Implementação e Avaliação de um Serviço de DNS (Bind9)

Alexandre A. F. Chain[1] Marcel Matsumoto[1]

[1] Instituto de Ciências Exatas e Tecnológicas (IEP)
Universidade Federal de Viçosa (UFV) - Campus Rio Paranaíba
Rio Paranaíba, MG - Brazil, 38810-000

{chain,alexandre}@ufv.br,{matsumoto,marcel}@ufv.br

Abstract. *The DNS server (Domain Name System) is considered one of the most important services in the field of computer networks, since without it we would not be able to browse the internet the way we currently use it, as its function allows than the domain names informed by an end user and transform them into IP addresses for the machine. Considering the vital importance of DNS services, and the way they operate within the user's lifetime on the World Wide Web, we have the proposal to implement and configure a DNS service using Bind9, using a virtual machine with linux operating system, presenting the step by step of its configuration.*

Resumo. *O servidor DNS (Domain Name System – Sistema de nome de domínio) é considerado um dos serviços mais importantes no âmbito de redes de computadores, visto que a sua inexistência não seríamos capazes de navegar na internet da maneira que utilizamos atualmente, pois sua função permite que os nomes de domínios informados por um usuário final e transformá-los em endereços IP's para a máquina. Considerando a vital importância dos serviços de DNS, e a maneira que operam dentro da vida útil do usuário na World Wide Web, temos a proposta de implementar e configurar um serviço de DNS utilizando o Bind9, utilizando uma máquina virtual com sistema operacional linux, apresentando o passo a passo de sua configuração.*

1. Introdução

Nós seres humanos, utilizamos diversas maneiras para serem identificados, e destes meios de identificação se dá através do nome, número de RG, número da carteira de motorista, pelo próprio CPF dentre outras formas. Ainda que exista diversas maneiras de ser identificado, torna-se viável utilizar uma forma do que outra conforme o cenário. Os sistemas do governo, por exemplo, é conveniente utilizar os CPF de seus usuários para garantir maior precisão na busca de suas informações, por outro lado as pessoas

preferem usar seus próprios nomes, visto que a facilidade de recordar palavras é mais fácil do que lembrar de uma sequência numérica [Kurose and Ross, 2006].

Desta forma, o mesmo acontece em hospedagens na Internet, usa-se um identificador conhecido como nome de hospedeiros (hostname) - www.google.com, pois é fácil de ser lembrado e é amigável para os seres humanos. Entretanto, como os nomes de hospedeiros utilizam-se caracteres alfanuméricos, isso faz com que os roteadores tenham uma difícil interpretação, necessitando utilizar números ao invés de caracteres, também conhecido como endereço IP.

Com base neste cenário em que as pessoas preferem identificações por meio de nomes de hospedeiros e roteadores os endereço IP, é preciso que haja uma harmonização entre essas preferências e é através disso que a Redes de Computadores utiliza um conceito, chamado serviço de diretório conhecido como DNS (domain name system — sistema de nomes de domínio). Então desta forma, sem este serviço seria impossível a conceituação de uso da internet como conhecemos. Analisando o DNS, vemos que ele faz a tradução dos nomes de um determinado hospedeiro para endereços IP e com via dupla, e esse recurso indispensável possibilita que ao informar um endereço (url) de um site na web, essa requisição será processada pelo DNS, que assimilará a busca através de uma pesquisa em seu banco de dados, e ao encontrar direciona para o IP do servidor em que realmente está hospedado.

Assim, se não utilizássemos o recurso DNS, podemos perceber que o que existiria seria uma base de números equivalentes a endereços de IP. Fazer a divulgação de um site sendo de sua propriedade ou não, seria muito complicado e engessado, também se estendendo aos emails.

Pode-se perceber então no quanto o serviço DNS exerce uma função imprescindível na experiência do usuário no uso da rede, e é crucial para quem é autor de um site, já que o seu produto se torna localizável e memorável.

Domínios não são vinculados exclusivamente a sites, existem diversas modalidades de registros DNS para que serviços em adendo funcionem.

Dentre esses tipos, existem os que permitem ao usuário acrescentar funções ao domínio respectivo. Notoriamente, ao registrar o domínio pode-se ter intenção de não somente usá-lo como página da web, mas também para um servidor de email ou até mesmo um (File Transfer Protocol) FTP, que possibilita a transferência de arquivos.

Deste modo, existem múltiplas designações de DNS que oferecem a implementação de outros serviços no servidor,como por exemplo: Registros A que conectam endereços IP a domínios, CNAME que criam redirecionamentos a domínios e subdomínios, PTR que ligam domínios a endereços IP, NS que identificam os servidores DNS de um website e MX que possibilita a configuração de endereços de email no determinado domínio.

2. Trabalhos Relacionados

Neste capítulo é apresentado os trabalhos relacionados que estarão direta ou indiretamente relacionados com os serviços DNS e que serviram de base para o desenvolvimento deste trabalho.

2.1. Implementação e Avaliação do Paralelismo Moderado no servidor DNS BIND9

Visando o desempenho abaixo do ideal do servidor DNS ISC BIND9 com vários threads este artigo relacionado explora abordagens práticas que endereçam o problema.

Nele são identificados os principais gargalos que ocorrem devido a sobrecargas para sincronização de encadeamentos. Esses gargalos são então eliminados fornecendo áreas de trabalho separadas com um grande pool de memória para threads, introduzindo operações mais rápidas em contadores de referência e implementando bloqueios de leitor-gravador eficientes.

Algumas das soluções desenvolvidas dependem de operações atômicas específicas da arquitetura de hardware, que são menos portáveis, mas a implementação resultante ainda suporta as mesmas plataformas de antes por meio de APIs abstratas.

A implementação aprimorada se adapta bem com até quatro processadores, seja operando como um servidor DNS autoritativo, com ou sem atualizações dinâmicas, ou como um servidor DNS de cache enquanto reduz o consumo de memória para grandes bancos de dados DNS.

Embora os resultados descritos neste trabalho sejam baseados em nossa experiência com o BIND9, as técnicas devem ser aplicáveis a outros aplicativos baseados em threads.

2.2. Implementação e avaliação de um módulo de aumento de imunidade para ISC BIND9

Este estudo se concentra em um módulo de segurança que aumenta a imunidade para proteger os servidores da Internet contra ataques cibernéticos. Ele consiste em funções imunes inatas e adaptativas: A função imune inata detecta ciberataques conhecidos e desconhecidos, enquanto a função imune adaptativa aprende e detecta os ciberataques detectados pela função imune inata.

Foi mostrado que esse módulo de segurança detectou e impediu de forma adaptativa ataques cibernéticos conhecidos e desconhecidos no aplicativo de servidor web de teste. Este artigo também descreve a implementação deste módulo para ISC BIND9, avaliando sua compatibilidade com um aplicativo de servidor comumente

usado na Internet. Eles realizaram testes atacando especificamente CVE-2015-5477 e CVE-2016-2776.

Os resultados mostraram que a precisão de detecção do módulo foi em média de 96,87% , enquanto a sobrecarga do módulo foi de 10,81%.

3. Proposta

Idealizado e desenvolvido na década de 80, o BIND (Berkeley Internet Name Domain) é um servidor DNS de ampla e mundial utilização, especialmente quando falamos de sistemas Linux, onde a escala é ainda maior. Visto que o servidor está presente na maioria das empresas que utilizam e operam um servidor DNS em Linux, é de considerável importância e aplicação o conhecimento teórico e prático do BIND para um profissional qualificado da área.

Considerando a vital importância já mencionada dos serviços de DNS, e a maneira que operam dentro da vida útil do usuário na World Wide Web, temos a proposta de criar um servidor DNS funcional usando o BIND, no sistema operacional LINUX.

4. Demonstração / Experimentação

Para demonstração do Bind9 utilizaremos uma máquina virtual com sistema operacional linux para realizar as configurações e implementação dos serviços de DNS e assim testá-las, todo o conteúdo poderá ser acessado através do repositório[1] no Github, onde se encontra toda fonte e passo a passo da demonstração.

4.1 Instalando o BIND

Com o comando a seguir, é possível instalar o bind a partir da rede no terminal.

apt-get install bind9

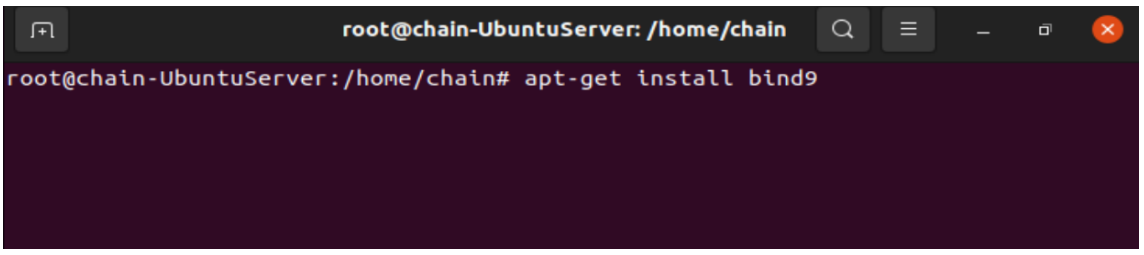

Figura 1. Instalando o Bind9 na máquina.
Fonte: (Autoria Própria)

[1] https://github.com/alehchain/ServerDNSBind9.git

4.2 Preparando a Rede

Antes de iniciar o bind9 iremos fazer as configurações iniciais na rede de IPv4 alterando de automático para manual, e inserindo o novo endereço, máscara de rede, gateway e DNS .

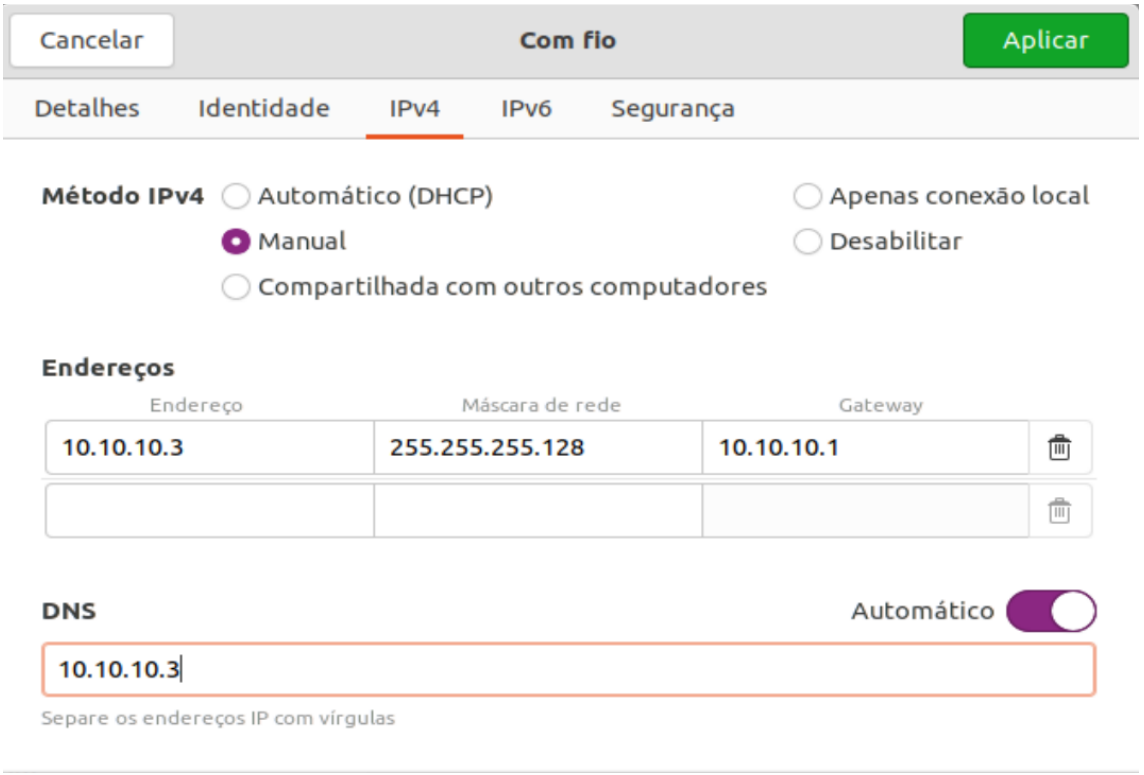

Figura 2. Configurações iniciais da Rede IPv4 e DNS.
Fonte: (Autoria Própria)

4.3 Localizando o BIND

Logo após as devidas configurações, voltamos ao terminal e adicionamos o seguinte comando *cd /etc/bind,* para entrar até o diretório do bind9.

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

Figura 3. Abrindo o diretório do Bind e listando seus conteúdos.
Fonte: (Autoria Própria)

4.4 Configurando o BIND

A configuração é editada a partir do arquivo /etc/named.conf.local. De modo a criar uma nova zona direta e zona reversa:

Figura 4. Criando as zonas direta e Reversa.
Fonte: (Autoria Própria)

O bind9 possui uma zona direta com arquivo padrão db.local e uma zona reversa com o arquivo padrão db.127, nesta etapa iremos fazer uma cópia destes arquivos, e configurá-los com base na configuração de redes que criamos anteriormente:

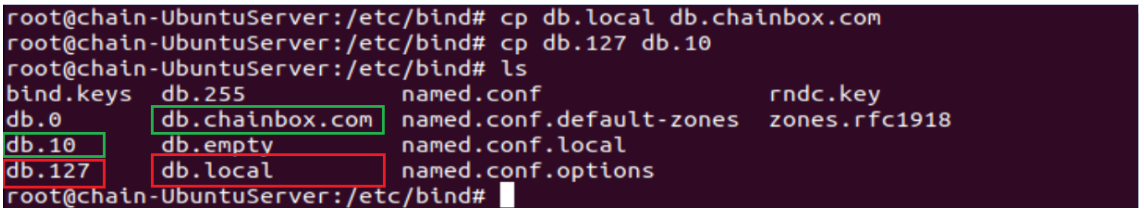

Figura 5. Fazendo uma cópia das zonas reversa e direta.
Fonte: (Autoria Própria)

Após a criação dos novos arquivos padrão, utilizamos o nano para realizar as devidas alterações no arquivo de zona:

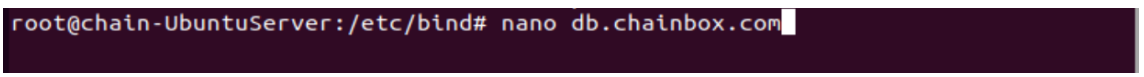

Figura 6. Abrindo o arquivo da zona direta.
Fonte: (Autoria Própria)

Por padrão o bind9 utiliza um domínio localhost ao qual devemos substituí los pelo nome de DNS ao qual definimos de “chainbox.com”, e substituimos o endereço de IP padrão 127.0.0.1 pelo novo endereço de IP 10.10.10.3, além de adicionar os arquivos de configuração www, ftp e voip com seus respectivos IP’s uma vez predefinidos:

```
  GNU nano 5.6.1                    db.chainbox.com *
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     chainbox.com. root.chainbox.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      chainbox.com.
@       IN      A       10.10.10.3
www     IN      A       10.10.10.4
ftp     IN      A       10.10.10.4
voip    IN      A       10.10.10.5
```

Figura 7. Alterando os domínios arquivo de configuração zona direta.
Fonte: (Autoria Própria)

Agora iremos fazer as configurações no arquivo da zona reversa, substituindo os localhost por chainbox.com, alteramos o “1.0.0” IN restante do endereço do IP, pelo 3.10.10 que também é o restante do IP criado na nova configuração :

```
  GNU nano 5.6.1                        db.10 *
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     chainbox.com. root.chainbox.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      chainbox.com.
3.10.10 IN      PTR     chainbox.com.
```

Figura 8. Alterando os domínios do arquivo de configuração zona reversa.
Fonte: (Autoria Própria)

Ao final das configurações de zona direta e reversa, devemos reiniciar o bind9:

```
root@chain-UbuntuServer:/etc/bind# /etc/init.d/bind9 restart
```

Figura 9. Reinicializando o Bind9.
Fonte: (Autoria Própria)

Após a reinicialização, podemos usar o seguinte comando *service named status*, para analisar os status do bind9:

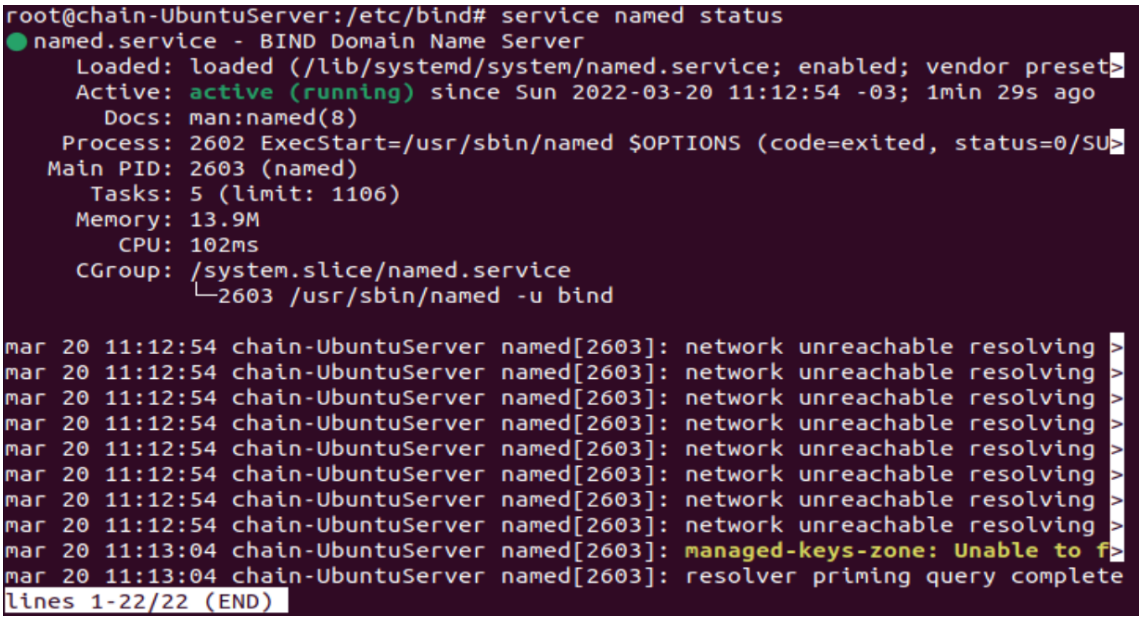

Figura 10. Verificando os status.
Fonte: (Autoria Própria)

4.5 Preparando o servidor DNS

Com o BIND devidamente configurado, vamos ajustar as configurações do servidor DNS e, com isso, verificar se ele está funcionando corretamente. No arquivo /etc/resolv.conf inserimos um novo nameserver com o endereço criado inicialmente.

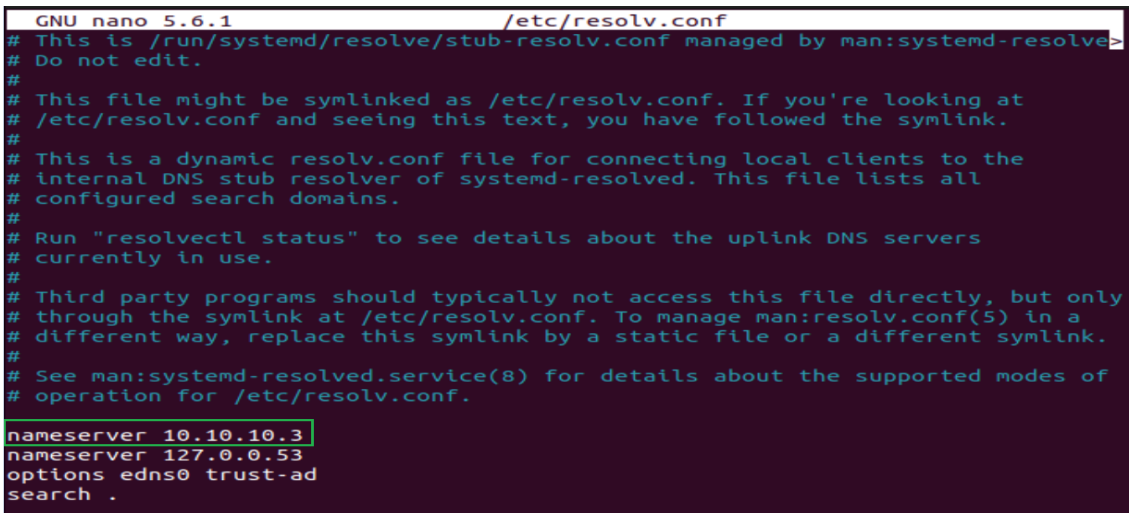

Figura 11. Adicionando nameserver no arquivo de resolvedor de nomes.
Fonte: (Autoria Própria)

4.6 Testando o servidor DNS

Com o DNS server devidamente criado, é possível registrar subdomínios, implementar serviços complementares totalmente customizados e muito mais. Para averiguar o funcionamento, e testar se as configurações estão devidamente funcionando, podemos usar comando no terminal utilizando o host com o nome criado "chainbox.com", como por exemplo:

```
root@chain-UbuntuServer:/etc/bind# host chainbox.com
chainbox.com has address 10.10.10.3
```

Figura 12. Analisando o endereço.
Fonte: (Autoria Própria)

É possível utilizar o *nslookup* para analisar o servidor e o endereço, usando o comando *nsloookp chainbox.com*.

```
root@chain-UbuntuServer:/etc/bind# nslookup chainbox.com
Server:         10.10.10.3
Address:        10.10.10.3#53

Name:   chainbox.com
Address: 10.10.10.3
```

Figura 13. Analisando o nome e o endereço.
Fonte: (Autoria Própria)

Outra maneira de testar o endereço é informar o nome de domínio usando o seguinte comando: *host www.chainbox.com*.

```
root@chain-UbuntuServer:/etc/bind# host www.chainbox.com
www.chainbox.com has address 10.10.10.4
root@chain-UbuntuServer:/etc/bind#
```

Figura 14. Analisando o endereço do DNS informado.
Fonte: (Autoria Própria)

Nas configurações iniciais também realizamos as configurações www, ftp, voip.

```
root@chain-UbuntuServer:/etc/bind# host www.chainbox.com
www.chainbox.com has address 10.10.10.4
root@chain-UbuntuServer:/etc/bind# host ftp.chainbox.com
ftp.chainbox.com has address 10.10.10.4
root@chain-UbuntuServer:/etc/bind# host voip.chainbox.com
voip.chainbox.com has address 10.10.10.5
root@chain-UbuntuServer:/etc/bind# nslookup voip.chainbox.com
Server:         10.10.10.3
Address:        10.10.10.3#53

Name:   voip.chainbox.com
Address: 10.10.10.5
```

Figura 15. Verificando os arquivos de configuração www, ftp e voip.
Fonte: (Autoria Própria)

5. Discussão

É evidente que o BIND é usado com sucesso para todos os aplicativos, desde a publicação da zona raiz DNS (assinado com DNSSEC) e muitos domínios de nível superior.

Pode ser utilizado por provedores de hospedagem que publicam arquivos de zonas muito grandes com muitas zonas pequenas e para empresas com zonas internas (privadas) e externas.

6. Conclusão

Podemos concluir que o DNS tem então o papel fundamental de evitar que o sistema de redirecionamento fosse feito à base de números correspondentes a endereços de IP. O trabalho dificultoso e anacrônico na divulgação e memorização dos endereços, impactaria em esquematizações de marketing, controles internos de empresas, utilização de serviços e o uso acessível que a internet hoje provê, e a situação seria ainda mais caótica quanto aos emails.

Portanto podemos concluir que o servidor DNS exerce um papel fundamental na experiência dos usuários quanto à navegação na Internet, se tratando de todos os envolvidos na organização e uso da rede.

Ao configurarmos um servidor DNS interno usando o software de servidor de nomes BIND, é possível resolver nomes de host e endereços IP privados. Isso fornece uma maneira central de gerenciamento dos seus nomes de host e endereços IP privados internos, o que é indispensável quando seu ambiente se expande para muitos hosts tratando com eficiência toda esta temática. Foi possível então, identificar a vitalidade do BIND para o âmbito de rede, e que sua ampla e dominante utilização especialmente dentre os sistemas LINUX é justificada e lógica.

7. Referências

Kurose, J. F., & Ross, K. W. (2006). Redes de Computadores e a Internet. São Paulo: Person, page 95.

Santos, J. M. M. D. (2015). Implementação de algoritmo de escalabilidade para DNS em contexto cloud (Doctoral dissertation, Universidade de Coimbra).

Simião, J. C. D. S. (2017). Análise e criação de algoritmos para garantia de segurança em servidores DNS.

Stearns, C. et al. BIND Best Practices - Recursive. 2022. Disponível em: <https://kb.isc.org/docs/bind-best-practices-recursive> Acesso em: 2022-03-16.