

DNS Bind9

Instalação e configuração:

Considerando um cenário onde a nossa máquina está em uma rede onde seu IP é o 192.168.1.35.

Iniciamos atualizando o sistema e instalamos o BIND9:

```
sudo apt update
sudo apt upgrade
sudo apt install bind9
```

Verificamos se o serviço está rodando:

```
sudo service bind9 status
```

Acessamos a pasta do Bind9 para manipularmos os arquivos:

```
cd /etc/bind/
```

Abrimos o arquivo named.conf.options:

```
sudo gedit named.conf.options
```

e colamos o conteúdo:

```
options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    // forwarders {
    //     0.0.0.0;
    // };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys. See https://www.isc.org/bind-keys
    //=====
    dnssec-validation auto;

    listen-on-v6 { none; };
    listen-on port 53 { any; };
    allow-query { any; };
    forwarders { 0.0.0.0; };
};
```

Onde:

listen-on-v6 { none; }; Essa linha especifica em quais endereços IPv6 o BIND9 deve escutar por conexões DNS. No caso de none, o BIND9 não escutará em nenhum endereço IPv6. Isso significa que o servidor BIND9 não aceitará conexões DNS IPv6.

listen-on port 53 { any; }; Esta linha define em quais endereços IPv4 o BIND9 deve escutar por conexões DNS na porta 53, que é a porta padrão para o DNS. O valor any significa que o BIND9 escutará em todos os endereços IPv4 disponíveis na máquina.

allow-query { any; }; Esta linha especifica quem tem permissão para enviar consultas DNS para o servidor BIND9. O valor any indica que todas as máquinas têm permissão para enviar consultas DNS para este servidor.

forwarders { 0.0.0.0; }; Esta linha define para onde o BIND9 encaminhará consultas de DNS que não pode responder localmente. O valor 0.0.0.0 significa que não há forwarders definidos, então o BIND9 não encaminhará consultas para nenhum outro servidor DNS. Isso implica que o BIND9 tentará resolver todas as consultas usando suas próprias configurações de zonas e não encaminhará consultas para servidores DNS externos.

Abrimos o arquivo `named.conf.local`:

```
sudo gedit named.conf.local
```

e colamos o conteúdo:

```
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "trabredes.teste" {  
    type master;  
    file "/etc/bind/forward.trabredes.teste";  
};  
zone "1.168.192.in-addr.arpa" {  
    type master;  
    file "/etc/bind/reverse.trabredes.teste";  
};
```

Especificamos a zona *trabredes.teste*, isso indica que este servidor BIND9 é autoritativo para o domínio *trabredes.teste*, o que significa que ele é responsável por responder consultas DNS para esse domínio. E definimos a zona reversa *1.168.192.in-addr.arpa*. Para ambos, definimos como master e definimos o local do arquivo de configuração de cada zona.

Criação das zonas:

Criamos o arquivo `forward.trabredes.teste` com base no arquivo `db.local`:

```
sudo cp db.local forward.trabredes.teste
```

```
sudo gedit forward.trabredes.teste
```

e colamos o conteúdo:

```
;  
;  
; BIND data file for local loopback interface  
;  
;  
$TTL      604800  
@         IN      SOA     primario.trabredes.teste. root.trabredes.teste. (  
    2             ; Serial  
    604800        ; Refresh  
    86400         ; Retry  
    2419200       ; Expire  
    604800 )      ; Negative Cache TTL  
;  
;  
@         IN      NS      primario.trabredes.teste.  
primario  IN      A       192.168.1.35  
www       IN      A       192.168.1.35  
mail      IN      A       192.168.1.35  
ServidorWEB IN      CNAME  www.trabredes.teste
```

Onde *192.168.1.35* é o endereço IP de cada servidor definido (www, mail, 'ServidorWEB').

Criamos o arquivo `reverse.trabredes.teste` com base no arquivo `db.127` e abrimos:

```
sudo cp db.127 reverse.trabredes.teste
```

```
sudo gedit reverse.trabredes.teste
```

e colamos o conteúdo:

```

;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA     primario.trabredes.teste. root.trabredes.teste. (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@         IN      NS      primario.trabredes.teste.
primario  IN      A       192.168.1.35
35        IN      PTR     primario.trabredes.teste.
35        IN      PTR     www.trabredes.teste.
35        IN      PTR     mail.trabredes.teste.

```

Reiniciamos o serviço do bind9 e vamos checar o status:

```

sudo service bind9 restart
sudo service bind9 status

```

Antes de testar, precisamos habilitar o serviço do bind9:

```

sudo systemctl enable bind9

```

ou:

```

sudo systemctl enable named

```

Podemos usar o próprio named para checar os arquivos de configuração:

```

sudo named-checkconf named.conf.local
sudo named-checkzone trabredes.teste forward.trabredes.teste
sudo named-checkzone trabredes.teste reverse.trabredes.teste

```

Criar arquivo para salvar logs:

Criar a Pasta 'named' em '/var/log':

```

sudo mkdir /var/log/named

```

Ajustar as Permissões de Acesso:

Ajustar as permissões de acesso para garantir que o BIND9 tenha permissão para escrever nos arquivos de log. Fazemos isso definindo o proprietário e o grupo da pasta como 'bind' (o usuário padrão usado pelo BIND9) e concedemos permissões de escrita:

```

sudo chown -R bind:bind /var/log/named
sudo chmod -R 755 /var/log/named

```

Configurar o BIND9 para Registrar Logs na Nova Pasta:

Depois de criar a pasta 'named' e ajustar as permissões, devemos configurar o BIND9 para direcionar os logs para essa pasta. Abra o arquivo de configuração do BIND9:

```

sudo nano /etc/bind/named.conf

```

Dentro deste arquivo podemos definir as configurações de logging para apontar para a nova pasta 'named'. É possível adicionar ou modificar as linhas relevantes para apontar para a pasta 'named'. No nosso exemplo configuramos o logging para registrar logs de consulta e respostas, adicionando o código:

```

logging {
    channel query_log {
        file "/var/log/named/query.log" versions 3 size 5m;
        severity debug;
        print-time yes;
        print-severity yes;
        print-category yes;
    };
}

```

```
};  
  
category queries {  
    query_log;  
};  
};
```

Este exemplo configura o BIND9 para registrar logs de consulta em ‘/var/log/named/query.log’.

Reiniciamos o serviço do bind9 e checamos o status:

```
sudo service bind9 restart  
sudo service bind9 status
```

Testando a configuração:

Podemos testar a configuração em outro computador na rede, com o comando ‘nslookup’:

```
nslookup www.trabredes.teste 192.168.1.35
```