Pràctica 3: Servei de noms (DNS)

Aplicacions i Serveis sobre Internet — Enginyeria de Sistemes TIC

Eric Roy Almonacid Francisco del Águila López

13 de març de 2025

Índex

1 Introducció

Per poder realitzar aquesta pràctica és indispensable haver completat la pràctica 1, donat que treballarem sobre el VPS creat anteriorment.

1.1 Objectius

Al finalitzar aquesta pràctica, l'estudiantat haurà:

1. Entès el funcionament de la resolució de noms de domini.
2. Adquirit un domini o subdomini, en el qual en té autoritat.
3. Creat registres al domini utilitzant un servei de tercers.

4. Entès el funcionament i configurat DNSSEC al domini.
5. Entès i configurat DDNS utilitzant serveis de tercers.

1.2 Condicions

Aquesta pràctica està cal·librada per ésser treballada en equips de 2 persones, i té una durada de 1 a 2 setmanes.

1.3 Lliuraments

S'haurà de realitzar una entrega a Atenea i mantenir operatiu el servidor i domini creats fins que la pràctica sigui avaluada. El format de la entrega està detallat a l'apartat 6.1.

2 El Servei de Noms de Domini

El Servei de noms de domini o *Domain Name Server* (DNS) va ser introduït l'any 1983 amb dues finalitats:

- Poder resoldre un nom de domini a una adreça IP, per evitar haver de memoritzar-la.
- Establir l'arbre de noms: definir l'estructura jeràrquica de noms distribuida en zones d'autoritat. Per exemple, qualsevol domini que acabi amb `upc.edu` significarà que pertany a la UPC. Qualsevol domini que acabi amb `epsem.upc.edu` significarà que pertany a l'escola de Manresa.

Així doncs, un servidor de DNS es pot distingir segons la funció que realitza:

- Autoritatiu: (*authoritative name server*): forma part de l'arbre de noms de domini, i defineix els continguts de la zona en la que hi té autoritat. Pot delegar a altres servidors DNS sub-zones d'autoritat.

  N'hi ha de dos tipus: primaris i secundaris. Els secundaris tenen la mateixa informació que els primaris i es fan servir per redundància.
- Local: (*local name server*): aquest servidor consulta iterativament als servidors autoritatius fins a obtenir el resultat de la consulta. A més, pot guardar en *caché* les respostes de les consultes.

Tot i que és possible fer-ho, en general no hi ha servidors autoritatius i locals alhora. Si es fa una consulta iterativa a un servidor autoritatiu aquest no cercarà la resposta.

En aquesta pràctica configurarem un servidor autoritatiu de tercers. Si teniu interès en desplegar el vostre propi servidor de noms us recomanem utilitzar el servei `bind`.

2.1 Dominis de primer nivell

Els dominis de primer nivell o *Top-Level Domains* (TLD) son els dominis directament descendents de l'arrel o *root*. Inicialment només n'hi havien 6: *.gov*, *.mil*, *.net*, *.edu*, *.org* i *.com*.

Amb el creixement d'Internet, aquest va arribar a territoris estrangers, i es va acabar assignant un TLD a cadascun d'ells: *.es*, *.pt*, etc. Actualment, l'ICANN crea TLDs per molts col · lectius

diferents, i delega la seva autoritat a una entitat. En el cas del TLD *.cat*, aquest és gestionat des dels seus inicis per la Fundació .cat : `https://fundacio.cat`.

Quan es parla col·loquialment d'*adquirir un domini*, es refereix a arribar a un tracte amb una entitat que disposa d'un TLD perquè aquesta ens reservi i delegui l'autoritat d'un subdomini. Cada TLD pot posar les condicions (preu, finalitat, idioma dels continguts) que desitja. En el cas d'un domini .cat, es demana que el contingut estigui en català.

Per facilitar la tasca de "llogar" dominis s'ha creat el concepte de registrador de dominis o *registrar* en anglès. Cada TLD escull quins registradors poden assignar sub-dominis en nom seu, i sota quines condicions. En el cas del domini .cat, podeu consultar els registradors disponibles a `https://domini.cat/comparativa-de-preus/`.

2.2 Registrar un domini

La primera tasca d'aquesta pràctica consistirà en registrar un domini amb un registrador. Qualsevol registrador és igual de vàlid, però si busqueu una alternativa econòmica us recomanem `https://dinahosting.com` pels dominis .cat i `https://cloudflare.com` per la resta (*.com*, *.net*, *.es*, ...).

Existeixen alternatives per si no voleu pagar per un domini. Hi ha serveis com `https://dynu.com` que et cedeixen gratuïtament un domini de l'estil `domini.dynu.com`. Utilitzar subdominis comporta algunes conseqüències, però no tenen cap impacte en les pràctiques d'aquesta assignatura.

Tasca 1 Adquiriu un domini o subdomini.

2.3 Gestionar un domini

Cada registrador té la seva interfície, però gairebé tots permeten gestionar els registres DNS. En cas que no ho permeti o que es vulgui utilitzar un altre servidor de noms de domini (ja sigui propi o un altre servei), un registrador sempre ha d'oferir la possibilitat de canviar les entrades `NS`. D'aquesta manera és possible gestionar un domini .cat amb *cloudflare*.

Un registrador també està obligat a oferir la possibilitat de traspassar el domini a un altre registrador. És un procés lent, però que garanteix que en cap moment el domini estarà "alliberat", és a dir, que cap persona externa el podrà adquirir.

Tasca 2 Creeu en el gestor del registrador un registre `A` que relacioni el domini adquirit (o un subdomini d'aquest) a l'adreça IPv4 del VPS de la pràctica 1. Creeu un registre `AAAA` amb la mateixa finalitat que l'anterior però per l'adreça IPv6.

Comproveu el funcionament de la tasca utilitzant les eines `ping` o `dig` en el vostre ordinador.

2.4 DNSSEC

Com molts protocols creats al principi d'Internet, no es va tenir en compte la seguretat en el DNS. Al tractar-se d'un servei que no requereix que es verifiqui l'autenticitat de les respostes a les consultes, resulta molt senzill realitzar atacs com *DNS Poisoning*.

Per mitigar aquest atac es va desenvolupar DNSSEC, unes extensions al protocol base que utilitzen claus asimètriques per demostrar que una resposta prové del remitent original. Podeu trobar

més informació sobre l'atac i la mitigació d'aquest a `https://www.cloudflare.com/learning/dns/dns-cache-poisoning/`.

S'entrarà més en detall amb aquest tema quan es faci una introducció a la seguretat en les sessions de teoria. Tanmateix, al estar treballant en un entorn hostil, es recomana utilitzar DNSSEC des del primer moment.

Tasca 3 Habiliteu DNSSEC pel vostre domini. Si el gestor del DNS és el mateix que el registrador, aquesta tasca consistirà en fer un únic clic.

3 DNS Invers

El DNS Invers o *Reverse DNS* és un sistema que permet obtenir un domini a partir d'una adreça. Moltes eines de xarxa (tcpdump, wireshark, ...) utilitzen aquest sistema per oferir una interfície més amable a l'usuari.

Es poden fer consultes de DNS invers amb l'opció `-x`. Per exemple: `dig -x 8.8.8.8` mostrarà el nom del servidor associat a aquesta IP: `dns.google`. Si fem `dig dns.google` tornem a obtenir l'adreça anterior, així tancant el cicle.

El concepte de *Fully Qualified Domain Name* (FQDN) no és més que el nom de domini complert d'un computador a Internet. Aquest FQDN inclou el nom de l'equip i el domini al que pertany. La comanda `hostname` i les seves variants (consulteu el manual) determinen el nom de l'equip, així com el domini associat al computador. Les bones pràctiques associades a la gestió de sistemes (computadors) recomanen que hagi coincidència entre el que existeix en el registres del sistema de DNS i el que el computador té configurat tant de nom de màquina com de nom de domini. D'aquesta manera, les consultes internes per part del sistema operatiu coincidiran amb les consultes al servei de DNS. Disposar d'un FQDN és de gran ajuda per donar credibilitat a un servidor de cara a realitzar certes tasques, com per exemple enviar correus electrònics.

Tasca 4 Configureu els registres PTR al proveïdor d'Internet del vostre servidor per obtenir un FQDN. Si és possible, realitzeu això per l'adreça IPv4 i IPv6. En el cas de Hetzner, haureu d'anar a la pestanya de *Networking*.

Compte! No tots els proveïdors permeten modificar els registres PTR.

Si esteu treballant sense VPS, el vostre proveïdor d'Internet és qui us hauria de proporcionar la possibilitat de definir el registre PTR. Pràcticament la totalitat dels proveïdors d'Internet **no** ofereixen aquesta opció.

Finalment, per acabar de preparar-nos per les següents pràctiques, canviarem el nom de la màquina VPS pel FQDN que haurem creat. Els servidors de correu utilitzen per defecte el domini que s'obté a l'executar la comanda `hostname --fqdn`. Per exemple, si el nom de la màquina és `correu` i el nom de domini és `itic.cat`, podrem crear adreces que acabin amb `@correu.itic.cat`. Per gestionar tant nom de l'equip com domini que té internament un computador, disposeu de les comandes `hostname` amb les seves opcions i `dnsdomainname`.

Tasca 5 Configureu adequadament el FQDN de la màquina virtual. Reinicia la màquina per aplicar els canvis.

4 Ampliació: DNS Dinamic

L'escassetat d'adreces IPv4 obliga els proveïdors d'internet fer alguns malabarismes per mantenir tots els usuaris connectats. La pràctica més utilitzada, si més no fins abans l'arribada del CG-NAT, era assignar una adreça IPv4 a l'usuari un cop aquest connectés l'encaminador a la xarxa, i alliberar l'adreça en el moment de la desconnexió. Aquesta tècnica es coneix com a IP Dinàmica.

La principal desavantatge de tenir una adreça que va canviant cada cert temps és que no ens la podem memoritzar o publicar, per tant no podem fer que altra gent es connecti de manera fiable al nostre encaminador. Una forma popular de sol·lucionar això és utilitzant un DNS Dinamic (DDNS).

El DDNS està format per dues parts:

- Un servidor DNS equipat amb una API per modificar els registres.
- Un programa que s'executa cada pocs minuts en una màquina dintre de la xarxa que té una IP Dinàmica. Aquest programa esbrinarà quina és l'adreça IP pública actual i, mitjançant l'API anterior, actualitzarà el registre DNS.

Hi ha moltes combinacions d'APIs i programes que podeu utilitzar per realitzar un DDNS. En aquesta pràctica us proposem la següent configuració.

Tasca 6 Configureu un DDNS en el vostre portàtil. No servirà de gran cosa: només per saber des de quina IPv4 es connecta l'ordinador. A continuació teniu un exemple de passos a seguir, però podeu utilitzar els serveis que vulgueu:

- Creeu-vos un compte d'usuari a `https://dynu.com`.
- Delegueu un subdomini als servidors de noms de Dynu, i associeu-lo al vostre compte (*Control Panel* → *DDNS Services* → *Add*).
- Creeu un *shell script* seguint el tutorial de `https://www.dynu.com/DynamicDNS/IP-Update-Protocol` per poder actualitzar l'adreça IP del subdomini.
- Utilitzeu *cron* o similars per fer que s'executi el script anterior cada cert temps. Podeu trobar un bon tutorial de *crontab* a `https://cronitor.io/guides/cron-jobs`.

5 Ampliació: Delegació d'una zona d'autoritat

La darrera part d'aquesta pràctica consisteix en delegar un subdomini (o zona) al vostre VPS. En aquest instal·larem un servidor de noms de domini (com per exemple `bind`) i servirem des d'aquest les respostes a les consultes autoritatives.

Per realitzar aquesta ampliació resulta imprescindible llegir l'enunciat alternatiu de la pràctica 3.

Tasca 7 Delegueu una zona d'autoritat al vostre VPS i serviu des d'allà algun registre DNS. Comproveu amb `dig` que podeu fer consultes autoritatives però no recursives al vostre servidor.

Per exemple, si el domini adquirit és `itic.cat`, es pot delegar `serv.itic.cat` al VPS amb aquestes dues línies en el vostre gestor de DNS:

```
vps.itic.cat.    A    100.200.100.200
```

```
serv.itic.cat.   NS   vps.itic.cat
```

Llavors, en el VPS, configureu BIND per afegir alguna cosa:

```
test.serv.itic.cat.    A    250.250.250.250
```

6 Avaluació

6.1 Entrega

S'ha d'entregar un fitxer comprimit (`P3_GX.zip`, on X és el número o lletra del grup) amb un fitxer de text amb el següent format:

```
Grup: GX
Domini adquirit: asi.itic.cat
VPS: srv1.asi.itic.cat
Contrasenya usuari profe: Lkv5YYyON8X
Port SSH: 22

(ometre si no heu fet les ampliacions)
DDNS: portatil.asi.itic.cat

(Comentaris referents a l'entrega, si s'escau)
```

La majoria de dades son referents a la pràctica 1. Es demana que les torneu a escriure, així teniu la possibiltat de canviar-les. Fixeu-vos també que no cal introduir adreces IP, ja que es poden obtenir a partir dels dominis.

Al servidor, creeu el directori `/entregues` a l'arrel, i a dins un directori `/entregues/p3`. Allà hi heu de deixar els scripts i/o manuals (el que cregueu convenient) que us farien falta si mai haguéssiu de repetir aquesta pràctica. Afegiu aquests fitxers també al fitxer comprimit de l'entrega.

Per exemple, podríeu indicar:

- Quin proveïdor de dominis heu utilitzat i per què.
- Quins subdominis heu fet servir per cada punt de la pràctica.
- Quins scripts o fitxers heu utilitzat o modificat.

No ha de ser extens; aquests documents us serviran a vosaltres si mai heu de crear un nou domini.

6.2 Qualificació

Aquesta pràctica s'avaluarà de la següent manera. La puntuació màxima és 100.

Concepte	Rang
Fitxer de l'entrega (`P3_GX.zip`) amb format correcte	$[-20, 0]$
Es pot resoldre el nom del servidor per IPv4 i IPv6	$[0, 20]$
El hostname del servidor és el del domini	$[0, 10]$
La resolució inversa de les adreces IPv4 i IPv6 del servidor permeten obtenir el domini (FQDN)	$[0, 10]$
Correcte funcionament del DDNS	$[0, 20]$
Configuració i correcte funcionament del servidor autoritatiu muntat al VPS	$[0, 10]$
Qualitat dels scripts/tutorials de `/entregues/p3`	$[0, 30]$
El servidor presenta problemes de seguretat greus	$[-10, 0]$

Nota: si el vostre proveïdor no us permet tenir una adreça IPv6 pública o modificar els registres de la resolució inversa indiqueu-ho al fitxer de la entrega.

Tingueu present que si algun element de la taula anterior no es pot avaluar aquest es qualificarà amb la nota més baixa.

Si es detecta algun tipus de frau en l'entrega aquesta rebrà una puntuació de zero.