⚒️ Configuració d'una subzona DNS amb Linux

Aquesta píndola configura el servidor fill `sublin.nomcognom.netsx.es` en una EC2 Ubuntu Server 24.04. Parteix del DNS públic pare `nomcognom.netsx.es` i crea una delegació real amb NS i *glue*.

1. Infraestructura AWS

Es crea una EC2 Ubuntu amb una Elastic IP pròpia, `IP_SUBLIN`. El *Security Group* i, si està actiu, UFW han de permetre entrada **UDP/53** i **TCP/53** des d'Internet.

La zona pare resideix en la EC2 inicial, amb `IP_PARE`. Aquesta IP i la de la subzona són diferents.

2. Delegació en la zona pare

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

```
sublin      IN NS dns1.sublin.nomcognom.netsx.es.
dns1.sublin IN A  IP_SUBLIN
```

L'A és el *glue* perquè el nom de l'NS està dins de la zona delegada. S'incrementa la sèrie i es recarrega el pare:

```
sudo named-checkzone nomcognom.netsx.es /etc/bind/forward.nomcognom.netsx.es
sudo systemctl reload named
```

3. BIND9 autoritatiu en el fill

En la nova EC2:

```
sudo apt update
sudo apt install bind9 bind9-utils bind9-doc dnsutils
sudo nano /etc/bind/named.conf.options
```

```
options {
    directory "/var/cache/bind";
    allow-query { any; };
    allow-transfer { none; };
    recursion no;
    dnssec-validation no;
    listen-on { any; };
    listen-on-v6 { none; };
};
```

Si s'utilitza UFW:

```
sudo ufw allow 53/udp
sudo ufw allow 53/tcp
```

4. Zona `sublin`

En `/etc/bind/named.conf.local`:

```
zone "sublin.nomcognom.netsx.es" IN {
    type primary;
    file "/etc/bind/forward.sublin.nomcognom.netsx.es";
    allow-update { none; };
};
```

En `/etc/bind/forward.sublin.nomcognom.netsx.es`:

```
$TTL 300
@ IN SOA dns1.sublin.nomcognom.netsx.es. admin.nomcognom.netsx.es. (
    1 3600 600 1209600 300
)
@    IN NS  dns1.sublin.nomcognom.netsx.es.
dns1 IN A   IP_SUBLIN
www  IN A   IP_SUBLIN
@    IN TXT "Subzona Linux de NOM_COGNOM"
```

Es valida i s'inicia:

```
sudo named-checkconf
sudo named-checkzone sublin.nomcognom.netsx.es
/etc/bind/forward.sublin.nomcognom.netsx.es
sudo systemctl enable named
sudo systemctl restart named
```

5. Comprovacions

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

Les consultes directes han de mostrar `aa`; la del pare ha de mostrar NS i *glue*; l'AXFR ha de ser denegat. La zona inversa de l'Elastic IP no es publica amb aquest BIND.

Configuració inicial del DNS a AWS · Delegació i glue