

## GNU/Linux Debian – Servidor DNS

Neste tutorial, será apresentado a configuração do serviço de rede *DNS* (*Domain Name System*) utilizando o sistema operacional *GNU/Linux*, distribuição *Debian* 7.5.

Antes de começamos a instalar e configurar o servidor *DNS*, é necessário que verifique o *Hostname*, ou seja, o nome de seu computador, e em seguida as configurações de rede do servidor, como endereço IP e Gateway.

**Nota.:** Para configurar o *Hostname* do seu servidor, acesse o arquivo ***/etc/hostname*** e adicione o nome desejado. Para realizar as configurações de rede, acesse o arquivo ***/etc/network/interfaces*** e aplique as configurações desejadas.

### 1 Instalação do Serviço

A instalação do serviço de resolução de nomes *DNS* no *Debian* é realizada instalando o pacote ***bind9***. Esta instalação pode ser feita de várias formas. A seguir listarei as duas formas mais utilizada para realizar sua instalação, utilizando o gerenciador de pacotes ***apt*** e através do pacote ***.deb***.

**Obs:** Caso não exista conexão com a internet para realizar instalação do pacote ***bind9*** de um repositório, podemos configurar o Sistema Operacional (SO) para instalar o pacote a partir do CD/DVD de instalação do *Debian*. Para isso, insira o CD/DVD de instalação do *Debian* e execute o seguinte comando:

```
root@certified:~# apt-cdrom add
```

Após a execução deste comando, o SO apresentará uma mensagem informando que passará a instalar os pacotes a partir do CD/DVD adicionado e que caso exista outros CD/DVDs, repita o processo.

Depois deste processo, podemos passar para os próximos passos. Lembrando que quem possui conexão com a internet, não precisa realizar este processo, basta passar diretamente para as etapas a seguir.

### 1.1 Instalação utilizando o gerenciador de pacotes “apt”

- No Shell do Linux, digite o comando “**apt-get update**”

```
root@certified:~# apt-get update
```

Este comando irá atualizar os repositórios (localizado na internet ou localmente – CD/DVD) utilizados para a instalação de pacotes no *Debian*.

- Após a atualização, podemos realizar a instalação do pacote **bind9**. Para isso, execute o comando “**apt-get install bind9**”

```
root@certified:~# apt-get install bind9
```

Após a execução deste comando, será apresentada uma mensagem informando quais pacotes (além do **bind9**) são necessários para o funcionamento do serviço *DNS*.

```
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  squid-common squid-langpack
Use 'apt-get autoremove' to remove them.
The following extra packages will be installed:
  bind9utils
Suggested packages:
  bind9-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9utils
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/455 kB of archives.
After this operation, 1,389 kB of additional disk space will be used.
Do you want to continue [Y/n]? _
```

Digite **Y** para aceitar a instalação e **N** para cancelar. Após aceitar a instalação, o SO realizará a instalação dos pacotes mencionados acima. Juntamente com a instalação, ele adicionará um usuário de sistema e um grupo denominado **bind**, que será utilizado para execução do serviço. Além disso, ele inicia automaticamente o serviço.

```
Preconfiguring packages ...
Selecting previously deselected package bind9utils.
(Reading database ... 24690 files and directories currently installed.)
Unpacking bind9utils (from .../bind9utils_9.7.2.dfsg.P3-1.1_i386.deb) ...
Selecting previously deselected package bind9.
Unpacking bind9 (from .../bind9_9.7.2.dfsg.P3-1.1_i386.deb) ...
Processing triggers for man-db ...
Setting up bind9utils (1:9.7.2.dfsg.P3-1.1) ...
Setting up bind9 (1:9.7.2.dfsg.P3-1.1) ...
Adding group `bind' (GID 107) ...
Done.
Adding system user `bind' (UID 104) ...
Adding new user `bind' (UID 104) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
#
Starting domain name service...: bind9.
```

## 1.2 Instalação utilizando o pacote .deb

A instalação do **bind9** utilizando o pacote .deb é realizada da seguinte maneira:

– Faça o *download* da última versão do pacote. O download do pacote pode ser efetuado diretamente no site oficial do *Debian*: <http://packages.debian.org/>

**Dica:** Para realizar o download, podemos utilizar o comando **wget** que irá realizar o download colocá-lo no diretório corrente do usuário. Para utilizar o comando, basta executá-lo com o endereço URL posto em sua frente, que o download será iniciado automaticamente.

**Sintaxe:** `wget http://packages.debian.org/bind9.x.x.deb`

– Após realizar o *download*, acesse o diretório onde o pacote está localizado e execute o seguinte comando: “**dpkg –i bind9.x.x.deb**”, onde “x.x” seria a versão do pacote a ser instalado. Se não ocorrer nenhum erro, o pacote será instalado corretamente, e o serviço *DNS* estará pronto para ser configurado.

**Nota.:** Recomenda-se a instalação do pacote `bind9` através do gerenciador de pacotes `apt`, pois caso haja alguma dependência, o mesmo tem condições de tratá-las de forma automatizada.

## 2 Configuração do bind9

Todas as configurações do serviço *DNS* no *Debian* são realizadas dentro de arquivos de textos. Todos os arquivos de configuração estão localizados no diretório `/etc/bind`. Ao acessar este diretório, podemos visualizar os seguintes arquivos:

```
root@certified:/etc/bind# ls
bind.keys  db.empty    named.conf.default-zones  zones.rfc1918
db.0       db.local    named.conf.local
db.127     db.root     named.conf.options
db.255     named.conf  rndc.key
root@certified:/etc/bind# _
```

### 2.1 named.conf

O arquivo `named.conf` é um dos principais arquivos de configuração do *DNS*. Neste arquivo especificamos os outros arquivos que serão utilizados para sua configuração.

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Como podemos visualizar na figura acima, para a adição das zonas dos domínios que serão publicados pelo servidor *DNS*, deverá ser utilizado o arquivo `named.conf.local`, que esta incluso (include) neste arquivo.

Além do `named.conf.local`, podemos verificar também a inclusão de mais dois arquivos que serão utilizados para a configuração do serviço, sendo o **`named.conf.options`** e o **`named.conf.default-zones`** que serão apresentados posteriormente.

## 2.2 `named.conf.local`

Como apresentado anteriormente, o `named.conf.local` é o arquivo utilizado pelo Debian para configurar os domínios que serão publicados pelo servidor. É neste arquivo que será explícito quais serão os arquivos e tipos de zonas utilizados pelo domínio. Para realizar a configuração deste arquivo, siga os passos.:

- Acesse o arquivo;
- Ao acessar o arquivo, veremos que não existe nenhuma configuração no mesmo, apenas alguns comentários informando que as configurações locais devem ser feitas neste arquivo e que elas são baseadas na RFC1918. Desta forma, devemos cadastrar todos os domínios que serão publicados, indicando as configurações e arquivos utilizados das zonas direta e reversa.
- Para a zona direta, siga o seguinte modelo.:

```
zone "cnetworking.local" {  
    type master;  
    file "/var/cache/bind/cnet.zone"  
};
```

### Onde.:

**zone** – Indica entre “aspas dupla” qual sufixo DNS do domínio que será publicado;

**type** – Indica o tipo de zona, podendo variar entre **master** e **slave**, ou seja, zona primária e secundária, em caso da utilização de mais de um servidor DNS para o domínio.

**file** – Indica o caminho e nome do arquivo que conterà as informações sobre a zona específica.

Além dessas opções, existem outras que podem ser utilizadas, como por exemplo a “**allow-transfer**” que define para qual servidor a zona poderá ser transferida (utilizada geralmente para transferir a zona para um servidor DNS slave/secundário do domínio) que será abordado em um outro momento.

- Para zona reversa siga o modelo.:

```
zone "1.168.192in-addr.arpa {  
    type master;  
    file "/var/cache/bind/cnet.rev"  
};
```

**Onde.:**

**zone** – Indica entre “aspas dupla” o endereço de rede (de forma reversa) do domínio que será publicado.

**type** – Indica o tipo de zona, podendo variar entre **master** e **slave**, ou seja, zona primária e secundária, em caso da utilização de mais de um servidor DNS para o domínio.

**file** – Indica o caminho e nome do arquivo que conterà as informações sobre a zona específica.

### 2.3 db.root

Arquivo responsável por armazenar as configurações dos servidores raízes (root Hint) que serão utilizadas para pesquisa interativa do servidor *DNS* local.

**Obs:** Não é recomendado que realize alterações neste arquivo (a menos que saiba o que esteja fazendo), pois qualquer tipo de alteração pode influenciar diretamente no funcionamento do serviço.

## 2.4 named.conf.options

O `named.conf.options` é o arquivo responsável por especificarmos qual o diretório padrão dos arquivos de zona, Forwarders (encaminhamento de requisição DNS para outro servidor, geralmente um slave da rede) e ativá-lo ou não para endereços IPv6, conforme podemos visualizar na figura abaixo.:

```
server:/etc/bind# cat named.conf.options
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;
    // };

    auth-nxdomain no;          # conform to RFC1035
    listen-on-v6 { any; };
};
```

## 2.5 Arquivos de Zona

As configurações de zonas direta/reversa no *DNS* tem como objetivo tratar a resolução de endereço IP para nome (Zona Reversa) e nome para endereço IP (Zona Direta).

Dentro do diretório `/etc/bind` existem dois arquivos modelos para a configuração das zonas, sendo o `db.local` (Zona Direta) e o `db.127` (Zona Reversa), porém não

é recomendado que utilize-os. De acordo com a documentação oficial do *Debian*, é recomendado que os arquivos sejam criados dentro do diretório **/var/cache/bind**. Sendo assim, você pode realizar uma cópia dos arquivos modelos e editá-los, ou simplesmente criar seus próprios arquivos.

### 2.5.1 Configurando Zona Reversa

Para configurar a zona reversa, siga os passos a seguir:

Acesse o arquivo de configuração criado dentro de **/var/cache/bind**. Lembrando que este arquivo pode possuir qualquer nome. Caso tenha realizado uma cópia do arquivo modelo (**db.127**), ao acessá-lo, será exibido o seguinte conteúdo.:

```
;$ORIGIN localhost.
; BIND reverse data file for local loopback interface
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        1          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
@         IN      NS       localhost.
1.0.0    IN      PTR      localhost.
```

Do contrário, caso tenha criado seu próprio arquivo, deverá acrescentar todos os registros e informações conforme apresentado posteriormente.

Neste arquivo, devemos definir qual será as opções do registro SOA, o servidor autorizado por responder as requisições desta zona, o FQDN da máquina e quais os registros do tipo PTR que serão utilizados.

Na primeira linha de configuração, devemos configurar o registro **SOA**, que é o registro responsável por apresentar informações sobre o domínio, como versão do arquivo de zona, e intervalo de tempo que afetam a renovação ou expiração do



arquivo de zona, bem como o cache DNS (lado do cliente). O primeiro item a ser adicionado, é o sinal de @, que representa o domínio.

Em seguida, utilização a opção **IN** para indicar qual será o tipo de registro utilizado, neste caso o registro **SOA**. Dando continuidade, digite o **FQDN** (hostname + sufixo DNS) de seu servidor, seguido de um ponto final (.), e em seguida repita novamente o **FQDN**, porém iniciando-se com o nome do administrador responsável pela zona, finalizando-o também com um ponto final (.). Por último, abra um parêntese, que será fechado logo adiante. Depois da alteração, a primeira linha deverá ficar conforme o exemplo abaixo.:

```
@      IN      SOA      ns1.cnetworking.local.  admin.ns1.cnetworking.local.  
(
```

```
@      IN      SOA      ns1.certified.local.    root.ns1.certified.local.  (
```

Em seguida, devemos definir qual a versão do arquivo de zona, e intervalo de tempo que afetam a renovação ou expiração do arquivo de zona, bem como o cache DNS (lado do cliente), como apresentado no modelo abaixo. Lembrando que com exceção do número do serial, todos os outros itens são definidos baseando-se em segundos.

```
2014112501 ;Serial  
604800     ;Refresh  
86400     ;Retry  
2419200   ;Expire  
604800 )   ;TTL
```

**Nota.:**

- No número de serial, para facilitar a identificação do arquivo de zona, sobre em qual versão do arquivo o mesmo se encontra, recomenda-se utilizar-se da data (ano, mês, dia) seguido do número da revisão/modificação.

Por último e não menos importante, devemos inserir os registros desta zona, que por se tratar de uma zona reversa, é basicamente “composto” por dois tipo, sendo

o **NS**, que defini qual(is) o(s) servidor(es) de nome responsável por responder as requisições solicitadas pelos clientes e o registro **PTR**, que tem como finalidade, realizar a conversão de endereços IPs para nomes.

Os registros do tipo **NS**, são formados pelo sinal de @, para identificar o domínio, a opção **IN** para especificar o registro utilizado, neste caso o **NS** e por último o endereço **IP** do servidor responsável por responder as requisições. Ex.:

```
@      IN      NS      192.168.1.1
```

Os registros do tipo **PTR** são formados pelo endereço final de um Host, que é definido de acordo com o endereço de rede utilizado e especificado dentro do arquivo **named.conf.local** que será apresentado posteriormente, seguido da opção **IN**, para indicar o registro **PTR** e por último o **FQDN** completo do Host, seguido por um ponto final. Ex.:

```
1      IN      PTR     ns1.certified.local.
```

**Obs.:** Para cada registro do tipo PTR, é criado um registro do tipo A, que será abordado no próximo tópico.

Após o preenchimento dos registros necessários para o funcionamento de sua zona, deverá ficar conforme o modelo abaixo.:

```
@      IN      NS      192.168.1.1
1      IN      PTR     ns1.cnetworking.local.
2      IN      PTR     srv02.cnetworking.local.
3      IN      PTR     host01.cnetworking.local.
```

Depois de todas as configurações, o arquivo de zona reversa deverá com a mesma estrutura abaixo, podendo variar na quantidade de registros e seus parâmetros:

```
@      IN      SOA      ns1.cnetworking.local.  admin.ns1.cnetworking.local.
(
      2014112501      ;Serial
      604800          ;Refresh
      86400           ;Retry
      2419200        ;Expire
      604800 )       ;TTL

@      IN      NS      192.168.1.1
1      IN      PTR     ns1.cnetworking.local.
2      IN      PTR     srv02.cnetworking.local.
3      IN      PTR     host01.cnetworking.local.
```

Feito as devidas configurações, salve o arquivo.

### 2.5.2 Configurando Zona Direta

Para configurar a zona direta, siga os mesmos passos da configuração da zona reversa, porém, utilizando o arquivo **db.local** como modelo, ou criando seu arquivo em branco.

Basicamente, as diferenças entre o arquivo de zona direta e reversa se resume-se em.:

- Os tipos de registros utilizados – Na zona direta, basicamente utilizamos os registros PTR, SOA e NS. Os registros apresentados acima são formados da seguinte forma.:

**hostname IN Tipo\_Registro Endereço\_IP**

Para a zona direta, dentre os diversos tipos de registros que podemos utilizar, os mais comuns são:

- **A** – Define o mapeamento de um host baseado em endereço IPv4, realizando a conversão do Hostname em endereço IP. Realiza o processo inverso do registro PTR. Ex.:

**ns1 IN A 192.168.1.1**  
**www IN A 200.1.2.3**

- **AAAA** – Idem ao registro A, porém baseado em um host de endereço IPv6. Ex.:

**ns1 IN A 2001:04A0:0:1::D**

- **MX** – Conhecido como Mail Exchange, tem a finalidade de definir quais serão os servidores de E-mail de seu domínio. Ex.:

**@ IN MX 10 mail.cnetworking.local**

No registro do tipo **MX** deve-se adicionar o número de “prioridade” do servidor de e-mail, para definir qual será o servidor principal, caso haja mais de um no domínio. Além disso, para cada registro **MX**, deve-se ter um registro do tipo **A** para identificar o host que será vinculado a ele.

- **CNAME** – Identificado como *Canonical Name*, tem objetivo de especificar um alias (apelido) para um outro registro do tipo A do mesmo domínio ou de outro domínio.

**ftp IN CNAME www.cnetworking.local**

- O registro **NS** é vinculado ao FQDN da máquina, juntamente com um ponto (.) no final e não ao endereço IP conforme apresentado na zona reversa.

No final de todas as configurações, o arquivo deverá ficar conforme o exemplo abaixo:

```
@      IN      SOA      ns1.cnetworking.local.  admin.ns1.cnetworking.loc
(
                                2014112501      ;Serial
                                604800      ;Refresh
                                86400      ;Retry
                                2419200     ;Expire
                                604800     )      ;TTL

@      IN      NS      ns1.cnetworking.local.
@      IN      NS      ns2.cnetworking.local.
@      IN      MX      10      mail.cnetworking.local.

ns1    IN      A      192.168.1.1
ns2    IN      A      192.168.1.5
mail   IN      A      192.168.1.10
host01 IN      A      192.168.1.2
srv01  IN      A      192.168.1.3
www    IN      A      192.168.1.1
ftp    IN      CNAME   www.cnetworking.local.
```

Feito as devidas configurações, salve o arquivo.

### 3 Inicializando o serviço

Após realizar todas as configurações listadas acima, basta reinicializar o serviço. Para isso, execute o comando: **"/etc/init.d/bind9 restart"** ou **"service bind9 restart"**. Se for emitida a mensagem abaixo, significa que o serviço foi reiniciado corretamente.

```
Stopping domain name service...: bind9.
Starting domain name service...: bind9.
```

**Dica:** Para iniciar, parar ou exibir o status do *DNS* no *Debian*, execute os seguintes comandos:

```
/etc/init.d/bind9 start ou service bind9 start (para iniciar o serviço)
/etc/init.d/bind9 stop ou service bind9 stop(para parar o serviço)
/etc/init.d/bind9 status ou service bind9 status (para verificar o status do
serviço)
```

#### 4 Configuração do Cliente *DNS* (resolver)

A configuração do cliente *DNS* é realizada através do arquivo de texto “**resolv.conf**”, localizado no diretório */etc*. Para realizar a configuração, siga os passos abaixo:

- Acesse o arquivo;
- Após acessar o arquivo, altere suas configurações conforme o exemplo abaixo:

```
nameserver 192.168.1.1
search cnetworking.local
```

**nameserver:** Indica o IP do servidor *DNS*. Caso exista mais de um servidor *DNS*, deverá ser adicionada uma linha para cada um deles;

**search:** Define o sufixo *DNS* referente ao domínio que consultará.

Feito as alterações, salve o arquivo.

#### 5 Realizando testes

Para realizar os testes de resoluções de nomes, utilizaremos a ferramenta **nslookup**.

**Exemplos:**

- **Identificando servidor *DNS* padrão:**

```
root@ns1:/# nslookup
> server
Default server: 192.168.1.1
Address: 192.168.1.1#53
```

- Consulta reversa:

```
root@ns1:/# nslookup 192.168.1.1
Server:      192.168.1.1
Address:     192.168.1.1#53

1.1.168.192.in-addr.arpa      name = ns1.cnetworking.local.1.168.192.in-addr.arpa.
```

- Consulta direta:

```
root@ns1:/# nslookup ns1
Server:      192.168.1.1
Address:     192.168.1.1#53

Name:   ns1.cnetworking.local
Address: 192.168.1.1

root@ns1:/# nslookup mail
Server:      192.168.1.1
Address:     192.168.1.1#53

Name:   mail.cnetworking.local
Address: 192.168.1.10
```

Se for obtida uma resposta para as pesquisas executadas, significa que o serviço *DNS* esta funcionando corretamente.

**Nota:** Caso seja realizada uma pesquisa de um host na rede local e o servidor *DNS* não consiga resolver a tradução de nome/IP, verifique nos arquivos de zonas se existe realmente o registro apontando para o host.

## 6 LOGs de Erros

Caso ocorra algum erro durante ou depois da configuração do servidor *DNS*, os mesmos poderão ser verificados através do arquivo **syslog** localizado no diretório **/var/log/syslog**. Segue abaixo um exemplo de como são dispostos os logs dentro do arquivo.

```
Nov 6 19:26:15 certified named[1678]: adjusted limit on open files from 1024 to
1048576
Nov 6 19:26:15 certified named[1678]: found 1 CPU, using 1 worker thread
Nov 6 19:26:15 certified named[1678]: using up to 4096 sockets
Nov 6 19:26:16 certified named[1678]: loading configuration from '/etc/bind/nam
ed.conf'
Nov 6 19:26:16 certified named[1678]: reading built-in trusted keys from file '
/etc/bind/bind.keys'
Nov 6 19:26:16 certified named[1678]: using default UDP/IPv4 port range: [1024,
65535]
Nov 6 19:26:16 certified named[1678]: using default UDP/IPv6 port range: [1024,
65535]
Nov 6 19:26:16 certified named[1678]: listening on IPv6 interfaces, port 53
Nov 6 19:26:16 certified named[1678]: listening on IPv4 interface lo, 127.0.0.1
#53
Nov 6 19:26:16 certified named[1678]: listening on IPv4 interface eth0, 192.168
.1.254#53
Nov 6 19:26:16 certified named[1678]: generating session key for dynamic DNS
Nov 6 19:26:16 certified named[1678]: set up managed keys zone for view _defaul
t, file 'managed-keys.bind'
Nov 6 19:26:16 certified named[1678]: automatic empty zone: 254.169.IN-ADDR.ARP
A
Nov 6 19:26:16 certified named[1678]: automatic empty zone: 2.0.192.IN-ADDR.ARP
A
--More--_
```

**Nota:** As configurações listadas acima são referentes às configurações básicas de resolução de nomes de um servidor *DNS*. Este serviço possui muitas outras configurações que podem ser abrangidas de acordo a solução desejada.

**DÚVIDAS? ENTRE EM CONTATO CONOSCO:**

[contato@cnetworking.com.br](mailto:contato@cnetworking.com.br)