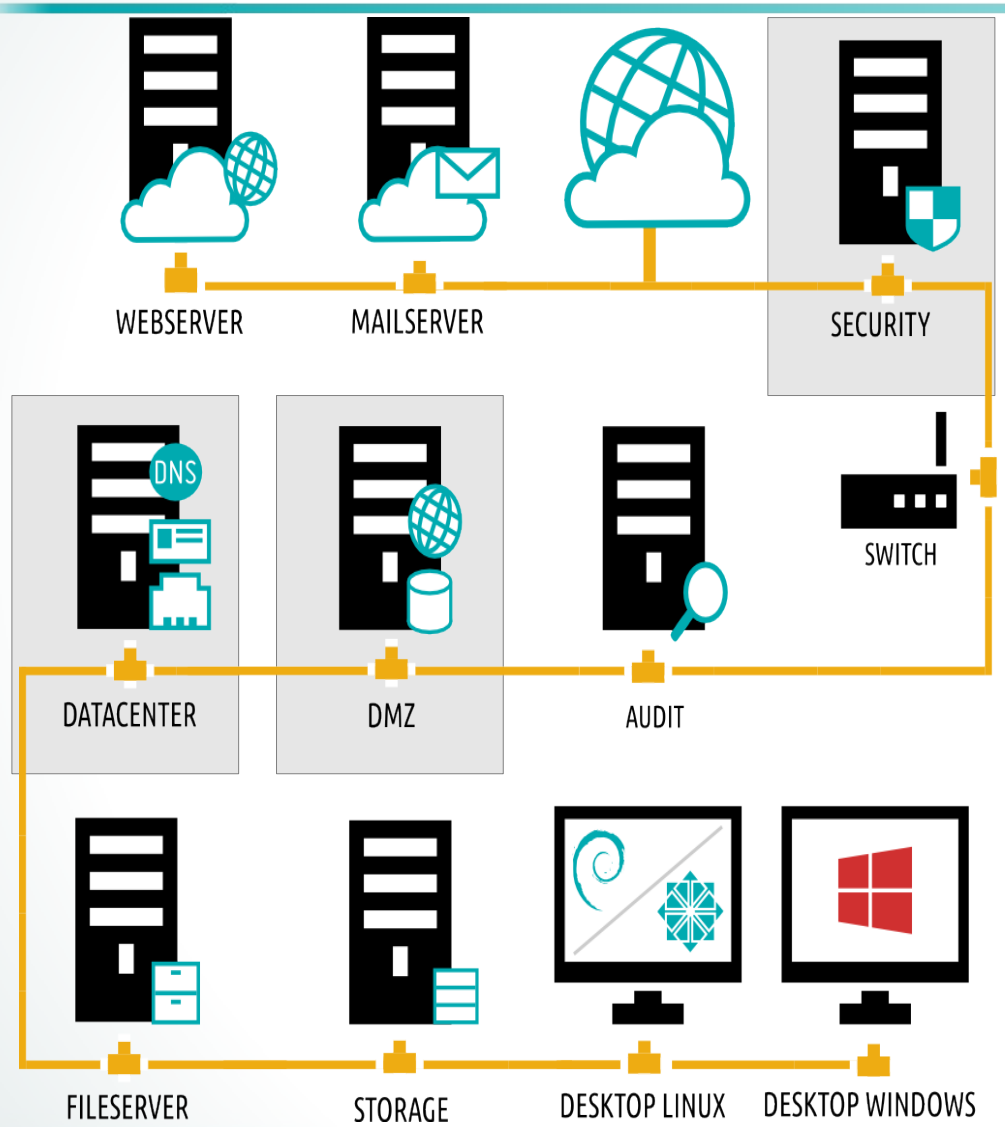

4LINUX
FREE SOFTWARE SOLUTIONS

Só na 4Linux você aprende MUITO MAIS!

Servidor DNS

iT EXPERIENCE



Nesta Aula:

- DataCenter – Local

  Acesso pelo VirtualBox

  SO: Debian Linux

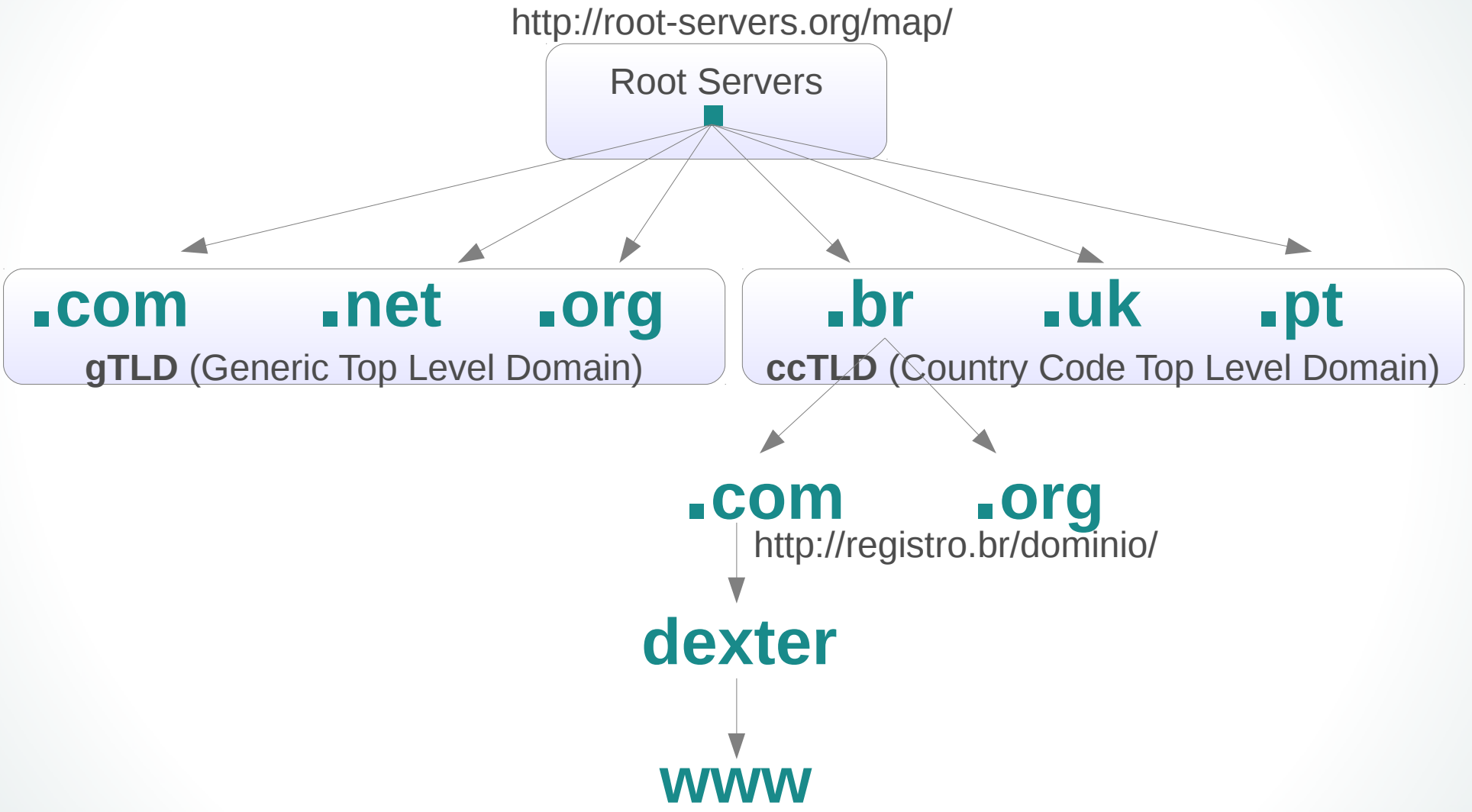
Servidor DNS

- DNS – Domain Name Server;
- Responsável pela resolução de Nome para IP e de IP para Nome;
- Criado e mantido pelo ISC (Internet System Consortium), mesmo grupo que mantém DHCP e NTP;
- Eles são divididos em "**gTLD**" (domínios genéricos "com", "edu", "gov", "mil", etc) e "**ccTLD**" (códigos de países ou "country-code", sempre com duas letras);
- A ICANN delega, de acordo com tratados internacionais, a responsabilidade pela administração de um "ccTLD";
- No caso do Brasil, essa responsabilidade pertence atualmente ao "CGI.br", mais especificamente ao "REGISTRO.br";

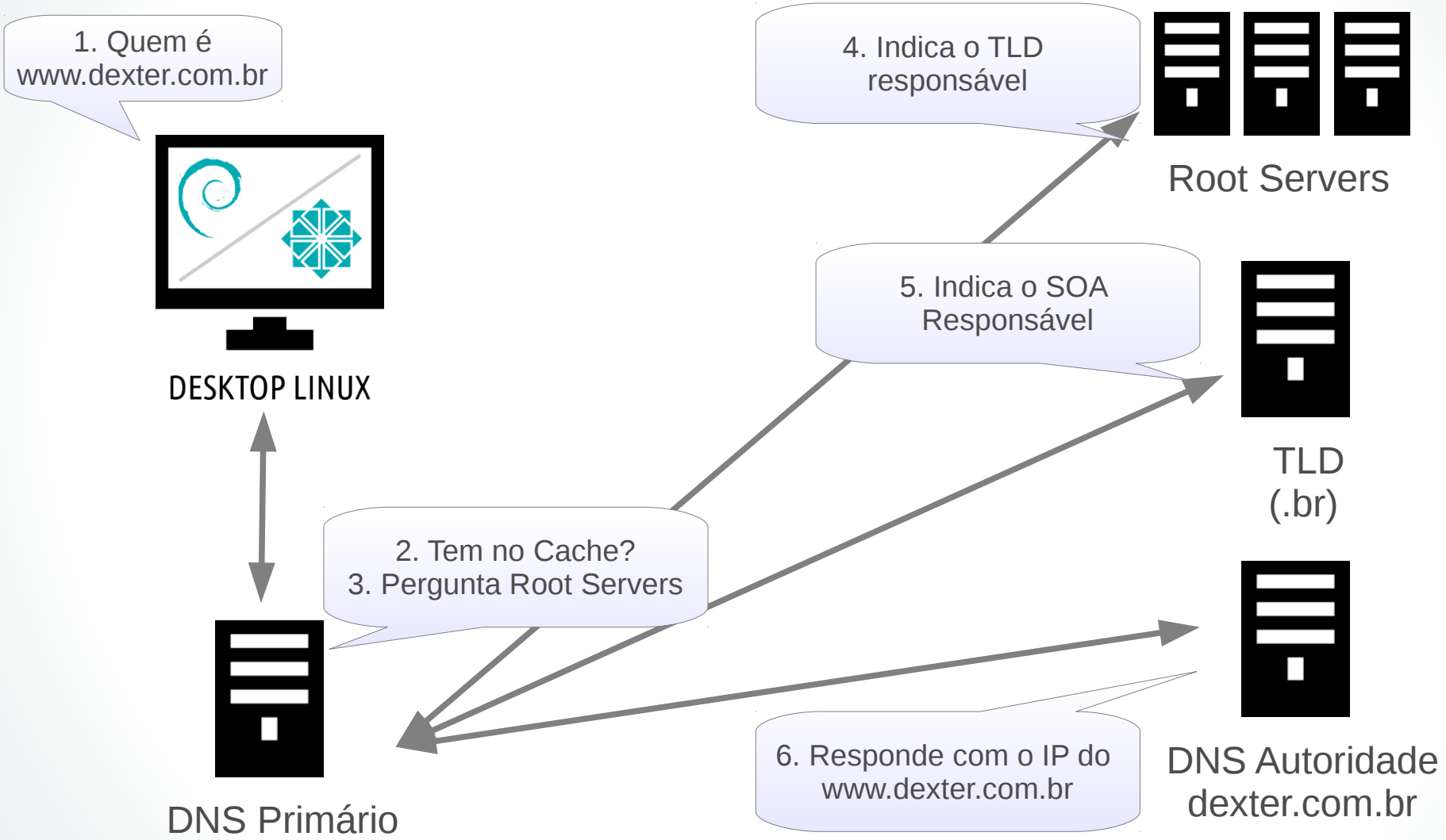
iT EXPERIENCE

- Dois servidores, o primário e o secundário, devem ter um mecanismo configurado corretamente para que eles se mantenham sincronizados;
- O DNS reverso deve estar configurado;
- O servidor deve trabalhar de forma autoritativa, responsável apenas pelos domínios dexter.com.br e mandark.com.br;
- Configurar o servidor primário para notificar o secundário quando houver atualização na zona;
- Restringir acesso apenas para a Rede Interna realizar Consulta recursiva;
- Restringir acesso apenas para o Servidor Secundário realizar transferência de Zona.

Servidor DNS



Servidor DNS



Servidor DNS

- Tipos de Registros do DNS:

SOA → Start Of Authotity - Indica onde começa a autoridade da zona;

NS → Name Server - Indica um servidor de nomes para a zona;

A → Address - Mapeamento de nome a endereço (IPv4);

AAAA → Address - Mapeamento de nome a endereço (IPv6);

MX → Mail eXchanger - Indica um servidor de email;

CNAME → Canonical Name (Alias) - Mapeia um nome alternativo (apelido);

PTR → Pointer Record (IP reverso);

TXT → Text – Permite incluir uma entrada de texto curto. Mais usado para SPF.

Servidor DNS

- Cliente DNS:

```
1# cat /etc/resolv.conf

2# host google.com

3# host -t MX google.com

4# host -t A webmail.4linux.com.br

5# host -t txt google.com

6# dig @8.8.8.8 -t txt google.com
```

Servidor DNS

- Servidor DNS:

```
1# aptitude install bind9
2# cd /etc/bind/
3# ls
4# cat db.root
5# cat named.conf.default-zones
6# cat named.conf.options
```

Servidor DNS

- Servidor DNS – Cache Only:

```
1# vim /etc/resolv.conf

   nameserver 127.0.0.1

2# host google.com

3# apt-get update
```

Servidor DNS

```
1# vim named.conf.local
   zone "dexter.com.br" {
        type master;
        file "db.dexter";
   };

2# cd /var/cache/bind

3# vim db.dexter
```

Servidor DNS

```
$TTL 86400
@   IN      SOA    ns1.dexter.com.br.  root.dexter.com.br. (
        2013010101; serial
        8h ; refresh
        1h ; retry
        3d ; expire
        3h ); negative caching ttl

@           IN      NS          ns1.dexter.com.br.
@           IN      MX  10      mail.dexter.com.br.
@           IN      A           192.168.X.2
ns1         IN      A           192.168.X.2
www         IN      A           192.168.X.2
intranet    IN      CNAME       www
mail        IN      A           192.168.X.2
```

Servidor DNS

```
1# named-checkzone dexter.com.br /var/cache/bind/

2# tail -f /var/log/daemon.log > /dev/tty2 &

3# /etc/init.d/bind9 stop

4# /etc/init.d/bind9 start

4# dig -t soa dexter.com.br

5# host dexter.com.br

6# host intranet.dexter.com.br
```

Servidor DNS

- Explorando a ferramenta RNDC:

```
1# rndc status
2# rndc reload
3# host uol.com.br
4# rndc dumpdb -cache
5# cat /var/cache/bind/named_dump.db
6# grep uol /var/cache/bind/named_dump.db
7# rndc flush
```

Transferência de Zona

- Transferência de Zona consiste no Servidor DNS Primário passar toda a configuração de uma determinada Zona;
- Pensando em Segurança, essa ação sempre deve ser restrita a apenas servidores DNS autorizados a receber as suas configurações;
- É muito comum SysAdmins deixarem a Transferência de Zona aberta no Servidor causando uma brecha de segurança.

```
1# dig dexter.com.br axfr
```

Transferência de Zona

- Protegendo seu DNS:

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

   zone "dexter.com.br" {
           type master;
           file "db.dexter";
           allow-transfer { 192.168.X.3; };
           notify yes;
           also-notify { 192.168.X.3; };
   };

2# /etc/init.d/bind9 restart

3# dig dexter.com.br axfr
```

allow-transfer Restringir a transferência de zona apenas para Servidores Autorizados;

As opções **notify** e **also-notify** determinam se o servidor primário notifica servidores secundários quando a informação de zona for atualizada.

Servidor DNS

DNS Reverso

- DNS reverso é um recurso que permite que outros servidores verifiquem a autenticidade do seu servidor. Para isso, ele checa se o endereço IP atual bate com o endereço IP informado pelo servidor DNS.

```
1# host mail.dexter.com.br
2# host 192.168.X.2
3# vim /etc/bind/named.conf.local
        zone "X.168.192.in-addr.arpa" {
            type master;
            file "rev.dexter";
        };
```

Servidor DNS

DNS Reverso

```
# vim /var/cache/bind/rev.dexter
$TTL 86400
@       IN      SOA    ns1.dexter.com.br.     root.dexter.com.br.(
        2013010101; serial
        8h; refresh
        1h; retry
        3d; expire
        3d ); negative cache ttl

@       IN      NS          ns1.dexter.com.br.
ns1     IN      A           192.168.X.2
2       IN      PTR         mail.dexter.com.br
```

Servidor DNS

DNS Reverso

```
1# /etc/init.d/bind9 restart

2# host mail.dexter.com.br

3# host 192.168.X.2
```

Servidor DNS

DNS Secundário

- Os servidores DNS Secundários ajudam a fornecer equilíbrio de carga e tolerância a falhas. Os servidores DNS secundários mantêm uma cópia somente leitura dos dados da zona transferidos periodicamente do servidor DNS Primário.

```
1# yum install bind

2# vim /etc/named.conf

        include “/etc/named.conf.local”
```

Servidor DNS

DNS Secundário

```
1# vim /etc/named.conf.local
      zone "dexter.com.br" {
         type slave;
         masters { 192.168.X.2; };
         file "/var/named/slaves/db.slave.dexter";
      };
2# /etc/init.d/named restart
3# ls /var/named/slaves/
4# cat /var/named/slaves/db.slave.dexter
```

DNS Recursivo

- DNS Recursivo é a funcionalidade que o DNS possui por padrão de realizar consultas para todos os domínios mesmo que ele não seja o Servidor autoritativo daquele domínio;
- Para evitar abuso em Servidores DNS que ficam disponível na Internet é importante limitar a recursividade apenas para redes autorizadas;

```
1# host 8.8.8.8
2# dig @8.8.8.8 -t a uol.com.br
3# host ns1.google.com
4# dig @216.239.32.10 -t a uol.com.br
```

Servidor DNS

DNS Recursivo

```
1# vim /etc/bind/named.conf.options
   options {
      directory "/var/cache/bind";
      allow-recursion { 127.0.0.1; 192.168.X.0/24; };
      allow-query { 127.0.0.1; 192.168.X.0/24; };
      auth-nxdomain no;
      listen-on-v6 { any; };
};

2# /etc/init.d/named restart
```

Laboratório Dexter

- Configure uma nova Zona no Servidor DNS do Servidor DataCenter para o domínio mandark.com.br;
- Libere transferência de Zona apenas para o Servidor DNS Secundário na máquina DMZ;
- No Servidor DMZ configure o DNS Secundário do domínio mandark.com.br;

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

Pergunta LPI

Usando apenas comandos presentes no named, qual é o comando, com opções ou parâmetros para fazer com que o named releia os arquivos de zona?

Resposta: _____

Os usuários de uma rede local se queixam de que a resolução de nomes não é rápido o suficiente. Insira o comando, sem o caminho ou opção, que mostra o tempo necessário para resolver uma consulta DNS.

Resposta: _____

Pergunta LPI

Usando apenas comandos presentes no named, qual é o comando, com opções ou parâmetros para fazer com que o named releia os arquivos de zona?

Resposta: _____ **Resposta: rndc reload**

Os usuários de uma rede local se queixam de que a resolução de nomes não é rápido o suficiente. Insira o comando, sem o caminho ou opção, que mostra o tempo necessário para resolver uma consulta DNS.

Resposta: _____ **Resposta: dig**


4LINUX
FREE SOFTWARE SOLUTIONS