

DNS só IPv6

Autor: Alejandro Acosta, José G. Cotúa
Coordenação e revisão: Guillermo Cicileo
Edição: Área de Comunicações
Área: Tecnología

Introdução	2
Pré-requisitos	2
Topologia de rede a ser usada para o estudo.....	2
Informações importantes para entender melhor este documento:	2
Configuração geral e primeiros passos.....	3
Noções básicas do DNS: Servidor Autoritativo vs. Servidor Recursivo.....	5
Configuração de um servidor DNS recursivo só IPv6	6
Passo 1:	6
Passo 2:	7
Configuração de um servidor DNS autoritativo só IPv6	9
Passo 1: configuração geral e básica	9
Passo 2: configuração para 'só' autoritativo.....	9
Passo 3:	9
Configuração de Zone-Transfer.....	10
Configuração no servidor DNS Primário (Master)	10
Configuração no servidor DNS Secundário (Slave)	10
Resumo da configuração do Bind9 para só IPv6	11
Resumo dos comandos para operação do servidor Linux e Bind9	12
Gerenciamento de interfaces e endereçamento IPv6.....	12
Gerenciamento do Bind9.....	12
Ver processos e Binding do Bind9	12
Testar o DNS IPv6 no nível local.....	12
Erros comuns ao implementar um servidor DNS IPv6	12
Referências e links de interesse	13

Introdução

O artigo a seguir apresenta de maneira ordenada as considerações e etapas a seguir para gerenciar um servidor DNS só IPv6.

Vamos tentar abranger vários aspectos básicos e as funcionalidades principais. No entanto, é importante lembrar que existem muitas funcionalidades adicionais a serem consideradas.

Pré-requisitos

Este artigo trata da administração e operação de um servidor DNS no sistema operacional GNU/Linux, com instalação orientada ao servidor. Para este estudo vamos usar o servidor [DNS BIND9](#) instalado sobre S.O. Debian.

O BIND9 é um dos servidores DNS mais amplamente usados em ambientes de rede de ISP e operadoras de rede.

O servidor BIND9 deve estar previamente instalado em seu Linux, preferencialmente em versão atualizada e/ou superior a v9.10. No entanto, os conceitos discutidos aqui são aplicáveis a qualquer servidor DNS em qualquer tipo de distribuição do Linux, e até mesmo em qualquer outro servidor DNS.

Da mesma forma, o leitor deve estar familiarizado com os conceitos básicos de operação e configuração de servidores em ambientes GNU/Linux e o funcionamento básico do BIND9, como a configuração de opções, configuração de zonas, entre outros.

Topologia de rede a ser usada para o estudo

Informações de endereçamento IPv6 da topologia:

- **Prefixo de Rede Clientes:** 2001:db8:abcd::/48
- **Servidor DNS Recursivo:** 2001:db8:123::2
- **Servidores DNS Autoritativos:** 2001:db8:cafe::2 e 2001:db8:cafe::3

Informações importantes para entender melhor este documento:

Arquivos de configuração que usaremos:

/etc/bind/named.conf

/etc/bind/named.conf.options

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

Configuração geral e primeiros passos

- a) A primeira coisa é ter certeza de que temos o Bind9 instalado. Podemos verificá-lo com o seguinte comando no nosso console Linux:

```
#named -v  
BIND 9.16.15-Debian (Stable Release) <id:4469e3e>
```

Além disso, podemos executar o seguinte comando para validar que o servidor Bind9 esteja ativo e funcionando normalmente:

```
#systemctl status named  
● named.service - BIND Domain Name Server  
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset: enabled)  
  Active: active (running) since Tue 2022-MM-DD HH:MM:SS UTC; 1 day 8h ago  
    Docs: man:named(8)  
 Main PID: 2779031 (named)  
   Tasks: 26 (limit: 9507)  
  Memory: 156.5M  
   CPU: 2min 8.314s  
 CGroup: /system.slice/named.service  
        └─2779031 /usr/sbin/named -f -u bind
```

Este comando mostra não apenas o estado da operação do servidor Bind9, mas também parâmetros como PID, memória, uptime, etc.

- b) Em seguida, precisamos verificar a configuração do endereçamento IPv6 do servidor. Para isso, é importante saber quais interfaces o servidor Linux e seus endereços IP possuem. É fundamental conhecer com antecedência o endereço IPv6 onde queremos que o Bind9 escute as conexões de entrada e aqueles a partir dos quais as conexões de saída serão feitas.

Inclusive é comum usar interfaces 'bridge' no Linux para configurar o endereçamento IPv6 para uso do Bind9. Essa prática é recomendada para evitar *flapping* e aumentar a estabilidade do serviço DNS.

Existem muitas formas de gerenciar as interfaces e o endereçamento IPv6 de um servidor Debian Linux; a seguir, lembramos algumas das mais usadas:

Ver as interfaces de rede do servidor:

```
#ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT
group default qlen 1000
    link/ether 9e:11:7b:f0:98:b9 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
3: loopback: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN mode
DEFAULT group default qlen 1000
    link/ether 4e:c0:be:49:cb:23 brd ff:ff:ff:ff:ff:ff
```

Ver os endereços IPv6 configurados no servidor:

```
#ip -6 address show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 state UNKNOWN qlen 1000
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 2001:db8:cafe::2/64 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::9c11:7bff:fef0:98b9/64 scope link
        valid_lft forever preferred_lft forever
```

Os comandos acima permitem observar o endereçamento IPv6 e as interfaces de rede do servidor. No nosso caso, vamos usar a interface ens18 com a IPv6 2001:db8:cafe::2/64 (GUA). Adicionalmente, podemos observar o endereçamento LLA (LLA: Link Local Address) das interfaces. Conhecer com precisão as interfaces de rede do servidor e o endereçamento IPv6 de cada uma delas é um input importante na hora de solucionar problemas, tanto do servidor Linux quanto do Bind9.

Noções básicas do DNS: Servidor Autoritativo vs. Servidor Recursivo

Lembre-se de que existem muitos tipos de servidores DNS, sendo os mais comuns os servidores recursivos e os servidores autoritativos.

Segundo dnslookup.es [2]:

Um servidor DNS autoritativo é aquele que possui uma resposta em seu banco de dados local para um domínio sobre o qual é questionado.

Um servidor DNS recursivo é aquele que, quando não encontra uma resposta no seu banco de dados local para um domínio, tenta consultá-lo com outros servidores DNS para tentar resolver o pedido que lhe for feito.

Se voltarmos para o nosso exemplo (ver topologia) vai ser:

- O Servidor DNS recursivo lhe oferece serviço DNS aos clientes da rede: 2001:db8:abcd::/48
- Os Servidores autoritativos têm a autoridade para o domínio example.com.
- Adicionalmente, o servidor 2001:db8:cafe::3 copia a zona via “zone transfer” o 2001:db8:cafe::2

Configuração de um servidor DNS recursivo só IPv6

Passo 1:

Uma vez conferida e garantida a questão das interfaces de rede, do endereçamento IPv6 do servidor Linux e do funcionamento normal do Bind9, devemos começar a configuração do Bind9 para garantir em primeira instância que este escute no IPv6 e permita conexões de entrada desde a rede 2001:db8:abcd::/48.

O arquivo de configuração principal do servidor Bind9 é `/etc/bind/named.conf`. O que fazemos é configurar os parâmetros IPv6 apropriados na seção `options{ ...}` localizada na primeira parte deste arquivo. É possível usar a diretiva `include` dentro do arquivo de configuração para citar outros arquivos e programar as configurações em sua totalidade de forma mais organizada, usando vários arquivos e segmentando a configuração conforme sua conveniência.

A configuração da seção `options { ... }` para operação IPv6 é ilustrada abaixo:

```
options {
    directory "/var/cache/bind";
    forwarders {
        2001:db8:db8::8888;
        2001:db8:db8::8844;
    };
    listen-on-v6 { any; };
    query-source-v6 address 2001:db8:cafe::2;
    listen-on-v6 { ::1; 2001:db8:cafe::2; };
    recursion yes;
    ...;
};
```

Para simplificar, e apenas para focar na configuração para o IPv6, colocamos somente os parâmetros do IPv6.

A seguir, uma breve explicação dos parâmetros de configuração IPv6 mais importantes:

- A opção `forwarders { 2001:db8:db8::8888; 2001:db8:db8::8844; };` é opcional e a colocamos apenas se quisermos fazer *forwarding* de **todas** as consultas DNS para outro servidor DNS. Neste caso configuramos dois servidores de encaminhamento no IPv6.
- A opção `listen-on-v6 { any; };` permite especificar ao Bind9 os endereços IPv6 nos quais eu quero que escute pedidos DNS IPv6. Podemos configurá-la com a diretiva `any` especificando para o Bind9 que escutará em todos os endereços IPv6 configurados no servidor Linux, até mesmo no `localhost6 '::1'`. Também, podemos especificar os endereços IPv6 nos quais quero que o Bind9 escute, colocando os endereços IPv6 separados por `';`. Por exemplo:

```
listen-on-v6 { ::1; 2001:db8:cafe::2; };
```

Claramente, qualquer endereço IPv6 especificado aqui já deve estar configurado em uma interface do servidor Linux.

- A opção *'query-source-v6 address 2001:db8:cafe::2;'* permite especificar o(s) endereço(s) IPv6 a partir dos quais o Bind9 estabelecerá conexões de saída. As conexões de saída são essenciais para resolver o DNS, seja por meio de 'forwarding' ou de forma recursiva.

É importante observar que, uma vez feitas as atualizações da configuração do arquivo *'/etc/bind/named.conf'* devemos aplicar essas mudanças reiniciando o servidor Bind9 ou recarregando sua configuração; a seguir, os comandos:

```
#systemctl reload named
#systemctl restart named
```

Após aplicar as mudanças, podemos executar os seguintes comandos para validar que o Bind9 está escutando nos endereços IPv6 configurados:

```
#netstat -pau | grep named
```

Passo 2:

Devemos permitir a recursão para nossos clientes, especificamente para clientes da rede 2001:db8:abcd::/48. Para permitir a recursão, é usada a diretiva **'allow-recursion'**, leve em consideração que o comportamento dessa diretiva mudou nas versões mais recentes do Bind. O que fazemos neste caso é criar um ACL com o endereçamento IPv6 da rede cliente e lhe aplicamos a diretiva, conforme abaixo:

;;;Configuração do Bind9, arquivo /etc/bind/named.conf, para recursão.

```
acl my_ipv6_net {
    2001:db8:abcd::/48;
};

options {
    ...
    recursion yes;
    allow-recursion { my_ipv6_net; };
    ...
};
```

Com o exemplo anterior estamos criando um ACL chamado *'my_ipv6_net'* e subsequentemente permitindo a recursão para esse ACL. Quer dizer, que os nossos clientes poderão usar o servidor perfeitamente.

Como recomendação de segurança importante: nunca usar a opção '*allow-recursion { any; }*', pois fazendo isso estaríamos criando um servidor 'Open Resolver' com tudo o que isso implica.

Configuração de um servidor DNS autoritativo só IPv6

Passo 1: configuração geral e básica.

Da mesma forma que fizemos para um servidor DNS recursivo, precisamos garantir que o Bind9 escute e permita conexões corretamente no IPv6. Isto é, a configuração de rede IPv6 do servidor e a configuração geral e básica do Bind9 são mantidas.

Passo 2: configuração para 'só' autoritativo.

Se quisermos que o Bind9 seja 'só' autoritativo e não permita recursão, devemos configurar o arquivo '/etc/bind/named.conf' com as seguintes opções:

```
options {
    directory "/var/cache/bind";
    forwarders {
        2001:db8:db8::8888;
        2001:db8:db8::8844;
    };
    listen-on-v6 { any; };
    query-source-v6 address 2001:db8:cafe::2;
    listen-on-v6 { ::1; 2001:db8:cafe::2; };
    recursion no;
    ...;
};
```

Passo 3:

Como o servidor DNS é autoritativo, devemos estabelecer a configuração da zona 'example.com' no arquivo '/etc/bind/named.conf'. Isto é feito assim:

```
options {
    ...;
};
zone "example.com" {
    type master;
    file "/etc/bind/example.com.db";
};
```

Nota importante: um servidor DNS pode ser autoritativo e recursivo ao mesmo tempo, mas tal configuração deve contemplar uma análise mais rigorosa dos aspectos de segurança.

Configuração de Zone-Transfer

Configuração no servidor DNS Primário (Master)

Na configuração do arquivo `/etc/bind/named.conf` do Servidor DNS Primário, indicamos que é *master* e definimos o endereçamento IPv6 daqueles que estão autorizados a solicitar zone-transfer.

A seguir, a configuração correspondente:

```
options {  
    ...;  
};  
zone "example.com" {  
    type master;  
    file "/etc/bind/zones/example.com.db";  
    allow-transfer { 2001:db8:cafe::3; };  
};
```

Configuração no servidor DNS Secundário (Slave)

Na configuração do arquivo `/etc/bind/named.conf` do Servidor DNS Secundário, especificamos que é *slave* e definimos o endereçamento IPv6 dos servidores *master*.

A seguir, a configuração correspondente:

```
options {  
    ...;  
};  
zone "example.com" {  
    type slave;  
    file "example.com.db";  
    masters { 2001:db8:cafe::2; };  
};
```

Resumo da configuração do Bind9 para só IPv6

<pre>;;Autoritativo, Não Recursivo ;;Master ;;Arquivo: /etc/bind/named.conf acl my_ipv6_net { 2001:db8:abcd::/48; }; options { directory "/var/cache/bind"; //forwarders { // 2001:db8:db8::8888; // 2001:db8:db8::8844; //}; query-source-v6 address 2001:db8:cafe::2; listen-on-v6 { ::1; 2001:db8:cafe::2; }; recursion no; ...; }; zone "example.com" { type master; file "/etc/bind/zones/example.com.db"; allow-transfer { 2001:db8:cafe::3; }; };</pre>	<pre>;;Autoritativo, Não Recursivo ;;Slave ;;Arquivo: /etc/bind/named.conf acl my_ipv6_net { 2001:db8:abcd::/48; }; options { directory "/var/cache/bind"; //forwarders { // 2001:db8:db8::8888; // 2001:db8:db8::8844; //}; query-source-v6 address 2001:db8:cafe::3; listen-on-v6 { ::1; 2001:db8:cafe::3; }; recursion no; ...; }; zone "example.com" { type slave; file "example.com.db"; masters { 2001:db8:cafe::2; }; };</pre>
---	--

Resumo dos comandos para operação do servidor Linux e Bind9

Gerenciamento de interfaces e endereçamento IPv6

```
ip link show
ifconfig -a
ip -6 address show
ip -6 route show
```

Gerenciamento do Bind9

```
systemctl status named
systemctl reload named
systemctl restart named
```

Ver processos e Binding do Bind9

```
netstat -puan | grep named
```

Testar o DNS IPv6 no nível local

```
nslookup www.google.com ::1
nslookup www.google.com 2001:db8:cafe::2
nslookup -type=AAAA www.google.com ::1
dig @::1 AAAA www.google.com
```

Erros comuns ao implementar um servidor DNS IPv6

- Erros de digitação na configuração do arquivo '/etc/bind/named.conf', principalmente nas opções que terminam ou usam o símbolo ';'. Portanto, recomenda-se ter muito cuidado ao editar e criar configurações.
- Usar de forma inapropriada as opções de recursão e de servidor autoritativo do Bind9, colocando-o como um 'Open Resolver' com todas as implicações de segurança associadas.
- Não validar corretamente os endereços IPv6 do servidor e não fazê-los corresponder nas configurações do Bind9.
- Fazer que o servidor Bind9 escute em endereços IPv6 configurados em interfaces *flapping*. Isso faz com que o serviço DNS seja intermitente.
- Editar incorretamente o nome dos arquivos das zonas.

Referências e links de interesse

- <https://kb.isc.org/docs/aa-00269>
- <https://www.isc.org/bind/>
- <https://labs.lacnic.net/RRL-en-BIND9/>