⚒️ Configuració del servei DNS a Ubuntu 24.04

En aquesta primera activitat es publica la zona `nomcognom.netsx.es` des d'una instància **Ubuntu Server 24.04 a AWS** amb BIND9. No és una pràctica de VirtualBox: el servidor ha de ser accessible des d'Internet perquè, al final, el professorat puga publicar la delegació i els *glue records*.

En totes les activitats, `nomcognom` es reemplaça pel nom i el primer cognom assignats, en minúscules, sense espais ni accents.

Objectiu i lliurament

En acabar, l'alumnat ha de lliurar al professorat:

- el nom del servidor autoritatiu: `dns1.nomcognom.netsx.es.`;
- l'**Elastic IP** associada a la instància;
- els *glue records* que cal publicar: `dns1.nomcognom.netsx.es. IN A IP_ELASTICA`;
- evidències de consultes autoritatives per UDP i TCP.

El professorat publicarà la delegació de `nomcognom.netsx.es` i el *glue* en `netsx.es`. Abans d'eixa publicació, les proves es fan consultant directament l'Elastic IP.

1. Preparar la instància d'AWS

Es crea una instància EC2 amb Ubuntu Server 24.04 i se li associa una **Elastic IP**. Aquesta IP és estable i serà la que apareixerà en els registres públics de la zona.

En el *Security Group* de la instància s'han d'autoritzar les entrades següents:

Protocol	Port	Origen	Finalitat
UDP	53	`0.0.0.0/0`	Consultes DNS públiques per UDP

Protocol	Port	Origen	Finalitat
TCP	53	`0.0.0.0/0`	Consultes DNS públiques per TCP

Aquesta configuració ja s'ha treballat en l'administració d'AWS. No s'ha d'oblidar cap dels dos protocols: una resposta DNS pot requerir TCP encara que la consulta habitual use UDP.

Es comprova l'adreça que veu la instància:

```
curl -4 https://checkip.amazonaws.com
```

El resultat ha de coincidir amb l'Elastic IP associada.

2. Instal·lar BIND9

En la instància s'instal·len BIND9, les utilitats i les eines de consulta.

```
sudo apt update
sudo apt install bind9 bind9-utils bind9-doc dnsutils
```

3. Configurar BIND com a servidor autoritatiu públic

S'obri el fitxer d'opcions.

```
sudo nano /etc/bind/named.conf.options
```

Se substitueix el bloc `options` pel següent:

```
options {
    directory "/var/cache/bind";

    // La zona autoritativa ha de poder ser consultada des d'Internet.
    allow-query { any; };

    // No s'autoritza cap transferència de zona.
    allow-transfer { none; };

    // Aquest servidor no actua com a resolutor públic.
    recursion no;

    // Es desactiva en aquesta pràctica per evitar errors de validació.
    dnssec-validation no;
```

```
    listen-on { any; };
    listen-on-v6 { none; };
};
```

- `allow-query { any; };` permet que qualsevol resolutor d'Internet consulte la zona quan ja estiga delegada.
- `allow-transfer { none; };` denega les transferències AXFR i IXFR.
- `recursion no;` evita convertir el servidor en un resolutor obert.
- `dnssec-validation no;` és necessari en aquesta activitat; DNSSEC es treballarà quan la delegació estiga preparada.
- `listen-on { any; };` fa que BIND escolte per IPv4 en la interfície de l'Elastic IP.

Si UFW està actiu dins de la instància, també s'obri el DNS per UDP i TCP:

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

El tallafoc de la instància **no substitueix** les regles del *Security Group*: s'han de complir les dues condicions.

4. Declarar la zona pública

S'obri la configuració de zones locals.

```
sudo nano /etc/bind/named.conf.local
```

S'afig la zona directa:

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

Aquesta és l'única zona que es publica en aquesta fase. La zona inversa no es declara ací: la gestió del PTR de l'Elastic IP correspon a AWS i no es pot delegar amb BIND des de la instància.

5. Crear la zona directa

Es crea el fitxer de zona:

```
sudo cp /etc/bind/db.local /etc/bind/forward.nomcognom.netsx.es
sudo nano /etc/bind/forward.nomcognom.netsx.es
```

Se substitueix tot el contingut. Cal reemplaçar `IP_ELASTICA` per l'Elastic IP real i `NOM_COGNOM` pel nom complet de l'alumne o alumna.

```
$TTL 300
@ IN SOA dns1.nomcognom.netsx.es. admin.nomcognom.netsx.es. (
    1        ; sèrie: s'incrementa en cada modificació
    3600     ; refresh
    600      ; retry
    1209600  ; expire
    300      ; TTL negatiu
)

@    IN NS  dns1.nomcognom.netsx.es.
dns1 IN A   IP_ELASTICA

; Tots els serveis d'aquesta activitat apunten al mateix host.
www  IN A   IP_ELASTICA
mail IN A   IP_ELASTICA
@    IN MX  10 mail.nomcognom.netsx.es.

; Identificació de l'alumnat.
@    IN TXT "NOM_COGNOM"
```

Els registres obligatoris són:

Nom	Tipus	Valor
`dns1`	A	Elastic IP
`www`	A	Elastic IP
`mail`	A	Elastic IP
`@`	MX	`10 mail.nomcognom.netsx.es.`
`@`	TXT	Nom de l'alumne o alumna

Els noms del SOA, de l'NS i de l'MX acaben en punt perquè són FQDN. L'A de `dns1` és imprescindible: serà el *glue record* que el professorat haurà de penjar al domini pare.

6. Validar i iniciar el servei

Es valida la configuració abans de reiniciar:

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

La comprovació de zona ha d'acabar amb `OK`. Després s'activa i es reinicia el servei:

```
sudo systemctl enable named
sudo systemctl restart named
sudo systemctl status named --no-pager
```

Quan es modifique la zona, s'incrementa el número de sèrie i s'aplica el canvi amb:

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

7. Comprovar el servei des d'Internet

Des d'una altra xarxa o màquina que no siga la instància, es comproven UDP i TCP. Es reemplaça `IP_ELASTICA`:

```
dig @IP_ELASTICA nomcognom.netsx.es. SOA +norecurse +notcp
dig @IP_ELASTICA nomcognom.netsx.es. SOA +norecurse +tcp

dig @IP_ELASTICA www.nomcognom.netsx.es. A +norecurse
dig @IP_ELASTICA mail.nomcognom.netsx.es. A +norecurse
dig @IP_ELASTICA nomcognom.netsx.es. MX +norecurse
dig @IP_ELASTICA nomcognom.netsx.es. TXT +norecurse
```

Totes les respostes de la zona han de mostrar la marca `aa`, que indica resposta autoritativa. Les dues primeres han de funcionar: si falla UDP o TCP, es revisen les regles d'entrada 53 del *Security Group*, UFW i l'estat de BIND.

També es comprova que la transferència de zona està denegada:

```
dig @IP_ELASTICA nomcognom.netsx.es. AXFR
```

La resposta ha de ser `REFUSED` o bé no ha de transferir la zona.

8. Zona inversa: es treballarà posteriorment

La resolució inversa d'una IP pública d'AWS no es publica amb un fitxer BIND de la instància. El domini invers de l'Elastic IP està sota el control d'AWS, que és qui ha de gestionar el PTR.

Més endavant es configurarà correctament la part de resolució inversa o interna segons l'escenari de la pràctica. De moment, no s'ha d'intentar publicar una zona `in-addr.arpa` per a l'Elastic IP des d'aquest BIND.

9. Dades per al professorat

Una vegada totes les verificacions siguen correctes, es lliuren aquestes dades:

```
Zona: nomcognom.netsx.es.
NS: dns1.nomcognom.netsx.es.
Glue: dns1.nomcognom.netsx.es. IN A IP_ELASTICA
Elastic IP: IP_ELASTICA
```

Amb aquestes dades, el professorat podrà crear la delegació en `netsx.es`. Després de la propagació, es podrà comprovar la resolució pública sense indicar l'IP del servidor.

Referències

- Manual de BIND9: control d'accés i transferències
- Registres i fitxers de zona
- Zones, delegació i glue