

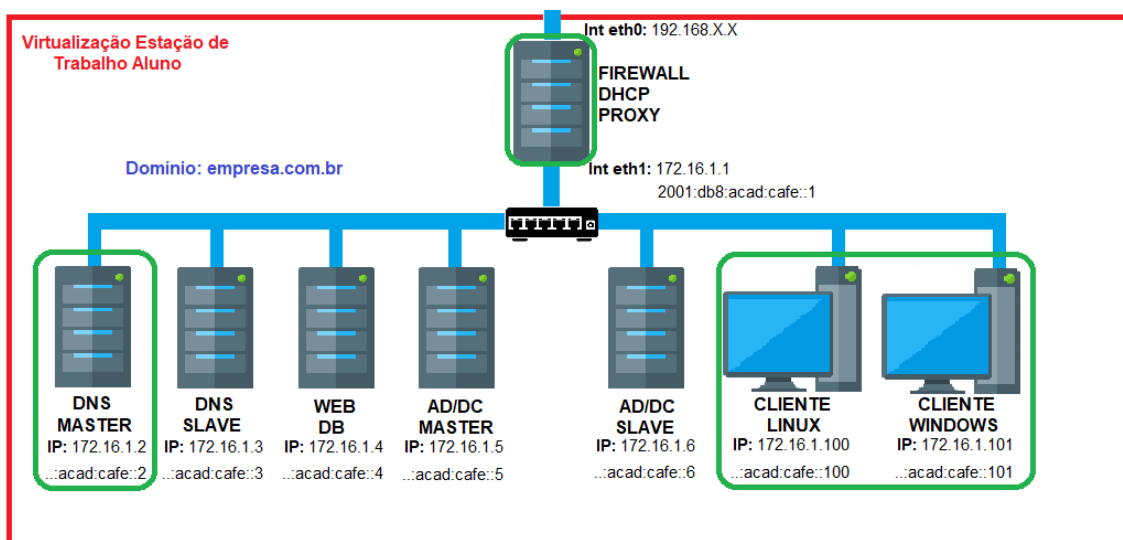
4. Implementação do DNS

4.1 Introdução

Para implementar o serviço de nomes e domínios instalaremos o BIND que é um software de código aberto. O nome BIND significa Berkeley Internet Name Domain, devido a sua origem na Universidade da Califórnia em Berkeley no início dos anos 80. Atualmente o BIND é o software mais utilizado para implementação desse serviço, fornecendo uma plataforma estável e robusta para a construção de sistemas distribuídos compatíveis com os padrões DNS publicados. A versão 9 do BIND foi praticamente reescrita, tornando-se mais segura, estável e passando a suportar novas funcionalidades como a extensão DNSSEC e o protocolo IPv6.

Para este laboratório serão utilizadas as seguintes Máquinas Virtuais:

- Appl-Debian10-Firewall - Firewall, DHCP e Compartilhamento da internet para rede interna
- Appl-Debian10-NS - Servidor DNS
- Appl-Debian10-Client ou Appl-Windows7-Client - Testes de resolução de nomes



4.2 Ajustes iniciais

Verifique os endereços IP da Appl-Debian10-NS, os endereços deverão ser fixados no arquivo interfaces ou entregues via DHCP como segue:

```
IPv4: 172.16.1.2
IPv6: 2001:db8:acad:cafe::2
```

No servidor DHCP, na VM Firewall, ajuste o servidor DNS para consultas que será entregue automaticamente via DHCP às estações clientes:

```
root@Firewall:/# vim /etc/dhcp/dhcpd.conf
```

```
option domain-name-servers 172.16.1.2;
```

Por fim, reinicie o serviço isc-dhcp-server:

```
root@Firewall:/# systemctl restart isc-dhcp-server
```

4.3 Instalação do Bind9

Para instalar o Bind9 serão utilizados os repositórios oficiais da distribuição Debian:

```
root@ns:/# apt-get update
root@ns:/# apt-get install bind9
```

Para realização dos testes de funcionamento do software e serviço a ser implementado, será necessário configurar o resolver do servidor. Para isso edite o arquivo *resolv.conf*:

```
root@ns:/# vim /etc/resolv.conf
```

Substitua o conteúdo do arquivo *resolv.conf* pelo seguinte:

```
search empresax.com.br
nameserver 127.0.0.1
```

4.4 Conhecendo os arquivos de configuração do Bind9

Para compreensão do funcionamento do software Bind9, é importante conhecer a função dos principais arquivos criados no diretório */etc/bind* durante a instalação, assim como os arquivos que criaremos para armazenar as configurações de zona de autoridade. Os arquivos *db.empresax.com.br* e *db.1.16.172* estão na lista abaixo, considerando a configuração do serviço de DNS para o domínio *empresax.com.br* pertencente a rede 172.16.1.0/24.

named.conf.default-zones	armazena as configurações de zonas padrão
named.conf.options	armazena as configurações globais do Bind9
named.conf.local	armazena as configurações de zonas de autoridade
db.root	contém os endereços de todos os servidores raiz de DNS

Além dos arquivos criados por padrão pelo Bind9, criaremos outros dois arquivos que terão como função armazenar as informações de zona de autoridade, os nomes utilizados para os arquivos de resolução “db.” são sugestões de acordo com os padrões comumente encontrados na internet. Você poderá nomear os arquivos da forma que desejar, desde que sejam referenciados no arquivo *named.conf.local*.

db.empresax.com.br	Responsável pela resolução direta do domínio “empresax.com.br”
db.1.16.172	Responsável pela resolução reversa do domínio “empresax.com.br”

Observação:

A utilização do arquivo db.1.16.172 supõe que o endereço de rede utilizado é o 172.16.1.0/24.

4.5 Configurando o Bind9

Nesta seção será realizada a configuração do Bind9, para responder pelo domínio “empresax.com.br”. Para isso, primeiramente será inserida as configurações de zona no arquivo *named.conf.local*.

```
root@ns:/# vim /etc/bind/named.conf.local
```

No arquivo será inserida as seguintes linhas:

```
zone “empresax.com.br” {
    type master;
    file “db.empresax.com.br”;
};

zone “1.16.172.in-addr.arpa” {
    type master;
    file “db.1.16.172”;
};
```

No arquivo de configuração global do Bind9 */etc/bind/named.conf.options* realizaremos duas configurações básicas, a fim de familiarizar-se com a aplicação. Para isso edite o arquivo.

```
root@ns:/# vim /etc/bind/named.conf.options
```

1. Serão adicionadas as linha responsável pela permissão de transferência de zona do servidor DNS primário para o servidor DNS secundário, esta configuração evita plágio de DNS. Neste laboratório utilizaremos o IP 172.16.1.3 como IP liberado para transferência de zona.

```
allow-transfer {
    172.16.1.3; #Servidor secundario
};
```

2. Será alterada a linha responsável por encaminhar as consultas DNS para outro(s) servidor(es), quando o servidor local não souber resolver. Utilize qualquer servidor público, por exemplo: 8.8.8.8.

```
forwarders {  
    8.8.8.8; #Servidores DNS google  
};
```

3. E por fim, ajuste a linha "dnssec-validation" de "auto" para "no":

```
dnssec-validation no;
```

Para uma melhor administração dos arquivos que serão responsáveis pelo armazenamento dos registros, criaremos um link simbólico denominado “*master*” do diretório padrão utilizado pelo BIND “*/var/cache/bind*” dentro do diretório “*/etc/bind*”.

```
root@ns:/# ln -sf /var/cache/bind /etc/bind/master
```

Dica:

Após editar os arquivos */etc/bind/named.conf.options* e */etc/bind/named.conf.local* é importante testar se não há erros de sintaxe, para isso pode ser utilizado o seguinte utilitário disponível no BIND. Não poderá retornar erros.

```
# named-checkconf
```

Agora criaremos o arquivo *db.empresax.com.br* conforme definido no arquivo *named.local*. Este arquivo será responsável por armazenar as configurações do domínio *empresax.com.br*. É nele que serão inseridos os registros referente ao domínio supracitado, assim como o mapa das máquinas da rede local. É importante lembrar que este arquivo não é criado durante a instalação do BIND, neste sentido, será necessário primeiramente criar o arquivo.

```
root@ns:/# vim /etc/bind/master/db.empresax.com.br
```

Neste arquivo será inserido o seguinte conteúdo:

```

$TTL 1D
@      IN      SOA  ns.empresax.com.br. admin.empresax.com.br. (
                                2018040501      ; Serial
                                3H                ; Refresh
                                15M               ; Retry
                                1W                ; Expire
                                1D )             ; Negative Cache TTL
;
@      IN      NS   ns.empresax.com.br.
; Servidores SMTP IN MX
@      IN      MX   2      mail.empresax.com.br.
; Servidores
firewall      IN      A          172.16.1.1
proxy         IN      CNAME     firewall
ns            IN      A          172.16.1.2
www           IN      A          172.16.1.4
sb4-master    IN      A          172.16.1.5
sb4-slave     IN      A          172.16.1.6
mail          IN      A          172.16.1.7

```

Dica:

Após a edição do arquivo de zona do domínio empresax.com.br, é importante verificar se não há erros de sintaxe, para isso pode ser utilizado o utilitário `named-checkzone` disponível no BIND.

```
root@ns:/# named-checkzone empresax.com.br /etc/bind/master/db.empresax.com.br
```

Deve retornar a resposta: Load Serial XXXXX OK

Se nenhum erro foi apresentado nos testes realizados, agora podemos reiniciar o serviço `bind9` e posteriormente verificar seu `status`.

```
root@ns:/# systemctl restart bind9
root@ns:/# systemctl status bind9
```

Observação:

Se o serviço já estiver no ar você pode utilizar o parâmetro `“reload”`, assim o serviço apenas aplicará os novos parâmetros sem reiniciar.

4.6 Testando o funcionamento do servidor DNS

Atenção:

Caso ocorrer erro durante os testes, após qualquer alteração realizada nos arquivos de configuração, você deve aplicar as novas configurações com o comando:

```
root@ns:/# systemctl reload bind9
```

4.6.1 Testes com o utilitário NSLOOKUP

Antes de iniciar os testes, instale o utilitário `dnsutils`:

```
root@ns:/# apt install dnsutils
```

Para realizar os testes com o utilitário NSLOOKUP, basta proceder como segue:

```
root@ns:/# nslookup ns.empresax.com.br
```

O resultado deverá ser:

Server: 127.0.0.1

Address: 127.0.0.1 #53

Name: ns.empresax.com.br

Address: 172.16.1.2

```
root@ns:/# nslookup firewall.empresax.com.br
```

O resultado deverá ser:

Server: 127.0.0.1

Address: 127.0.0.1 #53

Name: firewall.empresax.com.br

Address: 172.16.1.1

4.6.2 Testes com o utilitário PING

Para testar com o utilitário PING, basta enviar os pacotes ICMP para os endereços registrados no domínio e verificar se estes respondem:

```
root@ns:/# ping firewall.empresax.com.br
```

```
root@ns:/# ping ns.empresax.com.br
```

4.6.3 Testes a partir de estações clientes

Realize os testes a partir da estação cliente, para isso, é necessário configurar o resolver da estação.

Para estação Cliente Linux, substitua o conteúdo do arquivo `resolv.conf` pelo seguinte:

```
search empresax.com.br
nameserver 172.16.1.2
```

4.7 Configurando o DNS reverso

Para configurar o DNS reverso em nosso servidor, será necessário criarmos o arquivo `db.1.16.172` conforme definido no arquivo `named.local`. Este arquivo será responsável por armazenar as configurações reversas do domínio `empresax.com.br`. Assim como o arquivo `db.empresax.com.br`,

este arquivo não é criado durante a instalação do BIND, neste sentido, será necessário primeiramente criá-lo.

```
root@ns:/# vim /etc/bind/master/db.1.16.172
```

Neste arquivo será inserido o seguinte conteúdo:

```
$TTL 1D
@      IN      SOA  ns.empresax.com.br. admin.empresax.com.br. (
                                2018040501 ; Serial
                                3H          ; Refresh
                                15M         ; Retry
                                1W          ; Expire
                                1D )        ; Negative Cache TTL
;
@      IN      NS   ns.empresax.com.br.
; Servidores
1      IN      PTR  firewall.empresax.com.br.
2      IN      PTR  ns.empresax.com.br.
4      IN      PTR  www.empresax.com.br.
5      IN      PTR  sb4-master.empresax.com.br.
6      IN      PTR  sb4-slave.empresax.com.br.
7      IN      PTR  mail.empresax.com.br.
```

Após a criação do arquivo, podemos reiniciar o serviço bind9 e posteriormente verificar seu *status*.

```
root@ns:/# systemctl restart bind9
root@ns:/# systemctl status bind9
```

4.7.1 Testando o funcionamento do servidor DNS reverso

4.7.2 Teste com o utilitário NSLOOKUP

Para realizar os testes com o utilitário NSLOOKUP, basta proceder como segue:

```
root@ns:/# nslookup 172.16.1.2
O resultado deverá ser:
Server: 127.0.0.1
Address: 127.0.0.0 #53
2.1.16.172.in-addr.arpa name = ns.empresax.com.br
```

Teste a resolução reversa dos demais endereços configurados.

Observação:

Os comandos **dig** e **host** podem ser utilizados em substituição ao comando **nslookup**.

4.8 Configuração de Registros IPv6 no Bind9

4.8.1 Cinfiguração do DNS direto

Antes de iniciar a atividade, verifique se a interface `enp0s3` da sua máquina virtual "ns" está configurada com o IPv6 `2001:db8:acad:cafe::2`.

Configure sua Máquina Virtual Client com estático:

```
## Rede Interna – LAN IPv6 (enp0s3)
iface enp0s3 inet6 static
address 2001:db8:acad:cafe::100
netmask 64
```

Edite o arquivo "*db.empresax.com.br*":

```
root@ns:/# vim /etc/bind/master/db.empresax.com.br
```

Insira as seguintes linhas:

```
firewall      IN      AAAA    2001:db8:acad:cafe::1
ns            IN      AAAA    2001:db8:acad:cafe::2
```

Após a edição do arquivo, podemos reiniciar o serviço `bind9` e posteriormente verificar seu *status*.

```
root@ns:/# systemctl restart bind9
root@ns:/# systemctl status bind9
```

Testando o funcionamento do servidor DNS

Com o comando `host`:

```
root@ns:/# host -t AAAA ns.empresax.com.br
root@ns:/# host -t AAAA firewall.empresax.com.br
```

Com o comando `nslookup`:

```
root@ns:/# nslookup -type=ANY ns.empresax.com.br
root@ns:/# nslookup -type=ANY firewall.empresax.com.br
```

Ping o domínio para verificar se o mesmo responde:

```
root@ns:/# ping6 ns.empresax.com.br
root@ns:/# ping6 firewall.empresax.com.br
```


4.8.2 Configuração do DNS reverso

Edite o arquivo *named.conf.local*:

```
root@ns:/# vim /etc/bind/named.conf.local
```

Insira as seguintes linhas:

```
zone "e.f.a.c.d.a.c.a.8.b.d.0.1.0.0.2.ip6.arpa" {  
    type master;  
    file "db.empresax.reverse.ipv6";  
};
```

Verifique se não há erros de sintaxe:

```
root@ns:/# named-checkconf
```

Crie o arquivo "db.empresax.reverse.ipv6":

```
root@ns:/# vim /etc/bind/master/db.empresax.reverse.ipv6
```

E insira o seguinte conteúdo:

```
$TTL 1D  
@      IN      SOA  ns.empresax.com.br. admin.empresax.com.br. (  
                                2018040501 ; Serial  
                                3H          ; Refresh  
                                15M         ; Retry  
                                1W          ; Expire  
                                1D )        ; Negative Cache TTL  
@      IN      NS   ns.empresax.com. br.  
; Servidores  
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  firewall.empresax.com.br.  
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 IN PTR  ns.empresax.com.br.
```

Após a edição do arquivo, podemos reiniciar o serviço bind9 e posteriormente verificar seu *status*.

```
root@ns:/# systemctl restart bind9  
root@ns:/# systemctl status bind9
```

Testando o funcionamento do servidor DNS reverso

Teste a resolução de nomes:

```
root@ns:/# nslookup 2001:db8:acad:cafe::1
```

O resultado deverá ser:

Server: 127.0.0.1

Address: 127.0.0.1#53

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.a.c.d.a.c.a.8.b.d.0.1.0.0.2.ip6.arpa name = firewall.empresax.com.br.

```
root@ns:/# nslookup 2001:db8:acad:cafe::2
```

O resultado deverá ser:

Server: 127.0.0.1

Address: 127.0.0.1#53

2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.a.c.d.a.c.a.8.b.d.0.1.0.0.2.ip6.arpa name = ns.linux.empresax.com.br.

Por fim, teste o serviço de resolução a partir da estação cliente.