INSTALAÇÃO E CONFIGURAÇÃO DO SERVIDOR DNS (Bind9)

Administração de Sistemas Operacionais de Rede
FATEC OURINHOS
Profº Me. Paulo R. Galego H. Jr.
Última atualização: 04/05/2022

Sumário

Introdução

AVISO IMPORTANTE

Este material estará em constante evolução para sanar possíveis erros que possa conter. O autor não se responsabiliza por danos ou problemas que as configurações aqui descritas possam ocasionar em ambientes de produção. O autor ainda recomenda que todos os testes aqui realizados sejam feitos em ambiente de Máquinas Virtuais (VM), usando a última versão do software Oracle VirtualBox usando as VMs fornecidas pelo professor.

Esta apostila faz parte do material de apoio aos alunos do 3º ciclo do curso superior de Tecnologia em Segurança da Informação da Fatec Ourinhos, na matéria Administração de Sistemas Operacionais de Redes, e visa complementar todas as informações já vistas em sala de aula, incluindo os exercícios passados.

1. DNS

O DNS traduz nomes de máquinas e domínios para IP, informação utilizada para real comunicação entre as máquinas conectadas em rede.

Todo site ou serviço na Internet precisa de um endereço IP (seja ele IPv4 ou IPv6). Com este recurso, é possível localizar o servidor (ou o conjunto de servidores) que hospeda o site, e assim acessar as suas páginas. Na ocasião de escrita deste material, o IP do servidor web da Fatec era 201.55.32.12.

Pois bem. Tente decorar este número. Decorou? Parabéns! Agora, aguarde alguns minutos e tente se lembrar novamente deste endereço IP. Difícil, né? Agora, imagine ter que se lembrar dos endereços IP de todos os sites que você acessa diariamente, como Facebook, Twitter, e-mail, portais de notícias, etc. Pois é, praticamente impossível e nada prático, não é mesmo?

É basicamente por isso que utilizamos nomes de domínios para acessar os sites da Internet. Com isso, o usuário não precisa saber, por exemplo, o endereço IP da Fatec para acessá-lo, basta saber o seu domínio, no caso, www.fatecourinhos.edu.br. Trata-se de um esquema bastante prático, afinal, decorar nomes é muito mais fácil do que guardar sequências numéricas. Além disso, mesmo

que você não se lembre de um nome com exatidão, poderá digitá-lo em um mecanismo de busca e este o ajudará a encontrá-lo.

A questão é que, apesar do uso de domínios, os sites ainda precisam dos endereços IP, afinal, os nomes foram criados para facilitar a compreensão humana, não a dos computadores. E cabe ao DNS o trabalho de relacionar um domínio aos endereços IP.

1.1 O Serviço de DNS

Os serviços de DNS (*Domain Name System* – Sistema de Nomes de Domínios) da Internet são, em poucas palavras, grandes bancos de dados espalhados em servidores localizados em várias partes mundo. Quando você digita um endereço em seu navegador, como www.fatecourinhos.edu.br, seu computador solicita aos servidores de DNS de seu provedor de Internet (ou outros que você tenha especificado) que encontre o endereço IP associado ao referido domínio. Caso estes servidores não tenham esta informação, eles se comunicam com outros que possam ter.

Ajuda neste trabalho o fato de os domínios serem organizados hierarquicamente. Primeiramente temos o servidor raiz (*root server*), que pode ser entendido como o principal serviço de DNS e é representado por um ponto no final do endereço, como mostra o seguinte exemplo:

www.fatecourinhos.edu.br.

Repare que se você digitar o endereço exatamente como está acima – com ponto no final – em seu navegador, o programa encontrará o site normalmente. No entanto, não é necessário incluir este ponto, já que os servidores envolvidos já sabem de sua existência.

A Internet conta (pelo menos até a data de publicação deste material) com treze servidores raiz, sendo que dez se localizam nos Estados Unidos, dois na Europa (Estocolmo e Amsterdam) e um na Ásia (Tóquio). É claro que cada um destes tem seus espelhos espalhados pelo mundo, como mostra a Figura 1, onde o número dentro do círculo representa a quantidade de espelhos dos *root servers* dentro daquela região o

país. Quando um falha, os demais conseguem manter o funcionamento da rede sem maiores complicações.

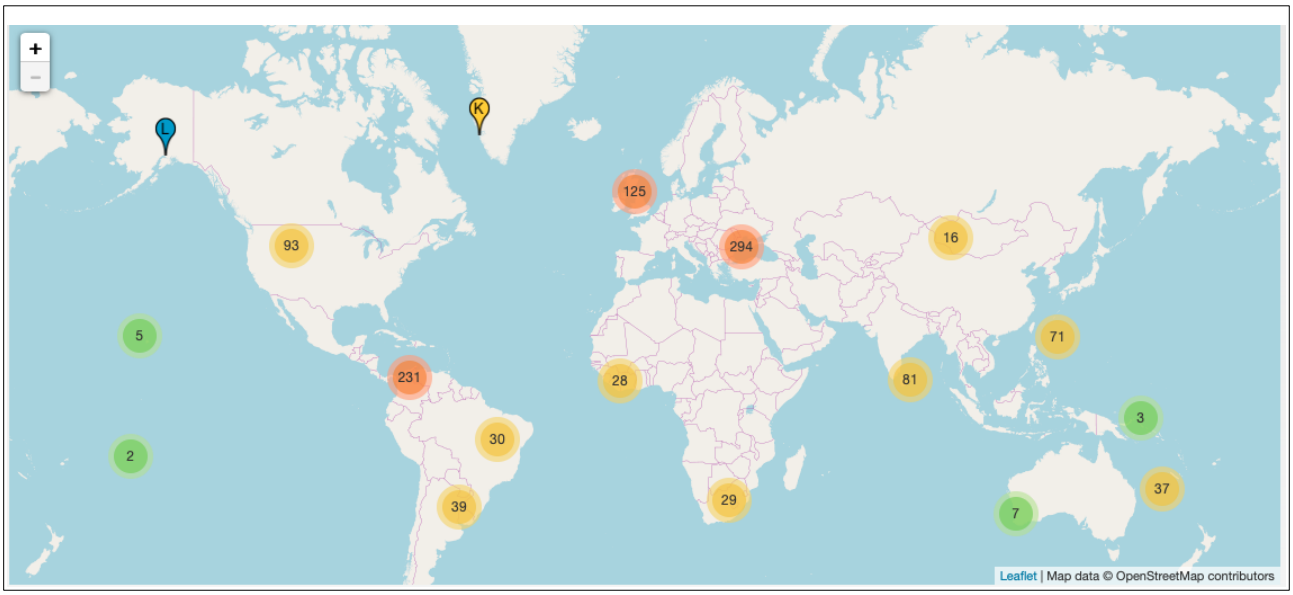

Figura 1- Quantidade de servidores raiz em cada região do mundo

O Brasil conta atualmente com 30 (trinta) espelhos, os quais a maioria concentra-se no estado de São Paulo, conforme ilustrado na Figura 2.

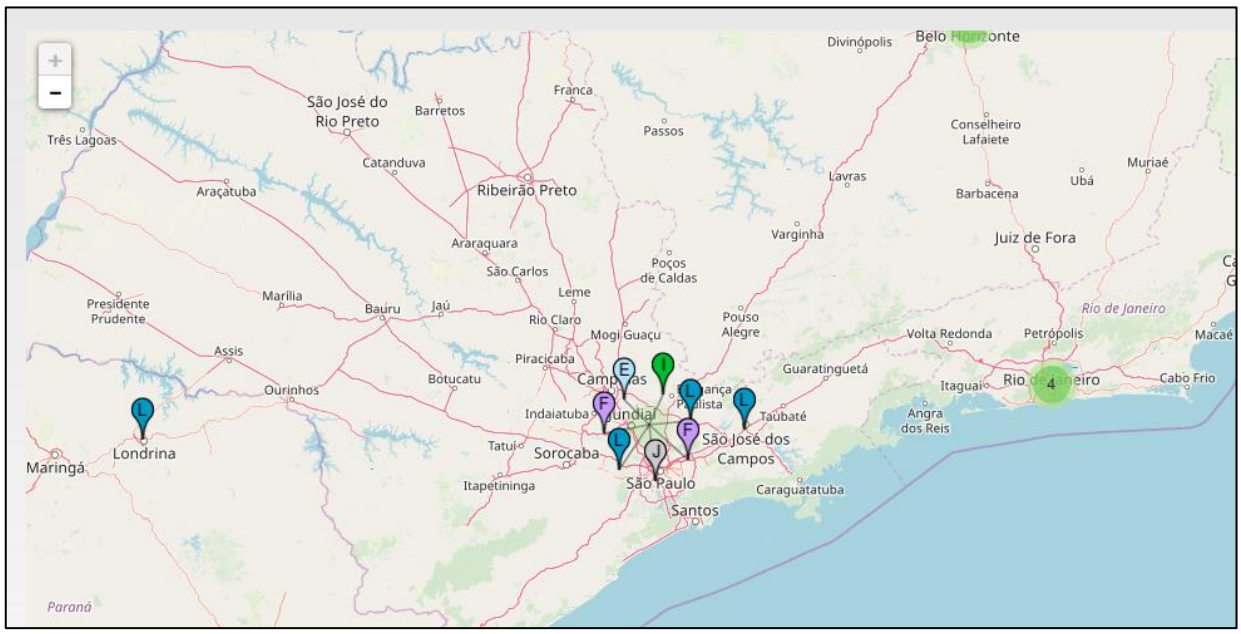

Figura 2 - Espelhos dos *root servers* no Brasil

Características do DNS:

- Sistema hierárquico distribuído
- Tradução de nomes para números IP
- Não existe um repositório único de informações
- Informação distribuída entre milhares de computadores
- Estrutura em árvore, semelhante à estrutura de diretórios de sistemas Unix.

A hierarquia é seguida com domínios que conhecemos bastante, como .com, .net, .org, .gov, .edu, .br, .me e vários outros. Estas são chamadas de gTLDs (Generic Top Level Domains - algo como Domínios Genéricos de Primeiro Nível).

Há também terminações orientadas a países, chamadas de ccTLDs (Country Code Top Level Domains - algo como Código de País para Domínios de Primeiro Nível). Por exemplo: .br para o Brasil, .jp para Japão, .fr para a França e assim por diante. Há combinações também, como .com.br e .edu.br.

Depois, aparecem os nomes que empresas ou instituições de ensino e pessoas podem registrar com estes domínios, como a palavra fatecourinhos em fatecourinhos.edu.br ou google em google.com.br.

Com a hierarquia, descobrir qual IP e, consequentemente, qual servidor está associado a um domínio – processo chamado de **resolução de nome –** fica mais fácil, já que este modo de funcionamento permite um esquema de trabalho distribuído, onde cada nível da hierarquia conta com serviços específicos de DNS.

Para entender melhor, veja este exemplo: suponha que você queira visitar o site www.uol.com.br. Para isso, o serviço de DNS do seu provedor (ou outro que você especificar) tentará descobrir se sabe como localizar o referido site. Caso negativo, primeiramente consultará o servidor raiz (*root server*). Este, por sua vez, indicará o servidor de DNS da terminação .br, que continuará o processo até chegar ao servidor que responde pelo domínio uol.com.br, que finalmente informará o IP associado, ou seja, em qual servidor está o site em questão.

Veja na Figura 3 o esquema de distribuição: servidores de DNS apontam para o próximo, até que o destino seja encontrado. No caso do servidor raiz, este possui meramente uma relação dos serviços de DNS responsáveis pelos domínios gTLD e ccTLD, sendo que estes se encarregam de dar sequência ao procedimento.

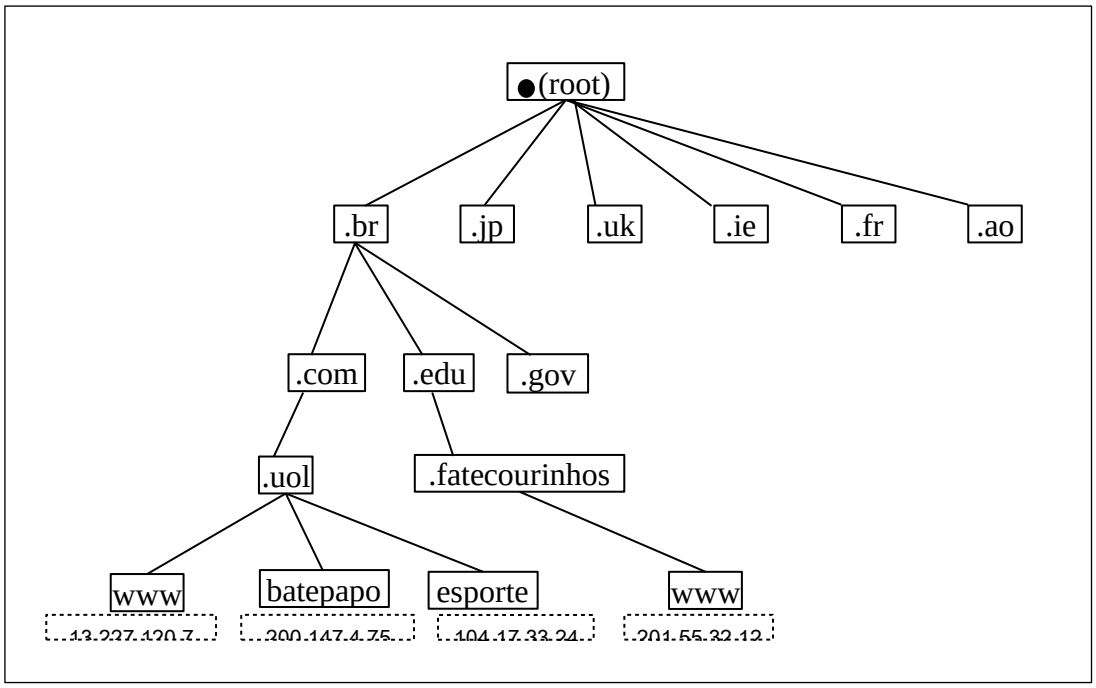

Figura 3 - Hierarquia do DNS

É importante frisar que a Figura 3 representa de forma didática a resolução de nomes para o domínio uol.com.br no que tange às terminações .com, .edu e .gov (gTLDs). Essa hierarquia característica em alguns países, incluindo o Brasil, é implementada localmente pelo órgão local que controla a designação de nomes de domínio, no caso do Brasil o CGI (Comitê Gestor de Internet), que será apresentado no próximo tópico. Também é importante salientar que os endereços IP ilustrados na figura podem mudar de acordo com as políticas implementados pelo provedor UOL.

1.2 Domínios

Nome que representa uma ou um conjunto de máquinas que seguem a mesma nomenclatura na sua identificação. Composto principalmente pela informação da localização (ex: br), tipo de serviço (ex: comercial**:** com, educacional**:** edu, governamental**:** gov) e o nome que, a princípio, representa a motivação daquele domínio (ex: fatecourinhos – Faculdade de Tecnologia de Ourinhos).

No Brasil o responsável pelo registro de nomes de domínio é o CGI (Comitê Gestor da Internet no Brasil – www.cgi.br), onde as suas decisões são implementadas pelo NIC.br (Núcleo de Informação e Coordenação do Ponto BR). São características de um registro de nome de domínio no Brasil:

- Pagamento de R$ 40,00 por domínio - taxa anual de manutenção atualmente
- Domínios para pessoas físicas (.nom, etc.)
- Verificação de registros
- http://registro.br (administrado pela FAPESP)
- Domínios: necessidade de registro
- Subdomínios: gerenciados pelo administrador de redes

As regras sintáticas para o registro de um nome de um domínio devem seguir:

- Tamanho mínimo de 2 e máximo de 26 caracteres, não incluindo a extensão
- Caracteres válidos são [A-Z;0-9] e o hífen.
- Nenhum tipo de acentuação é válido.

OBS.: Os domínios com extensões .nom.br deverão ser separados por um ponto, assim como nome.sobrenome.nom.br

1.2.1. Zonas de DNS

Usa-se a nomenclatura *zona de DNS* ao se referir a toda informação correspondente a um domínio. Por exemplo, são informações de um domínio o próprio domínio, suas máquinas, seu reverso, seu MX etc.

Domínio = fatecourinhos.edu.br
Máquinas = **www.fatecourinhos.edu.br**: 201.55.32.12
MX: alt1.aspmx.l.google.com

1.3 DNS Reverso (rDNS)

O serviço conhecido como DNS Reverso traduz endereços IP para nomes de máquinas. Utilizado, por exemplo, pelos servidores de e-mail para evitar Spam. O servidor de e-mail ao receber uma mensagem enviada por um IP, tenta encontrar o

nome do domínio que aquele IP pertence. Este nome de domínio deve ser o mesmo encontrado na remetente da mensagem, desta forma, o servidor de e-mail o julga válido.

Características peculiares:

- conhecido no jargão dos administradores de servidores como "PTR";
- obrigatório de acordo com a RFC 1912, seção 2.1;
- deve haver uma entrada de rDNS para todas as máquinas com nome na rede, não só para algumas;
- muitíssimo importante para servidores de e-mail, pois, confrontando o reverso do IP traduzido do domínio do remetente da mensagem podemos ver se realmente aquela mensagem saiu da origem informada.

Para configurar é preciso que sua operadora responda o reverso de seu domínio para você ou que sua operadora direcione as requisições de reverso de seu domínio para você responder.

1.4 *Cache* de DNS

Suponha que você tenha visitado um site que nunca tenha sido resolvido pelo serviço de DNS de seu provedor, de forma que este tenha que consultar outros servidores de DNS (por meio do já mencionado esquema de pesquisa hierárquica). Para evitar que essa pesquisa tenha que ser feita novamente quando outro usuário do provedor tentar acessar o mesmo site, o serviço de DNS pode guardar a informação da primeira consulta por algum tempo. Assim, em outra solicitação igual, o servidor já saberá qual o IP associado ao site em questão. Este procedimento é conhecido como cache de DNS.

No início, o *cache* de DNS somente guardava dados de consultas positivas, isto é, de quando um site é encontrado. No entanto, os serviços de DNS também passaram a guardar resultados negativos, de sites não existentes ou não localizados, como quando digitamos um endereço errado, por exemplo.

As informações do *cache* são armazenadas por um determinado período de tempo por meio de um parâmetro conhecido como TTL (*time to live,* ou tempo de vida). Este parâmetro é utilizado para evitar que as informações gravadas se tornem

desatualizadas. O período de tempo do TTL varia conforme as configurações determinadas para o servidor.

Graças a isso, o trabalho dos serviços de DNS dos servidores raiz e dos demais subsequentes é minimizado.

2. Características do Servidor DNS

Até o momento falamos das configurações do serviço de DNS, agora vamos abordar características de um Servidor DNS.

2.1. Caching-Only

Um cliente quando quer acessar um domínio, faz uma solicitação ao servidor *caching only* para que este faça a resolução de nome e retorne o endereço IP daquele domínio. Da próxima vez em que a mesma informação for solicitada, a resposta será fornecida diretamente a partir da consulta local ao cache de informações. As informações no cache serão reutilizadas até que o seu prazo de validade (TTL – Time to Live), se expire. Servidores *caching-only* não fornecem informação oficial sobre domínios. Tudo o que sabem é resultado de suas consultas e de sua operação diária. Se o processo for encerrado, todo o cache é descartado e começamos do zero novamente.

2.2. Primário

O servidor primário ou mestre (do inglês *master*), é responsável por uma zona de DNS. É o IP do servidor DNS Primário que deve ser colocado no registro.br para o registro de um domínio. Se o DNS primário sai do ar, não é mais possível obter informações daquele domínio.

Todas as informações para a resolução deste nome de domínio serão obtidas por meio de arquivos locais.

O domínio deve estar devidamente registrado no registro.br, com o endereço IP do servidor DNS apontando para o servidor em questão. Desta forma, ele se torna a fonte de dados oficial para resolução dos nomes para este domínio.

2.3. Secundário

O DNS secundário ou escravo (do inglês *slave*), é responsável por resolver nomes em caso de problemas com o DNS primário. Sua existência é obrigatória para que um domínio seja reconhecido como válido pelo registro.br, afinal são necessários dois servidores DNS para o registro de um domínio.

Deve ser configurada a Transferência de Zonas entre servidores primário e secundário.

Não são realizadas configurações nos servidores DNS Secundários para resolução de nomes de domínios. Sua base de dados é importada do seu DNS Primário.

O DNS Secundário também é fonte oficial de informação a respeito de um domínio.

2.4. Diferenças entre Primário/Secundário e Preferencial/ Alternativo

É muito importante nesta seção destacar a diferença entre os termos, DNS Primário e Secundário (*master e slave*) de DNS Preferencial e Alternativo, estes últimos comumente encontrados nas configurações de IP de máquinas Windows. Enquanto DNS Primário e Secundário se referem às características de um servidor DNS, no caso desse material um servidor *Bind*, os termos DNS Preferencial e Alternativo se referem à ordem a qual o Sistema Operacional Windows vai usar para fazer uma resolução de nome. Por exemplo para fazer a resolução do nome www.fatecourinhos.edu.br o Windows vai consultar primeiro o DNS Preferencial, e apenas se não obtiver nenhuma resposta deste (por ele estar inalcançável por exemplo) ele vai consultar o DNS Alternativo.

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.

3.1 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 convencional e Reverso. Foram feitos testes para checar se a zona de DNS configurada estava correta e foi abordado como fazer corretamente a checagem do arquivo de log que o BIND usa no Debian. Foram mostrados os erros mais comuns e como encontrá-los a partir da análise do log.

Também foi abordado como fazer os testes finais de um DNS, que é a efetiva resolução de um nome de domínio e subdomínio.

Nota do professor: Faça todas as configurações que foram apresentadas neste material em sua Máquina Virtual para aprender os conceitos do DNS. Simule erros, crie novas zona de DNS e teste todos os subdomínios com os comandos de resolução de nomes.

Fontes usadas na elaboração deste material:

http://www.infowester.com/dns.php

https://www.dicas-l.com.br/sysadmin/sysadmin_20070308.php

https://cooperati.com.br/2011/10/dns-criando-zonas-no-bind/

https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04-pt

Evi Nemeth et al. **Manual Completo do Linux: Guia do Administrador 2ªed.**, 2007, Pearson.