Trabalho Prático Nº3 – 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 *XubunCore7* inclui todos. Se não conseguir usar nenhum deles tente reinstalar o package com o comando:

```
$ sudo apt install bind9 bind9-dnsutils 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: `mannslookup` ou `man dig`) e no material de suporte procure responder às seguintes questões:

a) Qual o conteúdo do ficheiro */etc/resolv.conf* e para que serve essa informação?
b) Os servidores `www.uminho.pt.` e `www.ubuntu.com.` têm endereços IPv6? Se sim, quais?
c) Quais os servidores de nomes definidos para os domínios: "`sapo.pt.`", "`pt.`" e "`.`"?
d) Existe o domínio `open.money.`? Será que `open.money.` é um *host* ou um *domínio*?
e) Qual é o servidor DNS primário definido para o domínio `un.org.`? Este servidor primário (*master*) aceita queries recursivas? Porquê?
f) Obtenha uma resposta "*autoritativa*" para a questão anterior.
g) Onde são entregues as mensagens de correio eletrónico dirigidas a `presidency@eu.eu` ou `presidencia@2021portugal.eu`?
h) Que informação é possível obter, via DNS, acerca de `gov.pt`?
i) Consegue interrogar o DNS sobre o endereço IPv6 `2001:690:2080:8005::38` 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?
j) 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-2021.imn`), de modo a que se possam usar os nomes em vez dos endereços IP. No final deve, por exemplo, poder fazer-se "*ping Marte.cc.pt*" ou mesmo apenas "*ping Marte*" ou "*ping Marte.cc.pt.*"em vez de "*ping 10.2.2.1*". 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://ubuntu.com/server/docs/service-domain-name-service-dns
- https://help.ubuntu.com/community/BIND9ServerHowto
- https://bind9.readthedocs.io/en/latest/

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) ver se o servidor DNS pré-instalado está em execução, parando-o de seguida se necessário

```
$ sudo systemctl status bind9.service
$ sudo systemctl stop bind9.service
```
…confirmar se parou mesmo…
```
$ sudo systemctl status bind9.service
```

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 systemctl status apparmor.service
```
…
Neste caso vamos ter de reconfigurar essas permissões para que o /usr/sbin/named possa ler as novas directorias:

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

```
… (usar um editor de texto, como root, exemplo: sudo vim /etc/apparmor.d/usr.sbin.named )
 # 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 systemctl restart apparmor.service
$ sudo systemctl status apparmor.service
```

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 **1.1.10.in-addr.arpa.** relativos à rede 10.1.1.0/24 devem ser editados/mantidos no ficheiro **db.1-1-10.rev** (aplicar sempre o mesmo critério de nomes a outros domínios reversos que decida incluir)
- o servidor primário do domínio é o "**Server1**" com endereço 10.1.1.1, também designado por **ns.cc.pt**, tendo como secundário o "**Mercurio**" com endereço 10.2.2.2, com alias **ns2.cc.pt**. O administrador do domínio é o **PLYYGXX@cc.pt** (onde YY é o número do turno PL e XX é o número do grupo, ex: PL01G01).

- O domínio tem também um servidor Web (www.cc.pt) e um servidor de e-mail principal (mail.cc.pt) em **Server2**. O servidor *pop* e *imap* é o **Server3**, 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 **Laptop1.cc.pt** com alias **gXX.cc.pt** onde XX é o número do grupo, e **Marte.cc.pt, Mercurio.cc.pt** e **Venus.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 `10.1.1.1 Server1 ns.cc.pt` do primário e `10.2.2.2 Mercurio ns2.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*", "*1.1.10.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.1-1-10.rev` (ou outros, de acordo com as regras definidas acima);
NOTA: o simbolo "@" 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 1.1.10.in-addr.arpa /home/core/primario/db.1-1-10.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 systemctl stop bind9.service
```
Pára o named que já possa estar a correr... no arranque do sistema... substituir a palavra "stop" por "status" para ver o estado, ou por "disable" se pretender desativar de vez o arranque automático do serviço de DNS neste sistema Ubuntu.

```
$ 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-2021.imn*;

- Abrir uma bash no nó "**Server1**" e executar o comando de arranque do servidor:

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

- Abrir uma bash no nó "**Laptop1**" e testar uma *query* ao servidor primário:

```
$ nslookup - 10.1.1.1
> www.cc.pt
... ou ...
$ nslookup www.cc.pt. 10.1.1.1
...
```

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

(nota: esta opção pode não ser necessária; evitar editar o/etc/resolv.conf se estiver na sua máquina de trabalho Linux nativa; caso edite o ficheiro para efeitos deste trabalho, pode voltar a repor o conteúdo original, se o copiar previamente para outro local)

```
$ cat /etc/resolv.conf
      nameserver 10.1.1.1
      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 **Mercurio**):

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*", "*1.1.10.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.1-1-10.rev, etc.} por causa das permissões de escrita! Não os copie! O servidor secundário terá de os transferir e atualizar automaticamente! A ideia é que um servidor secundário se atualize automaticamente sozinho, sempre que houver alterações nos dados do servidor primário.

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 **Mercurio**. 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 - 10.2.2.2
> www.cc.pt
$ nslookup www.cc.pt. 10.2.2.2
(...)
```

Parte III: Preparação do relatório e submissão

1. Relatório

O relatório final deste trabalho TP3 deve incluir:

- Uma secção de "Questões e Respostas" que dê resposta adequada às questões enumeradas, incluindo para cada questão: a questão, a resposta e a prova da realização da mesma (se aplicável);
- Uma demonstração clara de que o domínio de nomes CC.PT está a funcionar na topologia CORE, quer o servidor primário quer o servidor secundário, dando resposta aos requisitos enumerados;
- Um ficheiro com todas as configurações criadas durante a execução do trabalho a submeter conforme instruções abaixo;

2. Submissão

Certifique-se que os seus servidores primário *(master)* e secundário *(slave)* estão operacionais. Só serão considerados trabalhos acompanhados nas aulas.

1. Coloque o relatório elaborado numa diretoria de nome "relatorio" em paralelo com as diretorias "primario" e "secundario".

```
$ cd ~
$ mkdir relatorio
...
```

2. Prepare um ficheiro `tar-gzip` com todos os ficheiros de configuração juntamente com o relatório elaborado e submeta-o no site da disciplina (https://elearning.uminho.pt), **através de Grupos/Troca de arquivos**, para avaliação.

   a) Exemplo de comando (em vez de x coloque o seu turno e em vez de yy a a identificação do seu grupo):

```
$ cd ~
$ tar czvf cc-dns-PLx-Gyy.tgz  primario/ secundario/ relatorio/
…
$ tar tzvf cc-dns-PLx-Gyy.tgz
```

   (… só para verificar que está ok …)

   b) Submeta depois o ficheiro na plataforma de elearning até à data limite