

## DNS

O DNS (Domain Name System) – Sistema de Nomes de Domínio tem como função resolver um nome para endereço IP e um endereço IP para nome.

Após instalar o serviço do DNS (BIND9) os arquivos de configuração ficarão no seguinte diretório **/etc/bind**

Entre no diretório **/etc/bind** e liste os arquivos conforme abaixo:

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

Arquivos	Descrição
db.0	Arquivo reverso para a zona broadcast
db.127	Arquivo reverso para a interface de loopback
db.255	Arquivo reverso para a zona de broadcast
named.conf	Arquivo de configuração principal do BIND DNS Server
named.conf.default-zones	O Arquivo com o mapeamentos dos root servers
named.conf.local	É neste arquivo que são adicionadas as zonas DNS
named.conf.options	Configurações adicionais do DNS

## Exemplo

Vamos criar um domínio chamado estudo.local que resolva nome para endereço IP e um domínio reverso para a rede 192.168.10.0 que resolva endereço IP para nome.

**Para criar o domínio estudo.local, siga os passos abaixo:**

a) Edite o arquivo **named.conf.local**, digitando

```
nano /etc/bind/named.conf.local
```

ou

```
cd /etc/bind
nano named.conf.local
```

```
GNU nano 2.2.2      Arquivo: named.conf.local      Modificado
//
// 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 "estudo.local" {
    type master;
    file "/etc/bind/arquestudo.local";
};

zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/reverso.local";
};

^G Ajuda      ^O Gravar     ^R Ler o Arq  ^Y Páq Anter  ^K Recort Txt ^C Pos Atual
^X Sair       ^J Justificar ^W Onde está? ^V Próx Páq  ^U Colar Txt  ^T Para Spell
```

### Opções do domínio estudo.local

Após o comando **zone** você deve definir o nome do domínio, obrigatoriamente entre aspas, como por exemplo, “**estudo.local**”. O **type** define se o domínio será primário (**máster**) ou secundário (**slave**). A opção **file** define o caminho e o nome do arquivo que armazenará as informações de resolução de nomes para endereço IP.

### Opções do domínio 10.168.192.in-addr.arpa

O domínio **10.168.192.in-addr.arpa** é o domínio reverso da rede 192.168.10.0, acrescido do **.in-addr.arpa**.

Ao criar os domínios no arquivo **named.conf.local** salve as alterações.

### Criando e configurando o arquivo arquestudo.local

Para criar o arquivo **arquestudo.local**, siga os passos abaixo:

a) Digite

```
nano /etc/bind/arquestudo.local
```

ou

```
cd /etc/bind
nano arquestudo.local
```

b) Digite as linhas abaixo no arquivo `arquestudo.local`

```
GNU nano 2.2.2      Arquivo: arquestudo.local      Modificado
$TTL      604800      _
@          IN          SOA      ns1.estudo.local root.ns1.estudo.local (
          1            ; serial
          604800       ; refresh
          86400        ; retry
          2419200      ; expire
          604800 )      ; negative cache TTL
;
@          IN          MX       5 mail01.estudo.local
@          IN          NS       ns1.estudo.local
@          IN          NS       ns2.estudo.local

ns1        IN          A        192.168.10.200
ns2        IN          A        192.168.10.202
mail01     IN          A        192.168.10.204
serverweb  IN          A        192.168.10.206

pop3       IN CNAME      mail01
smtp       IN CNAME      mail01
www        IN CNAME      serverweb

lab1       IN          A        192.168.10.220
lab2       IN          A        192.168.10.222
```

Opções do arquivo

**\$TTL 604800:** Define o tempo de vida do registro, o tempo que o registro ficará armazenado em cache após sua resolução.

**@ IN SOA ns1.estudo.local root.ns1.estudo.local(**

O parâmetro `@` faz referencia ao domínio da zona definida no arquivo `/etc/bind/named.conf.local`, ou seja, refere-se ao domínio **estudo.local**. Outro parâmetro desta linha estabelece o início de autoridade – SOA, o nome de máquina **ns1.estudo.local** determina o servidor que tem autoridade sobre a zona. Já **root.estudo.local** define o endereço de e-mail da pessoa responsável por este domínio, neste arquivo o `@` do e-mail é substituído por um `(.)`, pois como visto, o `@` tem outra finalidade.

**1 ; serial**

Este é o número serial que diz ao servidor secundário se este arquivo de registro de recurso foi atualizado. Toda vez que atualizar DNS, você deve alterar este número para um número maior, pois assim o DNS secundário fará sua atualização dinamicamente. O Servidor DNS secundário checka periodicamente o início de autoridade SOA e compara o seu número serial com o servidor, se o seu número serial for menor, ele será atualizado. Por isso ao alterar o banco de dados devemos incrementar o número serial.

### **604800 ; refresh**

Este é o período em segundo que o servidor DNS secundário utiliza para verificar periodicamente o número serial e, conseqüentemente, fazer a atualização, esta atualização só é feita caso o número serial do DNS secundário seja menor que o número serial do servidor DNS primário.

### **86400 ; retry**

Este é o ciclo de tentativas. O ciclo de tentativas determina o tempo que o servidor DNS secundário deve esperar por uma nova solicitação quando o servidor DNS primário falhar na resposta de um registro SOA. Exemplo: o servidor DNS secundário tenta verificar o número serial do servidor DNS primário e este não responde, então o servidor DNS secundário irá esperar por 86400 segundos para uma nova solicitação.

### **2419200 ; expire**

Este é o tempo limite, o período em segundo que o servidor DNS secundário deve continuar respondendo mesmo que não consiga atualizar o arquivo de zona primária, ou seja, mesmo que o servidor DNS primário não esteja respondendo.

### **604800 ) ; negative cache TTL**

Define o tempo de vida (time-to-live) em segundo que outro servidor de nomes irá armazenar em cache a informação de uma consulta de domínio não existente (no such domain – NXDOMAIN). Neste exemplo, quando um outro DNS realiza uma consulta que resultou um host não existente, por exemplo tentou achar o host naoexiste.sistemabaertos.com.br, esta consulta fica armazenada em cache.

### **Registro MX – Definindo servidores de mensagens**

**@ IN MX 5 mailserver.estudo.local**

O registro de recurso MX estabelece os servidores de mensagens (servidores de correio) para este domínio. Neste caso usamos também o servidor mailserver como sendo o servidor de correio, lembrando que para configurar um servidor de correio é necessário todo um processo de configuração, o que estamos fazendo é apenas um pré-requisito. Os registros MX redirecionam mensagens endereçadas para o domínio estudo.local. Todo e-mail enviado para [jpaulo@estudo.local](mailto:jpaulo@estudo.local) será recebido pelo servidor mailserver e pode ser repassado de acordo com a configuração do servidor de mensagens para outros hosts.

Logo depois da entrada MX existe um número, que define a prioridade do servidor de e-mail. Você pode ter várias entradas MX com diferentes servidores de e-mail. Cada servidor de e-mail deve ter prioridade diferente, sendo que quanto menor for o número, maior será a prioridade. Assim quando o servidor de maior prioridade falhar o segundo servidor de menor número fará o papel de servidor de e-mail deste domínio.

## Registro NS – definindo servidores de nome

```
@    IN    NS    ns1.estudo.local
@    IN    NS    ns2.estudo.local
```

O Registro de recurso define os servidores de nome oficiais para o domínio. Neste exemplo encontramos dois servidores de nome. O primeiro nome, **ns1** é o servidor de nomes primário, neste exemplo estamos adotando como servidor secundário o host **ns2**.

## Registro A – Definindo os hosts e seus IPs

```
ns1           IN    A    192.168.10.200
ns2           IN    A    192.168.10.202
mail01        IN    A    192.168.10.204
serverweb     IN    A    192.168.10.206
```

Acima de todas as funções o objetivo final deste arquivo é mapear nomes para endereços IP. Eis aqui um exemplo das próximas linhas do arquivo:

```
ns1           IN    A    192.168.10.200
```

Podemos traduzir esta linha para:

### Máquina ns1 em rede TCP/IP possui endereço IP 192.168.10.200

Assim deve ser feito para todas as máquinas da rede, toda máquina da rede deve ter uma linha com seu endereço IP neste arquivo. Quando você solicitar uma máquina através de um nome, a máquina que solicitou pergunta ao servidor DNS e ele responde conforme a linha traduzida acima, assim você obtém o requisitado endereço IP.

Neste caso colando apenas o primeiro nome, o sistema entende como pertencente ao domínio estudo.local.

## Registro CNAME

```
pop3 IN CNAME mail01
smtp IN CNAME mail01
www  IN CNAME serverweb
```

Este registro é utilizado para atribuir apelidos para um host. **CNAME** indica qual é o nome canônico para um alias. Nome canônico é o nome real da máquina. Deve-se notar que um nome canônico sempre tem um registro A associado para definir o seu endereço IP, portanto um registro **CNAME** sempre é acompanhado de um host que teve seu número IP referenciado por um registro A, nunca outro alias. Assim ao colocar um alias **www** para um host, este provavelmente é o servidor web deste domínio. Assim, seguindo nosso exemplo quando uma pessoa digitar em um browser [www.estudo.local](http://www.estudo.local), na verdade, estará acessando a máquina serverweb.estudo.local. Isto é interessante na medida que não é necessário decorarmos nomes de máquinas. Assim digitando [www.estudo.local](http://www.estudo.local) teremos a certeza de acessar o servidor web deste domínio.

## Arquivo de Zona Reversa

Assim como o DNS é capaz e converte nomes para endereço IP, o DNS também é capaz de converte números IP para nomes. Alguns serviços, como por exemplo o ftp, utilizam a resolução reversa para registrar o nome do host cliente FTP em vez de seu número IP em seu histórico.

Para que o DNS forneça este serviço precisamos criar o arquivo da base de dados da zona reversa. Antes disto, devemos criar uma zona reversa no arquivo **/etc/bind/named.conf.local** e, posteriormente, criar o arquivo de banco de dados.

**Nota:** Esta zona já foi criada anteriormente com nome de 10.168.192.in-addr.arpa. Lembre-se também que o arquivo da base de dados definido para esta zona deve ter o nome de **revverso.local**. Através do arquivo **named.conf.local** e da zona definida no exemplo, devemos criar este arquivo no diretório **/etc/bind**, o arquivo deverá ter o nome **revverso.local**. Segue abaixo a configuração deste arquivo:

```
GNU nano 2.2.2      Arquivo: revverso.local

$TTL 604800
@      IN      SOA      ns1.estudo.local    root.ns1.estudo.local (
        1      ; serial
        604800 ; refresh
        86400  ; retry
        2419200 ; expire
        604800 ) ; negative cache TTL
;
@      IN      NS       ns1.estudo.local
@      IN      NS       ns2.estudo.local
@      IN      MX       5 mail01.estudo.local

200    IN      PTR      ns1
202    IN      PTR      ns2
204    IN      PTR      mail01
206    IN      PTR      serverweb
220    IN      PTR      lab1
222    IN      PTR      lab2

[ Escrito 19 linhas ]
^G Ajuda  ^O Gravar  ^R Ler o Arq ^Y Pág Anter ^K Recort Txt ^C Pos Atual
^X Sair   ^J Justificar ^W Onde está? ^V Próx Pág  ^U Colar Txt ^T Para Spell
```

O arquivo da base de dados da zona reversa também possui um registro de recurso SOA em um registro de recurso NS. Geralmente os mesmos parâmetros utilizados no arquivo de banco de dados de zona. A finalidade da resolução reversa é obter o nome canônico de um host, baseado em seu IP. Para isto utiliza-se o registro de recurso PTR, que associa um endereço IP a um nome de host. O endereçamento reverso usa um domínio fictício convencionado como **in-addr.arpa** em que o número IP é de forma reversa.

Observe que a zona foi definida com o endereço de rede de trás para frente sendo **10.168.192.in-addr.arpa**. No arquivo da zona reversa deve ser estabelecido os outros octetos do endereço IP pertinente ao endereço do host, e deve ser também de trás para frente. Vejamos a máquina **ns1** que neste exemplo está definido como endereço de host **200**. Agora associe este endereço ao endereço de rede de trás para frente. Resultado:

**192.168.10.200**, o endereço IP exatamente ao contrário. Logo o endereço IP desta máquina interpretado pelo **named** será **192.168.10.200**. Depois de feito isso, os próximos passos são:

### Reiniciar o serviço do DNS

Para reiniciar o serviço do DNS, siga os passos:

`/etc/init.d/bind9 restart`      - Reinicia o serviço do DNS

Ou

`/etc/init.d/bind9 stop`      - Para o serviço do DNS

`/etc/init.d/bind9 start`      - Inicia o serviço do DNS

### Configurar o arquivo `/etc/resolv.conf`

Neste arquivo você deve definir o nome do domínio a ser resolvido e o endereço IP do servidor DNS primário e secundário.

```
GNU nano 2.2.2      Arquivo: /etc/resolv.conf      Modificado
search estudo.local
nameserver 192.168.10.200
nameserver 192.168.10.202

^G Ajuda      ^O Gravar      ^R Ler o Arg    ^V Pág Anter    ^K Recort Txt   ^C Pos Atual
^X Sair        ^J Justificar  ^W Onde está?  ^M Próx Pág     ^U Colar Txt    ^T Para Spell
```

### Configurando o servidor DNS Secundário

Este tipo de servidor é considerado também um servidor autorizado, pois tem um completo banco de dados de domínio que transfere do servidor primário.

Mas qual será a principal diferença entre os servidores DNS primário e secundário? O servidor DNS primário extrai seus dados diretamente de seus arquivos de registro de

banco de dados (arquivos locais), enquanto o servidor DNS secundário carrega os dados por meio de outro servidor DNS, através de um processo chamado de transferência de zona.

A grande vantagem de utilizar o servidor DNS secundário é a manutenção do servidor. Com o servidor DNS secundário você precisa manter a informação atualizada apenas no servidor DNS primário, pois o servidor DNS secundário faz uma transferência de zona do servidor DNS primário. Alterando o servidor DNS primário esta configuração será refletida, conseqüentemente, no servidor DNS secundário, assim a manutenção é totalmente centralizada no servidor DNS primário.

Para configurar o arquivo **named.conf.local** do servidor DNS secundário, siga os passos abaixo:

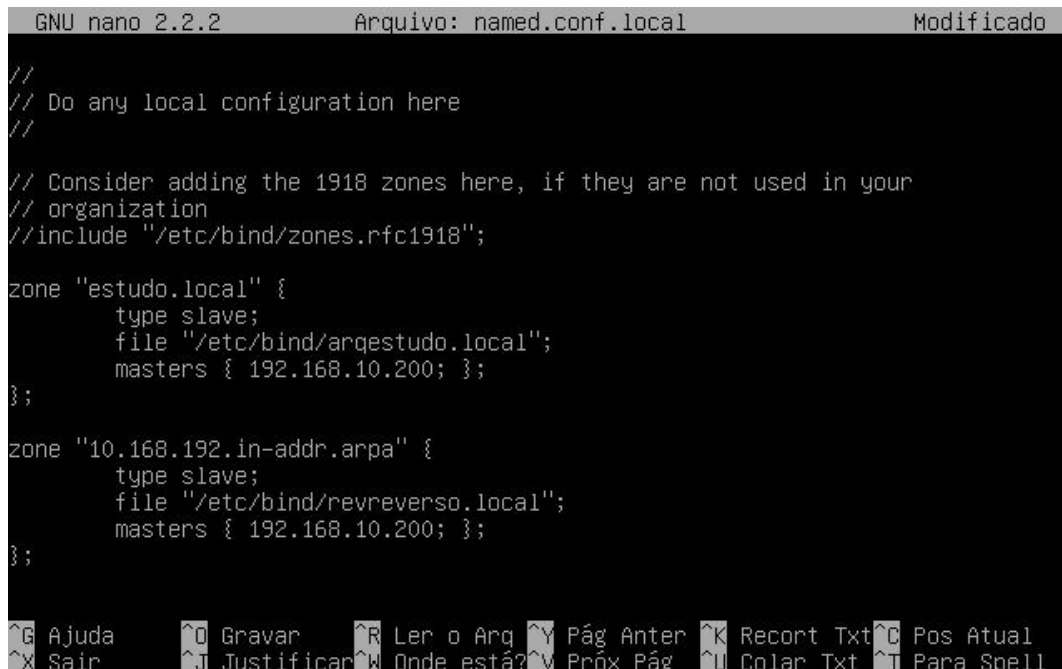
- a) Edite o arquivo named.conf.local, digitando

```
nano /etc/bind/named.conf.local
```

ou

```
cd /etc/bind  
nano named.conf.local
```

- b) Digite as linhas neste arquivo, conforme abaixo:



```
GNU nano 2.2.2      Arquivo: named.conf.local      Modificado  
//  
// 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 "estudo.local" {  
    type slave;  
    file "/etc/bind/argestudo.local";  
    masters { 192.168.10.200; };  
};  
  
zone "10.168.192.in-addr.arpa" {  
    type slave;  
    file "/etc/bind/revreverso.local";  
    masters { 192.168.10.200; };  
};  
  
^G Ajuda      ^O Gravar      ^R Ler o Arq  ^Y Pág Anter  ^K Recort Txt ^C Pos Atual  
^X Sair      ^J Justificar  ^W Onde está? ^V Próx Pág   ^U Colar Txt  ^T Para Spell
```

- c) Salve as alterações no arquivo named.conf.local e reinicie o serviço do DNS no servidor DNS secundário