

Trabalho Prático Nº.3 – Serviço de Resolução de Nomes (DNS)

Duração: 3 aulas

Parte I: Consultas ao serviço de nomes DNS

A maioria dos sistemas operativos (Windows, Linux, etc) inclui um cliente DNS genérico designado por “nslookup”. No entanto este cliente tem vindo a ser preterido a favor de outros como o “dig” e o “host”. O package “dnsutils” que está instalado na máquina virtual *Xubuncore* inclui todos. Se não conseguir usar nenhum deles tente reinstalar o package com o comando:

```
$ sudo apt-get install dnsutils
```

A forma mais simples de verificar se estão instalados é testar com uma interrogação simples, como por exemplo obter o endereço IP do servidor WWW da Universidade do Minho:

```
$ host www.uminho.pt
$ dig www.uminho.pt
$ nslookup www.uminho.pt
```

Com base no manual das aplicações (ex: `man nslookup` ou `man dig`) e no material de suporte procure responder às seguintes questões:

- Qual o conteúdo do ficheiro `/etc/resolv.conf` para que serve essa informação?
- Os servidores **www.sapo.pt.** e **www.yahoo.com.** têm endereços IPv6? Se sim, quais?
- Quais os servidores de nomes definidos para os domínios: “**uminho.pt.**”, “**pt.**” e “**.**”?
- Existe o domínio **nice.software.**? Será que **nice.software.** é um *host* ou um *domínio*?
- Qual é o servidor DNS primário definido para o domínio **msf.org.**? Este servidor primário (*master*) aceita queries recursivas? Porquê?
- Obtenha uma resposta “*autoritativa*” para a questão anterior.
- Onde são entregues as mensagens de correio eletrónico dirigidas aos presidentes **marcelo@presidencia.pt** e **bolsonaro@casacivil.gov.br**?
- Que informação é possível obter, via DNS, acerca de **whitehouse.gov**?
- Consegue interrogar o DNS sobre o endereço IPv6 **2001:690:a00:1036:1113::247** usando algum dos clientes DNS? Que informação consegue obter? Supondo que teve problemas com esse endereço, consegue obter um contacto do responsável por esse IPv6?
- Os secundários usam um mecanismo designado por “Transferência de zona” para se atualizarem automaticamente a partir do primário, usando os parâmetros definidos no Record do tipo SOA do domínio. Descreve sucintamente esse mecanismo com base num exemplo concreto (ex: **di.uminho.pt** ou o domínio **cc.pt** que vai ser criado na topologia virtual).

Parte II: Instalação, configuração e teste de um domínio CC.PT

Pretende-se que crie um domínio **CC.PT** para a topologia de rede que estamos a usar nas aulas práticas (CC-Topo-2020.imn), de modo a que se possam usar os nomes em vez dos endereços IP. No final deve, por exemplo, poder fazer-se “*ping Serv1.cc.pt*” ou mesmo apenas “*ping Serv1*” ou “*ping Serv1.cc.pt*” em vez de “*ping 10.3.3.1*”. Consulte os slides das aulas teóricas e os manuais do software BIND9 que vamos utilizar (*manpages unix* e manuais online) ou então tutoriais específicos para o sistema operativo Ubuntu (e.g. Google ‘bind9 ubuntu’):

- <https://help.ubuntu.com/community/BIND9ServerHowto>
- <https://help.ubuntu.com/lts/serverguide/dns.html>
- <https://www.isc.org/bind-9-11-arm/>

Antes de começar certifique-se que o software BIND9 está instalado (`sudo apt-get install bind9`). Este pacote vem já pré-configurado de base (ficheiros em `/etc/bind`) pelo que o número de alterações a efetuar é mínimo.

Preparativos especiais para ambiente CORE

Passo 1) replicar ficheiros de configuração

Para não criar conflitos, e uma vez que todos os nós da topologia CORE usam na realidade o mesmo *filesystem*, o primeiro passo é copiar os ficheiros de configuração para uma nova pasta. Sugere-se que use por exemplo **\$HOME/primario**, para o primário e **\$HOME/secundario** para o servidor secundário, onde \$HOME é a diretoria *default* do utilizador (no caso do user *core*, será /home/core):

```
$ rsync -av /etc/bind/ ~/primario/
$ rsync -av /etc/bind/ ~/secundario/
Nota: as "/" no fim são importantes e o ~ é na verdade a $HOME do utilizador actual... (se não sabe quem é, escreva "who am i" ☺ resulta...)
$ cd ~/primario; ls;
bind.keys      db.255        db.root        named.conf.local
db.0           db.empty     named.conf      named.conf.options
db.127         db.local     named.conf.default-zones zones.rfc1918
$ cd ~/secundario; ls;
...
```

Passo 2) parar o servidor DNS pré-instalado

```
$ sudo /etc/init.d/bind9 status
$ sudo /etc/init.d/bind9 stop
```

Passo 3) reconfigurar *apparmor* para permitir que /usr/sbin/named aceda a ficheiros noutros locais

O *kernel*/Linux inclui um sistema de proteção para evitar que alguns programas acedam a ficheiros que não devem! Para isso deve-se verificar se o *daemon* respetivo (*named*) consta na lista de perfis controlados pelo *apparmor*:

```
$ sudo /etc/init.d/apparmor status
...
```

Neste caso vamos ter de reconfigurar essas permissões para que o /usr/sbin/named possa ler as novas directorias:

➔ Editar o ficheiro /etc/apparmor.d/usr.sbin.named com vista a acrescentar duas novas linhas de permissões:

```
...
# See /usr/share/doc/bind9/README.Debian.gz
/etc/bind/** r,
/home/core/primario/** r,
/home/core/secundario/** r,
...
```

➔ Parar e reiniciar o *apparmor*:

```
$ sudo /etc/init.d/apparmor stop
$ sudo /etc/init.d/apparmor start
$ sudo /etc/init.d/apparmor status
```

2.1 Configuração do servidor primário

As configurações a fazer devem respeitar as seguintes regras:

- os dados do domínio **cc.pt** devem ser editados/mantidos no ficheiro **db.cc.pt**
- os dados do domínio reverso **3.3.10.in-addr.arpa**, relativos à rede 10.3.3.0/24 devem ser editados/mantidos no ficheiro **db.3-3-10.rev** (aplicar sempre o mesmo critério de nomes a outros domínios reversos que decida incluir)
- o servidor primário do domínio é o "**Serv1**" com endereço 10.3.3.1, também designado por **dns.cc.pt**, tendo como secundário o "**Hermes**" com endereço 10.4.4.1, com alias **dns2.cc.pt**. O administrador do domínio é o **grupoXX@cc.pt** (onde XX é o número do grupo).
- O domínio tem também um servidor Web (www.cc.pt) e um servidor de e-mail principal (mail.cc.pt) em **Serv3**. O servidor *pop* e *imap* é o **Serv2**, que é também servidor secundário do e-mail para o domínio;
- Sem prejuízo de outros registos que se possam considerar, devem estar registados também o **Portatil1.cc.pt** com alias **GrupoXX.cc.pt** onde XX é o número do grupo, e **Hermes.cc.pt**, **Atena.cc.pt** e **Zeus.cc.pt** no domínio de nomes e no domínio reverso.

Passos a seguir (pode ser feito tudo fora da topologia virtual do CORE, usando o CORE apenas para testes):

- 1) Editar o ficheiro `/etc/hosts` para incluir os registos `10.3.3.1 Serv1 dns.cc.pt` do primário e `10.4.4.1 Hermes dns2.cc.pt` do secundário; este passo é obrigatório para que os servidores DNS se identifiquem corretamente a si próprios;
- 2) Editar o ficheiro `primario/named.conf.options` por forma a incluir os servidores `193.136.9.240` e `193.136.19.1` (servidores do DI) como *forwarders*;
- 3) Editar o ficheiro `primario/named.conf` para incluir a indicação das novas zonas "*cc.pt*", "*3.3.10.in-addr.arpa*" etc (ver exemplos em `named.conf.default-zones`) e corrigir os nomes das diretorias, substituindo `/etc/bind/` pela nova diretoria (`/home/core/primario` ou outra equivalente). Não esquecer de incluir uma cláusula "*allow-transfer*" a dar permissão de transferência da base de dados ao servidor secundário.
- 4) Baseando-se por exemplo no conteúdo do ficheiro `primario/db.local`, procure criar o ficheiro de dados do domínio de nomes: `primario/db.cc.pt` (incluir a informação de acordo com as regras definidas acima)
- 5) Baseando-se por exemplo no conteúdo do ficheiro `primario/db.127` procure criar o ficheiro de dados do(s) domínio(s) de reverse: `primario/db.3-3-10.rev` (ou outros, de acordo com as regras definidas acima);
NOTA: o símbolo "@" é uma abreviatura do domínio que o ficheiro contém (ex: cc.pt); os nomes que não terminam com "." são considerados relativos ao domínio do ficheiro; www.cc.pt sem o ponto é na verdade www.cc.pt.cc.pt
- 6) Testar as configurações e os ficheiros de dados com auxílio de algumas ferramentas

```
$ /usr/sbin/named-checkconf -z /home/core/primario/named.conf
Verifica a configuração toda e tenta carregar os ficheiros de dados... reporta erros se os houver... corrigir todos os erros reportados!

$ /usr/sbin/named-checkzone cc.pt /home/core/primario/db.cc.pt
$ /usr/sbin/named-checkzone 3.3.10.in-addr.arpa /home/core/primario/db.3-3-10.rev
Verifica os ficheiros de zona... man named-checkzone para ver o manual... ou man named-checkconf ...
```

- 7) Executar o servidor, na linha de comando, fazendo por exemplo:

```
$ sudo /etc/init.d/bind9 stop
Pára o named que já possa estar a correr... no arranque do sistema... substituir stop por status para ver o estado...

$ sudo /usr/sbin/named -c /home/core/primario/named.conf -g
O parâmetro -g serve para ficar pendurado na linha de comando, dando output no terminal em vez de no ficheiro /var/log/syslog..
```

2.2 Configuração do cliente e teste do primário

Teste simples com nslookup:

```
$ nslookup - 127.0.0.1
> www.cc.pt
Interroga o servidor de nomes em 127.0.0.1 (ou seja no localhost)
```

Depois do teste passar, fora do emulador CORE, repetir os testes na topologia CORE:

- Iniciar o core com a topologia *CC-Topo-2020.imn*;
- Abrir uma bash no nó "**Serv1**" e executar o comando de arranque do servidor:

```
sudo /usr/sbin/named -c /home/core/primario/named.conf -g
```

- Abrir uma bash no nó "**Cliente1**" e testar uma *query* ao servidor primário:

```
$ nslookup - 10.3.3.1
> www.cc.pt
```

```
... ou ...
$ nslookup www.cc.pt. 10.3.3.1
...
```

- modificar o `/etc/resolv.conf` (editar fora do CORE) e testar de novo com nslookup ou dig:

```
$ cat /etc/resolv.conf
    nameserver 10.3.3.1
    domain cc.pt
    search cc.pt
$ nslookup www.cc.pt
$ dig www.cc.pt
```

2.3 Configuração do servidor secundário

Passos a seguir (ficheiros podem ser editados fora do CORE, mas teste deve ser feito numa *bash* no nó **Hermes**):

- 1) Editar o ficheiro `secundario/named.conf.options` por forma a incluir os servidores 193.136.9.240 e 193.136.19.1 (servidores do DI) como *forwarders*;
- 2) Editar o ficheiro `secundario/named.conf` para incluir a indicação das novas zonas “*cc.pt*”, “*3.3.10.in-addr.arpa*” etc, mas desta vez apenas como zonas do tipo “*slave*” (ver manual ou exemplos). Não se esqueça de cláusula “*masters*” adequada. Assegure-se que os ficheiros de dados das zonas vão para `/var/cache/bind/...{db.cc.pt, db.3-3-10.rev, etc.}` por causa das permissões de escrita! Não os copie! O servidor secundário terá de os transferir e atualizar automaticamente!

- 3) Testar as configurações e os ficheiros de dados com auxílio de algumas ferramentas

```
$ /usr/sbin/named-checkconf -z /home/core/secundario/named.conf
Verifica a configuração...
```

- 4) Executar o core e abrir um bash no nó **Hermes**. Executar o servidor, na linha de comando, fazendo por exemplo:

```
$ sudo /usr/sbin/named -c /home/core/secundario/named.conf -g
Nota: verificar se os dados foram transferidos do primário para o secundário
```

- 5) Teste simples com nslookup, em qualquer nó da topologia:

```
$ nslookup - 10.4.4.1
> www.cc.pt
$ nslookup www.cc.pt. 10.4.4.1
(...)
```