Ficha 6.2 – Serviços de gestão de nomes e endereços (DNS)

Tópicos abordados:
- Configuração do serviço DNS

1 Introdução

Atualmente os serviços de resolução de nomes são essenciais, e cada vez mais são as empresas que necessiatam de ter o seu próprio serviço DNS. Eis alguns ficheiros associados à resolução de nomes num cliente linux:

- `/etc/hosts` – lista de resolução local
- `/etc/host.conf` – ordem de resolução
- `/etc/resolv.conf` – definição dos servidores de dns e domínio. **Nas novas versões do Ubuntu este ficheiro não deve ser alterado!** Modificar antes um dos seguintes ficheiros:
  - `/etc/network/interfaces` com a diretiva `dns-nameservers x.x.x.x`, é a forma recomendada para servidores com IP fixo;
  - `/etc/resolvconf/resolv.conf.d/base` – informação a ser colocada no `/etc/resolv.conf`, é uma das soluções possíveis para servidores com IP fixo;
  - para reconstruir o ficheiro `/etc/resolv.conf` fazer `sudo resolvconf -u`
- `/etc/dhcp/dhclient.conf` – comportamento do cliente DHCP que pode ter diretivas para configurar o DNS. Este ficheiro **raramente precisa de ser modificado** e apenas serve para um cliente com IP e DNS dinâmicos, **não usar em servidores com IP fixo**.

Exercício 1.

1. Verifique o estado actual da configuração da sua rede: Identifique os seguintes endereços IP configurados na sua máquina Ubuntu:
    a. interface de rede `eth0`
    b. gateway por omissão
    c. servidor de DNS em uso
2. Analise o conteúdo do ficheiro `/etc/hosts`. (`man 5 hosts`)
3. Analise o conteúdo do ficheiro `/etc/resolv.conf` (`man 5 resolv.conf`)
4. Analise o conteúdo do ficheiro `/etc/nsswitch.conf`. Qual a finalidade desse ficheiro? (`man 5 nsswitch.conf`)

2 Introdução ao DNS

O DNS (Domain Name System) é um serviço destinado à resolução de nomes que funciona como uma base dados distribuída. A sua estrutura permite o controlo local de segmentos em toda a base dados através da replicação de dados entre servidores DNS. Os servidores de nomes (*nameservers*) contêm informação sobre alguns segmentos da base de dados de nomes e respondem aos pedidos dos clientes (chamados *resolvers*).
A estrutura da base dados é semelhante a uma árvore em que o "." (ponto) representa a raíz e cada sub-árvore um domínio (Figura 1).

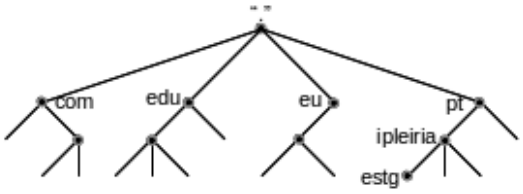

Figura 1- Estrutura do DNS

Cada domínio tem um nome único que identifica também a sua posição na base de dados. No DNS os nomes são uma sequência de rótulos (*labels*) separados por pontos (.) desde a folha da até à raíz da árvore. Por exemplo: estg.ipleiria.pt. (é habitual omitir o último ponto).

No DNS cada domínio pode ser dividido em subdomínios e a responsabilidade desses subdomínios pode ser atribuída a diferentes organizações. Por exemplo, a gestão do domínio "." é da responsabilidade do ICANN, pt é da responsabilidade da FCCN (Fundação para a Computação Científica Nacional), e o domínio ipleiria.pt é da responsabilidade do Instituto Politécnico de Leiria. Ao delegar a responsabilidade de ipleiria.pt cria-se uma nova zona com administração autónoma do espaço de nomes (*namespace*). A zona ipleiria.pt passa a ser independente de pt. O domínio ipleiria.pt pode ainda ser dividido em subdomínios, por exemplo estg.ipleiria.pt e alguns desses subdomínios podem também ser novas zonas se a responsabilidade pela sua gestão também for delegada. A localização dos nomes na base de dados DNS está espelhada no seu nome canónico. Assim, podemos ter vários servidores com o nome dei desde que o resto do seu nome canónico seja diferente, por exemplo: dei.uc.pt e dei.estg.ipleiria.pt. É possível ter até 127 níveis de profundidade numa árvore de DNS e cada rótulo pode ter até 63 carateres.

O tipo de informação obtida num pedido ao DNS depende do contexto. Por exemplo, ao enviar um email para ipleiria.pt o servidor de DNS devolve informação sobre como encaminhar o email, mas para fazer ssh ao ipleiria.pt devolve o endereço IP do servidor com esse nome.

Além de serem referidos por nomes relativos, os domínios e subdomínios são também referidos pelo seu nível hierárquico. Assim, é habitual falar-se em "domínios de topo" e "domínios de nível um" etc. Estes nomes significam:

- domínio de topo – é um domínio filho da raíz, exemplos: com, edu, org, pt
- donínio de 1º nível – é igual ao anterior
- domínio de 2º nível – é um domínio filho do 1º nível
- etc

A diferença entre domínios e zonas pode ser subtil. O domínio `ipleiria.pt` pode ter vários subdomínios, tais como `estg.ipleiria.pt`, `esslei.ipleiria.pt`, `ese.ipleiria.pt` e `estm.ipleiria.pt`. No entanto pode delegar a administração de uns subdomínios e de outros não. Assim, uma zona pode conter um ou mais subdomínios, conforme a delegação da responsabilidade de administração. Vamos supor que o subdomínio ese.ipleiria.pt não é delegado. Nesse caso a zona ipleiria.pt irá conter também o ese.ipleiria.pt. Veja a figura 2. É por esta razão que os servidores de DNS armazenam dados de zonas e não de domínios. Um servidor de DNS nunca irá conter dados de zonas delegadas, mas deve conter ponteiros para os servidores DNS com as zonas delegadas.

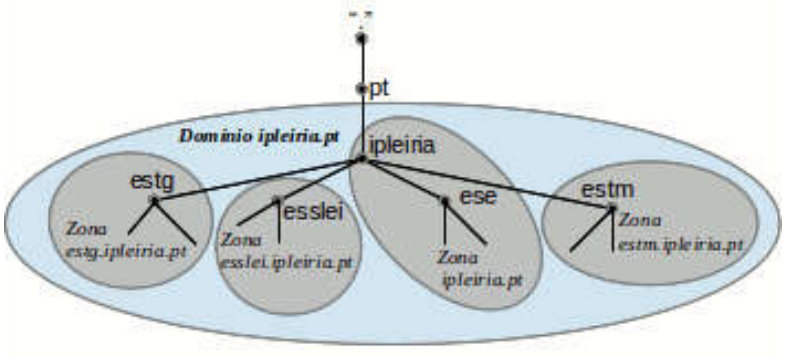

Figura 2 - Domínios versus Zonas.

A figura 2 representa um exemplo onde é possível distingir os conceitos de domínio e zonas. As áreas cinzentas representam zonas (parte do domínio que foram delegadas.

2.1 Tipos de servidores

Existem dois tipos de servidores de nomes: primário (*primary masters*) e secundário (*secondary masters*). O servidor primário de uma zona lê a informação que tem sobre essa zona nos seus ficheiros de configuração. Um servidor secundário (também designado slave server) obtém a informação de uma zona a partir de outro servidor designado master server. É habitual o primary master e o master server serem o mesmo servidor. Ambos os servidores de nomes master e slave de uma zona são servidores "autoridade" dessa zona. Os servidores slave servem para: aumentar a redundância (para o caso um servidor falhar) e para distribuir a carga dos pedidos gerados pelos clientes. Quando um servidor serve um pedido para resolver um nome do qual não é a "autoridade", então passa o pedido ao DNS do nível hierárquico superior até encontrar um servidor que seja a "autoridade" ou que tenha esse nome em memória cache.

Todas as organizações com servidores ligados diretamente à Internet têm obrigatoriamente de gerir um servidor DNS. Existem várias implementações do serviço DNS, a mais conhecida e usada chama-se bind e está disponível em vários sistemas operativos, desde sistemas Unix, Linux até ao Windows Server.

3 Clientes DNS e utilitários

No Linux existem vários clientes DNS, que possibilitam inquirir servidores DNS. Os mais conhecidos são o `nslookup`, o `host` e o `dig`. Em certas distribuições, o `nslookup` é

considerado obsoleto, pelo que não será aqui analisado (note-se que existe um utilitário de mesmo nome no Windows). Além destas ferramentas existem também outras que são úteis, nomeadamente:

- `ping` – comando de validação de comunicação (utiliza protocolo ICMP)
- `traceroute` – determina percurso a percorrer até ao destino
- `http://www.dnsinspect.com/` - Ferramentas web de análise web

Consulte as páginas do manual para as ferramentas mencionadas.

Exercício 2.

1. Recorrendo ao utilitário `host`, determine o endereço IP de `webmail.estg.ipleiria.pt`.
2. Repita a alínea anterior, mas recorrendo ao sítio http://centralops.net/co/. Interprete à luz da resposta anterior.
3. Obtenha todos os registos DNS associados ao domínio `estg.ipleiria.pt`.
4. Interprete os resultados de `host -a cnn.com`.
5. O utilitário `dig` apresenta funcionalidade semelhante ao `host`, embora seja considerado mais poderoso (permite um modo de processamento em lotes, entre outras características).
   a) Execute o comando `dig` e interprete os resultados.
   b) Obtenha a lista de todos os tipos de registos DNS do domínio `gmail.com`. Interprete os resultados tendo em conta as especificidades do domínio `gmail.com` (serviço de mail via Web).
   c) Efectue um *"reverse lookup"* de um dos endereços IP devolvidos pela alínea anterior.

4 Bind

O BIND é um conjunto de programas que implementam o serviço de nomes, sendo esse serviço informalmente conhecido como DNS.

Exercício 3.

1. Execute o comando `hostname` para obter o nome da máquina virtual. Mude a designação da máquina virtual para AS01, através do comando "`sudo hostname as01`". Este comando muda a designação, mas não de forma permanente. Se reiniciar a máquina virtual o nome antigo vai aparecer novamente. Para tornar a mudança efetiva deve fazer o seguinte:
   a) Editar o ficheiro `/etc/hostname` e colocar o novo nome
   b) Editar o ficheiro `/etc/hosts` e alterar para o novo nome a linha referente ao endereço `127.0.1.1`. Ou seja:
      `127.0.1.1 nome-antigo`, alterar para:
      `127.0.1.1 as01`
   c) Eim executar: `sudo service hostname start` ou em alternativa reiniciar a máquina virtual.

2. Proceda à instalação do BIND9, recorrendo ao comando `apt-get`.

```
apt-cache search bind9      # o package existe?
apt-cache show bind9        # informação suscinta
apt-cache showpkg bind9     # informação mais detalhada
apt-get install bind9       # procede à instalação
```

   a) Repita os passos anteriores para a package: `bind9-doc`
   b) Um conjunto de ficheiros deverão agora existir no directório `/etc/bind`. É nesse directório que serão criados os ficheiros apropriados para a definição de zonas DNS. De modo a preservar o conteúdo do directório (para futura referência), efectue uma cópia para o directório "Original".

3. Explore a utiliade dos seguintes ficheiros:
   a) `named.conf, named.conf.options, named.conf.local, db.root, db.127`
   b) Que caracter é empregue para o comentário de linhas?

4. O lançamento do serviço de resolução de nomes (também conhecido por `named`) é feito através do script de arranque `/etc/init.d/bind9`. Por omissão, a configuração do `syslog` faz com que as saídas deste serviço sejam redireccionadas para o `/var/log/syslog`. Verifique o estado do serviço através do comando `sudo service bind9 status`. Se o serviço estiver desligado, ative-o através do comando `sudo service bind9 start`.
   a) Qual é o nome do processo criado pelo serviço de resolução de nomes?
   b) Monitorize o ficheiro `/var/log/syslog`, recorrendo por exemplo, ao `grep <nome do processo> /var/log/syslog | less`.

5. Configure o seu sistema para "DNS forwarder". Para tal, terá que editar o ficheiro `named.conf.options`, acrescentando o seguinte:

```
// FILE: /etc/bind/named.conf.options
// Foward config
forwarders{
       8.8.8.8; // estes IPs são dos servidores DNS da google
       8.8.4.4;
};
```

6. Altere a configuração do seu sistema para garantir que a resolução de nomes é feita exclusivamente pelo seu sistema. Para isso execute: `cat /etc/resolv.conf`. Se o IP listado não for `127.0.0.1` terá de alterar o ficheiro:

```
# FILE: /etc/network/interfaces
iface eth0 inet static
        address 192.168.209.130
        netmask 255.255.255.0
        gateway 192.168.209.2
        dns-nameservers 127.0.0.1 # linha a alterar
        dns-search gars.pt        # linha a acrescentar
```

Depois reinicie a configuração da rede: `sudo /etc/init.d/networking restart`.

7. Como com muitos outros daemons Unix, é possível forçar o `named` a recarregar a configuração (leitura do`/etc/bind/named.conf`) através do envio do sinal

SIGHUP ao processo que executa o named. Recorrendo-se ao comando killall torna-se possível enviar um sinal a todos os processos especificando-se não os PIDs dos processos, mas o nome do executável que eles se encontram a executar. Execute o seguinte comando, mantendo-se atento ao ficheiro /var/log/syslog:

```
# envio do sinal SIGHUP para o daemond "named"
sudo killall -HUP named
```

- Caso não existisse o utilitário killall, como procederia para enviar o sinal SIGHUP ao processo named?

8. No conjunto de programas disponibilizados pelo serviço bind9, o rndc permite interagir com o servidor através do envio de comandos. Deste modo, para ordenar a releitura da configuração do bind basta executar (com os devidos privilégios):

```
rndc reconfig
```

a) Teste a sua configuração corrente, recorrendo ao host ou ao dig.

Exercício 4. Criação de um domínio

Neste exercício proceder-se-á a definição do domínio as.pt. Como referência poderá consultar o sítio http://www.madboa.com/geek/soho-bind/. A definição da zona será efectuada no ficheiro de configuração a ser guardado no directório /etc/bind/zones. O domínio as.pt é definido da seguinte forma:

- Máquinas: as01.as.pt (192.168.226.3), as02, …, as16.as.pt (IPs da mesma gama .202, .203, … .216)
- Servidor de nome do domínio, a sua máquina: as01.as.pt
- Aliases: , ftp → ftp01.as.pt; www → www01.as.pt
- Nameserver - as01.as.pt
- Servidores de mail:
  - mail1 (prioridade 10) → 192.168.226.3
  - mail2 (prioridade 20) → 192.168.234.30

1. Crie o directório `/etc/bind/zones`.
2. No referido directório, crie o ficheiro `db.gars.pt` que deverá conter a definição da zona `as.pt`.
3. Faça `sudo cp /etc/bind/db.local db.as.pt` para criar um ficheiro já com uma estrutura iniciada e depois proceda às alterações necessárias para incluir todas as máquinas, aliases, servidores de email e nameservers.
4. Defina o domínio `as.pt` no ficheiro `/etc/bind/named.conf.local`.

```
zone "as.pt" {
        type master;
        file "/etc/bind/zones/db.as.pt";
};
```

5. Execute o comando "`named-checkconf /etc/bind/named.conf`" e resolva eventuais problemas que tenham sido identificados.
6. Force a re-leitura dos ficheiros de configuração do servidor DNS.
7. Ainda na directoria `/etc/bind/zones` execute o comando `sudo cp /etc/bind/db.127 /etc/bind/zones/db.x.y.z` (substituir x.y.z pelos 3 primeiros octetos do seu IP) para configurar o domínio para resolução inversa de nomes (reverse DNS).
8. Faças as alterações necessárias e adicione todos os IPs da sua zona neste ficheiro. Não se esqueça que cada ficheiro de zona inversa só pode ter uma sub-rede.
9. A definição da zona inversa deve constar do ficheiro `/etc/bind/named.conf.local`.

```
# repetir estas linhas para cada sub-rede
zone "z.y.x.in-addr.arpa" { # inverter a ordem dos octetos
        type master;
        file "/etc/bind/zones/db.x.y.z";
};
```

10. Verifique novamente a sua configuração com os comandos em baixo e resolva eventuais problemas:
    - `named-checkconf /etc/bind/named.conf`
    - `named-checkzone as.pt /etc/bind/zones/db.as.pt`

- `named-checkzone z.y.x.in-addr.arpa /etc/bind/zones/db.x.y.z`

11. Reinicie o serviço bind.
12. Teste o seu serviço de nomes, tanto localmente, como numa máquina remota – recorra ao sistema operativo hospedeiro da sua máquina virtual, sendo que deverá indicar como servidor de nomes o IP da máquina virtual.
    - Com o utilitário `host` faça resolução dos nomes que definiu e obtenha os nomes a partir do endereço IP (reverse DNS)
    - Faça os mesmos testes com o comando `dig`. Os resultados são iguais? Justifique.

5 Bibliografia

- Páginas do manual (man) dos seguintes comandos: `host`, `dig`, `nslookup`, `named.conf`, `named-checkconf`, `named-checkzone`, `rndc`
- DNS & BIND, Paul Albitz, Cricket Liu,5th Edition, 2006, O'Reilly