};

options
{
        // Put files that named is allowed to write in the data/ directory:
        directory "/var/named"; // the default
        dump-file               "data/cache_dump.db";
        statistics-file         "data/named_stats.txt";
        memstatistics-file      "data/named_mem_stats.txt";

    // Перечисляем интерфейсы, на которых слушать запросы
        listen-on { 127.0.0.1; 192.168.127.1; 46.4.15.12; };
    // Отключаем рекурсию глобально
        recursion no;

    // Отклоняем запросы и не отвечаем подсетям, перечисленным в bogus_network
        blackhole { bogus_network; };
};

// Определяем кто сможет использовать управляющий канал. В нашем примере любой хост, который будет аутентифицироваться ключом RNDC
controls {
    inet * port 953 allow { any; } keys { "RNDC"; };
```

```
};


// Описываем логирование событий.
logging
{
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

// Далее мы определяем два представления. В external перечисляем зоны, для которых наш сервер является авторитативным.
// В internal описываем зоны, которые используются внутри локальной сети

view    "external"
{
        match-clients           { !trusted; any; };
        match-destinations      { any; };

        allow-query-cache { none; };

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

        zone "sys-adm.org.ua" {
                type master;
                file "masters/sys-adm.org.ua.zone";
        };
};

view    "internal"
{
        match-clients           { trusted; };
        recursion yes;

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

        zone "localhost" {
                type master;
                file "masters/localhost.zone";
                allow-update { none; };
        };

        zone "0.0.127-in-addr.arpa" {
```

```
                type master;
                file "masters/0.0.127-in-addr.arpa";
                allow-update { none; };
        };

        zone "sys-adm.local" {
                type master;
                file "masters/sys-adm.local.zone";
        };

        zone "127.168.192-in-addr.arpa" {
                type master;
                file "masters/127.168.192-in-addr.arpa";
        };
};
```

Основная идея данного конфигурационного файла состоит в создании двух представлений - **internal** и **external**. Клиенты, которые попадают в представление **internal** смогут использовать наш сервер рекурсивно, в то время как клиенты, которые попадают в представление **external** смогут запрашивать информацию о зонах, описанных в данном представлении.

Для начала скачиваем свежую версию файла описания зоны корневых серверов

```
# cd var/named
# wget ftp://ftp.internic.net/domain/named.root
```

Теперь создаем непосредственно файлы описания наших зон и выставляем необходимые права.

```
# mkdir masters
# cd masters
# touch sys-adm.local 127.168.192.in-addr.arpa 0.0.127.in-addr.arpa
localhost.zone sys-adm.org.ua.zone
# chown -R named:named var/named/masters
# chmod 770 var/named
```

А теперь производим описание самих зон.

/var/named/masters/0.0.127.in-addr.arpa

```
;0.0.127.in-addr.arpa
$TTL 1D
$ORIGIN 0.0.127.in-addr.arpa.

@       IN      SOA     localhost. root.localhost.  (
                            2010121501      ; Serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            3600 )          ; Minimum
```

```
@       IN      NS      localhost.
1       IN      PTR     localhost.
```

/var/named/masters/localhost.zone

```
;localhost.zone
$TTL 1D
$ORIGIN localhost.

@               IN SOA  @       root (
                            2010121501      ; Serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            3600 )          ; Minimum

                IN NS           @
                IN A            127.0.0.1
                IN AAAA         ::1
```

/var/named/masters/sys-adm.local.zone

```
;sys-adm.local.zone
$TTL 1D
$ORIGIN sys-adm.local.

@ IN SOA ns1.sys-adm.local. hostmaster.sys-adm.local. (
                            2010121501      ; Serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            3600 )          ; Minimum

@       IN      NS      ns1.sys-adm.local.
@       IN      NS      ns2.sys-adm.local.

ns1     IN      A       192.168.127.1
ns2     IN      A       192.168.127.2

@       IN      A       192.168.127.1

@       IN      MX 10   mail.sys-adm.local.

mail    IN      A       192.168.127.1
www     IN      A       192.168.127.1
```

/var/named/masters/127.168.192.in-addr.arpa

```
$TTL 1D
$ORIGIN 127.168.192.in-addr.arpa.
```

```
@ IN SOA ns1.sys-adm.local. hostmaster.sys-adm.local. (
                            2010121501      ; Serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            3600 )          ; Minimum

@       IN NS           ns1.sys-adm.local.

1       IN PTR          gw.sys-adm.local.
```

/var/named/masters/sys-adm.org.ua.zone

```
;sys-adm.org.ua.zone
$TTL 1D
$ORIGIN sys-adm.org.ua.

@ IN SOA ns1.sys-adm.org.ua. hostmaster.sys-adm.org.ua. (
                            2010121501      ; Serial
                            10800           ; Refresh
                            3600            ; Retry
                            604800          ; Expire
                            3600 )          ; Minimum

@       IN      NS      ns1.sys-adm.org.ua.
@       IN      NS      ns2.sys-adm.org.ua.

ns1     IN      A       46.4.15.12
ns2     IN      A       88.198.57.86

@       IN      A       46.4.15.12

@       IN      MX 10   mail.sys-adm.org.ua.
@       IN      MX 20   mail2.sys-adm.org.ua.

mail    IN      A       91.200.157.134
mail2   IN      A       188.230.122.62

www     IN      A       46.4.15.12
ftp     IN      CNAME   www
wiki    IN      CNAME   www

IN      TXT     "v=spf1 mx -all"
```

Теперь нам необходимо создать ключ RNDC

```
# cd etc
# dnssec-keygen -a hmac-md5 -b 128 -n HOST RNDC.
Krndc.+157+60579

# cat Krndc.+157+60579.private
```

```
Private-key-format: v1.2
Algorithm: 157 (HMAC_MD5)
Key: 0wdkY8QOk+VtEEshu/TjgA==

# touch rndc.key
```

Значения поля Key как раз и необходимо использовать как secret в описании ключа

```
key "RNDC" {
        algorithm       hmac-md5;
        secret          "0wdkY8QOk+VtEEshu/TjgA==";
};
```

Выставляем необходимые права на файл с ключом.

```
# chown root:named rndc.key
# chmod 640 rndc.key
```

Тестирование

Перед запуском самого демона проверим валидность самих зон

```
# named-checkzone sys-adm.local sys-adm.local.zone
zone sys-adm.local/IN: loaded serial 2010121501
OK

# named-checkzone 127.168.192.in-addr.arpa 127.168.192.in-addr.arpa
zone 207.168.192.in-addr.arpa/IN: loaded serial 2010121501
OK

# named-checkzone localhost localhost.zone
zone localhost/IN: loaded serial 2010121501
OK

# named-checkzone 0.0.127.in-addr.arpa 0.0.127.in-addr.arpa
zone 0.0.127.in-addr.arpa/IN: loaded serial 2010121501
OK

# named-checkzone sys-adm.org.ua sys-adm.org.ua.zone
zone sys-adm.org.ua/IN: loaded serial 2010121501
OK
```

А также валидность основного конфигурационного файла

```
# named-checkconf -t /var/named/chroot/
```

Если команда ничего не написала, то значит синтаксис без ошибок. Иначе вы увидите сообщение наподобие следуюущему

```
# named-checkconf -t /var/named/chroot/
/etc/named.conf:94: missing ';' before end of file
```

Запускаем named и проверяем статус

```
# service named start
Starting named:                                            [  OK  ]

# service named status
number of zones: 5
debug level: 0
xfers running: 0
xfers deferred: 0
soa queries in progress: 0
query logging is OFF
recursive clients: 0/1000
tcp clients: 0/100
server is up and running
named (pid  24492) is running...
```

```
# cat /var/log/messages | grep named
Dec 15 23:12:27 centos5 named[24492]: starting BIND 9.3.6-P1-
RedHat-9.3.6-4.P1.el5_5.3 -u named -t /var/named/chroot
Dec 15 23:12:27 centos5 named[24492]: found 1 CPU, using 1 worker thread
Dec 15 23:12:27 centos5 named[24492]: using up to 4096 sockets
Dec 15 23:12:27 centos5 named[24492]: loading configuration from
'/etc/named.conf'
Dec 15 23:12:27 centos5 named[24492]: max open files (1024) is smaller than
max sockets (4096)
Dec 15 23:12:27 centos5 named[24492]: using default UDP/IPv4 port range:
[1024, 65535]
Dec 15 23:12:27 centos5 named[24492]: using default UDP/IPv6 port range:
[1024, 65535]
Dec 15 23:12:27 centos5 named[24492]: listening on IPv4 interface lo,
127.0.0.1#53
Dec 15 23:12:27 centos5 named[24492]: listening on IPv4 interface eth0,
192.168.127.1#53
Dec 15 23:12:27 centos5 named[24492]: listening on IPv4 interface eth1,
46.4.15.12#53
Dec 15 23:12:27 centos5 named[24492]: command channel listening on
0.0.0.0#953
Dec 15 23:12:27 centos5 named[24492]: zone sys-adm.org.ua/IN/external:
loaded serial 2010121501
Dec 15 23:12:27 centos5 named[24492]: zone 0.0.127-in-addr.arpa/IN/internal:
loaded serial 2010121501
Dec 15 23:12:27 centos5 named[24492]: zone 127.168.192-in-
addr.arpa/IN/internal: loaded serial 2010121501
Dec 15 23:12:27 centos5 named[24492]: zone sys-adm.local/IN/internal: loaded
serial 2010121501
Dec 15 23:12:27 centos5 named[24492]: zone localhost/IN/internal: loaded
serial 2010121501
```

Если все запустилось без ошибок можно собственно произвести проверку.

```
# host -t ns sys-adm.org.ua 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

sys-adm.org.ua name server ns1.sys-adm.org.ua.
sys-adm.org.ua name server ns2.sys-adm.org.ua.

# host -t mx sys-adm.org.ua 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

sys-adm.org.ua mail is handled by 20 mail2.sys-adm.org.ua.
sys-adm.org.ua mail is handled by 10 mail.sys-adm.org.ua.

# host google.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

google.com has address 74.125.87.99
google.com has address 74.125.87.104
google.com mail is handled by 300 google.com.s9b1.psmtp.com.
google.com mail is handled by 400 google.com.s9b2.psmtp.com.
google.com mail is handled by 100 google.com.s9a1.psmtp.com.
google.com mail is handled by 200 google.com.s9a2.psmtp.com.

# host -t mx sys-adm.local 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

sys-adm.local mail is handled by 10 mail.sys-adm.local.

# host mail.sys-adm.local 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

mail.sys-adm.local has address 192.168.127.1

# host 192.168.127.1 127.0.0.1
```

```
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

1.127.168.192.in-addr.arpa domain name pointer gw.sys-adm.local.
```

На этом проверку нашего днс сервера можно считать завершенной

Проверка защиты от заражения кеша ДНС сервера. Слово **GREAT** свидетельствует о хорошей защите, в то время как **POOR** наоборот. Основная идея в защите состоит в использование случайных портов при отправке запросов.

```
# dig +short @127.0.0.1 porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"46.4.15.12 is GREAT: 26 queries in 4.4 seconds from 26 ports with std dev
20122"
```

А это плохие настройки. Если вы будете использовать опцию вида **query-source address xxx.xxx.xxx.xxx port 53**, т.е. жестко привяжет исходящий порт к определенному значению.

```
# dig +short @127.0.0.1 porttest.dns-oarc.net TXT
porttest.y.x.w.v.u.t.s.r.q.p.o.n.m.l.k.j.i.h.g.f.e.d.c.b.a.pt.dns-oarc.net.
"46.4.15.12 is POOR: 26 queries in 4.4 seconds from 1 ports with std dev 0"
```

Более подробно можно прочитать https://www.dns-oarc.net/oarc/services/porttest

~~DISCUSSION~~