

4.9 Configuração do Servidor DNS Secundário

4.9.1 Introdução

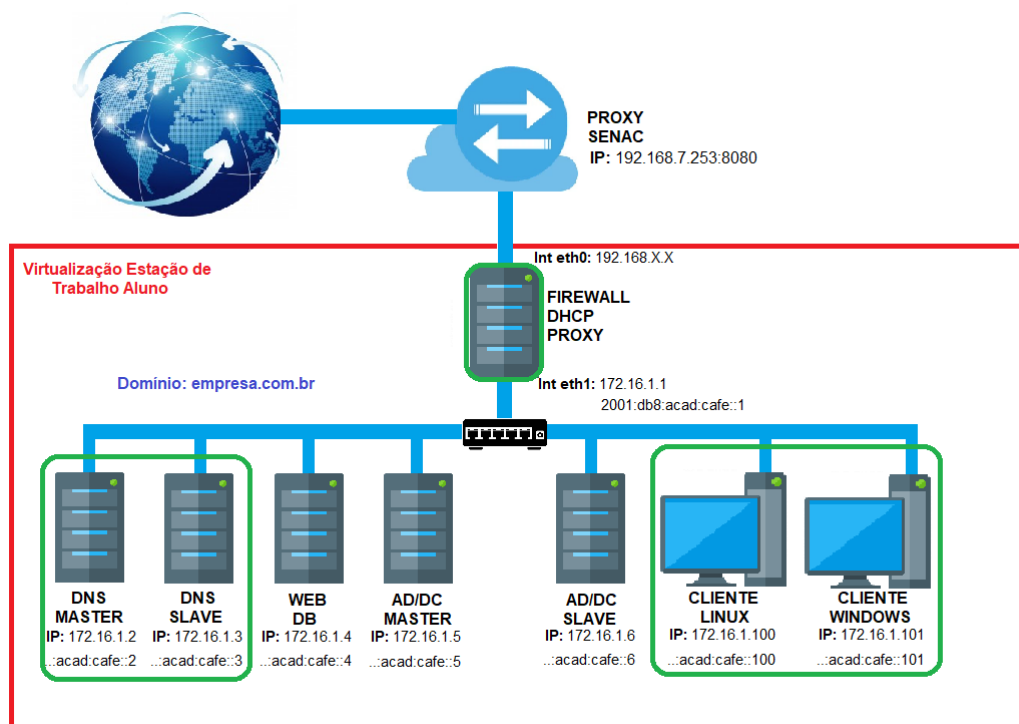
Um Servidor DNS secundário (slave), tem a função de armazenar uma cópia do servidor primário (master), a fim de, responder aos clientes quando o servidor primário, por algum motivo deixar de funcionar.

Nesse sentido, é importante destacar que é altamente recomendado que o servidor primário e o(s) servidor(es) secundário(s) estejam fisicamente em diferentes localizações (redes distintas), visando a disponibilidade dos serviços que o DNS é responsável.

Um servidor DNS pode funcionar como master e slave, de zonas distintas, ao mesmo tempo. Ou seja, na prática, o servidor master de uma empresa pode ser secundário de outra.

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-NS2 - Servidor DNS
- Appl-Debian10-Client ou Appl-Windows7-Client - Testes de resolução de nomes



4.9.2 Ajustes iniciais

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, 172.16.1.3;
```

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

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

4.9.3 Ajustes Máquina Virtual Appl-Debian10-NS2

Verifique os endereços IP da Appl-Debian10-NS2, os endereços deverão ser fixados no arquivo interfaces ou entregues via DHCP como segue:

```
IPv4: 172.16.1.3  
IPv6: 2001:db8:acad:cafe::3
```

Instale o servidor Bind9 e o pacote dnsutils

```
root@ns2:/# apt install bind9 dnsutils
```

Edite o arquivo resolv.conf:

```
root@ns2:/# vim /etc/resolv.conf
```

E defina o IP da máquina server como resolver:

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

4.9.4 Ajustes do Servidor Primário

A fim de identificar o servidor secundário para o domínio "empresax.com.br", será necessário a realização de ajustes no servidor DNS primário.

Ajustes no arquivo "db.empresax.com.br":

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

Insira o seguinte registro, abaixo da linha "@ IN NS ns.empresax.com.br", indicando o servidor DNS secundário para a zona "empresax.com.br":

```
@    IN    NS    ns2.empresax.com.br.
```

No fim do arquivo insira o registro relacionando o nome do servidor secundário a um IP:

```
ns2   IN    A    172.16.1.3
```

Ajustes no arquivo "db.1.16.172":

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

Insira o seguinte registro, abaixo da linha "@ IN NS ns.empresax.com.br", indicando o servidor DNS secundário para a zona "empresax.com.br":

```
@      IN      NS      ns2.empresax.com.br.
```

No fim do arquivo insira o registro relacionando o nome do servidor secundário a um IP:

```
3      IN      PTR      ns2.empresax.com.br.
```

Ajustes no arquivo "named.conf.options":

No laboratório de instalação e configuração do Servidor DNS Primário, vimos que é possível definir dentro do arquivo "named.conf.options" quais servidores DNS Secundários possuem autorização para realizar transferência de zona. Porém devido a possibilidade de um servidor DNS poder responder autoritativamente por diferentes zonas, essas linhas que definem a autorização podem ser inseridas diretamente no arquivo "named.conf.local" definindo os servidores secundários de cada zona criada.

Para realizar esse ajuste, edite o arquivo "named.conf.options":

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

E comente com "//" as três linhas referentes a autorização de transferência de zona:

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

Ajustes no arquivo "named.conf.local":

Como comentado anteriormente, a autorização para transferência de zona, será inserida no arquivo "named.conf.local", as linhas a serem incluídas serão:

- **allow-transfer**: restringe a transferência de zona apenas para Servidores autorizados.
- **notify**: habilita ou não se o servidor primário notificará os servidores secundários quando a informação de zona for atualizada.
- **also-notify**: quais servidores secundários serão notificados.

Para realizar esse ajuste, edite o arquivo "named.conf.local":

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

E insira as linhas em destaque:

```
zone "empresax.com.br" {  
    type master;  
    file "db.empresax.com.br";  
    allow-transfer {172.16.1.3; };  
    notify yes;  
    also-notify {172.16.1.3; };  
};  
  
zone "1.16.172.in-addr.arpa" {  
    type master;  
    file "db.1.16.172";  
    allow-transfer {172.16.1.3; };  
    notify yes;  
    also-notify {172.16.1.3; };  
};
```

Após os ajustes, reinicie o serviço bind9 e posteriormente verifique seu *status*.

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

Teste o funcionamento dos novos registros inseridos:

```
root@ns:/# nslookup ns2.empresax.com.br  
O resultado deverá ser:  
Server: 127.0.0.1  
Address: 127.0.0.1 #53  
Name: ns2.empresax.com.br  
Address: 172.16.1.3
```

```
root@ns:/# ping ns2.empresax.com.br
```

```
root@ns:/# nslookup 172.16.1.3  
O resultado deverá ser:  
Server: 127.0.0.1  
Address: 127.0.0.1 #53  
3.1.16.172.in-addr.arpa name = ns2.empresax.com.br
```

4.9.5 Instalação e configuração do Servidor DNS Secundário

Antes de iniciar a instalação e configuração do servidor DNS Secundário, é importante testar a resolução de nomes a partir da **VM NS2**:

```
root@ns2:/# nslookup ns2.empresax.com.br  
O resultado deverá ser:  
Server: 172.16.1.2  
Address: 172.16.1.2 #53  
Name: ns2.empresax.com.br  
Address: 172.16.1.3
```

```
root@ns2:/# ping ns2.empresax.com.br
```

```
root@ns2:/# nslookup 172.16.1.3
```

O resultado deverá ser:

Server: 172.16.1.2

Address: 172.16.1.2 #53

3.1.16.172.in-addr.arpa name = ns2.empresax.com.br

Edite o arquivo "named.conf.local":

```
root@ns2:/# vim /etc/bind/named.conf.local
```

E insira as seguintes linhas no arquivo:

```
zone "empresax.com.br" {  
    type slave;  
    file "slave/db.empresax.com.br";  
    masters {172.16.1.2;};  
};  
  
zone "1.16.172.in-addr.arpa" IN {  
    type slave;  
    file "slave/db.1.16.172";  
    masters {172.16.1.2;};  
};
```

Certifique que não há erros de parâmetros, verificando as configurações do arquivo através do comando `named-checkconf`:

```
root@ns2:/# named-checkconf
```

Para uma melhor administração do diretório que armazenará os arquivos transferidos do servidor primário, criaremos um diretório denominado "slave" em `/var/cache/bind` e posteriormente definiremos como proprietário desse, o usuário e grupo **bind**:

```
root@ns2:/# mkdir /var/cache/bind/slave
```

```
root@ns2:/# chown bind:bind /var/cache/bind/slave
```

E criaremos um link simbólico denominado "slave" do diretório `/var/cache/bind` dentro do diretório `/etc/bind`.

```
root@ns2:/# ln -sf /var/cache/bind/slave /etc/bind/slave
```

Após os ajustes, reinicie o serviço `bind9` e posteriormente verifique seu *status*.

```
root@ns2:/# systemctl restart bind9
```

```
root@ns2:/# systemctl status bind9
```

Nos logs apresentados pela opção `status`, é possível observar se de fato ocorreu a transferência

de zonas do servidor primário para o secundário, conforme destacado na figura abaixo:

```
root@Client:/home/aluno# systemctl status bind9
● bind9.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/bind9.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2017-09-28 12:32:54 -03; 6s ago
     Docs: man:named(8)
    Main PID: 3493 (named)
      Tasks: 4 (limit: 4915)
   CGroup: /system.slice/bind9.service
           └─3493 /usr/sbin/named -f -u bind

set 28 12:32:54 Client named[3493]: transfer of '1.16.172.in-addr.arpa/IN' from 172.16.1.1#53: Transfer status:
set 28 12:32:54 Client named[3493]: transfer of '1.16.172.in-addr.arpa/IN' from 172.16.1.1#53: Transfer complete
set 28 12:32:54 Client named[3493]: zone 1.16.172.in-addr.arpa/IN: sending notifies (serial 2017072101)
set 28 12:32:54 Client named[3493]: network unreachable resolving './DNSKEY/IN': 2001:500:3::42#53
set 28 12:32:54 Client named[3493]: zone empresa.com.br/IN: Transfer started.
set 28 12:32:54 Client named[3493]: transfer of 'empresa.com.br/IN' from 172.16.1.1#53: connected using 172.16.1
set 28 12:32:54 Client named[3493]: zone empresa.com.br/IN: transferred serial 2017072101
set 28 12:32:54 Client named[3493]: transfer of 'empresa.com.br/IN' from 172.16.1.1#53: Transfer status: success
set 28 12:32:54 Client named[3493]: transfer of 'empresa.com.br/IN' from 172.16.1.1#53: Transfer completed: 1 me
set 28 12:32:54 Client named[3493]: zone empresa.com.br/IN: sending notifies (serial 2017072101)
lines 1-19/19 (END)
```

Por fim, liste o conteúdo do diretório "/etc/bind/slave" e verifique se a réplica dos arquivos "db.empresax.com.br" e "db.1.16.172" estão disponíveis.

```
root@ns2:/etc/bind# ls /etc/bind/slave
db.1.16.172  db.empresax.com.br
root@Client:/etc/bind#
```

4.9.6 Teste de redundância do Serviço de DNS

Nesta seção será realizado os testes de redundância do serviço de DNS, para isso, será utilizada a VM Debian9-Client.

Ajuste o arquivo resolv.conf, de forma que a máquina virtual Client consulte os dois servidores DNS (Master e Slave). Edite o arquivo resolv.conf:

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

E defina o IP da máquina server como resolver:

```
search empresax.com.br
nameserver 172.16.1.2
nameserver 172.16.1.3
```

O primeiro teste a ser realizado é a verificação de quais servidores DNS respondem pela domínio "empresax.com.br, para isso será utilizado o comando **host** como segue:

Note que ao enviar uma consulta, informando o tipo de registro NS, o comando retorna os dois servidores DNS (master e Slave) configurados anteriormente.

Agora com o comando nslookup, faça uma consulta para saber qual IP o nome www.empresax.com.br mapeia:

Note que ao enviar uma consulta ao servidor DNS, a resposta obtida partiu do servidor DNS Primário 172.16.1.2 (destacado na figura).

Para testar a redundância do serviço, desligue o servidor DNS primário (VM Debian10-NS) e

```
root@Client:~# host -t NS empresax.com.br
empresax.com.br name server ns2.empresax.com.br.
empresax.com.br _ name server ns.empresax.com.br.
```

```
root@Client:~# nslookup www.empresax.com.br
Server:      172.16.1.2
Address:     172.16.1.2#53

Name:   www.empresax.com.br
Address: 172.16.1.4
```

posteriormente, com o comando nslookup, faça novamente a consulta para saber qual IP o nome www.empresax.com.br mapeia:

```
root@Client:~# nslookup www.empresax.com.br
Server:      172.16.1.3
Address:     172.16.1.3#53

Name:   www.empresax.com.br
Address: 172.16.1.4
```

Note que ao enviar uma consulta ao servidor DNS, a resposta obtida agora partiu do servidor DNS Secundário 172.16.1.3 (destacado na figura).