Instalando DNS server (BIND) no CentOS/RHEL 7

Esse artigo mostra os passos básicos para instalação e configuração do servidor de DNS BIND no CentOS 7.

Para esse tutorial vamos configurar um servidor master com os detalhes abaixo:

- Hostname: dns01.emanuel.lab
- Endereço IP: 172.16.1.10/24
- Sistema Operacional: CentOS 7 minimal server

Configurações do ambiente

############## CONFIGURAÇÕES BÁSICAS ##############

```
DOMINIO: EMANUEL.LAB
REDE: 172.16.1.0/24
IPS
.1      ROUTE
.53     DNS01 MASTER LNX01
.54     DNS02 SECUND WIN01
.80     WWW MASTER LNX02
.81     WWW SECUND WIN02
.80     FTP MASTER LNX
.81     FTP SECUND WIN
.30     FREENAS
```

##########ARQUIVO DE CONFIGURAÇÃO DO SERVIÇO##########
/etc/named.conf
Arquivo de Configuração de Zona
/var/named/emanuel.lab.zone
/var/named/1.16.172.rev
##

Instalando pacotes

Primeiro passo é instalar os pacotes necessários, como root:

```
1    [root@dns ~]# yum install -y bind bind-utils
```

Configurando o BIND

O arquivo de configuração principal do BIND é o `/etc/named.conf`, vamos edita-lo modificando alguns poucos detalhes. Na sessão `options` procure por `listen-on` e adicione o endereço IP do servidor. Nesse exemplo a linha ficará:

```
1    listen-on port 53 { 127.0.0.1; 172.16.1.10; };
```

Também em `options` procurar por `allow-query` adicionando os endereços de rede que terão permissão para consultar o nosso servidor. Nessa configuração de exemplo vou permitir apenas a rede interna, então a linha ficará assim:

```
1    allow-query     { localhost; 172.16.1.0/24; };
```

Se você deseja permitir que qualquer servidor consulte o seu DNS, basta colocar o valor `any`:

```
1    allow-query     { any; };
```

Caso seja necessário resolver hostnames externos que não são administrados pelo servidor que você esta configurando, se faz necessário configurar servidores para onde o seu DNS server irá encaminhar esses hostnames. Ainda em `options` adicione a opção `forwarders` com a lista de servidores entre chaves e separados por ponto e vírgula.

Abaixo um exemplo onde uso os servidores de DNS do Google e do OpenDNS como forwarders:

```
1    forwarders {
2        8.8.8.8;
3        208.67.222.222;
4    };
```

No final do arquivo, já fora da sessão `options`, devemos agora indicar as zonas que serão administradas pelo servidor. É necessário criar uma entrada de zona e também o reverso dessa zona. Para o domínio e endereço de rede do nosso tutorial as entradas ficam assim:

```
1    zone "emanuel.lab" IN {
2            type master;
3            file "emanuel.lab.zone";
4    };
5
6    zone "1.16.172.in-addr.arpa" IN {
7            type master;
8            file "1.16.172.rev";
9    };
```

O parâmetro `type` indica que esse servidor é master para essas zonas e `file` diz o nome do arquivo com detalhes da zona. Você pode indicar o caminho completo ou apenas o nome do arquivo, o que significa que ele estará no caminho padrão.

Encerramos aqui a edição do arquivo `/etc/named.conf`, abaixo a listagem completa do arquivo com as modificações feitas:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; 172.16.1.10; };
        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     { localhost; 172.16.1.0/24; };

        /*
         - 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;

        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

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

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

```
39
40          pid-file "/run/named/named.pid";
41          session-keyfile "/run/named/session.key";
42
43
44          forwarders {
45                  8.8.8.8;
46                  8.8.4.4;
47          };
48  };
49
50  logging {
51          channel default_debug {
52                  file "data/named.run";
53                  severity dynamic;
54          };
55  };
56
57  zone "." IN {
58          type hint;
59          file "named.ca";
60  };
61
62  include "/etc/named.rfc1912.zones";
63  include "/etc/named.root.key";
64
65  zone "emanuel.lab" IN {
66          type master;
67          file "emanuel.lab.zone";
68  };
69
70  zone "1.16.172.in-addr.arpa" IN {
71          type master;
72          file "1.16.172.rev";
73  };
```

Criando arquivos de zona

O segundo passo é criar os arquivos para as zonas indicados na configuração principal.

Por padrão os arquivos ficam em `/var/named`, então como indicamos em `/etc/named.conf` vamos criar o arquivo `/var/named/emanuel.lab.zone` com o conteúdo abaixo:

```
1
2
3   $TTL 24h
4   @       IN      SOA     dns01.emanuel.lab. root.emanuel.lab. (
5           2018032601      ; Serial
6           12h             ; Refresh
7           15m             ; Retry
8           3w              ; Expire
9           2h              ; Mininum TTL
10  )
11  ; INFORMAÇÕES DO SERVER NAME
12  @               IN      NS      dns01.emanuel.lab.
13
14  ; Endereços IP para Nomes do Servidor
15  dns01           IN      A       172.16.1.10
16
17  ; A - Registros do Tipo Hostname
18  www             IN      A       172.16.1.80 ; linux
29  www             IN      A       172.16.1.81 ; windows
21  emanuel.lab     IN      A       172.16.1.10
22
23  ; Alias  - Registros CNAME
24  ftp             IN      CNAME   www
25
26
```

A primeira linha com TTL indica o tempo padrão para essa zona que um registro DNS deve ser armazenado em cache. A segunda linha contém um registro do tipo SOA (Start of Authority) contendo os parametros globais para zona de domínio. Esse registro vai até o fechamento dos parenteses na oitava linha. O texto após o sinal de ponto e vírgula é comentário. Alguns detalhes sobre a primeira linha do registro SOA:

- `@`- É um substituto para o nome da zona apontado na configuração feita em `/etc/named.conf`.
- `dns.emanuel.lab.`- É o servidor master para essa zona, no nosso exemplo é o próprio servidor que estamos configurando.
- `root.emanuel.lab.`- É o email do responsável por essa zona. Esse formato corresponde ao email root@emanuel.lab.

A linha comentada como Serial contém um valor número de serial number para sincronismo dessa zona. Ele permite que um servidor secundário (slave) inicie uma atualização sempre que possuir esse valor menor do que o servidor master. Uma convenção usada para esse campo é a data no formato AAAAMMDDSS onde: AAAA = ano, MM = mês, DD = dia e SS é um número sequencial atualizado a cada modificação diária.

As quatro linhas seguintes possuem campos com registros de tempo para orientar servidores secundários.

O primeiro campo (Refresh) indica o tempo que o servidor slave deve aguardar para fazer novas consultas de atualização ao servidor master.

O segundo campo (Retry) indica o tempo que o slave deve aguardar para uma nova tentativa caso encontre falha na atualização.

O terceiro campo (Expire) diz o tempo máximo que um slave pode responder pela zona sem conseguir contato com o master.

O quarto campo (Mininum TTL) diz o tempo que um servidor slave deve aguardar antes de retornar a autoridade da zona para o master server.

Os valores desses campos podem ser em segundos ou abreviados onde: w = semanas (weeks), d = dias (days), h = horas (hours) e m = minutos (minutes).

Exemplificando o comportamento com os valores que definimos. Um servidor slave irá a cada 12 horas tentar atualização com o master server, a atualização acontecerá se o valor de Serial no slave for menor do que no master. Caso a comunicação entre os servidores falhe, o slave aguardará 15 minutos antes de uma nova tentativa. Se não houver comunicação entre master e slave, o slave trabalhará nessa condição por 3

semanas até considerar seus dados ultrapassados e não mais responder pela zona. Quando a comunicação entre os servidores voltar, o slave aguardará duas horas até aceitar atualizações do master.

A linha 10 contém um registro NS que indica o nameserver, no caso o próprio servidor e a linha 11 um registro do tipo A com o endereço IP do servidor. As demais linhas são apenas exemplos onde declaro outros endereços e um alias.

Finalizado esse arquivo devemos criar o arquivo reverso em `/var/named/1.16.172.rev`.

```
1   $TTL 86400
2   @       IN SOA  primary.emanuel.lab root.emanuel.lab. (
3                                   20180323        ; serial
4                                   3600            ; refresh
5                                   1800            ; retry
6                                   1W              ; expire
7                                   3H      )       ; minimum
8   ; INFORMAÇÕES DO SERVER NAME
9   @       IN      NS      primary.emanuel.lab.
10
11  ; Reverso lookup para o Name Server
12  8               IN      PTR primary.emanuel.lab
13
14
15  ;PTR - Registros Endereços IP Hostname
16  10              PTR     emanuel
17  40              PTR     mail.emanuel.lab
18  20              PTR     www.emanuel.lab
```

O registro SOA é idêntico ao arquivo de zona. Na linha 10 temos um registro NS e na linha 11 um registro do tipo PTR (pointer) para o nosso servidor. O valor 10 é o último octeto do endereço IP do servidor (172.16.1.10). Os registros do tipo PTR podem ser declarados apenas com o último octeto como nesse exemplo ou ser completos. Quando usado apenas o último octeto o restando é preenchido com o nome da zona declarado em `/etc/named.conf`.

O endereço completo para o mesmo IP seria 1.10.16.172.in-addr.arpa.

As demais entradas são apenas outros exemplos de registro PTR para cada registro exemplo criado no arquivo anterior. Finalizada a edição, basta salvar esse arquivo.

Liberando o firewall e subindo o serviço

Com os arquivos de configuração necessários editados e salvos, basta liberar as portas no firewall e iniciar o serviço:

```
1  firewall-cmd --permanent --add-service=dns
2  firewall-cmd --complete-reload
3  systemctl enable named.service
4  systemctl start named.service
```

Validando o servidor

Se tudo deu certo até aqui o serviço esta no ar pronto para ser testado. Altere o arquivo `/etc/resolv.conf` do servidor como no exemplo abaixo:

```
1  search emanuel.lab
2  nameserver 172.16.1.10
```

Teste com o comando:

```
 1  [root@dns01 ~]# dig dns01.emanuel.lab
 2
 3  ; <<>> DiG 9.9.4-RedHat-9.9.4-51.el7_4.2 <<>> dns01.emanuel.lab
 4  ;; global options: +cmd
 5  ;; Got answer:
 6  ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 4701
 7  ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
 8
 9  ;; OPT PSEUDOSECTION:
10  ; EDNS: version: 0, flags:; udp: 4096
11  ;; QUESTION SECTION:
12  ;dns01.emanuel.lab.             IN      A
13
14  ;; ANSWER SECTION:
```

```
dns01.emanuel.lab.      86400   IN      A       172.16.1.10

;; AUTHORITY SECTION:
emanuel.lab.            86400   IN      NS      dns01.emanuel.lab.

;; Query time: 0 msec
;; SERVER: 172.16.1.10#53(172.16.1.10)
;; WHEN: Seg Mar 26 01:01:53 -03 2018
;; MSG SIZE  rcvd: 76
```

Resolva algum dos hostnames registrado para validação:

```
[root@dns01 ~]# nslookup www.emanuel.lab
Server:         172.16.1.10
Address:        172.16.1.10#53

Name:   www.emanuel.lab
Address: 172.16.1.80
```

Arquivo: hosts

/etc/hosts

```
[root@dns01 ~]# cat /etc/hosts
172.16.1.10 dns01.emanuel.lab   dns01


```

Arquivo: hostname

/etc/hostname

```
[root@dns01 ~]# cat /etc/hostname
dns01.emanuel.lab
```

```
3
```

Arquivo: resolv.conf

/etc/resolv.conf

```
1  [root@dns01 ~]# cat /etc/resolv.conf
2  # Generated by NetworkManager
3  search emanuel.lab 172.16.1.10
4  domain emanuel.lab
5  nameserver 172.16.1.10
```

Concluímos com Sucesso! :)