9. Repàs i autoavaluació

9.1. Conceptes que cal distingir

Parella de conceptes	Diferència essencial
Domini / zona	Subarbre de noms / unitat d'autoritat que exclou les zones filles delegades.
Autoritatiu / recursiu	Publica dades pròpies / busca respostes per als clients.
Primari / secundari	Manté la font de la zona / replica la mateixa zona; tots dos són autoritatius.
Subzona / zona secundària	Una altra part de l'arbre / una còpia de la mateixa zona.
NS / A del DNS	Nom del servidor autoritatiu / adreça que permet contactar-hi.
Delegació / reenviament	Autoritat anunciada en la jerarquia / ruta de consulta particular d'un resolutor.
TTL / serial	Durada de dades en memòria cau / versió de la zona.
A / PTR	Relacions administrades en zones diferents; una no crea l'altra automàticament.
DNSSEC / HTTPS	Autenticació de dades DNS / protecció i autenticació de la connexió web.
Consulta directa / resolució pública	Contacte amb un servidor conegut / descobriment mitjançant DNS.

9.2. Preguntes per explicar amb paraules pròpies

1. En `https://www.nomcognom.netsx.es/apunts`, quina part consulta DNS i quina interpreta el servidor web?
2. Per què es va passar d'un fitxer central de noms a un sistema distribuït?
3. Pot un mateix nom tindre diverses IP? Poden diversos noms compartir IP? Quines conseqüències té per a un web?
4. Quina diferència hi ha entre la consulta del client al resolutor i les consultes del resolutor als servidors de la jerarquia?
5. Per què una resposta no autoritativa pot ser correcta?
6. Què diferencia `NXDOMAIN`, NODATA, `SERVFAIL`, `REFUSED` i un temps d'espera esgotat?
7. Per què s'han d'obrir UDP/53 i TCP/53 en el DNS públic?
8. En delegar `nomcognom.netsx.es`, quins registres controla el professorat i quins controla l'alumne?
9. Quina dependència resol el glue de `dns1.nomcognom.netsx.es`?
10. Per què `type forward` no substitueix una delegació pública?
11. Per què un segon servidor amb una zona filla no és necessàriament un servidor secundari?
12. Per què el PTR públic d'una IP d'AWS no es modifica simplement creant una zona inversa en BIND?
13. Què demostra `curl --resolve` i què continua pendent després de fer eixa prova?
14. Per què Let's Encrypt no veu una entrada del fitxer `hosts` de l'alumne?
15. Quines evidències permeten sospitar que una fallada només es produeix en la xarxa del centre?

9.3. Casos raonats

Cas A. Funciona amb la IP del DNS, però no amb el resolutor habitual

`dig @IP_DNS_ALUMNE www.nomcognom.netsx.es A` retorna la IP esperada amb `aa`. Una consulta sense servidor explícit falla.

La primera prova acredita que el servidor consultat serveix el registre. Queden pendents la delegació del pare, el glue, la visibilitat dels NS, la memòria cau i la validació del resolutor. Es consulta el pare, es fa `+trace` des d'AWS i es compara amb un resolutor recursiu. No es conclou encara que tot el DNS públic funcione.

Cas B. Es canvia una IP i uns clients encara veuen l'anterior

Es consulta directament cada autoritatiu i es compara la sèrie. Si tots tenen la nova dada, la diferència pot explicar-se per còpies en memòria cau amb TTL vigent. Si un secundari manté la dada antiga, cal revisar la transferència. Reiniciar el navegador no actualitza la còpia del resolutor extern.

Cas C. El web funciona per HTTP i el certificat no s'emet

Cal revisar el nom exacte sol·licitat, A i AAAA, accessibilitat externa del port 80, ruta del repte, VirtualHost i CAA si existeix. Un HTTP correcte només des de la pròpia màquina no demostra que la infraestructura d'ACME puga validar-lo.

Cas D. La prova falla a l'aula i funciona des de la instància web

Es conserven les dues consultes equivalents i es continua des d'AWS. Hi ha indicis d'una diferència en el camí de xarxa o en el client del centre, però encara cal verificar delegació pública i HTTPS. No es desactiva la seguretat de la infraestructura per una única prova fallida.

9.4. Llista de comprovació de la pràctica final

- [ ] S'ha acordat el nom de la subzona i s'han anotat les IP correctes.
- [ ] La zona carrega i respon SOA, NS i A amb autoritat.
- [ ] Les consultes funcionen des d'una altra instància per UDP i TCP.
- [ ] El pare publica NS i glue coherents amb el fill.
- [ ] Un resolutor extern i el recorregut de delegació arriben al registre del web.
- [ ] Els registres A/AAAA publicats corresponen a connectivitat funcional.
- [ ] El web respon al nom pel port 80.
- [ ] HTTPS funciona amb certificat vàlid per al nom, sense ignorar errors.
- [ ] S'ha comprovat la renovació automàtica.
- [ ] Les evidències indiquen origen, ordre, resultat i interpretació.
- [ ] Les diferències entre aula i AWS s'han documentat.

Les preguntes són de repàs; els requisits qualificables són els de l'enunciat de cada pràctica.

Consulta: referències i documentació de la unitat.