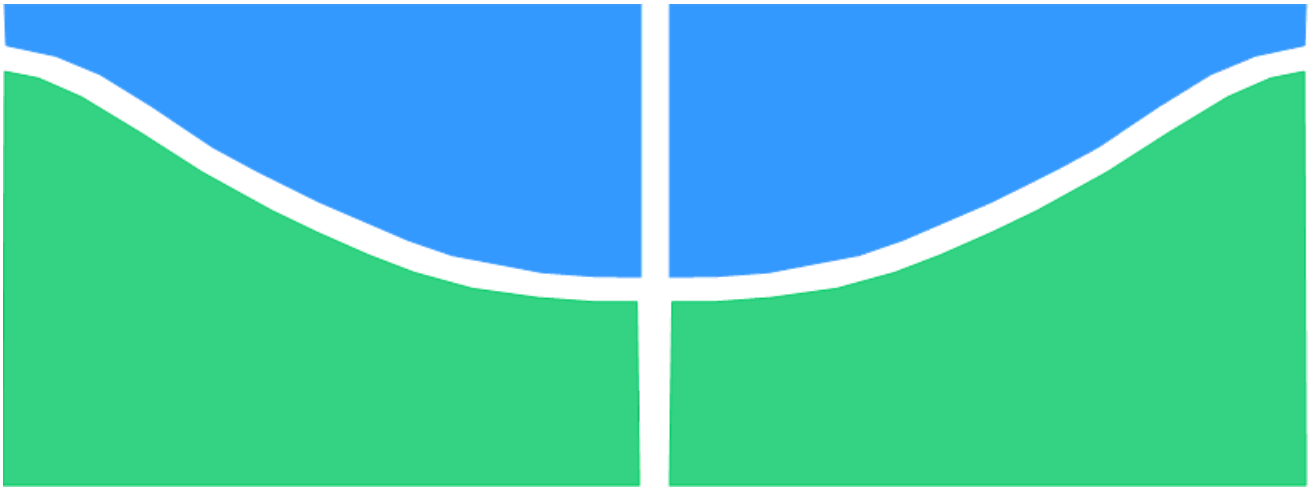

Universidade de

Brasília - UnB

Faculdade do

Gama - FGA

Fundamentos de Redes de

Computadores Prof.

Fernando William Cruz

Roteiro

Laboratório

DNS

Dupla: Vinicius Assumpção de Araujo/200028472
Victor Hugo Oliveira Leão/200028367

Introdução

O que é BIND

Também conhecido como named (pronuncia-se “neime-di”, sendo o elemento “d” uma referência a daemon, ou seja, “name daemon”), o BIND (Berkeley Internet Name Domain) é um software que surgiu na década de 1980, sendo este muito popular para tradução de nomes de domínio em endereços IP e, muitas vezes, componente de servidores Linux.

O BIND permite que o servidor comum se torne um servidor DNS (DNS server), tanto para rede de internet pública quanto privada (LAN). A maioria dos servidores DNS são baseados no BIND, o que faz deste programa muito confiável — além de ser bastante leve, com menos de 5 MB.

é importante entender a diferença entre dois elementos que nos acompanharão em toda a jornada de configuração: domínios (domains) e zonas (zones).

Domínios vs. zonas

Um domínio é "uma divisão lógica do espaço de nome de DNS, enquanto uma zona é física, pois as informações são armazenadas em um arquivo denominado arquivo de zona de DNS (DNS zone file)".

Em um exemplo bem simplório, a relação entre uma coisa e outra é um domínio "domain.com" ser armazenado em um zone file chamado "domain.com.txt".

Pensemos nessa estrutura como uma árvore hierárquica. No topo dela se encontra a zona do domínio raiz (Root Domain); abaixo dela, temos três zonas, que são .com, .net e .org.

Sempre que uma zona é criada, o arquivo de zona é gerado e armazenado em um servidor de DNS, guardando uma representação real da zona, contendo todos os registros para cada domínio ou subdomínio que faz parte dela (endereços de IP, dados de nome, registros MX etc.).

Fato é que não há uma explicação acerca do tema que não seja um pouco confusa. Tentando descomplicar por meio de analogia, vamos supor que estamos procurando um número de telefone (endereço IP) de Bruce Banner (o nosso servidor Apache).

Então, primeiramente, pegamos a agenda telefônica (nome de domínio) e procuramos pela lista B (zona ou arquivo de zona), onde estão todos os contatos cujo nome começa com a letra b (name servers, entre eles o servidor Apache).

Instalação do BIND em um servidor de DNS

Depois da breve explicação das diferenças entre domínios e zonas, voltaremos os olhares para o BIND, que nos permitirá trabalhar com hostnames e endereços de IP privados com facilidade — o que é extremamente útil quando o ambiente de rede se expande e / ou gera vários hosts diariamente, como acontece em provedores de serviços de cloud computing e outros modelos de computação.

Roteiro do experimento:

Pré-requisitos

servidor dns bind no linux

Em vez de um VPS, você pode criar um host virtual no próprio CentOS usando o Apache. Seja qual for a sua escolha, crie três hosts: Master DNS Server (servidor

principal), Slave DNS Server (usado para backup) e Client. As configurações de cada host que você verá aqui no exemplo:

Master DNS Server

IP Address: 192.168.10.1

Hostname: masterdns.com

Slave DNS Server

IP Address: 192.168.10.2

Hostname: slavedns.com

Uma vez que todos os hosts estão funcionando, acesse o servidor Master, abra o terminal e instale o BIND utilizando o seguinte comando: sudo yum install bind* -y.

Configurando o BIND nos servidores de DNS Master e Slave

Com os pacotes devidamente instalados, definiremos os arquivos de zona (lembra-se deles?) na configuração master. Para isso, nós acessaremos o arquivo named.conf usando um editor de texto, como o vim: sudo vim /etc/named.conf.

Vale observar que todos os procedimentos relacionados aos servidores de DNS terão de ser feitos tanto para o Master quanto para o Slave. Eles são exatamente os mesmos, mudando somente os endereços de IP a serem preenchidos.

Nos exemplos deste tópico serão configurados os parâmetros para o servidor Master. Para facilitar, destacamos os pontos que requerem atenção.

No penúltimo bloco é possível notar que configuramos uma zona de pesquisa reversa, que, segundo a Cloudflare, é uma zona utilizada para solucionar problemas e identificar tráfego e comportamentos maliciosos, como spam e bad bots, por meio do mapeamento a partir de um endereço IP para o host.

Vejamos o que significam as demais configurações em destaque:

recursion no: a opção “no” previne que consultas recursivas deixem o servidor mais propenso a sofrer ataques DDoS;

zone name: define o nome da zona (e-tinet.com);

type master: determina o tipo de servidor, no caso, master;

allow-update none: resulta na não utilização DNS dinâmico (DDNS).

Por mais que sejam discretas, algumas configurações são de suma importância para o bom funcionamento do servidor DNS.

Criando arquivos de zona para o servidor de DNS Master

Como vimos no início do artigo, os arquivos de zona são itens essenciais para o nosso

mecanismo rodar, e o meio para criá-los é necessário defini-lo no arquivo named.conf, inserindo as informações de acordo com o que foi configurado na etapa anterior. Exemplo:

fwd.zone

rev.zone

Em seguida, é necessário criar cópias dos arquivos de amostras / modelos de configuração predefinidos, ou samples de configuração, para criar arquivos de zona de encaminhamento (foward zone files). Para isso, utilize os comandos:

sudo cp /var/named/named.localhost /var/named/.fwd.zone

sudo cp /var/named/named.loopback /var/named/.rev.zone

Nos próximos tópicos, editaremos esses arquivos e, também, faremos outros procedimentos importantes a fim de assegurar o funcionamento dos servidores.

Criando arquivo de zona de encaminhamento

Edite o arquivo de zona de encaminhamento usando o comando:

sudo vim /var/named/e-tinet.fwd.zone

Com o arquivo aberto, preencha as informações dos servidores de DNS Master e Slave (sempre nessa mesma sequência) e os respectivos hosts que criamos. Você pode se basear no modelo, abaixo.

```
$TTL 86400
@       IN SOA  masterdns.root.com. (
                                2014090401      ; serial
                                3600        ; refresh
                                1800        ; retry
                                604800      ; expire
                                86400 )  ; minimum
; Name server's
@       IN      NS      masterdns.com.
@       IN      NS      slavedns.com.
; Name server hostname to IP resolve.
@       IN      A       192.168.0.1
@       IN      A       192.168.0.2
; Hosts in this Domain
masterdns       IN      A       192.168.0.1
slavedns        IN      A       192.168.0.2
```

Salve o arquivo conforme o atalho do seu editor de texto.

Criando o arquivo de zona de pesquisa reversa

Prosseguindo, chegou a hora de criar um arquivo de pesquisa reversa (reverse lookup file) utilizando aquela cópia que fizemos há pouco. Digite: sudo vim /var/named/e-tinet.rev.zone e configure conforme o exemplo, abaixo.

```
$TTL 86400
@       IN SOA  masterdns.root.com. (
                                2014090402      ; serial
                                3600            ; refresh
                                1800            ; retry
                                604800          ; expire
                                86400 )         ; minimum
; Name server's
@       IN      NS      masterdns..com.
@       IN      NS      slavedns.com.
; Name server hostname to IP resolve.
masterdns       IN      A       192.168.0.1
slavedns        IN      A       192.168.0.2
;Hosts in Domain
100             IN      PTR     masterdns.com.
102             IN      PTR     slavedns.com.
200             IN      PTR     client.com.
```

Só salvar e fechar o arquivo.

Verificando as configurações aplicadas

Para validarmos e nos certificarmos de que as configurações são funcionais e seguras, mudaremos o grupo para os arquivos de zona. Observação: faça isso caso eles pertençam a usuário root; verifique pelo comando sudo ls -l /var/named.

```
sudo chgrp named /var/named/e-tinet.fwd.zone
sudo chgrp named /var/named/e-tinet.rev.zone
```

O próximo passo é verificar se os arquivos de zona não têm erros utilizando o comando named-checkconf.

```
sudo named-checkconf /etc/named.conf
sudo named-checkzone masterdns.e-tinet.com /var/named/e-tinet.fwd.zone
```

sudo named-checkzone masterdns.e-tinet.com /var/named/e-tinet.rev.zone

Se os resultados exibidos forem “OK” podemos partir para a próxima etapa — caso contrário, sugerimos que revise as configurações. Certo, então qual é o próximo passo? Resolver uma restrição imposta pelo iptables, que é executado por padrão no sistema CentOS. Trata-se de uma restrição ao localhost, fazendo necessária a adição de uma regra na porta 53. Digite a seguinte sequência:

sudo iptables -I INPUT -p udp --dport 53 -m state --state NEW -j ACCEPT

sudo iptables -L INPUT

sudo service iptables save

sudo service iptables restart

Configurando o host cliente

Vamos fazer a máquina cliente se comunicar com os servidores de DNS recém-criados? Primeiramente, digite no terminal o comando setup e, então, nos campos Primary DNS Server e Secondary DNS Server, preencha com os endereços de IP dos servidores Master e Slave, respectivamente. Selecione a opção OK para confirmar.

Faça o mesmo com o arquivo /etc/resolv.conf por meio do editor de texto de sua preferência, inserindo as seguintes informações:

search domain.com # apenas reiterando que esse campo deve ser substituído pelo domínio que você criou, não necessariamente como neste exemplo

nameserver 192.168.0.1

nameserver 192.168.0.2

Sinta-se livre para fazer os testes via comandos dig e nslookup. Façamos um ping para finalizar a configuração:

ping masterdns.com -c 2

ping slavedns.com -c 2

ping 192.168.0.1 -c 2

ping 192.168.0.2 -c 2