⚒️ Configuració d'una subzona DNS amb Windows Server 2022

Aquesta píndola configura el servidor fill `subwin.nomcognom.netsx.es` en una EC2 Windows Server. És equivalent a la subzona Linux, però usa el rol DNS de Windows.

1. Infraestructura AWS

Es crea una EC2 Windows Server amb una Elastic IP pròpia, `IP_SUBWIN`. El *Security Group* permet **UDP/53** i **TCP/53** des d'Internet. El tallafoc de Windows també ha de permetre el servei DNS; RDP només s'autoritza des de l'origen d'administració.

2. Delegació des de la zona pare

En el fitxer de zona `nomcognom.netsx.es` del DNS pare s'afig:

```
subwin      IN NS dns1.subwin.nomcognom.netsx.es.
dns1.subwin IN A  IP_SUBWIN
```

S'incrementa la sèrie, es valida i es recarrega BIND al pare. Aquest A és el *glue* del servidor Windows.

3. Instal·lar i configurar el rol DNS

En **Administrador del servidor → Administrar → Afegir rols i característiques**, s'instal·la **Servidor DNS**.

En les propietats del servidor DNS:

- es desactiva la recursió;
- es desactiven les transferències de zona;
- no es configuren reenviadors per al servei públic;
- la zona no es signa amb DNSSEC en aquesta pràctica.

4. Crear la zona filla

En **Administrador DNS** → **Zones de cerca directa** → **Zona nova**, es crea una zona principal basada en fitxer:

```
subwin.nomcognom.netsx.es
```

No es permeten actualitzacions dinàmiques. En la zona s'han de crear:

Nom	Tipus	Valor
`@`	NS	`dns1.subwin.nomcognom.netsx.es.`
`dns1`	A	`IP_SUBWIN`
`www`	A	`IP_SUBWIN`
`@`	TXT	`Subzona Windows de NOM_COGNOM`

En el SOA, el primari és `dns1.subwin.nomcognom.netsx.es.`. L'A de `dns1` ha de coincidir amb el *glue* del pare.

5. Comprovacions

Des d'una EC2 Linux o una altra xarxa externa:

```
dig @IP_SUBWIN subwin.nomcognom.netsx.es. SOA +norecurse +notcp +ignore
dig @IP_SUBWIN subwin.nomcognom.netsx.es. SOA +norecurse +tcp
dig @IP_PARE www.subwin.nomcognom.netsx.es. A +norecurse
dig www.subwin.nomcognom.netsx.es. A
dig +trace www.subwin.nomcognom.netsx.es. A
dig @IP_SUBWIN subwin.nomcognom.netsx.es. AXFR
```

Les respostes directes han de ser autoritatives, el pare ha d'oferir la referència correcta i la transferència ha de quedar denegada.

Configuració inicial del DNS a AWS · Subzona Linux