### 2.5. O BIND

Será utilizado o BIND (*Berkeley Internet Name Domain*), o servidor mais amplamente usado para o serviço de DNS no mundo que implementa o protocolo DNS para Unix, Linux, Mac Os e Windows. A versão utilizada será a 9, a mais nova no momento de escrita deste material.

O Nome do processo responsável pelo serviço de DNS no Debian é named.

## 3. Instalando e configurando DNS Primário

Serão abordados aqui os passos para instalação e configuração do Bind como servidor Primário (máster) em um Servidor Linux Debian.

Para instalar o Bind, se este não estiver instalado:

```
apt-get install bind9
```

Criar a zona de DNS convencional Primário. Entre no arquivo de configuração da zona de DNS com o comando:

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

Inclua ao final do arquivo as seguintes linhas:

```
// DNS
zone "segfatecou.edu.br"  IN  {
type master;
file "/etc/bind/domains/segfatecou/db.segfatecou.edu.br";
};
```

Criar os diretórios onde os arquivos de configuração do domínio serão criados.

```
mkdir -p /etc/bind/domains/segfatecou
```

Dentro destes diretórios, criar os seguintes arquivos:

Para resolução de nome:

```
vi /etc/bind/domains/segfatecou/db.segfatecou.edu.br
```

Depois insira no arquivo as linhas abaixo.

**Dica importante:** Ao entrar no novo arquivo (em branco), crie apenas a primeira linha, com o $TTL 3600. Após isso, saia salvando o arquivo e volte a ele. Se você digitou o caminho corretamente, o vi irá salvar corretamente. Se houver algum erro, saia sem salvar e verifique o caminho do nome do arquivo e se as pastas foram criadas corretamente. Se o vi salvar o arquivo, ao voltar você notará que os caracteres agora estarão coloridos, melhorando a visualização de algum erro de sintaxe. Note também que a tabulação e indentação devem ser mantidas.

```
$TTL 3600; tempo de vida das respostas fornecidas pelo DNS
(cache)
@ IN SOA ns1.segfatecou.edu.br.  hostmaster.segfatecou.edu.br.
(
     2022042501; Serial para controle de atualizações entre
master e slave
     28800; tempo de atualizações entre master e slave
(refresh)
     7200; tempo de atualizações caso o refresh falhe
     604800; tempo de expiração do slave caso não contate o
master
     7200 );  tempo de vida das repostas negativas do servidor

     NS ns1.segfatecou.edu.br.
     NS ns2.segfatecou.edu.br.
     IN MX 10 smtp.segfatecou.edu.br.
     IN MX 20 smtp2.segfatecou.edu.br.

segfatecou.edu.br.  A         192.168.0.1

ns1                 A         192.168.0.1
ns2                 A         192.168.0.254

www                 A         192.168.0.1
smtp                A         192.168.0.3
smtp2               A         192.168.0.4
pop3                A         192.168.0.5
```

```
blog                    A          192.168.0.6
ftp                     A          192.168.0.1
owncloud                A          192.168.0.1
webmail                 CNAME      pop3
```

Obs: Estes números IP são fictícios, usados apenas para exemplificar.

Vamos entender as regras utilizadas, lembrando que os textos após o ; (ponto e vírgula) indicam comentários e não são lidos pelo Bind.

$TTL - (*Time to Live*) Esta opção diz ao Bind por quanto tempo ele deve manter em cache as informações de certo domínio. Lembrando que só são consultados os arquivos "zone" caso a informação procurada não se encontre no cache. Encontra-se em segundos, no nosso caso o TTL é de 1 hora (3600 segundos).

@ IN SOA ns1.segfatecou.edu.br. hostmaster.segfatecou.edu.br. (

A "@" na segunda linha indica a origem do domínio e, ao mesmo tempo, o início da configuração. Ela é sempre usada, assim como num endereço de e-mail.

O "IN" é abreviação de "Internet" e o "SOA" de "*Start of autority*". Em seguida vem o nome do servidor (que você checa usando o comando "hostname"), seguido do e-mail de contato do administrador. Note que, no caso do e-mail, temos a conta separada do domínio por um ponto, e não por uma @. O mais comum é criar uma conta chamada "hostmaster", mas isso não é uma regra. Você poderia usar "fulano.meudomonio.com.br", por exemplo.

Note também que existe um ponto depois do "ns1.segfatecou.edu.br" e do "hostmaster.fatecou.edu.br", que faz parte da configuração. O ponto se refere ao domínio raiz, de responsabilidade dos root servers. No exemplo, nosso servidor é o responsável pelo domínio "segfatecou", que faz parte do domínio ".edu.br", que por sua vez faz parte do domínio raiz. Lembre-se que os domínios são lidos da direita para a esquerda, de forma que, ao resolver o domínio, o cliente leria: raiz . br . edu . segfatecou.

A linha diz algo como "Na Internet, o servidor "segfatecou" responde pelo domínio segfatecou.edu.br o e-mail do responsável pelo domínio é "hostmaster@segfatecou.edu.br".

A primeira linha termina com um parêntese, que indica o início da configuração do domínio. Temos então:

2021031701; Serial

O "2021031701" é o número serial dos dados de configuração da zona. Esse número permite que o servidor DNS secundário mantenha-se sincronizado com o principal, detectando alterações na configuração. Este número em geral é composto da data da última alteração (como em: 2021/03/17), composta por ano, mês e dia, e um número de dois dígitos que será incrementado. Sempre que editar a configuração, ou sempre que configurar um servidor DNS a partir de um *template* qualquer, lembre-se de atualizar a data e/ou mudar os dois dígitos. É responsabilidade do administrador daquela zona de DNS alterar e/ou incrementar o número Serial a cada alteração.

As quatro linhas seguintes orientam o servidor DNS secundário (caso você tenha um). O primeiro campo indica o tempo que o servidor aguarda entre as atualizações (28800 segundos, ou 8 horas). Caso ele perceba que o servidor principal está fora do ar, ele tenta fazer uma transferência de zona, ou seja, tenta assumir a responsabilidade sob o domínio. Não esqueça que o serial nunca é incrementado automaticamente, isso é trabalho do administrador. Caso a transferência falhe e o servidor principal continue fora do ar, ele aguarda o tempo especificado no segundo campo (2 horas) e tenta novamente.

O terceiro campo indica o tempo máximo que ele pode responder pelo domínio, antes que as informações expirem (7 dias, tempo mais do que suficiente para você arrumar o servidor principal). O último campo instrui os servidores DNS clientes a armazenarem por duas horas informações sobre recursos não existentes do domínio em questão.

Estes valores são padrão, por isso não existem muitos motivos para alterá-los. A transferência do domínio para o DNS secundário é sempre uma operação demorada, por causa do cache feito pelos diversos servidores DNS espalhados pelo mundo: demora de um a dois dias até que todos atualizem suas tabelas de endereços. A

principal prioridade deve ser evitar que o servidor principal fique indisponível em primeiro lugar.

Opções utilizadas:

MX - Mail Exchange: Esta entrada permite que o named identifique o seu servidor de correio eletrônico. O número antes do nome do servidor é referente ao índice de prioridade, ou seja, a mensagem será direcionada sempre para o servidor com menor índice e caso ele não responda vai para o seguinte e assim por diante.

CNAME - Esta entrada diz ao named que o alias - no caso o webmail - é um apelido para um dado servidor ou domínio. Em nosso arquivo é o "pop3". Ou seja, o apelido "webmail" irá apontar para o mesmo local do "pop3" que é o host 192.168.0.5.

A - Address: com esta opção especificamos um endereço válido na área de atuação do servidor, podendo este ser um IP ou um domínio. Contudo, caso seja utilizado um domínio é obrigatório colocar um ponto final após o nome.

## 4. Ajustando e checando a configuração

É possível fazer a checagem da sintaxe dos arquivos de configuração com os comandos **`named-checkconf`** e **`named-checkzone.`**

Execute o comando a seguir para verificar a sintaxe do arquivo named.conf.local:

```
named-checkconf
```

Se seus arquivos de configuração não tiverem erros de sintaxe, você retornará ao shell e não verá nenhuma mensagem de erro. Se houver problemas com seus arquivos de configuração, reveja a mensagem de erro e a seção “Instalando e configurando DNS Primário”, e então tente o **`named-checkconf`** novamente.

O comando **named-checkzone** pode ser usado para verificar a correção dos arquivos da sua zona. Seu primeiro argumento especifica um nome de zona e o segundo especifica o arquivo da zona correspondente, sendo que ambos estão definidos em named.conf.local.

Por exemplo, para verificar a configuração da zona de DNS “segfatecou.edu.br”, que usa o arquivo de configuração db.segfatecou.edu.br que fica na pasta /etc/bind/domains/segfatecou/, execute o seguinte comando:

```
named-checkzone segfatecou.edu.br /etc/bind/domains/segfatecou/db.segfatecou.edu.br
```

E para verificar a configuração da zona reversa (que ainda será configurada na seção “7 DNS Reverso”) cujo nome será “0.168.192.in-addr.arpa”, execute o seguinte comando:

```
named-checkzone 0.168.192.in-addr.arpa /etc/bind/domains/segfatecou/db.0.168.192
```

Quando todos os arquivos de configuração e zona estiverem livres de erros, você está pronto para reiniciar o serviço BIND.

## 4.1 Ajustando as configurações do bind

Antes de reiniciar o serviço e fazermos a checagem do log, vamos alterar um arquivo de configuração, para que não fiquem aparecendo mensagens indesejáveis no log.

Abra o arquivo */*etc/default/bind9 (que dependendo da versão do Debian pode ser */*etc/default/named) com o vi como abaixo:

```
vi /etc/default/bind9  (ou vi /etc/default/named)
```

Altere a opção OPTIONS para ficar como está abaixo:

```
# startup options for the server
OPTIONS="-4 -u bind"
```

Esta mudança é necessária pois nessa nossa configuração não é usado IPv6, portanto a opção -4 faz o bind resolver endereços apenas para IPv4.

Outra alteração necessária para os nossos testes é desabilitar a checagem do DNSSec, a extensão de segurança para o DNS.

Para isso acesse o arquivo /etc/bind/named.conf.options com o comando:

```
vi /etc/bind/named.conf.options
```

Procure pela linha que contêm dnssec-validation auto; e altere para

```
dnssec-validation no;
```

Salve o arquivo e vamos para o próximo passo

## 5. Reiniciando o serviço e verificando o log

Agora vamos reiniciar o serviço e verificar o log. Para reiniciar o servidor bind deve-se executar o comando:

```
/etc/init.d/bind9 restart
```

Caso a versão do Debian não tenha o *daemon* do bind9 no diretório /etc/init.d, execute os comandos a seguir:

```
systemctl restart bind9
systemctl status bind9
```

Depois vamos verificar se o serviço foi iniciado corretamente rodando o comando tail no arquivo syslog, onde deve-se verificar as seguintes linhas:

```
tail /var/log/syslog
```

```
Mar 17 15:49:06 debian-asor named[3722]: command channel listening on
127.0.0.1#953
Mar 17 15:49:06 debian-asor named[3722]: command channel listening on ::1#953
Mar 17 15:49:06 debian-asor named[3722]: zone 0.in-addr.arpa/IN: loaded serial 1
Mar 17 15:49:06 debian-asor named[3722]: zone 127.in-addr.arpa/IN: loaded serial 1
Mar 17 15:49:06 debian-asor named[3722]: zone 255.in-addr.arpa/IN: loaded serial 1
Mar 17 15:49:06 debian-asor named[3722]: zone segfatecou.edu.br/IN: loaded
serial 2021031701
Mar 17 15:49:06 debian-asor named[3722]: zone localhost/IN: loaded serial 2
Mar 17 15:49:06 debian-asor named[3722]: managed-keys-zone ./IN: loaded serial 7
Mar 17 15:49:06 debian-asor named[3722]: running
Mar 17 15:49:06 debian-asor named[3722]: zone segfatecou.edu.br/IN: sending
notifies (serial 2021031701)
```

Note que há duas linhas em negrito. Elas identificam que a nossa zona da DNS segfatecou.edu.br, configurada com o serial 2021031701 foi carregada com sucesso (**loaded serial 2021031701**). Isso significa que a configuração foi feita corretamente e não houve erros.

## 6. Simulando erros na configuração

Vamos agora simular um erro de configuração no arquivo da zona de DNS (arquivo db.segfatecou.edu.br). Após o restart do bind, verifique o que aparece no arquivo syslog:

**tail /var/log/syslog**

```
Mar 17 16:08:17 debian-asor named[3992]: command channel listening on ::1#953
Mar 17 16:08:17 debian-asor named[3992]: zone 0.in-addr.arpa/IN: loaded serial 1
Mar 17 16:08:17 debian-asor named[3992]: zone 127.in-addr.arpa/IN: loaded serial 1
Mar 17 16:08:17 debian-asor named[3992]: zone 255.in-addr.arpa/IN: loaded serial 1
Mar 17 16:08:17 debian-asor named[3992]: dns_rdata_fromtext: /etc/bind/domains/s
egfatecou/db.segfatecou.edu.br:4: near 'tempo': syntax error
Mar 17 16:08:17 debian-asor named[3992]: zone segfatecou.edu.br/IN: loading from
master file /etc/bind/domains/segfatecou/db.segfatecou.edu.br failed: syntax
error
Mar 17 16:08:17 debian-asor named[3992]: zone segfatecou.edu.br/IN: not loaded
due to errors.
Mar 17 16:08:17 debian-asor named[3992]: zone localhost/IN: loaded serial 2
Mar 17 16:08:17 debian-asor named[3992]: managed-keys-zone ./IN: loaded serial 8
Mar 17 16:08:17 debian-asor named[3992]: running
```

Veja que há três linhas em negrito. Na primeira vê-se: **/etc/bind/domains/segfatecou/db.segfatecou.edu.br:4: near 'refresh,': syntax error**

O número 4 seguido do símbolo "**:**" (dois pontos) logo após o nome do arquivo db.segfatecou.edu.br indica que há uma grande chance do erro estar próximo à linha 4 (**db.segfatecou.edu.br:4**), próximo à palavra *refresh* (**near 'refresh'**). Uma verificada no arquivo e percebe-se que ao final da linha 4 faltava o ";"

**28800; tempo de atualizações entre *master* e *slave (refresh)***

A segunda e a terceira linhas em negrito indicam que o arquivo de configuração não foi carregado devido a erros no arquivo: **failed: syntax error e not loaded due to errors.**

Vejamos outro exemplo:

**tail /var/log/syslog**

```
Mar 17 15:52:51 debian-asor named[3790]: command channel listening on ::1#953
Mar 17 15:52:51 debian-asor named[3790]: zone 0.in-addr.arpa/IN: loaded serial 1
Mar 17 15:52:51 debian-asor named[3790]: zone 127.in-addr.arpa/IN: loaded serial
1
Mar 17 15:52:51 debian-asor named[3790]: zone 255.in-addr.arpa/IN: loaded serial
1
Mar 17 15:52:51 debian-asor named[3790]: dns_rdata_fromtext:
/etc/bind/domains/segf atecou/db.segfatecou.edu.br:7: near eol: unexpected end
of input
Mar 17 15:52:51 debian-asor named[3790]: zone segfatecou.edu.br/IN: loading from
master file /etc/bind/domains/segfatecou/db.segfatecou.edu.br failed: unexpected
end of input
Mar 17 15:52:51 debian-asor named[3790]: zone segfatecou.edu.br/IN: not loaded
due to errors.
Mar 17 15:52:51 debian-asor named[3790]: zone localhost/IN: loaded serial 2
Mar 17 15:52:51 debian-asor named[3790]: managed-keys-zone ./IN: loaded serial 7
Mar 17 15:52:51 debian-asor named[3790]: running
```

Repare novamente nas duas linhas em negrito. A primeira indica:

**/etc/bind/domains/segfatecou/db.segfatecou.edu.br:7: near eol: unexpected end of input**

Esta primeira linha em negrito indica que há um erro na linha 7 do arquivo db.segfatecou.edu.br, indicando um "final inesperado de entrada". A segunda linha em

negrito indica que o arquivo de configuração não foi carregado devido a erros no arquivo. Neste caso específico, o erro era a falta de um espaço na segunda linha:

```
$TTL 3600
@     IN SOA
ns1.segfatecou.edu.br.hostmaster.segfatecou.edu.br. (
                2021031701; Serial
                28800; refresh, seconds
                7200; retry, seconds
                604800; expire, seconds
                86400 ) ;  negative cache TTL, seconds
```

Como essa segunda linha é o início do bloco compreendido entre os parêntesis “( )” há essa confusão do bind indicando que o erro está na linha número 7. Isso mostra que o bind não é muito preciso ao informar os erros, mas mesmo assim é possível achar um erro facilmente através do log.

Agora mais um exemplo:

```
tail /var/log/syslog
```

```
Sep 24 09:39:26 debian-asor named[3921]: command channel listening on ::1#953
Sep 24 09:39:26 debian-asor named[3921]: zone 0.in-addr.arpa/IN: loaded serial 1
Sep 24 09:39:26 debian-asor named[3921]: zone 127.in-addr.arpa/IN: loaded serial 1
Sep 24 09:39:26 debian-asor named[3921]: zone 255.in-addr.arpa/IN: loaded serial 1
Sep 24 09:39:26 debian-asor named[3921]: zone segfatecou.edu.br/IN: loading from
master file etc/bind/domains/segfatecou/db.segfatecou.edu.br failed: file not
found
Sep 24 09:39:26 debian-asor named[3921]: zone segfatecou.edu.br/IN: not loaded
due to errors.
Sep 24 09:39:26 debian-asor named[3921]: zone localhost/IN: loaded serial 2
Sep 24 09:39:26 debian-asor named[3921]: managed-keys-zone ./IN: loaded serial
15
Sep 24 09:39:26 debian-asor named[3921]: running
```

Veja nas duas linhas em negrito que a zona de DNS não foi carregada. A linha de cima contém a seguinte informação:

```
file etc/bind/domains/segfatecou/db.segfatecou.edu.br failed:
file not found
```

O que indica que o arquivo db.segfatecou.edu.br não foi encontrado no endereço informado no arquivo /etc/bind/named.conf.local. Veja como estava esse arquivo:

```
// DNS
zone "segfatecou.edu.br" IN {
type master;
file "etc/bind/domains/segfatecou/db.segfatecou.edu.br";
```

```
};
```

É possível ver que faltou a / antes de etc, o correto seria: /etc/bind/domains/segfatecou/db.segfatecou.edu.br

## 7. DNS Reverso

Para resolução reversa de nomes vamos editar novamente o arquivo named.conf.local com o comando:

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

E então vamos acrescentar ao final do arquivo as seguintes linhas:

```
// DNS Reverso
zone "0.168.192.in-addr.arpa"  IN  {
type master;
file "/etc/bind/domains/segfatecou/db.0.168.192";
 };
```

Criar o arquivo da zona reversa:

```
vi /etc/bind/domains/segfatecou/db.0.168.192
```

colocar o seguinte conteúdo:

```
$TTL 3600
@ IN SOA ns1.segfatecou.edu.br. hostmaster.segfatecou.edu.br. (
          2022042701; Serial
          28800; refresh, seconds
          7200; retry, seconds
          604800; expire, seconds
          86400 ) ;  negative cache TTL, seconds

          NS ns1.segfatecou.edu.br.
          NS ns2.segfatecou.edu.br.

1         PTR     ns1.segfatecou.edu.br.
254       PTR     ns2.segfatecou.edu.br.
3         PTR     smtp.segfatecou.edu.br.
5         PTR     pop3.segfatecou.edu.br.
6         PTR     blog.segfatecou.edu.br.
```

Onde PTR aponta o último octeto do endereço IP para o nome do reverso.

# 8. Finalizando e testando o DNS

Após a criação da zona e configuração dos arquivos db dos domínios configurados neste servidor, **devemos informar à própria máquina que ela mesmo é responsável por resolver o DNS**. Para isso faça:

```
vi /etc/resolv.conf
```

colocar **apenas** o seguinte conteúdo abaixo:

```
nameserver 127.0.0.1
```

**Nota**: Se houver outras linhas no arquivo acima, **elas devem ser removidas** para não atrapalharem os testes da nossa máquina virtual.

Com estas configurações é possível utilizarmos este servidor DNS para responder perguntas sobre o domínio configurado, no nosso exemplo o domínio é o segfatecou.edu.br.

Para testar o funcionamento correto do servidor DNS podemos utilizar três comandos: **nslookup, dig e host**.

O comando nslookup é o mais comum, sua sintaxe com seu resultado são:

```
nslookup www.segfatecou.edu.br


Server:         127.0.0.1
Address:        127.0.0.1#53

Name:     www.segfatecou.edu.br
Address:  192.168.0.1
```

O comando host é mais atual e mais simples de ser trabalhado. Ele encontra-se instalado na VM mas para instalá-lo bastaria executar:

**apt-get install host**

Para utilizá-lo basta digitar:

**host -a www.segfatecou.edu.br**

O resultado deve ser a apresentação detalhada das informações do domínio pesquisado, como se segue:

```
host -a www.segfatecou.edu.br

Trying "www.segfatecou.edu.br"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 31923
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL:
2

;; QUESTION SECTION:
;www.segfatecou.edu.br.          IN    ANY

;; ANSWER SECTION:
www.segfatecou.edu.br.      345600      IN    A     192.168.0.1

;; AUTHORITY SECTION:
segfatecou.edu.br.    345600      IN    NS    ns1.segfatecou.edu.br.
segfatecou.edu.br.    345600      IN    NS    ns2.segfatecou.edu.br.

;; ADDITIONAL SECTION:
ns1.segfatecou.edu.br.      345600      IN    A     192.168.0.1
ns2.segfatecou.edu.br.      345600      IN    A     192.168.0.254

Received 123 bytes from 127.0.0.1#53 in 3 ms
```

No caso de a consulta ser feita ao domínio completo, a resposta seria a seguinte:

```
host -a segfatecou.edu.br

Trying "segfatecou.edu.br"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 21455
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 6, AUTHORITY: 0, ADDITIONAL:
4

;; QUESTION SECTION:
;segfatecou.edu.br.          IN    ANY

;; ANSWER SECTION:
```

```
segfatecou.edu.br.    345600     IN    SOA   ns1.segfatecou.edu.br.
hostmaster.segfatecou.edu.br. 2016032901 28800 7200 604800 86400
segfatecou.edu.br.    345600     IN    NS    ns1.segfatecou.edu.br.
segfatecou.edu.br.    345600     IN    NS    ns2.segfatecou.edu.br.
segfatecou.edu.br.    345600     IN    MX    20
smtp2.segfatecou.edu.br.
segfatecou.edu.br.    345600     IN    MX    10 smtp.segfatecou.edu.br.
segfatecou.edu.br.    345600     IN    A     192.168.0.1

;; ADDITIONAL SECTION:
ns1.segfatecou.edu.br.      345600     IN    A     192.168.0.1
ns2.segfatecou.edu.br.      345600     IN    A     192.168.0.254
smtp.segfatecou.edu.br.     345600     IN    A     192.168.0.3
smtp2.segfatecou.edu.br. 345600  IN    A     192.168.0.4
```

Para consulta reversa usa-se por exemplo o host 192.168.0.1, o resultado deve ser a apresentação das informações de reverso do IP pesquisado, como segue:

```
host 192.168.0.1
1.0.168.192.in-addr.arpa domain name pointer ns1.segfatecou.edu.br.
```

ou

```
host 192.168.0.3
3.0.168.192.in-addr.arpa domain name pointer smtp.segfatecou.edu.br.
```

Para o comando dig, usa-se

```
dig ns segfatecou.edu.br
```

Onde o resultado deve ser a apresentação das informações do domínio pesquisado, como segue:

## 9. Conclusão

O serviço de DNS é essencial para a Internet, possibilitando que não precisemos decorar endereços IP, permitindo que usemos nomes de domínios.

Para a configuração do serviço de DNS em nossa aula foi usado o BIND, servidor amplamente usado no mundo. Foram configurados serviços de DNS Primário