3. Registres i fitxers de zona

3.1. Què és un registre de recurs?

La informació DNS es publica en **registres de recurs**, abreujats RR. Un conjunt de registres amb el mateix nom, classe i tipus és un **RRset**. Un fitxer de zona és una representació textual d'aquesta informació, no una llista d'URL.

```
nom                TTL   classe   tipus   dades
www.example.com.   300   IN       A       192.0.2.20
```

El significat de les dades depén del tipus: una adreça en A, un nom de servidor en NS, text en TXT, etc. No tots els registres contenen una IP.

3.2. Tipus que s'han de conéixer

Tipus	Funció	Exemple de dades
A	Associa un nom amb IPv4.	`192.0.2.20`
AAAA	Associa un nom amb IPv6.	`2001:db8::20`
NS	Identifica un servidor autoritatiu d'una zona o una delegació.	`dns1.example.com.`
SOA	Defineix informació administrativa i temporal de la zona.	Servidor de referència, contacte, sèrie i temporitzadors.
CNAME	Fa que un nom siga àlies d'un altre nom.	`www.example.com.`
MX	Identifica un servidor receptor de correu i la seua preferència.	`10 mail.example.com.`

Tipus	Funció	Exemple de dades
PTR	Apunta a un nom; s'usa especialment en resolució inversa.	`www.example.com.`
TXT	Publica text per a usos definits per altres protocols.	Verificacions de domini o reptes DNS-01.
SRV	Publica servidor, port, prioritat i pes d'un servei.	`10 5 5060 sip.example.com.`
CAA	Restringeix quines autoritats de certificació poden emetre certificats.	`0 issue "letsencrypt.org"`

Els registres NS i MX apunten a **noms**, no directament a adreces. Els noms de destinació han de resoldre a les adreces adequades; no s'han de configurar com a àlies CNAME.

3.3. Lectura d'una zona completa

Exemple de documentació; no s'ha de publicar amb aquestes IP:

```
$ORIGIN example.com.
$TTL 300
@   IN SOA dns1.example.com. hostmaster.example.com. (
        2026111101 ; serial
        3600       ; refresh
        600        ; retry
        604800     ; expire
        300        ; negative cache minimum
)
    IN NS dns1.example.com.
dns1    IN A     192.0.2.10
@       IN A     192.0.2.20
www     IN A     192.0.2.20
www     IN AAAA  2001:db8::20
portal  IN CNAME www.example.com.
mail    IN A     192.0.2.25
@       IN MX    10 mail.example.com.
@       IN TXT   "Exemple docent de zona DNS"
@       IN CAA   0 issue "letsencrypt.org"
```

`$ORIGIN` estableix el sufix per als noms relatius. `@` representa l'origen actual. `$TTL` defineix el TTL que s'aplica quan un registre no n'indica un. El punt i coma inicia un comentari, i els parèntesis permeten repartir un registre en diverses línies.

Si una línia comença amb espais i omet el propietari, hereta el de l'anterior registre: en l'exemple, el NS pertany a `@`. Els espais inicials poden ser significatius; no s'han d'afegir indiscriminadament. El nom del fitxer, en canvi, és una decisió de l'administrador: la zona s'associa amb el fitxer des de la configuració del servidor.

No s'ha de publicar AAAA en una pràctica si no hi ha IPv6 funcional. Alguns clients i processos de validació intentaran utilitzar-lo; un A correcte no compensa un AAAA incorrecte.

3.4. El SOA, camp a camp

Camp de l'exemple	Interpretació
`dns1.example.com.`	MNAME: servidor de referència de la zona.
`hostmaster.example.com.`	RNAME: representa el correu `hostmaster@example.com`, amb convencions d'escapat si el nom local conté punts.
`2026111101`	Sèrie: versió de la zona; s'incrementa quan es modifica.
`3600`	Refresh: interval perquè els secundaris comproven la versió.
`600`	Retry: espera abans de repetir un intent fallit.
`604800`	Expire: límit sense refresc satisfactori després del qual el secundari deixa de servir la còpia com a vàlida.
`300`	MINIMUM: intervé en el TTL de les respostes negatives.

La forma `AAAAMMDDnn` de la sèrie és una convenció útil, no una data interpretada per DNS. Cal assegurar que augmente respecte del valor anterior. Els secundaris comparen versions amb les regles de l'aritmètica de sèrie DNS.

Incrementar la sèrie no buida les memòries cau dels clients. La sèrie ajuda a sincronitzar autoritatius; el TTL regeix la vida de les còpies dels resolutors. Són mecanismes diferents.

3.5. A, AAAA i CNAME

Amb A/AAAA es publica una adreça. Amb CNAME es publica un altre nom que s'ha de seguir. Un CNAME no és una redirecció HTTP: el navegador continua demanant el nom original al servidor web i el certificat ha de cobrir-lo.

Un nom amb CNAME no pot tindre alhora A, MX o altres dades ordinàries. Per això no s'utilitza un CNAME en l'àpex d'una zona clàssica, on ja existeixen SOA i NS. Per a servir el web en `nomcognom.netsx.es` sense `www`, es pot posar un A en `@`.

Diversos registres A amb el mateix nom poden repartir respostes, però això no equival a un balancejador amb comprovacions de salut. DNS no comprova automàticament si el web de cada IP funciona.

3.6. MX, TXT, SRV i CAA en context

En un MX, **la preferència numèrica menor té prioritat**. Amb valors 10 i 20 s'intenta primer el 10; un MX no crea bústies ni instal·la un servidor de correu.

TXT és un contenidor de text interpretat per una aplicació concreta. Per a DNS-01 s'utilitza un nom com `_acme-challenge.www.nomcognom.netsx.es`. No s'ha de confondre qualsevol TXT amb una autorització per emetre certificats.

SRV és útil per a aplicacions que saben consultar-lo; un navegador no canvia el port d'un web ordinari perquè s'haja creat un SRV. CAA indica autoritats autoritzades a emetre, però no emet ni instal·la cap certificat. Si es configura, ha de ser coherent amb l'autoritat que s'utilitzarà.

3.7. Resolució inversa

La resolució directa pregunta per un nom i obté A/AAAA. La inversa construeix un altre nom dins de `in-addr.arpa` per a IPv4 o `ip6.arpa` per a IPv6 i pregunta per PTR. **No es busca automàticament un A a l'inrevés.**

Per a `192.168.0.200`, el nom complet de consulta és:

```
200.0.168.192.in-addr.arpa.
```

En una zona privada `0.168.192.in-addr.arpa`, un fragment seria:

```
$ORIGIN 0.168.192.in-addr.arpa.
$TTL 300
@ IN SOA dns1.nomcognom.netsx.es. admin.nomcognom.netsx.es. (
    2026111101 3600 600 604800 300
)
  IN NS dns1.nomcognom.netsx.es.
```

```
1   IN PTR dns1.nomcognom.netsx.es.
200 IN PTR intranet.nomcognom.netsx.es.
```

Les dues zones, directa i inversa, s'administren per separat. Afegir un A no obliga el servidor a crear un PTR. Diversos noms poden compartir IP i el PTR no ha de retornar tots els noms que apunten a eixa IP.

En IPv6 es treballa amb dígits hexadecimals individuals en ordre invers. Per evitar errors manuals, `dig -x ADREÇA` construeix la consulta apropiada tant per a IPv4 com per a IPv6.

En AWS, ser administrador de `nomcognom.netsx.es` no dona autoritat sobre la zona inversa de la IP pública. El PTR públic depén del proveïdor de l'adreça i dels permisos disponibles. Crear un fitxer invers en BIND només demostra una resolució local si la delegació inversa pública no existeix. Aquesta limitació s'ha d'explicar en les evidències de la pràctica.

Consulta: RFC 1035, fitxers de zona BIND, RFC 2308, RFC 2782, SRV, RFC 8659, CAA i PTR en EC2.