**Pré-requisitos**

* O endereço IP do servidor é estático.

**Procedimento**

Instale os pacotes bind e bind-utils:

# **yum install bind bind-utils**

Edite o /etc/named.conf arquivo e faça as seguintes alterações na options instrução:

Atualize as instruções listen-on e listen-on-v6 para especificar em quais interfaces IPv4 e IPv6 o BIND deve atender:

* 1. **listen-on port 53 { *127.0.0.1; 192.0.2.1;* };**

**listen-on-v6 port 53 { *::1; 2001:db8:1::1;* };**

* 1. Atualize a allow-query instrução para configurar de quais endereços IP e intervalos os clientes podem consultar este servidor DNS:

**allow-query { *localhost; 192.0.2.0/24; 2001:db8:1::/64;* };**

* 1. Adicione uma allow-recursion instrução para definir de quais endereços IP e intervalos o BIND aceita consultas recursivas:

**allow-recursion { *localhost; 192.0.2.0/24; 2001:db8:1::/64;* };**

Por padrão, o BIND resolve consultas consultando recursivamente dos servidores raiz para um servidor DNS autoritativo. Alternativamente, você pode configurar o BIND para encaminhar consultas para outros servidores DNS, como os do seu provedor. Neste caso, adicione uma forwarders declaração com a lista de endereços IP dos servidores DNS para os quais o BIND deve encaminhar as consultas:

**forwarders { *198.51.100.1; 203.0.113.5;* };**

Verifique a sintaxe do /etc/named.conf arquivo:

# **named-checkconf**

Se o comando não exibir nenhuma saída, a sintaxe está correta.

Atualize as firewalld regras para permitir o tráfego DNS de entrada:

# **firewall-cmd --permanent --add-service=dns**

# **firewall-cmd --reload**

Inicie e habilite o BIND:

# **systemctl enable --now named**

Configurando zonas em um servidor BIND DNS

Uma zona DNS é um banco de dados com registros de recursos para uma subárvore específica no espaço do domínio. Por exemplo, se você for o responsável pelo example.com domínio, poderá configurar uma zona para ele no BIND. Como resultado, os clientes podem resolver [www.example.com](http://www.example.com) para o endereço IP configurado nesta zona.

Adicione uma definição de zona ao /etc/named.conf arquivo:

**zone "*example.com*" {**

**type master;**

**file "*example.com.zone*";**

**allow-query { *any;* };**

**allow-transfer { *none;* };**

**};**

Verifique a sintaxe do /etc/named.conf arquivo:

# **named-checkconf**

Create the /var/named/example.com.zone file, for example, with the following content:OPKOOK

**$TTL *8h***

**@ IN SOA *ns1.example.com.* *hostmaster.example.com.* (**

***2022070601*** **; serial number**

***1d*** **; refresh period**

***3h*** **; retry period**

***3d*** **; expire time**

***3h*** ) **; minimum TTL**

**IN NS** **ns1.example.com.**

**IN MX** **10 mail.example.com.**

**www** **IN A** **192.0.2.30**

**www** **IN AAAA** **2001:db8:1::30**

**ns1** **IN A** **192.0.2.1**

**ns1** **IN AAAA** **2001:db8:1::1**

**mail** **IN A** **192.0.2.20**

**mail** **IN AAAA** **2001:db8:1::20**

1. Defina permissões seguras no arquivo de zona que permitem que apenas o named grupo o leia:
2. # **chown root:named /var/named/*example.com.zone***
3. # **chmod 640 /var/named/*example.com.zone***
4. Verifique a sintaxe do /var/named/example.com.zone arquivo:
5. # **named-checkzone *example.com* */var/named/example.com.zone***
6. zone *example.com/IN*: loaded serial *2022070601*
7. OK
8. Recarregar BIND:
9. # **systemctl reload named**

<https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/deploying_different_types_of_servers/assembly_setting-up-and-configuring-a-bind-dns-server_deploying-different-types-of-servers>