Linux Network Servers

DNS – Parte 2

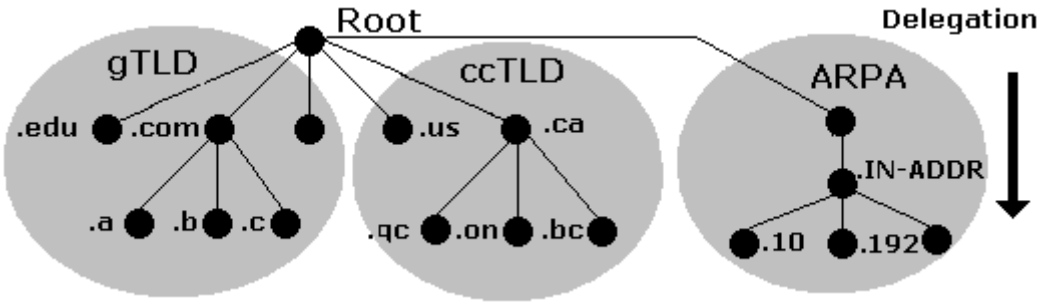
DNS Reverso

O DNS reverso existe como um mecanismo que outros servidores usam para verificarem a autenticidade do seu servidor. Para isso, eles verificam se o endereço IP atual bate com o endereço IP fornecido pelo servidor DNS.

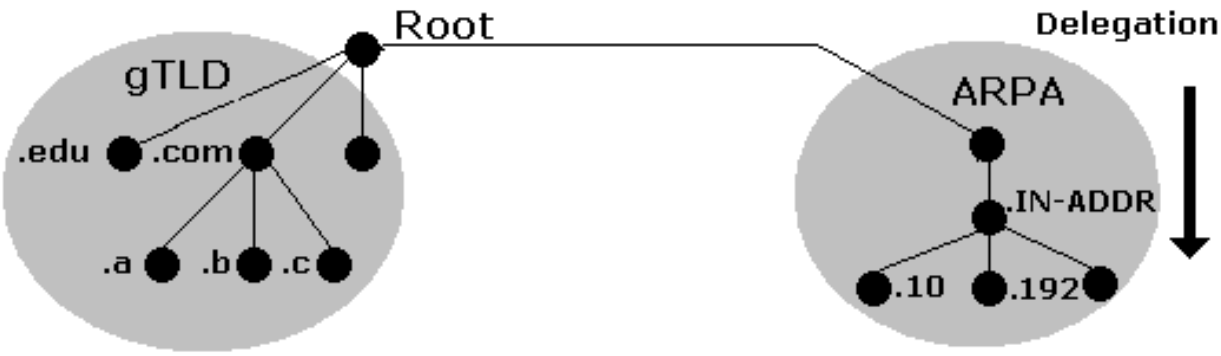
Prática:

```
$ dig mx.uol.com.br
mx.uol.com.br.        1858    IN      A       200.221.29.129

Faça uma busca reversa com o comando dig (use o parâmetro -x
conforme mostrado abaixo):

$ dig -x 200.221.29.129
129.29.221.200.in-addr.arpa. 2301 IN    PTR     mx.uol.com.br.
```

Observe na imagem abaixa como é feita a consulta do DNS reverso (veja que parte de ARPA até o endereço final, da raiz até o ramo):



Linux Network Servers



Configurando o reverso:

```
# vim /etc/bind/named.conf.local
```

```
zone "0.168.192.in-addr.arpa" {
  type master;
  file "/etc/bind/db.192.168.0.rev";
};
```

Nesse exemplo, o endereço IP do servidor reverso é 192.168.0.1. A regra é tirar o último octeto e escrevermos o resto do endereço de trás para frente, por isso temos: zone "0.168.192.in-addr.arpa".

Linux Network Servers

Edite o arquivo /etc/bind/db.192.168.0.rev

Observação: O nome do arquivo fica a seu critério, desde que você faça referência a ele corretamente no arquivo /etc/bind/named.conf.local.

```
$TTL 86400
@       IN      SOA ns.teste-ht.com.br.         root.teste-ht.com.br.(
                        2008080901;          serial
                        8h;                 refresh
                        1h;                 retry
                        3d;                 expire
                        3d );               default_ttl

        IN      NS      ns.teste-ht.com.br.
1       IN      PTR     www.teste-ht.com.br.
```

Observe a última linha desse arquivo:

```
1               IN      PTR     www.teste-ht.com.br.
```

PTR – Significa apontador de nome reverso. No início da linha você colocará somente o número do último octeto do IP.

Faça uma consultado a partir da própria máquina servidora:

```
$ dig @127.0.0.1 -x 192.168.0.1
```

Linux Network Servers

Agora, será mostrado como usar um servidor secundário.

Nesse cenário, existem dois servidores: um será o **master** e outro **slave**. Esses dois servidores devem ser colocados em redes diferentes para que realmente exista redundância. A vantagem disso é que se o servidor primário sair do ar, o secundário faz o papel do primário enquanto ele é arrumado.

No primário deve ter uma diretiva chamada "allow-transfer".

Abra o arquivo /etc/bind/named.conf.local

```
# vim /etc/bind/named.conf.local

zone “teste-ht.com.br” {
            type master;
        file “/etc/bind/db.teste-ht”;
};
```

Será feita uma pequena alteração!

Abaixo da diretiva "file" vai ser colocada a diretiva "allow-transfer".

Abra o arquivo /etc/bind/named.conf.local

```
# vim /etc/bind/named.conf.local

zone “teste-ht.com.br” {
            type master;
            file “/etc/bind/db.teste-ht”;
            allow-transfer { 10.0.0.2; };
};
```

No qual, 10.0.0.2 é o IP do secundário!

Linux Network Servers

No secundário deve ser feito as seguintes alterações:

```
zone "teste-ht.com.br" {
        type slave;
        file "db.teste-ht";
        masters { 10.0.0.1; };
};
```

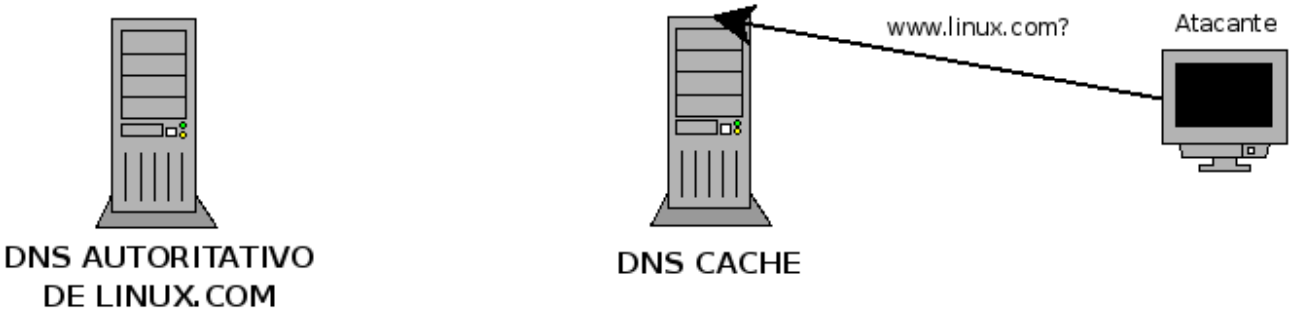
Eis uma boa questão: “E se eu tiver um firewall o que eu tenho que fazer?”

Devem ser liberadas as portas 53 (TCP E UDP) tanto na saída quanto na entrada.

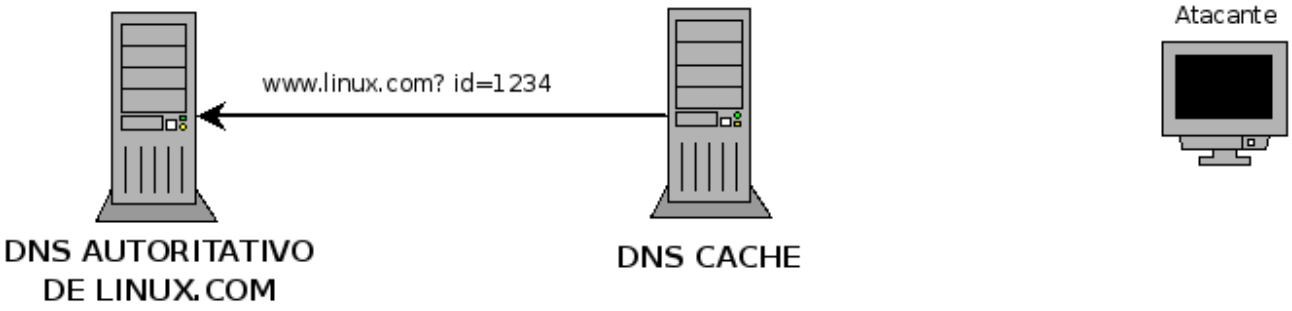
Cuidados com a segurança do servidor:

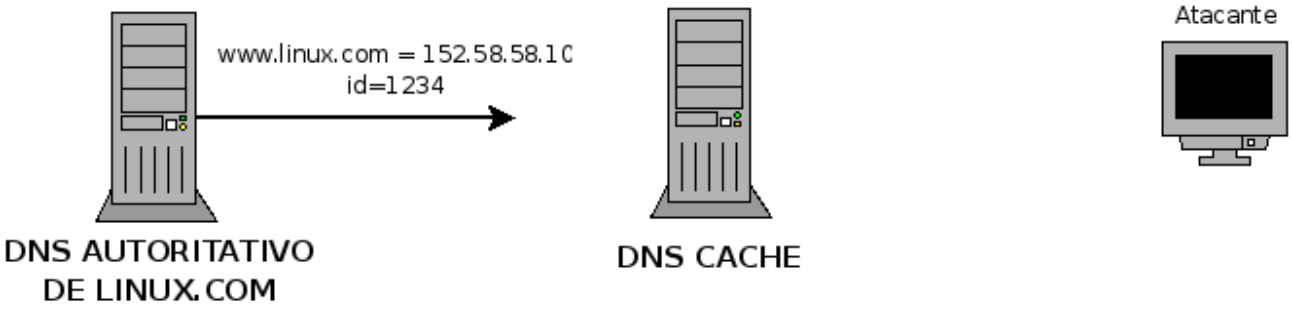
O BIND é configurado por padrão para aceitar consultadas de outros domínios (recursividade). Ele vem com a opção recursion yes. O DNS não responde apenas pelos domínios pelos quais ele tem autoridade, mas também funciona como cache.

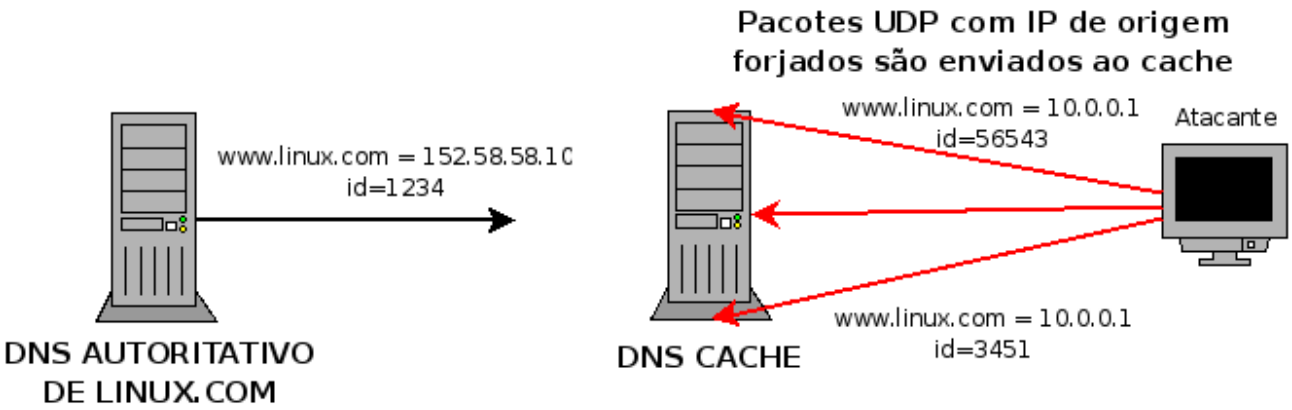
Se um servidor DNS vai ser usado além da rede local, é muito importante desabilitar a opção “recursion yes”. Com essa mudança, evita-se ataques do tipo DNS Poisoning, que acontece quando um cliente externo insere uma informação inválida no cache do DNS. Veja como isso seria feito abaixo nas imagens:



Linux Network Servers







Linux Network Servers

Proteger contra recursão

Tente consultar o DNS do site www.uol.com.br antes de proibir a recursão:

```
$ dig @127.0.0.1 www.uol.com.br
```

```
www.uol.com.br.        300     IN      A       200.98.249.120
www.uol.com.br.        300     IN      A       200.221.2.45
uol.com.br.            3600    IN      NS      borges.uol.com.br.
uol.com.br.            3600    IN      NS      eliot.uol.com.br.
```

Edite o arquivo: /etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";
        recursion no;
        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Salve o arquivo e reinicie o daemon do DNS:

```
# /etc/init.d/bind9 stop
# /etc/init.d/bind9 start

Repita a consulta após a alteração:
$ dig @127.0.0.1 www.uol.com.br
```

Compare com a consulta anterior.